



Sertifikat Microcredential

Bisnis Digital, Inovasi, dan Kewirausahaan
Nomor: 1967791850-166/MSD/BLSDM.2/DL.02/08/2024



Program: Digital Talent Scholarship, Microcredential – Startup Foundation
Mata Kuliah: Cybersecurity in Digital Business (April - Agustus 2024)
Pengajar: 1. Prof. Dr. Ir Ford Lumban Gaol, S.Si., M.Kom., SMIEEE
2. Ir. Setiadi Yazid, Ph.D.

Badan Pengembangan Sumber Daya Manusia, Kementerian Komunikasi dan Informatika, memberikan sertifikat kepada:

Nama: Mulkan Fadhli
Nomor Registrasi: 1967791850-166
Instansi: Universita Islam Negeri Ar-Raniry
Predikat/Nilai: Excellent (91,25/100)
Kehadiran: 93,75% (16 pertemuan)
Periode Perkuliahan: April s.d. Agustus 2024

Jakarta, 16 Agustus 2024

Ditetapkan oleh,
Kepala Puslitbang SDP3I, Badan Pengembangan Sumber Daya Manusia
Kementerian Komunikasi dan Informatika



Dr. Nusirwan, S.Ag, M.Si

LAMPIRAN: DETIL PERKULIAHAN

Keterangan Perkuliahan: *Online – Self-paced learning with instructor*

Kode	Kursus	Tujuan Pembelajaran	Capaian Pembelajaran	Jumlah SKS
M.108	<i>Cybersecurity in Digital Business</i>	Tujuan utama pembelajaran "Cybersecurity in Digital Business" adalah memberikan peserta pemahaman yang mendalam tentang tantangan dan strategi keamanan siber yang diperlukan dalam bisnis digital. Pertama, program ini bertujuan untuk membekali peserta dengan pemahaman menyeluruh tentang ancaman keamanan siber yang dapat memengaruhi bisnis digital. Peserta akan memahami jenis-jenis serangan, seperti serangan malware, phishing, Distributed Denial of Service (DDoS), dan lain-lain serta dampaknya terhadap operasional bisnis. Selanjutnya, tujuan Mata Kuliah ini adalah memberikan keterampilan praktis kepada peserta dalam mengimplementasikan langkah-langkah keamanan yang efektif. Peserta akan mempelajari praktik-praktik dalam pengelolaan kata sandi, perlindungan data pelanggan, dan pemantauan keamanan sistem. Dengan penguasaan keterampilan ini, peserta diharapkan dapat melindungi informasi sensitif, menjaga integritas sistem, dan memberikan keamanan yang diperlukan untuk menjalankan bisnis digital secara aman. Terakhir, Mata Kuliah ini bertujuan untuk membimbing peserta dalam memahami peran kebijakan keamanan dan kepatuhan. Peserta akan belajar merancang dan	1. Pemahaman Mendalam tentang Ancaman Keamanan Siber: Peserta dapat mengidentifikasi dan memahami berbagai jenis ancaman keamanan siber yang dapat mempengaruhi bisnis digital. Peserta mengenali serangan malware, phishing, DDoS, dan lain-lain serta memahami dampaknya terhadap operasional bisnis. Capaian ini menciptakan dasar pemahaman yang kokoh tentang lingkungan keamanan siber yang dinamis dan berubah-ubah. 2. Penerapan Praktik Keamanan Siber yang Efektif: Peserta menguasai keterampilan praktis dalam menerapkan langkah-langkah keamanan yang efektif dalam konteks bisnis digital. Peserta memahami tentang pengelolaan kata sandi yang aman, perlindungan data pelanggan, dan pemantauan keamanan sistem. Capaian ini menunjukkan kemampuan peserta untuk melibatkan praktik keamanan siber yang dapat melindungi informasi sensitif, mencegah serangan, dan menjaga integritas sistem. 3. Pengembangan Kebijakan Keamanan Siber yang Efektif: Peserta mampu merancang, mengimplementasikan, dan mempertahankan kebijakan keamanan yang efektif untuk bisnis digital mereka. Peserta memahami peran penting kebijakan keamanan dalam melindungi data dan sistem serta mematuhi standar kepatuhan yang berlaku. Capaian ini menciptakan kemampuan peserta untuk mengelola risiko keamanan siber melalui pengembangan kebijakan yang sesuai dengan konteks bisnis mereka. 4. Kemampuan Menanggapi dan Mengatasi Serangan Siber: Peserta memahami teknik dan prosedur tanggapan terhadap insiden keamanan siber. Peserta mampu merancang dan	3

Kode	Kursus	Tujuan Pembelajaran	Capaian Pembelajaran	Jumlah SKS
		mengimplementasikan kebijakan keamanan yang efektif sesuai dengan standar kepatuhan industri dan regulasi yang berlaku. Dengan demikian, peserta akan dapat menjalankan bisnis digital mereka dengan keamanan yang tinggi dan membangun kepercayaan pelanggan terkait perlindungan data.	melaksanakan tanggapan terhadap insiden, mengidentifikasi serangan dengan cepat, dan mengambil tindakan yang diperlukan untuk meminimalisasi dampak serangan. Capaian ini menunjukkan kesiapan peserta dalam menanggapi ancaman keamanan siber pada bisnis mereka secara efisien dan efektif. 5. Peningkatan Kesadaran Keamanan Siber: Peserta dapat meningkatkan kesadaran keamanan siber, khususnya pada bisnis digital mereka. Peserta memahami tentang pentingnya keterlibatan semua pemangku kepentingan dalam menjaga keamanan siber, termasuk karyawan, mitra, dan pelanggan. Capaian ini menciptakan budaya keamanan yang kuat di seluruh organisasi/kelompok, memastikan bahwa semua individu terlibat dalam menjaga keamanan bisnis digital dan melaporkan potensi ancaman dengan cepat.	

digitalent

Perkuliahan

Minggu	Topik	Deskripsi	Metode Pembelajaran
1	Pengantar Kemanan Siber	- Apa itu keamanan siber dan jenis keamanan siber - Sejarah Keamanan Siber, Perkembangan dan Penerapannya - Standar dan sertifikasi yang berlaku untuk keamanan siber	Pembelajaran Daring/luring, Pendampingan, dan Quiz
2	Prinsip Konsep Keamanan Siber	- Prinsip Keamanan Siber - Ancaman eksternal dan internal - Arsitektur keamanan siber - Kerangka Keamanan Siber	Pembelajaran Daring/luring, Pendampingan, dan Quiz
3	Manajemen Sistem Informasi Keamanan Siber	- Konsep keamanan siber - Kontrol akses - Manajemen sistem informasi keamanan siber	Pembelajaran Daring/luring, Pendampingan, dan Quiz
4	Keamanan Siber pada Sosial Media	- Sejarah keamanan siber pada sosial media - Jenis-jenis keamanan siber pada sosial media - Perkembangan keamanan siber pada sosial media	Pembelajaran Daring/luring, Pendampingan, dan Quiz
5	Rekayasa Sosial	- Konsep rekayasa sosial - implementasi dan contoh kasus rekayasa sosial	Pembelajaran Daring/luring, Pendampingan, dan Quiz
6	Perangkat Lunak Berbahaya	- Sejarah malware dan spyware - Perangkat lunak Mallware dan Jenisnya - Perangkat lunak Spyware dan Jenisnya	Pembelajaran Daring/luring, Pendampingan, dan Quiz
7	Perangkat Lunak Anti Virus	- Sejarah dan perkembangan perangkat lunak Anti virus - Jenis Perangkat lunak anti-virus	Pembelajaran Daring/luring, Pendampingan, dan Quiz
8	Mid Test	Mid Test	Multiple Choice
9	Otentikasi Kata Sandi	- Otentikasi multi-faktor dan berbasis kata sandi - Kemajuan keamanan kata sandi - Jenis Otentikasi kata sandi	Pembelajaran Daring/luring, Pendampingan, dan Quiz
10	Keamanan Jaringan internet	- Jaringan, protokol dan komunikasi komputer - Kerentanan dan ancaman jaringan	Pembelajaran Daring/luring, Pendampingan, dan Quiz

Minggu	Topik	Deskripsi	Metode Pembelajaran
11	Pengelolaan Risiko Keamanan Siber dalam Bisnis Digital	- Identifikasi dan Evaluasi Risiko keamanan siber yang spesifik untuk bisnis digital - Strategi Mitigasi Risiko - Manajemen Risiko Berkelanjutan	Pembelajaran Daring/luring, Pendampingan, dan Quiz
12	Perlindungan Data Pelanggan dan Kepatuhan Regulasi	- Prinsip-prinsip Perlindungan Data Pelanggan - Kepatuhan Regulasi sebagai pemilik bisnis digital	Pembelajaran Daring/luring, Pendampingan, dan Quiz
13	Kesiapan Bisnis Terhadap Serangan Siber	- Pengenalan Serangan Siber yang mungkin dihadapi dalam bisnis digital - Respons terhadap serangan siber pada bisnis	Pembelajaran Daring/luring, Pendampingan, dan Quiz
14	Implementasi Teknologi Keamanan Terbaru	- Penggunaan layanan cloud dalam bisnis digital - Sekilas AI dapat digunakan untuk mendeteksi dan mencegah serangan siber dalam konteks bisnis digital	Pembelajaran Daring/luring, Pendampingan, dan Quiz
15	Budaya Keamanan dan Kesadaran Pengguna	Bagaimana membangun pendidikan dan budaya kesadaran keamanan siber di antara owner, karyawan, dan pemangku kepentingan lainnya dalam bisnis digital	Pembelajaran Daring/luring, Pendampingan, dan Quiz
16	Final Test	Post-Test/Capstone Project/Sertifikasi	Multiple Choice & Essay/Presentasi/Laporan Proyek

digitalent

Nilai

No	Ujian	Nilai
1	Mid-Tes	87
2	Final-Tes	89,5

Tugas/Proyek

No	Tugas/Proyek	Deskripsi	Nilai
1	Week 2	Menganalisa Strategi Keamanan Cyber yang Efektif dari beberapa studi kasus	Mengerjakan
2	Week 6	Mendefinisikan dan membuat contoh tentang virus Trapdoors, Logic Bomb, Trojan Horse, Virus, Worm, dan Zombie	Mengerjakan
3	Week 7	Membuat Analisa dari Studi Kasus tentang bagaimana suatu individu/grup melakukan Cyber Crime	Mengerjakan
4	Week 10	Mengidentifikasi Studi Kasus tentang Network Security	Mengerjakan
5	Week 12	Menjelaskan dan membuat kesimpulan dari beberapa studi kasus tentang proteksi data	Mengerjakan
6	Week 14	Menjelaskan Masalah yang terjadi, Mitigasi dan Solusi dari Kasus yang menyoroti pentingnya keamanan cloud	Mengerjakan

Sertifikasi Pendamping

- N/A

digitalent

Pertemuan

Minggu ke-	Kehadiran
1	Hadir
2	Hadir
3	Hadir
4	Hadir
5	Hadir
6	Hadir
7	Hadir
8	Mid-Test: Hadir
9	Hadir
10	Tidak Hadir
11	Hadir
12	Hadir
13	Hadir
14	Hadir
15	Hadir
16	Final Test: Hadir

Rubrik:

Mid_Test*35%+Final_Test*40%+Kehadiran(10%)+Tugas(15%)

Excellent (E)	:	- Nilai akhir lebih dari 90. - Dapat dikonversi untuk 3.51 – 4.00. - Peserta dianggap mencapai pemahaman konsep yang sangat baik, memiliki keterampilan yang sangat baik, dan mampu menerapkan pengetahuan tersebut secara kreatif dan efektif.
Good (G)	:	- Nilai akhir antara 81 - 90. - Dapat dikonversi untuk 3.01 – 3.50. - Peserta dianggap memiliki pencapaian yang baik, memiliki pemahaman konsep yang baik, keterampilan yang baik, dan mampu menerapkan pengetahuan dengan baik dalam konteks yang diberikan.
Satisfactory (S)	:	- Nilai akhir antara 71 - 80. - Dapat dikonversi untuk 2.75 – 3.00. - Peserta dianggap memiliki tingkat pencapaian yang memadai, mencapai pemahaman dasar tentang konsep-konsep yang diajarkan, meskipun mungkin masih memerlukan pengembangan lebih lanjut.
Poor (P)	:	- Nilai akhir antara 61 - 70. - Dapat dikonversi untuk 2.50 – 2.74. - Peserta dianggap memiliki tingkat kinerja yang kurang memuaskan. Peserta mungkin mengalami kesulitan dalam memahami materi atau menerapkan keterampilan yang dibutuhkan, dan perlu melakukan perbaikan.
Failed (F)	:	- Nilai akhir di bawah 60. - Peserta tidak memenuhi standar yang ditetapkan.

Pengecekan Sertifikat:

1. Akses <https://digitalent.kominfo.go.id/cek-sertifikat>
2. Cek keaslian sertifikat dengan menggunakan **nomor registrasi** pelatihan yang tertera di sertifikat atau yang di kotak merah.



3. Klik “VALIDASI SERTIFIKAT”

Validasi e-Sertifikat Kelulusan

Silahkan periksa validitas e-sertifikat (hanya berlaku untuk e-sertifikat yang terbit mulai tahun 2023)

☐ I'm not a robot 
reCAPTCHA
Privacy - Terms

VALIDASI SERTIFIKAT



digitalent