 **Cyber Security Analyst**

Naseeb Hoque | USA | Phone: 8562469067 | Email: nasibul215@gmail.com

**USA Citizen**

**Professional Summary:**

* Highly skilled and dedicated Cyber Security Analyst with a strong background in identifying and mitigating security vulnerabilities.
* Proven expertise in network security, incident response, and risk assessment.
* Working knowledge on cloud security engineering and administrating for SaaS, PaaS, and IaaS (including AWS and Azure)
* Committed to staying abreast of emerging threats and technologies to ensure robust cyber defenses.
* Experienced in developing and implementing incident response plans to effectively address security breaches and mitigate their impact. Capable of conducting thorough investigations, identifying the root cause, and implementing remediation measures.
* Competent in assessing organizational risks and vulnerabilities, conducting risk assessments, and developing risk management strategies. Skilled in identifying and prioritizing critical assets and establishing appropriate controls.
* Proficient in working with a range of security tools and technologies, such as vulnerability scanners, SIEM (Security Information and Event Management) systems, intrusion prevention systems, and antivirus software.
* Extensive experience in implementing and managing SIEM solutions, such as Splunk, Azure Sentinel, and Google Chronicle.
* Proficient in configuring correlation rules, alerts, and reports to identify and respond to security incidents.
* Strong knowledge of security event log analysis, threat intelligence, and incident response procedures.

**Key Skills:**

* **SIEM Platforms**: Splunk, Azure Sentinel, and Google Chronicle.
* **Log Management**: Logstash, Syslog, Windows Event Forwarding
* **Networking**: TCP/IP, VLANs, VPNs, Firewalls
* **Operating Systems**: Windows, Linux, MacOS
* **Scripting Languages**: Python, PowerShell, Bash

**Work History:**

**Datto- SOC analyst**

**April 2022 - Present**

**Responsibilities:**

* Utilized NIST 800-53A and NIST 800- 53 rev-4 to review implemented controls and enter information into the Requirements Traceability Matrix (RTM) and findings into the Security Assessment Report (SAR).
* Participated in audits and compliance reviews based on FISCAM, FISMA, NIST SP 800-53 series, ISO 27001, OMB circular A-123 and A-127 frameworks.
* Coordinated IT related SOX compliance reviews, assessing IT Application Controls in connection with program development, change management, computer operations, security and configurations as well as vendor service providers.
* Designed, implemented, and managed the company's SIEM solution, including architecture design, log source integration, and rule creation.
* Developed correlation rules and alerts to detect and respond to security incidents in real-time.
* Conducted log analysis and investigations to identify security events and potential threats.
* Collaborated with incident response team to define and improve incident response procedures.
* Monitored SIEM platform performance, fine-tuned configurations, and optimized system performance.
* Provided training and guidance to junior SIEM analysts and assisted in knowledge sharing.
* Collaborated with network and system administrators to ensure proper log collection and normalization.
* Assisted in incident response efforts, including containment, eradication, and recovery.
* Conducted vulnerability assessments and provided recommendations for remediation.
* Participated in security audits and compliance assessments, ensuring adherence to industry standards.
* Conducted regular network security assessments, identified vulnerabilities, and implemented appropriate countermeasures.
* Actively monitored and responded to activity impacting various enterprise endpoints facilitating network communication and data handling (McAfee End Point Security, DLP, Splunk)
* Data Loss Prevention suit, Symantec DLP Product - Implementation and deployment as the champion team.
* Design DLP architecture and handle Third Party Risk Assessment and Managed SOX audits
* Experience with Symantec DLP and RSA DLP architecture and implementation for enterprise level. Designed Symantec DLP architecture, implemented Symantec DLP. Worked with Symantec DLP upgrades and patches. Implemented Symantec DLP Policy and Content Blade creation and tuning. Provided input into customer's operational and processes and procedures.
* Monitored network traffic and performed real-time analysis to detect and respond to security incidents.
* Developed and maintained incident response plans, coordinating with cross-functional teams during security incidents.
* Performed log analysis using SIEM tools to identify and investigate security incidents.
* Developed and maintained correlation rules and reports to enhance threat detection capabilities.
* Entirely responsible to perform production changes/upgrades via informing to all responsible teams and stakeholders
* Involve in weekly and monthly meeting with other teams to review and discuss about upcoming production changes and policy modification

**America Tech**– **SOC analyst**

**Jun 2019- Apr 2022**

* Conducted real-time security event monitoring as a Tier 1 SOC2 Analyst utilizing Splunk and Azure Sentinel.
* Configured and monitored endpoint security technologies
* Investigated various APTs (Advanced Persistent Threats) to better understand common tactics, techniques, and procedures.
* Performed threat analysis to mitigating and managing all threats and risks to data.
* Participating in high priority vulnerability assessments from start to finish, scanning the client's environment (Windows/Linux servers, databases, and websites), using a SIEM software, troubleshooting with the client to resolve network and scan related issues, manually analyzing the results to remove false positives before creating and delivering a final report.
* Evaluate, assess, and certify hardware, and software products prior to use on any accredited information system or network.
* Produce threat reports and briefings by integrating open-source data, to provide situational awareness on current issues for senior leadership for potential policy updates.
* Implement effective cyber security plans to maintain the security of computer files against unauthorized modification, destruction, and disclosure.
* Performed open-source research to identify overall public-facing attack surface.
* Performing Cyber and Technical Threat Analyses
* Applied different pivoting tools and techniques to navigate a network.
* Knowledge of NIST SP 800-61r2 about an incident response plan.
* Using federated authentication and SSO redefines user identities and access to digital services
* Supporting and Managing Security Services
* Network and System Administration Experience
* Creating, Modifying, and Updating Security Information Event Management (SIEM) using Splunk

**Appex Learners LLC Feb Jan 2019– May 2019**

**SOC analyst intern**

**Responsibilities:**

* Design AWS Cloud Formation templates to create custom sized VPC, subnets, NAT to ensure successful deployment of Web applications and database templates.
* Involved in designing and developing Amazon EC2, Amazon S3, Amazon RDS, Amazon Elastic Load Balancing, Amazon SWF, Amazon SQS, and other services of the AWS infrastructure.
* Managed Security and Compliance Dashboard inside Office 365 Tenant.
* Reviewed security logs (LogRythm SEIM) to ensure compliance with policies and procedures and identifies potential anomalies.
* Integrated IDS/IPS to ArcSight ESM and analysed the logs to filter out False positives and add False negatives in to IDS/IPS rule set
* Well versed in both remote and on-site user Splunk (SIEM) Support
* Centralizing the storage and interpretation of logs using Splunk (SIEM) System
* Worked in Security Incident and Event Monitoring SIEM platform - IBM Qradar, and Splunk.
* Experience in SOC (Security Operation Center) to facilitate strong planning as per security protocol needed Analyse main Steps in IT Governance & Familiar with Cyber Security Process and ISO/NISI/ANSI Standard.
* Conduct risk assessments regularly; ensure measures raised in assessments were implemented in accordance with risk profile, and root-causes of risks were fully addressed following NIST 800-30 and NIST 800-37.
* Responsible for monitoring and detecting security incidents in Arcsight (SIEM).
* Develops rules, lists, and active channels in ArcSight ESM.
* Experience in SOC team delivery using security analysis, investigations, reporting, Mitigation, and tuning efforts.

**Certifications:**

EC Council CEH

CompTIA Security+

CompTIA Network+

CompTIA A+