Modul 4 – Vulnerability Intelligence & Exposure Analysis

Memahami dan menganalisis risiko keamanan siber berdasarkan informasi publik yang tersedia, mulai dari CVE hingga katalog eksploitasi aktif.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Tujuan Pembelajaran

Pada akhir modul ini, peserta diharapkan mampu menghubungkan teknologi yang teridentifikasi dengan potensi risiko keamanan secara sistematis dan berbasis data intelijen publik.

Memahami CVE

Mengidentifikasi dan menafsirkan entri kerentanan dari database resmi.

Severity Rating

Mengevaluasi tingkat keparahan menggunakan skor CVSS dan metrik lainnya.

Risk Prioritization

Menentukan kerentanan mana yang harus ditangani lebih dahulu berdasarkan konteks.

Exposure Analysis

Membedakan antara vulnerability dan exposure untuk pengambilan keputusan yang tepat.

Tools Utama dalam Vulnerability Intelligence

Ekosistem intelligence kerentanan dibangun di atas beberapa database publik yang saling melengkapi. Berikut adalah sumber referensi utama yang digunakan dalam modul ini.

CVE Program

Sistem identifikasi standar untuk kerentanan yang dikenal secara publik. Setiap entri memiliki ID unik seperti CVE-2024-XXXX yang menjadi referensi universal.

NVD – National Vulnerability Database

Database resmi NIST yang memperkaya data CVE dengan skor CVSS, referensi teknis, dan metadata tambahan untuk analisis mendalam.

Exploit Database

Repositori proof-of-concept dan exploit publik. Digunakan sebagai referensi riset untuk memahami bagaimana suatu kerentanan dapat dieksploitasi secara teknis.

CISA KEV Catalog

Katalog kerentanan yang terbukti aktif dieksploitasi di dunia nyata. Menjadi acuan prioritas penanganan bagi organisasi dan lembaga pemerintah.

Memahami CVE: Common Vulnerabilities & Exposures

CVE adalah sistem penamaan standar internasional untuk kerentanan keamanan yang telah diidentifikasi secara publik. Setiap entri CVE mencakup tiga komponen inti:

ID Unik

Format: **CVE-[Tahun]-[Nomor]**. Memungkinkan referensi konsisten di seluruh tool dan platform keamanan.

Deskripsi Teknis

Penjelasan singkat tentang jenis kerentanan, komponen yang terdampak, dan kondisi eksploitasi.

Referensi Publik

Tautan ke advisory vendor, patch, serta laporan riset yang relevan untuk tindak lanjut.

Mengapa CVE Penting?

CVE menjadi **bahasa universal** antara tim keamanan, vendor, dan regulator. Tanpa standar ini, koordinasi respons insiden dan patch management akan jauh lebih kompleks dan rentan terhadap kesalahan komunikasi.

Saat ini terdapat lebih dari **200.000+ entri CVE** aktif yang terus bertambah setiap harinya.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Severity Rating: Mengukur Tingkat Keparahan

CVSS (Common Vulnerability Scoring System) adalah standar industri untuk mengukur keparahan suatu kerentanan secara objektif. Skor dihitung berdasarkan vektor serangan, kompleksitas, dan dampak terhadap kerahasiaan, integritas, serta ketersediaan sistem.

🟢 Low (0.1–3.9)

Dampak terbatas, memerlukan kondisi khusus. Prioritas rendah namun tetap perlu dipantau.

🟡 Medium (4.0–6.9)

Risiko signifikan dalam kondisi tertentu. Perlu dijadwalkan untuk remediation dalam waktu dekat.

🟠 High (7.0–8.9)

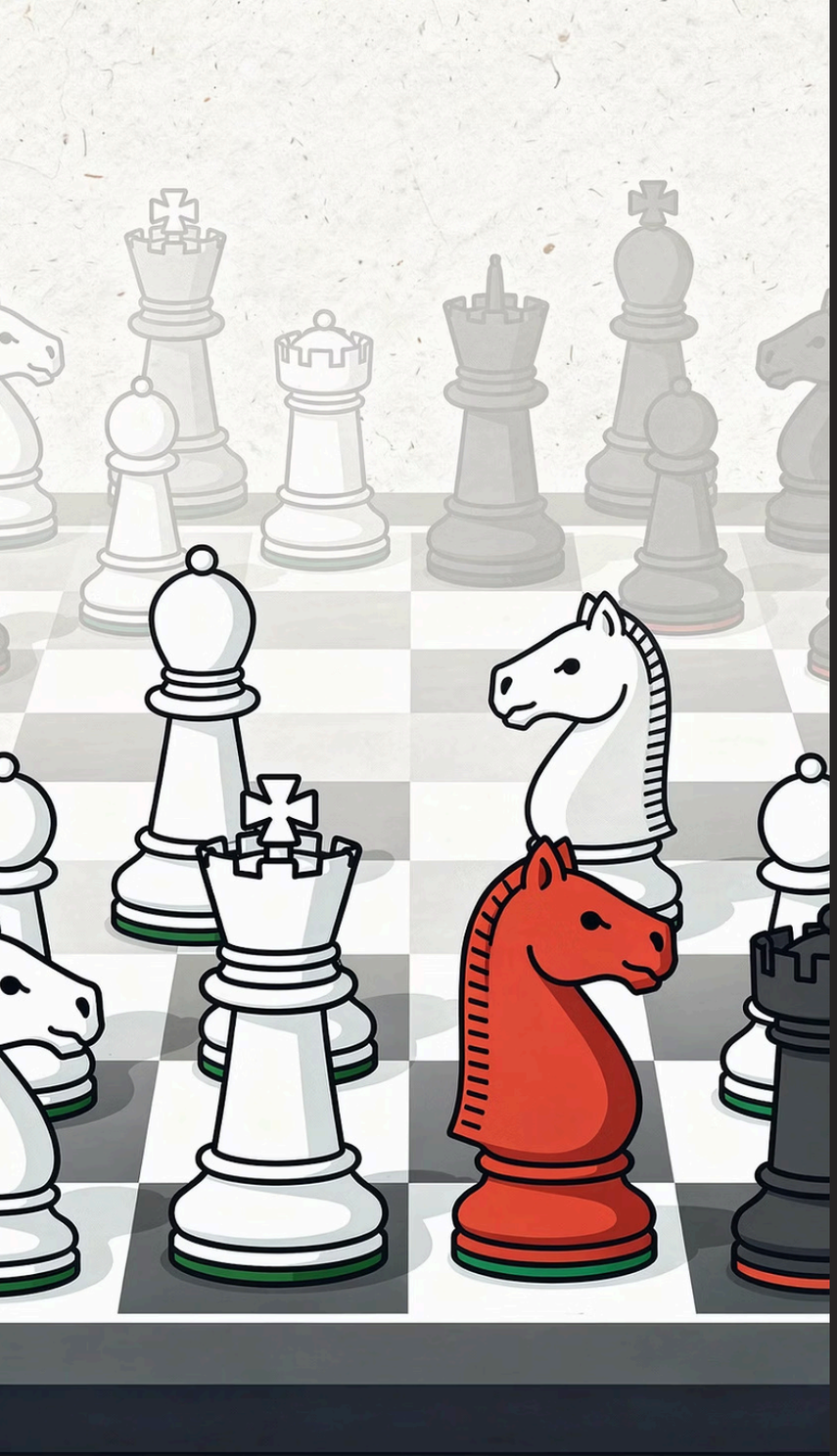
Eksploitasi memungkinkan akses tidak sah atau kerusakan data. Penanganan segera diprioritaskan.

🔴 Critical (9.0–10.0)

Eksploitasi jarak jauh tanpa autentikasi, dampak penuh. **Respon darurat diperlukan.**

⚠ CVSS skor bersifat kontekstual — skor tinggi tidak selalu berarti risiko tinggi bagi organisasi Anda. Faktor eksposur dan konteks lingkungan harus selalu dipertimbangkan.

EDY SUSANTO - FOUNDER C-SIX SECURITY



Risk Prioritization: Menentukan Mana yang Harus Ditangani Duluan

Tidak semua kerentanan dengan skor tinggi perlu ditangani segera. Risk prioritization menggabungkan skor teknis dengan faktor kontekstual organisasi untuk menghasilkan keputusan yang lebih tepat sasaran.

1

Identifikasi Aset Kritis

Tentukan aset mana yang paling bernilai dan sensitif bagi operasional organisasi.

2

Korelasi dengan KEV

Cek apakah kerentanan ada di CISA KEV Catalog — jika ya, prioritaskan segera.

3

Nilai Eksposur

Apakah sistem terhubung ke internet? Apakah ada kontrol kompensasi yang aktif?

4

Tindakan Remediation

Patch, mitigasi, isolasi, atau penerimaan risiko berdasarkan tingkat urgensi.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Threat Landscape Analysis

Apa itu Threat Landscape?

Threat landscape adalah gambaran menyeluruh tentang ancaman siber yang aktif dan relevan pada suatu waktu tertentu. Analisis ini mencakup jenis serangan, kelompok ancaman (threat actors), taktik, teknik, dan prosedur (TTP) yang sedang digunakan di dunia nyata.

Dengan memahami threat landscape, tim keamanan dapat:

- Memprioritaskan kerentanan yang sedang aktif dieksploitasi
- Mengantisipasi vektor serangan yang kemungkinan akan ditargetkan
- Menyelaraskan pertahanan dengan ancaman nyata, bukan hanya teoritis

Sumber Intelligence Landscape

MITRE ATT&CK

Framework TTP berbasis observasi serangan nyata.

Threat Reports Vendor

Laporan tahunan dari Mandiant, CrowdStrike, Microsoft, dll.

CISA Advisories

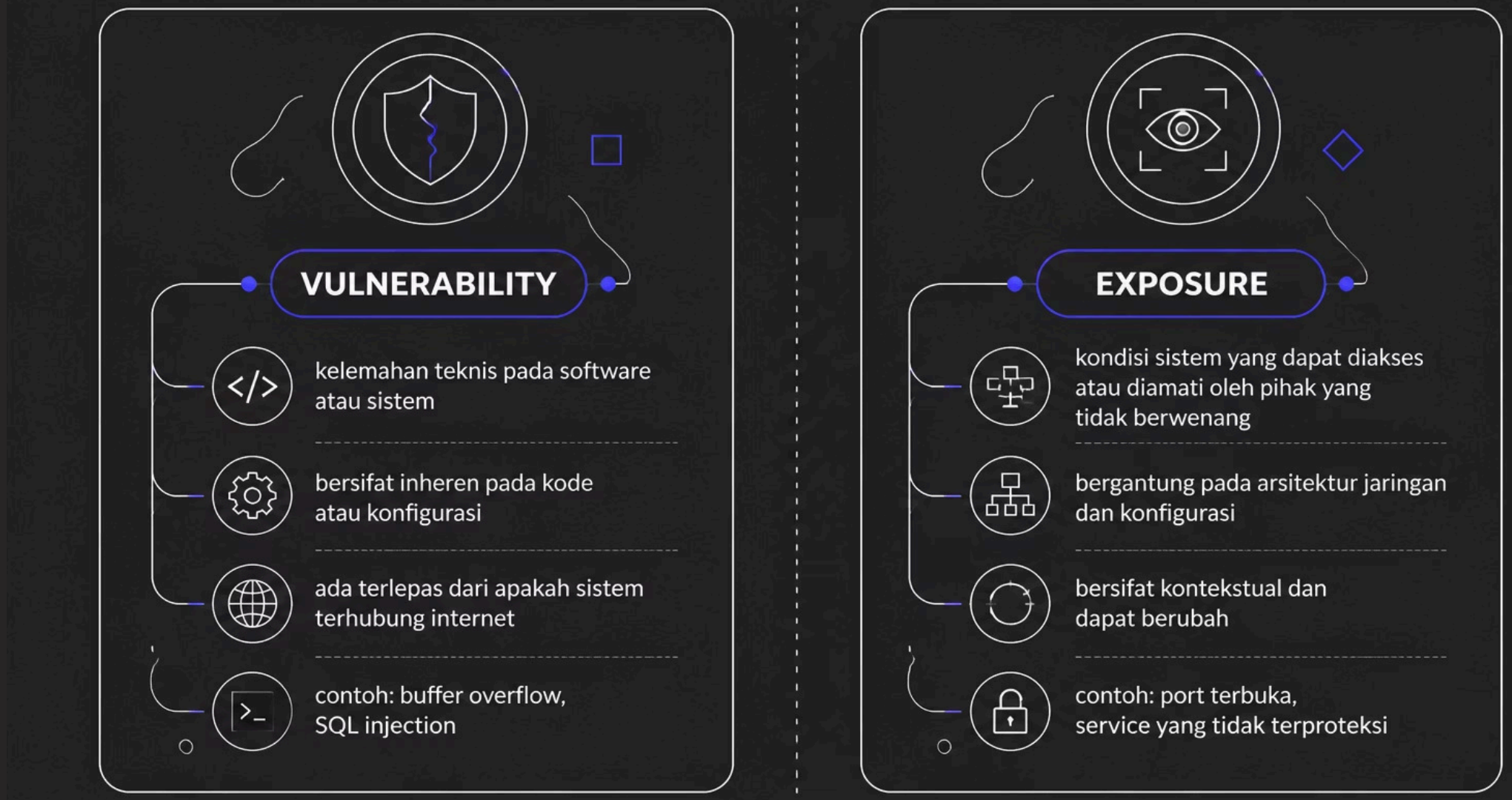
Peringatan ancaman aktif yang diterbitkan pemerintah AS.

OSINT & Dark Web

Monitoring forum, paste site, dan kanal underground.

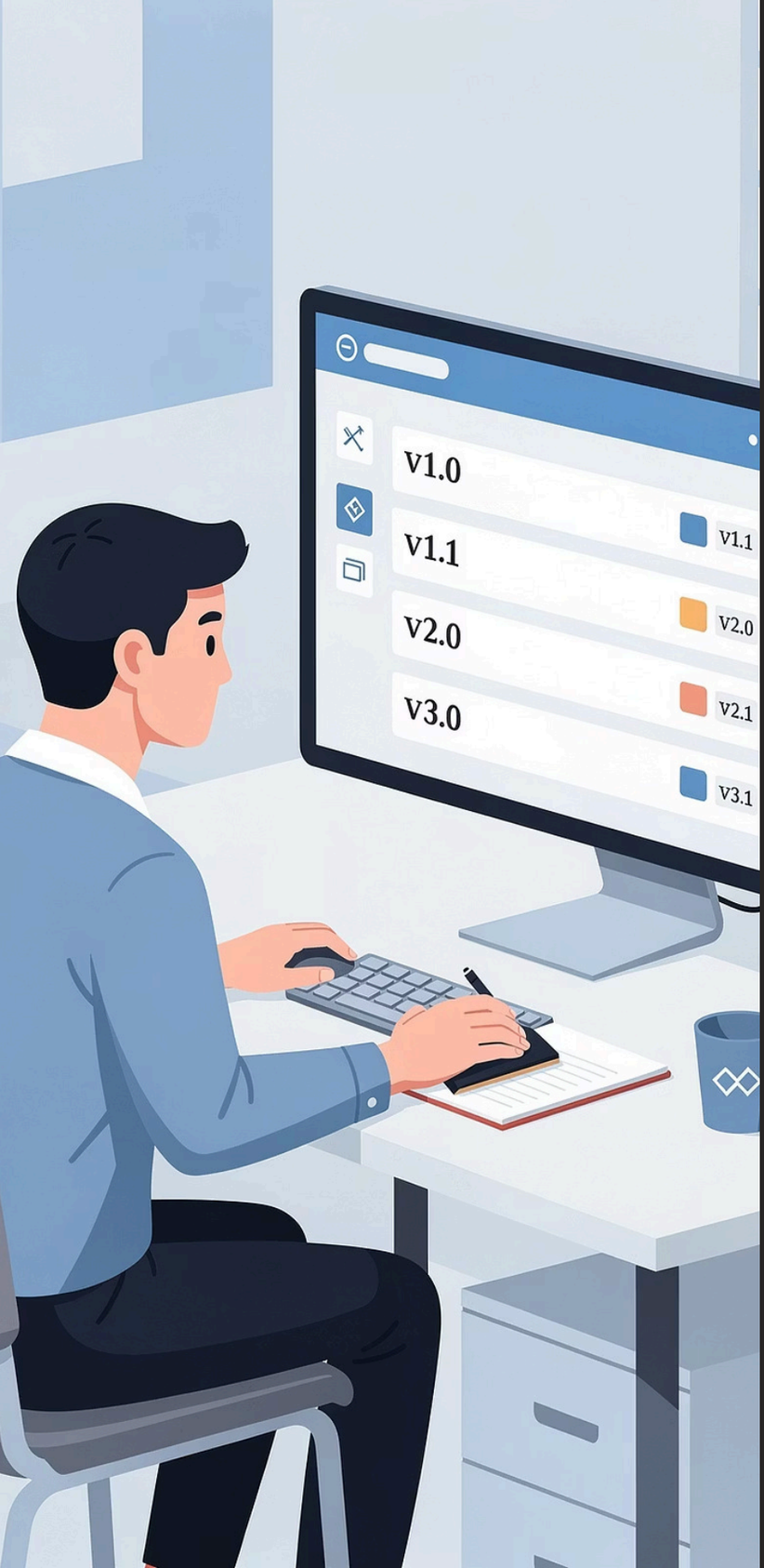
Exposure vs Vulnerability: Perbedaan yang Krusial

Dua istilah ini sering digunakan secara bergantian, namun memiliki makna teknis yang sangat berbeda dan berimplikasi langsung pada strategi mitigasi.



Sebuah vulnerability menjadi **risiko nyata** hanya ketika dikombinasikan dengan exposure. Sistem yang terisolasi dari internet dengan kerentanan kritikal memiliki risiko yang jauh lebih rendah dibanding sistem yang terekspos publik.

EDY SUSANTO - FOUNDER C-SIX SECURITY



Praktik: Analisis Risiko Berdasarkan Versi Software

Kemampuan mengidentifikasi versi software yang berjalan pada suatu sistem adalah fondasi dari vulnerability intelligence. Dari informasi ini, kita dapat memetakan kerentanan yang relevan secara akurat.

Identifikasi Versi Software

Gunakan tool seperti Nmap, Shodan, atau banner grabbing untuk mendeteksi versi OS, web server, dan aplikasi yang berjalan.

Cari CVE yang Relevan

Masukkan nama dan versi software ke NVD atau CVE.org. Filter berdasarkan tahun rilis dan skor CVSS untuk mempersempit hasil.

Verifikasi di CISA KEV

Periksa apakah CVE yang ditemukan terdaftar sebagai kerentanan yang aktif dieksploitasi. Jika ya, eskalasi prioritas penanganan.

Buat Laporan Risiko

Dokumentasikan temuan dengan konteks lingkungan, tingkat eksposur, dan rekomendasi remediation yang spesifik dan actionable.

EDY SUSANTO - FOUNDER C-SIX SECURITY

Ringkasan & Outcome Modul 4

Setelah menyelesaikan Modul 4, peserta memiliki kemampuan untuk menghubungkan teknologi yang teridentifikasi dengan potensi risiko keamanan secara terstruktur dan berbasis data intelijen publik yang valid.

CVE & NVD

Memahami dan menafsirkan entri kerentanan dari database standar internasional.

CVSS Scoring

Mengevaluasi tingkat keparahan secara objektif menggunakan metrik standar industri.

Risk Prioritization

Menentukan urutan penanganan berdasarkan eksposur, aset kritis, dan data KEV.

Threat Landscape

Menganalisis ancaman aktif dan mengontekstualisasikan risiko dalam lingkungan nyata.

Peserta kini siap melakukan **analisis risiko berbasis versi software** secara mandiri menggunakan tool-tool publik yang telah dipelajari dalam modul ini.