LAPORAN TAHUNAN

KOMINFO-CSIRT

2024

csirt.komdigi.go.id

Ringkasan

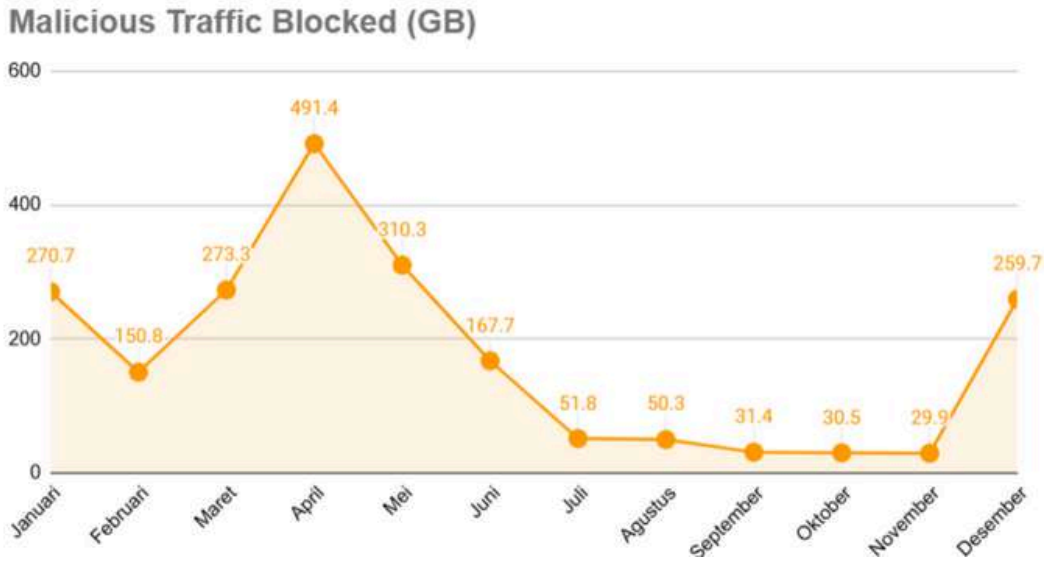
Laporan Tahunan Kominfo-CSIRT untuk tahun 2024 menyoroti berbagai peristiwa dan tren keamanan siber yang terjadi di Kementerian Komunikasi dan Informatika. Data menunjukkan bahwa **total trafik anomali** selama tahun berjalan mencapai **2.117 GBps**, dengan puncak **tertinggi** terjadi pada bulan **April (491,4 GB)** dan puncak **terendah** pada bulan **November (29,9 GB)**. Sebanyak **27 insiden siber** dilaporkan sepanjang tahun tersebut, dengan jumlah **tertinggi** terjadi pada bulan **Juli (6 insiden)**. Jenis insiden siber yang paling dominan adalah ***injected malicious file***, tercatat sebanyak **17 kali**. Selain itu, permintaan *Vulnerability Assessment/Penetration Testing* (VA/PT) **tertinggi** tercatat pada bulan **Maret dan Agustus**, dengan total **214 permintaan**. Data ini memberikan gambaran tentang kompleksitas dan eskalasi ancaman keamanan siber yang dihadapi oleh Kementerian Komunikasi dan Digital selama tahun 2024, dan menjadi landasan untuk strategi keamanan yang lebih efektif di masa depan.

TLP CLEAR

2.117 GBps

Total Trafik Anomali di lingkungan Kominfo

Total trafik anomali di Kementerian Komunikasi dan Informatika selama tahun 2024 adalah **2.117 GBps anomali**. Anomali trafik **tertinggi** terjadi pada bulan **April** dengan jumlah **491,4 GB anomali trafik**, sedangkan anomali **terendah** terjadi pada bulan **November** dengan jumlah **29,9 GB 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 periode Januari - Desember 2024:



Top 5 Trafik Anomali

Key	Category	Blocked
	DDoS Reputation	**61.1 GB**
	Location Based Threats	**1.9 GB**
	Command and Control	**390.0 MB**
	Mobile	**21.7 MB**
	Malware	**17.2 MB**

TLP CLEAR

Top 5 Negara Sumber dan Tujuan

Top Inbound Countries

Nation	Graph	Passed	Blocked	Percent
Indonesia		18.4 Mbps 5.3 kpps	561.7 kbps 111.6 pps	71 %
United States of America		4.4 Mbps 1.8 kpps	144.0 kbps 73.1 pps	17 %
Singapore		2.6 Mbps 532.1 pps	126.7 kbps 32.0 pps	10 %
Hong Kong		226.7 kbps 35.8 pps	41.6 kbps 5.1 pps	1 %
United Kingdom		178.3 kbps 98.2 pps	7.1 kbps 11.3 pps	1 %

TLP CLEAR

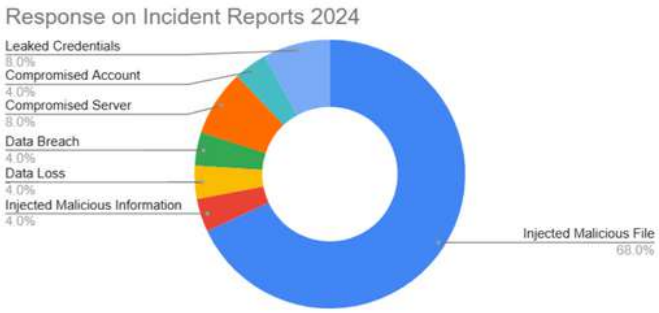
Rekapitulasi Insiden Siber

Incident response merupakan penindaklanjutan insiden siber dengan melibatkan Kominfo-CSIRT selaku CSIRT organisasi dan penanggung jawab sistem yang terdampak itu sendiri. Incident response dilakukan secepat mungkin dalam kurun waktu paling lambat 24 jam untuk mencegah insiden mengakibatkan dampak buruk lebih luas seperti masuknya kejadian insiden pada kanal berita yang dapat merusak citra instansi, pencurian data pribadi pengguna sistem, pengambilalihan kontrol penuh terhadap server, dan lain-lain.

Melalui laporan insiden siber yang masuk ke Kominfo-CSIRT, dilakukan verifikasi untuk mengetahui keabsahannya. Jika verifikasi sudah dilakukan dan insiden siber benar terjadi, maka dilakukan pengidentifikasian untuk menentukan tindak lanjut yang tepat seperti perlu atau tidaknya aplikasi web ditutup dari jaringan publik, penggunaan backup atau VPS (*virtual private server*) baru untuk menunjang pemulihan.

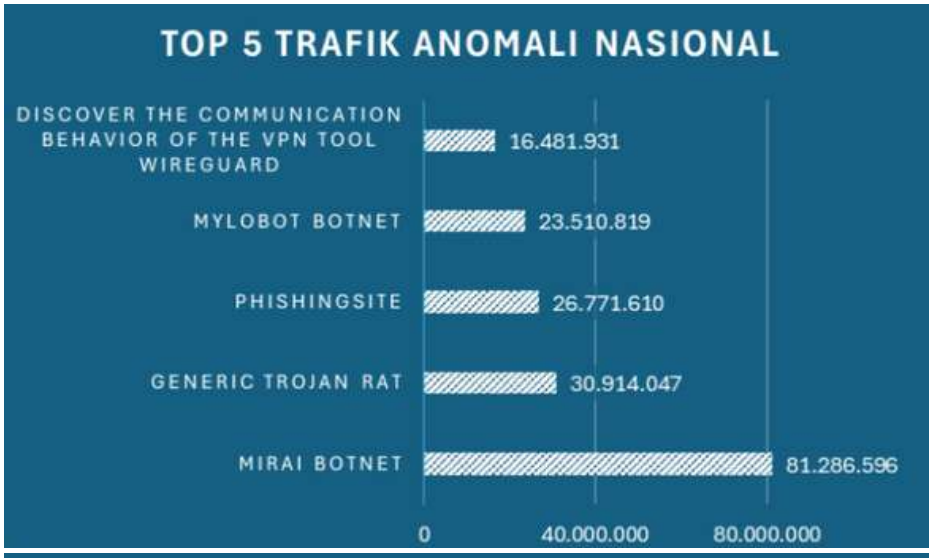
Sepanjang tahun **2024**, telah terjadi **27 kali insiden siber** di aplikasi web. Jumlah **tertinggi** insiden siber ada pada bulan **Mei** yakni sebanyak **5 kali** dan jumlah jenis insiden siber **tertinggi** berupa **injeksi berkas berbahaya (*injected malicious files*)** yakni sebanyak **14 kali**.

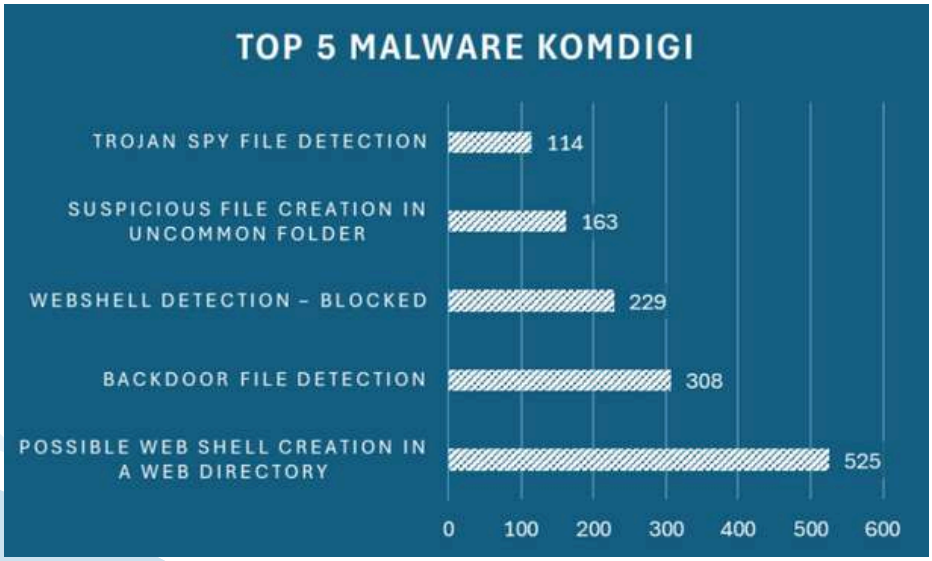
Melalui bantuan forensik dan investigasi penyebab terjadinya insiden siber, rekomendasi dan pendampingan perbaikan serta pemanfaatan XDR sebagai *anti-malware* dari Kominfo-CSIRT, sebanyak **27 kali insiden siber**, **26** insiden siber di antaranya **berhasil dipulihkan** sehingga dikembalikan ke jaringan publik, sementara **1 sisanya ditutup** karena memang **sudah tidak digunakan** lagi.



Top 5 Common Malware Activity

Malware (*Malicious Software*) dapat menjadi ancaman serius bagi organisasi dimana *malware* dapat merusak sistem, melakukan pencurian data, mengancam reputasi organisasi bahkan sampai mengakibatkan kerugian materiil . Kominfo-CSIRT telah mampu mencegah dan mengatasi beberapa *malware* yang saat ini sering menjadi penyebab terjadinya insiden dengan menggunakan tools *XDR* (*Extended Detections and Responses*). Berikut data 5 teratas trafik anomali nasional berdasarkan Lanskap Keamanan Siber 2024 BSSN dan data 5 teratas *malware* yang berhasil diatasi oleh tim Kominfo-CSIRT.



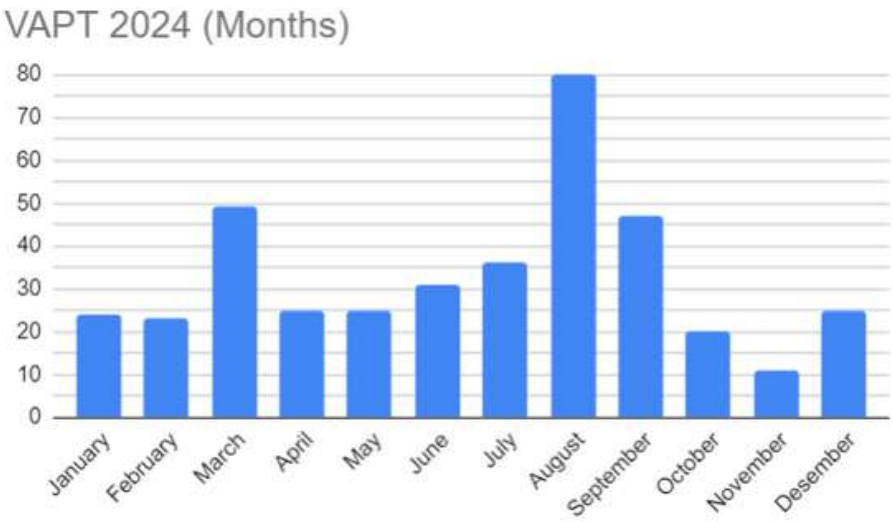


VA/PT pada KOMINFO-CSIRT

VA (*Vulnerability Assessment*)/ PT (*Penetration Testing*) merupakan kegiatan pengujian ketahanan sistem dalam upaya memanajemen potensi risiko siber. Melalui serangkaian pengujian terbarukan dan sistematik baik secara manual maupun menggunakan tools, temuan celah keamanan dikategorikan dan dijadikan dasar prioritas perbaikan. Tujuan utama VA/PT adalah memberikan pemahaman yang mendalam tentang keadaan keamanan siber terbaru dan membantu organisasi untuk fokus menangani kerentanan yang paling kritis.

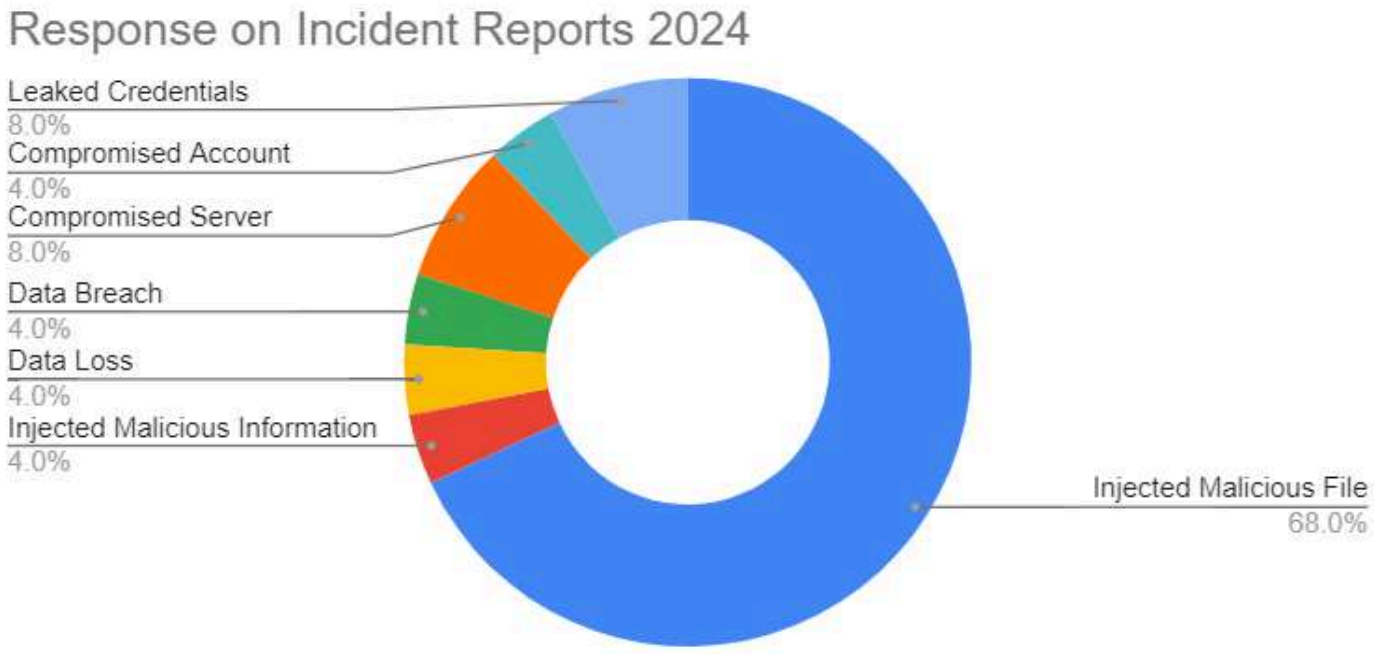
Melalui Helpdesk/aplikasi permintaan terhadap VA/PT dapat dilakukan oleh penanggung jawab aplikasi baik yang belum rilis maupun yang sudah rilis. Sebelum aplikasi diizinkan mendapatkan subdomain dan dapat diakses di jaringan publik/internet, aplikasi harus lolos dari VA/PT dengan kondisi tidak ada kerentanan dengan kategori sedang atau lebih tinggi.

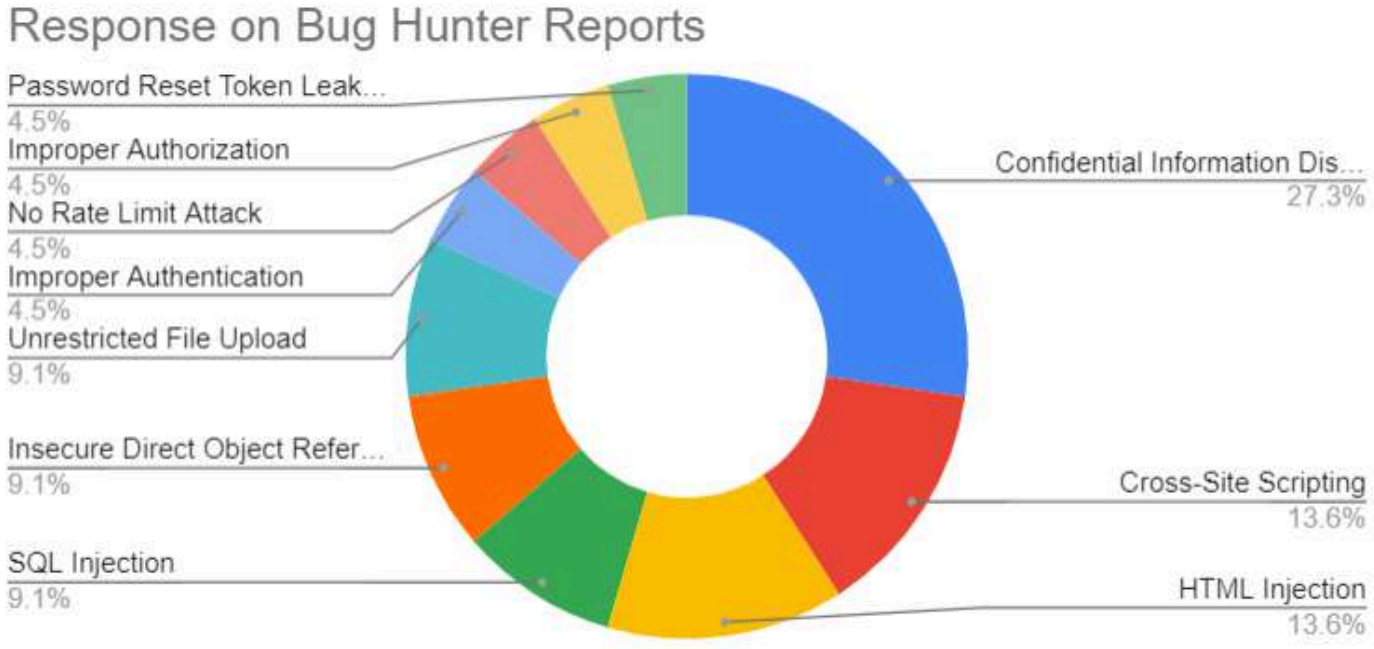
Dari data pada sistem informasi, didapatkan permintaan **VA/PT tertinggi** tahun 2024 terjadi di bulan **Agustus** 2024 memiliki jumlah **80** ***Request*** untuk dilakukan VA/PT.



TLP CLEAR

Top 5 Kerentanan





TLP CLEAR

Lesson Learned Top 5 Insiden Siber

1

Pentingnya Pemantauan dan Deteksi Dini:

- Kemampuan deteksi dini dan respon cepat terhadap ancaman siber menjadi kunci utama dalam meminimalisir dampak kerusakan.
- Perlu dilakukan investasi pada teknologi pemantauan dan analitik keamanan siber yang mumpuni.
- Tim keamanan siber harus selalu siaga dan proaktif dalam mengidentifikasi potensi ancaman.

2

Memperkuat Keamanan Infrastruktur TI:

- Infrastruktur TI yang rentan terhadap serangan siber menjadi celah bagi para pelaku cybercrime.
- Perlu dilakukan penguatan keamanan infrastruktur TI dengan menerapkan langkah-langkah seperti:
  - Patching kerentanan sistem operasi dan aplikasi secara berkala.
  - Menerapkan kontrol akses yang ketat dan autentikasi multi-faktor.
  - Melakukan segmentasi jaringan untuk membatasi penyebaran malware.

TLP CLEAR

Lesson Learned Top 5 Insiden Siber

3

Memperkuat Kerjasama dan Kolaborasi:

- Penanganan insiden siber membutuhkan kerjasama dan kolaborasi antar berbagai pihak.
- Perlu dibangun komunikasi dan koordinasi yang efektif antar unit di Kominfo, serta dengan lembaga terkait seperti BSSN, Polri, dan komunitas keamanan siber.
- Berbagi informasi dan pengetahuan tentang ancaman siber menjadi kunci untuk meningkatkan pertahanan kolektif.

4

Pentingnya Pengelolaan Risiko Siber:

- Pengelolaan risiko siber yang efektif membantu organisasi dalam mengidentifikasi, menilai, dan menanggapi potensi ancaman siber.
- Perlu dilakukan penerapan kerangka kerja manajemen risiko siber yang komprehensif di Kominfo.
- Penilaian risiko siber harus dilakukan secara berkala untuk memastikan keefektifan langkah-langkah mitigasi yang diterapkan.

5

Meningkatkan Kesadaran Keamanan Siber:

- Kurangnya kesadaran dan pengetahuan tentang keamanan siber menjadi faktor utama dalam banyak insiden siber.
- Perlu dilakukan edukasi dan pelatihan secara berkelanjutan kepada seluruh pegawai Kominfo tentang praktik keamanan siber yang baik.
- Penting untuk membangun budaya keamanan siber yang kuat di lingkungan Kominfo.

TLP CLEAR

World Water Forum 2024

Pada penyelenggaraan World Water Forum ke-10, Pusat Data dan Sarana Informatika (PDSI) bertugas dalam Bidang Keamanan Jaringan dan Pengelolaan Server. PDSI secara teknis menyiapkan server, memproteksi workstation dan monitoring jaringan koneksi internet di area Media Center dari serangan siber, malware, dan ancaman lainnya, serta memantau dan menangani permasalahan teknis terkait keamanan jaringan dan pengelolaan server. PDSI menyediakan infrastruktur dan keamanan siber untuk dua aset website yang digunakan pada WWF 2024, antara lain:

- Website Registrasi Media dan Konten media.worldwaterforum.org
- Website cloud media.worldwaterforum.org:2000

Keamanan siber server dan jaringan dilindungi oleh Web Application Firewall (WAF), Extended Detection Response (XDR) untuk server dan endpoint, serta monitoring dan pendeteksian serangan yang berpotensi terhadap aset website. Vulnerability Assessment and Penetration Testing (VA/PT) juga dilakukan dengan menguji kerentanan dan memberi rekomendasi pengamanan dalam meminimalisir celah kerawanan pada aset website. Secara keseluruhan, keamanan siber Media Center WWF 2024 berjalan lancar dan aman.

MSP-IAF 2024

Sama seperti pada kegiatan yang disebutkan sebelumnya, selama pelaksanaan Pengamanan Siber Media Center High-Level Forum on Multi-Stakeholder Partnerships (HLF MLP) dan Indonesia-Africa Forum (IAF) ke-2 Joint Leaders Session 2024 yang diselenggarakan pada tanggal 1 - 3 September 2024. Pada penyelenggaraan HLF MLP dan IAF 2024, Pusat Data dan Sarana Informatika (PDSI) bertugas dalam Bidang Pengelolaan Situs Resmi Media dan Registrasi Jurnalis serta Bidang Keamanan Jaringan dan Pengelolaan Sistem Informasi dengan memastikan seluruh koneksi jaringan di area Media Center aman dari serangan siber, malware, dan ancaman siber lainnya, merencanakan dan menyiapkan pembangunan sistem informasi, melakukan pemeliharaan serta pemantauan terhadap pemanfaatan fungsi dan kinerja sistem informasi, serta memantau dan menangani permasalahan teknis terkait keamanan jaringan dan pengelolaan sistem informasi di area Media Center. PDSI menyediakan infrastruktur dan keamanan siber untuk dua aset website yang digunakan pada HLF MLP dan IAF 2024:

- Website media.msp-iaf.id
- Website cloud.msp-iaf.id

Keamanan siber server dan jaringan dilindungi oleh Web Application Firewall (WAF), Extended Detection and Response (XDR) untuk server dan endpoint pada 20 PC di Media Center serta monitoring dan pendeteksian serangan yang berpotensi terhadap aset website. Vulnerability Assessment and Penetration Testing (VA/PT) juga dilakukan dengan menguji kerentanan dan memberi rekomendasi pengamanan dalam meminimalisir celah kerawanan pada aset website. Secara keseluruhan, keamanan siber Media Center HLF MLP dan IAF 2024 berjalan lancar dan aman.

Peringatan Hari Ibu ke-96 Tahun 2024

Peringatan Hari Ibu ke-96 Tahun 2024 telah diselenggarakan pada tanggal 21-22 Desember 2024, dengan acara puncak dipusatkan di Kantor Pusat Pemerintah Kota Tangerang, dengan dihadiri oleh Ibu Selvi Ananda, istri dari Wakil Presiden Indonesia, dan Menteri Pemberdayaan Perempuan dan Perlindungan Anak RI, serta jajaran pemangku kepetingan lainnya. PDSI mengamankan koneksi jaringan di area acara dari serangan cyber, malware, dan ancaman lainnya, memantau dan menangani permasalahan teknis terkait keamanan jaringan dan perlindungan endpoint (PC/laptop) yang digunakan untuk host video conference dan perangkat live streaming yang tersebar di 6 (enam) titik lokasi yaitu Provinsi Banten (Kota Tangerang), Provinsi Jawa Timur (Kota Malang), Provinsi Jambi (Kabupaten Muaro Jambi), Provinsi Kalimantan Selatan (Kabupaten Barito Kuala), Provinsi Gorontalo (Kabupaten Bone Bolango), dan Provinsi Nusa Tenggara Timur (Kota Kupang). Selama berlangsungnya kegiatan tersebut, Extended Detection Response (XDR) diinstall pada total 6 (enam) laptop yang digunakan untuk host video conference dan live streaming.

Kesimpulan dan Penutup

Laporan tahunan ini merupakan laporan dari hasil kegiatan semua program yang dilaksanakan di Kementerian Komunikasi dan Informatika sepanjang tahun 2024. Sepanjang tahun 2024, KOMINFO-CSIRT telah berupaya meningkatkan kesiapsiagaan, respons cepat, dan kapasitas dalam menghadapi berbagai tantangan keamanan siber. Ke depan, KOMINFO-CSIRT akan terus berkomitmen untuk memperkuat strategi keamanan siber melalui pengembangan kapabilitas, peningkatan kesadaran keamanan bagi seluruh pemangku kepentingan, serta implementasi kebijakan yang lebih adaptif terhadap dinamika ancaman siber.