SOC Analyst Portfolio

Alexander Isoev

Philadelphia, PA | (267)-564-3799 | alexanderisoevf@gmail.com
LinkedIn: linkedin.com/in/alexanderisoev

I am a motivated SOC Analyst with hands-on experience in monitoring, triage, and incident response. Through labs and real-world scenarios, I have developed practical skills in log analysis, phishing investigation, PowerShell threat detection, and SQL injection triage. My goal is to grow into Threat Hunting and Incident Response, helping organizations stay ahead of modern cyber threats.

■ *Case Study 1: Phishing Email Investigation*

- **Alert:** Suspicious email detected by SIEM with subject "Urgent Payroll Update".
- **Analysis:** Reviewed email headers (Received-SPF: fail), found malicious link redirecting to fake O365 login page.
- **Action:** Blocked sender domain, reported to Threat Intel, notified affected user.
- **MITRE Mapping:** T1566.002 (Phishing: Spearphishing Link)

■ *Case Study 2: Malicious PowerShell Execution*

- **Alert:** EDR detected PowerShell with `-ExecutionPolicy Bypass` and base64 payload.
- **Analysis:** Decoded script, identified AMSI bypass and remote payload download attempt.
- **Action:** Isolated host, terminated process, deleted malicious files.
- **MITRE Mapping:** T1059.001 (Command and Scripting Interpreter: PowerShell)

■ *Case Study 3: SQL Injection Attempt*

- **Alert:** IDS signature `ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT` fired.
- **Analysis:** Reviewed Apache logs, found repeated requests with `SLEEP(5)` payload.
- **Action:** Blocked source IP at firewall, escalated to web team for patch verification.
- **MITRE Mapping:** T1190 (Exploit Public-Facing Application)

■ *Case Study 4: CrowdStrike Alert Triage*

- **Alert:** CrowdStrike detected malicious process running under Administrator account.
- **Analysis:** Verified process tree, confirmed AMSI bypass and potential credential theft attempt.
- **Action:** Isolated host via EDR, deleted malicious files, reset compromised account password.
- **MITRE Mapping:** T1078 (Valid Accounts), T1055 (Process Injection)

■ *Case Study 5: Scheduled Task Persistence*

- **Alert:** Suspicious scheduled task creation detected (`schtasks /Create /TN WindowsDefenderCheck`).
- **Analysis:** Reviewed task XML, found it pointing to malicious PowerShell script in Temp directory.
- **Action:** Deleted task, removed script, scanned system for additional persistence mechanisms.
- **MITRE Mapping:** T1053.005 (Scheduled Task/Job: Scheduled Task)

■ *Case Study 6: IP IOC Investigation*

- **Alert:** Multiple failed RDP login attempts from IP 45.10.xxx.xxx.
- **Analysis:** Correlated events in Splunk, confirmed brute-force attempt.
- **Action:** Blocked IP at firewall, added to SIEM watchlist, reported to AbuseIPDB.
- **MITRE Mapping:** T1110 (Brute Force)

■ *Skills & Tools*

- SIEM: Splunk, IBM QRadar
- EDR: CrowdStrike Falcon
- Threat Intel: VirusTotal, AbuseIPDB
- Incident Response: Containment, Eradication, Recovery
- Frameworks: MITRE ATT&CK;, Cyber Kill Chain

■ *Certifications*

- CompTIA Security+ (Global Industry Certification)
- RangeForce Cybersecurity Analyst Program (251 modules, 96+ hours of hands-on labs)