Laporan Keamanan Siber Tahun 2024

Mengulas Kejadian Serangan, Statistik, Ancaman Paling Serius, CVE, dan Ancaman Terbaru

Edy Susanto - Senior Cyber Security Specialist

Serangan Siber 2024

Kategori	Statistik
Peningkatan Serangan	30%
Elemen Manusia	68%
Intrusi Cloud	75%
Rata-rata Tebusan	$2,73 juta
Malware via Email	94%
Biaya Pelanggaran	$4,45 juta
Biaya Kejahatan	$9,5 triliun USD

Peningkatan 30% dalam jumlah serangan siber mingguan yang tercatat oleh organisasi.

67% dari serangan siber yang berhasil disebabkan oleh kelalaian manusia atau serangan berbasis manusia, seperti phishing

68% dari pelanggaran melibatkan elemen manusia pada tahun 2024.

Peningkatan 75% dalam intrusi cloud, menyoroti kebutuhan akan langkah-langkah keamanan cloud yang kuat

Serangan Siber 2024

01

RANSOMWARE

Ransomware:

- $2,73 juta adalah rata-rata tebusan yang diminta dalam serangan ransomware, hampir $1 juta lebih tinggi dari tahun 2023.
- Hanya 8% dari bisnis yang membayar tebusan kepada peretas menerima semua data mereka kembali.
- 94% dari semua malware dikirim melalui email.

02

BIAYA DAMPAK

Biaya dan Dampak:

- Biaya rata-rata pelanggaran data global pada tahun 2023 adalah $4,45 juta, meningkat 15% selama tiga tahun.
- Biaya kejahatan siber global diperkirakan mencapai $9,5 triliun USD pada tahun 2024

Negara Paling Rentan

COUNTRY

AMERIKA SERIKAT
Serangan siber terbanyak, mencapai lebih dari 2 miliar kasus sejak tahun 2004.

JEPANG
8% dari total serangan siber global.

BRASIL
Mengalami 6% dari total serangan siber global.

KANADA
Menyumbang 5% dari total serangan siber global.

AUSTRALIA
menyumbang 4% dari total serangan siber global

MEKSIKO
menyumbang 4% dari total serangan siber global

KOREA SELATAN
Mengalami 2% dari total serangan siber global

CHILE
menyumbang 2% dari total serangan siber global

Sektor Paling Rentan

5 SEKTOR UTAMA SASARAN SERANGAN SIBER DI SELURUH DUNIA

SEKTOR KEUANGAN
Sektor ini selalu menjadi target utama karena akses langsung ke dana dan data keuangan sensitif

KESEHATAN
Serangan ransomware dan pelanggaran catatan kesehatan elektronik (EHR)

PEMERINTAHAN
Serangan siber dapat mengganggu layanan publik dan keamanan nasional

PENDIDIKAN
Serangan siber dapat mengganggu operasi dan merusak reputasi

ENERGI
Serangan siber yang dapat mengganggu pasokan energi dan layanan utilitas

Trend Keamanan Siber 2024

TREND 2024

EVOLUSI RANSOMWARE

Double extortion, mempublikasikan data sensitif korban jika tebusan tidak dibayarkan.

AI & ML

metode serangan yang lebih sulit dideteksi, seperti deepfake

PHISHING NEXT GENERATION

Serangan phishing semakin personal dengan teknik spear phishing,

ZERO TRUST

Prinsip zero trust semakin diadopsi untuk melindungi jaringan perusahaan, ekosistem

SERANGAN IOT

Perangkat IoT seperti smart home dan kamera keamanan rentan terhadap serangan

Serangan Siber 2024

Serangan Ransomware pada LoanDepot

Eksploitasi Massal Kerentanan Zero-Day Ivanti.

Serangan Midnight Blizzard pada Microsoft.

Serangan Ransomware pada Change Healthcare

Serangan oleh Volt Typhoon: Kelompok peretas yang didukung oleh China, Volt Typhoon

Serangan pada Snowflake: Kampanye yang menargetkan pelanggan Snowflake

Serangan pada Verizon, AT&T, dan T-Mobile: Kelompok spionase yang terkait dengan China, Salt Typhoon

CVE 2024

- CWE-79: Cross-site Scripting (XSS) - CVEs in KEV: 3
- CWE-787: Out-of-bounds Write - CVEs in KEV: 18
- CWE-89: SQL Injection - CVEs in KEV: 4
- CWE-352: Cross-Site Request Forgery (CSRF) - CVEs in KEV: 0
- CWE-22: Path Traversal - CVEs in KEV: 4
- CWE-125: Out-of-bounds Read - CVEs in KEV: 3
- CWE-78: OS Command Injection - CVEs in KEV: 5
- CWE-416: Use After Free - CVEs in KEV: 5
- CWE-862: Missing Authorization - CVEs in KEV: 0
- CWE-434: Unrestricted Upload of File with Dangerous Type - CVEs in KEV: 0
- CWE-94: Code Injection - CVEs in KEV: 7
- CWE-20: Improper Input Validation - CVEs in KEV: 1
- CWE-77: Command Injection - CVEs in KEV: 4
- CWE-287: Improper Authentication - CVEs in KEV: 4
- CWE-269: Improper Privilege Management

Prediksi Ancaman 2025

Serangan Berbasis AI yang Lebih Canggih:

Peningkatan Serangan Ransomware:

Ransomware-as-a-service (RaaS) akan semakin populer

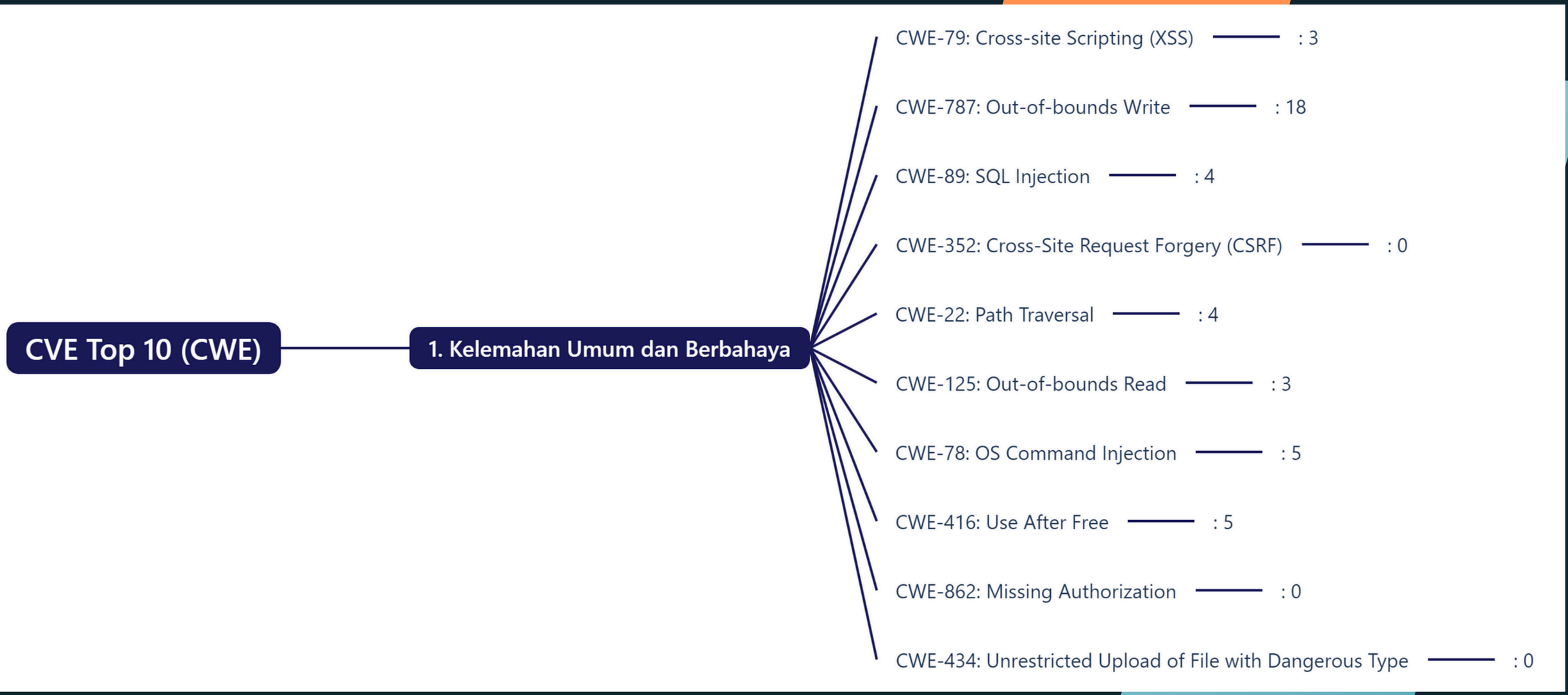
Serangan pada Infrastruktur Cloud

Disinformasi dan Manipulasi Data

Serangan pada Rantai Pasokan: Serangan pada rantai pasokan akan meningkat,

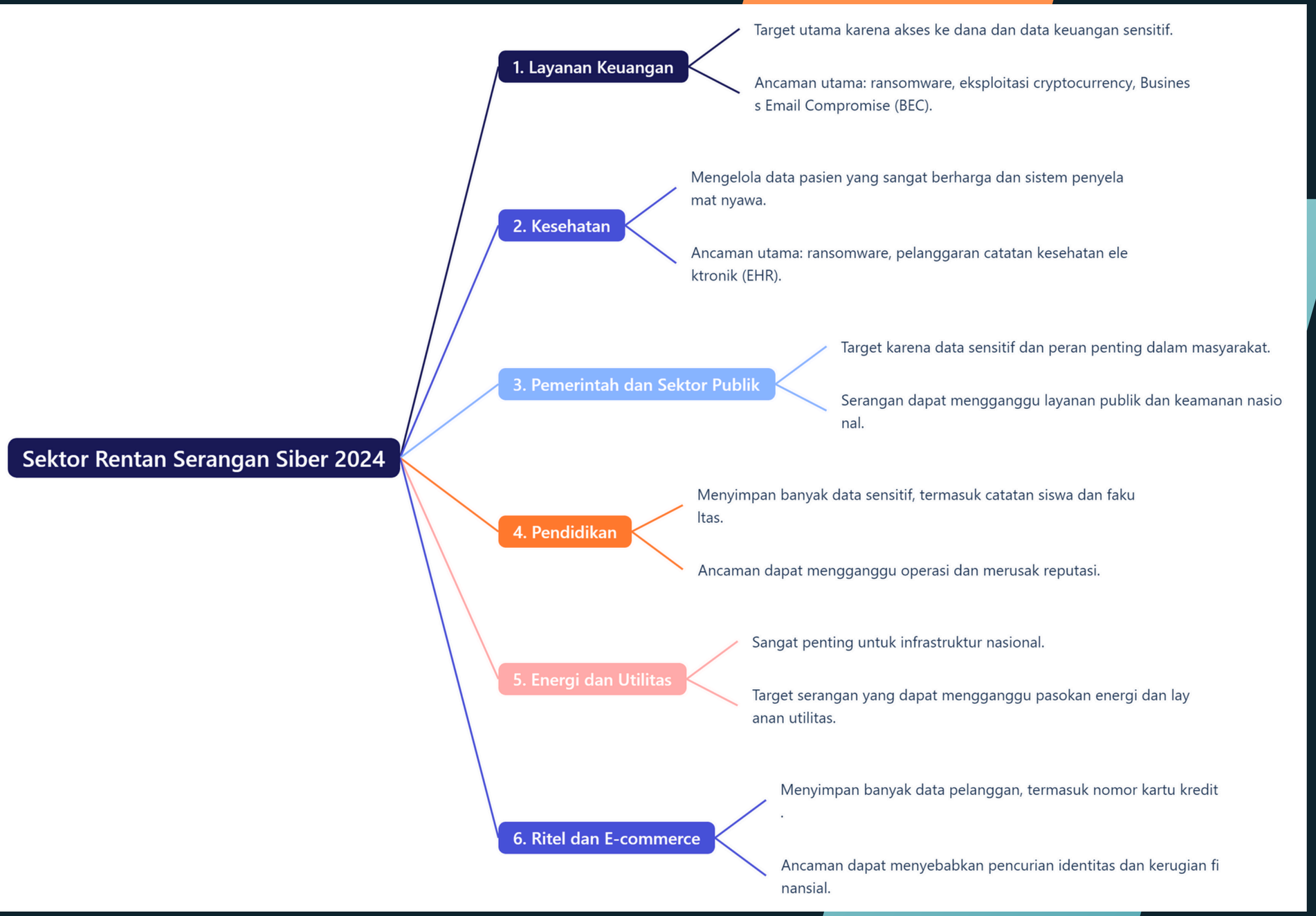
Konvergensi Ancaman Digital dan Fisik

Mind Mapping



Mind Mapping

Mind Mapping



EDY SUSANTO

Cyber Security | Blockchain | Tableau Specialist | Committed to Enhancing Data Security| www.edysusanto.com

Completed: Certified Ethical Hacker (CEH). Security and Mobile Security - Georgia Keensaw University. Cyber Attack Tools - IBM. EC-Council Certified Security Analyst(ECSA). Certified Penetration Testing (CPENT). Chief Of Information Security(CISO). Offensive Security Certified Professional(OSCP). Certified Information Systems Auditor(CISA). Certified Information Security Manager (CISM).Certified Information Systems Security Professional(CISSP). Information Systems Security Engineering Professional (ISSEP). RHCE.RHCSA.ITILV3.COBIT5.VCPDV.CSSA.CSGB.CSBB.CWNA.CWNE. Apsara Clouder Big Data. Apsara Clouder Security. Associate Cloud Security. Associate Cloud Computing. Tableau Specialist - UC Davis California. Data Science - Harvard University. Blockchain Specialist - Buffalo University. Linux Management and Security - Colorado University. Secure Coding - UC Davis California. Cloud Computing - Colorado University