DIGITAL TALENT SCHOLARSHIP

fga fresh graduate academy

Tidak untuk disebarluaskan
selain di website resmi DTS 2019

Update : 16 April 2019
Version : 2.0

SILABUS

cybersecurity

SILABUS CYBER SECURITY
DIGITAL TALENT SCHOLARSHIP 2019

INFORMASI UMUM	
Tema Pelatihan	Cybersecurity
Target Peserta	1000 peserta
Jumlah Jam Pelajaran	144 JP (1 JP=50 menit)
Jumlah JP/hari	4 JP/hari
Jumlah Pertemuan	36 hari
Pelaksanaan	1 Juli – 31 Agustus 2019
Lokasi Penyelenggaraan	1. Universitas Gadjah Mada 2. Universitas Indonesia – Fasilkom 3. Universitas Indonesia – FT 4. Institut Teknologi Bandung 5. Institut Teknologi Sepuluh Nopember 6. Universitas Udayana 7. Universitas Sriwijaya 8. Universitas Sumatera Utara 9. Universitas Sam Ratulangi 10. Universitas Diponegoro 11. Universitas Brawijaya (Terbuka untuk Tuna Rungu dan Tuna Daksa) 12. Universitas Syiah Kuala 13. Universitas Sebelas Maret (Terbuka untuk Tuna Netra)
Jenis Sertifikasi	Certificate of Completion dan *Congratulation Letter*: 1. CCNA Cybersecurity Operation (dengan *passing grade* 75%) 2. Certificate of Completion CCNA Security (dengan *passing grade* 75%) Industrial Certification: 1. CCNA Cybersecurity Operations (Cyber Ops) 2. CCNA Security
Persyaratan Peserta	• Warga Negara Indonesia • Usia Maksimal 29 Tahun pada saat mendaftar • Lulus Pendidikan Tingkat D3, D4, atau Strata-1 dalam bidang TIK dan MIPA, atau yang terkait • Belum/Tidak Memiliki Pekerjaan Tetap • Lolos Seleksi Administrasi dan Tes Substansi • Terbuka bagi penyandang disabilitas • Membawa laptop dengan spesifikasi sesuai yang ditentukan selama masa pelatihan
Persyaratan Sarana yang Harus Dimiliki Peserta	Laptop dengan spesifikasi: 1. RAM minimal 4 GB (Rekomendasi 8 GB) 2. Laptop dengan *Operating System* Windows 7,8,10, Linux, atau MAC OSX 3. Laptop dengan konektivitas WiFi 4. Oracle Virtual Box

INFORMASI UMUM	
Kriteria Pengajar	TRAINING INSTRUKTUR Kriteria menjadi Instruktur 1. Pastikan bahwa peserta yang didaftarkan dalam training instruktur WAJIB hadir dalam sesi training offline (luring). Tanggal training offline adalah 12 13 14 april 2019 (tentatif). 2. Email peserta yang akan didaftarkan dalam training HARUS memiliki peran (role) sebagai instruktur dalam sistem NETACAD. Silahkan menghubungi Academy Contact Manager di masing-masing Cisco Academy (CA). Mohon proses ini dilakukan sebelum memberikan email dan nama lengkap. 3. Peserta WAJIB mengambil dan lulus kursus Academy Orientation dalam NETACAD, bagi peserta yang baru saja memiliki account instruktur dalam sistem NETACAD. 4. Memenuhi kriteria kelulusan Training Instruktur Proses Training Instruktur 1. Peserta wajib mengerjakan semua chapter exam secara online (daring) sebelum pertemuan di Jogja (13 chapter untuk CCNA Cyber Ops dan 11 chapter untuk CCNA Security). 2. Pada sesi training offline akan dilakukan tutorial beberapa lab yang penting, final exam, skill based assessment dan diskusi. 3. Terdapat dua kelas sekaligus dan ID kelas adalah sebagai berikut: CCNA Security : ITC-Security-004 CCNA Cyber Ops : ITC-CYBEROPS-005 Persyaratan Lulus Training Instruktur Mendapatkan nilai minimal 80 untuk semua chapter exam, final exam dan skill based assessment.

DESKRIPSI PELATIHAN
Pelatihan ini meliputi 2 materi utama yaitu CCNA Cyber Ops dan CCNA Security. **CCNA Cybersecurity Operations (Cyber Ops)** Materi pelatihan CCNA Cyber Ops bertujuan untuk mengajarkan kemampuan mengamankan jaringan komputer yang sangat berguna untuk mendeteksi dan merespon ancaman keamanan siber. Materi ini juga menyiapkan peserta untuk memulai karir pekerjaan sebagai analis keamanan siber (*associate level*) dalam *Security Operations Center (SOC)*. Sertifikasi Cisco CCNA Cyber Ops telah diakui oleh Departemen Keamanan Amerika Serikat (DoD 8570.01-M) dalam kategori *CSSP Analyst* dan *CCSP Incident Responder*.

CCNA Security

Materi pelatihan CCNA Security menekan pada teknologi utama keamanan yang terdiri dari instalasi, troubleshooting dan memonitor perangkat jaringan untuk menjaga *integrity, confidentiality* dan *availability* data dan perangkat.

Sertifikasi Cisco CCNA Security telah diakui oleh Departemen Keamanan Amerika Serikat (DoD 8570.01-M) dan memenuhi standarisasi ISO 17024.

TUJUAN PELATIHAN	
Setelah mengikuti pelatihan ini, peserta diharapkan mampu untuk:	
1	**CCNA Cyber Ops** a. menjelaskan peran *Cybersecurity Operations Analyst.* b. menjelaskan fitur Sistem Operasi yang dibutuhkan untuk mendukung analisis keamanan siber. c. menjelaskan pengoperasian infrastruktur jaringan dan mengklasifikasikan berbagai serangan jaringan. d. menganalisis operasi dari layanan jaringan, protokol jaringan dan menggunakan perangkat monitoring untuk mengidentifikasikan serangan. e. menggunakan berbagai metode untuk menjaga akses berbahaya baik untuk komputer maupun data. f. menjelaskan pengaruh kriptografi pada monitoring keamanan jaringan. g. menjelaskan cara untuk menginvestigasi dan mengevaluasi kerentanan *endpoints* dan peringatan keamanan jaringan. h. menggunakan *virtual machines* (VM) untuk implementasi, evaluasi, dan analisis kejadian ancaman *cybersecurity*. i. menganalisis data intrusi jaringan untuk identifikasi komputer yang diretas dan kerentanannya. j. menerapkan *incident response model (CSIRSTs* dan *NIST)* untuk mengatur insiden keamanan.
2	**CCNA Security** a. mendeskripsikan ancaman keamanan yang dihadapi pada infrastruktur jaringan modern. b. mengamankan router dan switch Cisco. c. mendeskripsikan fungsionalitas AAA (*Authentication, Authorization and Accounting*) dan implementasi AAA pada router Cisco dengan router *database* lokal dan ACS berbasis server atau ISE. d. mencegah ancaman di jaringan menggunakan ACL dan *stateful* Firewall. e. mengimplementasikan IPS (*Intrusion Prevention System)* dan IDS (*Intrusion Detection System)* untuk mengamankan jaringan dari berbagai macam serangan yang terus berkembang. f. melakukan mitigasi ancaman pada email, serangan berbasis web dan serangan pada *endpoints* serta serangan umum pada Layer 2. g. mengamankan jalur komunikasi untuk menjamin aspek *integrity, authenticity,* dan *confidentiality*. h. mendeskripsikan tujuan VPN dan mengimplementasikan VPN *Remote Access* dan *Site-to-site.* i. mengamankan jaringan dengan menggunakan Cisco ASA (*Adaptive Security Appliance*).

PERATURAN KELAS	
Peserta pelatihan **WAJIB** menaati peraturan di bawah ini:	
1	Hadir tepat waktu selama perkuliahan.
2	Mengikuti 144 JP (Jam Perkuliahan) di lokasi yang telah dipilih oleh peserta.
3	Tidak menggunakan gawai selama mengikuti perkuliahan, kecuali bila dianjurkan atau diperintahkan oleh pengajar.
4	Membawa sarana pelatihan yang diwajibkan.
5	Mematuhi peraturan tempat perkuliahan termasuk cara berpakaian dan menjaga sarana prasarana.
6	Mematuhi peraturan dan ketentuan sebagai peserta DTS 2019.
7	Mengerjakan semua tugas dan ujian yang diberikan dengan penuh tanggung jawab dan jujur.

KOMPOSISI KURIKULUM		
No	**Metode**	**Catatan**
1	34 Pertemuan tatap muka (@4JP)	Pemaparan materi, diskusi interaktif, *hands-on lab* terkait dengan materi.
2	Ujian Chapter	Ujian Chapter (passing grade 75%): a. CCNA Cyber Ops - 13 chapter b. CCNA Security - 11 Chapter Ujian chapter dilakukan di luar kelas secara daring menggunakan sistem NETACAD.COM
3	Mid Test evaluation	Final Exam dan Skill-based Exam CCNA Cyber Ops (passing grade 75%)
4	Final Test evaluation	Final Exam dan Skill-based Exam CCNA Security (passing grade 75%)
5	Monitoring dan Evaluasi	*Course Analytic* dalam NETACAD.COM
5	Sertifikasi	Certificate of Completion: 1. CCNA Cyber Ops 2. CCNA Security Industrial Certification 1. CCNA Cyber Ops 2. CCNA Security **Industrial Certification* diambil melalui *Pearson Vue Testing Center*, lokasi terdekat bisa dilihat melalui laman https://home.pearsonvue.com/

RENCANA PERKULIAHAN				
No	**Pertemuan**	**Topik**	**Aktivitas Kelas**	**Durasi**
1.	Pertemuan Ke 1	● Pembukaan ● Penjelasan Rencana Pembelajaran ● Pengenalan Sistem NETACAD ● Pengenalan simulator Packet Tracer ● CCNA Cyber Ops - Chapter 0:	Pemaparan materi, diskusi dan *hands-on lab*	4JP

RENCANA PERKULIAHAN				
No	**Pertemuan**	**Topik**	**Aktivitas Kelas**	**Durasi**
		Welcome to CCNA Cybersecurity Operations ● CCNA Cyber Ops - Chapter 1: Cybersecurity and the Security Operations Center		
2.	Pertemuan Ke 2	CCNA Cyber Ops - Chapter 2: Windows Operating System	Pemaparan materi, diskusi dan *hands-on lab*	4JP
3.	Pertemuan Ke 3	CCNA Cyber Ops - Chapter 3: Linux Operating System	Pemaparan materi, diskusi dan *hands-on lab*	4JP
4.	Pertemuan Ke 4	CCNA Cyber Ops - Chapter 4: Network Protocols and Services (1)	Pemaparan materi, diskusi dan *hands-on lab*	4JP
5.	Pertemuan Ke 5	CCNA Cyber Ops - Chapter 4: Network Protocols and Services (2)	Pemaparan materi, diskusi dan *hands-on lab*	4JP
6.	Pertemuan Ke 6	CCNA Cyber Ops - Chapter 5: Network Infrastructure	Pemaparan materi, diskusi dan *hands-on lab*	4JP
7.	Pertemuan Ke 7	CCNA Cyber Ops - Chapter 6: Principles of Network Security	Pemaparan materi, diskusi dan *hands-on lab*	4JP
8.	Pertemuan Ke 8	CCNA Cyber Ops - Chapter 7: Network Attacks: A Deeper Look	Pemaparan materi, diskusi dan *hands-on lab*	4JP
9.	Pertemuan Ke 9	CCNA Cyber Ops - Chapter 8: Protecting the Network	Pemaparan materi, diskusi dan *hands-on lab*	4JP
10.	Pertemuan Ke 10	CCNA Cyber Ops - Chapter 9: Cryptography and the Public Key Infrastructure	Pemaparan materi, diskusi dan *hands-on lab*	4JP
11.	Pertemuan Ke 11	CCNA Cyber Ops - Chapter 10: Endpoint Security and Analysis	Pemaparan materi, diskusi dan *hands-on lab*	4JP
12.	Pertemuan Ke 12	CCNA Cyber Ops - Chapter 11: Security Monitoring	Pemaparan materi, diskusi dan *hands-on lab*	4JP
13.	Pertemuan Ke 13	CCNA Cyber Ops - Chapter 12: Intrusion Data Analysis (1)	Pemaparan materi, diskusi dan *hands-on lab*	4JP
14.	Pertemuan Ke 14	CCNA Cyber Ops - Chapter 12: Intrusion Data Analysis (2)	Pemaparan materi, diskusi dan *hands-on lab*	4JP
15.	Pertemuan Ke 15	CCNA Cyber Ops - Chapter 13: Incident Response and Handling	Pemaparan materi, diskusi dan *hands-on lab*	4JP
16.	Pertemuan Ke 16	Review CCNA Cyber Ops	Pemaparan materi,	4JP

RENCANA PERKULIAHAN				
No	**Pertemuan**	**Topik**	**Aktivitas Kelas**	**Durasi**
			diskusi dan *hands-on lab*	
17.	Pertemuan Ke 17	UTS: CCNA Cyber Ops Final Exam	Ujian daring melalui sistem NETACAD	4JP
18.	Pertemuan Ke 18	UTS: CCNA Cyber Ops Skill Based Assessment	Ujian Praktek melalui sistem NETACAD	4JP
19.	Pertemuan Ke 19	Evaluation CCNA Cyber Ops	Pemaparan materi dan diskusi interaktif	4JP
20.	Pertemuan Ke 20	CCNA Security – Chapter 1: Modern Network Security Threats	Pemaparan materi, diskusi dan *hands-on lab*	4JP
21.	Pertemuan Ke 21	CCNA Security – Chapter 2: Securing Network Devices	Pemaparan materi, diskusi dan *hands-on lab*	4JP
22.	Pertemuan Ke 22	CCNA Security – Chapter 3: Authentication, Authorization, and Accounting	Pemaparan materi, diskusi dan *hands-on lab*	4JP
23.	Pertemuan Ke 23	CCNA Security – Chapter 4:Implementing Firewall Technologies (1)	Pemaparan materi, diskusi dan *hands-on lab*	4JP
24.	Pertemuan Ke 24	CCNA Security – Chapter 4:Implementing Firewall Technologies (2)	Pemaparan materi, diskusi dan *hands-on lab*	4JP
25.	Pertemuan Ke 25	CCNA Security – Chapter 5:Implementing Intrusion Prevention	Pemaparan materi, diskusi dan *hands-on lab*	4JP
26.	Pertemuan Ke 26	CCNA Security – Chapter 6:Securing the Local Area Network (1)	Pemaparan materi, diskusi dan *hands-on lab*	4JP
27.	Pertemuan Ke 27	CCNA Security – Chapter 6:Securing the Local Area Network (2)	Pemaparan materi, diskusi dan *hands-on lab*	4JP
28.	Pertemuan Ke 28	CCNA Security – Chapter 7: Cryptographic Systems	Pemaparan materi, diskusi dan *hands-on lab*	4JP
29.	Pertemuan Ke 29	CCNA Security – Chapter 8: Implementing Virtual Private Networks	Pemaparan materi, diskusi dan *hands-on lab*	4JP
30.	Pertemuan Ke 30	CCNA Security – Chapter 9: Implementing the Cisco Adaptive Security Appliance	Pemaparan materi, diskusi dan *hands-on lab*	4JP
31.	Pertemuan Ke 31	CCNA Security – Chapter 10: Advanced Cisco Adaptive Security Appliance	Pemaparan materi, diskusi dan *hands-on lab*	4JP

RENCANA PERKULIAHAN				
No	**Pertemuan**	**Topik**	**Aktivitas Kelas**	**Durasi**
32.	Pertemuan Ke 32	CCNA Security – Chapter 11: Managing a Secure Network	Pemaparan materi, diskusi dan *hands-on lab*	4JP
33.	Pertemuan Ke 33	Review CCNA Security	Pemaparan materi, diskusi dan *hands-on lab*	4JP
34.	Pertemuan Ke 34	UAS: CCNA Security Final Exam	Ujian daring melalui sistem NETACAD	4JP
35.	Pertemuan Ke 35	UAS: CCNA Security Skill Based Assessment	Ujian Praktek melalui sistem NETACAD	4JP
36.	Pertemuan Ke 36	**Evaluation CCNA Security**	Diskusi interaktif, *hands-on lab,* dan latihan kuis	4JP