SOC · Batch 1

Mastering SOC Analyst: Deteksi Serangan & SIEM Monitoring dengan Wazuh

Dari Memasang Wazuh dan Menulis Rule Deteksi sampai Simulasi Serangan dan Respons Insiden

8 JP · Live Online via Zoom · 18 Des 2026 – 21 Des 2026

Ringkasan Eksekutif

Kelas ini melatih Anda bekerja sebagai analis SOC dengan Wazuh sebagai platform SIEM. Anda memasang Wazuh dan agent, menyusun rule deteksi, memantau integritas file dan lalu lintas jaringan dengan Suricata, lalu menyimulasikan serangan di lab sendiri. Hasil deteksinya Anda tindak lanjuti lewat active response dan notifikasi Telegram, ditutup dengan laporan insiden singkat.

Nama Program	Mastering SOC Analyst: Deteksi Serangan & SIEM Monitoring dengan Wazuh
Kode Program	SOC · Batch 1
Durasi	8 JP
Tanggal Pelaksanaan	18 Des 2026 – 21 Des 2026
Format & Platform	Live Online via Zoom
Mentor	Anggrahito, (CEH, ECSA, CHFI) MBA.
Bahasa	Bahasa Indonesia
Sertifikat	e-Certificate Taalenta (sesuai paket)

Kenapa Wajib Ikut

1. Lab yang Anda bangun sendiri

Anda menyiapkan lab empat mesin virtual (Wazuh Server, Ubuntu, Windows dengan Sysmon, dan Kali Linux) lalu memakainya sepanjang kelas.

2. Dari pemasangan sampai respons insiden

Silabus mengikuti alur kerja nyata: memasang Wazuh dan agent, menulis rule, memantau file dan jaringan, menyimulasikan serangan, lalu merespons dan melapor.

3. Deteksi dan respons otomatis

Anda mencoba Active Response untuk memblokir IP penyerang, integrasi VirusTotal untuk file berbahaya, dan notifikasi alert ke Telegram.

4. Dipetakan ke kerangka yang dipakai industri

Materi merujuk NIST SP 800-61 untuk siklus respons insiden dan MITRE ATT&CK untuk memetakan deteksi.

Outline Materi

1. Memahami SOC dan Arsitektur Wazuh

- Peran SOC Tier 1 sampai 3, perbedaan SIEM, XDR, dan SOAR, serta siklus Detect, Analyze, Respond menurut NIST SP 800-61.
- MITRE ATT&CK sebagai bahasa bersama untuk menjelaskan teknik serangan dan menyusun use case SOC.
- Komponen Wazuh (agent, server, indexer, dashboard), port yang dipakai, dan alur log dari decoder, rule, alert, sampai indexer.
- Pilihan model pemasangan (all-in-one, distributed, Docker/OVA), kebutuhan server, dan retensi data.

2. Memasang Wazuh dan Menghubungkan Agent

- Memasang Wazuh dengan wazuh-install.sh, mengambil kredensial, memeriksa layanan, dan masuk ke dashboard lewat HTTPS.
- Memasang agent di Linux dan Windows, memastikan agent terhubung, serta menelusuri masalah port, firewall, dan versi agent.
- Menyiapkan lab empat mesin virtual: Wazuh Server, web server Ubuntu, Windows dengan Sysmon, dan Kali Linux sebagai penyerang, dengan snapshot baseline.

3. Membaca, Menyusun, dan Menguji Rule Deteksi

- Struktur decoder dan rule XML, makna level 0 sampai 15 untuk triase, serta pemetaan rule ke MITRE ATT&CK.
- Membedakan ruleset bawaan dengan rule kustom di local_rules.xml, termasuk rentang ID kustom.
- Menguji log dengan wazuh-logtest, membuat rule anak, dan menyusun korelasi berbasis frekuensi dan jangka waktu.
- Berburu ancaman di dashboard dengan query DQL, saved query, kolom kustom, dan ekspor CSV.

4. Memantau File, Jaringan, dan Ancaman Berbasis Reputasi

- File Integrity Monitoring: memantau perubahan pada direktori penting di Linux dan Windows, lalu membaca alert-nya di dashboard.
- Memasang Suricata sebagai NIDS, mengirim log eve.json ke Wazuh, dan menguji deteksinya.
- Integrasi VirusTotal dengan active response untuk menghapus file berbahaya otomatis, diuji dengan file EICAR, lengkap dengan batas API publiknya.

5. Simulasi Serangan dan Respons Insiden

- Brute force dengan Hydra dan active response firewall-drop yang memblokir IP penyerang.
- Pemindaian dengan Nmap serta serangan SQL Injection dan XSS ke web server, lalu menelusuri alert yang muncul.
- Notifikasi alert ke Telegram lewat bot dan integrasi kustom, dengan filter level atau rule tertentu.
- Skenario terpadu dari pengintaian, brute force, sampai malware, ditutup dengan laporan insiden singkat.

6. Praktik Analis SOC yang Rapi

- Validasi true positive dan false positive, pengayaan konteks alert, eskalasi ke level berikutnya, dan dokumentasi tiket.
- Mengatur keseimbangan antara noise dan cakupan deteksi, pengecualian, pengamanan API key, dan risiko auto-delete.
- Pre-test, kuis di tiap sesi, post-test, dan roadmap lanjutan (Sysmon, vulnerability detection, SOAR).

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
~~Rp 400.000~~	~~Rp 500.000~~
Rp 275.000	**Rp 295.000**
per peserta	per peserta

Jadwal & Sesi

Sesi 1

18 Des 2026

19:00 – 21:00 WIB

Fondasi SOC & Wazuh: Arsitektur hingga Deploy Agent

- Perkenalan, tujuan pelatihan, aturan lab (etika & isolasi jaringan), pre-test 10 soal. Peran SOC Tier 1–3; SIEM vs XDR vs SOAR; siklus Detect–Analyze–Respond (NIST SP 800-61); MITRE ATT&CK sebagai bahasa deteksi; use case SOC. - Komponen Agent, Server (wazuh-remoted, wazuh-analysisd, wazuh-authd), Indexer, Dashboard; port 1514/1515/55000/9200/443; alur log → decoder → rule → alert → indexer. All-in-one vs distributed vs Docker/OVA; kebutuhan server AIO (4 vCPU / 8 GB RAM / 50 GB); OS yang didukung; retensi data. - Jalankan wazuh-install.sh -a (Wazuh 4.14), ambil kredensial dari wazuh-install-files.tar, verifikasi service wazuh-manager / wazuh-indexer / wazuh-dashboard, login dashboard HTTPS. - Agent Linux (repo apt + WAZUH_MANAGER) dan Windows (MSI silent install); verifikasi agent_control -l; troubleshooting port 1514/1515, firewall, versi agent ≤ manager. - Rekap konsep kunci, kuis singkat, persiapan Sesi 2.

Sesi 2

19 Des 2026

09:00 – 11:00 WIB

SOC Analysis: Lab Virtual, Anatomi Rule & Threat Hunting

- Cek status agent & kesiapan lab tiap peserta. Topologi 4 VM di VirtualBox/VMware/Proxmox: Wazuh Server, Ubuntu Web Server (Apache), Windows 10/11 + Sysmon, Kali Linux (attacker); jaringan NAT Network/Host-only 192.168.56.0/24; snapshot baseline. - Struktur decoder & rule XML; level 0–15 dan makna triase; rule.groups; mapping rule.mitre.id; ruleset bawaan /var/ossec/ruleset/ vs kustom /var/ossec/etc/rules/local_rules.xml; rentang ID kustom 100000–120000. - Modul Threat Hunting/Discover; query DQL: rule.id:5710, rule.level >= 10, agent.name, rule.groups:authentication_failed, rule.mitre.id, data.srcip; saved query, kolom kustom, export CSV. - Uji log dengan /var/ossec/bin/wazuh-logtest; rule anak (if_sid), korelasi frekuensi (frequency, timeframe, if_matched_sid, same_srcip); naikkan level & tambahkan MITRE; restart manager & validasi. - Validasi true/false positive, enrichment (reputasi IP, konteks agent), eskalasi ke L2, dokumentasi tiket. - Rekap, kuis rule.id, persiapan Sesi 3.

Sesi 3

20 Des 2026

09:00 – 11:00 WIB

Integrasi PoC: FIM, Suricata NIDS & Auto-Remediation VirusTotal

- Review custom rule & hasil hunting. - Konfigurasi : realtime, whodata (auditd / Windows SACL), report_changes; monitor /etc, /var/www/html, folder Downloads Windows; uji tambah/ubah/hapus; analisis alert & dashboard FIM. - Instal Suricata di Ubuntu agent, aktifkan ET Open (suricata-update), set HOME_NET & interface; kirim eve.json via log_format json; uji curl testmynids.org & Nmap; analisis rule.groups:suricata. - Blok virustotal (API key, group syscheck); FIM realtime di direktori target; skrip remove-threat (Linux) / remove-threat.exe (Windows); & pada rule 87105; uji file EICAR; batas API publik 4 req/menit & 500/hari. - Noise vs coverage, pengecualian (), pengamanan API key, risiko false positive pada auto-delete, change management.

Sesi 4

21 Des 2026

19:00 – 21:00 WIB

Simulasi Serangan, Active Response & Notifikasi Telegram

- Validasi ketiga PoC berjalan. - Hydra dari Kali ke Ubuntu agent; deteksi 5710/5760/5763; Active Response firewall-drop (timeout 180 detik); verifikasi IP penyerang terblokir & alert 651. - Nmap scan (terdeteksi Suricata); SQL Injection & XSS ke Apache (curl/browser) → 31103/31105/31106; opsional: brute force logon Windows → 60122/60204. - Bot via @BotFather, chat_id via getUpdates; skrip /var/ossec/integrations/custom-telegram (+ .py), izin 750 root:wazuh; blok dengan hook_url, level ≥ 10 atau rule_id tertentu; uji & format pesan. - Skenario terpadu: recon → brute force → drop malware; tim mendeteksi, merespons, menerima notifikasi Telegram, menyusun laporan insiden singkat. - Post-test, evaluasi pelatihan, roadmap lanjutan (Sysmon, vulnerability detection, SOAR).

Perlengkapan

- Laptop dengan spesifikasi yang memadai (menjalankan beberapa mesin virtual)
- Koneksi internet yang stabil

Pendaftaran

Daftar di halaman program:

taalenta.id/soc

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

Dokumen ini di-generate otomatis dari data terkini di sistem Taalenta. Harga, jadwal, dan ketersediaan paket dapat berubah; mohon konfirmasi ulang melalui WhatsApp/email di atas sebelum pengajuan resmi.

© 2023–2026 PT Taalenta Digital Inteleksia. Versi: 2026-11-19 02:03