**Jaimin Soni**

**667-425-2440**

**jayminsoni7252@gmail.com**

**Summary:**

* Experience in Cyber security domain for 8+ Years in SOC Analyst, Security Automation, Network Security, IAM, Risk management, Incident Response, Malware detection and System Administrator.
* Work in Threat Intelligence and Threat Hunting using STRIDE, MITRE ATT&CK, MISP and Threat connect for proactively searching incidents through IoC, TTPs.
* Experience Deploying Security controls such as McAfee, Symantec, ESET Antivirus & DLP and WSUS.
* Worked on Network security environment using Nmap, Nessus, Wireshark, Netcat, tcpdump, Metasploit, Aircrack-ng, NextGen Firewall, Snort, CloudFlare.
* Worked on Identity Access Management solution such as Okta, AWS IAM, MS Active directory, CyberArk, Oauth, OpenID, MFA, Tokens, SAML.
* Awareness of computing and OS infrastructures Windows 10/11, Kali Linux, MS Server 2012/2016, Ubuntu, Mac, VMWare, Microsoft Hyper-V.
* Having knowledge in Social engineering Techniques for Phishing campaign, User Awareness using GoPhish, Maltego, OSINT, SET.
* Triage and remediate Internal, external threats using Splunk ES, IBM Qradar, Cortex, crowdstrike falcon, MS defender.
* Stay up to date of Cyber breaches and threats through SANS threat Intel, Alient Vault OTX, DarkReading, threatpost and HackerNews.
* Knowledge on Red Teaming techniques and procedure, worked in authorized ethical hacking task for assessment purpose such as wifi password cracking, Phishing emails, Testing Web-site cracking, Internal Employee Social engineering.

**Skills & Tools**

TECHNICAL: Threat Intelligence, Risk Assessment, Vulnerability management, IAM, Cloud security, Incident Response, Palo Alto XSOAR, Splunk SIEM, Nessus, Nmap, Wireshark, Crowdstrike XDR, SentinelOne, Snort IDS, Cisco ASA, PCI DSS, NIST, ISO 27001, MITRE ATT&CK, Cyber kill chain, Ethical Hacking, AWS, Java, linux, Bash shell, cmd.

#

# Education & Certification

# Comptia Security +

# Bachelor of Science: Information Technology | Parul University, India 2016

# Professional Experience

**Paychex Rochester, NY Nov 2022 to till date**

**Cyber Security Analyst**

**Responsibilities:**

* Working as a SOC Tier-3 to Perform forensic analysis of security logs to Identified and resolved high severity and critical threats Zero-day, phishing, Credentials, Privilege escalation and reducing response time by 30%.
* Design, create, and update Incident response **playbooks** that outline the sequence of automated actions to be taken in response to specific security incidents.
* Guided to Junior security analysts to assist in development of **IOC** for active defensive countermeasures and passive detection signatures.
* Worked on **Cortex XSOAR** to automate 50% repetitive incident tasks and implement dynamic playbook branching to ensure workflow adapt.
* Integrated **Cortex XSOAR** with other security tools **Splunk ES**, **Crowstrike Falcon**, **Sentinelone** and AutoFocus Threat intelligence.
* worked in email security DMARC, DKIM, SPF in enterprise using Mimecast platform.
* Developed **Python** scripts to automate the enrichment of various IoCs using external threat intel feeds(**MITRE ATT&CK**).
* Wrote complex SPL within Splunk ES to correlate and analyze security event data, including system logs, network traffic and endpoint activity.
* Conducted **Vulnerabilities** assessment to assess the security posture of systems and network against NIST 800-53.
* Leveraged infrastructure as code tool **AWS** cloudFormation and terraform to automate deployment of secure cloud resources.
* Developed Incident response procedure for **AWS**, utilized tools like AWS cloudtrail and Amazon detective for forensic analysis.
* Participated in Threat hunting activities for proactive hunting for hidden threats using splunk, crowdstrike falcon and **MITRE att&ck**.
* Strong knowledge in **IAM Okta** Technology for enterprise and client credentials.
* Maintained compliance with **NIST 800-53**, **PCI DSS** frameworks, supporting audit readiness.
* Conducted security awareness training for 230+ Employees and 10 Stakeholders, reducing phishing incidents by 30%.

**Bath and Body works, Remote Nov 2021 – Nov 2022**

**IT Security Analyst**

**Responsibilities:**

* Managed analysis efforts within the SOC environment, leveraging **McAfee** security products to classify security events and incidents
* Monitor and manage network traffic for anomalies and threats using advanced solutions like Splunk, Wireshark, tcpdump and SolarWinds NPM.
* worked on data protection policies using encryption tools like **BitLocker**, VeraCrypt, and **Symantec** Encryption to ensure sensitive data is securely stored and transmitted.
* Addressed **WannaCry** behavior on network endpoints, guiding prompt isolation and patching to mitigate 80% of potential threats
* Deployed and manage VPN solutions such as **Cisco AnyConnect**, **OpenVPN** for secure remote access, ensuring compliance with security policies.
* Implemented and enforce network access controls and security policies using Cisco Identity Services Engine (ISE), ClearPass, and **Active Directory**.
* Continuously monitor and analyze various sources, including open-source intelligence, dark web forums, and industry-specific reports, to identify potential threats and vulnerabilities.
* Implemented network segmentation and micro-segmentation strategies using tools like **VMware NSX** and Cisco ACI.
* Developed security policies and procedures tailored to OT environments, aligning with NIST and ISO 27001 standards.
* Ensure the integrity of the network infrastructure through routine patch management and updates using Ansible, Puppet, and Chef for automated network security configuration.

**SunTrust Bank, Remote Feb 2021 – Oct 2021**

**Cloud Security Engineer**

**Responsibilities:**

* As an Identity and Access Management Specialist at AWS services, I specialize in guidance around managing and securing access to AWS resources for organizations of all sizes.
* Responding to threats and remediating findings detected by Amazon GuardDuty, Security Hub , Inspector, Audit Manager, Splunk cloud.
* Applied network security measures like **NACL**s, VPNs, and AWS PrivateLink to protect sensitive data and resources.
* Set up and manage **VPC**s (Virtual Private Clouds), subnets, route tables, and security groups to create secure and isolated network environments
* Utilized **AWS** services such as EC2, S3, RDS, Lambda, IAM, VPC, CloudFormation, and CloudWatch to meet business requirements
* As a security specialist, work in OWASP top vulnerabilities like, SQL Injection, XSS scripting, and other injection attacks, to help developer to write a code secure way. And provide some security related guidance.
* Familiarity with the **NIST** Risk Management Framework process and DOD Information Assurance Vulnerability Management program
* Ensured AWS compliance with frameworks like CIS and PCI DSS, automating audits with AWS Config and Security Hub.
* Reduced **IAM** misconfig by 40% enforce least privilege policies and implement MFA for critical accounts.
* Work with developer team to gather requirement of product and report to in case vulnerability find into product by fuzz testing and OAWSAP ZAP tool.
* Drove threat hunting initiatives from scouring the network environment for indicators of compromise (IOCs) and suspicious activities.
* Incorporate **MITRE ATT&CK** into incident response playbooks to ensure a comprehensive and standardized approach to handling security incidents.
* Deployed AWS shield advanced and **WAF** to mitigate DDoS and Web application attacks, resulting in zero downtime during peak attack periods.

**Honor Health, Scottsdale, AZ July 2019 to Jan 2021**

**SOC Analyst**

**Responsibilities:**

* As a team member at an HH, managed information security at a **24x7 SOC**, reviewed logs, scripting tasks or created structured queries and threat intelligence and management for leading internet service provider with 40+servers, 300+ desktops and 850+ end-users and documented formal reports to demonstrate weekly and monthly metrics.
* Designed and implemented automated workflows using **Cortex XSOAR** playbooks to streamline incident response processes.
* Developed an enrichment playbook that scores IoCs from sources like **Recorded Future** and **OpenCTI**, enabling prioritization in Splunk dashboards.
* Monitored and analyzed security events using SIEM tools, identifying and responding to potential security incidents.
* Implement and manage automated processes in **RSA Archer** for risk assessments, regulatory compliance tracking, and issue management.
* Integrate **RSA Archer** with other systems, such as **SIEM** and vulnerability management tools, for comprehensive risk analysis.
* Supported the deployment and configuration of encryption solutions to protect sensitive data across **IoT** and **OT** systems.
* Develop and disseminate **IoC**s, such as malware signatures, IP addresses, and domain names associated with known threats. This information is used to enhance detection and prevention capabilities.
* Incorporate MITRE ATT&CK into incident response playbooks to ensure a comprehensive and standardized approach to handling security incidents.
* Monitored service availability using tools to perform weekly audits, maintaining a 99.9% uptime for critical systems.
* Strong knolwdge in azure cloud services such as Databricks, Azure AD, Azure VPN, Azure VM.
* Employed automatic updates and guided 375 employees on cyber security best practices, and phishing simulations, reducing the risk of attacks by 27%
* Automated **malware** analysis by integrating **Cortex XSOAR** with VirusTotal, CrowdStrike, and Splunk, reducing triage time by 60%.
* Conducted regular performance tuning and benchmarking of Snort sensors to ensure optimal performance and scalability in high-traffic network environments.

**Marlabs, India Nov 2016 to May 2019**

**Network Engineer**

Responsibilities:

* Support deployment and maintenance of physical and virtual IT infrastructure, including servers, desktop and laptop computers, switches, firewall/routers, WAP, etc.
* Experience in Cisco switch configuration and management, Microsoft Server 2008 R2 - 2019, Windows 10, VMware ESXi and SAN technology.
* Responded to requests for technical assistance in person, via phone, via email for mentor help Desk team members and assist as needed, diagnose and resolve technical Network and Software issues.
* Configured all the required devices and equipment for remote vendors at various sites and plants.
* Worked on various Network protocols and it`s platform TCP/IP, IPv4,IPv6 SSH, Telnet ,VLAN, FTP so on.
* Created Standard Operating Procedures to transfer tasks from Engineering to Network Operations.
* Implement Quality of Service (QoS) and traffic management techniques to prioritize critical applications and services.
* Experience implementing WAN/MAN technologies including: T1, DS3, OC3, OC12, OC48, OC192, Metro-Ethernet, DWDM.
* Configuring standards and extended ACLs on Enterprise Routers.
* Documentation of network via VISIO and using Cisco packet tracer tool creating network topology best suites and troubleshooting network issue logically and connecting vendor, users network devices using Putty for resolve issues.
* Proficient in diagnosing issues such as DHCP IP assigned, DNS resolution failure, VLAN misconfigurations and routing problems.
* Installing and mouting over 100 Cisco access points within enterprise using SecureCRT/PuTTy.
* Helped maintain firewall rule sets(ACL`s) and VPN configuration to ensure network security.
* In-depth expertise in the implementation of analysis, optimization, troubleshooting and documentation of LAN/WAN networking systems.
* Maintaining, updating and upgrading firewall devices and their software according to the business needs.
* Expert level knowledge and experience with several key technologies like Routing, Switching, SD-WAN, wireless, firewalls and load balancers.
* with F5 load balancers to troubleshoot LTM, GTM, certificate and VIP based issues.
* Troubleshooting the Network Routing protocols BGP, MPLS EIGRP, and RIP during the Migrations and new client connections.
* Set up and maintain routers, switches, and wireless controllers to work with Cisco ISE for secure network access authentication and authorization.