Amrit Panthi

Security Operations Center (SOC) Analyst | Blue Team & Threat Detection Enthusiast

amritpanthi99@gmail.com | 647-200-2785 | Toronto, Ontario
LinkedIn: https://www.linkedin.com/in/amrit-panthi/
GitHub: https://github.com/AmritPanthi-99
Website: https://amritpanthi.com/

Professional Summary

SOC Analyst with hands-on experience in SIEM monitoring, alert triage, and incident investigation using Splunk, Sysmon, and network traffic analysis. Skilled in detecting brute-force attacks, suspicious authentication activity, and lateral movement through log correlation and endpoint telemetry. BTL1 certified with practical experience mapping threats to MITRE ATT&CK and responding to simulated real-world security incidents. Strong foundation in security operations workflows, escalation procedures, and threat detection.

Technical Skills

- **Security Operations:** SIEM Monitoring, Alert Triage, Incident Investigation, Log Correlation, Threat Detection, Incident Escalation, MITRE ATT&CK Mapping
- **Tools & Technologies:** Splunk, Wireshark, Sysmon, TCPDump, ELK Stack, Windows Event Logs, Linux Logs
- **Networking and Systems:** TCP/IP, DNS, HTTP/S, VPN, Active Directory Basics, Windows and Linux Environments
- **Scripting & Querying:** Basic Python for Log Parsing and Automation, Splunk SPL, Log Analysis Queries

Practical Projects / Home Lab Experience

- Built and configured a home SOC lab using Splunk, Sysmon, and Windows Event Logs to collect, monitor, and investigate security events.
- Investigated simulated security incidents, including brute-force attacks, unauthorized account access, suspicious PowerShell execution, and malware-related activity by analyzing logs and identifying indicators of compromise (IOCs).
- Analyzed network traffic using Wireshark to identify suspicious communications, insecure protocols, DNS activity, and potential credential exposure.
- Performed network reconnaissance and vulnerability assessments using Nmap to identify open ports, exposed services, and potential security weaknesses.
- Conducted phishing investigations by examining email headers, embedded links, attachments, and sender information to determine malicious intent.
- Created and tested custom Splunk searches and alert rules to detect failed logins, privilege escalation attempts, and anomalous user activity.
- Performed Windows endpoint investigations using Event Viewer and Sysmon logs to trace user activity, analyze security events, and reconstruct attack timelines.
- Applied MITRE ATT&CK and incident response methodologies to document findings, prioritize alerts, and simulate real-world SOC investigation workflows.

Professional Experience

Genese Solution, Kathmandu, Nepal

Pre-sales Associate **(May 2022 – Oct 2022)**

- Delivered technical product demonstrations and supported customers' onboarding, focusing on cloud-based (AWS, Azure, GCP, Huawei Cloud) and technical solutions.
- Assisted clients in understanding system workflows and resolving technical issues, strengthening communication of complex concepts.
- Collaborated with cross-functional teams to support solution implementation and customer success.
- Supported sales engineering efforts contributing to 95% client satisfaction across solution deployments.

F1Soft International Pvt. Ltd, Kathmandu, Nepal

Information Security Associate **(June 2021 – May 2022)**

- Assisted with vulnerability scanning and remediation tracking using security assessment tools.
- Reviewed Windows Event Logs, Sysmon logs, and SIEM alerts to identify suspicious activities and potential security incidents.
- Monitored and analyzed security events using SIEM and endpoint protection solutions to identify potential threats.
- Investigated phishing emails, malware alerts, and unauthorized access attempts, documenting findings and escalation actions.
- Assisted with user access reviews and security compliance assessments.
- Maintained incident records, security documentation, and remediation reports.
- Collaborated with IT teams to strengthen endpoint security and implement security best practices.

Softwarica College of IT and E-commerce, Kathmandu, Nepal

Security Operations Assistant **(Jan 2020 – May 2021)**

- Assisted in configuring and maintaining SIEM environments for security monitoring and threat detection activities.
- Assisted users and team members with security monitoring workflows, including alert triage and log analysis.
- Supported troubleshooting of security tools and environments, ensuring accurate log ingestion and alert visibility.
- Collaborated with teams to demonstrate practical use of cybersecurity tools for threat detection and monitoring.
- Documented security findings, alerts, and investigation results to support incident response activities.

Education

- **Post-Graduate in Project Management - IT** **(Jan 2023 – Aug 2024)**
  Lambton College, Toronto, Canada

- **Bachelor of Science with Honors in Computing** **(July 2018 – Feb 2022)**
  Softwarica College of IT and E-commerce, Kathmandu, Nepal

Training & Certifications

- Blue Team Level 1 (BTL1)
- Try HackMe - Security Operations Center (SOC) Level 1
- Google Cybersecurity Certificate (Linux, MySQL, Python hands-on labs)
- AWS Cloud Practitioner Essentials