****

**EXPERIENCE SUMMARY:**

Passionate SOC/IR Analyst with 3+ years of Experience in triaging, investigating, and preventing network, host and email-based attacks. Proficient in malware analysis, incident response, data loss prevention and improving SOC processes by utilizing top industry security solutions. Effortlessly adapt to various environments and workplaces. Operates well while working independently as well with team members. Self-motivated, goal-oriented, and customer-focused with excellent communication. Prioritize and manage multiple tasks concurrently. Troubleshoot and resolve complex issues in a demanding work environment quickly and efficiently.

**CERTIFICATION**

* AWS Certified Cloud Practitioner
* AWS Certified Solution Architect- Associate
* AWS Certified Security Specialty
* Certified Information Systems Security Professional- (CISSP)
* CompTIA Security Plus
* Splunk Fundamental 1
* Splunk Fundamental 2

**TECHNICAL EXPERIENCE**

* Malware Analysis/ Phishing Email Analysis/ Network Analysis
* Incident Response/Cyber Triage & Forensic
* Splunk/ Qradar
* Cloudflare/ Arbor/ Stealthwatch Cloud/ Sumo Logic
* Google Vault/McAfee DLP Manager
* Wireshark/ Moloch
* PCI-DSS/FIPS/NIST 800 Series
* Firepower/FireEye
* Carbon Black/Tanuim/ Microsoft Defender ATP, FireEye HX
* Sentinel One / Symantec Endpoint Protection
* Jira/ServiceNow/Resilient/Archer
* Bluecoat/ Cisco Umbrella/Zscaler
* •Palo Alto/Imperva/WAF/
* AWS Guard Duty / Azure Sentinel
* Linux/Windows/ Active Directory
* Archer/ServiceNow/Jira
* Microsoft Office 356 Security & Compliance, FireEye ETP, Cisco Ironport
* Thread grid/Cuckoo/ Any.run

**PROFESSIONAL EXPERIENCE**

**Ernst & Young 2/2021 – Present**

*Threat Detection and Response Analyst*

* Triage and investigate incoming alerts generated from Splunk ES to determine the severity and impact of the event or incidents.
* Give Client recommendations on how to resolve, remediate and
* Consistently monitor events generated on Splunk ES incident dashboard. Assist in creating Splunk dashboards to capture all customized logs generated by systems and applications.
* Investigate malicious embedded links, attachments obfuscated in phishing emails using Threat Grid, Ironport, O365 Threat explorer.
* Train employees how to handle phishing email cases and triage the phishing submission mailbox.
* Prioritizing and categorizing between potential intrusion attempts and false positives.
* Developing follow-up action plans to resolve reportable issues and communicating with other IT teams to address security threats and incidents accordingly
* Escalating incidents to Tier 2 and incident response analysts for further analysis
* Supporting Incident Response till resolution following Standard Operation Procedures (SOP)
* Assisting with the development of processes and procedures to improve incident response times, analysis of incidents, and overall SOC functions
* Responding to computer security incidents by collecting, analyzing, preserving digital evidence and ensuring that incidents are recorded and tracked in accordance with organizational SOC requirements
* Using McAfee DLP and Google Vault to protect intellectual property and ensuring compliance by safeguarding sensitive data
* Analyzing email logs to confirm malicious emails were not delivered or are quarantined
* and malicious attachments dropped.
* Monitoring and analyzing network traffic, Intrusion Detection Systems (IDS), security events and logs to identify abnormal and suspicious activity
* Working with SOC Engineers and other SMEs to operate Intrusion detection and prevention systems (IDS/IPS) such as SNORT and Sourcefire to analyze, detect worms and vulnerability exploit attempts
* Staying up to date with current vulnerabilities, attacks, and countermeasures

**Amazon 8/2017 – 2/2021**

*Security Operation Center (SOC) Analyst*

* Provided 24/7/365 real-time monitoring of security tools, dashboards, and email, network and malware alerts.
* Reported security incidents using ServiceNow ticketing system for events that become a declared incident and require Tier 3 Incident Response review.
* Performed triage on alerts by determining their criticality and scope of impact and root cause.
* Investigated, analyzed, and processed endpoint alerts using SIEM tools; CISCO FirePower, FireEye HX, Symantec End Point Protection, Carbon Black, Splunk Enterprise Security (Splunk ES) and OSINT tools.
* Triaged and investigated alerts coming from cloud endpoints such as AWS EC2, VPC, S3, CloudTrail, CloudWatch, GuardDuty and Security Hub.
* Reviewed and collected asset data; indicators of compromise, logs, configurations and running processes, on these systems for further investigation and reporting.
* Participated in planning and implementing preventative security measures and in building incident response and disaster recovery plans.
* Investigated, analyzed, and processed retrospective and reported phishing email alerts from IronPort and followed standard operating procedures as stated in the playbook. Used O365 Threat Explorer to analyze, scope and determine the recipients of the phishing emails withing the organization.
* Evaluated and processed Web Site Review Requests from internal users to access blocked websites using OSINT tools.
* Analyze and resolved DLP alerts from McAfee DLP Manager and Splunk Enterprise Security (Splunk ES) and escalated cyber privacy incidents to the Privacy Team.
* Worked incidents from initial assignment to final resolution.
* Assisted in building SOPs as needed or directed to facilitate SOC operations and processes.
* Fully documented assigned tickets to show all work performed and attach the required artifacts in order to pass SLRs.
* Performed Root Cause Analysis (RCA) and make preventative recommendations for incidents and events.
* Conducted forensics and investigations as needed using security tools such as Threat grid, Carbon Black Splunk, FireEye, Cisco IPS, OSINT, etc.
* Identified potential, successful, and unsuccessful intrusion attempts and compromises through reviews and analysis of security tools
* Created, tracked, and worked to resolution Normal and Standard job-related Change Requests
* Assisted with the creation of the daily SOC report and Shift reports and pass down emails to the incoming shift members
* Participated in daily security meetings with team members and customer teams.

**Amazon Web Services 10/2017 – 8/2018**

*InfraOps Support Engineer*

* Point of Contact for over 28,000 sever/network racks and over half a million customer instances for AWS data centers and their service owners.
* Knowledgeable in AWS Services: Ec2, , EFS, VPC, RDS, S3, Glacier, IAM,, CloudFront, Cloud Watch, Cloud Trail, Cloud Formation, DynamoDB, Route53, SNS, SQS, API Gateway
* Performed break\fix work in multiple clusters within the region.
* Provided deep level Linux diagnostics, Cisco/Junos/EPMS/BMS diagnostics and remediation. Advised hardware engineers with risk assessments to help mitigate potential future security vulnerabilities.
* On-call technician for multiple data centers. Work and meet SLA’s against assigned trouble tickets via a directed workflow. First line touch point for hardware troubleshooting and technical issues.
* Performed regular server hardware repairs (GPUs, CPUs, PDBs, drives, motherboards etc.)
* Performed fiber testing and troubleshooting on newly implemented proprietary fiber technology.
* Performed break\fix work on different server types and models in high temperature environments.
* Provided subject matter expertise on two site-wide power issues affecting thousands of customers to remedy major communication blockers and to customers.
* Proficient in Server Booting: POST, BIOS, PXE, GRUB/LILO, RAID
* Repaired virtual host, data base, production, and data sensitive priority devices.
* Performed installations and replacements of routers and switches in SLA based tickets.
* Proficient in network troubleshooting and repairs to include port security issues, reload and wipes, and configuration issues.

**Data Center Physical Security Area Supervisor - Command Security, Manassas 9/2015 – 10/2017**

* Provided assistance to customers, employees, and visitors in a courteous and professional manner
* Monitored alarms and electronic security systems
* Tracked employee time and attendance and help create training modules for new hires.
* Document significant incidents and facilitate in incident response efforts
* Enforce rules, regulations, policies, procedures, and respond to emergency situations requiring security assistance
* Tracked the progress of security patrols
* Initiated notification and escalation procedures on all security related incidents
* Responded to client requests and perform primary analysis on operational procedures

**EDUCATION**

**George Mason University 12/2023**

Bachelor of Science, Information Technology and Systems

**Northern Virginia Community College, VA**

Associates of Science, Information Technology