Prikshit

IT CYBER SECURITY ANALYST – SIEM, Incident Response, Identity Management

✉ prikshitprikshit01@gmail.com ☎ +1 (902)-978-2225 Calgary in LinkedIn

SKILLS

- **Security Operations & Incident Response**: Event monitoring, mitigate threat, SIEM- Microsoft Sentinel.
- **Network & Endpoint Security**: LAN/WAN/Wi-Fi troubleshooting, Meraki familiarity, and SentinelOne.
- **Scripting & Automation**: Python scripting for tasks, automation of alerts, integration with ticketing systems.
- **Cloud and ITSM Tools**: Azure security operations, ServiceNow, Jira, Remedy, Helix, and QualysGuard.

WORK EXPERIENCE

IT Security Analyst **January 2023 – Present**
Buchanan Technology *Remote, Canada*

- Reduced security incident resolution time by 30% with real-time threat hunting using Sentinel, Defender, and SentinelOne; optimized incident triage and alert correlation, and incident routing via MITRE ATT&CK mapping.
- Engineered automation of access review reports for 250+ user accounts using PowerShell, and enabling stakeholders to address access control issues, while mitigating cross-privilege violations, and improving security audits.
- Orchestrated deep-dive forensic investigations on 90+ phishing and malware threats using sandboxing, packet analysis, and IOC correlation to enhance detection accuracy, containment workflows, and response timelines.
- Coordinated change control with Infrastructure teams, modifying 25+ firewall and ACL rules; applied NAT configurations and zone-based policies to minimize system exposure and strengthen segmentation across network.
- Developed 15+ policy documents with NIST 800-53 and PCI DSS, incorporating data classification & SIEM correlation procedures to streamline audit readiness by 40% and standardize procedural controls across operations.
- Executed vulnerability scans using QualysGuard across 600+ assets, remediating 15,000+ CVEs; applied threat intelligence feeds and CVSS scoring to improve risk metrics in weekly dashboards by 28% using security KPIs.

Team Lead IT Operations Analyst **February 2022 – December 2022**
Buchanan Technology *Charlottetown, PE*

- Directed teams handling 500+ monthly ticket escalations & prioritization, enabling timely issue resolution and increasing SLA compliance by 20% via structured workflows across security and technical service categories.
- Assessed technician performance trends via operational dashboards, contributing to a 25% boost in throughput and increasing service ticket handling capacity to over 1,200 tickets per quarter within assigned reporting periods.
- Directed management reports on backlog metrics and process gaps using Power BI, reducing aged tickets by 15% and improving incident life cycle visibility across more than 10 departments through root cause data analysis.

Network Analyst Associate **January 2021 – February 2022**
ABI System *Mississauga, ON*

- Formulated and configured 50+ routers, firewalls, and switches to secure enterprise network infrastructure and ensure 99.9% performance stability across interconnected office locations with consistent connectivity up time.
- Executed firmware upgrades, and patch installations on 100+ networking devices, improving hardware resilience by 35% and reducing downtime by 20% via standardized baseline configurations across all production systems.
- Deployed network fault isolation using diagnostic tools and root cause analysis, reducing issue recurrence by 40% while improving SLA compliance by 25% on time-sensitive infrastructure-related technical incidents.

PROJECT EXPERIENCE

Security Tools Migration
Cybersecurity Engineer, Buchanan Technologies

- Built migration of security tools across 3 platforms, reducing licensing costs by 18% and maintained 0 downtime.
- Liaised with interdepartmental teams to streamline workflows, reducing expenses by 22%, & improving efficiency.

Third-Party Gap Analysis
Cybersecurity Engineer, Buchanan Technologies

- Conducted 50+ third-party risk assessments during IPO, remediating 15 critical control gaps for compliance.
- Collaborated with cross-functional teams using RSA Archer to align controls, boosting audit readiness by 30%.

EDUCATION

Electromechanical Engineering in Automation and Robotics January 2018 – December 2019
Centennial College of Arts and Technology

CERTIFICATIONS

- **Cisco Certified Network Associate (CCNA), SC-900: Microsoft Security Fundamentals**
- **SC-200: Microsoft Security Operations Analyst, CompTIA Security+, CompTIA CySA+**
- **Pursuing: CRISC**