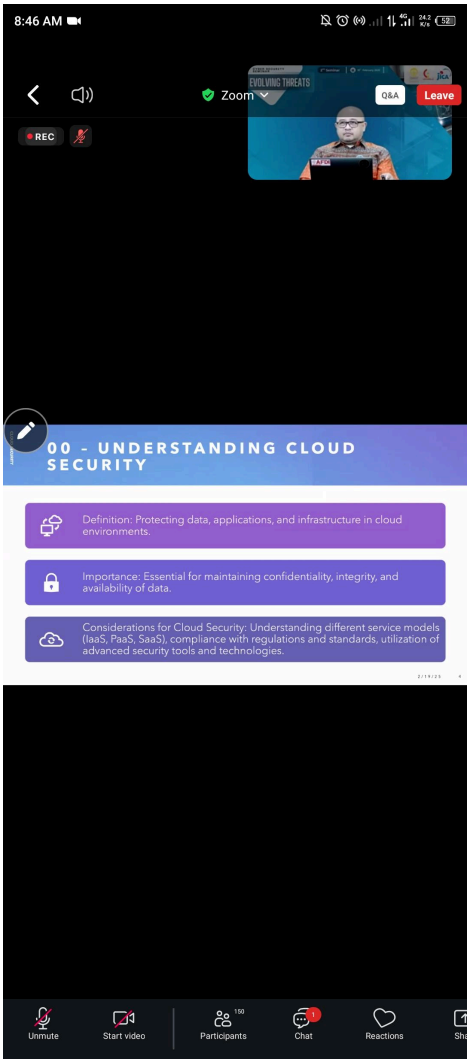
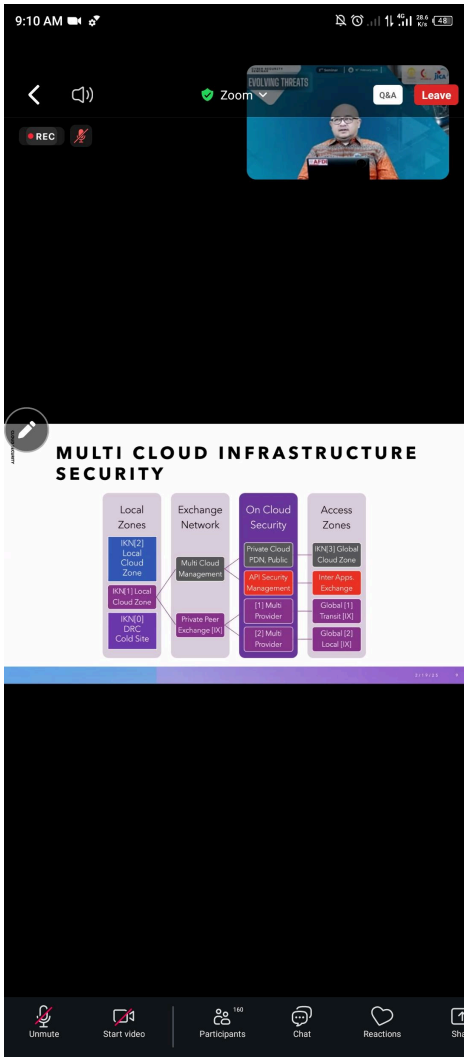
Ringkasan Materi Seminar/Webinar

Nama : Tomas Becket
NIM : 71230985

1. Cyber Security Seminar: Evolving Threats





Webinar ini diadakan pada tanggal 19 Februari 2025 Pukul 08.00-12.45.

A. Understanding Cloud Security

Definisi Cloud Security:
Menyediakan perlindungan untuk data, aplikasi, dan infrastruktur yang berada dalam lingkungan cloud.

Tujuan Utama Cloud Security:
Menjaga kerahasiaan (confidentiality), integritas, dan ketersediaan (availability) data serta layanan berbasis cloud.

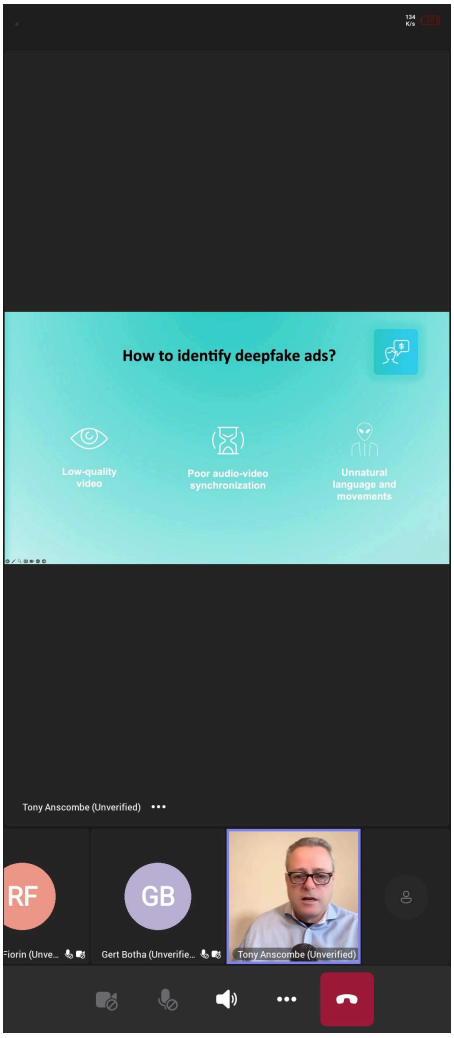
Konsep dan Prinsip Dasar:

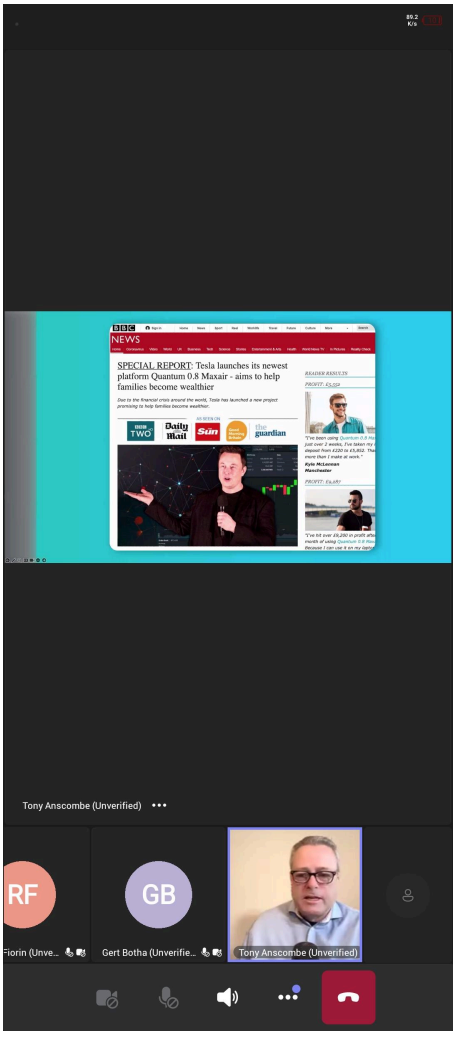
- Penting untuk memahami berbagai model layanan cloud (IaaS, PaaS, SaaS).
- Dibutuhkan pendekatan keamanan yang berbeda tergantung pada model layanan dan jenis cloud (public, private, hybrid).
- Keamanan cloud mencakup kebijakan, teknologi, dan kontrol untuk melindungi data dan infrastruktur.

B. Multi Cloud Infrastructure Security

- **Tantangan Multi Cloud**:
    - Setiap penyedia cloud memiliki sistem keamanan berbeda, sehingga organisasi perlu mengintegrasikan dan menstandarisasi kebijakan keamanan.
    - Perlunya monitoring, visibility, dan automation dalam mengelola keamanan di banyak platform cloud sekaligus.

2. H2 2024 THREAT Report webinar, Featuring ESET HQ's Chief Security Evangelist, Tony Anscombe





Webinar ini diadakan pada tanggal 19 Februari 2025 Pukul 15.00-16.00.

Topik Utama: Deepfake Ads dan Evolusi Ancaman Siber.

A. Cara Mengidentifikasi Iklan Deepfake

Ciri-Ciri Umum Iklan Deepfake:
- **Kualitas video rendah**: Gambar tampak kabur atau tidak halus.

- **Sinkronisasi audio dan video buruk**: Gerakan bibir tidak sesuai dengan suara.

- **Penggunaan bahasa yang tidak wajar**: Kalimat tidak alami, mengandung kesalahan tata bahasa atau terjemahan.

Tujuan Deepfake Ads:
- Biasanya digunakan untuk penipuan, phishing, atau kampanye disinformasi, memanfaatkan wajah tokoh publik untuk membangun kepercayaan palsu.

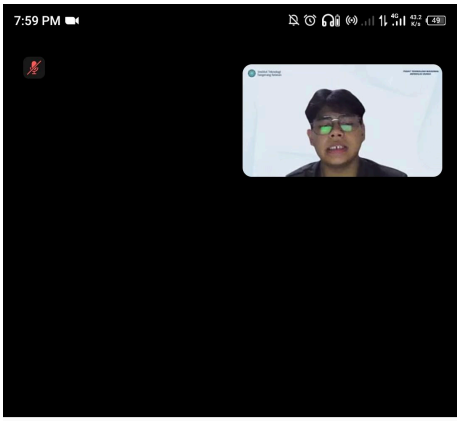
B. Contoh Kasus Nyata

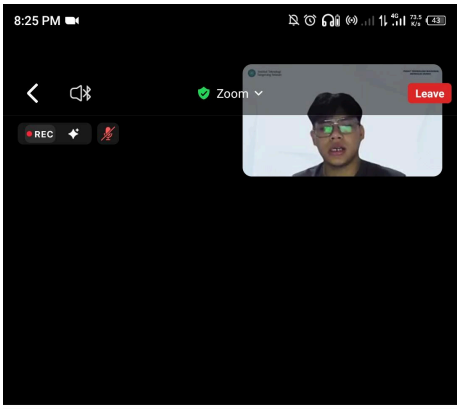
- Disorot berita terkait penipuan menggunakan video deepfake dari media populer, termasuk penyalahgunaan wajah tokoh terkenal untuk mempromosikan investasi palsu.

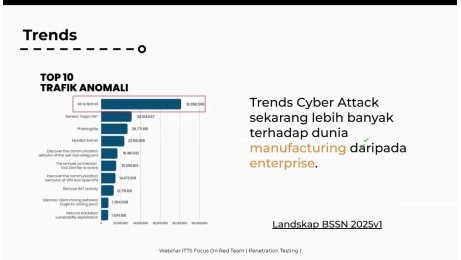
C. Implikasi dan Pencegahan

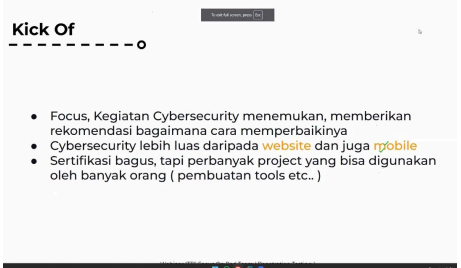
- Ancaman deepfake meningkat pesat dan mulai digunakan secara aktif oleh pelaku kejahatan siber.
- Edukasi masyarakat tentang cara mendeteksi konten palsu sangat penting.
- Disarankan untuk selalu verifikasi sumber konten, menggunakan alat pendeteksi deepfake, dan waspada terhadap video promosi yang tampak mencurigakan.

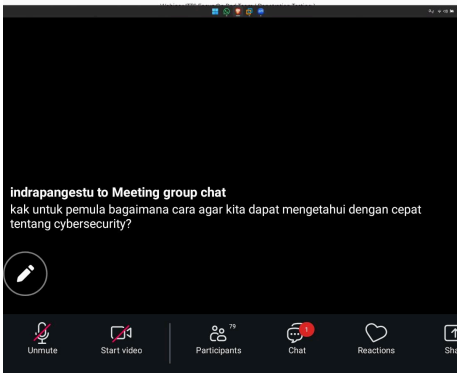
3. Webinar ITTS “Roadmap to Get Into Cyber Security Field: Red Team”











Webinar ini diadakan pada tanggal 23 Februari 2025 Pukul 19.30-20.30.

A. Kick Off

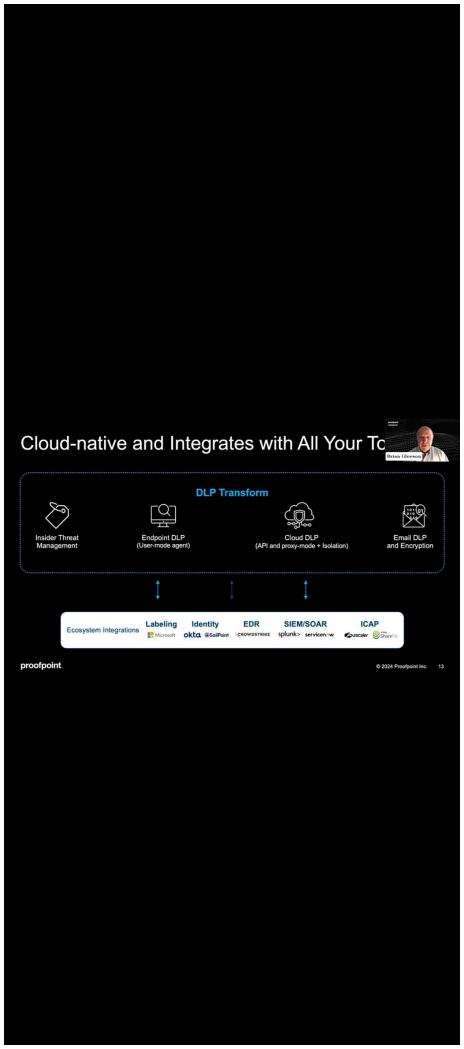
Fokus Utama Kegiatan ini: Kegiatan Cybersecurity difokuskan untuk menemukan, memberikan rekomendasi, dan memperbaiki celah keamanan dalam sistem.

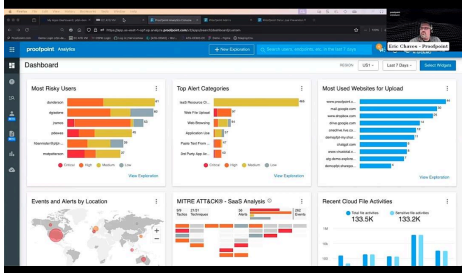
Area Cybersecurity: Cybersecurity tidak hanya terbatas pada website, tetapi juga mencakup aplikasi mobile.

B. Tren Serangan Siber (Cybersecurity Trends)

- **Statistik Top 10 Trafik Anomali**:
  Data menunjukkan jenis-jenis trafik anomali yang sering muncul, menjadi indikator jenis serangan yang sedang tren.
- **Target Serangan**:
  Saat ini, serangan siber lebih banyak menyasar dunia manufacturing dibandingkan dengan enterprise (perusahaan umum).

4. **Webinar Modern Data Loss Prevention**





Webinar ini diadakan pada tanggal 4 Maret 2025 Pukul 20.00-20.45.

A. Konsep Utama DLP (Data Loss Prevention)

DLP Modern bersifat Cloud-native:

- Dirancang untuk lingkungan cloud-first yang fleksibel dan dapat berintegrasi dengan berbagai alat serta platform.

- Cocok digunakan dalam ekosistem hybrid dan multi-cloud.

Transformasi DLP (DLP Transform):

- Klasifikasi Data secara otomatis untuk memahami jenis dan sensitivitas data.

- Identifikasi risiko berdasarkan perilaku pengguna dan pergerakan data.
- Pencegahan kehilangan data (Prevent data loss) melalui kontrol akses dan enkripsi.
- Monitoring dan analisis real-time untuk respons cepat terhadap potensi kebocoran data.

B. Dashboard dan Insight

- **Dashboard analitik menunjukkan:**
  - Kategori data paling berisiko (misalnya data keuangan, data pribadi, dll.)
  - Pengguna atau lokasi terbanyak yang terlibat dalam potensi kebocoran. Jenis aktivitas mencurigakan yang paling sering muncul (misalnya download masif, pengiriman via email eksternal, dll.)
- **Dashboard ini memungkinkan tim keamanan untuk:**
  - Mengambil keputusan berbasis data (data-driven decisions).
  - Memvisualisasikan tren insiden dan ancaman data secara lebih jelas dan cepat.