SHEILA DAY

Address | Phone | Email

CYBERSECURITY SPECIALIST

Analytical, solutions-focused, and self-driven professional with strong background as Cybersecurity Analyst supplemented by relevant skillset acquired through completed education and certification in cybersecurity and network technology. Manages and urgently addresses reports on cybersecurity attacks, analyzing firewall and system logs to validate threat and perform applicable incident response in alignment with security protocols. Remains up to date with emerging technology advancements to ensure effectiveness and efficiency of vulnerability assessments, network security tools, disaster recovery, and mitigation plans, elevating client experience. Seeking to apply relative experience, collaborative work ethic, and growth mindset into a new, challenging role to expand professional expertise.

CORE SKILLS & COMPETENCIES

- Cybersecurity Management
- Risk & Vulnerability Assessment
- Mitigation Planning & Strategy
- Incident Response & Reporting
- Security & Malware Analysis
- Preventative Maintenance
- Network & System Monitoring
- Client Communication
- Team Collaboration

Technical Acumen: Windows | Linux | IDS | IPS | Nessus | | Snort | Wireshark | Splunk | PowerShell | IBM QRadar | Microsoft Sentinel | Helix | EDR | Jira | Vulnerability Management | McAfee EPO

PROFESSIONAL EXPERIENCE

Cyber Security Analyst | Company | Location **Jul. 2022 – Present**

Works in a security operations centre as Tier 1 Analyst, responsible for addressing calls and reports on cybersecurity attacks, malicious malware, or security threats from 20+ organizations. Manages and ensures timely and efficient response to 1K+ of alerts a month, with key focus on reducing false positive reports.

- ✓ Improved incident response time through the introduction of automated responses, as well as efficiently utilizing and mastering threat hunting on EDR response tools, primarily Sentinel One.
- ✓ Configurated and updated client tools, including SIEMs and EDR, and refined/optimized security use cases from every organization, resulting to increased accuracy in threat detection.
- ✓ Recently participated in a hackathon organization with the company, gaining insightful experience from the opportunity and translating them into daily practice to improve workplace performance.

Key Responsibilities:

- ***Vulnerability Assessment:*** Utilizes SIEM tools, including IBM QRadar, Microsoft Sentinel, Helix, and Splunk, among others, to assess the threat based on specific use case, reviewing firewall, email, and system logs to validate if report is a malicious activity or confirmed breach. Takes appropriate action after thorough investigation in alignment with security guidelines.
- ***Incident Response:*** Directly notifies clients, through ticketing in Jira, email, or phone call, for any confirmed security breaches in the system, liaising with higher level analyst to work on next best steps to mitigate risks and impact in operations.
- ***Client Communication:*** Coordinates major security issues with utmost priority and provides tailored solutions to resolve current threat, managing entire process and supporting clients throughout the implementation.
- ***Preventative Maintenance:*** Identifies gaps and potential weaknesses, recommending proactive security measures to prevent risk while maintaining functionality and efficiency of existing security products and systems.
- ***Time Management:*** Ensures clear understanding of security threat, level of severity, and impact on business performance, in order to inform task prioritization and course plan of action for all reports. Employs investigative analysis to assess alarms and determine false positives from a valid threat, providing accurate incident response in a timely manner.
- ***Technology Integration:*** Maintains up to date knowledge of emerging technologies to ensure assessment strategy, security tools, and mitigation plans remain relevant and effective. Constantly pursues professional training and certification courses for newer platforms, gaining opportunity to directly work with sponsoring organization and learn of the best ways to implement solution.
- ***Work Culture:*** Innovative and possesses well-rounded skills gained through experience with a variety of use cases and current knowledge of new security technologies. Expands professional capabilities to ensure consistent delivery of accurate and timely incident response and disaster recovery plans, driving efficiency of organizational solutions while facilitating client success.

PROFESSIONAL EXPERIENCE (CONTINUED)

Shift Engineer | Company | Location **Mar. 2021 – Dec. 2021**

Ensured preventative maintenance measures for all pant equipment and input histories in a computer maintenance management system. Manages maximum energy efficiency, inspecting, operating, maintaining and repairing mechanical and electrical systems and equipment including boilers, chillers, HVAC equipment, pumps, generators etc.

Shift Engineer | Company | Location **Jul. 2019 – Mar. 2021**

Maintained accuracy, repairing and operating varied systems and utilities including oil and gas-fired boilers, chillers, water softeners, reverse osmosis treatment systems, air compressor and other related auxiliary equipment. Completed daily rounds of plant every 2 hours to guarantee smooth operation of equipment while recording observation. Responsible for reporting abnormalities to senior management before performing corrective maintenance.

EDUCATION

Diploma: Cybersecurity | Institute **2022**

Relevant Coursework: Hacker Tools, Techniques, & Incident Handling | Windows Forensic Analysis | Computers, Technology, & Security Introduction to Cyber Security | Cyber Threat Intelligence | Reverse-Engineering Malware | Cloud Security & DevSecOps Automation

Sampling of Skills Acquired:

- ***Security Concepts:*** Comprehensive understanding of TCP/IP protocol, security architecture, network and remote access security to techniques and products.
- ***Network Security:*** Set up and configured firewalls and other protective and detection systems to proactively ensure coordination and security. Monitored firewall logs to gather data, support incidents, and continuously improve security of network and devices.
- ***Risk Management:*** Utilized strategic approach to prioritize cyber threats, implementing cybersecurity risk management to ensure most critical threats were handled in a timely manner. Identified, evaluated, and addressed threats based on each potential impact.
- ***Vulnerability Management:*** Checked existing practices, security gaps and steps for continuous threat monitoring, focusing on advanced adversary simulation and penetration testing. Performed cyber vulnerabilities across endpoints, regular process of identifying, assessing, reporting and managing workloads and systems.

Key Projects Completed:

Vulnerability Scan

Successfully installed and configured nesses essentials to perform an efficient credentialed vulnerability scans against windows 10 hosts. Developed automated remediation process to pre-emptively deal with vulnerabilities from windows updates and third-party software.

Prevention/Detection System Development

Configured a system to determine types of incidents. Working within IDS and IPS to establish rules regarding types of incidents to detect and report.

Microsoft Sentinel

Configured Azure Sentinel workbook to display global attack data on world map, weighted according to physical location and magnitude of attack. Used customer power shell script to extract metadata, forwarding to third part API to derive geolocation data.

ADDITIONAL EDUCATION & CERTIFICATIONS

Diploma: Power Engineering | College **2019**

Cyber Defense Training

Network+

Security+