SCM · Batch 6

[SCM] Security Monitoring dengan WAZUH

13 · 27 Nov 2025 – 30 Nov 2025

Ringkasan Eksekutif

Nama Program	[SCM] Security Monitoring dengan WAZUH
Kode Program	SCM · Batch 6
Durasi	13
Tanggal Pelaksanaan	27 Nov 2025 – 30 Nov 2025
Mentor	Anggrahito, (CEH, ECSA, CHFI) MBA.
Bahasa	Bahasa Indonesia
Sertifikat	e-Certificate Taalenta (sesuai paket)

Kenapa Wajib Ikut

1. Menguasai Monitoring Keamanan

Belajar menguasai alat seperti Wazuh akan membuat Anda ahli dalam memonitoring keamanan sistem secara efektif. Bayangkan menjadi orang yang bisa mendeteksi ancaman siber sebelum mereka merusak sistem Anda.

2. Tingkatkan Kompetensi di Dunia IT

Dengan pengetahuan mendalam tentang SIEM dan Wazuh, Anda akan menjadi profesional IT yang diburu oleh banyak perusahaan. Keterampilan ini sangat dibutuhkan di era digital sekarang.

3. Lindungi Data Berharga Anda

Memahami dan mengimplementasikan konfigurasi Wazuh dapat membantu Anda melindungi data sensitif dari ancaman keamanan. Anda akan bisa tidur nyenyak tanpa khawatir data Anda bocor.

4. Siapkan Lingkungan Kerja yang Aman

Kelas ini mengajarkan Anda cara mengintegrasikan berbagai alat dan sistem untuk menciptakan lingkungan kerja yang aman dan terlindungi dari serangan siber.

Outline Materi

1. Pengenalan SIEM dan Wazuh

- Definisi dan fungsi SIEM: Keamanan siber, log collection, dan alerting.
- Pengenalan Wazuh: Komponen dan arsitektur.
- Persiapan Development: Instalasi Wazuh dan konfigurasi dashboard.

2. Log Analysis

- Pengantar Command Line Linux: Mengelola file, direktori, dan pemantauan sistem.
- Analisis Log Linux: Menggunakan command dan script bash.
- Wireshark Log Analysis: Analisis paket jaringan dan forensik jaringan.

3. Konfigurasi dan Integrasi Wazuh

- Monitoring dan Deteksi Serangan: Menggunakan Wazuh untuk monitoring file integrity.
- Integrasi dengan IDS: Pembuatan rules IDS dan manajemen alert.
- Konfigurasi Wazuh sebagai EDR/XDR: Script penghapusan file malicious dan otomasi konfigurasi.

4. Penggunaan Tool Tambahan

- Integrasi dengan Telegram: Mengatur alert melalui Telegram.
- Proof of Concept: Demonstrasi dan implementasi nyata konfigurasi yang diajarkan.

Profil Mentor

Anggrahito

Anggrahito, MBA, adalah seorang Expert di bidang Cybersecurity dan Penetration Testing dengan latar belakang akademis dan profesional yang kuat di keamanan siber. Keahliannya meliputi vulnerability assessment, ethical hacking, network security, dan penyusunan kebijakan keamanan informasi. Dengan 1 batch kelas di Taalenta, Anggrahito mengajar peserta memahami metodologi penetration testing, teknik identifikasi celah keamanan, serta strategi mitigasi risiko siber. Pendekatannya menggabungkan perspektif bisnis dari latar MBA dengan kompetensi teknis, relevan bagi profesional IT dan manajemen keamanan organisasi.

Investasi Program

Pilihan paket yang tersedia untuk program ini:

Elite	Supreme	e-Course
~~Rp 600.000~~	~~Rp 800.000~~	~~Rp 300.000~~
Rp 275.000	**Rp 295.000**	**Rp 155.000**
per peserta	per peserta	per peserta

Jadwal & Sesi

Sesi 1

27 Nov 2025

19:30 – 21:30 WIB

Log Analysis

Log Analysis 1. Linux Command o Pengantar Command line linux o Pengelolaan file dan direktori o Pemantauan sistem 2. Linux log Analysis o Analisis Log Linux dengan command o Script bash untuk log analisis 3. Wireshark Log Analysis o Overview / Pengantar Wireshark o Analisis Paket dengan Wireshark o Analisis forensic jaringan dengan Wireshark

1. Linux Command 2. o Pengantar Command line linux 3. o Pengelolaan file dan direktori 4. o Pemantauan sistem 5. Linux log Analysis 6. o Analisis Log Linux dengan command 7. o Script bash untuk log analisis 8. Wireshark Log Analysis 9. o Overview / Pengantar Wireshark 10. o Analisis Paket dengan Wireshark 11. o Analisis forensic jaringan dengan Wireshark

Sesi 2

28 Nov 2025

19:30 – 21:30 WIB

Pengenalan SIEM dan Wazuh

Pengenalan SIEM dan Wazuh 1. Pengenalan SIEM o Definisi dan fungsi SIEM (Security Information and Event Management) o Manfaat SIEM dalam keamanan siber o Komponen utama SIEM (Log Collection, Correlation, Alerting, Reporting) 2. Pengenalan Wazuh o Mengenal Wazuh o Arsitektur Wazuh: Komponen dan fungsinya (Manager, Agent, Dashboard) 3. Persiapan development o Persyaratan sistem dan instalasi Wazuh o Konfigurasi dasar Wazuh Manager dan Agent o Pengenalan Wazuh Dashboard (Kibana) 4. Instalasi dan Konfigurasi Dasar o Instalasi Wazuh Manager dan Agent pada server o Konfigurasi koneksi antara Manager dan Agent o Mengakses dan memahami Wazuh Dashboard

1. Pengenalan SIEM 2. o Definisi dan fungsi SIEM (Security Information and Event Management) 3. o Manfaat SIEM dalam keamanan siber 4. o Komponen utama SIEM (Log Collection, Correlation, Alerting, Reporting) 5. Pengenalan Wazuh 6. o Mengenal Wazuh 7. o Arsitektur Wazuh: Komponen dan fungsinya (Manager, Agent, Dashboard) 8. Persiapan development 9. o Persyaratan sistem dan instalasi Wazuh 10. o Konfigurasi dasar Wazuh Manager dan Agent 11. o Pengenalan Wazuh Dashboard (Kibana) 12. Instalasi dan Konfigurasi Dasar 13. o Instalasi Wazuh Manager dan Agent pada server 14. o Konfigurasi koneksi antara Manager dan Agent 15. o Mengakses dan memahami Wazuh Dashboard

Sesi 3

29 Nov 2025

13:00 – 15:00 WIB

Konfigurasi dan Integrasi Wazuh part 1

Konfigurasi dan Integrasi Wazuh part 1 1. Monitoring dan Deteksi Serangan o Menggunakan Wazuh untuk monitoring file integrity (FIM) o Konfigurasi analisis log dan deteksi ancaman o Pembuatan dan manajemen alert 2. Integrasi dengan IDS (Intrusion Detection System) o Pengenalan IDS (Intrusion Detection System) o Membuat Rules IDS yang diintegrasikan

1. Monitoring dan Deteksi Serangan 2. o Menggunakan Wazuh untuk monitoring file integrity (FIM) 3. o Konfigurasi analisis log dan deteksi ancaman 4. o Pembuatan dan manajemen alert 5. Integrasi dengan IDS (Intrusion Detection System) 6. o Pengenalan IDS (Intrusion Detection System) 7. o Membuat Rules IDS yang diintegrasikan

Sesi 4 30 Nov 2025 19:30 – 21:30 WIB	**Konfigurasi dan Integrasi Wazuh part 2** Konfigurasi dan Integrasi Wazuh part 2 1. Integrasi dengan Messanger Telegram o Melakukan integrasi dengan Telegram o Melakukan konfigurasi o Proof of Concept 2. Konfigurasi Wazuh sebagai EDR/XDR o Membuat script menghapus file malicious dengan python o Melakukan konfigurasi Otomatisasi o Proof of Concept 1. Integrasi dengan Messanger Telegram 2. o Melakukan integrasi dengan Telegram 3. o Melakukan konfigurasi 4. o Proof of Concept 5. Konfigurasi Wazuh sebagai EDR/XDR 6. o Membuat script menghapus file malicious dengan python 7. o Melakukan konfigurasi Otomatisasi 8. o Proof of Concept

Pendaftaran

Daftar di halaman program:

taalenta.id/scm

Atau scan QR di samping untuk membuka langsung.

Kontak

PT Taalenta Digital Inteleksia

Jl. Prof. Herman Yohanes, Depok, Sleman, D.I. Yogyakarta

WhatsApp / Telepon: 0851-8313-3328

Email: halo@taalenta.id