SILABUS MATA KULIAH

MATA KULIAH	Nama MK	: Manajemen Insiden Keamanan Siber
	Kode MK	: ET234401
	Kredit	: 3 SKS
	Semester	: 4

DESKRIPSI MATA KULIAH

Mata kuliah ini membekali mahasiswa dengan pengetahuan, keterampilan, dan kemampuan untuk secara efektif mempersiapkan, menghadapi, dan memberantas ancaman dan pelaku ancaman dalam suatu insiden. Kelas ini menyediakan seluruh proses Penanganan dan Respons Insiden serta laboratorium praktik yang mengajarkan prosedur dan teknik taktis yang diperlukan untuk Merencanakan, Mencatat, Memprioritaskan, Memberi Tahu, dan Membendung secara efektif. Mahasiswa akan mempelajari penanganan berbagai jenis insiden, metodologi penilaian risiko, serta hukum dan kebijakan terkait penanganan insiden. Setelah mengikuti kuliah, mahasiswa akan dapat membuat kebijakan IH&R dan menangani berbagai jenis insiden keamanan seperti *malware*, keamanan email, keamanan jaringan, keamanan aplikasi web, keamanan *cloud*, dan insiden terkait ancaman orang dalam.

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 proses penanganan insiden dan respons.

CPMK-2 : Mahasiswa mampu menjelaskan kesiapan forensik dan respons pertama.

CPMK-3 : Mahasiswa mampu menjelaskan proses penanganan insiden *malware*.

CPMK-4 : Mahasiswa mampu menjelaskan proses penanganan insiden keamanan email.

CPMK-5 : Mahasiswa mampu menjelaskan proses penanganan insiden keamanan jaringan.

CPMK-6 : Mahasiswa mampu menjelaskan proses penanganan insiden keamanan aplikasi web.

CPMK-7	: Mahasiswa mampu menjelaskan proses penanganan insiden keamanan *cloud*.
CPMK-8	: Mahasiswa mampu menjelaskan proses penanganan ancaman orang dalam.

POKOK BAHASAN

1. Isu-Isu Utama Keamanan Informasi
2. Memerangi Ancaman Keamanan Siber
3. Manajemen Insiden
4. Manajemen Kerentanan dan Risiko
5. Praktik Terbaik dan Standar Keamanan Siber
6. Perencanaan Program Penanganan Insiden
7. Dasar-Dasar Forensik Komputer
8. Prosedur Respons Pertama
9. Teknik Anti-Forensik
10. Teknik Penanganan Insiden Secara Sistematis

PRASYARAT

-

PUSTAKA

- *Cybersecurity Incident Response*, Apress. 2018.
- CyBOK, The Cyber Security Body Of Knowledge *(https://www.cybok.org/) Security Operations & Incident Management: The configuration, operation and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence.*
- EC Councils, ECIH *(https://www.eccouncil.org/programs/ec-council-certified-incident-handler-ecih/)*