SILABUS MATA KULIAH

MATA KULIAH	Nama MK	: *Malware* dan *Cyber Threat Intelligence*
	Kode MK	: ET234713
	Kredit	: 3 SKS
	Semester	: 7

DESKRIPSI MATA KULIAH

Mata kuliah ini membahas mengenai *malware analysis* dan *threat intelligence*. Analisis *malware* adalah studi atau proses menentukan fungsionalitas, asal, dan potensi dampak dari sampel *malware* tertentu seperti *virus, worm, trojan horse, rootkit*, atau *backdoor*. Kelas ini juga membekali siswa dengan pengetahuan dalam menemukan, meneliti, dan menilai ancaman dan perdagangan musuh, penerapan praktis intelijen dalam berbagai fungsi dan inisiatif operasional, dan melakukan aktivitas peningkatan berkelanjutan pada proses, prosedur, metode, dan peralatan.

CAPAIAN PEMBELAJARAN LULUSAN YANG DIBEBANKAN MATA KULIAH

CPL-4 : Mampu mengimplementasikan, mengelola, dan mengamankan informasi yang didistribusikan melalui jaringan komputer untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi.

CAPAIAN PEMBELAJARAN MATA KULIAH

CPMK-1 : Mahasiswa mampu menjelaskan konsep dasar dan penelitian terkini mengenai *Malware*.

CPMK-2 : Mahasiswa mampu menjelaskan konsep dasar dan penelitian terkini mengenai *Adversarial Behavior*.

CPMK-3 : Mahasiswa mampu menjelaskan konsep dasar dan penelitian terkini mengenai *Threat Intelligence*.

POKOK BAHASAN

1. Detail Teknis dari Eksploitasi
2. Sistem Berbahaya yang Didistribusikan
3. Pendekatan Penemuan dan Analisis Terkait
4. Motivasi, Perilaku, dan Metode yang Digunakan Penyerang
5. Pengantar *Threat Intelligence*
6. Ancaman Dunia Maya dan Metodologi *Kill Chain*
7. Persyaratan, Perencanaan, Arahan, dan Tinjauan

8. Pengumpulan dan Pemrosesan Data
9. Analisis Data
10. Pelaporan Intelijen dan Diseminasi

PRASYARAT

-

PUSTAKA

- *Cyber Malware*, Apress 2024.
- *Malware Analysis Using Artificial Intelligence and Deep Learning*, Apress, 2020.
- *Malware Analysis and Detection Engineering*, Apress, 2020.
- CyBOK, The Cyber Security Body Of Knowledge *(https://www.cybok.org/) Malware & Attack Technologies: Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches*.
- EC Councils, CTIA *(https://www.eccouncil.org/programs/threat-intelligence-training/)*