ASAD NOOR

SOC Analyst | SIEM Engineer

Lahore, Pakistan | +92-343-4666264 | asadnoor951@gmail.com | linkedin.com/in/asadnoor951

PROFESSIONAL SUMMARY

Results-driven SOC Analyst and SIEM Engineer with 3+ years of hands-on experience designing, deploying, and operating enterprise security monitoring infrastructure in high-availability fintech environments. Specializes in building on-premises SIEM solutions using ELK Stack, Wazuh, and Splunk — covering full-cycle log ingestion, normalization, correlation rule development, and real-time threat detection across Windows, Linux, firewall, and network device environments. Proven expertise in Tier 1 & Tier 2 SOC operations including alert triage, threat classification, incident investigation, root cause analysis, and structured escalation. Skilled in detection engineering mapped to the MITRE ATT&CK framework, having developed 40+ custom use cases targeting ransomware, lateral movement, and persistence techniques. Experienced in threat hunting, File Integrity Monitoring (FIM), endpoint telemetry via Elastic Defend, and vulnerability management using OpenVAS and Nmap. Proficient in Linux command-line administration, SOC automation using n8n pipelines, and developing SOPs and playbooks that streamline incident handling. Additionally holds hands-on experience in web application security testing (Burp Suite, OWASP Top 10), network fundamentals (TCP/IP, VLANs, Routing, NAT), and cloud security concepts. Committed to continuous learning and advancing detection capability across evolving threat landscapes.

CORE COMPETENCIES

SIEM Engineering	ELK Stack (Elasticsearch, Logstash, Kibana), Wazuh, Splunk, Log Ingestion & Normalization, Correlation Rule Development, Index & Pipeline Management, Alert Tuning
SOC Operations	Tier 1 & 2 Alert Triage, Incident Investigation, Threat Classification, Root Cause Analysis, Structured Escalation, Shift-Based Operations, SOC Workflow Management
Detection Engineering	MITRE ATT&CK Mapping, Custom Use Case Development (40+ Rules), Ransomware Detection (T1486), Execution Detection (T1059), False Positive Reduction (40%), Threat Hunting
Incident Response	Incident Triage, Containment & Mitigation, Escalation Workflows, Evidence Collection, Digital Forensics Basics, Playbook Execution, Post-Incident Documentation
Endpoint & FIM	Elastic Defend (EDR), File Integrity Monitoring (FIM), Endpoint Telemetry, Ransomware Behavior Detection, Process & Network Activity Monitoring
Vulnerability Mgmt	OpenVAS, Nmap, CVE Analysis & Remediation, Patch Management, CIS Benchmarks, OS Hardening (Linux & Windows Server), Attack Surface Reduction
Linux & Systems	Ubuntu, CentOS, CLI Administration, Proxmox VE, VMware, Windows Server (Active Directory, DNS), MikroTik RouterOS, Zimbra Mail, TCP/IP, VLANs, NAT
Web App Security	Burp Suite, OWASP Top 10, WAF / NGFW / Proxy Concepts, SQL Injection, XSS, Authentication Testing, Vulnerability Reporting
Automation & Docs	n8n Alerting Pipelines (Telegram/Email), SOP & Playbook Development, Firewall Config Documentation, Incident Reports, Network Topology Documentation
Cloud & Compliance	AWS Cloud Security Concepts, Fundamentals of Cloud Security (Palo Alto), SOC Principles, Data Encryption, Information Security Fundamentals, DevSecOps Basics

WORK EXPERIENCE

SOC Analyst & SIEM Engineer (Assistant Manager – Data Center) | PostEx (Fintech)

Jan 2025 – Present • Lahore, Pakistan

- Architect and operate a fully on-premises SIEM environment using ELK Stack and Wazuh, onboarding 500+ endpoints and network devices (Linux, Windows, MikroTik, firewall) for centralized log ingestion and real-time threat detection.
- Perform Tier 1 & Tier 2 SOC duties: monitor security dashboards, triage alerts, classify threats, investigate incidents end-to-end, and conduct root cause analysis with full documentation.
- Engineer 40+ custom SIEM detection rules mapped to the MITRE ATT&CK framework (T1059 – Command & Scripting Interpreter, T1486 – Data Encrypted for Impact, and more), significantly improving threat visibility.
- Reduced SIEM false positives by 40% through systematic alert tuning, log filtering, correlation logic refinement, and whitelist management across ELK Stack and Wazuh.
- Integrated Elastic Defend for advanced endpoint telemetry, real-time ransomware behavior detection, process monitoring, and File Integrity Monitoring (FIM) across critical servers.
- Built n8n-based automated alerting pipelines routing critical SIEM alerts to Telegram and email within 1–2 minutes of detection, enabling sub-2-minute mean time to notify (MTTN).
- Conduct proactive threat hunting sessions across log data and endpoint telemetry, identifying anomalous behaviors, persistence mechanisms, and lateral movement indicators.
- Manage complete incident response lifecycle: initial detection, triage, containment, escalation to senior engineers for complex cases, remediation coordination, and post-incident reporting.
- Perform regular vulnerability scans using OpenVAS and Nmap across critical infrastructure; lead CVE remediation and OS hardening aligned with CIS Benchmarks.
- Develop and maintain SOC SOPs, detection playbooks, escalation procedures, and firewall configuration documentation to ensure operational consistency and knowledge transfer.
- Monitor firewall health (CPU, memory, throughput, system logs) and administer enterprise services including MikroTik routers, Proxmox VE, VMware, and Linux/Windows VMs.
- Collaborate cross-functionally with network, development, and infrastructure teams to implement zero-trust controls and enforce security policies enterprise-wide.

Assistant Network Administrator | PostEx (Fintech)

May 2023 – Dec 2024 • Lahore, Pakistan

- Monitored network infrastructure health and identified performance and configuration issues across firewalls, routers, and switches; supported early-stage security alert response.
- Assisted in firewall rule updates, VLAN configuration, and network segmentation to enforce access control and security policies.
- Configured and maintained MikroTik routers and switches including routing protocols (OSPF, BGP) and L2VPN tunnels to ensure high availability and secure inter-site connectivity.
- Troubleshot connectivity and routing issues across enterprise LAN/WAN environments using TCP/IP protocols; maintained accurate network topology documentation.
- Collaborated with security teams to implement zero-trust security controls, network hardening measures, and access restriction policies.
- Maintained up-to-date documentation of network topology, device configurations, firewall rules, and operational procedures.

Technical Support Engineer | StormFiber

Feb 2023 – May 2023 • Pakistan

- Provided technical support for network connectivity issues, diagnosing faults at L1/L2/L3 layers and escalating unresolved cases following defined procedures.
- Assisted in troubleshooting routing, switching, and ISP-related incidents; performed basic network device configuration and interface status verification.
- Coordinated with field engineers and NOC teams to restore service availability and minimize downtime during network outages.
- Logged and tracked incidents in the ticketing system; maintained documentation of recurring issues and resolution steps to build a knowledge base.

- Provided clear written and verbal communication to customers and internal teams during incident handling and service restoration.

EDUCATION

Bachelor of Science – Computer Science | NCBA&E, Lahore | Sep 2018 – Aug 2022
Skills: Windows Server, Linux System Administration, Active Directory, Network Administration, L2VPN, Cyber Security, Microsoft Office, Project Management

Cisco Certified Network Administrator (CCNA) | Corvit System Multan | Mar 2022 – Jul 2022
Activities: Routing protocols – EIGRP, OSPF, RIP, BGP, OSI Model, IPv4, IPv6
Skills: TCP/IP, MikroTik, Network Security, Network Administration, LAN, L2TP, Network Automation

Intermediate of Computer Science (ICS) | Punjab Group Colleges | May 2016 – Oct 2018

Matric – Computer Science | Muslim Public Higher Secondary School | Mar 2012 – Jul 2014

CERTIFICATIONS

- Advent of Cyber 2025 – TryHackMe (Blue Team Operations, Log Analysis, Threat Investigation)
- Cyber Security 101 Learning Path – TryHackMe (Core Security Principles, Threat Analysis, SOC Basics)
- Web Fundamentals Learning Path – TryHackMe (Web Architecture, HTTP, Authentication, Web App Security)
- Pre Security Learning Path – TryHackMe (Networking, Operating Systems, Security Fundamentals)
- Jr. Penetration Tester Learning Path – TryHackMe (Web App Pentesting, SQL Injection, XSS, Auth Testing)
- DevSecOps Learning Path – TryHackMe (CI/CD Security, Infrastructure Hardening, Container Security)
- CyberOps Associate – Cisco (Detection Engineering, MITRE ATT&CK, Incident Handling, Network Sweeps, Vulnerability Management)
- Ethical Hacker – Cisco (OWASP Top 10, Password Hacking, Burp Suite, Digital Forensics, Web App Security)
- Cybersecurity Essentials – Cisco (MITRE ATT&CK, Ransomware Mitigation, Log Encryption, Digital Forensics)
- Introduction to Packet Tracer – Cisco Networking Academy
- NDG Linux Unhatched – Cisco Networking Academy
- Security Operations Center (SOC) – Palo Alto Networks (MITRE ATT&CK, Digital Forensics, Incident Response)
- Fundamentals of Network Security – Palo Alto Networks (Firewalls, NGFW, Access Control, Network Security)
- Fundamentals of Cloud Security – Palo Alto Networks (Cloud Security, Information Security)
- Hands-on Web Application Security – EC-Council (Burp Suite, TCP/IP, Vulnerability Reporting)
- SQL Injection Attacks – EC-Council