AMIT BIRAJDAR

SECURITY OPERATIONS ANALYST - SIEM, EDR & LOG ANALYSIS

birajdaramit272@gmail.com +1 (226) 998-8141 Ontario LinkedIn

SKILLS

- **Security Operations & Threat Detection**: SIEM (QRadar, Splunk), EDR, IDS/IPS, Incident Triage
- **Network Security & Firewall Management**: Palo Alto, Fortinet, Cisco Firepower, VPN, VLANs, DNS
- **Digital Forensics & Scripting**: Wireshark (PCAP Analysis), PowerShell, Bash, Python (Automation)
- **Compliance & Frameworks**: MITRE ATT&CK, NIST 800-53, ISO 27001, OWASP, HIPAA, TCP/IP
- **Endpoint & System Management**: Windows Support, Patch Management, Asset Tracking, Ticketing System

WORK EXPERIENCE

Customs Broker Rep 1 **August 2022 – Present**
UPS SCS *Canada*

- Facilitated critical security alerts, including VPN anomalies, improving incident triage speed by 35%.
- Analyzed system logs to identify & remediate network irregularities, increasing troubleshooting accuracy by 30%.
- Resolved Tier 1 technical support issues across phone & remote tool, achieving 95% first-contact resolution rate.
- Configured and maintained over 70 devices with enterprise software, reducing setup time by 20%.
- Diagnosed 100+ Windows, VPN & access issues, enhancing user satisfaction through faster resolution.

Help Desk Support Rep **May 2019 – January 2021**
UPS Logistics Pvt. Ltd. *India*

- Deployed security patches and application updates, reducing system vulnerabilities and downtime incidents.
- Managed IT inventory of 500+ assets, ensuring hardware replacements & reducing repair turnaround time.
- Authored 10+ internal guide & user documentation, standardizing support protocol & improving issue resolution.
- Delivered email-based support for U.S. clients, cutting response time by 25% & increasing satisfaction scores.
- Collaborated across 3+ departments to reduce repeat support tickets by 15% through troubleshooting strategies.

Associate / User Support Technician **December 2019 – May 2020**
Wipro *India*

- Delivered phone & email support, maintaining a 95% customer satisfaction rate & resolving queries within SLA.
- Improved support procedures, reducing ticket escalations by 20% through knowledge base enhancements.
- Mentored 2 desktop refresh projects, minimizing business disruption and maintaining data continuity.
- Created and updated 15+ internal knowledge base articles to document recurring technical problems and fixes.
- Liaised with 4+ vendors for hardware repair & license renewal, reducing downtime & ensuring system compliance.

PROJECTS

Live SOC Monitoring (LetsDefend) *SOC Analyst*

- Monitored 100+ real-time alerts using SIEM tools, identifying suspicious login attempts and phishing activity.
- Conducted log analysis to trace 3+ malware execution paths, escalating confirmed threats for mitigation.

QRadar Log Integration & Threat Detection *SOC Analyst*

- Configured 10+ QRadar log sources & created custom detection rules to identify brute force & malicious activity.
- Reduced false positives by 25% through advanced log correlation techniques and optimized rule sets.

SOC Analyst Simulation (TryHackMe) *SOC Analyst*

- Investigated logs from 5+ Windows and Linux environments to detect intrusion attempts and malware infections.
- Leveraged 4+ SIEM & EDR tools to simulate workflows to phishing, ransomware, and data theft scenarios.

EDUCATION

Post Graduate in Supply Chain Management May 2021 – December 2021
Conestoga College, Brantford

Bachelor of Engineering in Electronics May 2012 – December 2016
Pune University, India

CERTIFICATIONS

- **Cisco Network Security , Qualys Policy Compliance**
- **ISC2 Certified in Cybersecurity (CC) , CompTIA A+**
- **Google Cybersecurity Certificate , Fortinet Certified Associate in Cybersecurity**
- **CompTIA Security+ , Microsoft SC-200: Security Operations Analyst** *(In Progress)*