**Harivardhan M**

**732-702-2681**

[**Harivardhan821@gmail.com**](mailto:Harivardhan821@gmail.com)

**Cyber Security Analyst/Consultant**

**Professional profile**

* Garnered over 9+ years of professional experience in the realm of Cybersecurity, with a specialized focus on Security Operations.
* Demonstrates a keen ability to independently grasp new technologies by leveraging accessible documentation and proactive engagement with vendors.
* Extensive background in collaborating and communicating effectively across multifaceted IT teams, encompassing networks, systems, databases, applications, and security, to strategize and oversee impactful security operations.
* Proficient in hands-on utilization of Security Information and Event Management tools such as IBM Q-Radar, Azure Sentinel, and Splunk. Capable of tasks including onboarding log sources, crafting reports and dashboards, and developing customized parsers and correlation rules.
* Mastery of advanced skills such as Threat Hunting and Malware Analysis.
* Well-versed in regulatory compliance frameworks such as PCI-DSS and ISO 27001.
* Possesses unwavering analytical and problem-solving acumen crucial for the effective execution of responsibilities in the role of a SOC analyst
* Execute Nessus vulnerability scans and Nessus agent scans
* Performed scan policy analysis & configuration to determine the impact of vulnerability scanning against target devices
* Designs, develops, engineers, and implements Tenable.sc solutions that meet security requirements following DISA requirements
* Performed and reviewed technical security assessments of Tenable.sc and Trellix ESS server to identify points of vulnerability and non-compliance with established information security standards and recommend mitigation strategies.
* Troubleshoot credential failure issues by performing configuration analysis against the target device
* Check McAfee Data Loss Prevention -DLP Console for unauthorized Personal Identifiable
* Information –PII leaving the network
* Examine spam/phishing emails to hosts and identify threats
* Conduct incident handling procedures and provided remediation solutions to eliminate vulnerabilities, viruses, malware, and possible system compromises
* Review daily log data gathered from various resources such as sensors alert logs, firewall logs, content filtering logs
* Respond to new threats; initiate and assist in drafting remediation strategies
* Monitored Intrusion Detections Systems (IDS) console for active alerts and determine priority of response
* Monitor Security Intrusion Prevention -IPS activities include detecting and reporting malicious network traffic and false positive reduction
* Analyze all level of problems and document findings in accordance with procedures
* Identify possible intrusion attempts or other anomalies
* Identify and document newly discovered vulnerabilities and exploits along with providing diagnosis and remediation and suggestions for mitigation
* Conduct vulnerability analysis, research and collaborate with system administrators to mitigate identified vulnerabilities and/or author Plans of Actions and Milestones (PO&AM) as needed.

**TECHNICAL SKILLS**

**Continuous Monitoring:** Vulnerability Management, Web Application Scanning, Threat Protect, Policy Compliance, Cloud Agents, Asset Management, Governance, Risk Management and Compliance, Source fire, Nexpose, Force point, Rapid7

**Event Management:** RSA Archer, Blue Coat Proxy, Splunk, Net Witness, Tenable SC, Log Rhythm, HP Arc sight

Endpoint Protections: Symantec, McAfee, Bit9, Tanium, Crowd Strike, Cylance, Splunk

**Vulnerability Management** McAfee MVM, Tenable Nessus, Tripwire IP360, Rapid7 Nexpose, Qualys, IBM App Scan, HP Web Inspect

**Pen Test Tools:** Rapid 7, Burp Suite, Encase, Metasploit, NMAP, Wire shark and Kali

**DLP:** McAfee, Symantec, MS Office 365

**Frameworks:** NIST SP 800-171, ISO 27001/31000, HIPPA, HITRUST CSF, PCI DSS

**Firewalls:** Check Point, ISA 2004/2006, Palo Alto PA 3000/5000

**Routing:** OSPF, EIGRP, BGP, RIP-2, PBR, Route Filtering, Redistribution, Summarization, Static Routing

**Switching:** VLAN, VTP, STP, PVST+, RPVST+, Inter VLAN routing & Multi-Layer Switching, Multicast operations, Layer3 Switches, Ether channels, Transparent Bridging

**Protocols:** TCP/IP, L2TP, PPTP, IPSEC, IKE, SSL, SSH, UDP, DHCP, DNS, SSL, TLS

**Security Standards:** NIST, PCI-DSS, HIPPA, SOX and ISO standards (ISO 27001)

**PROFESSIONAL HISTORY**

**Sr Cyber Security Engineer**

**Lowes, Mooresville, NC October 2023 to Present**

**Responsibilities:**

* Install, monitor, test, troubleshoot, and administer ACAS/Nessus Vulnerability Scanner applications on classified and unclassified networks.
* Provides technical support to different teams involving a wide range of software, hardware, and DoD specific applications with respect to the ACAS solutions
* Analyzed and assist in the application of (STIGs) and (IAVAs)
* Ensure scheduled scans are covering 100% of intended assets and scans are being run successfully
* Troubleshoot scan problems related to Tenable.sc and Nessus tools
* Ensure Security Center is being updated regularly; addresses unsuccessful updates of the SC Configure, optimize, and test vulnerability scans against new and existing Operating Systems and platforms
* Execute Nessus vulnerability scans and Nessus agent scans
* Performed scan policy analysis & configuration to determine the impact of vulnerability scanning against target devices
* Designs, develops, engineers, and implements Tenable.sc solutions that meet security requirements following DISA requirements
* Performed and reviewed technical security assessments of Tenable.sc and Trellix ESS server to identify points of vulnerability and non-compliance with established information security standards and recommend mitigation strategies.
* Troubleshoot credential failure issues by performing configuration analysis against the target device
* Conduct vulnerability analysis, research and collaborate with system administrators to mitigate identified vulnerabilities and/or author Plans of Actions and Milestones (PO&AM) as needed
* Configure, operate, and maintain Trellix Server and its software modules; Trellix Agent, Data Loss Prevention, Host Intrusion Prevention System, Policy Auditor, ESS, Baseline Monitor, and Solid Core on Windows and Linux platforms.
* Perform troubleshooting of local and remote installation of Trellix ESS components and deployments of HBSS products and policies
* Create, deploy, and manage custom HBSS signatures Monitor HBSS software to ensure that the clients/servers are operational and reporting properly
* Install updates to McAfee software as released and in compliance with STIG requirements
* Deploy, maintain, and tune Trellix HBSS products so that clients meet current and future standards
* Provide guidance on vulnerability and malware remediation
* Monitoring, analyzing, detecting, and responding to Cyber events and incidents within information systems and networks
* Manage, monitor and support of Red Seal application for the agency
* Applied leading theories and concepts to development, maintenance and implementation of information security standards, procedures and guidelines.

**Senior Consultant -Cyber Security Engineer**

**Centene Corporation St Louis, Missouri May 2021 to September 2023**

**Responsibilities:**

* Responsible for Vulnerability Management and Remediation using Tenable Nessus vulnerability application
* Assist clients with improving the security posture of their deployed systems and addressing challenges with system configuration, patching, administration, and sustainment
* Identify security risks, threats, and vulnerabilities of client's networks, systems, applications, and new technology initiatives using the of best-of-breed SIEM tools, including Nessus, McAfee.
* Install, Upgrade and Manage host-based security system (HBSS) ePolicy Orchestrator (ePO) server administration and maintenance
* Analyze policies for Host Intrusion Prevention Systems firewall, application whitelisting, and intrusion prevention exclusions
* Provide expert oversight in the development, testing, and operation of firewalls, intrusion detection systems, enterprise anti-virus systems, and software deployment tools
* Conduct complex security architecture analysis to evaluate and mitigate issues and perform product evaluations, recommendations, and implementations of products and services for network security
* Validate and test security architecture and design solutions to produce detailed engineering specifications with recommended vendor technologies
* Interact with clients and provide recommendations on information assurance engineering standards, implementation dependencies, and the impact of changing information assurance related technologies
* Assess the impact caused by theft, destruction, alteration, or denial of access to critical information and services on the client's Network
* Define and developed an installation and usage documentation for McAfee ePO server
* Update cisco defense center signature files weekly.
* Determined areas for improvement and implemented processes to alleviate problems.
* Analyzed problematic areas to provide recommendations and solutions.
* Monitored technology use and program functionality, updating programs and making changes to enhance output.

**Information Security Analyst**

**Amway Corp ADA, MI November 2018 to April 2021**

**Responsibilities:**

* Analyzed potential malicious network traffic using tools (Splunk Console, Blue Coat Reporter, and McAfee ePO, Defence Center, Net witness, FireEye and Malila)
* Perform historic traffic queries and log analysis to identify malicious activity
* Use malware analysis tools to aide in identifying intrusion attempts, exploits, malware payloads and malicious activity
* Collaborate with the Intrusion Prevention Engineers to update and create active channels and custom signatures
* Check McAfee Data Loss Prevention -DLP Console for unauthorized Personal Identifiable
* Information –PII leaving the network
* Examine spam/phishing emails to hosts and identify threats
* Conduct incident handling procedures and provided remediation solutions to eliminate vulnerabilities, viruses, malware, and possible system compromises
* Review daily log data gathered from various resources such as sensors alert logs, firewall logs, content filtering logs
* Respond to new threats; initiate and assist in drafting remediation strategies
* Monitored Intrusion Detections Systems (IDS) console for active alerts and determine priority of response
* Monitor Security Intrusion Prevention -IPS activities include detecting and reporting malicious network traffic and false positive reduction
* Analyze all level of problems and document findings in accordance with procedures
* Identify possible intrusion attempts or other anomalies
* Identify and document newly discovered vulnerabilities and exploits along with providing diagnosis and remediation and suggestions for mitigation
* Filter all normal network traffic for enhanced reporting accuracy
* Summit's malware samples to anti-virus vendors such as McAfee, Sophos and Kaspersky
* Open service now tickets and report any malicious network traffic payloads and escalate them for remediation
* Assist fellow analysts in researching, generating reports, and diagnosing tickets and projects as assigned by the remediation team and engineers
* Produce reports, investigation, critiques on security related incident.
* Analyzed network traffic and system logs to detect malicious activities.
* Worked with other teams to enforce security of applications and systems.
* Implemented security measures to reduce threats and damage related to cyber-attacks.
* Investigated and resolved incidents of unauthorized access to sensitive information.

**System Engineer**

**Dhruvsoft Services Private Limited, Hyderabad, India April 2016 to August 2018**

**Responsibilities:**

* Facilitate authorized user network and service access by providing initial technical support for security, networking and occasionally telecom
* Follows pre-defined processes and procedures for troubleshooting, notes deficiencies in processes and procedures, and escalates as needed
* Generates metrics/reports on effectiveness of controls and investigate attempted efforts to compromise security protocols and escalate issues to higher level associates
* Provided wide range of troubleshooting that include but not limited to company property software's such as cisco NAC, checkpoint VPN and Symantec PKI client
* Provided initial support for the preventative, detective and educational IT Security controls
* Security controls includes malware detection/prevention, network access controls, network and application layer firewalls, virtual private networks, E-mail spam and virus filtering, web browser proxy filtering, endpoint protection, remote access and two-factor authentication, security awareness provisioning and training
* Reports malicious network traffic to be remediated
* Track and report on server and security baseline deviations and compliance with security standards
* Performs patch reconnaissance on security, telecoms and networking technologies
* Participate in occasional after hours and weekend maintenance windows for changes to security and network systems
* Written updates to knowledge base, incident response plans, tickets and change controls
* Generate status reports and performance reports
* Monitor and maintain automated systems for monitoring security and operational availability.

**Security Analyst**

**Avon Technologies Pvt Ltd Hyd India October 2015 to March 2016**

**Responsibilities:**

* Provide day-to-day technical support to employees for network infrastructure and internal systems issues
* Responsible for Vulnerability Management and Remediation using Retina vulnerability application
* Interpret and respond to vulnerabilities in the global network which supports
* Telecommunications, Financial and Clients Data related services
* Conduct security monitoring, forensic analysis, incident response and cyber-crime investigations
* Assist in the coordination and escalation of security issues to the VP of Enterprise IT Security
* Understand and maintain knowledge of the latest security issues
* Function as an internal consulting resource on information security issues
* Investigate attempted efforts to compromise security protocols and escalate issues to higher level associates
* Updates job knowledge by participating in educational opportunities; reading professional publications; maintaining personal networks; participating in professional organizations.