

Ancaman, Vektor Serangan, dan Faktor Manusia

Minggu 2 - 13S4121 Keamanan Siber

Malware, phishing, DoS/DDoS, MITM, insider threat, APT, dan attack surface

Albert Sagala, S.T., M.T.

Sarjana Teknik Elektro - Institut Teknologi Del

Posisi Materi dalam RPS

Sub-CPMK 2

Menganalisis malware, phishing, DoS, MITM, APT, insider threat, dan faktor manusia. [C3]

Kata kunci minggu ini

- ▶ Threat actor dan attack vector
- ▶ Malware, phishing, DoS/DDoS, MITM
- ▶ Insider threat dan APT
- ▶ Attack surface dan telemetry

Orientasi belajar

- ▶ Analisis tidak berhenti pada nama serangan
- ▶ Hubungkan aktor, tujuan, vektor, aksi, dan dampak
- ▶ Pisahkan fakta, inferensi, dan hal yang belum diketahui
- ▶ Rancang kontrol manusia, proses, dan teknologi

Materi ini merupakan versi mahasiswa dan tidak memuat kunci jawaban asesmen final.

Capaian Pembelajaran Mingguan

Pada akhir pertemuan, mahasiswa mampu:

- ▶ Mengklasifikasikan ancaman berdasarkan **pelaku**, **motivasi**, **kemampuan**, dan **target**.
- ▶ Menyusun **attack surface** dari komponen, identitas, antarmuka, data, dan ketergantungan.
- ▶ Menghubungkan taktik ancaman dengan peluang **deteksi** dan **mitigasi defensif**.
- ▶ Menganalisis faktor manusia tanpa menyederhanakan masalah sebagai kesalahan korban.

Indikator keberhasilan kelas

Mahasiswa dapat membuat threat model tingkat tinggi yang menyebutkan aset, actor goal, entry point, prasyarat, dampak, telemetry, dan kontrol berlapis.

Rencana Perkuliahan 100 Menit

Waktu	Aktivitas pembelajaran
0-10 menit	Apersepsi: mengapa ancaman tidak cukup dijelaskan dengan nama malware.
10-30 menit	Klasifikasi aktor, tujuan, vektor serangan, dan attack surface.
30-50 menit	Pembahasan kategori ancaman: phishing, malware, DoS/DDoS, MITM, insider, APT.
50-70 menit	Studi kasus terpandu: perubahan rekening vendor melalui surel palsu.
70-90 menit	Aktivitas kelompok: threat model fiktif dan kontrol berlapis.
90-100 menit	Rangkuman, tugas mingguan, dan pertanyaan pemahaman.

Alokasi waktu dapat disesuaikan dengan dinamika diskusi kelas.

Alur Konsep Threat Model



Prinsip pengarah

ATTACK SURFACE = entry points + identities + data paths + dependencies

Model ancaman menghubungkan niat dan akses dengan konsekuensi serta peluang deteksi.

Threat Actor vs Attack Vector

Threat actor

Pihak atau kondisi yang dapat menyebabkan kejadian merugikan, misalnya kriminal, pihak internal, pemasok, aktivis, atau kesalahan manusia.

- ▶ Motivasi: finansial, reputasi, ideologi, kelalaian
- ▶ Kapabilitas: sumber daya, akses, pengetahuan
- ▶ Target: data, layanan, identitas, proses bisnis

Attack vector

Jalur atau metode yang digunakan untuk mencapai tujuan, misalnya surel, kredensial, API, jaringan Wi-Fi, atau akses fisik.

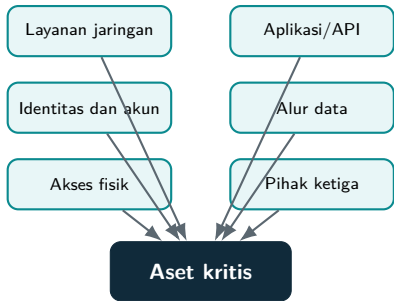
- ▶ Vektor bukan selalu celah teknis
- ▶ Satu aktor dapat memakai banyak vektor
- ▶ Satu vektor dapat dipakai oleh banyak aktor

Klasifikasi Ancaman yang Berguna

Dimensi	Pertanyaan analisis
Pelaku	Siapa atau kondisi apa yang dapat menyebabkan gangguan?
Motivasi	Apa tujuan atau insentif yang mendorong aksi?
Kapabilitas	Akses, alat, pengetahuan, dan sumber daya apa yang tersedia?
Target	Aset, layanan, data, identitas, atau proses apa yang disasar?
Pola waktu	Apakah aksinya oportunistik, berulang, tersembunyi, atau berjangka panjang?
Kendala	Hambatan apa yang membatasi aktor: kontrol, biaya, risiko tertangkap, atau waktu?

Catatan penting. Label seperti *APT* tidak otomatis menjelaskan teknik, dampak, atau prioritas risiko; analisis tetap harus spesifik terhadap aset dan konteks organisasi.

Menyusun Attack Surface



Pertanyaan kendali

- ▶ Entry point apa yang dapat menerima input?
- ▶ Identitas apa yang mempunyai hak akses?
- ▶ Jalur data mana yang melewati batas kepercayaan?
- ▶ Ketergantungan eksternal apa yang memengaruhi layanan?
- ▶ Siapa owner dan kontrol untuk setiap elemen?

Permukaan serangan yang besar tidak selalu tidak aman; masalah utamanya adalah elemen tanpa pemilik, kontrol, dan telemetry.

Phishing: Serangan pada Keputusan

Phishing memanfaatkan komunikasi dan keputusan pengguna untuk memperoleh kredensial, persetujuan, data, atau perubahan proses.

- ▶ Vektor: surel, pesan singkat, telepon, tautan, lampiran, halaman tiruan.
- ▶ Sinyal defensif: domain baru, login anomali, pola pengiriman tidak wajar.
- ▶ Dampak: akun diambil alih, pembayaran salah, data bocor, perluasan akses.

Analisis faktor manusia harus memperhatikan desain proses, tekanan waktu, dan kualitas sinyal, bukan hanya menyalahkan pengguna.

Kontrol berlapis

- ▶ MFA tahan phishing
- ▶ Verifikasi kanal terpisah
- ▶ Pembatasan perubahan sensitif
- ▶ Pelaporan yang mudah
- ▶ Edukasi berbasis skenario

Malware: Fungsi Berbahaya pada Endpoint dan Data

Malware adalah perangkat lunak atau kode yang menjalankan fungsi berbahaya, misalnya mencuri informasi, mengenkripsi data, melakukan persistensi, atau menjadi pintu masuk lanjutan.

- ▶ Sasaran: endpoint, file, kredensial, konfigurasi, data cadangan.
- ▶ Sinyal: proses tidak biasa, koneksi keluar anomali, perubahan file masif.
- ▶ Dampak: kebocoran data, gangguan operasi, pemulihan mahal.

Kontrol defensif

- ▶ Allowlisting aplikasi
- ▶ EDR atau anti-malware terkelola
- ▶ Segmentasi dan least privilege
- ▶ Backup yang diuji pemulihannya
- ▶ Patch dan hardening konfigurasi

DoS/DDoS dan MITM

DoS/DDoS

Serangan menguras kapasitas layanan sehingga availability terganggu.

- ▶ Sinyal: lonjakan trafik, error, saturasi CPU/memori/bandwidth
- ▶ Kontrol: rate limit, redundancy, upstream protection, capacity planning

MITM

Penyerang berada pada jalur komunikasi dan berpotensi memengaruhi kerahasiaan atau integritas data.

- ▶ Sinyal: sertifikat tidak valid, rute anomali, perubahan payload
- ▶ Kontrol: TLS yang benar, validasi sertifikat, VPN sesuai kebutuhan, monitoring

Pesan utama

Kedua kategori ini harus dianalisis melalui kebutuhan layanan: availability, confidentiality, integrity, dan batas toleransi gangguan.

Insider Threat dan APT

Insider threat

Ancaman yang memanfaatkan akses sah, pengetahuan internal, atau proses yang lemah.

- ▶ Tidak selalu berniat jahat; bisa kelalaian atau tekanan proses
- ▶ Sinyal: akses di luar tugas, perubahan masif, bypass prosedur
- ▶ Kontrol: least privilege, review akses, separation of duties

APT

Ancaman berkemampuan tinggi, persisten, dan berorientasi target.

- ▶ Bukan ukuran dampak dan bukan nama teknik tunggal
- ▶ Relevan bila ada tujuan, aset, dan pola operasi yang jelas
- ▶ Deteksi memerlukan telemetry lintas identitas, jaringan, endpoint, dan aplikasi

Faktor Manusia dan Desain Kontrol

Sumber kesalahan yang sering muncul

- ▶ Instruksi keamanan ambigu
- ▶ Beban kerja dan tekanan waktu
- ▶ Sinyal peringatan terlalu lemah atau terlalu sering
- ▶ Proses bisnis memaksa jalan pintas
- ▶ Kultur pelaporan yang menghukum pelapor

Desain kontrol yang baik

- ▶ Default aman
- ▶ Verifikasi ganda untuk tindakan sensitif
- ▶ Proses pelaporan mudah
- ▶ Pelatihan berbasis konteks kerja
- ▶ Akuntabilitas tanpa menyembunyikan akar masalah

Tujuan kontrol adalah mengurangi peluang kesalahan, meningkatkan deteksi, dan menurunkan dampak ketika kesalahan terjadi.

Threat-Informed Defense

Threat-informed defense menggunakan observasi taktik dan teknik dunia nyata untuk memperbaiki pertahanan.

- ▶ Gunakan istilah taktik dan teknik secara konsisten.
- ▶ Hubungkan teknik dengan aset, jalur ancaman, dan telemetry.
- ▶ Nilai deteksi dan mitigasi berdasarkan konteks organisasi.
- ▶ Jangan mengganti analisis risiko dengan checklist teknik.

Peran MITRE ATT&CK

MITRE ATT&CK dapat membantu pemetaan taktik, teknik, sumber telemetry, dan mitigasi. Namun, pemetaan tersebut tetap perlu diterjemahkan menjadi risiko, owner, prioritas, dan acceptance test.

Tabel Analisis dan Keputusan

Kategori	Contoh sasaran	Sinyal defensif	Kontrol utama
Phishing	Kredensial dan persetujuan	Domain baru, login anomali	MFA tahan phishing, verifikasi kanal
Malware	Endpoint dan data	Proses atau koneksi tidak biasa	Allowlisting, EDR, backup
DoS/DDoS	Kapasitas layanan	Lonjakan beban dan error	Rate limit, redundancy, upstream protection
Insider	Akses sah	Akses di luar tugas	Least privilege, review, separation of duties

Cara membaca tabel

Kategori ancaman harus diterjemahkan menjadi sasaran, sinyal, dan kontrol. Tanpa sinyal defensif, organisasi sulit membuktikan apakah kontrol bekerja.

Contoh Terpandu: Perubahan Rekening Vendor

Skenario

Sebuah akun staf menerima permintaan perubahan rekening melalui surel yang menyerupai pesan pimpinan.

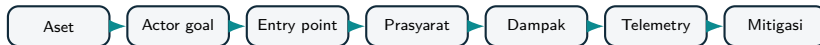
Attack surface

- ▶ Identitas pengirim dan penerima
- ▶ Proses persetujuan
- ▶ Antarmuka surel
- ▶ Data vendor
- ▶ Sistem pembayaran

Kontrol yang lebih kuat dari filter surel

- ▶ Verifikasi melalui kanal terpisah
- ▶ Dua pihak pemberi persetujuan
- ▶ Pembatasan nilai transaksi
- ▶ Alert perubahan rekening
- ▶ Log perubahan dan rekonsiliasi

Kerangka Analisis Skenario



Format ringkas risk statement

Karena [sebab/prasyarat], **aktor** dapat [aksi] melalui [vektor], sehingga [dampak] pada [aset/tujuan].

Tuliskan fakta, inferensi, asumsi, dan hal yang belum diketahui secara terpisah.

Aktivitas Kelompok: Threat Model Fiktif

Instruksi

Gunakan kartu skenario fiktif untuk membuat threat model tingkat tinggi. Petakan aset, actor goal, entry point, prasyarat, dampak, telemetry, dan mitigasi.

Produk diskusi

- ▶ Diagram attack surface sederhana
- ▶ Minimal dua risk statement
- ▶ Tiga kontrol berlapis
- ▶ Bukti efektivitas kontrol

Batas aktivitas

- ▶ Tidak membuat payload
- ▶ Tidak melakukan phishing nyata
- ▶ Tidak mengakses akun di luar laboratorium
- ▶ Tidak melakukan pemindaian sistem nyata

Bukti Minimum dan Etika Laboratorium

Bukti minimum

- ▶ Scope, otorisasi, topologi/setup, versi konfigurasi
- ▶ Raw log atau observasi dengan identifier dan timestamp
- ▶ Tabel yang memisahkan bukti, asumsi, dan interpretasi
- ▶ Hasil uji positif dan negatif terkait acceptance criterion
- ▶ Anomali, keterbatasan, rollback, dan residual risk

Keselamatan dan akses

Aktivitas keamanan hanya dilakukan pada sistem atau data laboratorium yang memiliki izin eksplisit. Gunakan metode non-destruktif, minimalkan data, hormati stop conditions, dan segera eskalasi dampak tidak terduga.

Tugas Mingguan

Tugas 2

Analisis satu insiden publik menggunakan sumber terpercaya. Pisahkan fakta, inferensi, dan hal yang belum diketahui; gambarkan attack surface; lalu usulkan tiga kontrol berlapis dan bukti efektivitasnya.

Struktur laporan yang disarankan

1. Ringkasan insiden dan sumber rujukan.
2. Aset, aktor, tujuan, vektor, aksi, dampak, dan telemetry.
3. Tabel fakta - inferensi - belum diketahui.
4. Attack surface dan tiga kontrol berlapis.
5. Bukti efektivitas, keterbatasan, residual risk, dan rekomendasi owner.

Pertanyaan Pemeriksaan Diri

1. Apa bedanya **threat actor** dan **attack vector**?
2. Mengapa **APT** bukan ukuran dampak?
3. Bagaimana faktor manusia memengaruhi desain kontrol?
4. Apa manfaat **telemetry** dalam threat model?
5. Mengapa pemetaan MITRE ATT&CK tidak sama dengan penilaian risiko?

Dua pertanyaan penutup untuk diskusi kelas

- ▶ Kontrol apa yang paling efektif bila phishing berhasil melewati filter surel?
- ▶ Telemetry apa yang perlu dikumpulkan agar insider threat dapat dideteksi tanpa melanggar prinsip minimisasi data?

Checklist Mutu Pengumpulan

- ▶ Istilah dan identifier digunakan secara konsisten.
- ▶ Batas sistem, tanggal, scope, dan otorisasi terlihat.
- ▶ Bukti mendukung klaim dan dapat ditelusuri.
- ▶ Rahasia serta data pribadi tidak dimasukkan tanpa kebutuhan.
- ▶ Keterbatasan, confidence, dan residual risk dinyatakan.
- ▶ Rekomendasi memiliki owner, prioritas, dan acceptance test.

Rangkuman satu kalimat

Analisis ancaman yang baik mengubah label serangan menjadi skenario yang terukur: aktor, tujuan, vektor, aksi, dampak, sinyal, kontrol, dan bukti.

Referensi dan Bacaan Lanjutan

1. Stallings, W. *Cryptography and Network Security: Principles and Practice*. Pearson.
2. Easttom, C. *Computer Security Fundamentals*. Pearson.
3. NIST. *Cybersecurity Framework (CSF) 2.0*. <https://www.nist.gov/cyberframework>
4. MITRE. *MITRE ATT&CK Knowledge Base*. <https://attack.mitre.org/>
5. OWASP. *OWASP Top 10:2025*. <https://owasp.org/Top10/2025/>

Catatan penggunaan referensi

Standar, threat intelligence, katalog kerentanan, dan dokumentasi alat dapat diperbarui. Catat judul, versi, tanggal akses, parameter, dan lingkungan yang digunakan.