ABHISHEK ASHOK

CYBERSECURITY ANALYST - Security Operations Center, Malware Analysis & Threat Hunting

abhishekashok14@gmail.com +1 (437) 982-9936 Toronto, Canada LinkedIn GitHub

SKILLS

- **SIEM & Security Monitoring**:Splunk, Microsoft Sentinel, Sumo Logic for alerts, analyzing security alerts.
- **Endpoint & Network Security**:SentinelOne, Defender, Wireshark, Nmap, Nessus,investigation, containment.
- **Security Operations & Incident Response**: SOC monitoring, incident lifecycle, forensics, malware analysis.
- **Threat Analysis & Adversary Techniques**:TTPs, attack chain, kill chain mapping,Burp Suite testing basics.
- **Cloud & Identity Security**: Azure, AWS, IAM, MFA, Zero Trust, Defender, cloud monitoring solutions.
- **Automation & Scripting**: Python for security automation, SQL for querying and correlation, PowerShell.

WORK EXPERIENCE

Cybersecurity Analyst - SOC **September 2023 – November 2024**
Mjolnir Security Inc *Ontario*

- Monitored and analyzed 5,000+ SIEM alerts daily across network, endpoint, and cloud security controls, identifying 250+ critical threats with complete scope evaluation metrics.
- Triaged over 400 security events monthly by analyzing logs, IOCs, and anomaly patterns, reducing false positives by 30% and improving escalation accuracy for Tier-1 SOC.
- Documented 350+ investigation findings systematically in incident management systems, ensuring precise knowledge transfer, audit trails, and escalation procedures for ongoing SOC operations.
- Resolved more than 200 Tier-1 security incidents per month by following SOC playbooks, standard operating procedures, and automated response workflows, ensuring continuous service uptime.
- Communicated 150+ security incidents weekly to clients, providing technical updates, detailed investigation summaries, and mitigation recommendations, ensuring timely and actionable response delivery.
- Maintained and updated SOC documentation across 25+ internal processes, improving internal knowledge base accuracy and streamlining response times for recurring incident types and anomalies.
- Applied MITRE ATTCK framework to map 100+ adversary TTPs, analyzing attack chains and supporting 50+ threat hunting operations, improving detection coverage across multiple network domains.
- Collaborated with 5 internal SOC teams and 3 cross-functional departments during active incidents, assisting containment, remediation, and system recovery workflows to reduce dwell time by 40%.

SOC Analyst **July 2021 – August 2022**
Trent Limited, FBSSL *Ontario*

- Monitored 3,500+ SIEM, IDS/IPS, firewall, and endpoint alerts weekly to identify potential threats and malicious activity, escalating confirmed threats with full investigative context.
- Conducted triage for over 300 low-severity incidents per month, analyzing phishing, malware, and suspicious user behaviors, reducing incident backlog by 25% and improving SOC efficiency metrics.
- Escalated 150+ confirmed security events monthly with detailed documentation, timeline mapping, and mitigation recommendations for Tier-2 review, improving incident handling consistency and accuracy.
- Analyzed 400+ network and authentication logs weekly to detect anomalous patterns, early-stage breaches, and lateral movement, enhancing threat detection coverage across enterprise systems.
- Guided in 24/7 SOC shift handovers and on-call rotations, ensuring continuous monitoring and immediate response to high-priority security events, reducing system exposure duration by 30%.
- Updated and maintained SOC playbooks by documenting common attack patterns, response procedures, and incident trends, optimizing response workflows and reducing investigation cycle time by 20%.
- Facilitated SOC operational tasks, including log correlation, event validation, and alert configuration adjustments, improving detection accuracy and minimizing false positive rates by 35% monthly.
- Influenced threat hunting and anomaly detection by integrating new correlation rules, analyzing historical events, and providing actionable insights, improving overall SOC defense readiness by 25%.

EDUCATION

Postgraduate Diploma in Cybersecurity & Wireless Networking September 2022 – December 2023
George Brown College, Toronto, Canada

Bachelor of Engineering in Information Technology August 2018 – May 2021
University of Mumbai, India

CERTIFICATIONS

- **CompTIA Security+**
- **EC-Council SOC Essentials S-CE**
- **ISC2 Certified in Cybersecurity**
- **Sumo Logic Certified**