Sangram Rajput

LinkedIn | Portfolio | GitHub | sangramrajput436@gmail.com | (+91) 9404567417

SOC Analyst with hands-on experience in SIEM alert triage, incident investigation,and phishing & malware analysis within a simulated 24×7 SOC environment. Experienced in alert correlation, IOC validation, log analysis using Splunk SIEM, and endpoint investigation using EDR tools. Strong understanding of SOC workflows, incident documentation, and escalation with actionable next steps.

Experience

SOC Analyst (L1/L2 Exposure) | Worldsec Technologies *Jan 2025 – Sep 2025 (Internship - Completed)*

- Monitored and investigated real-time security alerts in a 24×7 SOC environment.
- Performed SIEM alert triage and investigation using Splunk across Windows, Linux, and firewall logs.
- Used SPL queries to analyze suspicious activity and validate true vs false positives.
- Conducted phishing email analysis including header review, URL reputation, and IOC extraction.
- Performed endpoint investigations using CrowdStrike Falcon EDR.
- Analyzed malware behavior, persistence mechanisms, and lateral movement techniques.
- Escalated confirmed incidents per client SLAs with clear documentation in ServiceNow.
- Utilized Cortex XSOAR for alert enrichment and response automation.

Skills

SIEM: Splunk (Alert Triage, Log Analysis, Correlation Rules, Dashboards)

EDR: **C**rowdStrike Falcon (Endpoint Investigation, IOC Analysis, Host Isolation – Basic)

SOAR: Cortex XSOAR (Playbooks, Automation, Incident Handling)

Security: Incident Response, Threat Hunting, IOC Analysis, MITRE ATT&CK

Tools: ServiceNow, Nessus, OSINT, Windows/Linux Logs

Projects

Phishing Email Analysis – SOC Tier 2 (PDF | GitHub)

• Performed end-to-end phishing investigation including header analysis, URL/IP reputation checks, and IOC extraction.

• Mapped attacker techniques to MITRE ATT&CK framework.

• Recommended mitigation actions such as blocking malicious domains, IPs, and hashes.

SOC Alert Triage & Brute Force Detection (Splunk)(PDF | GitHub)

• Built an end-to-end SOC workflow using Splunk to detect brute-force authentication attacks, investigate Windows security logs, classify incident severity, and document escalation with remediation recommendations.

Suspicious PowerShell & Lateral Movement Detection (Splunk)(PDF | GitHub)

• Designed and implemented detection logic in Splunk to identify suspicious PowerShell execution using Windows Event ID 4688.

• Analyzed encoded commands, IEX usage, and abnormal parent-child processes (winword.exe → powershell.exe).

• Correlated authentication logs (Event ID 4624 – Logon Type 3) to investigate potential lateral movement.

• Mapped findings to MITRE ATT&CK (T1059.001, T1021) and documented full incident response workflow.

Firewall Threat Hunting & Port Scan Detection (Splunk)(PDF | GitHub)

• Analyzed 5,000 firewall events to detect reconnaissance and lateral movement

• Built port scan detection using distinct port correlation logic.
• Identified exposed RDP services and internal scanning behavior.
• Created real-time SOC alerts and monitoring dashboard.

Automated Incident Response System(PDF | GitHub)

• Built an automated incident response system integrating Splunk SIEM with Python.

• Created detection logic for brute force attacks (Event ID 4625) using SPL queries.

• Integrated VirusTotal API for threat enrichment and classification of IPs.

• Automated incident reporting (TXT/CSV) and simulated response actions.

VPN Log Monitoring & Account Misuse Detection (PDF | GitHub)

• Built a Splunk SIEM-based VPN monitoring system detecting brute-force and anomalous logins

• Implemented impossible travel detection using streamstats

• Created real-time alerts and performed SOC investigation & escalation

Certifications

Certified Ethical Hacker (CEH) – ICOREX | Sep 2024
Certified SOC Analyst (CSA) – SIEM XPERT | Jun 2025

Education

Ravindranath Tagore College, Aurangabad, Maharashtra, India

Bachelor's of Science, Computer Science