SILABUS MATA KULIAH

MATA KULIAH	Nama MK	: *Security Operations Center*
	Kode MK	: ET234402
	Kredit	: 3 SKS
	Semester	: 4

DESKRIPSI MATA KULIAH

Mata kuliah ini adalah langkah pertama untuk bergabung dengan pusat operasi keamanan (SOC). Hal ini dirancang untuk analis SOC Tingkat I dan Tingkat II saat ini dan yang bercita-cita tinggi untuk mencapai kemahiran dalam melakukan operasi tingkat pemula dan menengah. Program ini berfokus pada penciptaan peluang karir baru melalui pengetahuan yang luas dan teliti dengan kemampuan tingkat yang ditingkatkan untuk berkontribusi secara dinamis pada tim SOC. Ini secara menyeluruh mencakup dasar-dasar operasi SOC, sebelum menyampaikan pengetahuan tentang manajemen log dan korelasi, penerapan SIEM, deteksi insiden tingkat lanjut, dan respons insiden. Selain itu, siswa akan belajar mengelola berbagai proses SOC dan berkolaborasi dengan CSIRT pada saat dibutuhkan.

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 operasi dan manajemen keamanan.

CPMK-2 : Mahasiswa mampu menjelaskan ancaman *cyber*, IOC, dan metodologi serangan.

CPMK-3 : Mahasiswa mampu menjelaskan insiden, peristiwa, dan pencatatan.

CPMK-4 : Mahasiswa mampu menjelaskan deteksi insiden dengan *Security Information and Event Management (SIEM)*.

CPMK-5 : Mahasiswa mampu menjelaskan deteksi insiden yang disempurnakan dengan intelijen ancaman.

POKOK BAHASAN

1. Operasi dan Manajemen Keamanan
2. Ancaman Siber, IoC, dan Metodologi Serangan

3. Insiden, Peristiwa, dan Pencatatan
4. Deteksi Insiden dengan *Security Information and Event Management (SIEM)*
5. Peningkatan Deteksi Insiden dengan Intelijen Ancaman

PRASYARAT

-

PUSTAKA

- *Designing a HIPAA-Compliant Security Operations Center*, Apress, 2020.
- 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, CSA *(https://www.eccouncil.org/programs/certified-soc-analyst-csa/)*
- SKKNI *Security Operations Center*, Nomor 391 Tahun 2020 *(https://skkni.kemnaker.go.id/dokumen)*