Career Objective

I am having 5 years of experience in IT domain. Professional and skilled Security Engineer with 4.8+ years of experience in security technologies efficiently in a demanding and dynamic work environment with skills of Incident Handling and Response management. Certified SECEON OTM Artificial Intelligence SIEM, Qualys Certified Professional, Fortinet Threat Landscape Certified Professional NSE-01, Cyber Security Threats U.S. Department of Homeland Security and ICSI | Certified Network Security Specialist professional with knowledge of various security products. Possess good communication and customer service skills. Ability to work under pressure, in adverse settings and fix emergency issues. Enthusiastic and hardworking with good critical thinking and interpersonal skills.

Seeking a challenging position as a Sr. Security Analyst role in IT Information Security domain which utilizes technical expertise, leadership and analytical skills to drive organizational performance.

Skills

|  |  |  |
| --- | --- | --- |
| * Customer Service Management | * Decoy Tool - Smokescreen |  |
| * Security Operations Center (SOC) | * CCNA |  |
| * Incident tracking and Monitoring | * WAF – Imperva By Redware |  |
| * Vulnerability Assessment | * Antivirus/EDR – Crowdstrike |  |
| * SIEM – HP ArcSight, Qradar, Seceon | * Gateway- Office365 |  |
| * Threat Detection - IDS/IPS |  |  |

Tool Inventory Knowledge

* **Antivirus/Security:** Crowdstrike
* **SIEM:** HP ArcSight, Qradar, Seceon
* **EDR:** CrowdStrike
* **Mail Gateway:** Office365
* **Monitoring Tools:** Observium
* **Service desk and Ticketing tool:** Archer, ServiceNow (SecOps)
* **Packet Analysis –** Wireshark

Professional Experience

**Sr. Security Analyst, Cyber Security, Jan 2020 to Till Date**

**Tech Mahindra, (Pune)**

**Key Responsibilities:**

* Preparing Daily Incident report and attending huddle call with client on daily basis
* Analyzing Qradar alerts and escalating to Onshore team if required.
* Fine tuning of Alerts in Qradar and suggesting new Use cases.
* Analyzing Crowdstrike alerts and escalating to Onshore team if required.
* Analyzing Spam emails reported by the user on O365.
* Working and tracking of IoCs sent by TechM Team.
* Preparing MSSP/MSR Reports on weekly and monthly basis respectively for client.
* Regular performance review of L1 resources through Ticket Audits on weekly basis.
* Received **BRAVO** as a token of appreciation.

**Sr. Security Analyst, Cyber Security, April 2019 to Jan 2020**

**Tata Com Limited, (Pune)**

**Project: UBI – UNION BANK OF INDIA (Apr 2019 to Jan 2020)**

**Key Responsibilities:**

* Planning, scheduling, running and mitigating vulnerability and configuration scans in accordance with direction of Client HOD using tool Qualys Guard.
* Preparing vulnerability reports and sharing to the stakeholders for fixing and patching.
* Documents all issues and assists in their resolution.
* Monitoring the incoming mails and releasing as per the client requirements using O365.

**Cyber Security Engineer (Incident Handling), Sept 2016 to Apr 2019**

**Paladion Networks, (Navi Mumbai)**

**Highlights:**

* Worked efficiently in a demanding and dynamic work environment; oversaw incident management on internal and external NHAI (National Highway Authorization Of INDIA) network and guided SOC team to resolve issues in compliance with organizations security and IT policies.
* Monitoring NHAI domains/websites for brand abuse and malware. Managing DDOS alerts sent by Airtel and TATA ISPs. Diligent monitoring of alerts from ArcSight, SmokeScreen and NMS dashboards.

**Key Responsibilities:**

* Preparing Daily Incident report and huddle call with client on daily basis
* Fine tuning of Alerts in Arcsight for whitelisting the false positives in our environment.
* Analyzing all AD and proxy logs connecting towards malicious domains.
* Monitoring ArcSight, Smokescreen dashboard for malicious activities with detailed analysis and taking respective actions.
* Monitoring Smokscreen dashboard and raising and reviewing incidents.
* Maintaining iZoologic and Zerofox for brand abuse.
* Taking preventive actions for the network anomaly alerts through Lancope(Stealth Watch)
* Raising artifacts for change management as per the requirement.
* Preparing Runbook/SOPs for various incidents and use cases monitored in ArcSight.
* Working and tracking of IoCs sent by Paladion Team and sharing reports to SEBI
* Provided regular status updates on issues and MIS reports to Project Manager.
* Received **Award for Handling Challenging Client - NHAI project.**

Education

**MDIMART University of Pune**Master of Computer Applications (Information Technology) (June 2015)

Professional Development

**CERTIFICATIONS:**

* **Nov 2019:** Certified SECEON OTM Artificial Intelligence SIEM
* **Aug 2019:** Qualys Certified Professional
* **Aug 2020:** Cyber Security Threats U.S. Department of Homeland Security
* **June 2020:** ICSI | Certified Network Security Specialist professional [International Cyber Security Institute]
* **July 2020:** CYBER ARK Security Professional Certified

**TRAINING COURSES AND WORKSHOPS:**

* **July 2016** Cisco Certified Network Associate Security (CCNA Security)
* **July 2016:** Juniper Networks Certifies Associate (JNCIA)

Personal Information

* **Nationality:** Indian
* **Date of Birth:**04/02/1992
* **Passport No:** U2120945
* **Marital Status:** Married
* **Language:** Fluent in English, Hindi, and Marathi