DIMASQI RAMADHANI

+6282254331579 | dimasqiramadhani@gmail.com | https://dimasqiramadhani.com

Tangerang Regency, Banten, 15810

Security Engineer focused on detection engineering, SIEM/XDR implementation, vulnerability assessment, and security validation. Hands on experience building monitoring pipelines, endpoint detection coverage, technical documentation and offensive security assessment. Skilled in Wazuh, Elastic Stack, Tenable One, Picus Security, Python, Linux/Windows, and network security operations.

EXPERIENCES

PT. Visionet Data Internasional — **Tangerang Regency, Banten**

Security Engineer — **Nov 2025 - Now**

- Built custom Auditbeat decoders for Linux and Windows log sources in a SIEM proof of concept, supporting log normalization, more accurate analytics, and actionable alerting.
- Conducted penetration testing on AS400, Active Directory, and web application environments to identify security weaknesses, validate exposure, and support remediation recommendations.
- Led the initial implementation of Wazuh multi-cluster monitoring for PT Rintis Sejahtera, covering 350+ endpoints, agent configuration, ruleset tuning, and log ingestion validation.
- Deployed Nessus Agent and Scanner for BNI to support vulnerability scanning across 2,000 endpoints, including 500 Kubernetes based endpoints.
- Troubleshot and optimized Auditbeat to Wazuh integrations through isolated error log analysis and validation of security event visibility.

Security Analyst — **Tangerang Regency, Banten**

- Performed level 1 security monitoring and alert triage across Graylog, SOC Fortress, Grafana, and Wazuh. — **Oct 2025 - Nov 2025**
- Validated initial alerts, conducted basic incident classification, and escalated confirmed security events.
- Supported recurring dashboard checks and routine monitoring activities to maintain daily security operations.

PT. Inixindo Amiete Mandiri — **Bandung, West Java**

Junior Network Instructor — **Jun 2025 - Sep 2025**

- Assisted senior instructors in delivering basic networking training, including TCP/IP, OSI Layer, subnetting, routing, switching, and troubleshooting
- Supported hands on lab sessions using Cisco Packet Tracer and basic network simulation tools.
- Helped prepare training materials, lab exercises, and technical documentation for networking classes.
- Guided client during practical configuration tasks and answered basic technical questions.
- Assisted in evaluating participant progress and improving learning outcomes during the 3 month probation period.

PT. Pupuk Kalimantan Timur — **Bontang, East Kalimantan**

IT Infrastructure Intern - Magenta Pupuk Kaltim Apprentice Challenge Batch X — **Agu 2024 - Feb 2025**

- Developed and monitored dashboards to improve network visibility and threat detection in support of ISO 27001 and NIST aligned requirements.
- Built network traffic monitoring dashboards using NetFlow and the Elastic Stack to support network quality analysis and IT audit standards.
- Supported server resource monitoring and technical documentation to improve operational visibility and data driven IT activities.

PROJECTS

NetFlow Integration for Network Visibility and Detection Engineering — **Agu 2024 - Feb 2025**

- Implemented a NetFlow based network traffic monitoring pipeline using Wazuh, pmacct, and custom JSON normalization to collect and analyze network flow data.
- Configured pmacct as a NetFlow collector to process traffic metadata including source IP, destination IP, ports, protocols, bytes, and packet count.
- Developed custom Wazuh decoders and detection rules to identify suspicious network activity, unusual port usage, and internal/external traffic patterns.
- Integrated NetFlow logs with Wazuh Agent using localfile monitoring to forward normalized network telemetry into the SIEM for alerting and investigation.
- Built SOC style dashboards and validated the detection pipeline, generating 4,472 NetFlow events and 982 high severity alerts in a environment.
- Performed end-to-end validation of the NetFlow ingestion pipeline by testing log collection, JSON parsing, Wazuh decoding, rule matching, and alert generation.
- Documented NetFlow alert evidence, dashboard results, traffic patterns, and detection logic to support SOC investigation and future rule tuning.

Endpoint Detection Engineering with Wazuh, Falco, Sysmon, and Auditd — **Mar 2026 - Apr 2026**

- Assess an endpoint detection engineering using Wazuh, Falco, Sysmon, and auditd to monitor Linux, Windows, and container runtime security events.
- Integrated multi source telemetry into Wazuh, including Linux audit logs, Windows Sysmon events, Falco runtime alerts, and security related endpoint activity.
- Configured Wazuh agents on Linux and Windows endpoints to centralize security event collection, normalization, and alert forwarding.
- Developed custom Wazuh detection rules to identify suspicious endpoint behavior, privilege related activity, process execution patterns, and runtime security events.
- Mapped detection logic to MITRE ATT&CK techniques to improve detection coverage, investigation context, and security monitoring maturity.
- Created custom Wazuh dashboards to visualize endpoint telemetry, high-severity alerts, event trends, and detection coverage across monitored endpoints.
- Validated the detection pipeline with real case generated activity, producing over 55,000 endpoint events, 12,000 Falco events, 7,900 Sysmon events, and 10/10 successful test cases.

Active Directory Red Team Simulation with Wazuh Detection Engineering **Mei 2026 - Jun 2026**

- Assess controlled Active Directory offensive security to simulate real-world enterprise attack paths and validate domain security weaknesses.
- Performed end-to-end Active Directory enumeration covering domain users, groups, shares, services, authentication exposure, and network reachable assets.
- Used tools such as Nmap, Impacket, BloodHound, PowerView, and CrackMapExec to identify misconfigurations, exposed credentials, and privilege escalation opportunities.
- Simulated common Active Directory attack techniques including credential discovery, Kerberos based attacks, weak password validation, and lateral movement scenarios.
- Analyzed attack paths to understand how low privileged access could escalate into higher impact domain compromise scenarios.
- Documented each testing phase with command evidence, findings, affected assets, risk context, and remediation recommendations.
- Produced security hardening recommendations for Active Directory environments, including credential hygiene, privilege control, service account review, and attack path reduction.

Production Wazuh SIEM Architecture and Infrastructure Automation **Mei 2026 - Jul 2026**

- Designed and deployed a production like Wazuh SIEM/XDR architecture with clustered managers, distributed indexers, centralized dashboard, and load balanced agent communication.
- Implemented Wazuh manager clustering using primary and worker nodes to improve SIEM availability, agent coordination, and operational resilience.
- Configured a 3 node Wazuh indexer cluster with index/shard planning to support scalable log ingestion, retention, and search performance.
- Integrated HAProxy as a load balancer for Wazuh agent enrollment and event forwarding to distribute traffic across manager nodes.
- Created complete technical documentation covering architecture design, deployment steps, node validation, agent onboarding, and SIEM operational evidence.
- Performed post deployment validation by checking cluster health, node connectivity, agent status, dashboard access, and log ingestion flow.
- Configured agent grouping and centralized configuration management to support structured endpoint onboarding, policy separation, and scalable SIEM operations.

Nutanix Integration with SOC Fortress for Enchance Authentication Log Visibility **Jun 2026 - Jul 2026**

- Designed and implemented centralized authentication log integration from Nutanix Prism Central and CVM audit sources into SOC Fortress using Graylog, OpenSearch, and Grafana.
- Configured a TCP Syslog input and dedicated Graylog stream to support structured ingestion, routing, and management of Nutanix security logs.
- Developed two Graylog processing pipelines containing eight parsing and field-extraction rules for three Nutanix log types.
- Created detection rules for failed authentication, privilege escalation, API errors, configuration changes, and other critical administrative activities.
- Built Python based synthetic log generator and log feeder scripts to simulate Nutanix events and validate end-to-end ingestion, parsing, indexing, and detection workflows.
- Developed a Grafana security monitoring dashboard backed by OpenSearch to visualize authentication activity, operational events, errors, and detection indicators.
- Produced comprehensive technical documentation and validation evidence covering architecture, deployment, pipeline configuration, detection rules, troubleshooting, and operational handover.

EDUCATION

Universitas Merdeka Malang **Malang, East Java**

Bachelor of Information Systems | GPA: 3.85/4.00 **Sep 2020 - Feb 2024**

- Awarded Second Best Graduate in the Faculty of Information Technology.
- Participated in a community service project to support the digitalization of local businesses in Djamoesoedirjo, with responsibilities including landing page deployment, public hosting and DNS setup, and protection of digital assets through copyright registration.
- Specialized in IT Infrastructure: Network Administration, Server Management, Information Security, and Virtualization Technology.

SKILLS

- Vulnerability Assessment : Tenable One
- SIEM Monitoring : Wazuh, Elastic Security
- Infrastructure & DevOps : Git, Network, Docker, VMware, Ansible
- Offensive Security : Picus Security
- Operating Systems : Windows, Linux
- Scripting and Query : Bash, SQL, PowerShell
- Application Security : Access Control, OWASP Top 10, Input Validation, Authentication Security, Secure Code

CERTIFICATIONS

- Continuous Security Validation Purple Academy by Picus Security
- Cyber Security Courses Online Complete Bundle by ITBOX
- Cyber Security Bootcamp by PT Visionet Data Internasional
- SOC Level 1 by TryHackMe
- SOC Level 2 by TryHackMe