Md. Abu Saeid

Dhaka, Bangladesh contact.abusaeid@gmail.com +880 1752791256 mdabusaeid SaeidSec saeidsec

Professional Summary

SOC Analyst and Incident Responder with hands-on experience in security monitoring, alert triage, and SIEM engineering across L1/L2 SOC operations. Skilled in threat detection, log analysis, and incident investigation using Wazuh, Elastic Stack, Splunk, and IBM QRadar. Proven expertise in building enterprise-grade SIEM architectures, threat hunting, and detection engineering aligned to MITRE ATT&CK. Strong background in automation using Python and n8n to reduce false positives and improve MTTR through ML-driven anomaly detection pipelines.

Core Competencies

- Security Monitoring & Alert Triage
- Incident Investigation & Response (L1/L2)
- SIEM Operations & Architecture
- Threat Hunting & Detection Engineering
- Log Analysis & Correlation
- SOC Automation & SOAR

Experience

Founder & Security Architect – Aegisryx Labs, Dhaka **Jan 2026 – Present**

- Architected enterprise-grade SIEM infrastructure with 99.9% availability supporting 10,000+ endpoints
- Engineered distributed Wazuh Master/Worker cluster with 3-node OpenSearch indexer for zero data loss
- Developed custom FastAPI-based Wazuh-Proxy with mTLS-secured ingestion and rate limiting
- Implemented dual-layer load balancing (Nginx L4 + HAProxy L7) achieving 40% throughput improvement
- Deployed full-stack observability ecosystem (Zabbix, Prometheus, Grafana) for SIEM health monitoring
- Automated SOAR workflows using DFIR-IRIS and n8n reducing incident response time by 60%
- Integrated honeypots (Cowrie, Beelzebub) and Trivy vulnerability scanning for threat intelligence

SOC Intern – Cyber Academy, Pakistan **Aug 2025 – Sep 2025**

- Performed SIEM operations using Wazuh correlating Windows Event Logs and Sysmon data
- Improved alert accuracy by 40% through enhanced correlation rules and detection tuning
- Developed incident escalation procedures and endpoint monitoring capabilities

SOC Intern – Center for Cyber Security Studies & Research **Apr 2024 – Aug 2024**

- Collaborated with researchers analyzing IoT vulnerabilities, contributing to 3 security reports
- Deployed Wazuh and ELK Stack monitoring 500+ daily security events for threat detection
- Presented threat landscape findings enhancing team awareness of emerging attack vectors

SOC Intern – Chaitanya Cyber Strix Technologies Pvt Ltd, India **Nov 2023 – Mar 2024**

- Monitored security events using SIEM platforms identifying and triaging 20+ potential threats
- Drafted 10+ incident response reports with mitigation recommendations
- Conducted malware analysis identifying 5+ IOCs using threat intelligence platforms

Projects

Enterprise-Grade Wazuh SIEM Deployment with High Availability **2025**

- Designed fault-tolerant SIEM architecture with multi-zone security segmentation
- Implemented active-active Wazuh Manager cluster for horizontal scalability
- Configured Keepalived-based HA with floating VIPs eliminating single points of failure

- Validated disaster recovery through simulated failure scenarios maintaining uninterrupted operations

eBPF-Sentry: Linux Kernel Security System **2025**

- Built high-performance eBPF-based IDS/IPS for syscall-level threat detection
- Implemented real-time active defense and process termination capabilities
- Designed stateful behavioral detection for multi-stage attacks with hot-reloadable rules

Network Traffic Monitoring and Analysis System **2025**

- Developed full-stack network traffic analysis platform supporting live and PCAP analysis
- Implemented deep packet inspection using Scapy and Wireshark with real-time dashboard
- Automated protocol, port, and endpoint analysis for rapid threat identification

Education

Bachelor of Science in Computer Science and Engineering – Green University of Bangladesh
Thesis: NeuroCrypt – A Secure Framework for Brain-Computer Interface Data Sharing **Feb 2021 – Mar 2025**

Certifications

- **Blue Team Junior Analyst** (2025) – SOC operations, incident response, threat detection
- **ISO/IEC 27001:2022 Lead Auditor** (2025) – Information security management systems
- **Practical Ethical Hacking - The Complete Course** (2025) – Offensive security, penetration testing
- **Mastering Cyber Threat Intelligence for SOC Analysts** (2025) – Threat intel, OSINT, IOC analysis
- **SOC Level 1 Learning Path, TryHackMe** (2024) – SIEM monitoring, log analysis, alert triage
- **Linux/Windows Privilege Escalation for Beginners** (2025) – Post-exploitation techniques

Technical Skills

SOC & Security Tools: Wazuh SIEM, Elasticsearch (ELK), Splunk, IBM QRadar, Microsoft Sentinel, Suricata IDS/IPS, Snort, Wireshark, Nmap, YARA, VirusTotal, Sysmon, Burp Suite, Metasploit, OSQuery, Velociraptor, The Hive, Cortex
Monitoring & Logging: Log Analysis, SIEM Operations, Alert Correlation, Threat Hunting, Filebeat, Zeek
Automation & SOAR: Python Playbooks, n8n, DFIR-IRIS, Enrichment Pipelines, SIEM Health Automation
Infrastructure & DevOps: Docker, Kubernetes, Ansible, HAProxy, Nginx, Keepalived, AWS, Proxmox, VMware
Operating Systems: Linux, Windows Server, Active Directory
Languages: Python, Bash, PowerShell, C, C++, Java, Go, eBPF (BCC)
Frameworks: MITRE ATT&CK, NIST Cybersecurity Framework, Cyber Kill Chain, Zero Trust Architecture, OWASP Top 10
Platforms: TryHackMe, Hack The Box, LetsDefend