LANSKAP
KEAMANAN SIBER INDONESIA

2024

Id-SIRTII/CC – BSSN

Jalan Harsono RM No. 70 Ragunan.
Jakarta Selatan, 12550, Indonesia

TLP: CLEAR

LANSKAP
KEAMANAN SIBER INDONESIA
2024

Id-SIRTII/CC – BSSN

Jalan Harsono RM No. 70 Ragunan.
Jakarta Selatan, 12550, Indonesia

TLP: CLEAR

“

Ingatlah bahwa kechilafan satu orang sahaja tjukup sudah menjebabkan keruntuhan negara.

dr. Roebiono Kertopati
Bapak Persandian Indonesia

Letjen TNI (Purn)
Hinsa Siburian

> BSSN berkomitmen menjaga ruang siber nasional melalui kolaborasi dan kebijakan strategis, sebagaimana dituangkan dalam Buku Lanskap Keamanan Siber 2024 untuk mendukung transformasi digital yang aman dan berkelanjutan.

SAMBUTAN KEPALA BADAN SIBER DAN SANDI NEGARA

Sesuai dengan amanat Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yaitu untuk melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial, Badan Siber dan Sandi Negara (BSSN) melalui Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara terus berkomitmen untuk menjaga ruang siber nasional sebagai bagian integral dari upaya melindungi kedaulatan negara.

Dalam era digital yang terus berkembang, kita dihadapkan pada tantangan besar di ruang siber. Ancaman terhadap infrastruktur digital semakin meningkat seiring dengan kemajuan teknologi. Kebocoran data, serangan siber, dan eksploitasi kerentanan sistem kini menjadi isu utama yang memengaruhi berbagai sektor kehidupan, baik di tingkat individu maupun nasional. Hal ini menuntut kolaborasi strategis untuk memastikan ruang siber yang aman, andal, dan produktif.

BSSN sebagai garda terdepan dalam menghadapi ancaman siber terus mengembangkan kebijakan, standar, dan pedoman yang relevan untuk memperkuat keamanan siber nasional. Salah satunya adalah melalui Lanskap Keamanan Siber, yang kami harapkan dapat menjadi forum strategis untuk menggali wawasan, berbagi pengalaman, dan mengidentifikasi solusi inovatif bagi pengelolaan risiko dan kerentanan siber.

Buku Lanskap Keamanan Siber 2024 yang kami sajikan kali ini merupakan refleksi dari komitmen BSSN dalam menjaga ruang siber nasional. Dokumen ini tidak hanya menggambarkan tantangan yang ada, tetapi juga memberikan panduan langkah-langkah strategis dalam menghadapi dinamika ancaman yang terus berkembang. Kami mengajak seluruh pemangku kepentingan untuk bersama-sama terlibat secara langsung dan bertanggung jawab dalam menjaga keamanan siber demi mendukung transformasi digital yang aman dan berkelanjutan.

Tanggung jawab terhadap keamanan siber adalah milik kita bersama. Dengan kolaborasi yang erat antara pemerintah, sektor swasta, akademisi, dan masyarakat, saya percaya kita dapat menciptakan ruang siber yang tangguh, responsif, dan terpercaya. Semoga Lanskap Keamanan Siber 2024 ini dapat menjadi sumber pengetahuan yang berguna dan menjadi inspirasi bagi kita semua dalam menghadapi dinamika tantangan dunia maya yang semakin kompleks di masa depan.

Demikian sambutan ini saya sampaikan. Semoga Tuhan Yang Maha Kuasa senantiasa memberikan kesehatan, kekuatan, dan petunjuk kepada kita semua dalam menjalankan amanah menjaga ruang siber nasional. Mari bersama-sama kita jadikan keamanan siber sebagai prioritas dalam mendukung Indonesia yang maju, aman, dan sejahtera.

Komjen. Pol.
Albertus Rachmad Wibowo, S.I.K., M.I.K.

Percepatan transformasi digital melalui SPBE sangat penting untuk mewujudkan tata kelola pemerintahan yang baik dan pelayanan publik yang terintegrasi, namun hal ini harus diimbangi dengan penguatan keamanan siber yang memadai untuk melindungi infrastruktur vital serta menghadapi ancaman siber yang semakin kompleks dan canggih di masa depan.

SAMBUTAN WAKIL KEPALA BADAN SIBER DAN SANDI NEGARA

Dalam rangka percepatan transformasi digital yang sedang giat dilaksanakan oleh pemerintah, Sistem Pemerintahan Berbasis Elektronik (SPBE) memegang peranan penting dalam mewujudkan tata kelola pemerintahan yang baik serta pelayanan publik yang berkualitas dan terintegrasi. Integrasi ini memungkinkan konvergensi antara infrastruktur TI dan OT, serta meningkatkan interkonektivitas melalui layanan dan sistem lintas domain. Hal ini menciptakan ekosistem siber yang sangat kompleks.

Namun, harus diakui bahwa sepanjang tahun 2024, Sektor Administrasi Pemerintah masih menjadi sektor yang paling banyak terdampak oleh permasalahan keamanan siber. Hal ini menunjukkan bahwa percepatan transformasi digital yang kita lakukan belum sepenuhnya diimbangi dengan penerapan keamanan siber yang memadai. Oleh karena itu, refleksi ini menjadi pengingat bahwa transformasi digital harus disertai langkah-langkah keamanan siber yang baik. Setiap instansi perlu membangun postur keamananyang kokoh untuk mengurangi kerentanan terhadap serangan siber yang dapat mengganggu layanan publik.

Peristiwa insiden di Pusat Data Nasional Sementara (PDNS) 2 Surabaya telah memberikan pelajaran berharga kepada kita semua tentang pentingnya “Interdependent Security”. Keamanan suatu sistem atau jaringan tidak dapat dipisahkan dari elemen lain dalam ekosistem yang lebih luas. Artinya, keamanan tidak hanya bergantung pada langkah- langkah internal yang diambil oleh suatu institusi, tetapi juga pada keamanan institusi lain dalam jaringan atau ekosistem yang sama.

Dengan diterbitkannya buku "Lanskap Keamanan Siber 2024", diharapkan seluruh pihak dapat memahami dinamika perkembangan tren ancaman siber saat ini dan yang akan datang. Salah satu tren yang menonjol adalah penggunaan kecerdasan buatan untuk mengembangkan teknik serangan yang lebih rumit dan terotomatisasi. Perilaku interaksi pelaku kejahatan siber juga semakin kompleks, dengan beberapa pihak menjadikan kejahatan siber sebagai produk yang diperdagangkan atau yang kita kenal dengan istilah Cyber Crime as a Service.

Harapan kami, dengan pemahaman ini, semua pihak dapat mengambil langkah-langkah strategis dan kolaboratif dalam menghadapi tantangan keamanan siber di masa depan. Langkah-langkah ini sangat penting untuk mendukung transformasi digital yang aman dan berkelanjutan serta melindungi infrastruktur informasi vital Republik Indonesia.

MAYOR JENDERAL TNI DOMINGGUS PAKEL, S.Sos., M.M.S.I

> BSSN melalui Deputi Bidang Operasi Keamanan Siber dan Sandi berkomitmen memperkuat ketahanan siber nasional dengan menyusun Lanskap Keamanan Siber 2024 sebagai langkah strategis untuk menghadapi ancaman siber, mendukung stabilitas keamanan, dan menciptakan ekosistem digital yang aman dan tangguh bagi Indonesia.

SAMBUTAN DEPUTI BIDANG OPERASI KEAMANAN SIBER DAN SANDI

Seiring dengan semakin berkembangnya era digital, ancaman di ruang siber terus mengalami peningkatan baik dari segi kompleksitas maupun intensitas. Dalam menghadapi dinamika ini, Badan Siber dan Sandi Negara (BSSN) melalui Deputi Bidang Operasi Keamanan Siber dan Sandi terus berkomitmen untuk memperkuat ketahanan siber nasional demi mendukung stabilitas keamanan serta melindungi kepentingan masyarakat dan negara dari berbagai potensi ancaman. Melalui koordinasi yang intensif dengan berbagai pihak, Deputi Bidang Operasi Keamanan Siber dan Sandi telah meluncurkan program-program mitigasi insiden yang berbasis pada standar internasional dan praktik terbaik di bidang keamanan siber.

Sebagai wujud tanggung jawab operasional, Deputi Bidang Operasi Keamanan Siber dan Sandi telah mengarahkan penyusunan Lanskap Keamanan Siber 2024 untuk memetakan situasi keamanan siber secara strategis dan operasional sepanjang tahun 2024. Lanskap Keamanan Siber ini dirancang sebagai langkah strategis untuk mengidentifikasi ancaman siber utama, menyusun pendekatan mitigasi berbasis data, dan mendorong inovasi dalam pengelolaan risiko yang terukur, dengan mendasarkan pada evaluasi ancaman dan proyeksi tren serangan siber untuk menghadapi prediksi ancaman siber di tahun 2025.

Saya menyampaikan apresiasi yang setinggi-tingginya kepada seluruh tim yang terlibat dalam penyusunan Lanskap Keamanan Siber. Dengan penuh harap, Lanskap Keamanan Siber 2024 dapat menjadi referensi yang bermanfaat bagi seluruh pemangku kepentingan dalam menjaga keamanan ruang siber nasional. Saya percaya, dengan kepemimpinan strategis dan dukungan penuh dari seluruh pemangku kepentingan, kita dapat menciptakan ekosistem digital yang aman dan tangguh untuk menghadapi tantangan yang ada. Semoga Tuhan Yang Maha Esa senantiasa memberikan kekuatan dan petunjuk kepada kita semua dalam menjaga kedaulatan ruang siber Indonesia. Mari bersama-sama kita wujudkan ruang siber yang tangguh, dan mendukung kemajuan bangsa.

Andi Yusuf, M.T.

Direktorat Operasi Keamanan Siber berkomitmen mendukung BSSN melalui penyusunan Lanskap Keamanan Siber 2024 sebagai panduan strategis untuk menghadapi ancaman siber yang dinamis, meningkatkan kesiapan nasional, dan mendorong kolaborasi lintas elemen dalam menjaga ruang siber Indonesia.

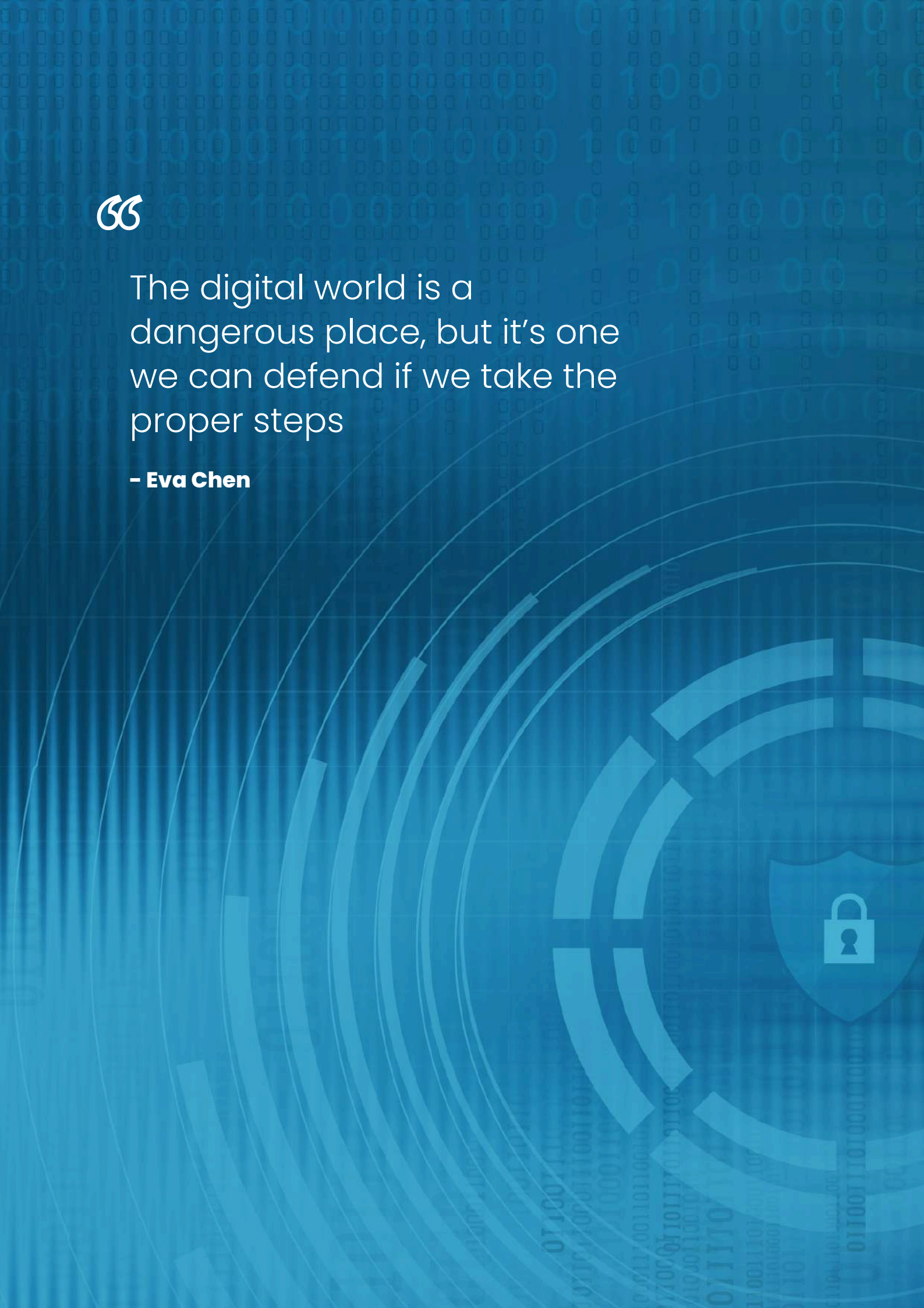
SAMBUTAN DIREKTUR OPERASI KEAMANAN SIBER

Marilah kita panjatkan puji syukur ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya sehingga kita dapat menyelesaikan penyusunan Lanskap Keamanan Siber Tahun 2024 dengan baik. Sebagai bagian dari Direktorat Operasi Keamanan Siber, kami terus berkomitmen mendukung Badan Siber dan Sandi Negara (BSSN) dalam menjalankan amanat yang tertuang dalam Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021. Dalam kerangka tugas tersebut, kami telah melaksanakan berbagai langkah strategis untuk memantau, menganalisis, dan meningkatkan kesiapan Indonesia menghadapi ancaman siber yang semakin dinamis di tahun 2024.

Di tahun ini, serangan siber yang menargetkan berbagai sektor penting nasional terus meningkat. Hal ini menuntut perhatian lebih besar dalam penerapan inovasi teknologi keamanan siber, serta peningkatan koordinasi dalam melaksanakan kebijakan teknis di bidang operasi keamanan siber. Sebagai wujud tanggung jawab, Lanskap Keamanan Siber Tahun 2024 ini disusun untuk memberikan gambaran menyeluruh tentang kondisi ruang siber Indonesia pada periode tahun ini.

Kami berharap Lanskap Keamanan Siber ini tidak hanya menjadi referensi penting dalam menentukan arah kebijakan strategis negara, tetapi juga menjadi panduan bagi masyarakat, organisasi, dan industri dalam menghadapi ancaman siber. Kolaborasi semua elemen bangsa sangatlah diperlukan untuk menjaga integritas ruang siber nasional dari berbagai risiko yang ada.

Rasa terima kasih saya sampaikan kepada seluruh pihak yang telah berkontribusi dalam penyusunan Lanskap Keamanan Siber Tahun 2024. Diharapkan, penyusunan Lanskap Keamanan Siber ini dapat bermanfaat dalam meningkatkan kesadaran dan ketahanan siber kita bersama. Semoga Tuhan Yang Maha Kuasa senantiasa memberikan kekuatan dan perlindungan kepada kita dalam menjalankan tugas untuk bangsa dan negara.



The digital world is a dangerous place, but it's one we can defend if we take the proper steps

– Eva Chen

LANSKAP KEAMANAN SIBER INDONESIA 2024

Oleh Direktorat Operasi Keamanan Siber

Dokumen Lanskap Keamanan Siber Indonesia 2024 merupakan kajian komprehensif di berbagai aspek penting dalam keamanan siber di Indonesia selama 2024. Dokumen ini memberikan wawasan dan membantu pemangku kepentingan dapat proaktif dalam membangun strategi pertahanan siber yang efektif.

DAFTAR ISI

RINGKASAN

Total trafik anomali di Indonesia selama tahun **2024** adalah **330.527.636** anomali dengan jenis trafik anomali tertinggi yaitu Mirai Botnet dengan total sebanyak 81.286.596 aktivitas. Mirai Botnet merupakan salah satu jenis Botnet yang menargetkan perangkat *Internet of Things* (IoT) dan dibuat untuk melakukan serangan *Distributed Denial of Service* (DDoS) pada situs *web* atau layanan *online*, sehingga mengakibatkan adanya gangguan atau *downtime*. Pada tahun 2024 Terdapat **2.487.041** aktivitas ***Advanced Persistent Threat* (APT), 514.508** aktivitas ***Ransomware*** dan **26.771.610 aktivitas *phishing*.** BSSN telah mengirimkan **1.367** notifikasi indikasi insiden ke *stakeholder* dengan jenis notifikasi terbanyak dikirimkan adalah ***Data Breach***. Adapun pengelompokan sektor dilakukan berdasarkan Peraturan Presiden No. 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV). Berdasarkan hasil pemantauan dan analisis *Cyber Threat Intelligence*, BSSN juga melakukan penelusuran dugaan insiden siber dengan jumlah total **241 dugaan insiden kebocoran data**. Hasil penelusuran pada *darknet*, ditemukan adanya **56.128.160** temuan ***data exposure*** yang berdampak pada 461 *stakeholder* di Indonesia. Pada kasus ***web defacement*** ditemukan sebanyak **5.780 kasus** yang menargetkan beberapa domain dan sebanyak **4.071 *web defacement*** terkait judi online yang menargetkan situs pemerintah. Berdasarkan laporan yang diterima dari *stakeholder* pada layanan aduan siber, diperoleh sebanyak **1.814 aduan** pada tahun 2024.

BSSN telah mempublikasikan **51 imbauan keamanan**. Salah satu Top CVE global berdasarkan skor *Common Vulnerability Scoring System* (CVSS) yang memiliki tingkat dampak *Critical* yaitu CVE-2024-3400 yang memungkinkan *threat actor* untuk mencuri informasi, memasang *malware*, atau mengganggu operasi penting pada sistem. Sedangkan, salah satu Top CVE nasional berdasarkan jumlah *hit* terbanyak di Indonesia yaitu CVE-2024-23897 yang menyebabkan pengungkapan informasi sensitif, *Server-Side Request Forgery* (SSRF), serta eksekusi skrip lokal untuk mengendalikan server atau meningkatkan hak akses pada sistem. Selain itu, BSSN melakukan pengujian kerentanan sistem elektronik melalui kegiatan *IT Security Assessment* (ITSA). Berdasarkan hasil pengujian, ditemukan sebanyak **1.931 kerentanan** yang terdiri dari 256 kerentanan *critical*, 405 kerentanan *high*, 350 kerentanan *medium*, 621 kerentanan *low*, serta 299 kerentanan *info* pada 462 aplikasi yang menjadi target ITSA, mencakup aplikasi web, *mobile*, maupun infrastruktur.

BSSN telah melaksanakan **76 kegiatan asistensi tanggap insiden siber** di 66 stakeholder. Kategori pelaksanaan asistensi tanggap insiden siber yaitu proses asistensi dilakukan secara penuh oleh BSSN, proses asistensi dilakukan secara penuh oleh PSE/CSIRT, dan proses asistensi dilakukan oleh PSE/CSIRT bekerja sama dengan BSSN. Oleh karena itu, disusun lesson learned 5 (lima) jenis kasus terbanyak berdasarkan asistensi tanggap insiden siber yaitu *Data Breach*, *Illegal Access*, *Web defacement*, *Ransomware*, dan *Distributed Denial of Service* (DDoS). Secara umum, dalam rangka mengantisipasi dan mencegah terjadinya insiden siber, maka langkah yang dapat dilakukan di antaranya *security hardening* pada sistem operasi server, pembaruan sistem dan perangkat lunak, menetapkan kebijakan penggunaan *password* yang kuat sesuai standar, edukasi *security awareness* kepada pengguna, dan lain-lain.

BSSN juga melakukan kolaborasi dengan berbagai *stakeholder* di Indonesia serta aktif mengikuti forum-forum internasional untuk meningkatkan keamanan siber sebagai upaya untuk menjaga ruang siber Indonesia. Kolaborasi yang dilakukan oleh BSSN meliputi nasional sebanyak 9 *event*, internasional 26 *event*, dan kompetisi internasional 4 *event*. Kerja sama lain yang dilakukan adalah seperti layanan Honeynet antara BSSN dengan Swiss-German University (SGU) dan Komunitas Indonesia Honeynet Project (IHP). Selain itu, BSSN juga melaksanakan kerja sama Laboratorium Forensik Digital untuk mendukung pelaksanaan forensik digital pada bidang insiden keamanan siber.

BSSN melaksanakan amanat Rancangan Pembangunan Jangka Menengah Nasional (RPJMN) dan Rencana Strategis Tahun 2020-2024 dengan melaksanakan kegiatan *National Cyber Exercise*. Kegiatan ini diikuti 7.121 peserta dari 1.174 instansi. *National Cyber Exercise* terbagi menjadi 3 (tiga) kegiatan besar yaitu *Cross Sectoral Cyber Exercise*, *Table Top Exercise*, dan *CSIRT Day*. Puncak dari rangkaian kegiatan *National Cyber Exercise* adalah *CSIRT Day* yang diikuti oleh peserta yang berasal dari pengelola CSIRT Indonesia dengan total 614 peserta dari 176 instansi. Kegiatan ini mencerminkan pentingnya sinergi antar organisasi dalam memperkuat keamanan siber melalui kolaborasi yang efektif.

Berdasarkan analisis BSSN diperoleh beberapa potensi ancaman siber bersifat sosial maupun teknis yang diprediksi akan muncul di tahun 2025. Potensi ancaman siber bersifat sosial antara lain: Pornografi, Judi Online, *Scam Online*, Penyebaran Konten Terorisme, Disinformasi dan Misinformasi, Penyalahgunaan AI. Potensi ancaman siber bersifat teknis antara lain: *Web defacement*, *AI Powered Cyber Threat*, *Phishing*, *Trojan dan Malware*, *Advanced Persistent Threat* (APT), *Denial of Service* (DoS), Ransomware, dan *Stolen Credential Data*.

PROFIL DIREKTORAT OPERASI KEAMANAN SIBER

BADAN SIBER DAN SANDI NEGARA

Berdasarkan Peraturan Presiden Nomor 53 Tahun 2017

Badan Siber dan Sandi Negara (BSSN) merupakan hasil dari penggabungan beberapa entitas pemerintah sebelumnya, antara lain Lembaga Sandi Negara (Lemsaneg), Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika (Kemenkominfo), serta Indonesia *Security Incident Response Team on Internet Infrastructure* (Id-SIRTII). Proses penggabungan ini diwujudkan melalui Peraturan Presiden Nomor 53 tahun 2017 tentang BSSN.

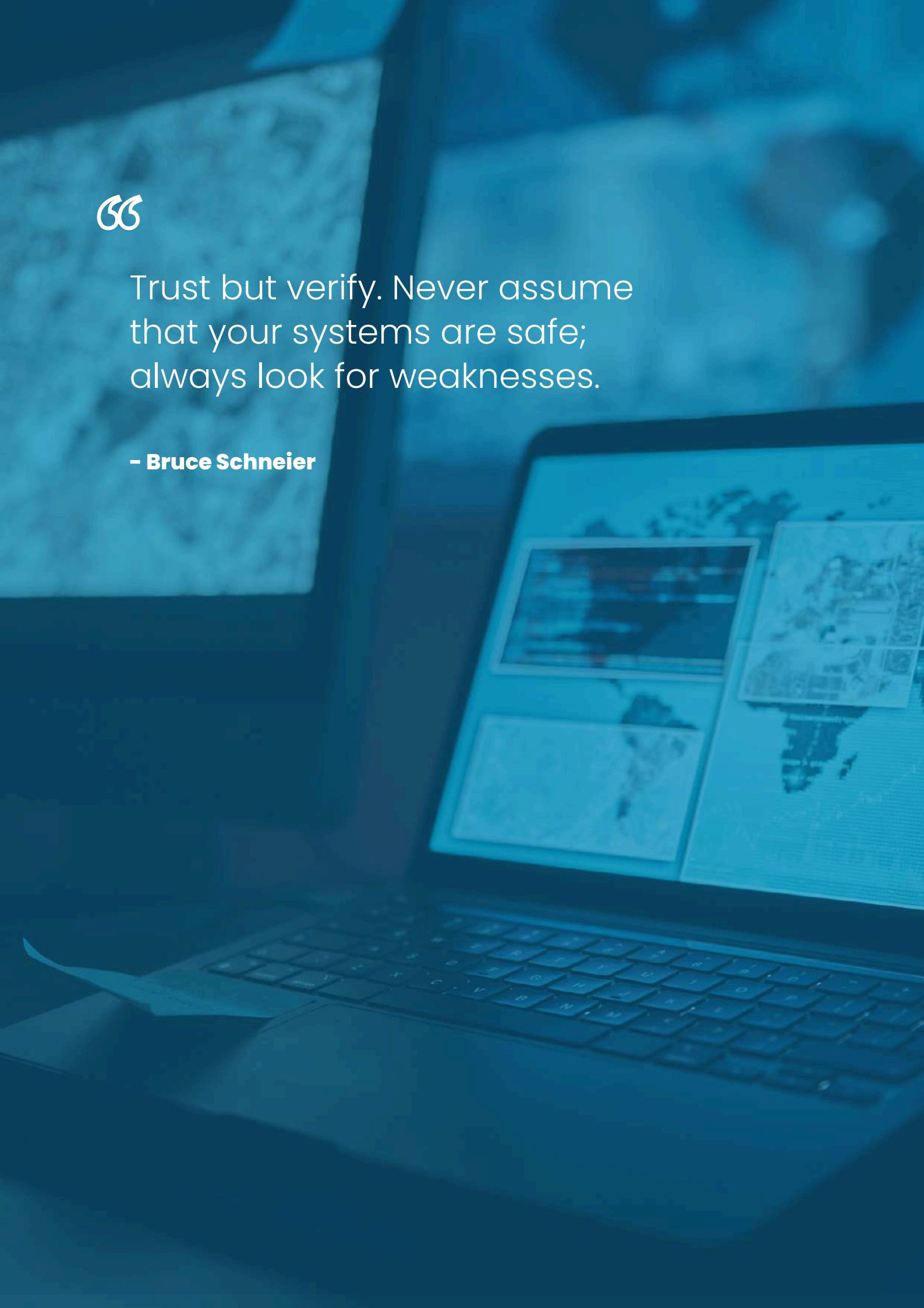
DIREKTORAT OPERASI KEAMANAN SIBER

Berdasarkan Peraturan Presiden Nomor 28 Tahun 2021

Presiden Republik Indonesia, Joko Widodo, menandatangani Peraturan Presiden (Perpres) Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (BSSN) pada tanggal 13 April 2021. Penerbitan Perpres ini didasarkan pada kebutuhan untuk merancang kembali struktur organisasi BSSN, dengan tujuan mencapai keamanan, perlindungan, dan kedaulatan siber nasional. Selanjutnya, organisasi dan tata kerja BSSN dijelaskan lebih lanjut dalam Peraturan BSSN Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja BSSN.

Direktorat Operasi Keamanan Siber merupakan bagian dari Deputi Bidang Operasi Keamanan Siber dan Sandi di lingkungan Badan Siber dan Sandi Negara. Direktorat Operasi Keamanan Siber bertanggung jawab untuk melakukan koordinasi, merumuskan, dan melaksanakan kebijakan teknis di sektor operasi keamanan siber. Direktorat Operasi Keamanan Siber melaksanakan fungsi-fungsi berikut:

- Penyiapan perumusan kebijakan teknis operasional di bidang identifikasi, proteksi, deteksi, penanggulangan, dan pemulihan
- Penyelenggaraan koordinasi dan implementasi identifikasi, proteksi, deteksi, penanggulangan, dan pemulihan
- Pengelolaan tanggap insiden siber nasional dan sektor pemerintah, kontak siber nasional, serta pengelolaan krisis siber nasional
- Pengelolaan informasi mengenai ancaman siber secara proaktif dan analisis *big data* serta analisis *malware*
- Pendukung penyidikan, forensik digital, dan memberikan bantuan sebagai ahli dalam kasus keamanan siber
- Pelaksanaan pemantauan, evaluasi, dan pelaporan di bidang operasi keamanan siber
- Pelaksanaan urusan perencanaan, keuangan, rumah tangga, kepegawaian, ketatalaksanaan, persuratan, kearsipan, serta penyusunan evaluasi dan pelaporan.


Trust but verify. Never assume that your systems are safe; always look for weaknesses.
- Bruce Schneier

01

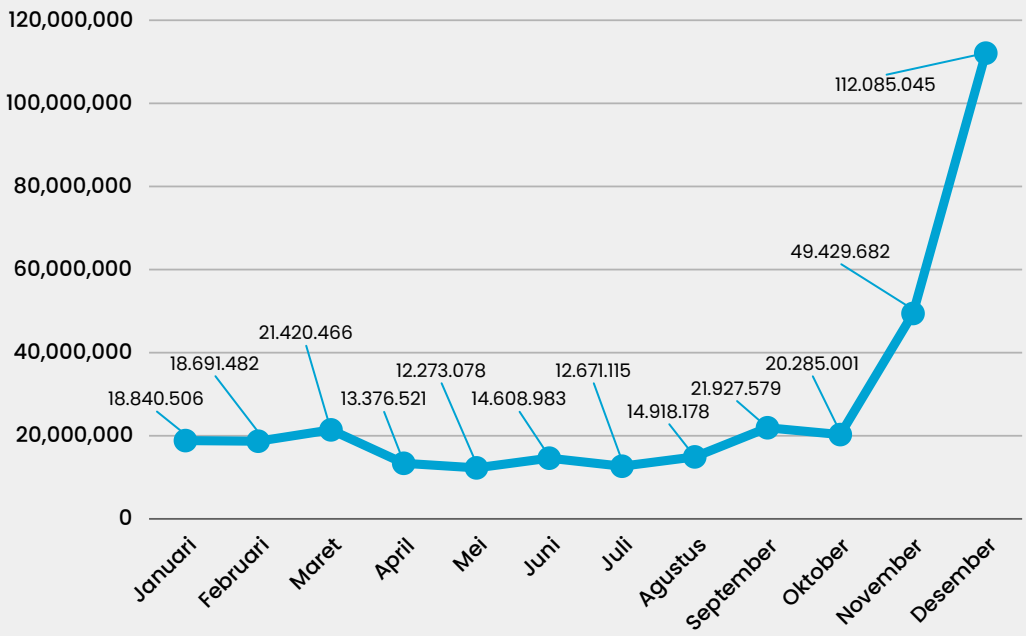
TREN TRAFIK ANOMALI

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2024

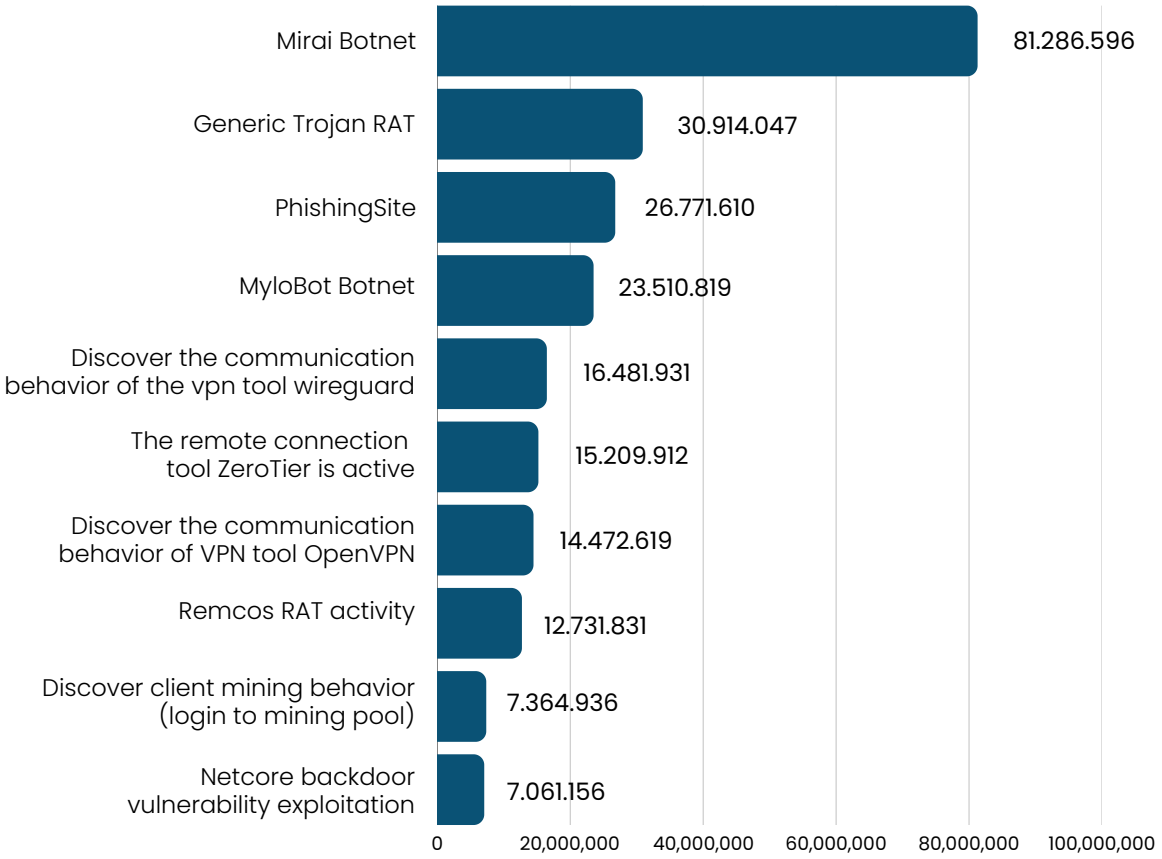
TRAFIK ANOMALI SERANGAN SIBER DI INDONESIA

330.527.636
Total Trafik Anomali

Total trafik anomali di Indonesia pada tahun 2024 adalah **330.527.636 anomali**. Anomali trafik tertinggi terjadi pada bulan Desember dengan jumlah **112.085.045 anomali**, sedangkan anomali terendah terjadi pada bulan Mei dengan jumlah **12.273.078 anomali**. Aktivitas anomali trafik ini dapat berdampak pada penurunan performa perangkat dan jaringan, pencurian data sensitif, hingga perusakan reputasi dan penurunan kepercayaan terhadap suatu organisasi. Berikut merupakan grafik trafik anomali pada tahun 2024:



TOP 10 TRAFIK ANOMALI



01 MIRAI BOTNET

Mirai Botnet adalah salah satu jenis *botnet* yang menargetkan perangkat *Internet of Things* (IoT). *Botnet* ini dibuat untuk melakukan serangan *Distributed Denial of Service* (DDoS) pada situs web atau layanan *online*, sehingga mengakibatkan adanya gangguan atau *downtime*. Mirai Botnet bekerja dengan melakukan identifikasi perangkat IoT yang memiliki *password default* atau yang mudah ditebak. Setelah itu, Mirai akan memanfaatkan kelemahan tersebut untuk menginfeksi perangkat dan menambahkannya ke dalam *botnet*. Perangkat-perangkat yang terinfeksi kemudian dapat dikendalikan oleh *threat actor* dan digunakan untuk meluncurkan serangan DDoS. Mirai Botnet dapat mengakibatkan penurunan performa atau kerusakan pada perangkat yang terinfeksi dan kerusakan reputasi akibat penggunaan perangkat terinfeksi untuk aktivitas berbahaya. Sebagai bentuk upaya pencegahan, pengguna disarankan untuk melakukan penggantian *password default* dengan *password* yang sesuai standar keamanan, memperbarui *firmware* pada perangkat IoT, melakukan segmentasi jaringan antara jaringan utama dan perangkat IoT, menonaktifkan fitur yang tidak diperlukan pada IoT, dan melakukan pemantauan keamanan secara berkelanjutan.

02 GENERIC TROJAN RAT

Generic Trojan RAT adalah *signature* yang mengindikasikan adanya aktivitas *backdoor communication* menuju domain *malicious* yang terindikasi sebagai *command and control server* milik *threat actor*. Aktivitas ini berpotensi digunakan untuk melakukan berbagai kegiatan mencurigakan seperti pencurian informasi, penghapusan data, pemblokiran, penyalinan informasi, serta menjalankan program pada perangkat yang terinfeksi di luar kehendak pengguna. Generic Trojan RAT menargetkan komputer dengan sistem operasi Windows dan dapat menyebar melalui tautan pada e-mail, tautan pada pesan singkat, pengunduhan melalui drive, ataupun dibawa oleh *malware* yang lebih dahulu menginfeksi perangkat. Perangkat yang terinfeksi Generic Trojan RAT akan menjalankan program pada *background process* tanpa diketahui oleh pengguna. Hal ini dapat berdampak pada pelambatan kinerja sistem, pengubahan konfigurasi, dan perangkat akan lebih sering menampilkan pesan *error*. Sebagai bentuk upaya pencegahan, pengguna disarankan untuk melakukan pembaruan sistem operasi dan semua perangkat lunak yang diinstal, menggunakan perangkat antivirus yang selalu diperbarui secara berkala, menggunakan aplikasi asli yang diunduh dari sumber resmi, serta selalu berhati-hati saat membuka lampiran atau menerima file dan saat mengklik tautan dari suatu halaman situs web.

03 PHISHINGSITE

PhishingSite merupakan salah satu aktivitas infeksi *malware* yang dilakukan dengan memanfaatkan situs *phishing*. Situs *phishing* merupakan situs web palsu yang diciptakan untuk menipu pengguna agar memberikan informasi pribadi, seperti *password* atau rincian keuangan. Situs palsu ini sering kali menggunakan tautan yang didistribusikan melalui *e-mail phising* yang tampak meyakinkan. PhishingSite meningkatkan risiko keamanan dengan menggabungkan serangan *phishing,* potensi pengunduhan, dan instalasi *malware* pada perangkat korban. Pihak-pihak yang ditargetkan adalah individu, perusahaan, dan organisasi yang tidak waspada terhadap ancaman siber yang dapat mengekspos data sensitif dan merusak integritas sistem. Dampak dari PhishingSite adalah pencurian identitas, akses ilegal ke akun korban, pencurian informasi akun keuangan, dan potensi kerusakan pada perangkat atau jaringan yang terinfeksi *malware*. Sebagai bentuk upaya pencegahan, pengguna disarankan untuk tidak sembarang mengklik tautan dari *e-mail* yang mencurigakan, selalu melakukan verifikasi keaslian situs web sebelum memasukkan informasi sensitif, dan melakukan pembaruan perangkat antivirus secara berkala.

06 THE REMOTE CONNECTION TOOL ZEROTIER IS ACTIVE

Peringatan ini merujuk pada aktivitas penggunaan *tool remote connection* ZeroTier pada sistem atau jaringan. ZeroTier adalah salah satu solusi VPN berjenis *mesh* yang memungkinkan pengguna untuk membuat jaringan pribadi virtual (VPN) secara instan dan aman melalui internet. Dalam konteks keamanan siber, ZeroTier yang aktif dalam kondisi tidak dikenali oleh *administrator* sistem dapat menjadi indikasi adanya aktivitas mencurigakan atau potensi ancaman, misalnya mungkin telah menginstal ZeroTier pada sistem tanpa sepengetahuan pengguna untuk mendapatkan akses jarak jauh. Sebagai bentuk upaya pencegahan, pengguna disarankan mengimplementasikan pemantauan aktif terhadap aktivitas jaringan terkait ZeroTier, melakukan konfigurasi *firewall* sesuai dengan standar keamanan, mengaktifkan *logging* yang rinci, melakukan segmentasi jaringan, menggunakan ZeroTier dengan menerapkan mekanisme autentikasi yang kuat dan terbatas hanya kepada pengguna yang membutuhkan akses jarak jauh, serta melakukan pembaruan perangkat lunak secara rutin.

07 DISCOVER THE COMMUNICATION BEHAVIOR OF VPN TOOL OPENVPN

Trafik anomali ini berkaitan dengan pendeteksian penggunaan protokol *Virtual Private Network* (VPN) pada aplikasi OpenVPN. OpenVPN merupakan aplikasi berbasis *open-source* yang menggunakan protokol VPN untuk menciptakan *private tunnel* terenkripsi untuk terhubung ke internet. OpenVPN akan membuat koneksi dengan menggunakan *Point to Point* (PTP) *Tunnel* yang telah dienkripsi menggunakan *username* dan *password*. Aplikasi ini sebenarnya legal, namun saat ini *threat actor* dapat menyisipkan *malware* ke dalam aplikasi OpenVPN dan memanfaatkannya untuk melakukan spionase pada perangkat korban. Selain itu, node pada jaringan publik yang digunakan sebagai *relay agent* VPN seringkali merupakan Alamat IP yang memiliki reputasi buruk. Sebagai bentuk upaya pencegahan, pengguna diharapkan dapat melakukan pemantauan aktif terhadap lalu lintas jaringan OpenVPN, melakukan konfigurasi *firewall* yang baik dan *logging* yang intensif, menerapkan kebijakan otorisasi pengguna yang ketat, melakukan segmentasi jaringan serta audit keamanan secara rutin, dan menggunakan aplikasi OpenVPN versi terbaru yang diunduh dari sumber resmi.

04 MYLOBOT BOTNET

Mylobot Botnet adalah salah satu jenis *botnet* yang menargetkan sistem operasi Windows. *Botnet* ini menyebar melalui spam *e-mail* ataupun unduhan file yang telah terinfeksi, dan memiliki kemampuan sebagai gerbang untuk mengunduh muatan (*payload*) tambahan dari *server Command and Control* (C2) dan menginstalnya pada perangkat korban. Setelah terinstal pada perangkat korban, *botnet* akan menonaktifkan Windows Defender dan Windows Update sehingga berpotensi untuk mengambil kendali penuh atas sistem pengguna. Perilaku umum MyloBot adalah melakukan *callback* ke sejumlah domain yang dihasilkan oleh *Domain Generation Algorithm* (DGA). DGA menjadi salah satu metode yang digunakan untuk mempersulit kegiatan deteksi terhadap aktivitas *malware* karena dapat menghasilkan nama domain yang variatif dengan karakteristik dan pola penamaan yang acak dalam jumlah besar. Mylobot juga memiliki teknik anti-VM dan anti-*sandboxing* yang canggih untuk menghindari deteksi dari proses analisis. Sebagai bentuk upaya pencegahan, pengguna disarankan untuk melakukan *update* sistem dan antivirus yang digunakan secara berkala, melakukan pencadangan data secara berkala, menggunakan *password* yang kuat, menghindari akses terhadap situs web atau domain yang tidak terpercaya, dan menghindari mengunduh serta membuka *e-mail* dari alamat pengirim yang tidak dikenal.

05 DISCOVER THE COMMUNICATION BEHAVIOR OF THE VPN TOOL WIREGUARD

Wireguard merupakan salah satu *tool* VPN yang digunakan untuk membuat komunikasi secara *private* antara 2 (dua) *endpoint* yang terhubung melalui suatu jaringan secara cepat dan efisien. Namun, terdapat beberapa kerentanan yang ditemukan dalam Wireguard, salah satunya adalah kerentanan CVE-2023-35838 yang merujuk pada kerentanan dimana klien Wireguard 0.5.3 pada Windows mengkonfigurasi sistem operasi dan *firewall* dengan cara yang tidak aman sehingga lalu lintas ke jaringan lokal yang menggunakan alamat IP non-RFC1918 diblokir. Hal ini memungkinkan untuk memanipulasi korban agar memblokir lalu lintas IP ke alamat IP dan layanan tertentu bahkan saat VPN diaktifkan. Kerentanan lain yang ditemukan adalah CVE-2019-14899 yang memungkinkan *threat actor* untuk mengendalikan tautan pada layer 2 (*data link layer*) dan mengirim paket khusus ke perangkat korban untuk secara aktif memeriksa beberapa properti dari koneksi TCP yang berasal dari perangkat korban. Perlu diperhatikan bahwa terdeteksinya penggunaan Wireguard tidak secara otomatis mengindikasikan adanya ancaman, karena banyak organisasi dan individu menggunakan Wireguard untuk tujuan yang sah, seperti akses jarak jauh ke server atau jaringan. Oleh karena itu, penting untuk memahami konteks dan konfigurasi spesifik sistem atau jaringan sebelum menentukan apakah aktivitas ini merupakan ancaman. Sebagai bentuk upaya pencegahan, pengguna disarankan melakukan konfigurasi pada *firewall* untuk mengontrol lalu lintas dan menerapkan enkripsi yang kuat pada protokol Wireguard, melakukan pemantauan aktif terhadap lalu lintas jaringan, melakukan audit konfigurasi secara berkala, menerapkan autentikasi ganda untuk lapisan keamanan tambahan, melakukan pembaruan perangkat lunak secara rutin, mengaktifkan *logging* yang rinci, dan menerapkan segmentasi jaringan.

08 REMCOS RAT

Remcos RAT adalah *Remote Access Trojan* (RAT) yang pertama kali ditemukan pada tahun 2016. Pada awalnya Remcos merupakan *legitimate software* yang digunakan untuk melakukan *penetration testing*, tetapi Remcos memiliki kemampuan berbahaya dan telah digunakan dalam berbagai *hacking campaigns*. Remcos sering digunakan untuk melakukan serangan seperti pencurian data dan pembuatan *botnet*. Ramcos biasanya menyebar melalui lampiran berbahaya pada *email phising* yang biasanya berbentuk *file* Microsoft Office. *Trojan* ini memiliki berbagai kemampuan seperti mencuri data, mengunggah dan mengunduh file, mengambil tangkapan layar, mengambil alih *webcam*, serta melakukan *keylogging*. Setelah menginfeksi korban, Ramcos akan melakukan perubahan pada *registry* untuk mempertahankan keberadaannya. Untuk mengelabuhi perangkat keamanan, Ramcos melakukan teknik *obfuscated* dengan menggunakan algoritma enkripsi RC4 dan Base64. Remcos dapat melakukan pendeteksian lingkungan virtualisasi atau *sandbox* dengan tujuan menghindari deteksi.

09 DISCOVER CLIENT MINING BEHAVIOR (LOGIN TO MINING POOL)

Trafik anomali ini merujuk pada pendeteksian perilaku komunikasi antara perangkat lunak *mining* dengan *mining pool*. Komunikasi tersebut bertujuan untuk *login* ke *mining pool* dan memulai proses *mining cryptocurrency*. Apabila proses *mining* tersebut bukan merupakan proses yang legal, maka terdapat kemungkinan bahwa perangkat korban sudah terinfeksi malware *mining*. Hal tersebut mengakibatkan *threat actor* dapat menggunakan perangkat korban untuk melakukan *mining cryptocurrency* secara ilegal. Sumber daya *Central Processing Unit* (CPU) dan *Graphical Processing Unit* (GPU) pada perangkat korban akan digunakan secara berlebihan sehingga dapat mengurangi kinerja perangkat dan menyebabkan kerusakan. Sebagai bentuk upaya pencegahan, pengguna diharapkan dapat melakukan pemblokiran pada koneksi yang ilegal, menerapkan segmentasi jaringan, melakukan pembaruan keamanan secara rutin, dan melakukan pemantauan keamanan secara berkelanjutan.

10 NETCORE BACKDOOR VULNERABILITY EXPLOITATION

Trafik anomali ini berkaitan dengan pendeteksian proses eksploitasi Netcore Backdoor Vulnerability. Netcore Backdoor Vulnerability merujuk pada kerentanan yang ditemukan pada beberapa router Netcore yang memungkinkan *threat actor* untuk mendapatkan akses root pada perangkat korban. *Threat actor* melakukan eksploitasi kerentanan ini dengan mengirimkan perintah khusus melalui *port* UDP 53413. Setelah terhubung, *threat actor* menggunakan string autentikasi *hard-coded* atau kredensial yang sudah tertanam dalam *firmware* dan tidak bisa diubah oleh pengguna untuk mendapatkan akses *root*. Hal tersebut mengakibatkan *threat actor* dapat memiliki akses penuh pada perangkat korban sehingga *threat actor* dapat mengubah konfigurasi pada *router*, mengakses data sensitif, memasukkan perangkat korban pada *botnet*, dan melakukan serangan lanjutan. Sebagai bentuk upaya pencegahan, pengguna diharapkan dapat melakukan pemblokiran pada akses eksternal ke Port UDP 53413, menerapkan segmentasi jaringan, melakukan pembaruan pada *firmware* yang rentan, dan melakukan pemantauan keamanan secara berkelanjutan.

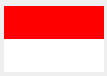
TOP 10

SUMBER DAN TUJUAN ANOMALI

Berdasarkan hasil deteksi trafik anomali, didapatkan alamat IP sumber dan tujuan anomali yang dapat menunjukkan dari negara mana anomali berasal dan ke negara mana anomali ditujukan.

Adapun negara-negara yang terdeteksi sebagai sumber anomali belum dapat dipastikan sebagai negara asal anomali karena *threat actor* berpotensi menggunakan alamat IP tersebut sebagai *proxy* untuk menyembunyikan atau menyamarkan alamat IP asli *threat actor*.

TOP 10 SUMBER ANOMALI


Indonesia
164.432.795

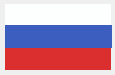

Amerika Serikat
20.606.740


Singapura
4.821.163


Bulgaria
3.776.822


Belanda
3.214.422


Tiongkok
2.615.326


Rusia
1.810.428


Jerman
1.592.177


Hong Kong
1.462.164


Romania
1.182.215

TOP 10 TUJUAN ANOMALI


Indonesia
194.562.390


Amerika Serikat
30.670.349


Jerman
17.644.837


Hong Kong
11.232.698


Singapura
10.221.545


Irlandia
8.592.002


Prancis
8.416.562


Britania Raya
5.567.376

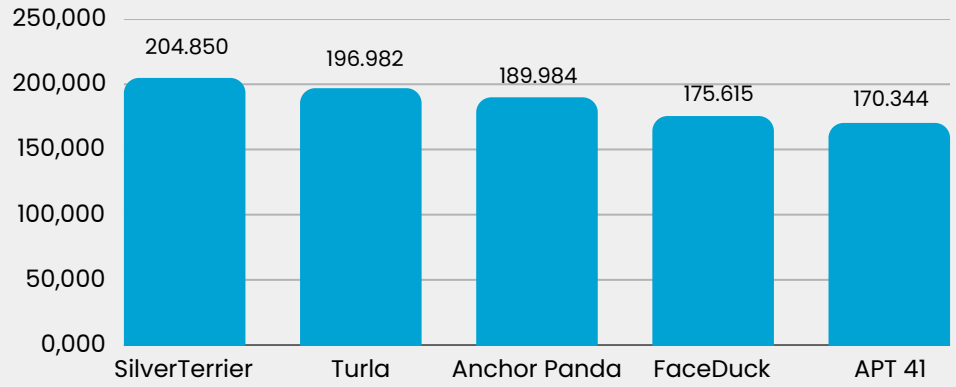

Belanda
4.321.678


India
3.120.616

ADVANCED PERSISTENT THREAT

2.487.041
Aktivitas APT di Indonesia

Advanced Persistent Threat (APT) merupakan *attack campaign* yang dilakukan oleh kelompok serangan siber atau *threat actor* yang memiliki keterkaitan (*state-sponsored*) ataupun tidak berkaitan (*non-state sponsored*) dengan negara tertentu. *Threat actor* ini menggunakan berbagai metode dan teknik canggih yang dirancang untuk melakukan serangan siber secara terus-menerus tanpa terdeteksi perangkat keamanan untuk mendapatkan akses ke sistem dan bertahan dalam sistem tersebut dalam jangka waktu yang lama. Tujuan kelompok serangan siber ini adalah mengakses, memantau, dan mengumpulkan informasi dari sistem atau jaringan target untuk melakukan pencurian data yang bernilai seperti informasi rahasia perusahaan, data keuangan, atau rancangan teknologi tinggi dengan tujuan eksploitasi jangka panjang. Berikut grafik 5 APT yang paling banyak ditemukan pada ruang siber Indonesia:



TOP 5 ADVANCED PERSISTENT THREAT

01 SILVERTERRIER

SilverTerrier merupakan APT yang diindikasikan berasal dari Nigeria dan telah aktif sejak tahun 2014. APT tersebut menargetkan berbagai organisasi sepeti teknologi, Pendidikan tinggi, dan manufaktur. Dalam melakukan operasinya, SilverTerrier menggunakan skema BEC (*Business Email Compromise*) yaitu *threat actor* menyamar sebagai pihak yang sah untuk menipu karyawan atau individu lainnya dalam organisasi. Skema BEC biasanya dilakukan dengan mengirimkan email yang terlihat sah yang berisi permintaan untuk melakukan pengiriman dana atau pemberian data *sensitive*. SilverTerrier menggunakan beberapa jenis *malware* seperti Agent Tesla, DarkComet, Lokibot, NanoCore, dan NETWIRE. Dalam melakukan komunikasi antara sistem korban dengan C2 *server*, SilverTerrier menggunakan protokol umum seperti HTTP (*Hypertext Transfer Protocol*) untuk menyembunyikan lalu lintas komunikasi pada aktivitas web yang sah, FTP (*File Transfer Protocol*) untuk mentransfer *file* dan memungkinkan akses jarak jauh, serta SMTP (*Simple Mail Transfer Protocol*) untuk mengirimkan perintah atau menerima *respons* melalui *email*. Tujuan utama dari APT ini adalah untuk mendapatkan keuntungan finansial. Mitigasi yang dapat dilakukan untuk mencegah atau meminimalisir dampak dari APT SilverTerrier diantaranya adalah sebagai berikut:

- Melakukan pemantauan aktivitas pada sistem dan jaringan untuk mendeteksi adanya aktivitas berbahaya;
- Memastikan *email* yang diterima berasal dari sumber yang sah untuk mencegah infeksi awal dari *threat actor*.

02 TURLA

Turla merupakan APT yang diindikasikan berasal dari Rusia. APT tersebut menargetkan berbagai sektor seperti pemerintahan, militer, kedutaan besar, pendidikan, penelitian, dan komersial dengan tujuan untuk mengumpulkan informasi intelijen.APT ini biasanya melakukan infeksi awal melalui *spearphising* dan *watering hole attack*. Pada kasus *spearphising*, Turla mengirimkan email pada target dengan lampiran berupa file berbahaya. Sedangkan pada kasus watering *hole attack*, Turla menginfeksi korban saat korban mengunjungi situs web yang telah dimodifikasi. Untuk mendukung operasinya, Turla menggunakan *WordPress* atau *Virtual Private Server* (VPS) yang telah disusupi sebagai server *command and control* (C2). Selain itu, Turla juga mengembangkan malware khusus dan memodifikasi *tools* yang tersedia di publik. Mitigasi yang dapat dilakukan untuk mencegah atau meminimalisir dampak dari APT Turla diantaranya adalah sebagai berikut:

- Melakukan pemantauan aktivitas pada sistem dan jaringan untuk mendeteksi adanya aktivitas berbahaya;
- Menerapkan *Multi-Factor Authenticaition* (MFA) dan menggunakan *password* yang sesuai standar keamanan untuk mengurangi risiko penyalahgunaan kredensial;
- Melakukan *update* keamanan pada aplikasi yang memiliki kerentanan agar tidak dieksploitasi oleh *threat actor*;
- Memastikan situs web yang dikunjungi dan email yang diterima berasal dari sumber yang sah untuk mencegah infeksi awal dari *threat actor*.
- Melakukan manajemen akun dengan hak istimewa dengan menerapkan prinsip *least privilege* untuk menghindari penyalahgunaan.

03 ANCHOR PANDA

Anchor Panda juga dikenal sebagai APT 14, merupakan kelompok serangan siber yang diindikasikan berelasi dengan Tiongkok. Kelompok ini diketahui aktif sejak tahun 2012 dan dikenal dengan keterlibatannya dalam aktivitas serangan yang terkoordinasi dan bertarget tinggi. Anchor Panda menargetkan entitas maritim dan kelautan, membawa dampak signifikan pada industri pelayaran, pembangkit listrik, dan teknologi kelautan. Modus operandi kelompok ini melibatkan penggunaan teknik serangan canggih, seperti *spear-phishing*, eksploitasi kerentanan perangkat lunak, dan penggunaan *malware* khusus yang dirancang untuk menyusup dan bertahan dalam jangka waktu yang panjang. *Malware* yang digunakan oleh Anchor Panda antara lain Gh0st RAT, Poison Ivy, dan Torn RAT. Anchor Panda dikenal karena tujuannya yang berkaitan dengan intelijen dan ekonomi. Ancaman dari APT Anchor Panda tidak hanya mencakup risiko pencurian data sensitif, tetapi juga spionase industri yang dapat mengguncang fondasi teknologi dan ekonomi, serta risiko kerahasiaan nasional. Mitigasi yang dapat dilakukan untuk menghindari serangan APT Anchor Panda adalah sebagai berikut:

- Melakukan pemantauan aktivitas pada sistem dan jaringan untuk mendeteksi adanya aktivitas berbahaya;
- Melakukan *update* keamanan pada aplikasi yang memiliki kerentanan agar tidak dieksploitasi oleh *threat actor*;
- Memastikan *e-mail* yang diterima berasal dari sumber yang sah untuk mencegah infeksi awal dari *threat actor*.

04 FACEDUCK

FaceDuck merupakan APT yang diindikasikan berasal dari Vietnam. Kelompok ini diketahui sudah aktif sejak tahun 2021 dan menggunakan *malware* Ducktail Infostealer sebagai senjata utamanya. Penyebaran *malware* Ducktail dilakukan menggunakan format ZIP yang di-*hosting* pada file *sharing platform* dengan menyamar sebagai aplikasi *crack* atau versi gratis dari aplikasi populer seperti Microsoft Office dan *game*. Setelah berhasil menginfeksi, Malware Ducktail akan mencuri berbagai data sensitif seperti kredensial *login*, informasi pribadi, dan akun *wallet cryptocurrency*. Data yang dicuri kemudian dikirim ke *server* C2 melalui saluran HTTP. Mitigasi yang dapat dilakukan untuk mencegah atau meminimalisir dampak dari FaceDuck adalah sebagai berikut:

- Melakukan pemantauan aktivitas pada sistem dan jaringan untuk mendeteksi adanya aktivitas berbahaya;
- Memastikan seluruh perangkat lunak yang digunakan merupakan perangkat lunak yang sah atau bukan merupakan perangkat lunak bajakan.

05 APT 41

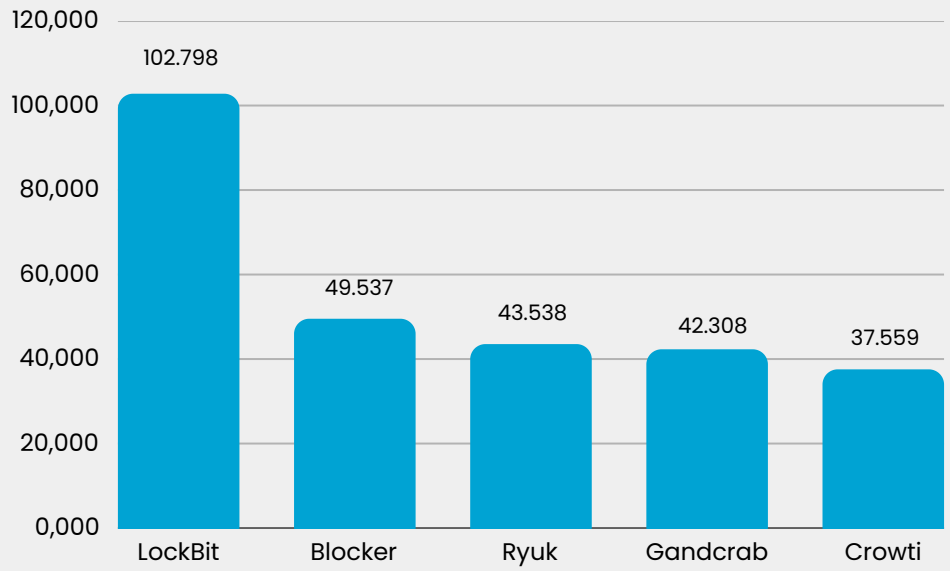
APT 41 merupakan APT yang berasal dari Tiongkok dan memiliki tujuan untuk melekukan spionase dan memperoleh keuntungan finansial. Target utama APT41 meliputi organisasi multinasional, lembaga pemerintah, dan perusahaan yang memiliki data sensitif. APT ini mampu menyusup ke jaringan korban dan mempertahankan akses untuk jangka waktu yang lama. APT 41 biasanya mengawali serangan dengan melakukan eksploitasi kerentanan perangkat lunak yang memungkinkan untuk masuk ke sistem. Selain itu, APT ini juga menggunakan *spearphishing* untuk mengirim *e-mail* yang mengandung *malware* atau tautan berbahaya kepada korban tertentu. Untuk mendukung operasinya, APT 41 menggunakan *tools* publik seperti Mimikatz dan BadPotato. Selain itu APT ini juga melakukan pencurian sertifikat untuk menandatangani *malware* yang mereka gunakan. Mitigasi yang dapat dilakukan untuk mencegah atau meminimalisir dampak dari APT 41 adalah sebagai berikut:

- Melakukan pemantauan aktivitas pada sistem dan jaringan untuk mendeteksi adanya aktivitas berbahaya;
- Melakukan *update* keamanan pada aplikasi yang memiliki kerentanan agar tidak dieksploitasi oleh *threat actor*;
- Memastikan *e-mail* yang diterima berasal dari sumber yang sah untuk mencegah infeksi awal dari *threat actor*;
- Menggunakan fungsi hash yang kuat untuk menyimpan *password* pada sistem untuk melindungi pencurian kredensial.
- Melakukan manajemen akun dengan hak istimewa dengan menerapkan prinsip least *privilege* untuk menghindari penyalahgunaan.

AKTIVITAS RANSOMWARE

514.508
Aktivitas Ransomware

Ransomware adalah jenis *malware* yang digunakan untuk menyandera aset korban, seperti dokumen, sistem, ataupun perangkat. Setelah aset terenkripsi, korban akan diminta membayar tebusan untuk mendekripsi dan kembali mendapatkan akses pada aset. *Ransomware* menargetkan individu, perusahaan, organisasi, bahkan Pemerintah. Dampak *ransomware* dapat berupa kehilangan akses terhadap data, kerugian finansial, hingga penurunan reputasi. Berikut adalah 5 r*ansomware* yang paling banyak ditemukan pada ruang siber Indonesia berdasarkan hasil monitoring trafik anomali:



TOP 5 RANSOMWARE

01 LockBit

LockBit adalah jenis *malware* berbahaya yang melakukan enkripsi data korban dan meminta tebusan Bitcoin. LockBit disebarkan melalui *e-mail phishing*, tautan berbahaya, atau penggunaan perangkat lunak yang rentan. Jika tebusan tidak dibayarkan, maka data korban akan dipublikasikan atau dihapus.

02 Blocker

Blocker Ransomware merupakan jenis *malware* yang bertujuan untuk mengganggu fungsi normal sistem operasi. Ransomware ini menyebar melalui iklan *malicious* dan email *phishing*. Setelah menginfeksi perangkat korban, *malware* ini dapat memblokir *editor registry*, menampilkan jendela yang tidak dapat ditutup, mengubah *wallpaper desktop*, dan mengunci layar. Selain itu, *ransomware* ini juga dapat mengenkripsi file pengguna sehingga tidak dapat diakses, setelah itu *threat actor* akan meminta tebusan untuk mendekripsi file milik pengguna.

03 Ryuk

Ryuk merupakan jenis *ransomware* yang pertama kali ditemukan pada Agustus 2018. Proses penyebaran Ryuk biasanya dilakukan melalui *malware* Trickbot atau Emotet yang didistribusikan melalui *e-mail phising*. Setelah berhasil menginfeksi korban, *threat actor* akan melakukan *lateral movement* untuk menanamkan Ryuk pada berbagai perangkat di jaringan. Ryuk akan melakukan enkripsi *file* pada perangkat yang terinfeksi dan mengubahnya menjadi *file* dengan ekstensi .RYK. Namun Ryuk tidak bisa melakukan enkripsi pada *file* sistem penting seperti .exe, .dll, dan .hrmlog.

04 GandCrab

GandCrab pertama kali muncul pada Januari 2018 dan sempat menjadi salah satu *ransomware* paling aktif di dunia. *Ransomware* ini menargetkan pengguna Windows dengan metode penyebaran melalui *e-mail phishing*, tautan berbahaya, atau penggunaan perangkat lunak yang rentan. *Ransomware* ini melakukan enkripsi file dengan algoritma RSA dan AES. Jika tebusan tidak dibayarkan dalam waktu tertentu, data korban akan dihapus.

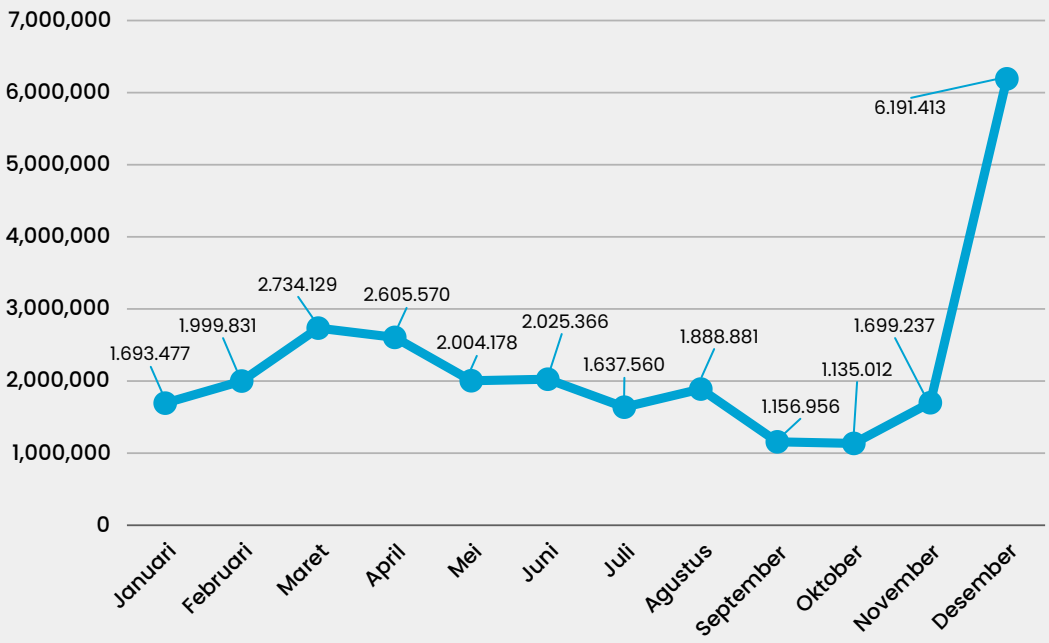
05 Crowti

Crowti merupakan jenis *ransomware* yang melakukan enkripsi pada file kemudian meminta tebusan untuk melakukan dekripsi. *Ransomware* ini masuk ke sistem dengan cara diunduh oleh *malware* lain atau diunduh tanpa disadari oleh pengguna saat mengunjungi stus berbahaya. Untuk mempertahankan keberadaannya, Crowti melakukan perubahan *registry* agar dapat dijalankan secara otomatis setelah perangkat dihidupkan kembali. Crowti juga melakukan tindakan perlindungan dengan mengapus dirinya sendiri setelah dieksekusi.

AKTIVITAS PHISHING

26.771.610
Aktivitas Phishing

Phishing merupakan metode serangan siber yang dilakukan dengan menggunakan teknik rekayasa sosial untuk menyamar sebagai entitas yang terpercaya. Metode ini biasanya dilakukan melalui *e-mail*, pesan teks, atau situs web palsu yang berisi lampiran atau tautan berbahaya. *Phishing* bertujuan agar korban mengakses lampiran atau tautan berbahaya tersebut sehingga program berbahaya akan tereksekusi pada perangkat korban. Total aktivitas yang diindikasikan sebagai *phishing* di Indonesia pada tahun 2024 adalah **26.771.610 aktivitas**. Jumlah aktivitas *phishing* tertinggi terjadi pada bulan Desember sebesar **6.191.413 aktivitas**, sedangkan jumlah terendah terjadi pada bulan Oktober sebesar **1.135.012 aktivitas**. *Phishing* dapat menjadi pintu masuk bagi *malware* atau akses tidak sah lainnya ke sistem yang berpotensi mengakibatkan serangan lanjutan. Berikut merupakan grafik aktivitas *phishing* tahun 2024:



02

REKAPITULASI NOTIFIKASI DAN DUGAAN INSIDEN SIBER

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2024

PENGIRIMAN NOTIFIKASI TAHUN 2024

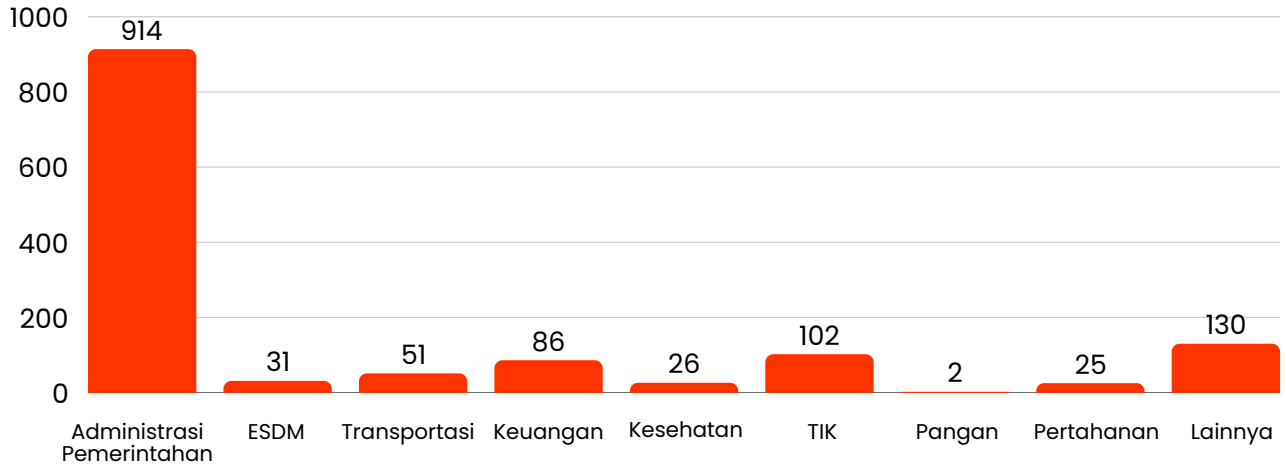
1.367
NOTIFIKASI TERKIRIM

58%
NOTIFIKASI DIRESPON

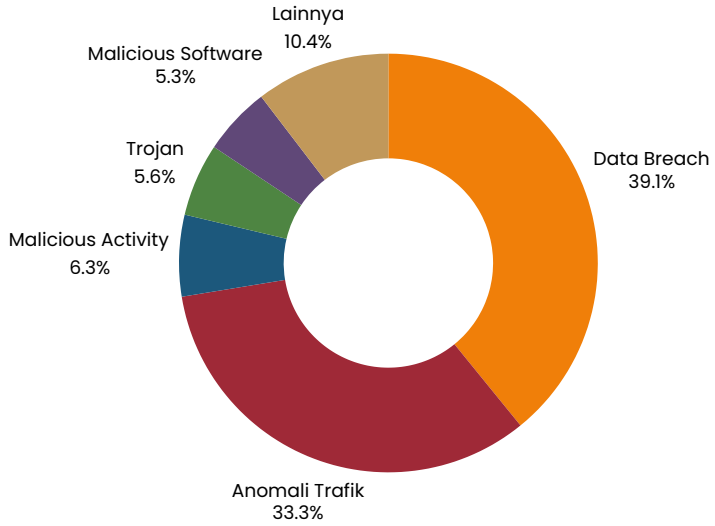
42%
NOTIFIKASI TIDAK DIRESPON

Tim Pusat Kontak Siber BSSN telah mengirimkan sebanyak **1.367 notifikasi** indikasi insiden siber ke berbagai sektor. Sebanyak **58%** atau **797 notifikasi** sudah direspon oleh stakeholder dan sebanyak **42%** atau **570 notifikasi** tidak direspon.

REKAPITULASI NOTIFIKASI BERDASARKAN SEKTOR



REKAPITULASI NOTIFIKASI BERDASARKAN KLASIFIKASI INDIKASI INSIDEN



Dari 1.367 Notifikasi terkirim, didapatkan hasil Top 5 Klasifikasi Indikasi Insiden yang dinotifikasi oleh BSSN yaitu *Data Breach* sebanyak 535, Anomali Trafik sebanyak 455, *Malicious Activity* sebanyak 86, Trojan sebanyak 77, dan *Malicious Software* sebanyak 72.

CYBER THREAT INTELLIGENCE

593
DUGAAN INSIDEN SIBER

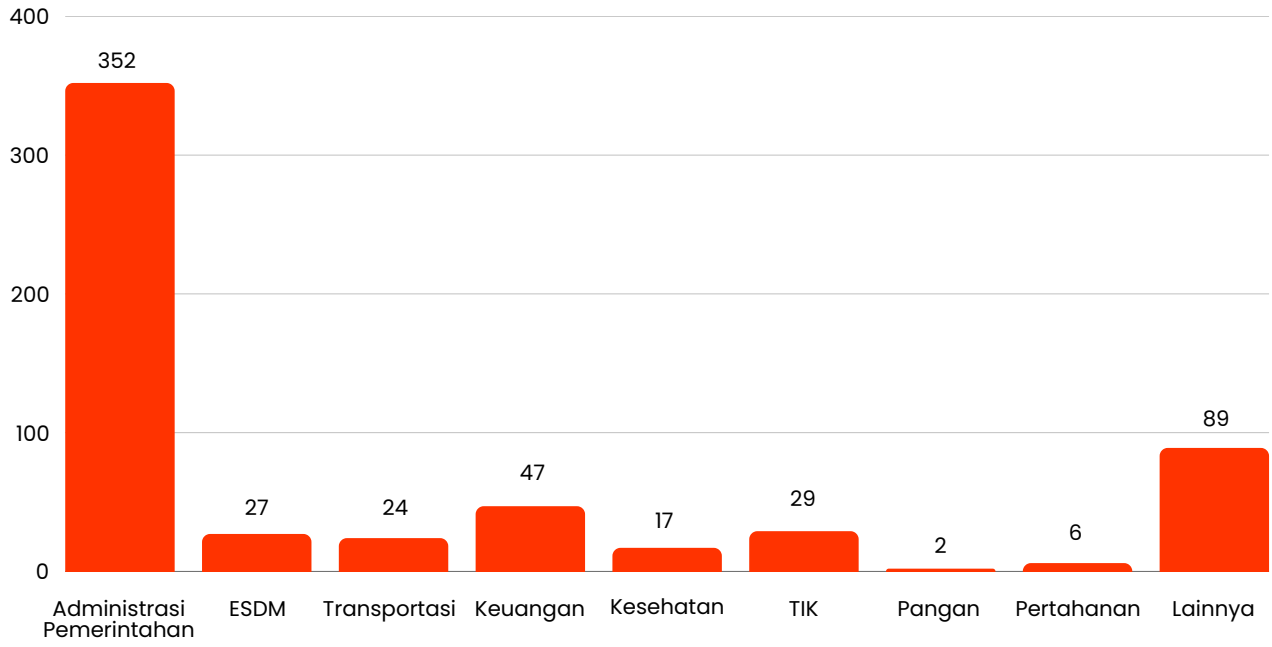
Hasil pemantauan *Cyber Threat Intelligence* (CTI) ditemukan sebanyak **593 dugaan insiden siber** di antaranya yaitu kebocoran data, *ransomware*, *web defacement*, indikasi potensi serangan DDoS, dan pemantauan proaktif dugaan insiden siber.

243
PENELUSURAN DUGAAN INSIDEN

350
PEMANTAUAN PROAKTIF DUGAAN INSIDEN

Penelusuran insiden siber merupakan upaya pendalaman terhadap temuan indikasi dugaan insiden siber yang telah terpublikasi melalui forum dan media pada *surface web*, *deepweb*, dan *darkweb*, seperti publikasi dugaan kebocoran data dan publikasi *ransomware*. Pemantauan proaktif dugaan insiden siber merupakan pemantauan secara proaktif terhadap dugaan insiden siber pada *darkweb* seperti *data exposure* yang disebabkan oleh *malware stealer*, informasi potensi serangan siber pada forum *hacking discussion*, serta informasi IoC dan TTP dari *state sponsored threat actor*.

REKAPITULASI DUGAAN INSIDEN SIBER BERDASARKAN SEKTOR



DARKNET EXPOSURE

Darknet exposure merupakan kondisi ketika terdapat data/informasi kredensial akun pada suatu instansi/organisasi tertentu yang terekspos di *darknet*, baik itu pada forum jual beli data, forum diskusi *hacker*, maupun pada *instant messaging*, sehingga berpotensi dapat disalahgunakan oleh pihak yang tidak berkepentingan. *Darknet exposure* dapat disebabkan adanya infeksi *malware stealer* pada perangkat pengguna, ataupun disebabkan adanya pencurian/*dump database* suatu organisasi.

56.128.160

TEMUAN DATA EXPOSURE

Telah ditemukan sebanyak **56.128.160 temuan** *data exposure* dari 461 instansi terdampak selama periode 2024. Dari data tersebut diketahui persentase paling tinggi terdapat pada sektor Administrasi Pemerintahan, yaitu sebesar 58,34% dari keseluruhan *data exposure*, kemudian sektor Lainnya sebesar 30,14%, sektor Keuangan sebesar 3,58%, sektor TIK sebesar 2,73%, sektor Transportasi sebesar 2,70%, sektor ESDM sebesar 1,88%, sektor Kesehatan sebesar 0,34%, sektor Pangan sebesar 0,19%, dan sektor Pertahanan sebesar 0,11%.

REKAPITULASI DARKNET EXPOSURE 2024

Sektor	Jumlah Data Exposure	Jumlah Instansi
Adm. Pemerintahan	32.746.601	141
Lainnya	16.918.536	51
Keuangan	2.007.935	71
TIK	1.530.780	40
Transportasi	1.514.236	51
ESDM	1.052.765	47
Kesehatan	189.863	29
Pangan	106.055	21
Pertahanan	61.389	10

Rekomendasi yang dapat diterapkan terkait dengan ancaman pencurian kredensial pengguna antara lain yaitu dengan menerapkan manajemen akun pengguna, *Restrict File and Directory Permissions*, kebijakan *password* terkait kombinasi karakter, tidak menggunakan akun/kredensial dinas untuk kepentingan selain kedinasan, dan segmentasi jaringan, serta melakukan himbauan pergantian *password* kepada setiap individu.

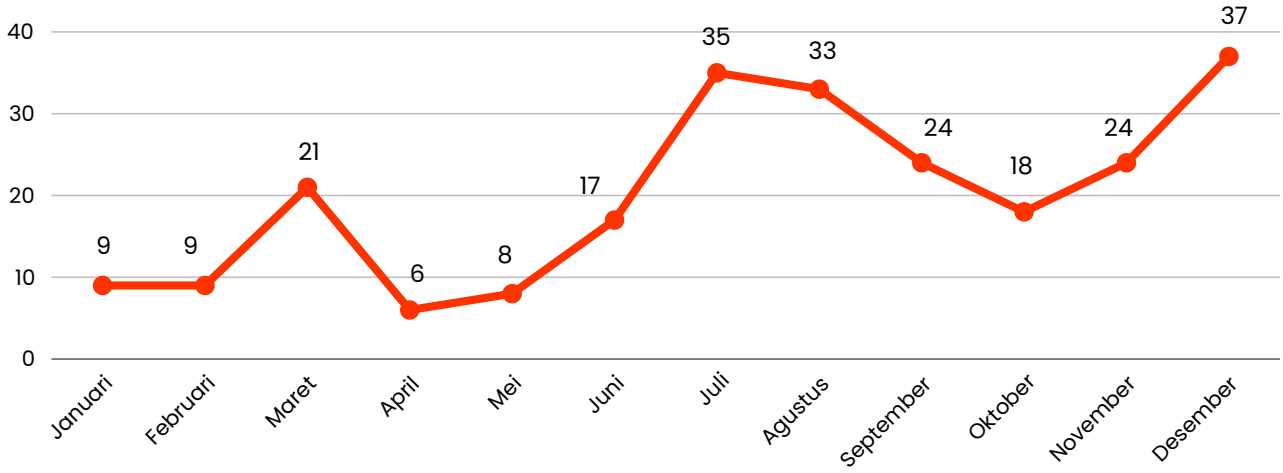
REKAPITULASI DUGAAN KEBOCORAN DATA

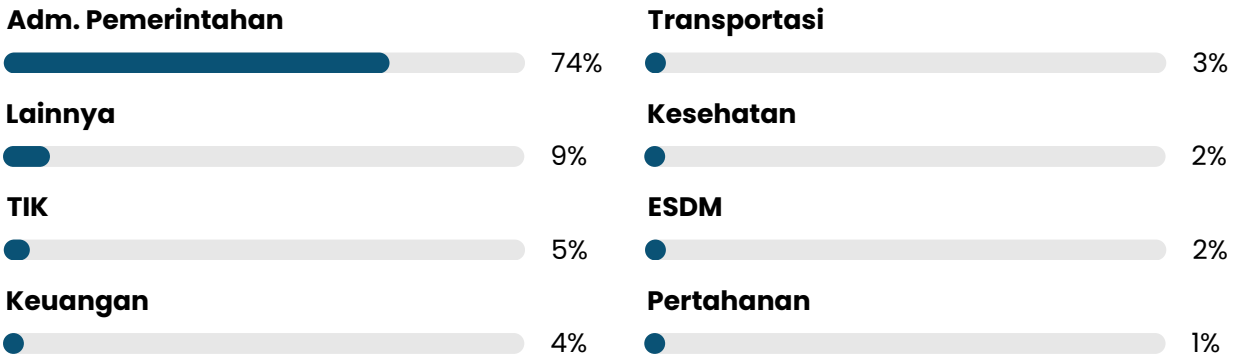
241 DUGAAN INSIDEN KEBOCORAN DATA

199 STAKEHOLDER SUDAH RESPON

Pada periode 2024, tim BSSN berhasil melakukan deteksi terhadap **241 dugaan** insiden kebocoran data. Dugaan insiden kebocoran data tertinggi terjadi pada bulan Desember 2024 sebanyak **37 dugaan insiden**. Sebanyak **199 respon** telah diberikan oleh *stakeholder* terhadap notifikasi yang diberikan.

REKAPITULASI NOTIFIKASI DUGAAN KEBOCORAN DATA 2024





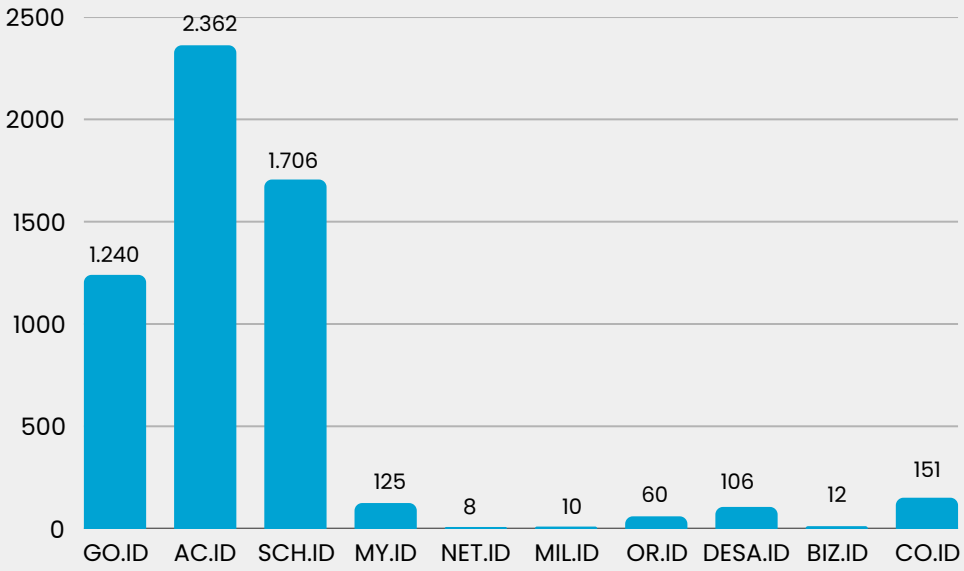
Sektor Administrasi Pemerintahan tercatat memiliki jumlah dugaan insiden terbanyak dengan total 183 dugaan insiden. Kemudian Lainnya dengan 21 dugaan insiden, sektor Teknologi Informasi dan Komunikasi dengan tercatat memiliki 11 dugaan insiden. Sektor Keuangan dengan 9 dugaan insiden, sektor Transportasi dengan 7 dugaan insiden. Sementara itu, sektor Kesehatan 5 dugaan insiden, sektor Energi dan Sumber Daya Mineral 3 dugaan insiden, dan sektor Pertahanan dengan 2 dugaan insiden. Data ini menunjukkan bahwa sektor Administrasi Pemerintahan merupakan area yang paling banyak terdampak, yang memerlukan perhatian khusus dalam manajemen risiko dan peningkatan keamanan siber.

WEB DEFACEMENT

5.780
Dugaan Web Defacement

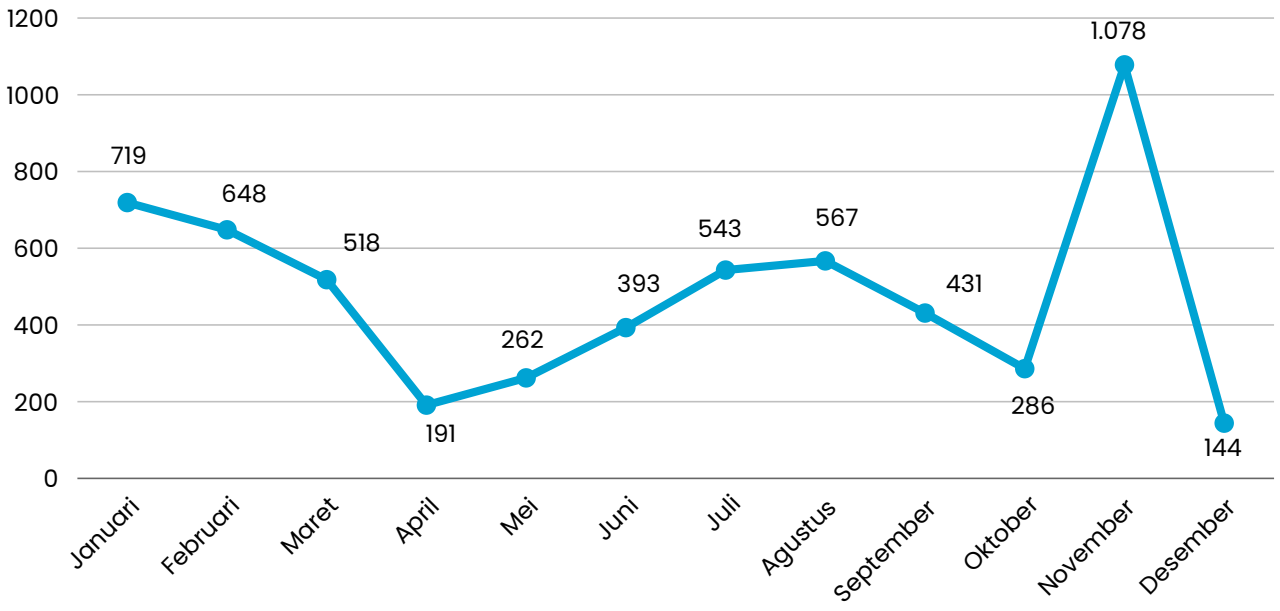
Serangan *web defacement* merupakan serangan yang dilakukan untuk mengeksploitasi situs web atau *server web* yang rentan dengan memanfaatkan kerentanan dari sistem sehingga *threat actor* dapat merusak, memodifikasi, atau menghapus konten halaman web yang telah diretas. Pelaku serangan *web defacement* disebut sebagai *defacer*. Terdapat **5.780** dugaan *web defacement* yang terdeteksi berdasarkan pemantauan dari sumber terbuka, seperti yang ditunjukkan pada grafik berikut:

GRAFIK DOMAIN TERDAMPAK



> Every company should assume that it is a target for cyber-attacks, and it's up to them to put systems in place to protect themselves.
>
> **- John W. Thompson**

GRAFIK SEBARAN KASUS DUGAAN WEB DEFACEMENT



Berdasarkan grafik di atas diperoleh informasi puncak tertinggi *web defacement* terjadi pada bulan November sebanyak **1.078 dugaan insiden**. Aktivitas serangan ini menunjukkan tren fluktuatif sepanjang tahun, dengan jumlah tertinggi di awal tahun sebanyak 719 dugaan insiden dan kembali melonjak tajam menjelang akhir tahun. Penurunan signifikan terlihat pada bulan April sebanyak 191 dugaan insiden yang merupakan titik terendah, diikuti oleh pola kenaikan yang beragam hingga Agustus. Data ini mengindikasikan potensi peningkatan kerentanan situs web pada periode tertentu, terutama menjelang akhir tahun, yang perlu diantisipasi dengan langkah mitigasi keamanan siber yang lebih kuat.

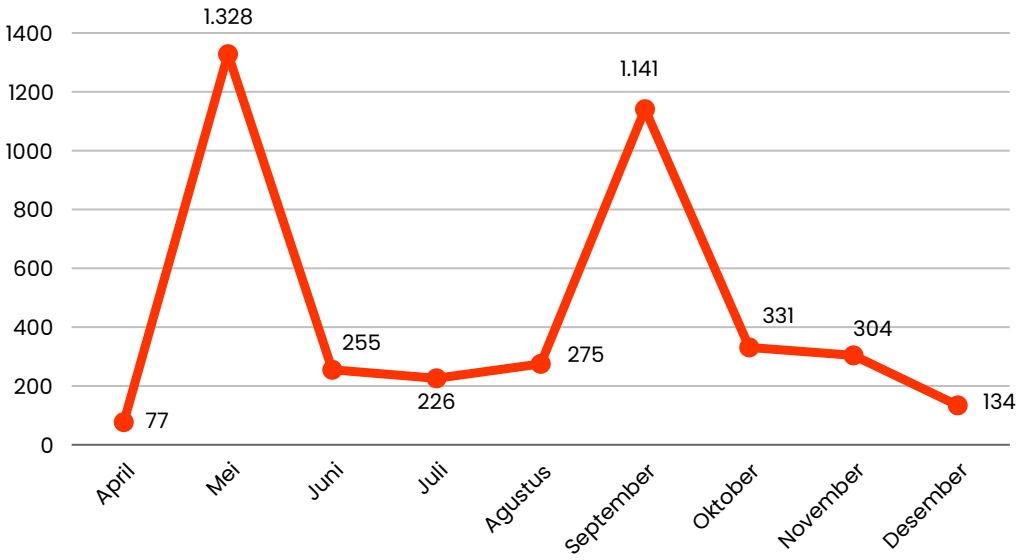
WEB DEFACEMENT SLOT JUDI ONLINE

4.071
WEB DEFACEMENT

Ditemukan sebanyak **4.071 dugaan *web defacement* judi online** yang menargetkan situs pemerintah. Deteksi ini menggunakan metode *dorking* yang dimulai pada bulan April 2024.

Website yang tersisipi konten judi online merupakan situs web resmi yang telah disusupi oleh pihak tidak bertanggung jawab untuk menyematkan tautan, skrip, atau konten yang mengarahkan pengguna ke *platform* perjudian daring. Penyusupan ini biasanya terjadi melalui celah keamanan pada sistem, seperti kerentanan pada *Content Management System* (CMS), *plugin*, atau kurangnya pembaruan perangkat lunak. Dampak dari penyusupan ini dapat mencoreng reputasi instansi pemerintah dan membahayakan keamanan data pengunjung situs.

GRAFIK TEMUAN DUGAAN WEB DEFACEMENT JUDI ONLINE



Metode pendeteksian sistus pemerintah yang menjadi korban penyusupan judi online menggunakan metode *dorking*. Metode *dorking* yaitu teknik pencarian menggunakan kata kunci dan operator khusus di Google untuk menemukan halaman yang mencurigakan atau terindikasi mengandung konten judi online. Kata kunci disusun berdasarkan pola umum dari situs judi online, seperti penggunaan istilah tertentu atau struktur URL yang spesifik. Hasil pencarian dianalisis untuk mengidentifikasi anomali pada situs pemerintah. Temuan dari proses ini dicatat dan dilaporkan kepada pihak terkait dengan rekomendasi tindakan mitigasi guna meningkatkan keamanan situs.

PENCEGAHAN WEB DEFACEMENT

Berikut merupakan langkah-langkah utama yang direkomendasikan untuk mencegah *web defacement*. Implementasi langkah-langkah ini akan meningkatkan ketahanan sistem terhadap ancaman siber.

01 Security Hardening

Security hardening adalah proses mengurangi potensi risiko keamanan pada sistem atau perangkat dengan mengonfigurasi dan mengurangi adanya kemungkinan kerentanan yang ditimbulkan. Ini mencakup langkah-langkah seperti menonaktifkan fitur yang tidak diperlukan, memperbarui perangkat lunak, dan mengonfigurasi pengaturan sistem agar lebih aman.

02 Autentikasi Pengguna

Autentikasi pengguna adalah proses verifikasi identitas pengguna sebelum diberikanya akses ke sistem atau aplikasi. Ini umumnya melibatkan penggunaan *username* dan *password*, untuk meningkatkan keamanan dapat juga digunakan metode tambahan seperti otentikasi dua faktor (2FA) atau biometrik.

03 Centralized Log Collector

Centralized log collector adalah sistem yang mengumpulkan, menyimpan, dan mengelola *log* dari berbagai perangkat atau aplikasi dalam satu tempat. Tujuan utamanya adalah untuk memudahkan pemantauan dan analisis, serta mendeteksi insiden atau ancaman keamanan dengan cara yang lebih efisien.

04 Vulnerability Scanning

Vulnerability scanning adalah proses pemindaian otomatis untuk mengidentifikasi kerentanan dalam sebuah sistem, aplikasi, atau jaringan. Alat pemindai ini mencari celah atau kerentanan yang bisa dieksploitasi oleh penyerang, memungkinkan organisasi untuk segera memperbaiki masalah tersebut.

05 Patching

Patching adalah proses memperbarui perangkat lunak atau sistem untuk memperbaiki kerentanannya. Ini dilakukan dengan menginstal pembaruan (*patch*) yang dirilis oleh pengembang untuk mengatasi *bug*, masalah keamanan, atau perbaikan lainnya guna memastikan sistem tetap aman dan berfungsi dengan baik.

> The most significant cyber threat that we face is not the one coming from criminal hackers, but from inside our organizations.

- Kevin Mitnick

03

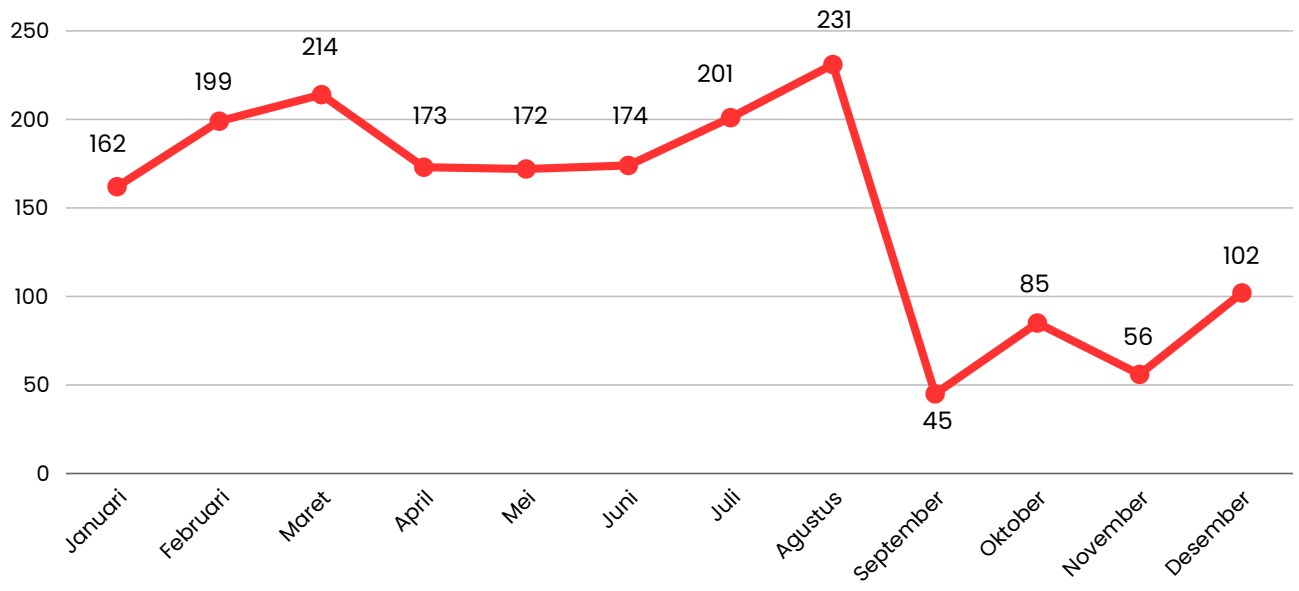
ADUAN SIBER DAN IMBAUAN KEAMANAN

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2024

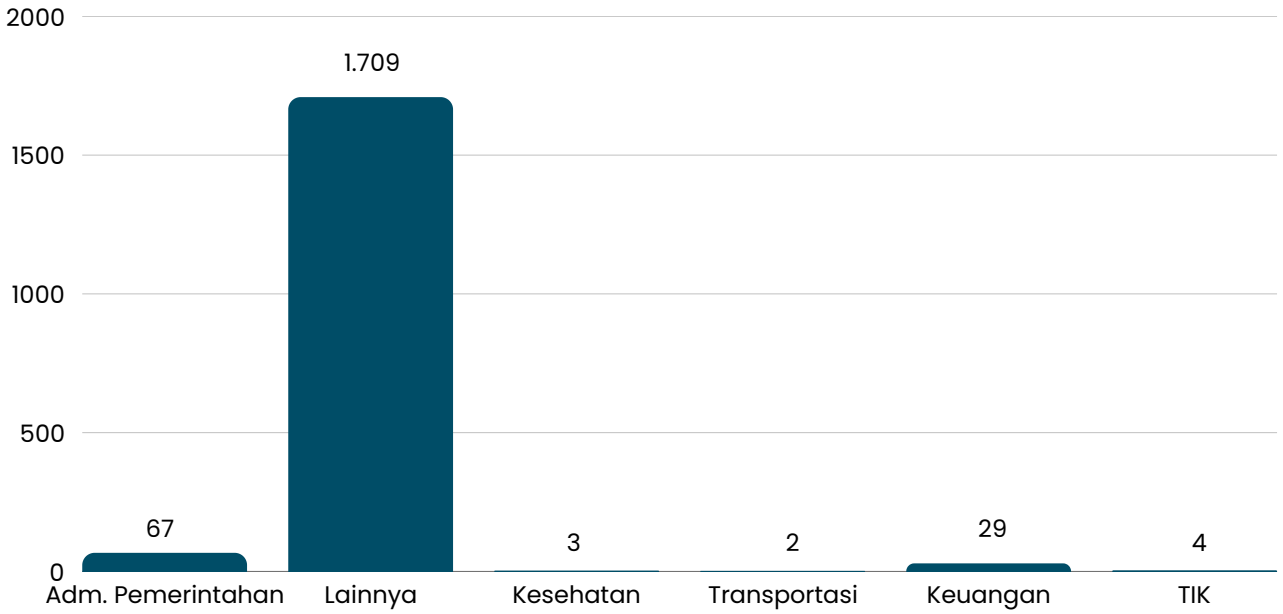
ADUAN SIBER

1.814
ADUAN SIBER

Selama Tahun 2024, Tim Pusat Kontak Siber BSSN menerima sebanyak **1.814 aduan** siber yang berasal dari berbagai sektor. Adapun aduan terbanyak terdapat pada bulan Agustus dengan jumlah **231 aduan**.

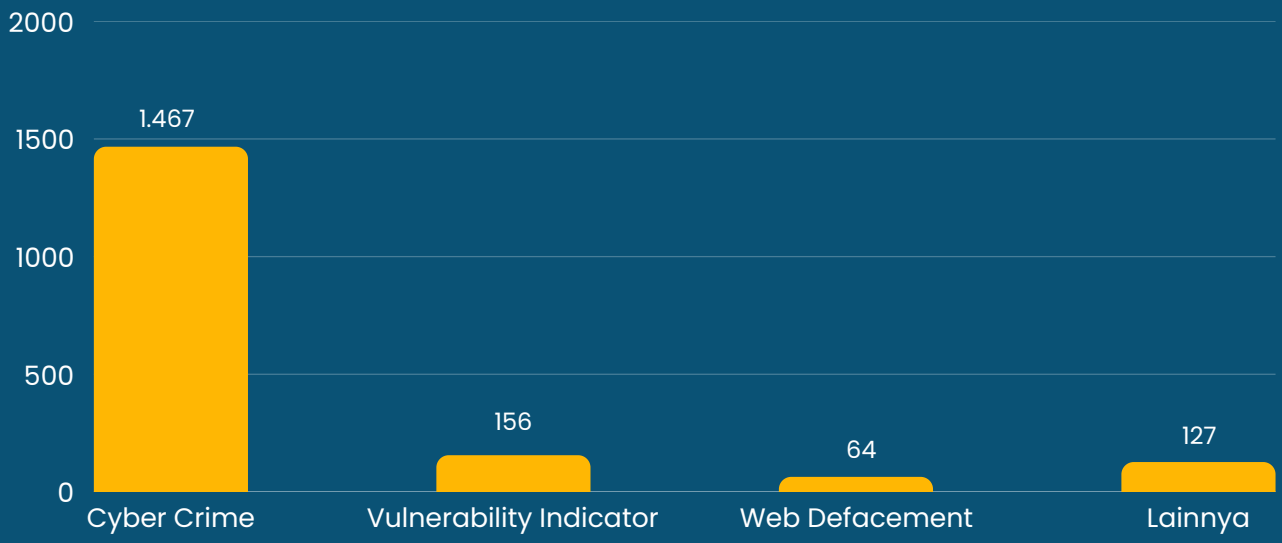


REKAPITULASI ADUAN SIBER BERDASARKAN SEKTOR



KATEGORI ADUAN SIBER

Aduan siber yang diterima oleh BSSN terdiri dari 15 kategori aduan dengan 3 kategori tertinggi yaitu sebagai berikut:



81%

Cybercrime

Tercatat sebanyak **1.467 aduan**. *Cybercrime* adalah tindakan kriminal yang memanfaatkan teknologi, mulai dari perangkat hingga jaringan internet.

7%

Lainnya

Tercatat sebanyak **127 aduan**. Kategori aduan lainnya terdiri dari beberapa kategori yaitu *Ransomware*, *Illegall Access*, *Phishing*, dll.

9%

Vulnerability Indicator

Tercatat sebanyak **156 aduan**. *Vulnerability Indicator* merujuk pada kelemahan atau celah dalam suatu sistem yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab.

3%

Web Defacement

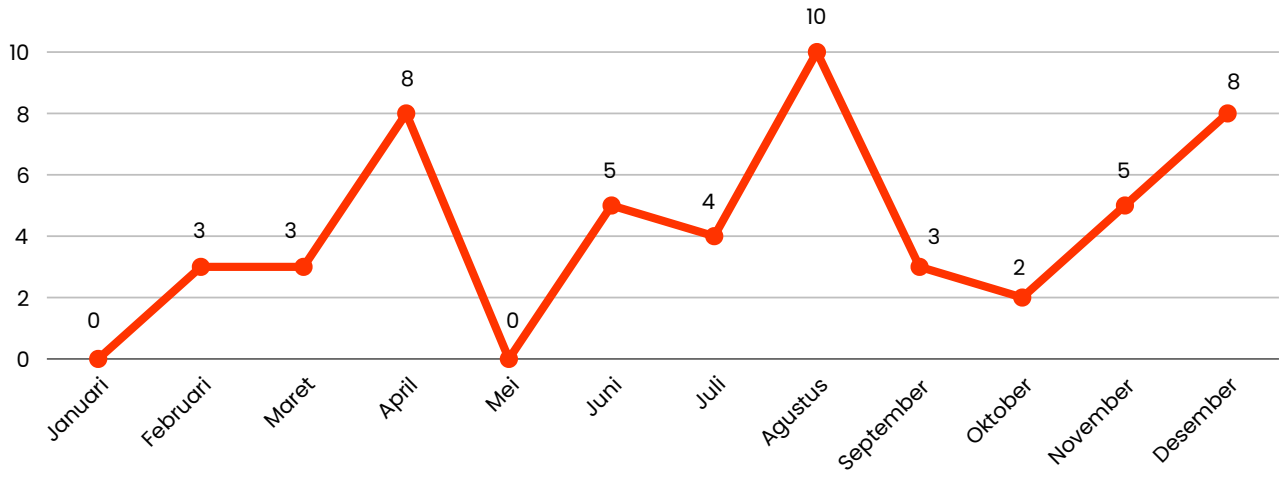
Tercatat sebanyak **64 aduan**. *Web defacement* adalah serangan yang dilakukan oleh pihak yang tidak sah untuk mengeksploitasi situs web dengan cara merusak, melakukan modifikasi, atau menghapus isi pada web.

IMBAUAN KEAMANAN

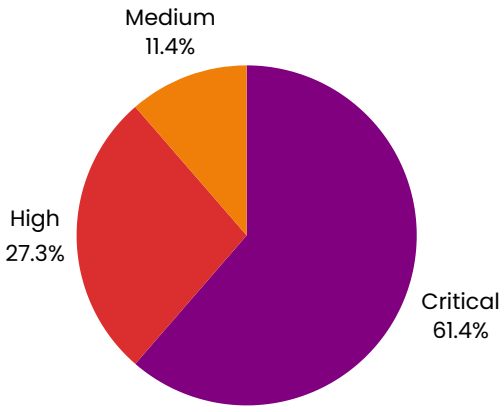
51	44	7
TOTAL IMBAUAN KEAMANAN	IMBAUAN KEAMANAN CVE	IMBAUAN KEAMANAN TREN

Pada tahun 2024, BSSN telah menerbitkan **51 imbauan keamanan** yang bertujuan untuk memberikan informasi terkait peringatan kerentanan suatu sistem dan ancaman siber, termasuk daftar *Common Vulnerabilities and Exposures* (CVE) yang berlaku secara global. Imbauan keamanan terbagi menjadi dua jenis, yaitu berdasarkan CVE dan berdasarkan tren terkini. Setiap imbauan mencakup nomor identifikasi, deskripsi, dan dampak dari ancaman tersebut. Imbauan ini tidak hanya membantu organisasi dan masyarakat dalam mengenali potensi ancaman, tetapi juga memudahkan kerjasama antara organisasi dan masyarakat dalam menangani potensi ancaman siber.

REKAPITULASI IMBAUAN KEAMANAN



IMBAUAN KEAMANAN BERDASARKAN CVE



Sebanyak 44 imbauan berasal dari identifikasi CVE. Dari jumlah tersebut, 27 imbauan memiliki *severity* tingkat *critical*, 12 imbauan memiliki tingkat *high*, dan 5 imbauan memiliki tingkat *medium*. Salah satu contoh imbauan kemanan berasal dari CVE dengan *severity critical* adalah sistem yang menggunakan GlobalProtect, fitur firewall dari Palo Alto Networks PAN-OS memungkinkan terjadi ancaman siber akibat *threat actor* dapat memanfaatkan kerentanan pada CVE tersebut untuk mendapatkan hak akses penuh tanpa perlu *login* terlebih dahulu.

> Cybersecurity is not just about stopping hackers; it's about managing risk and reducing vulnerabilities.
>
> **- Christopher Young**

IMBAUAN KEAMANAN BERDASARKAN TREN TERKINI

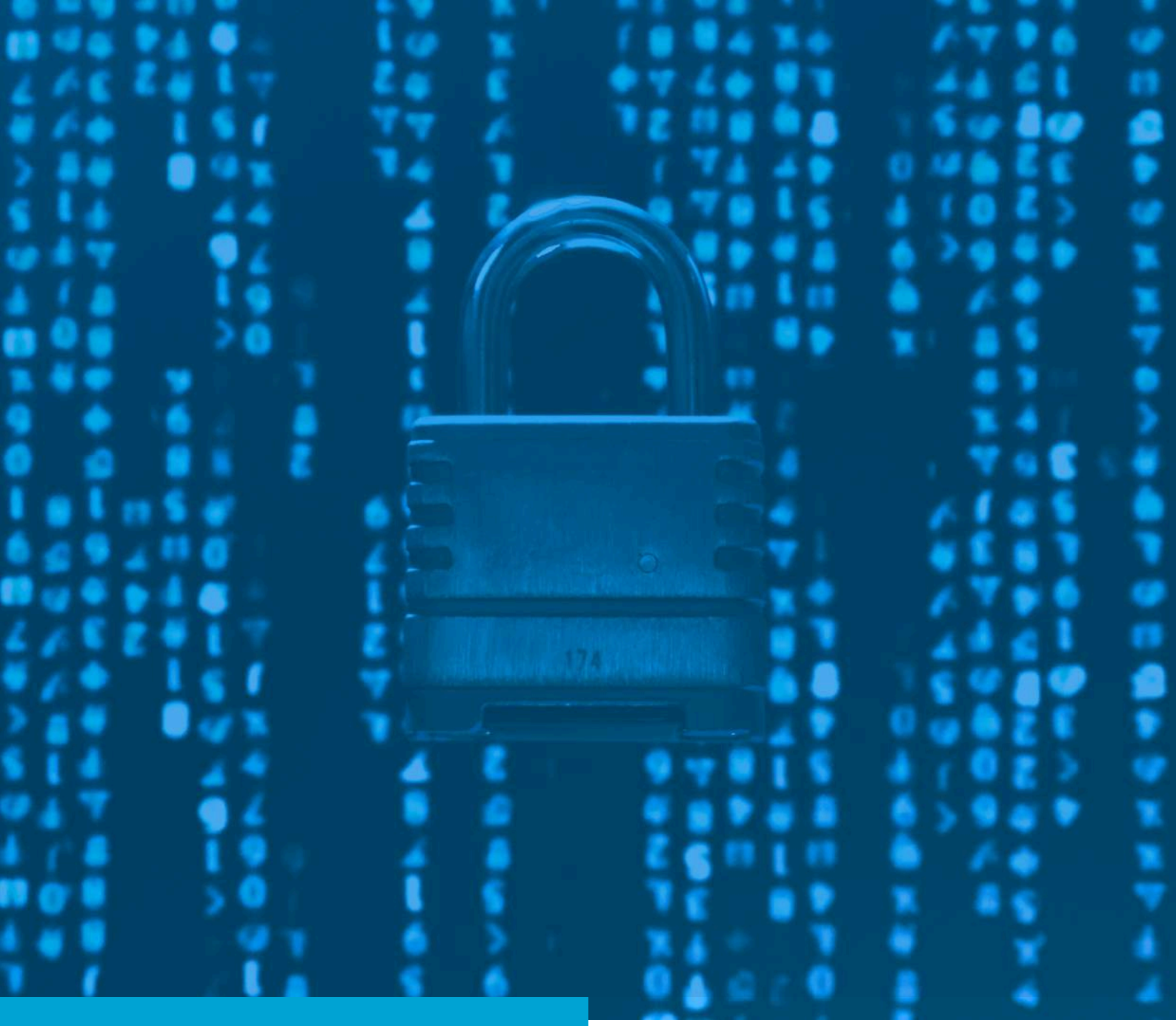
Selain berdasarkan CVE, terdapat 7 imbauan keamanan yang diterbitkan berdasarkan tren siber yang sedang berkembang.

Nama Imbauan Keamanan
APK Pemilu 2024
Lockbit 4.0
Penipuan Mengatasnamakan Direktorat Jenderal Pajak (DJP)
Serangan Ransomware Agenda
Aktivitas Kelompok Ancaman Siber yang Menargetkan Sektor IIV
Microsoft Global IT Outage Due to CrowdStrike
Phishing atas nama Insiden PDNS

Beberapa imbauan keamanan, seperti yang terkait dengan APK Pemilu 2024, penipuan yang mengatasnamakan DJP, dan serangan phishing atas nama insiden PDNS, memiliki dampak langsung bagi masyarakat Indonesia. Ancaman ini umumnya disebarkan melalui *file* atau *link* berbahaya yang dikirimkan ke perangkat pribadi masyarakat. Adanya imbauan keamanan ini sangat penting untuk meningkatkan kesadaran dan kewaspadaan masyarakat dalam menghadapi ancaman siber.

As cyber threats become more sophisticated, our defenses need to be equally innovative and agile.

- Lisa Monaco



04

TOP 5 COMMON VULNERABILITIES AND EXPOSURES (CVE)

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2024

TOP 5 CVE GLOBAL

Top 5 CVE Global merupakan 5 (lima) jenis kerentanan pada sistem maupun aplikasi dengan pengguna di seluruh dunia/global yang dipublikasikan pada Tahun 2024. Adapun kerentanan ini menjadi perhatian karena memiliki skor *Common Vulnerability Scoring System* (CVSS) yang memiliki tingkat dampak *Critical*.

01 CVE-2024-3400

CVE-2024-3400 memiliki nilai CVSS 10.00 dengan tingkat dampak *CRITICAL*. Kerentanan CVE-2024-3400 adalah kerentanan kritis pada perangkat lunak *Palo Alto Networks* PAN-OS yang secara khusus memengaruhi versi 10.2, 11.0, dan 11.1. Kerentanan ini memungkinkan *threat actor* untuk mengambil alih kontrol penuh *firewall* dengan menjalankan kode berbahaya pada tingkat administrator (*root*) tanpa adanya otentikasi yang dibutuhkan.

DAMPAK

Dampak dari kerentanan ini adalah memungkinkan *threat actor* untuk dapat mencuri informasi, memasang *malware*, atau mengganggu operasi penting.

PANDUAN MITIGASI

- Melakukan *update* adalah cara paling efektif untuk mengatasi kerentanan. *Palo Alto Networks* merilis patch pada 14 April 2024 untuk memitigasi kerentanan ini.
- Jika tidak dapat segera menerapkan *update*, nonaktifkan fitur *gateway GlobalProtect* atau *telemetry* perangkat untuk mengurangi risiko yang ada.

02 CVE-2024-3094

CVE-2024-3094 memiliki nilai CVSS 10.00 dengan tingkat dampak *CRITICAL*. Kerentanan CVE-2024-3094 melibatkan penemuan kode jahat dalam paket *tarball upstream* xz, dimulai dari versi 5.6.0. Melalui serangkaian obfuskasi kompleks, proses pembangunan liblzma mengekstrak sebuah *file* objek yang telah dibangun sebelumnya dari sebuah *file* uji tersembunyi yang ada di dalam *source code*, yang kemudian digunakan untuk memodifikasi fungsi-fungsi spesifik dalam kode liblzma. Hal ini menghasilkan sebuah *library* liblzma yang dimodifikasi yang dapat digunakan oleh perangkat lunak manapun yang terhubung dengan *library* ini, dengan cara mencegat dan memodifikasi interaksi data dengan *library* ini.

DAMPAK

Dampak dari kerentanan ini adalah memungkinkan *threat actor* untuk menyisipkan kode jahat dengan tujuan untuk merusak keamanan sistem.

PANDUAN MITIGASI

- Melakukan pembaruan perangkat lunak xz ke versi terbaru yang telah memperbaiki kerentanan ini.
- Melakukan pemindaian menyeluruh pada *source code* untuk mendeteksi keberadaan kode jahat atau modifikasi yang tidak sah.
- Memperhatikan tanda-tanda aktivitas tidak biasa atau mencurigakan pada sistem yang menggunakan *library* liblzma yang terpengaruh.

03 CVE-2024-23897

CVE-2024-23897 memiliki nilai CVSS 9.80 dengan tingkat dampak *CRITICAL*. Kerentanan CVE-2024-23897 berdampak pada *Jenkins* yang berasal dari adanya kekurangan validasi *input* yang memungkinkan *threat actor* menjalankan kode secara *remote* dan membaca *file* yang tersimpan pada *server Jenkins*. Pada versi terdampak, kerentanan ini diakibatkan karena belum dinonaktifkannya fitur *parser* perintah CLI yang menggantikan karakter '@' yang diikuti argumen *uniform resource locator* (url) dari *file* yang diunggah.

DAMPAK

Dampak dari kerentanan ini adalah memungkinkan *threat actor* dapat memperoleh akses secara tidak sah dan melakukan pencurian atau modifikasi pada data yang tersimpan di *server Jenkins*.

PANDUAN MITIGASI

Menggunakan versi *Jenkins* yang terbaru dan tidak terpengaruh oleh kerentanan ini, melakukan pembatasan akses terhadap *server* sehingga hanya pengguna yang berkepentingan yang dapat mengakses, memeriksa dan memperbaiki konfigurasi *Jenkins*, dan menambahkan *firewall* untuk mengurangi risiko dari akses tidak sah.

04 CVE-2024-3273

CVE-2024-3273 memiliki nilai CVSS 9.80 dengan tingkat dampak *CRITICAL*. Kerentanan ini ditemukan pada D-Link DNS-320L, DNS-325, DNS-327L dan DNS-340L hingga 20240403, yang mengandung kerentanan *Command Injection*. Jika digabungkan dengan CVE-2024-3272 dapat menyebabkan *Remote Code Execution* (RCE) yang tidak sah. Permasalahan ini mempengaruhi bagian fungsi yang tidak diketahui dari *file* /cgi-bin/nas_sharing.cgi dari komponen HTTP GET *Request Handler*. Eksploitasi telah diungkap ke publik dan dapat digunakan. Pengidentifikasi terkait kerentanan ini adalah VDB-259284.

DAMPAK

Dampak dari kerentanan ini mempengaruhi produk lama D-Link. Seluruh revisi *hardware* terkait telah mencapai siklus *end-of-life* (EOL) atau *end-of-service* (EOS) dan harus dihentikan serta diganti sesuai instruksi *vendor*.

PANDUAN MITIGASI

- Menggunakan *library calls* dari proses eksternal untuk membuat ulang fungsionalitas yang diinginkan.
- Memastikan semua perintah eksternal yang dipanggil dari program dibuat secara statis.
- Mengizinkan penegakan kebijakan *run-time* untuk mencegah penggunaan *non-sanctioned commands*.
- Menetapkan *permissions* yang mencegah pengguna mengakses/membuka *file* dengan hak istimewa.

> The greatest threat to our national security is our collective ignorance to the vulnerabilities of our own systems.
>
> **- Michael Hayden**

05 CVE-2024-45519

CVE-2024-45519 memiliki nilai CVSS 9.80 dengan tingkat dampak *CRITICAL*. Kerentanan keamanan yang kritis pada komponen pemrosesan *email Zimbra Collaboration* yang memungkinkan eksekusi perintah jarak jauh tanpa autentikasi melalui protokol SMTP yang menimbulkan risiko signifikan bagi organisasi yang menggunakan *platform* ini. Masalah ini disebabkan oleh penanganan data email yang tidak aman pada fitur *journaling*.

DAMPAK

Dampak dari kerentanan ini karena kelemahan di layanan postjournal yang memungkinkan pelaku menyerang untuk menjalankan perintah arbitrer. Celah ini ditemukan dalam konfigurasi atau kode yang tidak memvalidasi input dengan benar, sehingga pelaku dapat mengeksploitasi kelemahan ini tanpa perlu autentikasi sebelumnya. Akibatnya, *server* yang rentan dapat dikompromikan untuk eksekusi kode jarak jauh, memberikan kontrol penuh kepada *threat actor* atas sistem target.

PANDUAN MITIGASI

Memastikan semua perangkat lunak, termasuk sistem operasi, aplikasi, dan *plugin*, diperbarui ke versi terbaru untuk menutup kerentanan yang diketahui serta melakukan enkripsi data sensitif baik dalam penyimpanan maupun saat transmisi untuk melindungi dari akses yang tidak sah.

TOP 5 CVE NASIONAL

Top 5 CVE Nasional adalah daftar 5 (lima) jenis kerentanan yang memiliki jumlah *hit* terbanyak di Indonesia pada tahun 2024. Kerentanan-kerentanan ini memiliki tingkat dampak *Critical*. Dalam bab ini, akan disajikan rincian penjelasan mengenai setiap CVE, dampaknya terhadap sistem dan aplikasi, panduan mitigasi untuk mengurangi risiko, serta kategori sektor yang mungkin terpengaruh oleh masing-masing kerentanan dalam Top 5 CVE Nasional.

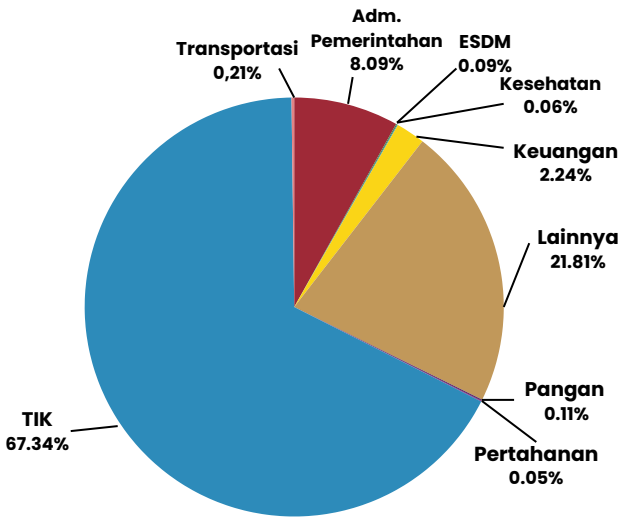
01 CVE-2024-23897

CVE-2024-38476 memiliki nilai CVSS 9.8 dengan tingkat dampak *CRITICAL*. Penyebab utama dari kerentanan ini adalah kelemahan dalam mekanisme pemrosesan *header respons* yang diterima dari aplikasi *backend*. Server Apache HTTP versi 2.4.59 dan sebelumnya mempercayai dan memproses *header respons* tanpa validasi yang memadai, sehingga membuka peluang bagi *threat actor* untuk menyisipkan atau memanipulasi *header* yang berisi data berbahaya. Selain itu, tidak adanya prosedur sanitasi atau pengecekan yang cukup pada *header respons* memungkinkan data yang telah dimanipulasi memicu perilaku *server* yang tidak diinginkan.

DAMPAK

Dampak dari kerentanan ini dapat menyebabkan pengungkapan informasi sensitif, *Server-Side Request Forgery* (SSRF), serta eksekusi skrip lokal untuk mengendalikan *server* atau meningkatkan hak akses.

SEKTOR TERDAMPAK



PANDUAN MITIGASI

- Pengguna Apache HTTP Server versi 2.4.59 dan sebelumnya sangat disarankan untuk melakukan pembaruan versi ke versi terbaru saat ini yaitu versi 2.4.62.
- Memastikan semua *header* respons dari aplikasi *backend* diverifikasi dan disanitasi sebelum diterima oleh *server*.
- Mengonfigurasi *server* untuk membatasi akses ke aplikasi *backend* hanya melalui jalur aman dan autentikasi yang ketat.

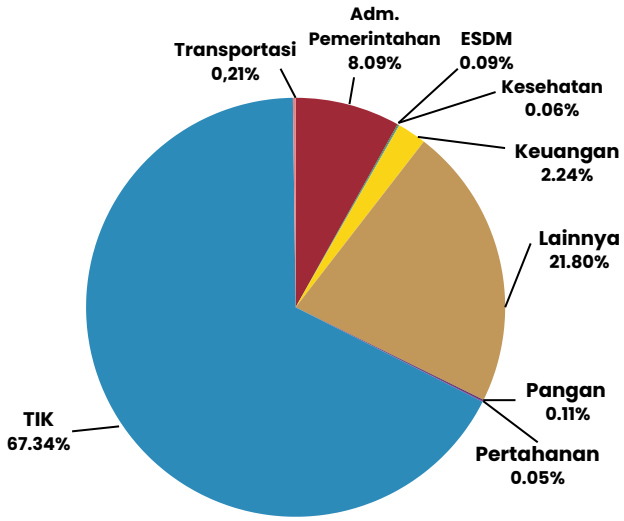
02 CVE-2024-38474

CVE-2024-38474 memiliki nilai CVSS 9.8 dengan tingkat dampak *CRITICAL*. Kerentanan ini disebakan adanya masalah pada mekanisme substitusi pengkodean (*substitution encoding*) yang digunakan oleh modul mod_rewrite pada Apache HTTP Server versi 2.4.59 dan sebelumnya. Masalah ini memungkinkan *threat actor* untuk mengeksploitasi konfigurasi *server* dengan cara mengeksekusi skrip dalam direktori yang diizinkan tetapi tidak langsung dapat diakses melalui URL, atau mengungkapkan skrip yang seharusnya hanya dijalankan sebagai *Computer-generated imagery* (CGI).

DAMPAK

Kerentanan ini memungkinkan *threat actor* untuk mengeksploitasi kelemahan mod_rewrite, mengungkapkan informasi sensitif, atau menjalankan skrip berbahaya di direktori yang tidak dapat diakses langsung, yang berpotensi merusak *server* dan mencuri data.

SEKTOR TERDAMPAK



PANDUAN MITIGASI

- Pengguna Apache HTTP Server versi 2.4.59 dan sebelumnya sangat disarankan untuk melakukan pembaruan versi ke versi terbaru saat ini yaitu versi 2.4.62.
- Meninjau dan ubah semua *RewriteRule* dalam konfigurasi untuk memastikan tidak menangkap dan menggantikan *input* secara tidak aman.
- Mengaktifkan *flag* UnsafeAllow3F hanya jika benar-benar diperlukan serta jika memahami risiko dan telah memvalidasi kebutuhannya dengan benar.
- Mengonfigurasikan *server* untuk membatasi akses ke direktori yang berisi skrip yang seharusnya hanya dijalankan sebagai CGI.

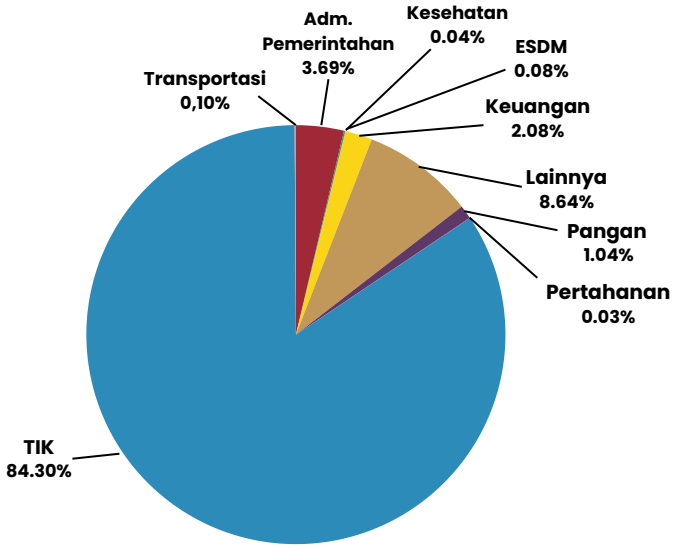
03 CVE-2024-4577

CVE-2024-4577 memiliki nilai CVSS 9.8 dengan tingkat dampak *CRITICAL*. Kerentanan ini terdapat pada PHP 8.1 (sebelum versi 8.1.29), PHP 8.2 (sebelum versi 8.2.20), dan PHP 8.3 (sebelum versi 8.3.8). Penyebab utama dari kerentanan ini terletak pada kombinasi penggunaan PHP-CGI dengan Apache pada sistem operasi Windows, terutama ketika sistem dikonfigurasi untuk menggunakan kode halaman tertentu yang memicu perilaku "*Best-Fit*" oleh Windows. Pada kerentanan ini, modul PHP-CGI salah menafsirkan karakter yang telah diganti oleh Windows sebagai opsi atau argumen untuk binari PHP yang sedang dijalankan sehingga *threat actor* dapat memanfaatkan kelemahan ini untuk menyisipkan opsi berbahaya ke dalam PHP-CGI.

DAMPAK

Dampak dari kerentanan ini *threat actor* dapat mengungkapkan kode sumber skrip PHP, menjalankan kode PHP *arbitrer* untuk mengendalikan *server*, serta menyisipkan parameter berbahaya untuk memanipulasi aplikasi. Selain itu, *threat actor* dapat meningkatkan hak akses mereka di *server* dan mengganggu operasional *server*, termasuk menghentikan layanan yang berjalan.

SEKTOR TERDAMPAK



PANDUAN MITIGASI

- Pengguna Apache HTTP Server versi 2.4.59 dan sebelumnya sangat disarankan untuk melakukan pembaruan versi ke versi terbaru saat ini yaitu versi 2.4.62.
- Meninjau dan ubah semua *RewriteRule* dalam konfigurasi untuk memastikan tidak menangkap dan menggantikan *input* secara tidak aman.
- Mengaktifkan *flag* UnsafeAllow3F hanya jika benar-benar diperlukan serta jika memahami risiko dan telah memvalidasi kebutuhannya dengan benar.
- Mengonfigurasikan server untuk membatasi akses ke direktori yang berisi skrip yang seharusnya hanya dijalankan sebagai CGI.

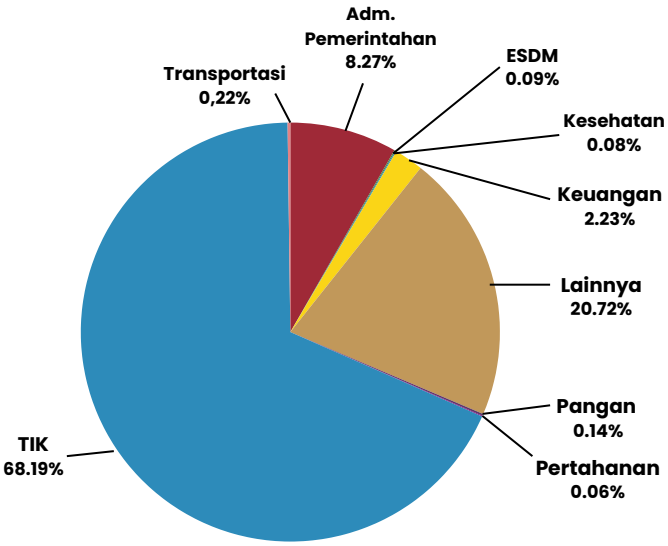
04 CVE-2022-36760

CVE-2022-36760 memiliki nilai CVSS 9.0 dengan tingkat dampak *CRITICAL*. Kerentanan ini merupakan dengan jenis HTTP *Request Smuggling* yang terdapat pada modul mod_proxy_ajp dalam Apache HTTP Server. Penyebab kerentanan ini adalah karena adanya komunikasi yang tidak konsisten antara Apache HTTP Server versi 2.4.54 dan sebelumnya dengan *server* Apache JServ *Protocol* (AJP) dalam menangani struktur HTTP *request*.

DAMPAK

Dampak dari adanya kerentanan ini adalah *threat actor* dapat mengirimkan permintaan HTTP yang dirancang khusus untuk memanfaatkan perbedaan interpretasi antara kedua *server* tersebut sehingga *threat actor* dapat menyembunyikan permintaan berbahaya yang tidak dikenali oleh *server* Apache tetapi tetap diproses oleh *server* AJP yang dituju.

SEKTOR TERDAMPAK



PANDUAN MITIGASI

- Pengguna Apache HTTP Server versi 2.4.59 dan sebelumnya sangat disarankan untuk melakukan pembaruan versi ke versi terbaru saat ini yaitu versi 2.4.62.
- Jika *server* tidak memerlukan protokol AJP, nonaktifkan mod_proxy_ajp untuk mengurangi vektor serangan.
- Memperbaiki konfigurasi mod_proxy dan mod_rewrite untuk memastikan tidak ada kelemahan dalam komunikasi antara *server* Apache dan *server* AJP.

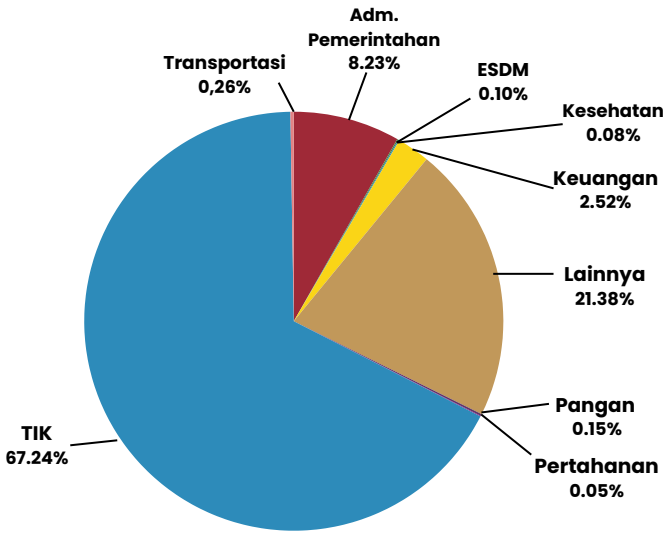
05 CVE-2021-40438

CVE-2022-36760 memiliki nilai CVSS 9.0 dengan tingkat dampak *CRITICAL*. Kerentanan ini merupakan dengan jenis HTTP *Request Smuggling* yang terdapat pada modul mod_proxy_ajp dalam Apache HTTP Server. Penyebab kerentanan ini adalah karena adanya komunikasi yang tidak konsisten antara Apache HTTP Server versi 2.4.54 dan sebelumnya dengan *server* Apache JServ *Protocol* (AJP) dalam menangani struktur HTTP *request*.

DAMPAK

Dampak dari adanya kerentanan ini adalah *threat actor* dapat mengirimkan permintaan HTTP yang dirancang khusus untuk memanfaatkan perbedaan interpretasi antara kedua *server* tersebut sehingga *threat actor* dapat menyembunyikan permintaan berbahaya yang tidak dikenali oleh *server* Apache tetapi tetap diproses oleh *server* AJP yang dituju.

SEKTOR TERDAMPAK



PANDUAN MITIGASI

- Pengguna Apache HTTP Server versi 2.4.59 dan sebelumnya sangat disarankan untuk melakukan pembaruan versi ke versi terbaru saat ini yaitu versi 2.4.62.
- Jika *server* tidak memerlukan protokol AJP, nonaktifkan mod_proxy_ajp untuk mengurangi vektor serangan.
- Memperbaiki konfigurasi mod_proxy dan mod_rewrite untuk memastikan tidak ada kelemahan dalam komunikasi antara *server* Apache dan *server* AJP.

Security vulnerabilities are inevitable, but how we respond to them is what defines our resilience.

– Bruce Schneier

05

HIGHLIGHT IT SECURITY ASSESMENT (ITSA)

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2024

HIGHLIGHT ITSA

462
APLIKASI

131
INSTANSI

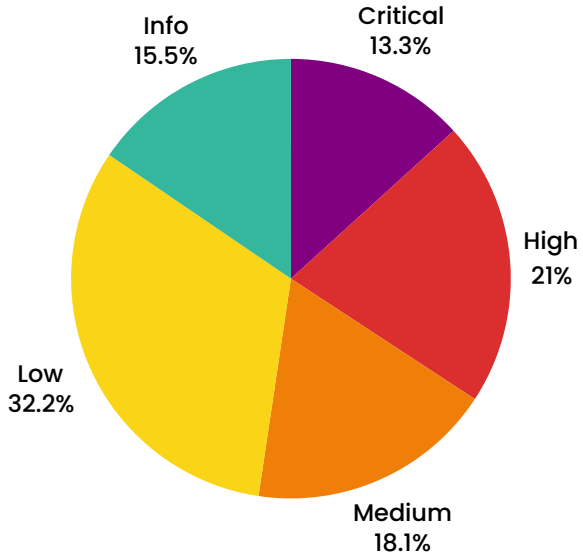
1.931
KERENTANAN

IT *Security Assessment* (ITSA) merupakan salah satu layanan identifikasi kerentanan pada sistem elektronik yang diberikan oleh Direktorat Operasi Keamanan Siber. Layanan ini bertujuan untuk mengidentifikasi celah kerentanan serta potensi resiko yang ada pada sistem serta rekomendasi perbaikannya sehingga sistem elektronik diharapkan dapat digunakan dengan baik dan optimal. Layanan ini telah diberikan dan diterima oleh berbagai instansi baik instansi pusat, pemerintah daerah, maupun sektor IIV.

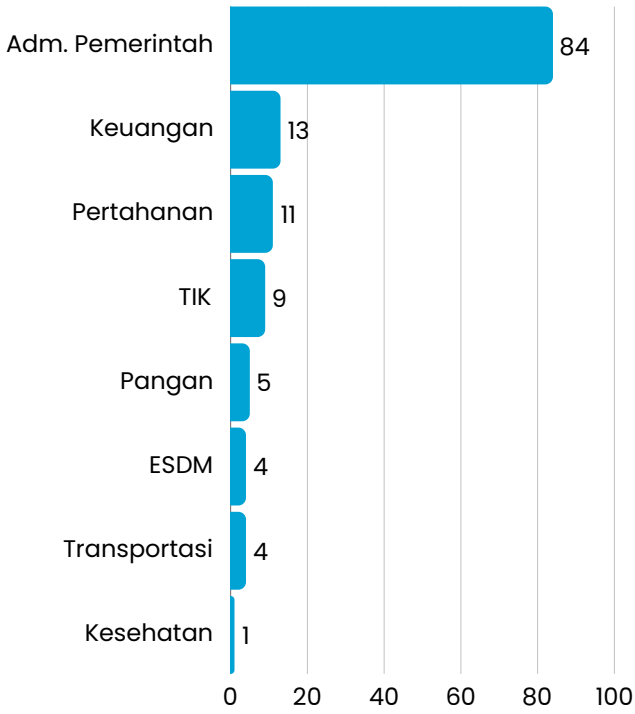
Sepanjang tahun 2024, telah dilakukan ITSA pada 462 aplikasi objek ITSA pada 131 instansi dengan hasil identifikasi kerentanan sebanyak 1.931 kerentanan yang terdiri dari 256 kerentanan *critical*, 405 kerentanan *high*, 350 kerentanan *medium*, 621 kerentanan *low,* serta 299 kerentanan info. Aplikasi yang menjadi target ITSA mencakup aplikasi *web*, *mobile* maupun infrastruktur.

GRAFIK TINGKAT RISIKO

Celah keamanan dibagi berdasarkan tingkat risiko (*risk severity*) yaitu *Critical, High, Medium, Low, dan Info.*



GRAFIK SEBARAN SEKTOR ITSA



Kontak ITSA

Media yang dapat digunakan untuk mendapatkan layanan publik ITSA, yaitu melalui telepon, surat elektronik (email), ataupun datang secara langsung ke Kantor BSSN.

+6282122230970 itsa@bssn.go.id

TOP 5 KERENTANAN

Berdasarkan hasil ITSA pada tahun 2024, ditemukan sebanyak 1.931 kerentanan yang memiliki tingkat risiko yang beragam. Dari seluruh kerentanan yang terdeteksi, berikut merupakan 5 (lima) kerentanan dengan tingkat risiko tinggi pada tahun 2024.

01 INFORMATION DISCLOSURE

Information Disclosure merupakan jenis kerentanan yang terjadi ketika aplikasi tidak melindungi informasi-informasi yang memungkinkan dapat terungkap kepada pihak-pihak yang tidak seharusnya memiliki/mengetahui akses terhadap informasi tersebut. Kerentanan ini menyebabkan pencurian identitas terjadi ketika informasi pribadi yang sensitif terungkap, menyebabkan kerugian finansial dan masalah lainnya, penipuan timbul dari pengungkapan informasi keuangan sensitif, serta gangguan proses bisnis dapat terjadi ketika informasi bisnis rahasia terungkap, menyebabkan hilangnya penjualan dan penurunan laba. Oleh karena itu, untuk mengatasi kerentanan ini, diperlukan *review* kembali informasi apa saja yang perlu ditampilkan sesuai dengan hak akses dan *request* yang dikirimkan.

02 INSECURE DIRECT OBJECT REFERENCE

IDOR adalah kerentanan yang terjadi saat aplikasi *web* atau API menggunakan *input* yang diberikan oleh pengguna untuk langsung mengakses objek dalam *database internal* tanpa melakukan pengecekan kontrol akses atau otentikasi. Kerentanan IDOR dapat memungkinkan *threat actor* untuk mengakses data sensitif, seperti informasi pengguna, informasi keuangan, atau kekayaan intelektual. Untuk mengatasi kerentanan IDOR diperlukan penggunaan identifikasi unik global (GUID) atau identifikasi acak untuk mengidentifikasi objek secara unik dalam database, penerapan akses kontrol, agar pengguna hanya bisa mengakses *resources* yang sesuai dengan haknya serta pemindahan ID *query* ke *post body* atau tempat lainnya dengan juga memanipulasi pemanggilan ID nya.

03 CROSS-SITE SCRIPTING

Terdapat dua jenis *cross-site scripting* (XSS) yaitu *stored XSS* dan *reflected XSS*. *Stored XSS* adalah jenis serangan *cross-site scripting* (XSS) yang terjadi ketika kode berbahaya disimpan pada *server web*. Kode berbahaya ini kemudian dapat dieksekusi oleh pengguna mana pun yang mengakses masukkan yang mengandung *script* tersebut. Sedangkan R*eflected Cross Site Scripting* (XSS) adalah serangan injeksi kode pada sisi klien dengan menggunakan sarana halaman *website*. XSS terjadi karena adanya kerentanan pada *form input website* yang dapat mengeksekusi *script web* (php, html, js, dll). Dampak yang ditimbulkan dari kerentanan ini yaitu *threat actor* dapat melakukan eksekusi *script* berbahaya yang dapat menyebabkan pencurian *cookie*, serangan DoS, ataupun mengirimkan *phishing* kepada korban. Hal yang dapat dilakukan untuk menangani kerentanan ini, antara lain: mengonfigurasi WAF untuk deteksi *rules* XSS, melakukan sanitasi input melalui *whitelist possible character* pada setiap *field input*, menerapkan *output encoding*, melakukan HTML encode pada halaman yang memiliki masukkan dari *user,* dan melakukan HTML *Sanitizion* untuk membersihkan laman HTML dari *script* XSS (cth. DOMpurify).

04 WEAK PASSWORD POLICY

Weak Password Policy merupakan jenis kerentanan dimana tidak diimplementasikannya kebijakan *password* yang baik dan benar. Dampak dari kerentanan ini yaitu *threat actor* dapat dengan mudah mengubah *password* pengguna lain dengan *password* yang lemah dan mengakibatkan pengambil alihan akun. Rekomendasi yang disarankan untuk kerentanan ini yaitu mengganti *password* dengan menerapkan kebijakan penggunaan *password* yang baik sebagaimana mengacu pada NIST 800-63 dan/atau PCI DSS *Standards Requirement* 8 dan memastikan konfigurasi persyaratan pembuatan *password* berjalan dengan benar.

05 BROKEN ACCESS CONTROL

Broken Access Control adalah kerentanan yang terjadi ketika pengguna dapat mengkses sebuah data atau melakukan suatu fungsi yang seharusnya tidak dalam kewenangannya atau tanpa adanya otorisasi yang diperlukan. Dampak dari kerentanan ini adalah pelanggaran data terjadi ketika individu yang tidak berwenang mengakses data sensitif, yang dapat digunakan untuk tujuan jahat seperti pencurian identitas atau penipuan serta gangguan operasional, disebabkan oleh pihak yang mencoba mengakses sistem kritis, dapat menyebabkan waktu tidak beroperasi yang signifikan dan kerugian finansial. Rekomendasi yang disarankan untuk kerentanan ini yaitu penggunaan autentikasi dan otorisasi yang kuat, Penerapan kontrol akses berbasis peran (RBAC) dan kendalikan akses dengan ketat. Penerapan validasi *input* pengguna sesuai hak aksesnya, serta pemindahan ID *query* ke *post body* atau tempat lainnya dengan juga memanipulasi pemanggilan ID nya.

06

TOP 10 CYBERSECURITY INSIGHT

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2024

TOP 10 CYBERSECURITY INSIGHT

Keamanan siber menjadi isu krusial di era digital saat ini, baik di tingkat nasional maupun internasional, seiring dengan meningkatnya ancaman siber yang semakin kompleks. Berikut adalah Top 10 berita *cybersecurity* mengenai tren dan ancaman keamanan siber pada tahun 2024. Informasi ini relevan secara nasional dan internasional yang dihadapi berbagai negara.

01 SERANGAN RANSOMWARE TERHADAP LAYANAN PEMERINTAH

Grup "*Brain Cipher*" menyerang lebih dari 160 lembaga pemerintah pada Juni 2024, mengganggu layanan imigrasi dan bandara utama. *Threat actor* ini meminta tebusan 8 juta USD, meski banyak data belum dicadangkan. Insiden ini menyoroti pentingnya strategi cadangan data yang andal.

02 LOCKBIT KEMBALI DAN MENGANCAM UNTUK MENARGETKAN LEBIH BANYAK ORGANISASI PEMERINTAH

Setelah operasi penegakan hukum melumpuhkan mereka, LockBit membangun infrastruktur baru dan mulai membocorkan data korban. Mereka juga mengatasi eksploitasi FBI terhadap kerentanan PHP yang sebelumnya mematahkan operasi mereka. Ancaman ini menunjukkan bahwa LockBit tetap menjadi ancaman serius bagi sektor pemerintah.

03 SERANGAN SIBER PADA SEKTOR KESEHATAN DI AMERIKA SERIKAT DINILAI MERUPAKAN INSIDEN SIBER TERBESAR SEPANJANG MASA

Ransomware menyerang Change Healthcare, mengganggu sistem kesehatan besar-besaran, merugikan 100 juta USD per hari. Penyedia layanan kesulitan memproses pembayaran dan otorisasi, sementara beberapa rumah sakit terganggu dalam menyediakan layanan medis. Ancaman ini menjadi peringatan terhadap celah keamanan pada perangkat medis yang terhubung.

04 PERETAS 'ARCANEDOOR' MERETAS FIREWALL CISCO UNTUK MENGAKSES JARINGAN PEMERINTAH

Threat actor menggunakan dua kerentanan *zero-day* pada perangkat Cisco untuk menyerang jaringan pemerintah global. Serangan ini memungkinkan pencurian data dan pengawasan lalu lintas jaringan. Meski Cisco merilis pembaruan, tren serangan terhadap perangkat keamanan jaringan semakin mengkhawatirkan.

05 EKSPLOITASI *CLOUD* UNTUK SMS *PHISHING*

Threat actor menggunakan layanan penyimpanan *cloud* seperti Amazon S3 untuk mengelabui *firewall* dan membuat pesan *phishing* terlihat sah. Dengan menyematkan URL berbahaya di layanan *cloud*, pengguna diarahkan ke situs berbahaya tanpa menyadari risiko. Serangan ini menonjolkan perlunya deteksi keamanan lebih canggih untuk penyimpanan *cloud*.

06 ASCENSION DIRETAS SETELAH KARYAWAN MENGUNDUH FILE MALICIOUS

Ascension terkena *ransomware* akibat karyawan yang mengunduh *file* berbahaya, mengganggu sistem rekam medis dan layanan lainnya. Perusahaan berupaya memulihkan sistem meski beberapa layanan tetap terganggu. Investigasi menunjukkan sebagian kecil *file* mungkin bocor, tetapi data rekam medis lengkap tidak ditemukan dicuri.

07 VARIAN BARU MALLOX MENARGETKAN SISTEM LINUX

Ransomware Mallox kini menyasar sistem Linux dengan enkripsi AES-256 CBC yang sulit dipecahkan. Mallox juga mengadopsi model *Ransomware-as-a-Service* dengan taktik multi-pemerasan. Peneliti menemukan *decryptor* untuk Mallox, memberi harapan pada korban namun tetap menekankan pentingnya cadangan dan keamanan.

08 APT PEACH SANDSTORM YANG DIDUKUNG IRAN MENYEBARKAN BACKDOOR TICKLER BARU

Kelompok APT yang didukung Iran, Peach Sandstorm, mengembangkan *backdoor* baru bernama Tickler untuk spionase siber. Targetnya termasuk sektor minyak, gas, dan pemerintah di AS serta UEA. Mereka memanfaatkan layanan Azure untuk mengoperasikan *server* C2 dan mengumpulkan data jaringan.

09 HACKER MENGELABUHI CHATGPT UNTUK MEMBERIKAN INSTRUKSI RINCI UNTUK MEMBUAT BOM RAKITAN

Threat actor menggunakan teknik *social engineering* untuk memanipulasi ChatGPT agar memberikan instruksi membuat bom rakitan. Insiden ini menunjukkan celah keamanan dalam pembatasan sistem AI yang dapat dieksploitasi untuk tujuan berbahaya.

10 PERETAS KOREA UTARA MENYEBARKAN ROOTKIT FUDMODULE MELALUI EKSPLOITASI ZERO-DAY

ChromeGrup Lazarus menggunakan celah zero-day di Chrome untuk menyebarkan *rootkit FudModule*, menargetkan lembaga keuangan dan individu di industri *cryptocurrency*. Mereka mengeksploitasi CVE-2024-7971 dan *bug kernel* untuk akses mendalam. Insiden ini menegaskan pentingnya pembaruan keamanan secara cepat.

In cybersecurity, the more systems we secure, the more vulnerabilities we discover.

– Dan Kaminsky

07

ASISTENSI TANGGAP INSIDEN SIBER

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2024

ASISTENSI TANGGAP INSIDEN SIBER

76

ASISTENSI TANGGAP INSIDEN SIBER

BSSN telah melaksanakan 76 kegiatan asistensi tanggap insiden siber di 66 *stakeholder*. Adapun terdapat 3 (tiga) kategori pelaksanaannya sebagai berikut:

HANDLE BSSN

13 Insiden

Proses asistensi penanganan insiden siber dilakukan secara penuh oleh BSSN.

KOLABORASI

33 Insiden

Proses asistensi penanganan insiden siber dilakukan oleh PSE/CSIRT yang bekerja sama dengan BSSN.

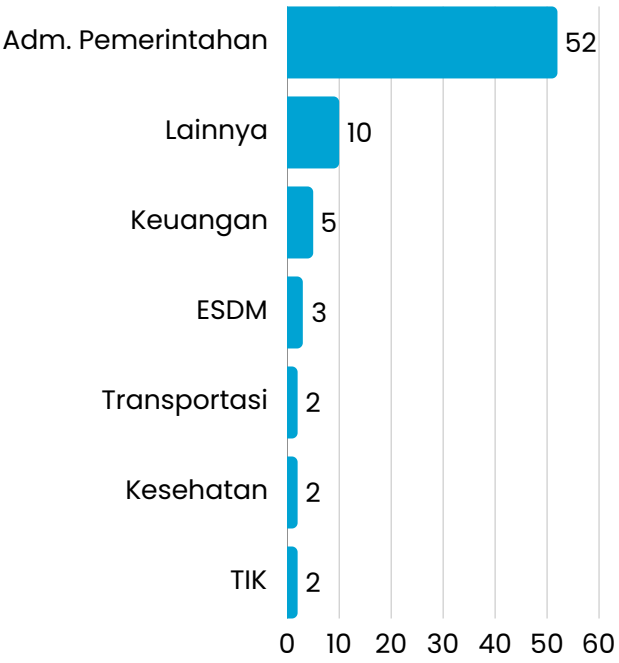
HANDLE PSE/CSIRT ORGANISASI

30 Insiden

Proses asistensi penanganan insiden siber yang dilakukan secara penuh oleh PSE/CSIRT.

Berikut merupakan klasifikasi insiden dan sektor yang dilakukan Layanan Asistensi Tanggap Insiden Siber:

GRAFIK SEBARAN SEKTOR



KLASIFIKASI INSIDEN	JUMLAH
Data Breach	22
Illegal Access	13
Web Defacement	11
Ransomware	9
Anomali Trafik	7
DDoS	7
Malware	3
Account Hijacking	2
Compromise Account	1
Vulnerability Indicator	1

Adapun dari 71 insiden yang diasistensi ditemukan adanya 3 (tiga) insiden dengan kasus terbanyak di tahun 2024 yaitu *Data Breach, Illegal Access* dan *Web defacement*.

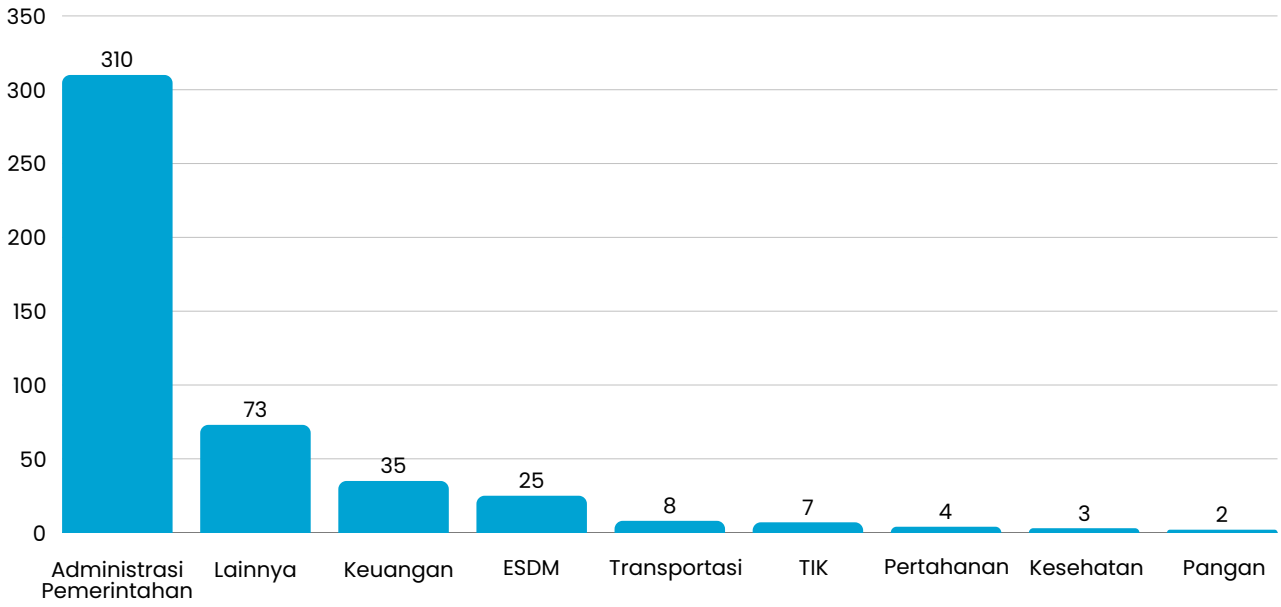
JUMLAH TIM TANGGAP INSIDEN SIBER TEREGISTRASI

467
TTIS ORGANISASI

3
TTIS SEKTORAL

Tim Tanggap Insiden Siber (TTIS) adalah tim khusus yang bertanggung jawab untuk menerima, meninjau, dan merespons laporan serta aktivitas yang berkaitan dengan insiden keamanan komputer. Tim ini berperan penting dalam menjaga keamanan informasi dan teknologi dalam suatu organisasi dengan mengidentifikasi kerentanan, memberikan mitigasi, serta memulihkan sistem dari serangan siber. Selain itu, CSIRT juga berkoordinasi dengan pihak-pihak terkait, baik internal maupun eksternal, untuk menangani ancaman keamanan secara efektif dan efisien.

SEBARAN TTIS ORGANISASI



SEBARAN CSIRT SEKTORAL

NO	SEKTOR	NAMA CSIRT
1	TTIS Sektor Pemerintahan	GOV-CSIRT
2	TTIS Sektor Keuangan	TTIS-SK
3	TTIS Sektor Perhubungan	CSIRT SEKTOR TRANSPORTASI

Cybersecurity is a race between criminals trying to exploit vulnerabilities faster than companies can defend against them.

-Alex Stamos

08

VOLUNTARY VULNERABILITY IDENTIFICATION AND PROTECTION (VVIP-PROGRAM)

VOLUNTARY VULNERABILITY IDENTIFICATION AND PROTECTION

Pengesahan Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber merupakan langkah konkret pemerintah untuk menghadapi ancaman siber yang semakin kompleks. BSSN selaku instansi yang bertugas melaksanakan pemerintahan dibidang keamanan siber dan sandi, dalam penyelenggaraan strategi keamanan siber nasional membentuk Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber (RAN Kamsiber) Tahun 2024-2028. Salah satu Kegiatan pada RAN Kamsiber adalah menyelenggarakan *Voluntary Vulnerability Identification and Protection* (VVIP) Program.

Melalui VVIP Program, BSSN telah membuka ruang terciptanya kolaborasi *triplehelix*, yaitu antara Instansi Penyelenggara Negara (IPN) sebagai Penyelenggara Sistem Elektronik (PSE), BSSN sebagai penyelenggara VVIP program dan masyarakat terkhusus pegiat siber selaku *bug hunter* untuk bersama menjaga keamanan siber. VVIP Program adalah program yang melibatkan masyarakat secara sukarela untuk berkolaborasi dengan BSSN dalam melakukan identifikasi kerentanan & proteksi pada sistem elektronik milik IPN. Tujuan dari VVIP Program menciptakan kolaborasi antara pemerintah dan Masyarakat dalam menjaga ruang siber, pemilik sistem menerima layanan identifikasi dan proteksi kerentanan yang berkesinambungan, dan peserta dalam hal ini Masyarakat memperoleh wadah dalam menyalurkan kompetensinya, serta menerima apresiasi atas partisipasinya. Adapun melalui program ini diharapkan dapat memberikan manfaat meningkatkan keamanan ruang siber Indonesia dan menciptakan kolaborasi antara pemerintah dan Masyarakat dalam menjaga ruang siber untuk menurunkan tingkat risiko terjadinya insiden siber di Indonesia. VVIP Program diatur lebih lanjut pada Peraturan Kepala BSSN No. 5 Tahun 2023 Tentang Penyelenggaraan Program Identifikasi Kerentanan dan Proteksi Secara Sukarela.

Sebagai upaya dalam memperkenalkan dan memperluas jangkauan VVIP Program, BSSN melaksanakan berbagai kegiatan bersama IPN dan/atau masyarakat, diantaranya BSSN melaksanakan kegiatan konsolidasi pada tahun 2024 yang dapat diikuti berbagai kalangan secara *online* sebanyak 5 kali kegiatan dan melaksanakan kegiatan *bug hunter meet-up* sebagai upaya untuk mempererat jalinan kerjasama dengan masyarakat terkhusus *bug hunter*.

Pada tahun 2024 VVIP Program melibatkan sebanyak 14 IPN dengan target sistem yang diuji sebanyak 41 aplikasi.

Penyelenggara Sistem Elektronik yang Berpartisipasi

VVIP II

BSSN
1 Aplikasi

Pemprov Jateng
4 Aplikasi

Pemprov Bali
3 Aplikasi

Pemprov Jatim
3 Aplikasi

LKPP
5 Aplikasi

VVIP III

Pemprov DIY
4 Aplikasi

Pemkab Bantul
3 Aplikasi

Pemkab Kulon Progo
3 Aplikasi

Pemkab Sleman
2 Aplikasi

Pemkot Yogya
6 Aplikasi

VVIP IV

Kemenhan
2 Aplikasi

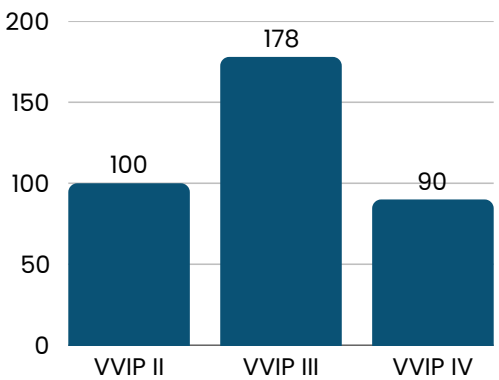
Disinfolahtal
2 Aplikasi

Disinfolahtau
2 Aplikasi

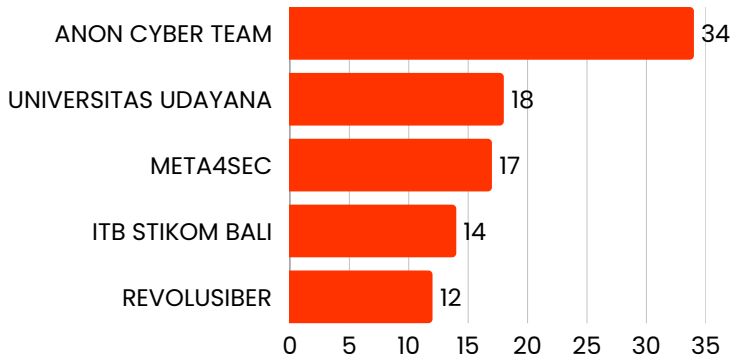
Poltek SSN
1 Aplikasi

Selain IPN dalam pelaksanaan VVIP Program juga melibatkan 400 orang *bug hunter* yang berasal dari berbagai kalangan untuk melakukan pengujian pada 41 aplikasi tersebut. Dari 400 orang *bug hunter* tersebut jumlah *bug hunter* paling banyak terlibat pada VVIP Program tahap III dan terdapat Top 5 komunitas *bug hunter* yang anggotanya banyak terlibat dalam VVIP Program.

Jumlah *Bug Hunter*: 386 orang



TOP 5 Komunitas *Bug Hunter*



LAPORAN VVIP PROGRAM

744
LAPORAN VVIP

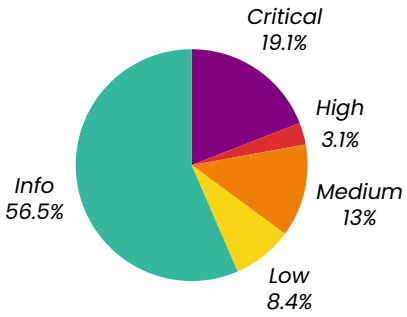
VVIP II
131
LAPORAN

VVIP III
246
LAPORAN

VVIP IV
367
LAPORAN

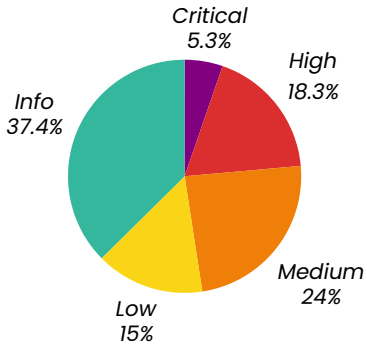
Dari pelaksanaan VVIP 2024 didapatkan **744 laporan** dan ditemukan sebanyak **744 temuan** kerentanan dengan tingkat risiko *critical* sebanyak 148, *high* sebanyak 136, *medium* sebanyak 185, *low* sebanyak 54, dan *info* sebanyak 221. Dengan adanya VVIP Program, *stakeholder* sebagai Penyelenggara Sistem Elektronik dapat dengan segera memperbaiki temuan celah kerentanan yang ditemukan oleh para *bug hunter*.

Laporan Berdasarkan Tingkat Risiko Kerentanan (*Severity*)



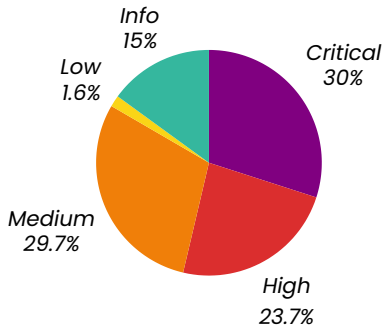
VVIP II

Pelaksanaan VVIP II ditemukan sebanyak **131 temuan** kerentanan dengan tingkat risiko *critical* sebanyak 25 kerentanan, *high* sebanyak 4 kerentanan, *medium* sebanyak 17 kerentanan, *low* sebanyak 11 kerentanan, dan *info* sebanyak 74 kerentanan.



VVIP III

Pelaksanaan VVIP III ditemukan sebanyak **246 temuan** kerentanan dengan tingkat risiko *critical* sebanyak 13 kerentanan, *high* sebanyak 45 kerentanan, *medium* sebanyak 59 kerentanan, *low* sebanyak 37 kerentanan, dan *info* sebanyak 92 kerentanan.



VVIP IV

Pelaksanaan VVIP IV ditemukan sebanyak **367 temuan** kerentanan dengan tingkat risiko *critical* sebanyak 110 kerentanan, *high* sebanyak 87 kerentanan, *medium* sebanyak 109 kerentanan, *low* sebanyak 6 kerentanan, dan *info* sebanyak 55 kerentanan.

09

LESSON LEARNED TOP 5 INSIDEN SIBER

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2024

INSIDEN DATA BREACH (KEBOCORAN DATA)

Data Breach adalah insiden di mana data yang sensitif, rahasia, atau dilindungi diakses, dicuri, atau diungkapkan oleh pihak yang tidak berwenang. Sering kali insiden ini terjadi akibat dari serangan siber, kesalahan manusia, kerentanan sistem, *insider threat*, atau penyimpanan data yang tidak aman. Data yang bocor dapat mencakup informasi pribadi seperti nama, alamat, data finansial seperti nomor kartu kredit, data medis hingga data rahasia perusahaan. Insiden ini dapat menyebabkan kehilangan privasi, kerugian finansial, kerusakan reputasi, serta pelanggaran regulasi yang berujung pada denda hukum.

SKEMA TERJADINYA INSIDEN

Information Gathering

Threat actor akan menentukan sasaran, melakukan pemindaian untuk mencari informasi dalam sistem yang dapat dieksploitasi. Selain itu, *threat actor* juga akan berupaya mendapatkan data pengguna yang dapat digunakan sebagai sasaran dalam serangan *phishing*.

Attack

Threat actor menggunakan informasi sistem yang telah diperoleh untuk mengeksploitasi sistem dan berusaha untuk tetap ada serta bahkan melakukan *lateral movement* ke administrator, atau dengan mengirimkan serangan *phishing* kepada pengguna yang sudah dikenali sebelumnya untuk menyebarkan *malware*.

Exfiltration Data

Setelah berhasil masuk ke sistem, *threat actor* akan mengakses dan mengekspor basis data atau dokumen penting lainnya. Informasi tersebut juga diperjual belikan di *darkweb*.

TOP 3 ATTACK VECTOR

Compromised Account T1586

Threat actor mengambil alih akun yang ada untuk mendukung proses penargetan, terutama dalam operasi rekayasa sosial.

Mitigasi:
Melakukan penguatan kebijakan pengelolaan akun dan pemantauan aktivitas yang mencurigakan.

Brute Force T1110

Threat actor dapat menebak kata sandi secara sistematis menggunakan mekanisme yang berulang atau iteratif. *Brute force* dapat terjadi di berbagai tahap, seperti saat mencoba mengakses akun sah dengan informasi yang diperoleh dari teknik lain, misalnya pengambilan kredensial (*OS Credential Dumping*), penemuan akun, atau kebijakan kata sandi.

Mitigasi :
- Menggunakan kebijakan penguncian akun (M1036).
- Mengimplementasikan autentikasi multifaktor (M1032).
- Menerapkan kebijakan kata sandi yang kuat (M1027).

Exploitation for Credential Access T1212

Threat actor dapat mengeksploitasi kerentanan dalam perangkat lunak untuk memperoleh akses tidak sah ke sistem dengan cara mencuri kredensial pengguna, seperti kata sandi atau token otentikasi.

Mitigasi :
- Memperbarui perangkat lunak secara berkala (M1050)
- Menggunakan alat deteksi kerentanan (M1019).

LESSON LEARNED INSIDEN DATA BREACH

01 *SCANNING* DAN PEMBARUAN KEAMANAN SECARA BERKALA

Salah satu langkah krusial dalam menjaga keamanan sistem adalah melakukan *scanning* kerentanan secara berkala. Hal ini bertujuan untuk mengidentifikasi celah keamanan yang mungkin dimanfaatkan oleh *threat actor* Hasil dari pemindaian ini harus ditindaklanjuti dengan segera, terutama untuk kerentanan dengan tingkat risiko tinggi. Pembaruan sistem secara berkala juga sangat penting untuk menutup celah keamanan yang telah diketahui dan mencegah eksploitasi lebih lanjut.

02 MENERAPKAN KRITERIA STRONG PASSWORD

Pengguna diharapkan dapat menerapkan kriteria *strong password* seperti membuat *password* dengan jumlah 8 karakter atau lebih dengan kombinasi alfanumerik dan simbol, tidak menggunakan *password* yang sama pada aplikasi atau sistem yang berbeda, serta mengganti *password* secara berkala.

03 MENERAPKAN AUTENTIKASI DUA *FACTOR* (2FA)

Penerapan 2FA seperti *password* dan OTP dapat mengurangi risiko *threat actor* berhasil *login* pada situs jika kredensial yang digunakan sudah ter-*compromise*.

04 MELAKUKAN PENONAKTIFAN LAYANAN SISTEM YANG TIDAK DIGUNAKAN

Sistem layanan yang tidak digunakan sebaiknya untuk dinon-aktifkan karena dapat menjadi risiko untuk disalahgunakan oleh *threat actor*. Selain itu, pemilik sistem disarankan untuk menutup *port* - *port* yang tidak digunakan, Hal ini diakibatkan karena layanan sistem dan *port* dapat digunakan oleh *threat actor*, salah satunya yang ditemukan oleh Tim adalah menggunakan SMB, SSH dan RDP untuk melakukan *lateral movement* dari salah satu yang terinfeksi kedalam sistem lainnya untuk menimbulkan dampak yang lebih besar.

05 MELAKUKAN *COMPROMISED ASSESSMENT*

Compromised Assessment dilakukan untuk mendeteksi adanya aktivitas *suspicious* atau *malicious* yang mungkin masih terjadi pada sistem serta mendeteksi artefak yang masih tertinggal pada sistem. Tujuan dari proses ini adalah untuk membersihkan sistem dari segala bentuk ancaman, mencegah penyebaran serangan ke sistem lain, serta memahami bagaimana serangan terjadi sehingga langkah-langkah pencegahan yang lebih baik dapat diterapkan di masa mendatang.

06 MENINGKATKAN *SECURITY AWARENESS*

Perlunya meningkatkan kesadaran keamanan di kalangan pengguna. Dengan memberikan informasi yang jelas dan terkini mengenai berbagai jenis ancaman siber, pengguna dapat lebih proaktif dalam menjaga keamanan data pribadi dan organisasi. Selain itu dapat menghimbau pengguna untuk tidak menggunakan akun dinas untuk keperluan pribadi seperti penggunaan pada *platform e-commerce*.

INSIDEN ILLEGAL ACCESSS

Kejadian *Illegal Access* merupakan tindakan memasuki atau menyusupi sistem komputer atau jaringan tanpa izin dari pemiliknya. Akses ilegal dapat dilakukan dengan berbagai tujuan, seperti: mencuri data sensitif, merusak sistem atau jaringan, melakukan penipuan, menyebarkan *malware*, dan mencari keuntungan finansial secara ilegal.

TOP 3 ATTACK VECTOR

***Command and Scripting Interpreter* (T1059)**

Threat actor dapat mengeksekusi perintah atau skrip berbahaya untuk mendapatkan akses atau menjalankan perintah tanpa izin di dalam sistem.

Mitigasi :

- Menggunakan antivirus untuk mendeteksi dan menangani *file* berbahaya.
- Nonaktifkan atau hapus *shell* atau *interpreter* yang tidak diperlukan (M1042).
- Melakukan audit terhadap instalasi skrip dan *interpreter* yang tidak sah (M1047).

***External Remote Services* (T1133)**

Threat Actor dapat menggunakan layanan jarak jauh yang menghadap ke luar, seperti VPN, Citrix, atau *Windows Remote Management*, untuk mendapatkan akses awal atau mempertahankan akses ke jaringan. Biasanya, akses ini membutuhkan kredensial yang diperoleh melalui pencurian atau akun yang telah ter-*compromise*. Selain itu, *Threat Actor* dapat memanfaatkan layanan terbuka tanpa autentikasi, seperti API *Docker* atau Kubernetes, untuk memperluas akses mereka ke lingkungan yang terkontainerisasi.

Mitigasi :

- Membatasi akses ke layanan jarak jauh melalui VPN atau konsentrator yang dikelola (M1035).
- Menggunakan kebijakan akses yang ketat untuk layanan jarak jauh (M1035).

***Content Injection* (T1659)**

Teknik di mana *Threat Actor* memasukkan atau memodifikasi konten dalam sistem atau komunikasi jaringan untuk memanipulasi target. Teknik ini dapat digunakan untuk mengelabui korban, menyebarkan perangkat lunak berbahaya, atau mencuri data dengan memanfaatkan celah keamanan pada saluran komunikasi, seperti koneksi antara klien dan server.

Mitigasi :

- Menggunakan VPN atau enkripsi lainnya untuk melindungi lalu lintas yang melibatkan data sensitif (M1021).
- Membatasi konten *web* yang diunduh atau ditransfer yang dapat digunakan dalam serangan (M1021).

LESSON LEARNED INSIDEN ILLEGAL ACCESS

01 MEMPERKUAT MEKANISME DAN MANAJEMEN AUTENTIKASI PENGGUNA YANG MENGAKSES *SERVER* SECARA *REMOTE*

Membatasi akses autentikasi akun untuk *remote access* dengan menerapkan sertifikat SSH, menentukan hak akses *root* secara selektif, dan melakukan *review* akses pengguna secara berkala.

02 MENERAPKAN KRITERIA STRONG PASSWORD

Pengguna diharapkan dapat menerapkan kriteria *strong password* seperti membuat *password* dengan jumlah 8 karakter atau lebih dengan kombinasi alfanumerik dan simbol, tidak menggunakan *password* yang sama pada aplikasi atau sistem yang berbeda, serta mengganti *password* secara berkala.

03 MELAKUKAN *BACKUP* SECARA TERPISAH

Backup data sangat penting dilakukan untuk menghindari *complete loss* ketika *server* telah terkompromi. Pastikan bahwa fitur *backup* aktif dan terjadwal secara berkala. Jika memungkinkan simpan *file backup* pada perangkat *offline/cloud* yang terpisah dengan sistem untuk menghindari kemungkinan *backup* diserang oleh *threat actor*.

04 MELAKUKAN *SECURITY HARDENING* PADA SERVER DAN APLIKASI

Hal tersebut dilakukan untuk mengurangi kemungkinan vektor serangan pada OS *server* baik pada *server* yang digunakan sehingga semakin sulit bagi para *threat actor* untuk menyerang *server* tersebut. Selain itu Pemilik Sistem diharapkan dapat memastikan bahwa semua fitur *debugging* telah di nonaktifkan ketika *server* sudah di-deploy dalam *production environment* agar celah yang ada tidak ditemukan *threat actor*.

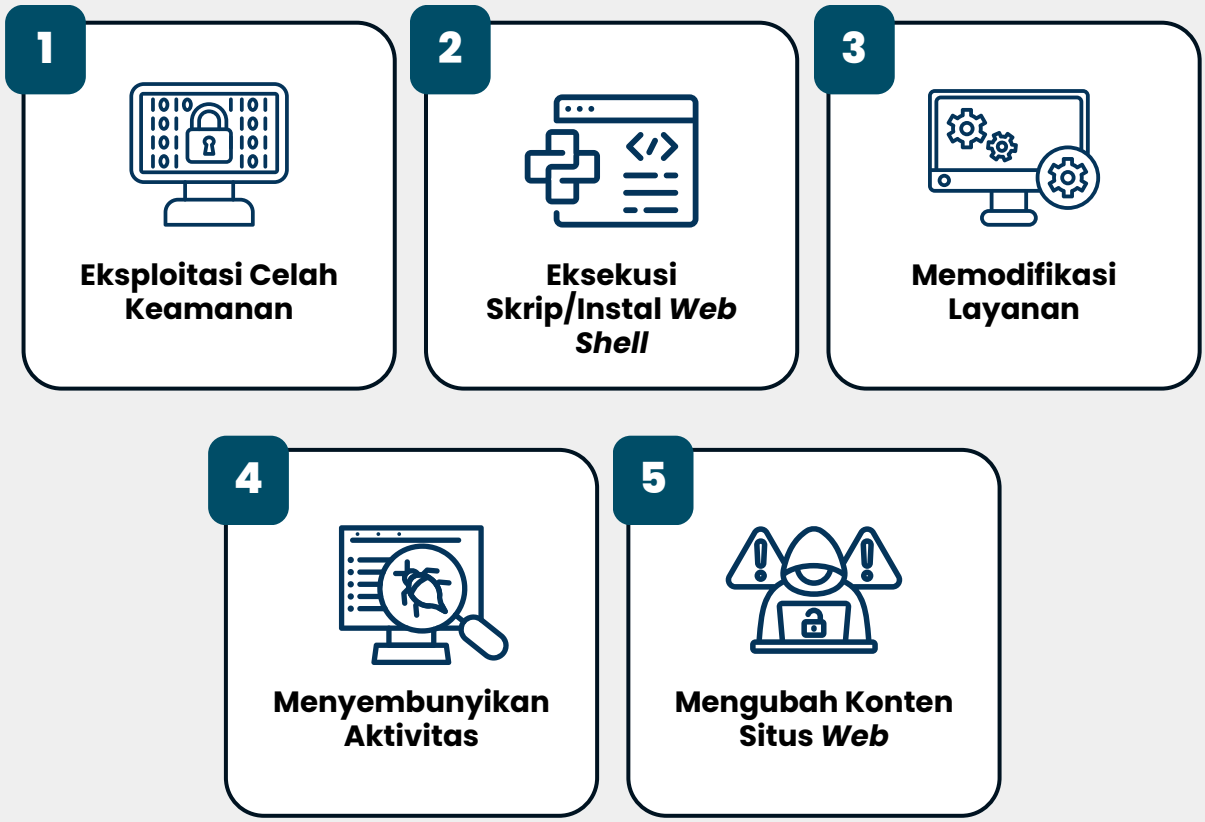
05 PEMANTAUAN DAN DETEKSI KEAMANAN

Pengguna diharapkan dapat memasang sistem pemantauan proaktif, seperti *Intrusion Detection System* (IDS) atau *Security Information and Event Management* (SIEM), untuk mendeteksi aktivitas mencurigakan secara *real-time*.

INSIDEN WEB DEFACEMENT

Web defacement adalah tindakan merusak atau mengubah tampilan sebuah situs web tanpa izin, biasanya oleh individu atau kelompok yang memiliki niat jahat. Tindakan ini sering kali dilakukan dengan mengeksploitasi kerentanan dalam sistem keamanan situs *web* untuk mendapatkan akses ke *server* dan mengubah konten di dalamnya. *Web defacement* biasanya dianggap sebagai bentuk *cybervandalism* dan bisa berdampak pada reputasi, kepercayaan pengguna, serta kerugian finansial bagi pemilik situs. Kejahatan ini sering ditangani melalui peningkatan keamanan sistem dan investigasi oleh pihak berwenang.

SKEMA TERJADINYA INSIDEN



TOP 3 ATTACK VECTOR

***Exploit Public-Facing Application* (T1190)**

Threat actor mengeksploitasi kelemahan pada sistem yang terhubung ke Internet, seperti *bug* perangkat lunak, gangguan sementara, atau kesalahan konfigurasi, untuk mendapatkan akses awal. Target umumnya adalah situs *web, server web*, basis data, layanan standar (SMB/SSH), atau protokol jaringan dengan soket terbuka.

Mitigasi :

- Menggunakan sistem *patch* manajemen (M1050).
- Melakukan pengujian keamanan berkala (M1044).

***Content Injection* (T1659)**

Teknik di mana *Threat Actor* memasukkan atau memodifikasi konten dalam sistem atau komunikasi jaringan untuk memanipulasi target. Teknik ini dapat digunakan untuk mengelabui korban, menyebarkan perangkat lunak berbahaya, atau mencuri data dengan memanfaatkan celah keamanan pada saluran komunikasi, seperti koneksi antara klien dan *server*.

Mitigasi :

- Menerapkan perlindungan WAF (M1030).
- Menggunakan pemantauan keamanan secara *real-time* (M1049).

***Server Software Component: Web Shell* (T1505.003)**

Threat Actor memasang *web shell* pada *server web* untuk mendapatkan akses berkelanjutan. *Web shell* adalah skrip yang memungkinkan akses ke *server* sebagai pintu masuk ke jaringan, dengan fungsi eksekusi atau sarana untuk menjalankan perintah.

Mitigasi :

- Menonaktifkan fitur *debugging* pada aplikasi produksi (M1041).
- Melakukan *hardening* pada *server* (M1026).

LESSON LEARNED WEB DEFACEMENT

01 PEMANTAUAN PROAKTIF DAN MELAKUKAN *COMPROMISED ASSESSMENT*

Melakukan pemantauan sistem secara berkelanjutan setelah insiden untuk mendeteksi aktivitas mencurigakan atau tanda-tanda serangan lebih lanjut. *Compromised Assessment* penting untuk memastikan tidak ada artefak berbahaya yang tertinggal, serta mendeteksi potensi akses yang belum terdeteksi sebelumnya. Langkah ini memastikan sistem tetap aman dan dapat menghindari serangan berulang.

02 PENGUJIAN KEAMANAN BERKALA

Melakukan pengujian keamanan secara rutin untuk mengidentifikasi kerentanannya sebelum dimanfaatkan oleh *threat actor*. Pengujian ini mencakup analisis terhadap jaringan, aplikasi, dan infrastruktur untuk menemukan celah yang mungkin ada. Pengujian keamanan yang konsisten membantu organisasi memastikan bahwa sistem pertahanan tetap efektif, dan semua kelemahan segera diperbaiki setelah ditemukan.

03 *SECURITY HARDENING* PADA *OPERATION SYSTEM, FRAMEWORK*, DAN *LIBRARY*

Melakukan *hardening* pada sistem operasi *server, framework,* dan *library* yang digunakan untuk mengurangi vektor serangan. Hal ini termasuk mengonfigurasi *server* dengan pengaturan keamanan yang ketat, menonaktifkan fitur yang tidak diperlukan, dan memastikan tidak ada *port* terbuka yang bisa dieksploitasi. Selain itu, fitur *debugging* harus dinonaktifkan pada *server* produksi untuk menghindari celah yang bisa dimanfaatkan *threat actor*.

04 PENGGANTIAN *PASSWORD* SECARA BERKALA

Melakukan penggantian *password server* dan akun pengguna secara rutin (minimal 3 bulan sekali) dan memastikan penggunaan *password* yang berbeda pada setiap perangkat atau akun. Ini penting untuk meminimalkan dampak dari serangan *brute force* atau rekayasa sosial yang dapat memanfaatkan kredensial yang bocor. Penggantian *password* yang tepat dapat memperkecil ruang lingkup potensi kompromi.

05 UPDATE DAN UPGRADE SOFTWARE SECARA RUTIN

Melakukan pembaruan dan *upgrade* pada semua perangkat lunak yang digunakan, baik untuk aplikasi, perangkat jaringan, maupun *server*. Dengan memastikan semua perangkat lunak dalam keadaan ter-*update*, organisasi dapat mengurangi risiko kerentanannya akibat *bug* atau celah keamanan yang ada pada versi lama, yang sering kali menjadi target utama bagi *threat actor*.

INSIDEN RANSOMWARE

Insiden *ransomware* adalah serangan siber yang disebabkan oleh *malware* yang menginfeksi perangkat dan mengenkripsi data yang terdapat pada perangkat tersebut Setelah menginfeksi perangkat, *ransomware* akan mengenkripsi *file-file* penting sehingga tidak dapat dibuka lagi. *Threat actor* kemudian akan meminta tebusan dalam bentuk uang digital untuk mengembalikan akses ke data yang telah dienkripsi. Serangan *ransomware* tidak hanya menyebabkan kerugian finansial, tetapi juga dapat mengganggu operasional bisnis dan merusak reputasi suatu organisasi. Untuk mencegah serangan ransomware, sangat penting untuk membuat cadangan data secara teratur, menggunakan perangkat lunak antivirus yang andal, dan selalu memperbarui sistem operasi serta aplikasi.

SKEMA TERJADINYA INSIDEN

1

Akses Awal

Threat actor mengakses sistem melalui *phishing* atau eksploitasi aplikasi publik

2

Eksekusi

Ransomware dijalankan melalui skrip atau eksploitasi perangkat lunak

3

Persistensi

Ransomware memodifikasi sistem untuk mempertahankan akses dan eksekusi otomatis

4

Peningkatan Hak Akses

Menggunakan kredensial yang dicuri atau mengeksploitasi kerentanannya untuk mendapatkan hak akses lebih tinggi

5

Penghindaran Deteksi

Menggunakan teknik *obfuscation* untuk menyembunyikan keberadaan dan membersihkan jejak serangan

6

Dampak

Mengenkripsi atau menghancurkan data untuk menyebabkan kerugian besar

TOP 3 ATTACK VECTOR

***Phishing* (T1566)**

Phishing adalah serangan yang dilakukan dengan mengirimkan pesan berbahaya untuk memperoleh akses ke sistem korban. *Threat actor* mengirim email berisi lampiran atau tautan berbahaya untuk mengeksekusi *malware*. Teknik lain termasuk memanipulasi metadata email atau memalsukan identitas pengirim. Korban juga dapat diarahkan untuk menelepon nomor tertentu yang mengarah pada URL berbahaya untuk mengunduh *malware* atau memasang alat jarak jauh.

Mitigasi :

- Melakukan edukasi kepada karyawan tentang *phishing* (M1017).
- Menggunakan alat deteksi *email* berbahaya (M1021).

***Exploitation for Initial Access* (T1203)**

Threat actor dapat mengeksploitasi kerentanannya dalam perangkat lunak untuk mendapatkan akses awal ke jaringan korban. Misalnya, mengeksploitasi kerentanannya dalam aplikasi yang tidak diperbarui (seperti Microsoft Office atau *browser*) atau perangkat lunak lainnya yang tidak di *patch*.

Mitigasi :

- Menerapkan *patch* perangkat lunak secara teratur (M1050).
- Menggunakan EDR untuk deteksi awal (M1040).

***Valid Accounts* (T1071)**

Threat actor sering menggunakan kredensial yang sah (mencuri atau membeli) untuk mengakses sistem yang lebih jauh, seperti menggunakan akun administrator untuk menyebarkan *ransomware* ke seluruh jaringan. Ini dapat mencakup penggunaan *Remote Desktop Protocol* (RDP) atau VPN.

Mitigasi :

- Menggunakan *Multi Factor Authentication* (MFA) (M1017).
- Melakukan pelatihan kepada pengguna untuk menghindari pemberitahuan yang mencurigakan (M1017).

LESSON LEARNED INSIDEN *RANSOMWARE*

01 KEBIJAKAN PENGGUNAAN *PASSWORD* DAN *MULTIFACTOR AUTHENTICATION*

Kebijakan penggunaan *password* dan MFA merupakan hal yang penting untuk meningkatkan keamanan sistem. Penggunaan *password* yang kuat, unik untuk setiap akun, dan menggantinya secara berkala dapat mengurangi risiko akses tidak sah. Penerapan MFA memberikan lapisan tambahan dengan mengharuskan autentikasi lebih dari satu metode.

02 PERLINDUNGAN LEVEL *ENDPOINT*

Perlindungan level *endpoint* adalah langkah-langkah yang diambil untuk melindungi perangkat akhir seperti komputer, laptop, dan perangkat *mobile* yang terhubung ke jaringan dari ancaman siber. *Antivirus*, *EDR*, serta *firewall* dapat membantu untuk mencegah, mendeteksi, dan merespons ancaman yang dapat mengeksploitasi kerentanannya. Selain itu, kebijakan pembaruan perangkat lunak dan *patching* yang rutin, kontrol akses berbasis peran, dan penggunaan enkripsi untuk melindungi data juga merupakan bagian penting dari perlindungan ini. Secara keseluruhan, perlindungan level *endpoint* bertujuan untuk mengurangi potensi vektor serangan yang dapat digunakan oleh *threat actor* untuk mengakses dan mengeksploitasi sistem.

03 SEGMENTASI JARINGAN

Penerapan segmentasi jaringan berbasis zona atau VLAN dengan aturan *firewall* yang ketat, menggunakan *micro-segmentation* untuk membatasi komunikasi antar sistem di dalam segmen jaringan serta tempatkan *SIEM, backup*, dan sistem keamanan lainnya di segmen terpisah dengan akses terbatas. Implementasikan solusi berbasis *Zero Trust* untuk membangun model keamanan yang lebih tangguh.

04 MELAKUKAN *BACKUP*

Backup yang efektif dilakukan secara rutin dan memastikan data terbaru selalu tersalin. Selain itu, metode backup yang berbeda seperti *full backup*, *incremental*, atau *differential* bisa diterapkan untuk efisiensi penyimpanan. Penyimpanan *backup* juga sebaiknya dilakukan di lokasi yang aman dan terpisah dari sistem utama untuk mengurangi risiko terhadap ancaman yang dapat mempengaruhi seluruh jaringan.

05 DISASTER RECOVERY PLAN

Recovery fokus pada penerapan strategi pemulihan untuk memulihkan sistem, memperbaiki kerusakan, dan melanjutkan operasional di perangkat alternatif asli atau baru. Pada selesainya *recovery*, sistem informasi akan berfungsi dan mampu menjalankan fungsinya kembali.

06 SUPPLY CHAIN MANAGEMENT

Membatasi hak akses pengguna dapat membantu mengurangi dampak serangan dengan memastikan bahwa hanya sistem yang terkompromi yang terpengaruh. Sebelum mengimplementasikan produk atau teknologi baru, penting untuk melakukan evaluasi menyeluruh, termasuk memeriksa reputasi produk dan respons *vendor* terhadap masalah keamanan. Selain itu, penting untuk memeriksa teknologi *Remote Monitoring & Management* (RMM) yang digunakan oleh mitra teknologi eksternal guna meminimalkan kerentanannya terhadap ancaman keamanan.

07 DUKUNGAN TOP LEVEL MANAGEMENT

Dukungan dari manajemen puncak sangat penting dalam memperkuat keamanan siber, termasuk dengan merekrut profesional yang kompeten, memastikan kepatuhan terhadap regulasi, serta menginvestasikan sumber daya untuk teknologi keamanan. Keputusan strategis yang berbasis analisis risiko dan pengawasan yang konsisten akan memastikan kebijakan keamanan tetap efektif dan relevan.

INSIDEN DDOS

Serangan siber di mana *threat actor* mencoba untuk membuat layanan atau situs *web* tidak dapat diakses oleh pengguna yang sah dengan membanjiri sistem target dengan lalu lintas jaringan yang sangat besar. Dalam serangan ini, *threat actor* menggunakan sejumlah besar perangkat yang terinfeksi untuk mengirimkan permintaan secara bersamaan, menyebabkan kelebihan beban pada *server* atau jaringan target, sehingga menghentikan layanan atau menyebabkan penurunan kinerja yang signifikan. Tujuan utama dari serangan DDoS adalah untuk mengganggu layanan dan menurunkan ketersediaan sumber daya yang diinginkan.

TOP 3 ATTACK VECTOR

01 ***Network Denial of Service* (T1498)**

Teknik ini bertujuan untuk membanjiri infrastruktur jaringan dengan lalu lintas yang sangat tinggi, sehingga menghabiskan sumber daya jaringan dan mengganggu ketersediaannya bagi pengguna yang sah.

Mitigasi :

- Menggunakan penyedia mitigasi DoS atau CDN untuk mencegah banjir lalu lintas (M1031).
- Menggunakan filter untuk memblokir lalu lintas serangan sebelum mencapai *server* target (M1060).

02 ***Endpoint Denial of Service* (T1499)**

Teknik ini menargetkan sistem atau aplikasi tertentu untuk mengganggu layanan di tingkat *endpoint*. Dengan membebani sumber daya sistem, serangan ini dapat mencegah operasi normal pada layanan yang di*hosting* di *endpoint* tersebut.

Mitigasi :

- Menyaring lalu lintas masuk di perbatasan jaringan dengan memblokir alamat IP yang digunakan dalam serangan (M1037).
- Menggunakan sistem deteksi intrusi dan *firewall* untuk membatasi akses ke *endpoint* (M1032).

03 ***Application Layer Denial of Service* (T1499.003)**

Serangan ini menargetkan aplikasi tertentu, seperti *server web* atau API, dengan mengirimkan sejumlah besar permintaan yang dirancang untuk membanjiri lapisan aplikasi. Tujuan serangan ini adalah untuk menghabiskan daya pemrosesan atau menyebabkan kerusakan pada aplikasi, yang akhirnya mengganggu ketersediaan layanan bagi pengguna.

Mitigasi :

- Menggunakan alat WAF untuk melindungi aplikasi *web* (M1030).
- Memantau permintaan aplikasi secara *real-time* (M1049).

LESSON LEARNED INSIDEN DDOS

01 PENINGKATAN KAPASITAS INFRASTRUKTUR

Meningkatkan kapasitas *bandwidth* dan *server* untuk menangani lonjakan lalu lintas yang tiba-tiba. Ini termasuk penggunaan layanan berbasis *cloud* atau infrastruktur elastis yang memungkinkan skalabilitas otomatis ketika terjadi serangan.

02 PENGGUNAAN *WEB APPLICATION FIREWALL* (WAF)

Implementasi WAF untuk melindungi aplikasi web dari serangan yang dapat memanfaatkan kerentanannya. WAF dapat membantu mengidentifikasi dan memblokir lalu lintas berbahaya yang dapat digunakan dalam serangan DDoS.

03 MELAKUKAN *BACKUP* SECARA TERPISAH

Backup data sangat penting dilakukan untuk menghindari *complete loss* ketika *server* telah terkompromi. Pastikan bahwa fitur *backup* aktif dan terjadwal secara berkala. Jika memungkinkan simpan *file backup* pada perangkat *offline/cloud* yang terpisah dengan sistem untuk menghindari kemungkinan *backup* diserang oleh *threat actor*.

04 MELAKUKAN *SECURITY HARDENING* PADA *SERVER* DAN APLIKASI

Hal tersebut dilakukan untuk mengurangi kemungkinan *vektor* serangan pada OS *server* baik pada server yang digunakan sehingga semakin sulit bagi para *threat actor* untuk menyerang *server* tersebut. Selain itu Pemilik Sistem diharapkan dapat memastikan bahwa semua fitur *debugging* telah di nonaktifkan ketika *server* sudah di-*deploy* dalam *production environment* agar celah yang ada tidak ditemukan *threat actor*.

05 PEMANTAUAN DAN DETEKSI KEAMANAN

Pasang sistem pemantauan proaktif, seperti *Intrusion Detection System* (IDS) atau *Security Information and Event Management* (SIEM), untuk mendeteksi aktivitas mencurigakan secara *real-time*.

10

PENGAMANAN SIBER PADA EVENT NASIONAL DAN INTERNASIONAL

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2024

EVENT DI 2024

BSSN berperan aktif di **7 *event* internasional** seperti F1H2O, WWF, IAF, IISF, MOTOGP, Pengamanan Siber pada Kunjungan Apostolik Paus Fransiskus, Bali *International Air Show* dan **6 *event* nasional** seperti PON, Pengamanan HUT RI, Pemilu dan Pilkada, Penyelenggaraan Forum *Group Discussion* NSOC dengan ISP/NAP dan *Stakeholder*, Penyelenggaraan Forum Eksistensi dan *Livehack Program* dan Pelantikan Presiden dalam menjaga keamanan siber melalui pengujian sistem, pemasangan alat deteksi dan *monitoring*, tanggap insiden dan *digital forensic incident response*. Proses ini mencakup fase pra pelaksanaan hingga *recovery pasca-event*, termasuk perbaikan celah keamanan yang terdeteksi.

01 F1H2O

Operasi pengamanan siber F1H2O 2024 dilaksanakan pada tanggal 26 – 6 Maret 2024 di Kabupaten Toba, Sumatera Utara. kegiatan ini bertujuan untuk memastikan seluruh aspek keamanan siber dan sandi berjalan optimal, mengurangi potensi ancaman, serta meningkatkan kepercayaan seluruh pihak terhadap keamanan teknologi informasi. Dengan pendekatan sistematis dan komunikasi yang intensif, pengamanan siber dan sandi ini berjalan dengan baik dan memberikan hasil yang memuaskan.

02 *INTERNASIONAL WORLD WATER FORUM* (WWF)

Pengamanan penyelenggaraan *World Water Forum* ke-10 di Bali telah dilaksanakan pada tanggal 18-24 Mei 2024. Dengan melibatkan berbagai pihak terkait, BSSN telah melakukan berbagai upaya seperti pembentukan satuan tugas khusus, koordinasi lintas lembaga, serta pengembangan sistem deteksi intrusi. Melalui upaya-upaya ini, BSSN berhasil menjaga keamanan data dan sistem informasi selama penyelenggaraan acara.

03 *INTERNASIONAL INDONESIA AFRICA FORUM* (IAF)

Operasi pengamanan siber HLF/MSP IAF Ke-2 tahun 2024 berlangsung selama 11 hari dari 27 Agustus hingga 6 September 2024, mencakup pemasangan perangkat *monitoring*, ITSA, pemantauan kebocoran data di *dark web*, penerapan *honeypot*, forensik digital, dan *compromise assessment*. Operasi ini bertujuan untuk menanggulangi potensi insiden siber dan mengatasi ancaman yang teridentifikasi selama kegiatan HLF/MSP IAF Ke-2.

04 *INDONESIA INTERNASIONAL SUSTAINABILITY FORUM* (IISF)

Tim Operasi Pengamanan Siber dan Sandi pada IISF 2024 berhasil melaksanakan pengamanan pada tanggal 4 s.d 7 September 2024 melalui metode *on-site* dan pemantauan dari NCC Jakarta dengan melibatkan 48 personel. Operasi mencakup perencanaan, persiapan, pelaksanaan, hingga pengakhiran dengan penggunaan teknologi keamanan mutakhir seperti sensor NIDS, EDR, *dark web monitoring*, dan perangkat kontra penginderaan.

05 MOTOGP

Operasi Pengamanan Siber dan Sandi *event internasional* gelaran MotoGP Mandalika dilaksanakan pada tanggal 20 s.d. 30 September 2024. Adapun tugas pokok Satgas yaitu memberikan dukungan keamanan siber dan sandi pada aset elektronik yang digunakan untuk penyelenggaraan MotoGP Mandalika 2024.

06 PEKAN OLAHRAGA NASIONAL

Dalam rangka mengamankan pelaksanaan PON XXI Aceh-Sumut 2024, BSSN mengirimkan Tim Satuan Tugas Operasi Pengamanan Siber dan Sandi pada kedua lokasi yaitu Aceh dan Sumatera Utara. Operasi Pengamanan Siber dan Sandi kegiatan PON XXI Aceh-Sumut 2024 dilaksanakan pada tanggal 25 Agustus s.d. 22 September 2024. Tugas pokok Tim Satuan Tugas PON XXI Aceh-Sumut 2024 adalah upaya deteksi dini serangan siber dan sandi, serta penyiapan skenario penanggulangan pemulihan terjadinya insiden keamanan siber dan sandi, sehingga penyelenggaraan dapat berjalan lancar dan aman.

07 HUT RI

BSSN membentuk sebuah Tim Pengamanan HUT RI Ke-79 yang bertugas sejak tanggal 26 Juli hingga 20 Agustus 2024. Pengamanan kegiatan dilakukan di dua lokasi yaitu di Istana Garuda Ibu Kota Nusantara dan Istana Merdeka Jakarta. Tim Pengamanan Siber HUT Republik Indonesia ke-79 dimaksudkan untuk melakukan identifikasi, deteksi, proteksi, pemantauan serta penanggulangan dan pemulihan segala potensi insiden keamanan dan ancaman baik yang bersumber dari dalam maupun luar negeri yang difokuskan pada penyelenggaraan kegiatan HUT RI Ke-79.

Sesuai dengan Peraturan Presiden No. 63 Tahun 2022 tentang Perincian Rencana Induk Ibukota Nusantara, BSSN diberikan mandat untuk menyusun tata kelola terkait IKN. Oleh karena itu, BSSN telah menyiapkan *Grand Design SSOC* IKN, Pengujian Keamanan Sebelum dan Setelah *Go Live* Pada Layanan IKN, Standar Keamanan Aplikasi Pada Kementerian/Lembaga IKN, Standar Keamanan Pertukaran Data Pada Kementerian/Lembaga IKN v1.0, Standar Keamanan Jaringan Pada Kementerian/Lembaga IKN.

08 PEMILIHAN UMUM DAN PEMILIHAN KEPALA DAERAH TAHUN 2024

Satuan Tugas Operasi Pengamanan Siber dan Sandi Pemilu BSSN (Satgas Pamsibersan BSSN) mengamankan aspek siber dan sandi pada pelaksanaan pemilihan umum serentak tahun 2024 yang mencakup Pemilihan Presiden/Wakil Presiden, Pemilihan Anggota Legislatif dan Pemilihan Kepala Daerah. Kegiatan pengamanan siber dan sandi untuk mendukung Pemilu & Pilkada 2024 telah dilakukan di seluruh provinsi di Indonesia dan berjalan dengan lancar. Satgas merespons gangguan yang ada serta telah mendeteksi dan mengatasi berbagai ancaman dengan cepat.

09 PENGAMANAN SIBER PADA KUNJUNGAN APOSTOLIK PAUS FRANSISKUS

Pengamanan kedatangan Paus Fransiskus ke Indonesia dilakukan secara menyeluruh untuk memastikan keamanan beliau selama kunjungannya. Langkah-langkah pengamanan melibatkan berbagai elemen, termasuk pengamanan siber dan sandi yang dilakukan oleh BSSN. Pengamanan dimulai sejak hari pertama persiapan kedatangan hingga selesai acara resmi yang direncanakan berlangsung selama beberapa hari. Pelaksanaan pengamanan dilakukan pada 3-6 September 2024. Termasuk saat hari ibadah Misa Agung yang dipimpin oleh Paus Fransiskus pada Kamis, 5 September 2024 di Stadion Gelora Bung Karno (GBK).

10 PENYELENGGARAAN *FORUM GROUP DISCUSSION* NSOC DENGAN ISP/NAP DAN *STAKEHOLDER*

Forum Group Discussion (FGD) NSOC adalah kegiatan kolaborasi lintas sektor yang dilaksanakan Direktorat Operasi Keamanan Siber BSSN pada 16 Juli 2024 di Hotel Aston *Priority* Simatupang, Jakarta Selatan. Kegiatan ini menjadi inisiatif strategis untuk memperkuat kerjasama operasional dan implementasi kebijakan keamanan siber antara BSSN dan pemangku kepentingan dalam pelaksanaan operasional *monitoring* keamanan siber, yaitu *Internet Service Providers* (ISP), *Network Access Providers* (NAP), dan *stakeholder* sektor Pemerintahan. Pada Tahun 2024, kegiatan FGD NSOC mengusung tema "Sinergi dan Kolaborasi dalam Mewujudkan Keamanan Siber Nasional".

11 PENYELENGGARAAN FORUM EKSISTENSI DAN *LIVEHACK PROGRAM*

Rangkaian forum Eksistensi dan *Livehack* yang diselenggarakan sepanjang tahun 2024 dihadirkan sebagai ruang diskusi interaktif bagi perwakilan berbagai instansi pemerintah, akademisi, serta mahasiswa yang tertarik pada isu-isu pertahanan dan keamanan siber. Kegiatan ini bertujuan untuk memfasilitasi dialog terbuka serta bertukar gagasan mengenai strategi - strategi efektif dalam menangani ancaman siber yang semakin kompleks. Melalui forum ini, peserta diharapkan dapat memperoleh wawasan mendalam mengenai tantangan dan solusi terkait keamanan siber nasional.

12 BALI *INTERNATIONAL AIR SHOW*

Kegiatan pengamanan siber dan sandi pada Penyelenggaraan Bali *International Air Show* 2024 (BIAS 2024) dilaksanakan pada tanggal 18-21 September 2024 di *General Aviation* Ngurah Rai *International Airport*. Tim operasi yang melibatkan personil dari Direktorat Operasi Keamanan Siber dan Komunikasi Publik telah melaksanakan rangkaian kegiatan pengamanan berupa identifikasi aset, pelaksanaan ITSA, dan pemasangan sensor pada aset TIK yang digunakan pada pelaksanaan BIAS 2024.

13 PELANTIKAN PRESIDEN

Tim BSSN melaksanakan tugas pengamanan siber dan informasi selama pelantikan Presiden dan Wakil Presiden 2024 di Jakarta pada 19-21 Oktober, dengan posko utama di Hotel Sultan, Jakarta. Pengamanan mencakup pemantauan trafik jaringan dan data, serta monitoring informasi di media *online* dan sosial terkait acara tersebut. Selain itu, pengamanan sinyal dilakukan untuk memastikan keamanan komunikasi di Gedung DPR/MPR dan Istana Negara.

11

KOLABORASI KERJASAMA & KOMPETISI INTERNASIONAL

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2024

KOLABORASI NASIONAL

01 *Cyber Investigative Tools and Exercise*

BSSN mengirimkan 4 (empat) delegasi dalam Pelatihan yang diadakan oleh *Federal Bureau of Investigation* (FBI) bersama *National Cyber-Forensics and Training Alliance* (NCFTA) bertema "*Cyber Investigative Tools and Exercise*" yang dilaksanakan pada tanggal 18–22 November 2024 di Bali.

Pelatihan ini bertujuan untuk meningkatkan kemampuan para peserta dalam investigasi melalui Peralatan dari sumber terbuka dan media sosial atau *open-source intelligence* (OSINT), analisis domain (peralatan analisis *domain*, WHOIS, dan DNS pasif), Kripto - dengan demonstrasi/latihan, peralatan OSINT untuk menelusuri *Dark Web*, serta studi kasus. Pelatihan ini juga diikuti oleh instansi-instansi seperti POLRI dan PPATK yang memiliki peran penting untuk bekerja sama dan berkolaborasi dalam melakukan investigasi kejahatan di dunia siber.

02 *Data 4 Development (D4D) Fellowship Program*

Kegiatan *Data 4 Development (D4D) Fellowship Program* yang diselenggarakan oleh *Commonwealth Scientific and Industrial Research Organization* (CSIRO) bertujuan untuk meningkatkan kemampuan spesialis data dari lembaga pemerintah di Indonesia.

Program ini bertujuan untuk:

1. Pengembangan keahlian teknis: Memberikan pelatihan dan bimbingan untuk memecahkan masalah kompleks yang terkait dengan pengembangan dan penggunaan data.
2. Kolaborasi internasional: Menghubungkan peserta dengan komunitas riset di Australia dan membangun hubungan kelembagaan jangka panjang antara organisasi Australia dan Indonesia.
3. Pengembangan kapasitas institusional: Meningkatkan kemampuan data di lembaga asal peserta, dengan dukungan mentor dari lembaga tuan rumah.
4. Kontribusi pembangunan ekonomi: Mendorong pertumbuhan ekonomi yang berkelanjutan, pengurangan kemiskinan, dan stabilitas di Indonesia.

03 *PORT SECURITY WORKSHOP*

Kedutaan Besar Amerika Serikat menyelenggarakan *Port Security Workshop* di Surabaya pada tanggal 10-14 Juni 2024. *Workshop* ini bertujuan untuk meningkatkan pemahaman dan kapasitas dalam keamanan pelabuhan, termasuk perlindungan terhadap ancaman siber dan fisik yang relevan di area pelabuhan. Pelatihan ini melibatkan ahli dari Amerika Serikat sebagai narasumber utama serta diikuti oleh perwakilan dari instansi terkait di Indonesia, termasuk Badan Siber dan Sandi Negara (BSSN). Kegiatan ini akan membahas strategi keamanan, manajemen risiko, dan praktik terbaik yang dapat diterapkan untuk menjaga keamanan operasional pelabuhan.

04 OIC CERT *Technical Workshop*

Pada 2024, BSSN menyelenggarakan dua webinar penting untuk memperkuat keamanan siber. Webinar pertama, OIC-CERT Technical Webinar 2024, dilaksanakan pada 23 Oktober dengan tema "*Securing The Future: Threat Information Sharing and Prediction on Critical Infrastructure Sector*", menghadirkan Bapak Basuki Erwin Setiyadi untuk membahas *cyber threat intelligence*. Webinar kedua, OIC-CERT *Technical Workshop* 2024, berlangsung pada 21 November dengan tema "*Collaborative Strategy to Improve Cyber Security in Indonesia*", yang menghadirkan Bapak Indra Adi Putra dan membahas *Voluntary Vulnerability Identification and Protection Program* (VVIP Program) serta interaksi dengan *bug hunter*. Kedua kegiatan ini memperkuat kolaborasi BSSN dengan OIC-CERT, ID-SIRTII, *stakeholder*, dan komunitas untuk meningkatkan keamanan siber nasional.

05 *Workshop Ransomware Detection and Response*

Workshop dari Trellix ini dirancang untuk membantu Team *cybersecurity* untuk memahami berbagai jenis *ransomware*, cara mendeteksi dan merespons serangan *ransomware*, serta *best practices* untuk melindungi data dan sistem dari serangan *ransomware*. Narasumber dalam kegiatan ini adalah Gary Woo sebagai Trellix *Cybersecurity Practitioner* dan Sharon Lekahena sebagai Trellix *Solution Engineer*.

06 Pelatihan *Digital Talent Scholarship* Kementerian Komunikasi dan Informatika 2024

Digital Talent Scholarship (DTS) 2024 Professional Academy Batch 1 adalah program pelatihan daring yang diselenggarakan oleh Kementerian Komunikasi dan Informatika. Program ini bertujuan untuk mengembangkan kompetensi Pegawai Negeri Sipil, termasuk pegawai BSSN, guna mendukung tugas dan fungsi instansi. Pelatihan ini mencakup berbagai tema seperti *Cloud Computing, Machine Learning, Python, Data Engineering*, dan *Data Analytics*. Dengan kuota 3.100 peserta, pelatihan berlangsung dari 12 Februari - 31 Maret 2024.

07 *FBI Digital Forensics Training*

Federal Bureau of Investigation (FBI) menyelenggarakan Pelatihan *Digital Forensic* yang dihadiri oleh perwakilan penyidik, *security analyst, cyber threat intelligence analyst, incident response team*, dan *forensic analyst* dari beberapa instansi yang memiliki kepentingan sebagaimana tema pelatihan. Kegiatan pelatihan ini dilaksanakan pada tanggal 31 Juli - 2 Agustus 2024 bertempat di Gedung Presisi Divisi TIK Mabes Polri, Kota Jakarta Selatan, DKI Jakarta. Kegiatan ini dilaksanakan sebagai wadah untuk meningkatkan keterampilan para pemangku kepentingan dalam hal menganalisis *log* baik dalam Sistem Operasi Windows maupun Linux, meningkatkan kemampuan *Threat Hunting*, serta meningkatkan kemampuan dalam menganalisis *log* melalui *Security Information and Event Management* (SIEM). Selain itu, dalam sesi pelatihan ini juga disampaikan hal-hal yang berkaitan dengan tahapan-tahapan dalam menangani insiden siber, *tools* OSINT yang dapat dimanfaatkan untuk pengayaan informasi, serta tools yang dapat dimanfaatkan untuk melakukan analisis *malware* ataupun untuk keperluan *digital forensic*.

08 Pelatihan SANS SEC 511

Pelatihan SEC 511: *Cybersecurity Engineering*: *Advance Threat Detection and Monitoring* merupakan pelatihan yang diselenggarakan oleh SANS Institute pada tanggal 13-18 Mei 2024 secara daring. Pelatihan ini bertujuan untuk membekali peserta pelatihan dengan pengetahuan dan keterampilan untuk melindungi dan memantau aset digital. Pelatihan ini mengeksplorasi mengenai teknik dalam melakukan *monitoring* pada *cloud*, *Network Detection and Response* (NDR), *Endpoint Detection and Response* (EDR), *Security Information and Event Management* (SIEM), *Endpoint Protection Platform* (EPP), *Secure Access Service Edge* (SASE), *Endpoint Protection Platform* (EPP), *Zero Trust, Generative Artificial Intelligence* (GenAI), *Large Language Model* (LLM) *Application Defense*, dan kapabilitas lain dalam melakukan *threat detection* serta *threat hunting*. Selain melakukan pelatihan, terdapat pelaksanaan sertifikasi GIAC GMON untuk menunjukkan bahwa peserta telah memiliki pengetahuan dan keterampilan yang diajarkan.

09 WORKSHOP ON CYBER AWARENESS

Office of Defence Cooperation (ODC) *Chief and the Institute for Security Governance* (ISG) menyelenggarakan *Workshop On Cyber Awareness* pada tanggal 13-14 November 2024 di Jakarta. *Workshop* ini menjelaskan tentang perkembangan lanskap ancaman siber dan menunjukkan kerentanan yang dapat berpotensi menjadi ancaman siber yang lebih *advance*. Materi yang disampaikan pada kegiatan ini adalah *Understanding Cyber Mission Dependencies*, selain itu terkait *Cyber Resilience and Mitigation Strategies*.

KOLABORASI INTERNASIONAL

01 UNODC *Regional Ransomware Training Exercise* (2nd *Batch*)

Kegiatan UNODC *Regional Ransomware Training Exercise* (2nd *Batch*) merupakan kegiatan pelatihan yang diadakan oleh *United Nation Office on Drugs and Crime* (UNODC) di Manila pada tanggal 16-19 Januari 2024. Kegiatan diikuti oleh perwakilan dari beberapa negara di ASEAN, diantaranya Indonesia, Malaysia, Thailand, Vietnam, Filipina, Kamboja, dan Laos.

Pelatihan ini memberikan materi dan wawasan terkait dengan investigasi digital terkait dengan kasus *ransomware* melalui pemberian materi dan praktik kelompok. Kegiatan ini memberikan wawasan pemahaman mengenai investigasi *ransomware*, penanganan barang bukti elektronik, dan juga hubungan kerja sama nasional dan internasional dalam rangka bantuan hukum dan teknis. Peserta dikenalkan juga dengan *open source tools* yang dapat digunakan untuk melakukan investigasi *ransomware*.

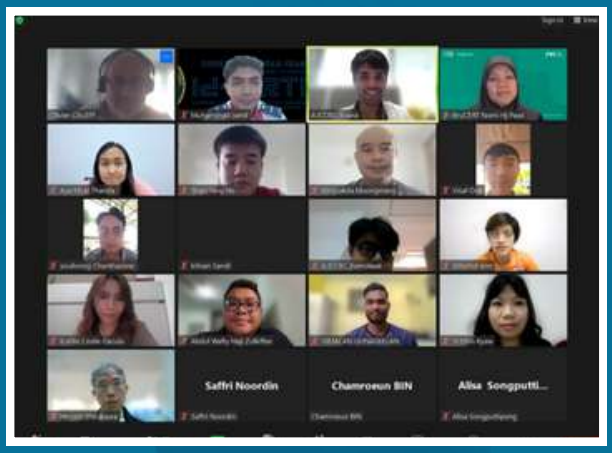
02 OIC *Gulf Information Security Expo* & *Conference* (GISEC GLOBAL) Dubai

Pada 23-25 April 2024, BSSN dan Huawei berpartisipasi dalam GISEC GLOBAL 2024 di Dubai, Uni Emirat Arab, yang dihadiri oleh profesional keamanan siber dan pakar dari seluruh dunia. Salah satu kegiatan utama yang diikuti BSSN adalah *cyber drill*, simulasi serangan siber terbaru yang melibatkan 108 negara dan mencatatkan rekor dunia di Guinness.

BSSN juga turut serta dalam *working group* OIC-CERT yang membahas keamanan 5G dan *Cloud* serta aktif dalam *Cybersecurity Enablement Bootcamp* untuk memperoleh wawasan tentang legislasi dan standar keamanan siber. Sebagai *Deputy Chair* OIC-CERT, BSSN mendukung pameran Kolaborasi OIC CERT & Huawei, yang menunjukkan komitmen sektor publik dan swasta dalam membangun ruang siber yang aman. Partisipasi ini menegaskan pentingnya kolaborasi global dalam mengatasi tantangan keamanan siber.

03 Pelatihan AJCCBC *(Security Incident Management Maturity Model and Jupyter Notebooks In Incident Response)*

ASEAN-Japan *Cybersecurity Capacity Building Centre's Training* (AJCCBC) adalah program pelatihan yang bertujuan untuk meningkatkan kapasitas dan kompetensi para profesional keamanan siber di kawasan ASEAN. Pelatihan ini mencakup berbagai topik dalam keamanan siber, yaitu *Security Incident Management Maturity Model* (SIM3) pada tanggal 26-27 Juni 2024 dan *Jupyter Notebooks In Incident Response* pada tanggal 3-4 Juli 2024.



04 *UNODC Regional Exercise on the Handling of Digital Evidence for Cases Related to Business Email Compromise and Online Scams*

Pertemuan regional yang diselenggarakan oleh UNODC pada 2–4 Oktober 2024 akan memberikan pelatihan penanganan bukti digital untuk kasus-kasus yang terkait dengan peretasan *email* bisnis dan penipuan daring. UNODC melalui pertemuan regional ini mengundang peserta dari beberapa lembaga-lembaga pemerintah yang memiliki keahlian dalam kejahatan dunia maya yang terkait dengan penipuan daring dan peretasan *email* bisnis, serta bukti elektronik.

05 *Real Cyber Security Exercise* (RCSE)

Kegiatan *Real Cyber Security Exercise* (RCSE) merupakan *cyber exercise* yang dirancang untuk meningkatkan kemampuan teknis *cyber expert*, khususnya tim tanggap insiden siber agar lebih siap dalam menghadapi serangan siber yang semakin kompleks. RCSE dilatarbelakangi oleh kesenjangan antara serangan siber yang terus berkembang dengan skenario *exercise* yang digunakan selama ini. Kegiatan ini dilaksanakan pada tanggal 4-15 November 2024.



06 UNODC *Training Course on Collection, Investigation, Preservation, Handling, and Management of Digital Evidence during a Ransomware Event*

United Nations Office on Drugs and Crime (UNODC) menyelenggarakan pelatihan pada 19-21 November 2024 di Jakarta mengenai manajemen pengambilan bukti yang dapat digunakan di persidangan pada saat terjadi insiden *ransomware*. BSSN mengirimkan 9 (sembilan) orang perwakilan untuk turut serta berpartisipasi mengikuti pelatihan ini. Selain itu, pelatihan ini juga dihadiri oleh instansi lain yakni perwakilan Polisi, PPATK, Kejaksaan, dan Hakim yang berkantor di Jakarta.

07 UNODC *Training on Operational Cooperation Between Law Enforcement Authorities and Computer Emergency Response Teams (CERTs) on Ransomware and Cyber-Attacks on Critical Infrastructures*

UNODC menyelenggarakan pelatihan pada 25-27 November 2024 yang bertempat di Kuala Lumpur, Malaysia. Pelatihan ini membahas mengenai penanganan insiden siber pada infrastruktur vital dan pelacakan alamat kripto pada studi kasus *ransomware* yang semakin marak di seluruh dunia. Pada pelatihan ini, BSSN turut berpartisipasi dengan mengirimkan 2 (dua) orang perwakilan. Selain itu, pelatihan ini dihadiri oleh perwakilan Penegak Hukum dan *Cybersecurity Analyst* beberapa Negara ASEAN diantaranya Vietnam, Malaysia, Thailand, Filipina, dan Indonesia.

08 2nd *Egypt Cybersecurity & Data Integration Systems Conference (CDIS)* Mesir

2nd *Egypt Cybersecurity & Data Integration Systems Conference* (CDIS) berlangsung pada 18-22 Mei 2024 di *Egypt International Exhibition Center*, Kairo, Mesir. Dalam rangkaian kegiatan CDIS 2024 ini, delegasi BSSN Indonesia diwakili oleh Taufik Nurhidayat selaku Ketua Pelaksana ID-SIRTII, turut berpartisipasi sebagai panelis dalam diskusi bertajuk *Shaping the Future of Cybersecurity in an Era of Complex Information Challenges*. Kegiatan ini juga mencakup sesi *Courtesy Call* dengan Duta Besar Indonesia untuk Mesir, serta *Board Meeting* yang dihadiri oleh perwakilan dari Indonesia, Oman, Malaysia, Azerbaijan, Uni Emirat Arab, dan Mesir untuk membahas laporan kegiatan, kondisi keuangan, kendala pelaksanaan, serta rencana perubahan *manual operation*.

09 *Japan International Cooperation Agency (JICA)*

Program "*Defense Practice Against Cyber Attacks*" adalah pelatihan peningkatan kapasitas SDM yang diselenggarakan oleh JICA bekerja sama dengan negara-negara di kawasan Asia-Pasifik. Pelatihan ini berlangsung pada 19 Mei - 1 Juni 2024 di JICA Tokyo Center, dengan menggandeng Trend Micro sebagai *trainer* utama. Program ini dirancang untuk memperkuat kemampuan menghadapi serangan siber melalui berbagai kegiatan, seperti sesi kelas, aktivitas laboratorium berbasis *cloud*, serta kunjungan lapangan ke Trend Micro dan JSOC.

Kegiatan ini diikuti oleh 20 peserta dari 11 negara, termasuk Indonesia, Malaysia, Kyrgyzstan, Bhutan, Bangladesh, Vietnam, Mongolia, Thailand, Cook Island, Kamboja, dan Laos, yang masing-masing mewakili berbagai institusi dan keahlian di bidang keamanan siber.

10 *WORKSHOP FOR REGIONAL CERT COOPERATION AND CYBERSECURITY STANDARDS IN ASEAN*

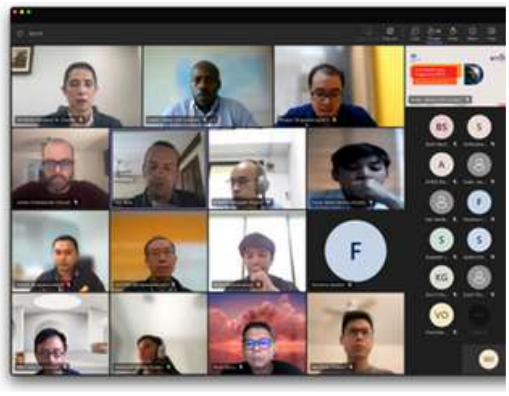
Workshop for Regional CERT *Cooperation and Cybersecurity Standards in* ASEAN, yang diselenggarakan oleh Ministry of Internal Affairs and Communications (MIC) Japan pada 12-13 Desember 2024 di Tokyo, Jepang. MIC Japan juga mengundang perwakilan dari negara-negara anggota ASEAN, termasuk delegasi ADGSOM (ASEAN Digital Senior Officials Meeting) dan ANSAC (ASEAN Network Security Action Council), untuk berpartisipasi dalam kegiatan ini.

Melalui kolaborasi ini, diharapkan dapat tercapai penguatan kapasitas, pertukaran pengetahuan keamanan siber, dan harmonisasi kebijakan yang mendukung ekosistem digital yang aman dan inovatif di kawasan ASEAN.

11 OIC-CERT *Board Meeting* Muscat

BSSN Indonesia menghadiri The 12th *Regional Cybersecurity Summit* pada 28-29 Oktober 2024 di Muscat, Oman, yang membahas strategi terbaik dalam keamanan siber dan inovasi untuk ekonomi digital. Delegasi BSSN, Novian Nur Cahya dan Renaltha Puja Bagaskara, berpartisipasi dalam diskusi panel dan melakukan *Courtesy Call* kepada Duta Besar Indonesia untuk Oman, Mohamad Irzan Djohan, membahas perpanjangan kepengurusan OIC-CERT.

Selain itu, ID-SIRTII Indonesia meraih peringkat 1 dalam dua skenario simulasi pada *Regional Cyber Drill* 30-31 Oktober 2024. Partisipasi BSSN menegaskan komitmen Indonesia dalam kolaborasi global untuk keamanan siber.



12 *1OIC-CERT Mobile World Congress*, Spanyol

Delegasi BSSN Indonesia berpartisipasi dalam serangkaian kegiatan OIC-CERT yang diselenggarakan bersamaan dengan MWC 2024 pada 26 Februari hingga 1 Maret 2024. OIC-CERT, yang berada di bawah Organisasi Kerja sama Islam (OIC), adalah forum kerja sama keamanan siber antar negara-negara OKI. Kegiatan ini mencakup OIC-CERT *Special Board Meeting* dan OIC-CERT *Cybersecurity Roundtable Discussion*. OIC-CERT *Board Meeting* dilaksanakan setiap 2-3 bulan, dengan rapat fisik kali ini diadakan bersamaan dengan MWC 2024, dihadiri oleh anggota seperti Oman, Malaysia, Indonesia, Uni Emirat Arab, Azerbaijan, Mesir, dan Brunei. Rapat membahas capaian KPI 2023, rencana KPI 2024, dan urgensi lainnya. Sementara itu, *Cybersecurity Roundtable Discussion* diikuti oleh anggota OIC-CERT, termasuk Bangladesh, Nigeria, dan Yordania. Diskusi membahas legislasi, peraturan keamanan siber, serta peran pemangku kepentingan dalam ketahanan dan jaminan keamanan siber.

13 29th AJCCBC Cybersecurity Technical Training – J5 Penetration Test Training ASEAN-JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE (AJCCBC)

ASEAN-Japan Cybersecurity Workforce menyelenggarakan 29th AJCCBC *Cybersecurity Technical Training – J5 on Penetration Test* di Bangkok, Thailand pada tanggal 22–26 Januari 2024. Pelatihan ini bertujuan untuk memenuhi kebutuhan akan pelatihan uji penetrasi sebagaimana tercermin dari *ASEAN-Japan Cybersecuity Workforce Survey* 2021. Pelatihan ini difokuskan untuk membangun pemahaman mendalam tentang perencanaan, ruang lingkup uji penetrasi, serta analisis kerentanan dalam sistem informasi. Modul pelatihan disusun berdasarkan standar internasional, dengan mengacu pada modul uji penetrasi dari CompTIA.

14 *ASEAN-Japan Cybersecurity Capacity Building Centre's Training (AJCCBC) Core Testing Capabilities and Defence in Depth*

Tim BSSN dilibatkan sebagai peserta dalam kegiatan "*Cyber 'Bootcamp' for Managers* dan *Core Testing Capabilities and Defence in Depth*" yang diselenggarakan oleh AJCCBC bekerja sama dengan British Embassy Jakarta. Pelatihan pada 6–7 Februari 2024 mengangkat tema *Cyber 'Bootcamp' for Managers*. Pokok bahasan pelatihan mencakup edukasi tentang lanskap keamanan siber terkini, jenis ancaman yang dihadapi organisasi, serta pentingnya keamanan siber dalam dunia digital saat ini. Pelatihan pada 8–9 Februari 2024 bertema *Core Testing Capabilities and Defence in Depth*. Bahasan utama mencakup identifikasi kerentanan melalui teknik seperti pengujian penetrasi, penilaian efektivitas kontrol keamanan, serta integrasi pengujian ke dalam siklus hidup pengembangan.


15 Positive Hack Days Fest 2

Positive Technologies mengundang perwakilan dari BSSN untuk bergabung sebagai Tim Biru dalam kegiatan Standoff. Kehadiran BSSN diharapkan dapat memberikan kontribusi signifikan dalam harmonisasi upaya keamanan siber global, sekaligus memperkuat hubungan antara komunitas keamanan siber Indonesia dengan para ahli dan profesional di seluruh dunia. Acara ini diadakan di Moskow, Rusia, pada tanggal 23-26 Mei 2024 dan akan menawarkan berbagai sesi, termasuk presentasi, lokakarya, dan kompetisi yang dirancang untuk meningkatkan keterampilan dan pemahaman peserta tentang tren dan teknologi terbaru dalam keamanan siber.

15 UNODC *Training Cybercrime and Online Fraud Investigation Training Course: Identification, Investigation Techniques and Best Practises*

UNODC menyelenggarakan kegiatan pelatihan nasional lintas lembaga di tempat sebagai bagian dari teknis untuk memerangi dan mencegah penipuan *online*, dan kejahatan terkait mata uang kripto, serta penanganan bukti digital dengan prinsip-prinsip hak asasi manusia dan proses hukum, tetapi juga untuk mengembangkan budaya kerja sama, baik di tingkat nasional maupun internasional antara lembaga penegak hukum dan sektor swasta. Pelatihan ini memberikan gambaran umum dan teknik investigasi kepada para peserta mengenai kompromi *email* bisnis, tipologi penipuan *online* dan penggunaan mata uang kripto secara ilegal dalam penipuan tersebut. Kegiatan ini mencakup pengumpulan bukti, penerapan teknik OSINT, serta kerja sama internasional dalam memperoleh bukti digital dan melacak transaksi mata uang kripto.

16 *Global Cybersecurity Camp* 2024

Global Cybersecurity Camp (GCC) merupakan program pelatihan keamanan siber internasional tahunan yang berlangsung selama 1 minggu. Kegiatan ini bertujuan memperkuat komunitas keamanan di seluruh Asia dan membina pemimpin global masa depan. GCC memiliki misi untuk memperkuat komunitas keamanan di seluruh Asia dan membina *future leader* secara global. Sejumlah 50 delegasi terbaik dari 10 negara anggota berkumpul untuk bertukar pengalaman, menjalin persahabatan seumur hidup, dan belajar dari para profesional terbaik dibidang *cyber security*. Program ini didukung oleh para pemimpin industri yang peduli terhadap digitalisasi yang aman di dunia. Dari acara-acara sebelumnya sejak tahun 2018 ada beberapa negara yang turut berpartisipasi juga sebagai panitia penyelenggara di GCC, yaitu Singapore, South Korea, Taiwan, Thailand, Vietnam, Australia, Malaysia, Japan. Selain itu, banyak organisasi dan perusahaan atau industri di setiap negara komite yang bermitra dan mensponsori seluruh delegasi dari masing-masing negara.

17 *32nd AJCCBC Cybersecurity Technical Training – J9 on Cyber Defense Exercise with Recurrence (CYDER) and Network Forensics*

AJCCBC menyelenggarakan program pelatihan tatap muka dengan dukungan JICA untuk meningkatkan kesiapan menghadapi ancaman serangan siber menjadi isu penting di wilayah ASEAN. Pelatihan diikuti oleh perwakilan yang berasal dari seluruh negara ASEAN. Kegiatan ini diselenggarakan pada tanggal 11 s.d 15 November 2024 di Bangkok, Thailand.

Manfaat dari pelatihan ini peserta diharapkan mampu mengidentifikasi penyebab dan situasi keseluruhan, menangani situasi secara tepat berdasarkan kondisi sebenarnya, memberikan laporan kepada pimpinan secara tepat waktu dengan laporan yang memadai, meningkatkan kemampuan respons insiden keamanan siber, dan meningkatkan kesadaran akan pentingnya forensik digital.

18 UNODC *Women in Cryptocurrency Summit*, Malaysia

Pertemuan Regional UNDOC *Women in Cryptocurrency Summit* yang diselenggarakan oleh UNODC merupakan wadah bagi pemangku kepentingan yang meliputi perwakilan pemerintah dan pakar industri dari negara di Asia Tenggara dalam rangka mendukung dan meningkatkan partisipasi tenaga profesional perempuan yang bekerja dalam bidang kejahatan siber *scam* (penipuan) dan mata uang kripto.

19 *The 7th UNODC Southeast Asia Cryptocurrencies Working Group Meeting*, Malaysia

UNODC menyelenggarakan 7th *Southeast Asia Cryptocurrencies Working Group* yang bertujuan untuk memperkuat kolaborasi internasional yang berkelanjutan antara negara-negara Asia Tenggara dalam menghadapi kejahatan siber dan kejahatan terkait *cryptocurrency*. Dalam kegiatan ini, pemerintah, pembuat kebijakan, lembaga penegak hukum, sektor swasta, akademisi, dan para ahli berkumpul dalam rangka berbagi wawasan, pengalaman, dan praktik terbaik (*best practices*) dalam merancang kerangka regulasi yang efektif serta respons operasional terhadap kejahatan aset virtual.

20 UNODC *Regional Roundtable Discussion on Cryptocurrencies Regulation, Investigation and Seizure,* Thailand

Pertemuan *Regional Roundtable Discussion on Cryptocurrencies Regulation, Investigation and Seizure* yang diselenggarakan oleh UNODC berlangsung selama 2 hari dan berfokus pada peningkatan kapasitas dan kesadaran badan penegak hukum dan regulator Asia tenggara tentang aset *virtual*. Selain itu, kegiatan ini juga bertujuan untuk mendukung dan meningkatkan kolaborasi pada bidang investigasi mata uang kripto.

21 *Capacity Building for Responding to Cryptocurrency in ASEAN Region,* Korea Selatan

BSSN mengikuti kegiatan *Capacity Building for Responding to Cryptocurrency Heist in ASEAN Region* Tahun 2024. Kegiatan ini diselenggarakan secara daring dan luring di Seoul, Korea Selatan dalam rangka meningkatkan kapasitas keamanan siber pada otoritas keuangan dan penegakan hukum terkait aset *virtual* di negara penerima, serta bursa aset *virtual* untuk memperkuat kapasitasnya. Pada program ini terdapat tiga tahapan utama yang harus diselesaikan oleh peserta meliputi penyusunan *country report*, penyusunan *action plan*, serta penerapan *action plan* yang telah dibuat.

22 *Study Visit (Cryptocurrency Investigation Laboratory)*

UNODC menyelenggarakan rangkaian kegiatan yang berfokus pada penanggulangan kejahatan siber, termasuk pertemuan pakar regional ahli tentang kejahatan siber. Kegiatan ini dibagi menjadi tiga program, salah satunya adalah *"Study Visit (Cryptocurrency Investigation Laboratory)"* yang diadakan di Thailand. Tujuan kegiatan ini adalah untuk meningkatkan kemampuan peserta dalam menuntut tindak pidana kejahatan siber, seperti penipuan daring, serta kemampuan dalam pelacakan dan penyitaan mata uang kripto ilegal. Selain itu, pelatihan ini bertujuan untuk mengasah keterampilan peserta dalam mengelola dan mengamankan barang bukti digital.

23 *Regional Expert Group Meeting on Cybercrime*

UNODC menyelenggarakan rangkaian kegiatan yang berfokus pada penanggulangan kejahatan siber, termasuk pertemuan pakar regional ahli tentang kejahatan siber. Kegiatan ini dibagi menjadi dua program, salah satunya adalah *"Regional Expert Group Meeting on Cybercrime"* yang diadakan di Malaysia. Tujuan kegiatan ini adalah untuk meningkatkan kemampuan peserta dalam menangani tindak pidana kejahatan siber seperti penipuan online dengan memberikan pemahaman praktis terkait OSINT, analisis data, dan verifikasi informasi.

24 *Gulf Information Technology Exhibition (GITEX Global): "Global Collaboration to Forge a Future AI Economy"*

GITEX Global menyelenggarakan konferensi dan lokakarya untuk para profesional keamanan siber, perwakilan keamanan siber dari pemerintah, pimpinan industri, dan komunitas pegiat teknologi global, yang dapat meningkatkan kemampuan sumber daya organisasi mengenai kemajuan terkini dan perkembangan strategis dalam industri teknologi dan keamanan siber. Perwakilan Pemerintah dari berbagai negara, Pimpinan Kementerian dan Pejabat sektor Publik, serta para praktisi memaparkan terkait hasil inisiatif utama dan inovasi di bidang digital dan keamanan siber serta *public private partnership* pada sektor teknologi.

25 *Roundtable Discussion by Kaspersky*

Kaspersky menyelenggarakan *Roundtable Discussion* yang mengusung tema *"Advancing Digital Resilience in key economies: Priorities, challenges and the need for transparency"*, sebagai wadah untuk melakukan pertukaran gagasan dan bentuk kolaborasi antara sektor pemerintah sebagai *regulator*, bersama pelaku di sektor publik dan swasta, sehingga dapat membantu *regulator* menerapkan regulasi dan tata kelola untuk mendorong ketahanan siber pada level organisasi maupun nasional. Hadir pula RANSOMWARE.E. Dr. Mohamed Al Kuwaiti selaku *Head of CSC UAE*.

26 *Policy Dialogue and Launching of The Handbook of Financial Crime Investigations Involving Cryptoassets*

Kegiatan *"Policy Dialogue and Launching of The Handbook of Financial Crime Investigations Involving Cryptoassets"*, salah satu agendanya adalah melakukan *launching* Buku Saku Investigasi Kejahatan yang Melibatkan Aset Kripto pada tahun 2024 yang diselenggarakan oleh UNODC. Buku tersebut diseminasikan kepada seluruh *stakeholder* yang berkaitan dengan investigasi kejahatan yang melibatkan aset kripto. BSSN bersama *stakeholder* terkait, terlibat dalam penyusuan buku tersebut.

KOMPETISI INTERNASIONAL

01 *ASEAN CYBER SHIELD HACKING CONTEST*

Tim BSSN dilibatkan menjadi peserta dalam kegiatan *Asean Cyber Shield* (ACS) *Hacking Contest* Tahun 2024. Kegiatan ini diselenggarakan oleh ASEAN *Korea Cooperation Fund* (AKCF) yang bekerja sama dengan *Korea Internet & Security Agency* (KISA). ACS 2024 merupakan kegiatan lomba *Capture The Flag* (CTF) yang diikuti oleh 10 negara di ASEAN. Perlombaan CTF dilakukan dengan tipe *Jeopardy* dan *Attack and Defense*, dengan soal-soal yang terdiri dari *Reverse Engineering, Cryptography, Misc, Pwnable*, dan *Web Exploitation*.

BSSN berhasil memenangkan penghargaan "*Best Write Up*" atas analisis dan dokumentasi pengerjaan pada soal-soal yang ada. Kegiatan ACS 2024 berjalan dengan lancar tanpa ada kendala yang berarti. Tim BSSN kembali ke Jakarta pada tanggal 23 Oktober 2024 dengan pengalaman dan pengetahuan yang telah didapatkan pada kegiatan ACS 2024.

02 *Cyber SEA Game 2024*

Tim BSSN dilibatkan menjadi peserta dalam kegiatan Cyber SEA Game tahun 2024. Kegiatan ini diselenggarakan AJCCBC yang bekerja sama dengan *Japan International Coorperation Agency* (JICA). Cyber SEA Game 2024 merupakan kegiatan lomba *Capture The Flag* (CTF) yang diikuti oleh 10 negara-negara ASEAN. Perlombaan CTF dilakukan dengan tipe *Jeopardy*, dengan soal-soal yang terdiri dari *Reverse Engineering, Forensics, Cryptography, OSINT, Steganography, Network* dan *Web Exploitation*.

Tim BSSN yang mewakili Indonesia meraih peringkat ketiga dengan total poin terakhir 5645. Tim BSSN kembali ke Jakarta pada tanggal 26 Oktober 2024 dengan pengalaman dan pengetahuan yang telah didapatkan pada kegiatan *Cyber SEA Game* 2024.

03 CTF STANDOFF 14

Standoff sebuah *platform* spesialis keamanan informasi berlokasi di Rusia menyelenggarakan kegiatan *cyber battle* pada 26-29 November 2024. Pada kegiatan ini BSSN turut berpartisipasi secara daring dengan mengirimkan Tim Langit Biru yang terdiri dari 15 (lima belas) orang perwakilan yang berperan sebagai Blue Team. Tim Langit Biru berhasil menyelidiki 15 serangan siber dan menemukan insiden siber terbanyak sejumlah 178 insiden siber. Kegiatan ini diikuti oleh *cybersecurity analyst* di seluruh dunia diantaranya berasal dari negara Vietnam, Malaysia, dan Ethiopia.

04 STANDOFF 365

Direktorat Operasi Keamanan Siber BSSN berpartisipasi dalam Standoff 365, sebuah kompetisi siber bergengsi pada *St. Petersburg International Economic Forum* (SPIEF) 2024, yang berlangsung pada 4-7 Juni secara daring. Tim Langit Biru, terdiri dari 11 personel, berhasil menyelesaikan 12 dari 14 investigasi insiden kritis dengan catatan waktu rata-rata investigasi tercepat 1 jam 42 menit, termasuk 36 laporan deteksi insiden dalam waktu rata-rata 30 menit. Tim ini meraih juara pertama kategori Blue Team dan dinobatkan sebagai "*One of The Best Team*". Prestasi ini menegaskan kemampuan BSSN dalam investigasi insiden siber sekaligus memperkuat kolaborasi internasional dengan CSIRT dan CERT global, serta meningkatkan eksistensi Indonesia di forum keamanan siber dunia.

KERJA SAMA LAYANAN HONEYNET

Kerja sama ISIF Project

Kolaborasi Honeynet BSSN dengan *Swiss German University* dan komunitas Indonesia Honeynet Project (IHP) sudah berlangsung sejak tahun 2018. Kerjasama ini berfokus pada kerjasama riset yang dilakukan bersama SGU dan IHP dalam penelitian ISIF (*The Information Society Innovation Fund*) ASIA. Tujuan dari *ISIF Project* ini adalah untuk menyediakan platform sharing bagi setiap organisasi di Indonesia (nantinya dapat diterapkan di negara-negara ASEAN atau Asia Pasifik) untuk berbagi informasi ancaman keamanan yang dikumpulkan melalui *honeypot* pada organisasi di suatu negara. Selain itu, *project* ini juga menjadi sebuah inovasi dan pertama kali dilakukan dengan menggabungkan upaya penelitian antara pemerintah (BSSN), lembaga pendidikan (SGU), dan komunitas keamanan siber (IHP) untuk membangun *platform threat information sharing*.

Pemasangan Honeypot

Pada tahun 2024, terdapat penambahan 6 titik pemasangan honeypot, sehingga jumlah Honeypot BSSN yang terpasang mencapai 111 titik yang tersebar di 27 provinsi di Indonesia. Penambahan titik Honeypot ini diharapkan dapat mengumpulkan data serangan siber lebih luas yang menyerang Indonesia berdasarkan sistem Honeynet BSSN yang telah terpasang. Informasi serangan siber yang diperoleh dari sistem Honeynet BSSN selanjutnya dapat digunakan sebagai salah satu referensi peningkatan *security perimeter* milik Mitra Honeynet sekaligus meningkatkan *cyber security awareness* bagi masyarakat.

111
titik
yang tersebar di 27 provinsi

Untuk informasi lebih lanjut terkait Layanan Honeynet BSSN, termasuk di dalamnya terdapat Laporan Tahunan Honeynet BSSN sejak tahun 2018, dapat diakses melalui tautan berikut:

https://bssn.go.id/honeynet

KETERLIBATAN KEGIATAN **PAMERAN**

01 Pameran Indosec 2024

IndoSec 2024 adalah konferensi keamanan siber terkemuka di Indonesia yang mempertemukan para profesional, akademisi, pelaku industri, dan pemerintah untuk berdiskusi mengenai tantangan dan inovasi dalam dunia keamanan siber. IndoSec 2024 kembali digelar di **Jakarta Convention Center (JCC)** pada tanggal **24-25 September 2024**. Acara yang telah memasuki edisi ketujuh ini berhasil mengumpulkan **lebih dari 2000 pakar keamanan siber** dari berbagai sektor, baik publik maupun swasta. Dengan mengusung tema **"Encrypting Indonesia for a Secure Tomorrow"**, IndoSec 2024 menjadi wadah bagi para peserta untuk berbagi pengetahuan, pengalaman, serta inovasi terbaru dalam menghadapi tantangan keamanan siber yang semakin kompleks menghadirkan sesi presentasi, lokakarya, dan diskusi panel yang dirancang untuk menggali solusi terhadap ancaman siber yang semakin kompleks. **Layanan Honeynet BSSN** turut memberikan dukungan pada acara tersebut untuk memperkenalkan teknologi keamanan siber di bidang pengelolaan informasi dini ancaman siber yang telah dimiliki BSSN. Masyarakat umum dapat menambah informasi terkait teknologi keamanan siber dan mengetahui pentingnya pemanfaatan Honeynet yang dapat dijadikan sebagai sumber data informasi serangan siber.

02 Pameran Indonesia CSIRT Day

Indonesia CSIRT Day adalah salah satu rangkaian kegiatan ***National Cyber Exercise*** yang merupakan amanat dari Rancangan Pembangunan Jangka Menengah Nasional (RPJMN) dan Rencana Strategis Tahun 2020-2024. Melalui kegiatan ini, Direktorat Operasi Keamanan Siber melibatkan *Cyber Security Incident Response Team* (CSIRT) dan Pengelola Sistem Elektronik (PSE) di Indonesia untuk berperan serta dalam **kesiapsiagaan keamanan siber** baik secara teknis maupun manajerial. Pameran ini diadakan tanggal **3 Desember 2024** berlokasi di Jakarta dan berhasil mendatangkan **200 (dua ratus) lebih anggota CSIRT dari berbagai daerah**. Layanan Honeynet BSSN turut berpartisipasi dalam pameran untuk memperkenalkan teknologi keamanan siber di bidang pengelolaan informasi dini ancaman siber dan juga memberikan edukasi *security awareness* terhadap *malware* dan *phishing* yang marak di Indonesia.

03 Pameran ASN Culture Festival

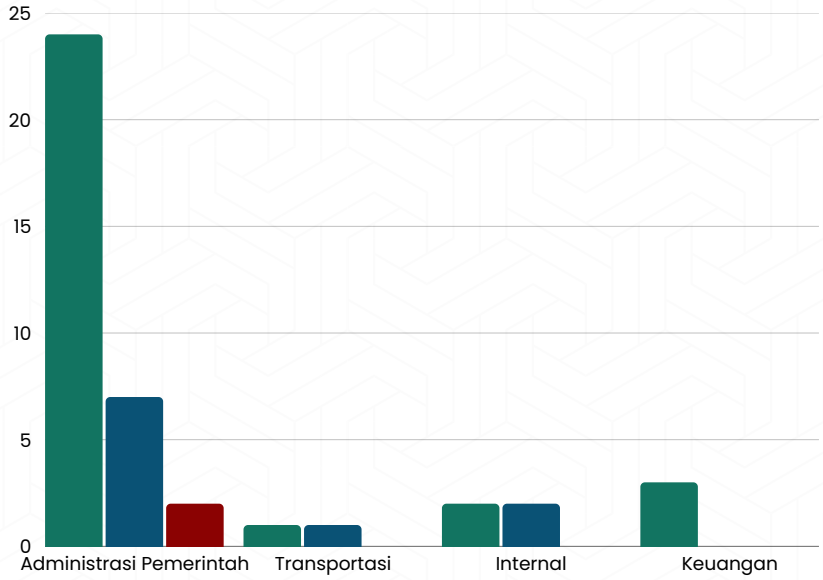
Aparatur Sipil Negara (ASN) ***Culture Festival*** yang diadakan setiap tahunnya menjadi agenda rutin dalam penguatan budaya kerja ASN. ASN *Culture Festival* merupakan ajang pesta budaya kerja untuk dapat **meningkatkan citra ASN** di mata masyarakat, **meningkatkan keterikatan** (*engagement*) ASN, dan **memberikan penghargaan** kepada Instansi Pemerintah yang memiliki **komitmen kuat** dalam penguatan budaya kerja. Pada 2024 ini, Kementerian PANRB kembali menggelar festival budaya kerja. Festival budaya kerja yang diisi oleh para ASN inspiratif dan berbakat, serta akan menampilkan layanan dan inovasi dari berbagai Instansi Pemerintah melalui sebuah stan pameran. Pameran ini diadakan tanggal **10 Desember 2024 di Jakarta**. **Tim Layanan Honeynet BSSN** hadir untuk memeriahkan acara dan memperkenalkan teknologi keamanan siber di bidang pengelolaan informasi dini ancaman siber.

KERJA SAMA LABORATORIUM FORENSIK DIGITAL

40
layanan LFD

Laboratorium Forensik Digital Direktorat Operasi Keamanan Siber (LFD Dit Opskamsiber) BSSN merupakan laboratorium yang mendukung pelaksanaan forensik digital pada bidang **insiden keamanan siber** seperti *ransomware*, kebocoran data, *web defacement, illegal access,* pemalsuan data, serta insiden lainnya.

Jenis Layanan Laboratorium Forensik Digital sejumlah **30 Pemeriksaan Forensik Digital, 8 Dukungan Penyidikan,** dan **2 Bantuan Keterangan Ahli.**

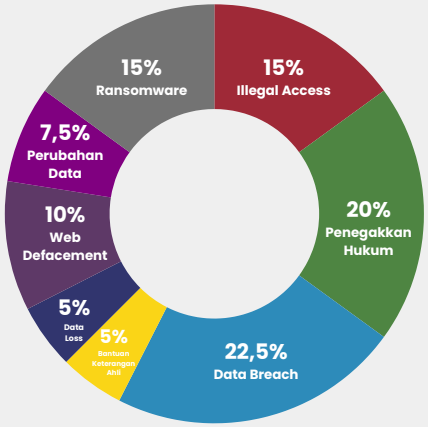


30
Pemeriksaan Forensik Digital

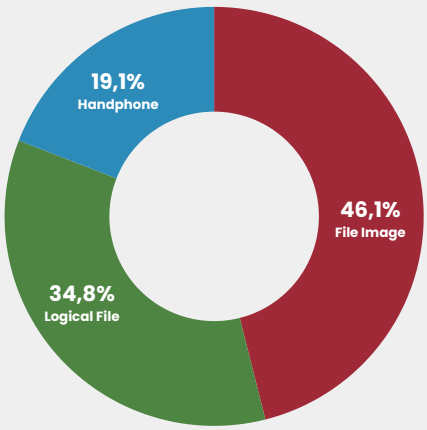
8
Dukungan Penyidikan

2
Bantuan Keterangan Ahli

40
Jenis Insiden



89
Alat Bukti Elektronik



AKREDITASI LABORATORIUM FORENSIK DIGITAL

MANAJEMEN SISTEM MUTU LABORATORIUM FORENSIK DIGITAL DIT OPSKAMSIBER BSSN BERDASARKAN STANDAR ISO/IEC 17025:2017

Laboratorium Forensik Digital Dit Opskamsiber BSSN melakukan manajemen sistem mutu berdasarkan standar ISO/IEC 17025:2017 dengan kegiatan sebagai berikut:

01 Laboratorium Forensik Digital Dit Opskamsiber BSSN Raih Sertifikat Akreditasi ISO/IEC 17025:2017

LFD Dit Opskamsiber telah melewati seluruh tahapan akreditasi sehingga berhasil mendapatkan sertifikat akreditasi SNI ISO/IEC 17025:2017 per tanggal 23 Agustus 2023 dan berlaku sampai tanggal 22 Agustus 2028. Sertifikat akreditasi ini menunjukkan bahwa LFD Dit Opskamsiber BSSN kompeten sebagai laboratorium penguji berdasarkan SNI ISO/IEC 17025:2017.

02 Uji Banding Antar Laboratorium Forensik Digital Berdasarkan ISO 17025:2017

Berdasarkan persyaratan rangkaian akreditasi ISO 17025:2017, suatu Laboratorium yang telah terakreditasi perlu melakukan uji banding minimal kepada 2 (dua) laboratorium dalam 1 (satu) tahun yang mulai dilaksanakan paling cepat 6 (enam) bulan setelah LFD Dit Opskamsiber BSSN terakreditasi untuk memastikan bahwa kompetensi laboratorium sesuai dengan persyaratan yang ditetapkan pada standar. Pada tahun 2024, uji banding laboratorium dilakukan bersama Laboratorium Barang Bukti Elektronik Komisi Pemberantasan Korupsi (Lab BBE KPK).

03 Kegiatan Bersama Asosiasi Forensik Digital Indonesia (AFDI)

Berdasarkan persyaratan rangkaian akreditasi ISO 17025:2017, suatu Laboratorium yang telah terakreditasi perlu melakukan uji banding minimal kepada 2 (dua) laboratorium dalam 1 (satu) tahun yang mulai dilaksanakan paling cepat 6 (enam) bulan setelah LFD Dit Opskamsiber BSSN terakreditasi untuk memastikan bahwa kompetensi laboratorium sesuai dengan persyaratan yang ditetapkan pada standar. Pada tahun 2024, uji banding laboratorium dilakukan bersama Laboratorium Barang Bukti Elektronik Komisi Pemberantasan Korupsi (Lab BBE KPK).

04 Uji Profisiensi Bersama China National Accreditation Service for Conformity Assessment (CNAS)

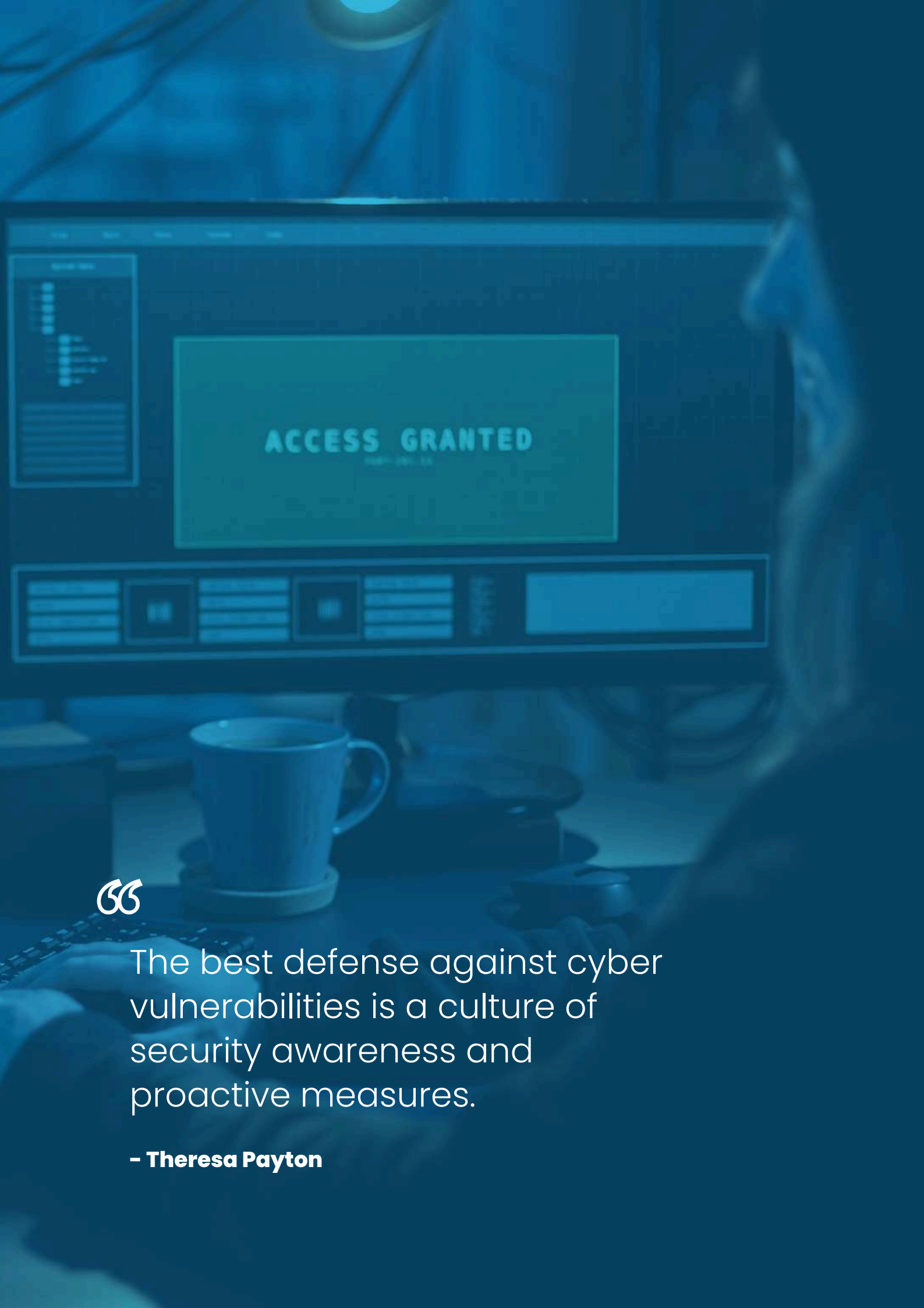
LFD Dit Opskamsiber terus meningkatkan kualitas layanan dan kompetensinya melalui pelaksanaan Uji Profisiensi yang terakreditasi oleh *China National Accreditation Service for Conformity Assessment* (CNAS). Uji profisiensi ini merupakan salah satu bentuk evaluasi eksternal yang bertujuan untuk memastikan bahwa proses analisis dan hasil pengujian di laboratorium memenuhi standar internasional. Dengan mengikuti uji profisiensi yang diakui oleh CNAS, LFD Dit Opskamsiber dapat menunjukkan konsistensi dan akurasi dalam prosedur teknisnya, serta membangun kepercayaan para pemangku kepentingan terhadap validitas hasil analisis forensik yang dilakukan. Partisipasi dalam program ini juga memberikan peluang untuk *benchmarking* dan identifikasi area yang dapat ditingkatkan.

BUKU PENANGANAN KERENTANAN

Tim BSSN terlibat dalam pembuatan Buku Kajian Ketahanan Siber: Manajemen Kerentanan. Buku Manajemen Kerentanan ditujukan untuk pemangku kepentingan dan organisasi penyedia sistem elektronik. Buku ini ditulis oleh Tim Penulis yang dipimpin oleh Taufik Nurhidayat, dengan 10 orang anggota yaitu Dr. Susila Windarta, Nanang Trianto, M. Fadhli Maghfur Shofiyuddin, Nabella Permatasari, Satrya Mahardhika, Muhammad Azza Ulin Nuha, Dwi Novazrianto, Alfian Adi Saputra dan Nur Annisa Kadarwati Febriyani. *Launching* buku dilaksanakan pada tanggal 8 Oktober 2024 dalam acara *National Cybersecurity Connect* 2024 di Jakarta.

Buku manajemen Kerentanan membahas secara mendalam terkait penerapan siklus manajemen kerentanan, melalui pendekatan terkini dalam mengidentifikasi, menilai, dan menangani kerentanan yang ada di berbagai infrastruktur teknologi. Buku manajemen kerentanan diharapkan dapat menjadi rujukan dan memberikan penekanan pentingnya kolaborasi antar pemangku kepentingan, mulai dari peneliti, *vendor*, hingga *regulator* dalam menciptakan ekosistem keamanan yang kuat.

Buku Manajemen Kerentanan dapat diunduh secara bebas melalui website BSSN dan Poltek SSN.



“

The best defense against cyber vulnerabilities is a culture of security awareness and proactive measures.

– Theresa Payton

12

NATIONAL CYBER EXERCISE

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2024

NATIONAL
CYBER EXERCISE

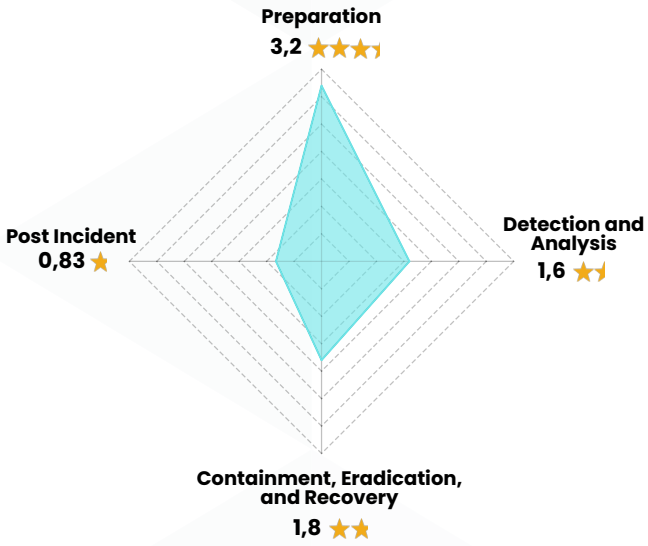
7.121 Total Peserta

1.174 Total Instansi

National Cyber Exercise merupakan kegiatan yang diamanatkan oleh Rancangan Pembangunan Jangka Menengah Nasional (RPJMN) dan Rencana Strategis Tahun 2020-2024. *National Cyber Exercise* terbagi menjadi tiga kegiatan besar yaitu *Cross Sectoral Cyber Exercise, Table Top Exercise*, dan *CSIRT Day*. *Cross Sectoral Cyber Exercise* merupakan kegiatan yang diselenggarakan untuk melatih anggota CSIRT dalam menangani insiden siber yang terdiri dari beberapa skenario diantaranya *Web Defacement, Ransomware, Malware Stealer*, dan APT. *Cross Sectoral Cyber Exercise* terbagi ke dalam 11 (sebelas) seri yaitu *Full Online*, Depok, Surabaya, Bogor, Bali, Medan, dan Manado. Dalam rangka melakukan evaluasi terkait kompetensi peserta yang mengikuti *Cross Sectoral Cyber Exercise*, ditunjukkan radar penilaian dengan nilai menggunakan skala 0 (nol) hingga 5 (lima). Radar tersebut terdiri dari 4 (empat) komponen *Preparation; Detection and Analysis; Containment, Eradication,* dan *Recovery*, serta *Post Incident.*

A. Cross Sectoral Cyber Exercise

01 National Cyber Exercise: Cross Sectoral Cyber Exercise 0 Full Online

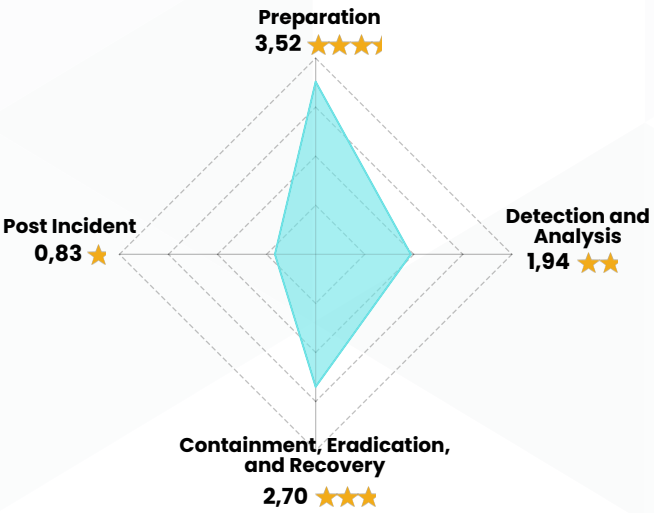


408 Total Peserta

108 Total Instansi

National Cyber Exercise: *Cross Sectoral Cyber Exercise #0 Full Online* dilaksanakan pada 28 Maret 2024 dengan total peserta yang berpartisipasi sejumlah 408 peserta dari *Computer Security Insident Response Team* (CSIRT) Organisasi dan Penyelenggara Sistem Elektronik (PSE) di Indonesia yang dilaksanakan secara daring. Pada kesempatan ini, penyampaian materi webinar oleh Bapak Sida Nala Rukma Januarto (Co-Founder Blueteam.ID) dengan tema materi *Web Defacement.*

02 National Cyber Exercise: Cross Sectoral Cyber Exercise #1 Depok

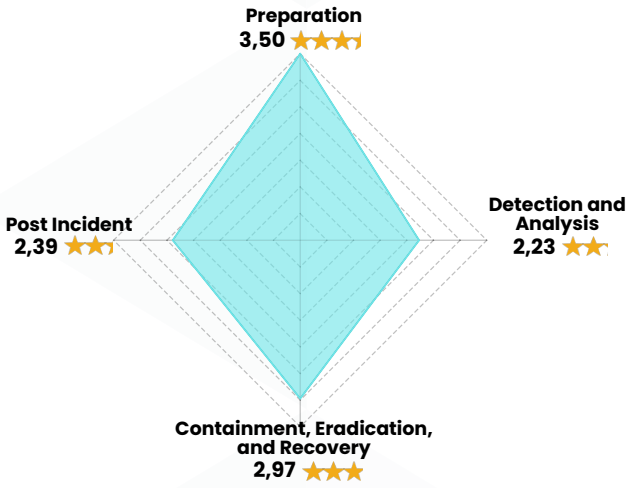


361 Total Peserta

111 Total Instansi

National Cyber Exercise: Cross Sectoral Cyber Exercise #1 Depok dilaksanakan pada 29 s.d. 30 April 2024 di Kantor BSSN, Sawangan, Depok dengan total peserta yang berpartisipasi sejumlah 361 orang. Pada kegiatan ini turut mengundang pembicara dengan topik bahasan "Potensi Krisis dari Insiden *Ransomware*". Adapun pembicara yang diundang yaitu Bapak Bapak Dr. Pratama Persadha, S.Sos., M.M (*Chairman* Lembaga Riset Keamanan Siber CISSReC), Bapak Adi Nugroho, S.ST., S.Kom (Sekretaris BSSN-CSIRT), dan Dr. Adi Affandi Rotib, MT (Direktorat Layanan Aplikasi Informatika Pemerintahan).

03 National Cyber Exercise: Cross Sectoral Cyber Exercise #2 Pontianak



368 Total Peserta

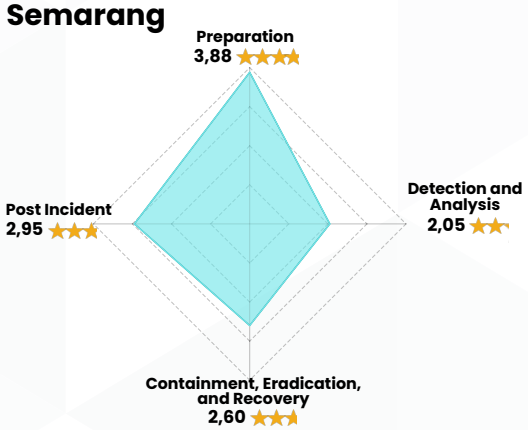
108 Total Instansi

National Cyber Exercise: Cross Sectoral Cyber Exercise #2 Pontianak, Kalimantan Barat dilaksanakan pada 13 s.d. 15 Mei 2024 di Hotel Aston Pontianak. Peserta yang berpartisipasi pada kegiatan ini sejumlah 368 peserta *online* dan *offline* dengan mengerjakan skenario *Malware Stealer*.

04 National Cyber Exercise: Cross Sectoral Cyber Exercise #3 Semarang

613
Total Peserta

127
Total Instansi

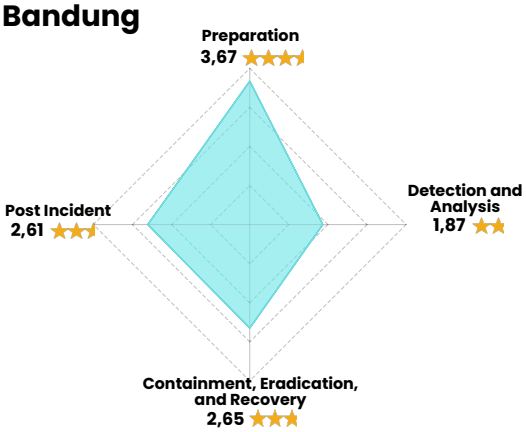


Kegiatan Indonesia *Cross Sectoral Cyber Exercise* #3 Semarang *Malware Stealer* dilaksanakan baik secara luring maupun daring. Kegiatan CSCE#3 dilaksanakan pada 1 s.d. 4 Juli 2024 secara luring di MG Setos Hotel Semarang dan secara daring melalui *Zoom Webinar*. Kegiatan dilaksanakan dengan skema *Cyber Exercise* yang bertemakan Tanggap Insiden *Malware Stealer*. Kegiatan dihadiri oleh 613 peserta. Peserta yang mengikuti berasal dari pengelola CSIRT dan Penyelenggara Sistem Elektronik (PSE) di Indonesia.

05 National Cyber Exercise: Cross Sectoral Cyber Exercise #4 Bandung

505
Total Peserta

152
Total Instansi

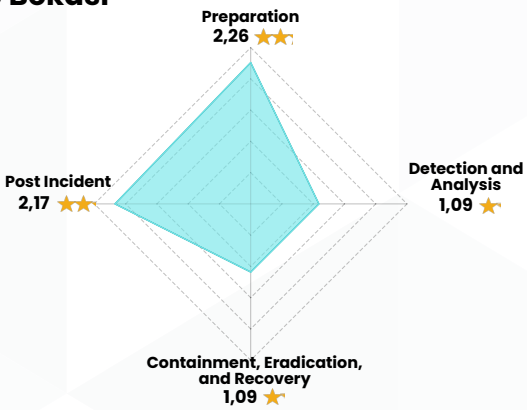


National Cyber Exercise: Cross Sectoral Cyber Exercise #4 Bandung, Jawa Barat dilaksanakan pada 23 s.d. 24 Juli 2024 di Hotel Ibis Trans Studio Bandung. Peserta yang berpartisipasi pada kegiatan ini sejumlah 505 peserta *online* dan *offline* dengan mengerjakan skenario *Malware Stealer*.

06 National Cyber Exercise: Cross Sectoral Cyber Exercise #5 Bekasi

501
Total Peserta

131
Total Instansi

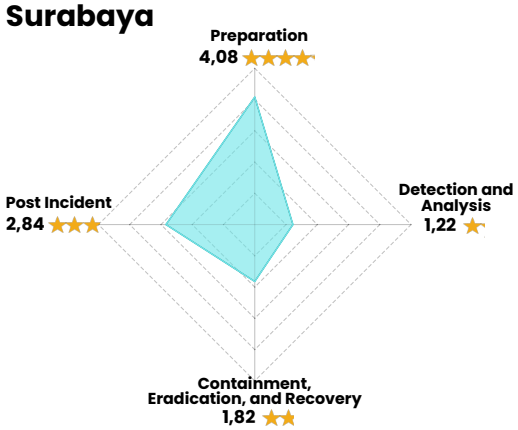


Kegiatan Indonesia *Cross Sectoral Cyber Exercise* #5 dilaksanakan pada 6 s.d. 8 Agustus 2024 secara luring di Ballroom Sanggabuana Hotel Santika Premiere Kota Harapan Indah Kota Bekasi secara luring dan daring melalui *Zoom Webinar*. CSCE#5 dilaksanakan dengan skema *Cyber Exercise* yang bertemakan Tanggap Insiden *Malware Stealer*. Kegiatan diikuti oleh 501 peserta. Peserta yang mengikuti berasal dari pengelola CSIRT dan Penyelenggara Sistem Elektronik (PSE) di Indonesia.

07 National Cyber Exercise: Cross Sectoral Cyber Exercise #6 Surabaya

511
Total Peserta

114
Total Instansi

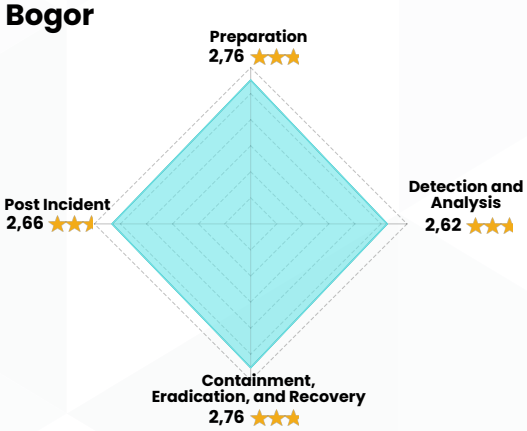


National Cyber Exercise: *Cross Sectoral Cyber Exercise* #6 Surabaya dilaksanakan pada 20 s.d. 22 Agustus 2024 di Hotel Mercure Grand Mirama, Surabaya dengan total peserta yang berpartisipasi sejumlah 511 peserta. Pada kegiatan ini turut mengundang pemapar dengan tema materi *Advanced Persistence Threat* (APT) yang dibawakan oleh Bapak Ryan Fabella (*Consultant* MCG A/S, Denmark) dan Bapak Nikko Enggaliano Pratama (*Senior Cyber Security Engineer*, PT Negeri Seni Indonesia).

08 National Cyber Exercise: Cross Sectoral Cyber Exercise #7 Bogor

555
Total Peserta

135
Total Instansi

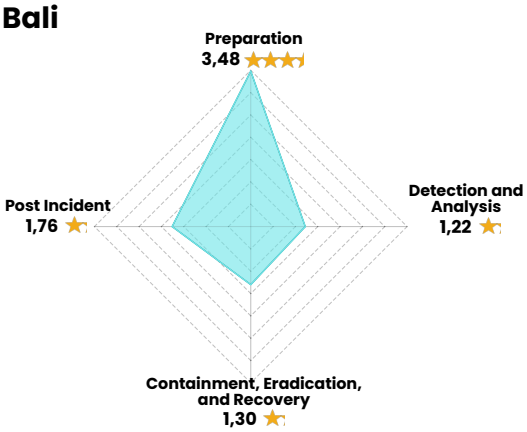


National Cyber Exercise: *Cross Sectoral Cyber Exercise* #7 Bogor dilaksanakan pada 27 s.d. 29 Agustus 2024 berlokasi di Kantor BSSN Sentul, Bogor, Jawa Barat dengan total peserta yang berpartisipasi sejumlah 555 orang. Narasumber pada kegiatan ini yaitu Ibu Claudia Dwi Amanda, S.ST., M.Mhan., Sandiman Ahli Madya BSSN dengan Materi Pembahasan Rencana Kontingensi Krisis Siber (RKKS) dan Novian Nur Cahya, S.ST, M.Kom., Sandiman Ahli Muda BSSN dengan Materi Tim Tanggap Insiden Siber (TTIS). Skenario yang digunakan pada kesempatan ini adalah *Web Defacement*.

09 National Cyber Exercise: Cross Sectoral Cyber Exercise #8 Bali

639
Total Peserta

184
Total Instansi

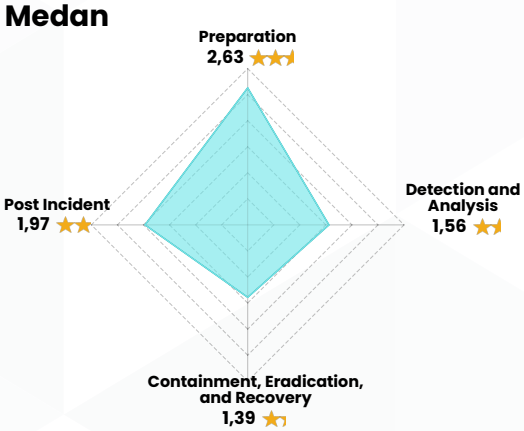


National Cyber Exercise: *Cross Sectoral Cyber Exercise* #8 Bali dilaksanakan pada 9 s.d. 11 September 2024 yang diselenggarakan di Kuta Paradiso Hotel, Bali. Peserta yang berpartisipasi pada kegiatan ini sejumlah 639 orang dengan tema skenario yaitu APT. Adapun paparan narasumber pada kegiatan ini adalah Bapak I Putu Agus Eka Pratama (Univ. Udayana) dan Leonardo Hutabarat (Exabeam).

10 National Cyber Exercise: Cross Sectoral Cyber Exercise #9 Medan

605
Total Peserta

182
Total Instansi

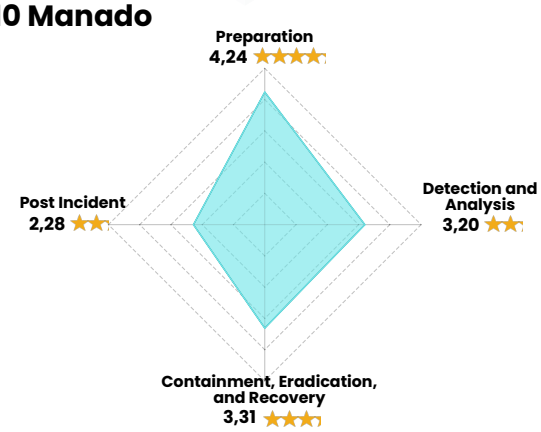


National Cyber Exercise: Cross Sectoral Cyber Exercise #9 Medan, Sumatera Utara dilaksanakan pada 22 sd 23 Oktober 2024 di Hotel Four Points Medan. Peserta yang berpartisipasi pada kegiatan ini sejumlah 605 peserta *online* dan *offline* dengan mengerjakan skenario *Malware Stealer*.

11 National Cyber Exercise: Cross Sectoral Cyber Exercise #10 Manado

378
Total Peserta

114
Total Instansi



National Cyber Exercise: Cross Sectoral Cyber Exercise #10 Manado dilaksanakan pada 5 s.d. 7 November 2024 yang diselenggarakan di Aryaduta Hotel Manado. Peserta yang berpartisipasi pada kegiatan ini sejumlah 378 peserta dengan mengerjakan skenario *Web Defacement*. Pada kegiatan ini paparan materi disampaikan oleh Bapak Alwin Melkie Sambul, S.T., M.Eng., Ph.D (Dosen Universitas Sam Ratulangi) dan Satrya Mahardhika, S.Tr.Kom (Sandiman Ahli Pertama, BSSN).

B. Table Top Exercise

1.046
Total Peserta

Table Top Exercise memiliki konsep *roleplay* dan diberikan injeksi berupa permasalahan yang akan didiskusikan oleh peserta berdasarkan peran (*role*) yang telah dipilih oleh peserta. *Table Top Exercise* terbagi ke dalam 3 (tiga) seri yaitu Sawangan, Bali, dan Jakarta.

01 National Cyber Exercise: Table Top Exercise #1 Depok

National Cyber Exercise: *Table Top Exercise* #1 dilaksanakan di Kantor BSSN Sawangan, Depok pada 29 s.d. 30 April 2024 dengan total peserta 407 peserta yang berasal dari *Computer Security Incident Response Team* (CSIRT) Organisasi dan Penyelenggara Sistem Elektronik (PSE) di Indonesia. Peran yang dapat dipilih oleh peserta yaitu peran *management* (pimpinan), hubungan masyarakat, CSIRT, Pengelola TIK, dan Tata Kelola. Terdapat 9 (sembilan) injeksi permasalahan yang diberikan kepada peserta dengan tema *ransomware*.

02 National Cyber Exercise: Table Top Exercise #2: Bali

National Cyber Exercise: *Table Top Exercise* #2 Bali dilaksanakan pada 9 s.d. 11 September 2024 di Kuta Paradiso Hotel, Bali dengan total peserta 639 peserta yang berasal dari CSIRT dan PSE di Indonesia. *Table Top Exercise* bertajuk tema "Pola Komunikasi Menghadapi Krisis Siber". Peserta dibagi ke dalam peran yang berbeda dan kemudian melakukan diskusi untuk membahas bagaimana menjalankan peran tersebut dan merespons situasi darurat sesuai skenario yang telah ditetapkan. Kegiatan ini melibatkan peran fasilitator yang bertugas memandu jalannya diskusi selama kegiatan.

03 National Cyber Exercise: Table Top Exercise #3 Jakarta

National Cyber Exercise: *Table Top Exercise* #3 Jakarta dilaksanakan pada 3 Desember 2024 di Jakarta bertempat di Discovery Hotel Ancol Jakarta Utara dengan total peserta 614 orang yang berasal dari CSIRT dan PSE. *Table Top Exercise* bertajuk tema "Collaborative Security on CSIRT". Peserta dibagi ke dalam peran yang berbeda dan kemudian melakukan diskusi untuk membahas bagaimana menjalankan peran tersebut dan merespons situasi darurat sesuai skenario yang telah ditetapkan. Kegiatan ini melibatkan peran fasilitator yang bertugas memandu jalannya diskusi selama kegiatan.

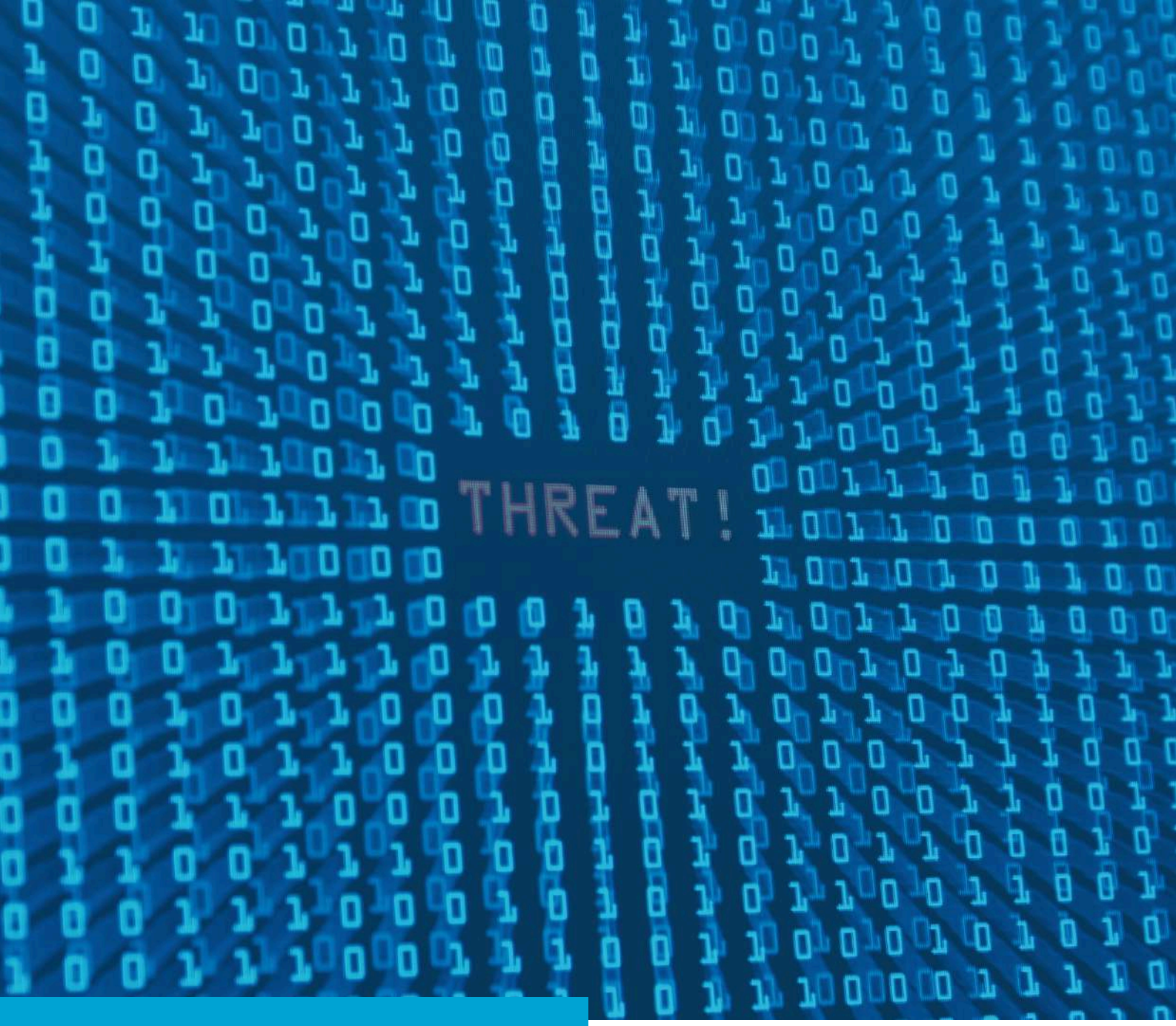
C. CSIRT Day

614
Total Peserta

CSIRT Day merupakan puncak dari rangkaian kegiatan *National Cyber Exercise* dengan mengusung tema "Collaborative Security on CSIRT" yang mencerminkan pentingnya sinergi antar organisasi dalam memperkuat keamanan siber melalui kolaborasi yang efektif.

Kegiatan Indonesia CSIRT Day dilaksanakan baik secara luring maupun daring. Kegiatan Indonesia CSIRT Day dilaksanakan pada 2 s.d 6 Desember 2024 secara luring di Discovery Hotel Ancol Jakarta dan secara daring melalui *Zoom Webinar*. Kegiatan dihadiri oleh 614 orang peserta dari 176 instansi, dengan rincian 204 orang peserta luring dan 410 orang peserta daring. Peserta berasal dari pengelola CSIRT di Indonesia. Narasumber pada Kegiatan *National Cyber Exercise*: *Indonesia CSIRT Day* adalah Prof. Dr. Dwiza Riana, S.Si, M.M, M.Kom., IPU, ASEAN.Eng. (*Deputy 2 Finance - Academy CSIRT*), Andi Mappesona (*Lead Cybersecurity Digital Forensic and Incident Response, Grab*); dan Daniel Kristian Wongso (*Managing Director* PT Tri Kreasi Mandiri Teknologi).

> We must rethink our approach to cybersecurity as an ongoing, never-ending challenge, and a critical business issue.
>
> **– John Chambers**



13

PREDIKSI POTENSI ANCAMAN SIBER TAHUN 2025

LANSKAP KEAMANAN SIBER INDONESIA TAHUN 2024

PREDIKSI POTENSI ANCAMAN SIBER TAHUN 2025

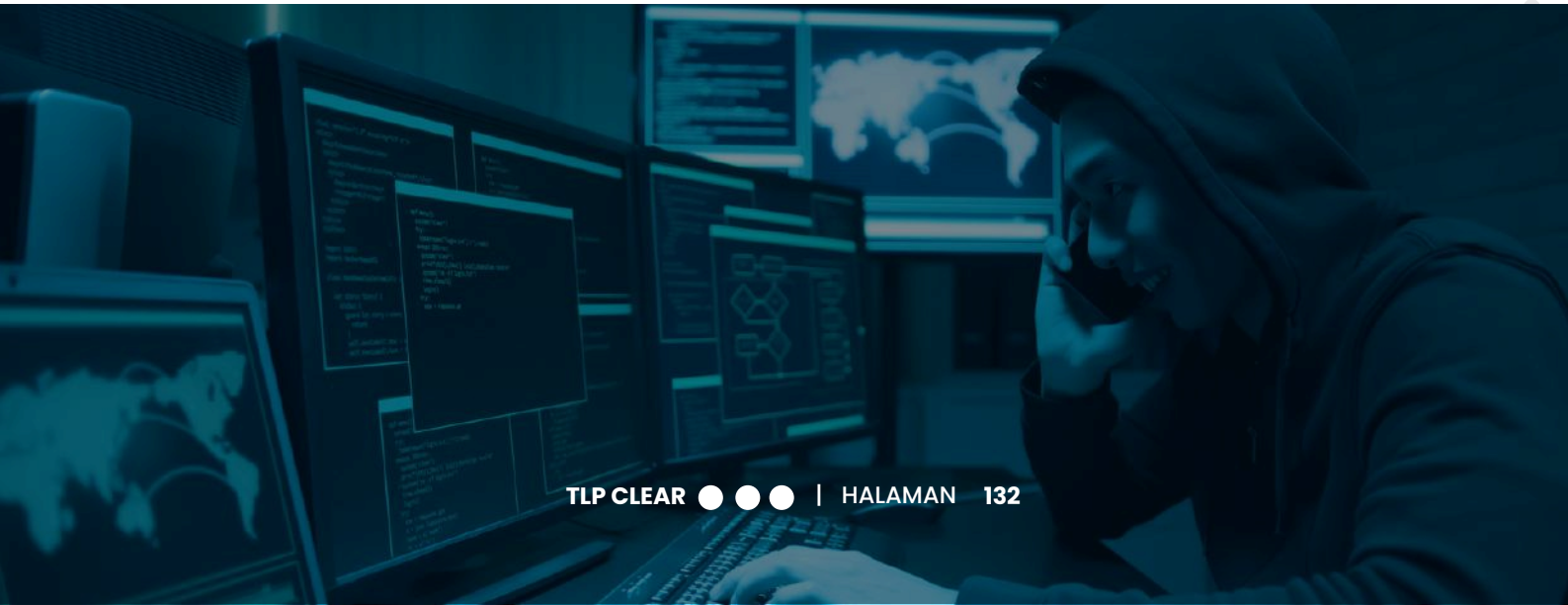
Dalam lingkup *digital* yang semakin kompleks, ancaman siber tidak hanya mencakup serangan teknis saja, tetapi juga manipulasi sosial di ruang siber yang memanfaatkan kerentanan psikologis manusia. Merujuk pada Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, disebutkan bahwa keamanan siber adalah upaya adaptif dan inovatif untuk melindungi seluruh lapisan ruang siber, termasuk aset informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik yang **bersifat teknis maupun sosial**. Sehingga, keamanan siber dapat dikategorikan ke dalam dua jenis yaitu keamanan siber teknis dan keamanan siber sosial.

Keamanan Siber Sosial

Keamanan siber sosial (*social cybersecurity*) berfokus untuk memanipulasi atau mempengaruhi individu manusia, kelompok, atau komunitas yang berdampak pada perilaku mereka terhadap isu sosial, budaya, dan politik. Keamanan siber sosial melibatkan manusia dalam menggunakan teknologi untuk mempengaruhi manusia lain.

Keamanan Siber Teknis

Keamanan siber (*cybersecurity*) yang berfokus pada infrastruktur, teknologi, dan teknik serangan yang berdampak pada kerugian materiil seperti *Data Breach*, DDos, dan *Malware*. Keamanan siber teknis melibatkan manusia dalam mengoperasikan teknologi untuk meretas teknologi lain.



PREDIKSI POTENSI ANCAMAN SIBER SOSIAL

Survei *World Economic Forum Global Risk Perception Survey* tahun 2023 – 2024 memperlihatkan *insight* baru bahwa risiko jangka pendek paling serius yang sedang dan akan dihadapi dunia yaitu misinformasi dan disinformasi yang dipengaruhi oleh maraknya penggunaan *Artificial Intelligence* (AI). Disisi lain, *Enisa Thread Landscape* tahun 2024 mengungkapkan bahwa *social engineering* dan *information manipulation* menjadi ancaman siber sosial yang mengemuka. Berkaitan dengan hal tersebut, data dari Kementerian Komunikasi dan Digital (Komdigi) 2024 semakin menguatkan indikasi tingginya ancaman siber sosial, yaitu dengan jumlah 8.312.713 penanganan kasus konten negatif pada situs dan 2.365.749 pada media sosial dengan persebaran konten yang paling banyak antara lain perjudian, pornografi, penipuan, dan pelanggaran kekayaan intelektual. Selain itu, sepanjang tahun 2024 BSSN telah melakukan penanganan konten negatif dengan mengajukan rekomendasi pemutusan akses, baik yang berasal dari aduan masyarakat dan instansi, maupun hasil dari patroli dan deteksi dini BSSN. Tercatat sebanyak 179 aduan dan 4.155 URL, meliputi isu perjudian daring, *scam, scam-phishing, phising,* hingga pornografi.

Berbagai data di atas menunjukkan bahwa ancaman siber di tahun 2024 didominasi oleh perjudian daring, pornografi, scam, disinformasi dan misinformasi, serta terorisme. Oleh karena itu, dengan memperhatikan pemanfaatan teknologi yang terus meningkat ditambah dengan berbagai ancaman siber teknis yang bermunculan, BSSN meyakini bahwa ancaman tersebut akan tetap ada. BSSN memprediksi, pada tahun 2025 ancaman siber sosial yang akan dihadapi berupa **penyebaran konten pornografi, judi *online*, *scam online*, terorisme, disinformasi dan misinformasi yang diperparah dengan potensi penyalahgunaan teknologi AI.**

PENYEBARAN KONTEN PORNOGRAFI

Potensi peningkatan penyebaran dan distribusi konten pornografi dengan berbagai metode produksi pada *platform digital* dapat menimbulkan dampak negatif bagi individu dan masyarakat. Pada jenis ancaman siber sosial pornografi, terdapat beberapa modus yang mungkin akan muncul, seperti penyebaran konten pornografi, kasus pornografi *online* anak, hingga *revenge porn* atau penyebaran konten pornografi yang didasari oleh motif balas dendam.

JUDI ONLINE

Ancaman judi *online* atau perjudian daring menjadi ancaman siber sosial dikarenakan maraknya peningkatan persebaran situs atau konten yang digunakan untuk melakukan aktivitas dan mendukung promosi perjudian daring melalui berbagai *platform digital*. Saat ini banyak ditemui konten bermuatan promosi perjudian daring yang memberikan penawaran menarik kepada masyarakat. Selain itu, konten perjudian daring juga disisipkan pada berbagai aplikasi seperti *game*.

SCAM ONLINE

Ancaman penipuan *online* diprediksi akan menjadi salah satu bentuk ancaman siber sosial yang akan mengalami peningkatan pada tahun 2025. Terdapat berbagai bentuk penipuan yang memanfaatkan perkembangan teknologi seperti *phising*, *social engineering*, maupun pembuatan situs/aplikasi palsu untuk mengelabui calon korban. Selain itu, pelaku juga memanfaatkan inovasi teknologi baru seperti *deepfake* untuk menyembunyikan identitas asli mereka sehingga dapat mempersulit proses pelacakan. *Scam Online* memerlukan perhatian lebih karena dapat berpotensi menimbulkan kerugian finansial yang semakin besar baik kepada individu maupun organisasi.

PENYEBARAN KONTEN TERORISME

Potensi ancaman terorisme didasari karena adanya kelompok teroris yang memanfaatkan ruang siber sebagai alat strategis untuk menyebarkan ideologi atau propaganda melalui berbagai *platform digital*, seperti media sosial, forum diskusi *online*, dan aplikasi pesan instan untuk menarik simpati dan dukungan masyarakat. Selain itu, kelompok teroris juga menggunakan ruang siber untuk menggalang dana secara global melalui metode seperti *crowdfunding*, donasi anonim, hingga penggunaan mata uang kripto yang memungkinkan mereka untuk mendanai operasi tanpa terdeteksi.

DISINFORMASI DAN MISINFORMASI

Penyebaran disinformasi dan misinformasi dilakukan dengan melakukan perubahan terhadap informasi dan menyebarkannya secara luas dengan tujuan untuk menyesatkan, membentuk atau mempengaruhi opini publik, dan merusak kepercayaan terhadap sumber informasi yang sah. Tindakan ini dilakukan melalui berbagai cara seperti penyebaran berita palsu/hoaks, maupun pembuatan konten manipulatif yang dirancang untuk menciptakan kebingungan, memecah belah, dan memperkuat agenda tertentu di masyarakat.

PENYALAHGUNAAN AI

Bersamaan dengan pemanfaatannya, kemajuan teknologi AI berpotensi untuk disalahgunakan terutama dalam pembuatan dan penyebaran disinformasi serta misinformasi. Teknologi seperti *deepfake* dapat dimanfaatkan untuk membuat konten menyesatkan seperti video atau audio dan disebarkan pada berbagai *platform* media sosial. Penyalahgunaan ini memungkinkan pelaku menyebarkan informasi palsu secara masif dan cepat, mempengaruhi opini publik, dan merusak kepercayaan publik.

Ancaman-ancaman tersebut berpotensi akan muncul dengan berbagai pendekatan *cyber influence*. Contoh pendekatan yang mungkin digunakan meliputi provokasi, propaganda, *point and shriek*, pembanjiran informasi (*flooding*) dan *laundering*.

PROVOKASI

Provokasi merupakan tindakan mengeksploitasi isu-isu sensitif untuk memancing orang dan menimbulkan kemarahan serta ketidakharmonisan. Metode ini seringkali menggunakan teknik pengaruh informasi berupa *social cognitive hacking, deceptive identities,* dan *malicious rhetoric.*

POINT AND SHRIEK

Strategi "*Point and Shriek*" dibangun berdasarkan taktik yang digunakan oleh aktivis sosial memanfaatkan ketidakadilan yang dirasakan dalam kelompok sosial tertentu dan meningkatkan emosi terkait isu-isu tersebut untuk mengganggu diskursus rasional.

PROPAGANDA

Propaganda merupakan upaya sistematis untuk menyebarkan informasi, ide, atau narasi tertentu yang dirancang untuk mempengaruhi pandangan, sikap, atau perilaku orang banyak melalui ruang siber yang bertujuan untuk memanipulasi atau membentuk opini publik dengan cara menguntungkan pihak tertentu, baik itu individu atau kelompok sehingga menyebabkan keresahan sosial di masyarakat.

PEMBANJIRAN INFORMASI

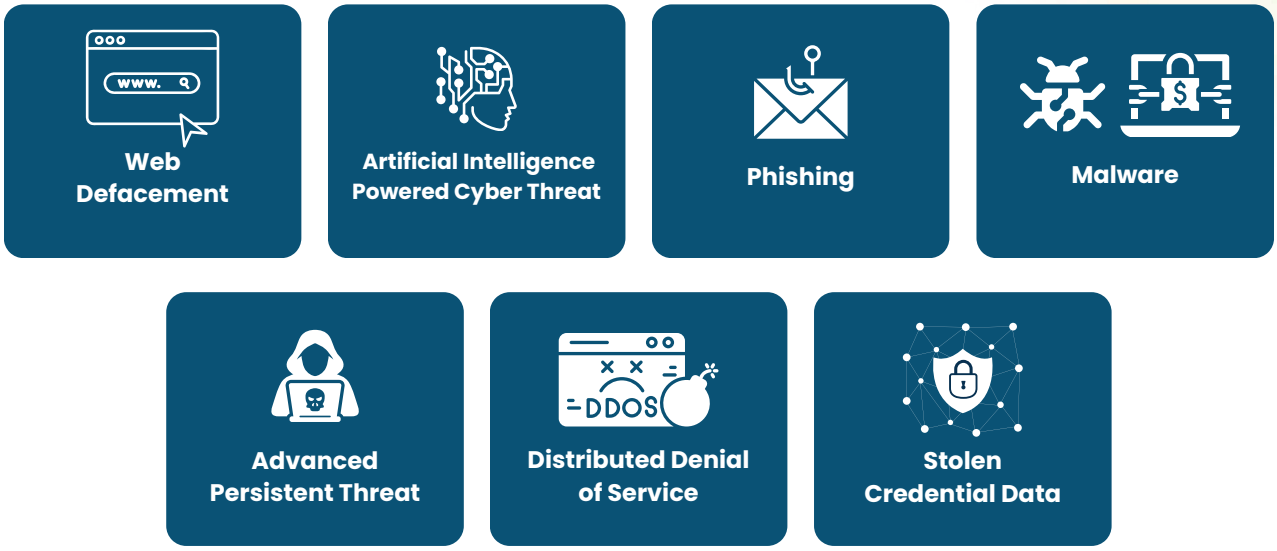
Pembanjiran Informasi (*flooding*) adalah suatu metode yang dirancang untuk menciptakan kebingungan dengan cara membanjiri audiens dengan informasi, baik positif, negatif, atau tidak relevan sehingga dapat melemahkan audiens dalam membedakan informasi yang sah. Hal ini dapat dilakukan dengan *spamming* dan *trolling* di media sosial dengan menyebarkan disinformasi ke sumber media yang sah.

LAUNDERING

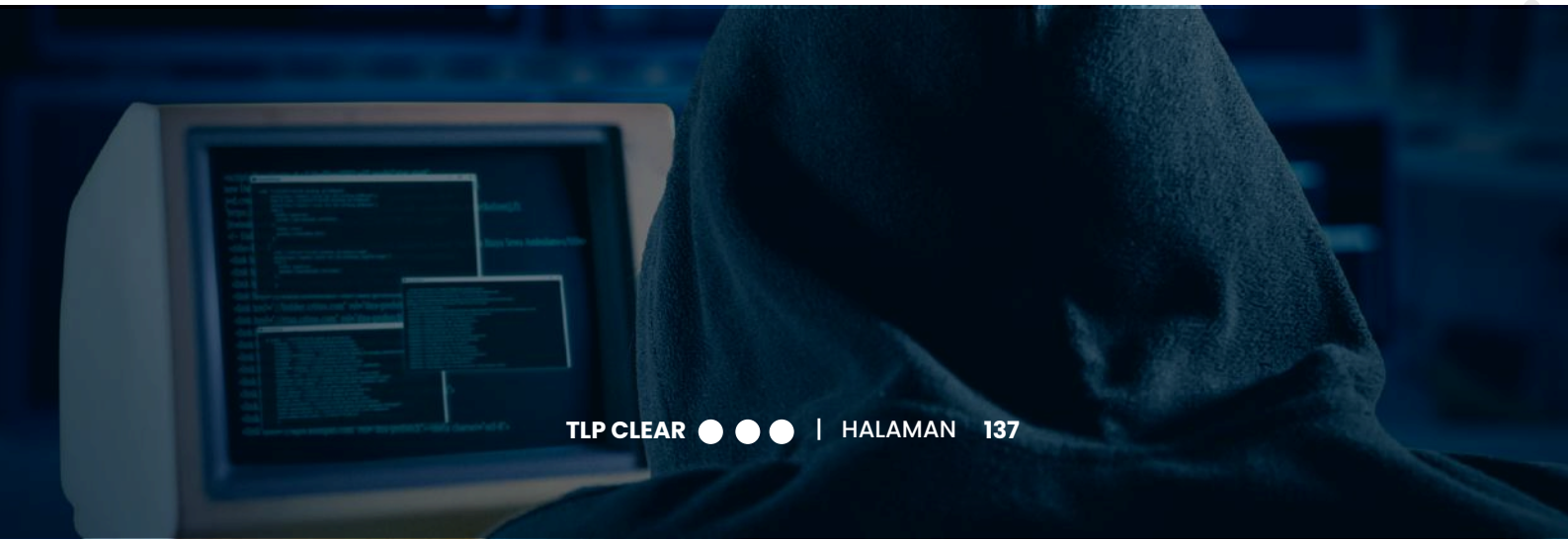
Laundering merupakan sebuah metode yang menggunakan proses distorsi bertahap dan de-kontekstualisasi informasi, sehingga menjadi sulit untuk mengetahui apakah sumbernya benar atau salah. Strategi ini dapat menggunakan *deceptive identities*, disinformasi, manipulasi, dan *symbolic action* dengan kombinasi peretasan sosial dan kognitif untuk menciptakan jaringan informasi palsu.

Untuk mengantisipasi potensi ancaman siber sosial, diperlukan sinergi dan kolaborasi seluruh pemangku kepentingan (Pemerintah, Pelaku Usaha, Akademisi, dan Komunitas/Masyarakat). Selain itu, langkah strategis yang dapat dilakukan di antaranya penguatan aspek teknis dan non teknis, serta penguatan kerja sama berbagai pihak dengan seluruh pemangku kepentingan.

PREDIKSI POTENSI ANCAMAN SIBER TEKNIS



Berdasarkan pengumpulan data dari sumber terbuka, hasil deteksi keamanan siber dari trafik internet Indonesia, penelusuran *cyber threat intelligence,* analisis celah kerentanan pada aplikasi berbasis internet yang telah dilakukan pengujian keamanan oleh BSSN, dan *lesson learned* dari penanganan insiden, telah diprediksi potensi ancaman siber yang dapat menjadi serangan pada tahun 2025. Ancaman tersebut meliputi *web defacement, AI powered cyber threat, phishing, malware*, APT, DDoS, dan *stolen credential data*. Penetapan potensi ancaman ini didasarkan pada peningkatan jumlah yang signifikan dalam beberapa tahun terakhir, menunjukkan kecenderungan meningkat yang diperkirakan akan berlanjut pada tahun 2025. Dalam rangka mengantisipasi potensi ancaman ini, langkah-langkah yang disarankan antara lain melakukan *backup* data secara berkala, menerapkan pembatasan hak akses, dan melakukan pembaruan sistem operasi secara teratur.



WEB DEFACEMENT

Ancaman *web defacement* merupakan upaya mengubah tampilan suatu situs web dengan tujuan menyampaikan pesan atau merusak reputasi pemiliknya. Web yang menjadi target umumnya memiliki nilai simbolis, seperti situs web pemerintah, perusahaan besar, atau lembaga penting. Pesan yang disampaikan bervariasi, mulai dari pesan teks, gambar, hingga pesan politis atau ideologis. *Threat actor* sering kali memanfaatkan celah keamanan pada situs web atau menggunakan teknik hacking untuk mendapatkan akses tidak sah, sehingga dapat dengan mudah mengganti halaman utama situs tersebut dengan pesan atau konten yang dimaksudkan. Ancaman *web defacement* bukan hanya merupakan pelanggaran terhadap privasi dan integritas suatu situs web, tetapi juga dapat memiliki dampak serius terhadap reputasi dan kepercayaan pengguna yang mengakses situs tersebut.

ARTIFICIAL INTELLIGENCE POWERED CYBER THREAT

Pada tahun 2025, ancaman siber berbasis *Artificial Intelligence* (AI) diprediksi semakin kompleks. AI berpotensi dimanfaatkan *threat actor* untuk menciptakan *malware* adaptif, *phishing* yang dipersonalisasi, dan *deepfake* untuk manipulasi data. Teknologi ini memungkinkan eksploitasi celah keamanan lebih cepat, serangan DDoS yang menyesuaikan pola secara *real-time*, serta *ransomware* yang secara otomatis memilih target paling rentan. Dengan kemampuan adaptasi dan pembelajaran mandiri, AI menjadikan serangan siber semakin canggih dan sulit dideteksi.

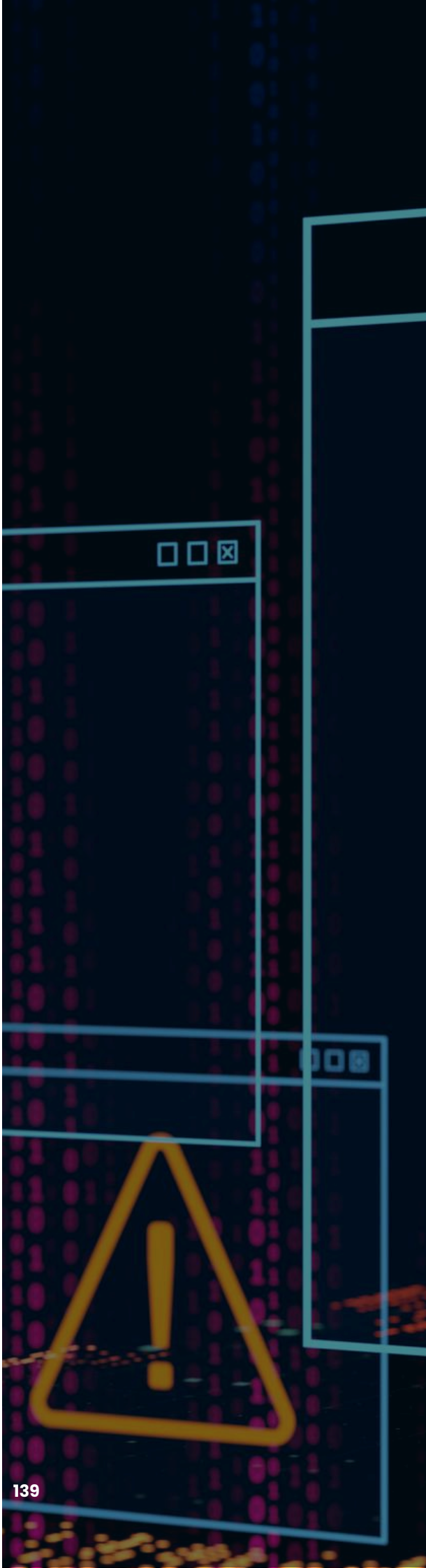
PHISING

Phishing adalah salah satu bentuk ancaman siber yang dilakukan dengan cara membuat tampilan atau sistem yang menyerupai sistem asli untuk menipu korban. Melalui serangan ini, pelaku berusaha mencuri data kredensial, seperti *username* dan *password*, atau informasi sensitif lainnya dengan menggunakan komunikasi yang tampak sah, seperti *email*, situs web, atau pesan instan. Dengan menyamar sebagai entitas terpercaya, pelaku *phishing* memanfaatkan kelengahan pengguna untuk mengeklik tautan palsu atau memasukkan informasi pribadi ke dalam situs yang sebenarnya dikendalikan oleh pelaku. Serangan ini sering kali terlihat meyakinkan, sehingga penting bagi pengguna untuk selalu waspada dan memeriksa keaslian sumber komunikasi sebelum memberikan data sensitif.

MALWARE

Malware, atau *malicious software*, adalah istilah umum untuk perangkat lunak berbahaya yang dirancang untuk tujuan jahat, seperti merusak sistem komputer, mencuri data, atau mengganggu jalannya bisnis. Salah satu jenis *malware* yang sangat merugikan dan terus berkembang adalah *ransomware*. *Ransomware* bekerja dengan mengenkripsi data korban, membuatnya tidak dapat diakses, dan kemudian meminta tebusan sebagai imbalan untuk memberikan kunci dekripsi. Penyebaran *ransomware* bisa melalui berbagai cara, mulai dari *email phishing* yang menipu pengguna untuk mengeklik tautan atau membuka lampiran berbahaya, unduhan ilegal dari sumber yang tidak terpercaya, hingga eksploitasi kerentanan pada perangkat lunak. Dampak yang ditimbulkan *ransomware* sangat signifikan, mulai dari kehilangan data penting dan sensitif yang berakibat pada terganggunya operasional bisnis, penelitian, bahkan kehidupan pribadi, hingga lumpuhnya sistem dan infrastruktur TI yang menyebabkan penghentian total layanan. Kerugian finansial juga tak terhindarkan, baik akibat pembayaran tebusan kepada *threat actor*, biaya pemulihan data, hilangnya pendapatan karena gangguan operasional, maupun denda yang mungkin dikenakan oleh *regulator* akibat pelanggaran data. Serangan *ransomware* juga berpotensi merusak reputasi organisasi dan menurunkan kepercayaan pelanggan.

Beberapa langkah yang dapat dilakukan untuk melakukan pencegahan dan mengatasi ancaman *ransomware* antara lain melakukan *backup* data secara rutin dan menyimpannya di lokasi terpisah, menerapkan sistem keamanan siber berlapis yang mencakup penggunaan perangkat lunak *antivirus* dan *anti-malware* yang mutakhir, *firewall*, dan sistem deteksi intrusi, melakukan *patching* dan pembaruan perangkat lunak secara teratur untuk menutup celah keamanan, meningkatkan kesadaran keamanan siber melalui pelatihan kepada pengguna, serta memiliki rencana respons insiden yang jelas untuk meminimalkan dampak dan mempercepat pemulihan jika terjadi serangan.



ADVANCED PERSISTENT THREAT

APT merupakan serangan yang dilakukan oleh suatu kelompok atau *threat actor* yang dapat berkaitan dengan negara tertentu. *Threat actor* ini menggunakan berbagai metode dan teknik canggih yang dirancang untuk melakukan serangan siber secara terus-menerus tanpa terdeteksi perangkat keamanan untuk mendapatkan akses ke sistem dan bertahan dalam sistem tersebut dalam jangka waktu yang lama. Tujuan *threat actor* adalah mengakses, memantau, dan mengumpulkan informasi dari sistem atau jaringan target untuk melakukan pencurian data yang bernilai seperti informasi rahasia perusahaan, data keuangan, atau rancangan teknologi tinggi dengan tujuan eksploitasi jangka panjang. Biasanya serangan ini menargetkan informasi dan aset vital suatu negara.

DISTRIBUTED DENIAL OF SERVICE

Serangan *Denial of Service* (DoS) merupakan jenis serangan yang ditujukan untuk menguras sumber daya sistem jaringan, sehingga sistem tersebut tidak dapat beroperasi sebagaimana mestinya dan menghalangi akses pengguna lain ke layanan yang disediakan. Serangan ini memanfaatkan kelemahan sistem seperti keterbatasan *bandwidth*, kapasitas memori, daya *server*, atau celah lain dalam sistem. Umumnya, DoS menargetkan usaha kecil hingga menengah yang memiliki sumber daya terbatas. Meskipun tujuan utamanya adalah membuat sistem tidak berfungsi, terdapat juga kasus di mana *threat actor* meminta tebusan untuk menghentikan serangan.

DoS dilakukan dengan menggunakan satu perangkat komputer dan satu koneksi internet. Namun, untuk serangan dalam skala besar, *threat actor* dapat mengontrol banyak perangkat dan koneksi internet secara bersamaan menggunakan Botnet. Botnet terdiri dari perangkat-perangkat yang telah terinfeksi *malware* tanpa sepengetahuan pemiliknya. Jika serangan dilancarkan melalui banyak perangkat secara serentak, maka serangan ini disebut *Distributed Denial of Service* (DDoS).

STOLEN CREDENTIAL DATA

Pencurian data kredensial adalah salah satu bentuk ancaman siber yang semakin sering terjadi. Pencurian data kredensial, milik individu maupun organisasi memiliki daya tarik tersendiri bagi *threat actor* untuk mendapatkan keuntungan materi. Tindakan ini melibatkan pengambilan informasi autentikasi secara ilegal. Informasi yang dicuri ini dapat digunakan untuk mengakses sistem korban secara tidak sah atau dijual di pasar gelap (*dark web*). Salah satu cara yang sering digunakan oleh *threat actor* adalah memanfaatkan kerentanan pada sistem atau mengirimkan *malware stealer* yang dirancang khusus untuk mencuri data tersebut. Kredensial yang dicuri ini menjadi aset berharga yang memungkinkan pelaku ancaman melancarkan serangan lanjutan atau mendapatkan keuntungan finansial langsung. Dampak dari pencurian kredensial ini sangat besar, baik bagi individu maupun organisasi. Dari sisi individu, kehilangan akses ke akun pribadi, seperti media sosial atau layanan finansial, dapat menyebabkan kerugian materi dan pelanggaran privasi. Sementara itu, bagi organisasi, kredensial yang dicuri bisa membuka pintu bagi pelaku ancaman untuk masuk ke dalam sistem mereka, mencuri data berharga, atau bahkan melumpuhkan operasional perusahaan. Kebocoran data semacam ini tidak hanya merugikan secara finansial tetapi juga dapat mencemarkan reputasi dan kepercayaan publik terhadap organisasi yang terdampak

Malware seperti Lumma dan StealC menjadi salah satu *malware stealer* yang digunakan *threat actor* berdasarkan hasil *monitoring* BSSN. Target utama dari pencurian kredensial ini mencakup individu, organisasi, dan penyedia layanan teknologi. Individu sering menjadi korban pencurian data pribadi, seperti akun media sosial atau layanan keuangan. Di sisi lain, organisasi, termasuk perusahaan dan lembaga pemerintah, menjadi sasaran untuk akses terhadap data strategis atau pelanggan. Tidak hanya itu, penyedia layanan teknologi seperti *platform cloud* dan penyedia *email* juga menjadi target karena menyimpan data dalam jumlah besar yang dapat dimanfaatkan oleh *threat actor.*

LANSKAP KEAMANAN SIBER INDONESIA

2024

BADAN SIBER DAN SANDI NEGARA

TLP: CLEAR