JAHNAVI C

CYBER SECURITY ANALYST

**Email:** Jahnavic91@gmail.com **Phone: +1 863-345-2716**

Skilled Cyber Security Analyst with 8+ expertise in vulnerability management, SIEM, incident response, risk assessments & management, security audits, unauthorized access, viruses, and a wide range of vulnerabilities and threats. Well-versed in direct and remote analysis with strong critical thinking, communication, and people skills. Able to thrive in fast-paced and challenging environments where accuracy and efficiency matter.

# SUMMARY

* Professional with 8+ years of extensive experience in the areas of **Risk Analysis, SIEM, Endpoint Security, DLP, Network Security, Email Security, Web Gateway, Vulnerability Assessment, Pen testing, Windows Server, Domain technology, and Antivirus servers.**
* Expert in Vulnerability Assessment using **Qualys, Nessus and Nexpose** tools to evaluate attack vectors, identify system vulnerabilities and develop remediation plans and security procedures.
* Assisted in integrating regulatory compliance requirements (**e.g., HIPAA, PCI, NIST**) into the organizational security roadmap.
* Experience in planning, developing, implementing, monitoring, and updating security programs, and advanced technical information security solutions, and sound knowledge in **SOX and PCI compliance requirements** and understanding of **NIST and ISO** standards.
* Configure, maintain, and design network security solutions including firewalls (Checkpoint, Cisco ASA, and Fortinet), IDS/IPS (Cisco, CheckPoint and Sourcefire), **VPN, ACLs, Web Proxy, etc**.
* Hands on experience on Operations and management of Aruba based wireless network providing multiple SSID platform for DoD users.
* Hands on experience on **Web Application Firewalls and attack mitigation techniques.**
* Work closely with clients Information Assurance analysts to oversee the preparation of a comprehensive and executive and Accreditation (C&A) packages for approval of an Authorization to Operate (ATO); generate, review and update System Security Plan (SSP) against NIST and NIST requirements.
* Establish a strong GRC (Governance, Risk and Compliance) practice to ensure adherence to best practice, regulatory requirements, and **ISO 27001.**
* Facilitate implementations of information security policies, account security policies and standards for logical and physical security.
* Perform Risk Assessment, Gap analysis & create Risk Mitigation plan.
* Good experience to provide remediation consultation to organizations and system owners, ensuring

# vulnerabilities are remediated NIST and Cyber Threat Intelligence research.

* Led an effort to create a new process in filtering and manage **IPS events** by automating the process and streamline Security Operation Center (SOC) triage efforts.
* Managed **McAfee ePO**, configured **HIPS 8.0** policies, verified and created server tasks, monitored events, created and enforced DLP policy, managed Rogue System Detection.
* Support deployment of all HBSS point products and updates to include **McAfee agent, HIPS, VSE, DLP**.
* Experienced with Proxy and **Malware-mitigation** (**Websense, Cloudflare, FireEye**), **threat detection**

and data leakage protection (**Network DLP /Symantec, Websense Security Analytic**).

* Dedicated, multifaceted, and detail-oriented professional with progressive experience in Cybersecurity operations; complemented with wide ranging knowledge of **McAfee ePolicy Orchestrator (ePO)** and networking technologies such as firewalls, switches, and routers.

# SKILLS

**Vulnerability Management Tools:** Qualys VMDR, Rapid 7, Nexpose, Tenable IO, SC, Continues Monitoring, Web Application Scanning, Threat Protect, Policy Compliance, Cloud Agents, Asset Management, Governance, Risk Management and Compliance.

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

**Packet capture**: NetFlow integrator, Wireshark, SolarWinds, Tcpdump

**E-Mail security**: Office365 Security & Compliance, & FireEye email security (EX series)

**Security tools:** ZAP Proxy, Nikto, Metasploit, Burp suite, Snyk & Veracode

**Pen Test Tools:** NMAP, Wireshark and Kali.

**Threat Intel**: STIX, TAXII, Trustar

**DLP**: Zscaler, Websense, Symantec & McAfee

**Web Application Firewall (WAF):** Cloudflare, F5 Silverline, Signal Science, Akamai

**Security Software**: Qualys, Nessus, InsightVM, Nmap, Metasploit, Snort

**Frameworks**: NIST SP 800-171, ISO 27001/31000, HIPPA, HITRUST CSF, PCI DSS, CVE and SANS 25

**Antivirus Tools:** Symantec, McAfee ePO, McAfee Endpoint Protection Suite

**SIEM**: IBM QRadar & Sumologic

**Firewalls**: ASA, FTD, F5 WAF, Cloudflare WAF

**Scripting Languages:** Python

**Operating Systems:** Windows2008,2012, 2016, 2019, UNIX, Linux- RHEL, Ubuntu, CentOS, Kali

**Databases**: Oracle & MS SQL

**Load balancer:** Big IP F5 LTM and GTM

**Network:** Cisco Routers, Switches

# Education Details:

Bachelor’s degree in Computer Science from Gandhi Institute of Technology and Management, India-2016

# Certifications:

FORTINET NSE 1, NSE 2 Certified.

Rapid7 Certified Nexpose Administrator

# WORK EXPERIENCE

**Sr. Cyber Security Analyst Nov 2021 - Present**

# Tele Tracking, Pittsburgh, PA Responsibilities:

* Responsible for articulating technical security requirements, monitoring the effectiveness of IT Security controls framework, and raising the level of security awareness and policy compliance among workforces.
* Experienced with **Office 365 DLP, Bluecoat web sense, Proofpoint, Trend Micro, and IBM QRadar Enterprise SIEM security tools** to monitor network environment.
* Worked on tools like Information security and **Group Policy, McAfee Data Loss Prevention, Symantec End- Point Protection** Manager, Symantec Endpoint Encryption, Windows Server Update service, Websense Proxy, Syslog’s, GFI.
* Experienced primary Voltage secure data encryption engineer heading up the International Project encryption servers worldwide.
* Oversee Vulnerability assessment/penetration testing of scoped systems and applications to identify system vulnerabilities.
* Experience with **QRadar & Sumologic** SIEM.
* Experience with **Threat and vulnerability** trends and analysis.
* Experience with **MITRE ATTACK** framework and integrate threat intelligence platforms.
* Experience with email security i.e., **DLP, ATP, anti-spam and anti-phishing** using O365 Security & Compliance
* Experience with **Qualys, Tenable, InsightVM.**
* Prioritize vulnerabilities/assets **from Tenable Nessus and Tenable IO** that should be patched during maintenance cycles.
* Used automated Vulnerability assessment tools such as **Nessus and Tenable IO.**
* Monitoring and remediating daily security alerts generated by end users with the tools like **Intel/QRadar SIEM, Zscaler, Websense,** and responsible for effectiveness of tools and scans, as well as assessing and tracking risk of exposure.
* Performing vulnerability assessment using **Nessus and Tenable IO.**
* Experience with **CIS** standards and framework adherence.
* Experience with **AWS and GCP** cloud environments.
* Application support for **FIM,** research and understand all aspects of tripwire and troubleshooting as well as find other ways to automate practices. Would help other teams in cyber security as well for any projects dealing with **Nessus tools vulnerability** management, risk and compliance in NERC standards.
* Lead a team of cloud security engineers in various areas of expertise to execute complex solutions to meet delivery timelines.
* Recognize, adopt, utilize, and teach best practices in cloud security engineering.
* Internal Network Vulnerability Assessments to enhance the Information Security culture of an organization through **identifying, analyzing, and reporting the gaps**.
* Converting existing AWS infrastructure to server less deployed via Terraform or **AWS Cloud formation**.

# Frameworks used ISO 27001 ISMS, PCI DSS, SSAE16, OWASP, SANS, Forcepoint, Zscaler.

**Sr. Information Security Analyst June 2020- Nov 2021 Walmart, Dallas, TX**

# Responsibilities:

* Proactively implemented updates, maintained, managed, monitored, and supported enterprise network and systems security operations infrastructure throughout the shared services environment.
* Perform daily **DLP Incident monitoring**, analysis and reporting, solution checks, client interaction, and **day-to-day DLP** operations.

# Managing SIEM - Net forensics.

* Create and run routine reports and data analytics in Excel and Tableau. **Audit and validate data/report**.
* Responsible for delivering an end-to-end continuous **integration - continuous delivery** system for the products in an **agile development** approach using **Chef/Ansible and Jenkins** and Shell Scripts.
* Wrote Ansible playbooks to setup **Continuous Delivery pipeline** and this primarily consists of a Jenkins and Sonar server, the infrastructure to run these packages and various supporting software components such as Maven.
* Managed the large security, risk and compliance initiatives of **SOX-404 IT, PCI DSS and HIPAA/HITECH, Privacy Act, and FTC** including security policies, procedures and controls.
* Experience with Windows, Linux, vulnerability assessment tools, firewalls, IDS/IPS, HIPS/HIDS, Nessus, NMAP, SIEM, Splunk, Rapid7 Nexpose and InsightVM, WAF, routers, switches, VMware, Endpoint Security, Cloud Security, Symantec Endpoint Protection.
* Assesses a residual risk rating for the vendor based upon their control environment Monitor, analyze and 0respond to network incidents and events. Participate in disaster recovery implementation and testing under **NIST framework**, **HIPPA, & HITECH** standards.
* Developed approaches for industry-specific threat analyses, application-specific penetration tests and the generation of vulnerability reports.
* Work with the network team to architecture **Azure and AWS VPN, AWS Direct Connect, and Azure Express Route connections.**
* Lead, Assess & advise the Vulnerability Management program about the contextual severity and urgency of patching efforts as it relates to vulnerability mitigation using **Qualys VMDR.**
* Drive end-to-end vulnerability lifecycle from discovery to closure.
* Identify internal and external threats that could result in unauthorized disclosure, misuse, altering, or destruction of customers' information assets.
* Drive a program to deliver a portfolio that adheres to policies and standards. This is inclusive of managed and third-party applications and services.
* Conduct **Network and System Vulnerability assessments** using **Qualys** and documentation of corrective/remediation actions.
* Demonstrate strong knowledge in **IT controls**, **risk assessments**, and the design and testing of security controls.
* Find opportunities to continuously improve the program through innovation with tangible value to the organization.
* Assists customers in identifying security risks to their applications and implementing appropriate data security procedures and products.
* Experience with security audit frameworks i.e., **ISO27001, SOC II and HiTRUST**.
* Write reports, assessments and provide decision support on information security risks and controls to executives.
* Responsible for enhancing the **Information Security Risks & Controls.**
* Perform cybersecurity assessments on emerging business initiatives, third-party services by assessing the impact and likelihood of risk events.
* Support customer business partners to understand **IT security risks, standards, and best practices.**
* Provide technical and non-technical **audits, risk analyses**, and document **compliance and/or noncompliance** based on findings.

# Cyber Security Analyst

**Rapid 7, Boston, MA Dec 2018- Apr 2020**

# Responsibilities:

* Interface with users, technicians, engineers, vendors, and other Technical Maintenance personnel to install, update and debug automated systems.
* Ensure products and systems comply with cyber security standards and practices.
* Develop test routines and monitoring solutions. Penetration testing using **Nmap and Wireshark.**
* Provide day to day support of servers, workstations, network and other equipment. Document support procedures specific to systems to be utilized by the Technical Maintenance and Engineering departments.
* Plan, execute and oversee remediation activities for valid vulnerabilities which are identified using Application Scanning tools. Experience with application scanning to identify security vulnerabilities in the web application and architectural weaknesses.
* Architecture design and Implementation of centralized **IBM QRadar SIEM** for High Availability and Redundancy
* Manage **IBM QRadar configuration** files like inputs, props, transforms, and lookups.
* Upgrading the **IBM QRadar Enterprise and security patching**.
* Installs, configures, and maintains multi-user software to be accessed from file servers.
* Administer and maintain end user accounts, permissions, and access rights.
* Works in close cooperation with **Systems Analyst** and Lead Information Technology Technician to facilitate management of computer labs, installing any software needed for each semester and/or special seminars.
* Orders software, hardware, and other supplies as required for the institutional computer network, personal computers, and computer labs.

# Information Security Analyst

**Ciber, Bangalore, India Jan 2017- April 2018**

# Responsibilities:

* Advanced knowledge of Cisco wireless LAN controllers, Cisco access points, Cisco ISE, Cisco routers, Cisco L2/L3 switches, Cisco Prime, Generic Routing Encapsulation, load balancing (F5 BIG-IP Local Traffic Manager, Cisco Load Balancer, Citrix, Azure load balancer), QOS, PBR, WCCP, VPN, NAT, VoIP, IPSec, Multicast, DNS services, MPLS networks, LAN, WAN, Juniper Networks Firewall, Cisco ASA firewalls and network and routing protocols (Ethernet, TCP/IP, SNMP, VLAN Trunking, BGP, OSPF, ISIS, EBGP,IBGP,RIP).
* Excellent written and verbal communication skills. Ability to create, update and maintain technical documentation. Ability to work independently. Experience with Service Now.
* Provided guidance and policy regarding the administration of all computer security systems and their corresponding or associated software, including endpoint security, intrusion detection systems, and application whitelisting.
* Participated in strategic security relationships between internal resources and external entities, including government, customers, vendors, and partner organizations.
* Collecting and organizing information from various sources like computer & server data
* Identifying and solving problems in various fields or specialized areas
* Examine the data to figure out what is important to the problem and which methods are best to analyze it.
* Use statistical methods to analyze information and develop solutions to business problems.
* Advise managers on findings and the various courses they can take to address the problem.
* Write memos and reports for managers to look over the findings and recommendations.

# Security Analyst

**Marlabs, Bangalore, India April 2014- Nov 2016**

# Responsibilities:

* Utilize cyber security tools to actively hunt for threats in the enterprise network.
* Analyze and investigate adverse events and incidents using an enterprise security information and event monitoring (XDR), logs from firewalls, IDS/IPS, proxies, servers, endpoints, and other network devices to determine threats, attack vector, scope of activity, and appropriate response.
* Identify, contain, mitigate, recover, and report on cyber-security incidents affecting the enterprise, business, and subsidiary networks globally.
* Research the latest vulnerabilities, exploits, and other relevant information on potential threats to the organization.
* Collaborate with other teams within Cyber Defense / Infosec / Wider divisions to improve detection and monitoring, develop cyber defenses, and perform advanced network and host analysis.
* Coordinate with peers and stakeholders across global functional and business unit teams as needed to analyze and respond to adverse events and incidents and improve corporate security posture.
* Assist teams with mitigating findings including assessment of impacts, possible solutions, and efficacy of remedies.
* Assist with the secure integration of cloud applications and infrastructure.
* Develop and maintain technical support/knowledge base.
* Develops Service Level Agreements to set expectations and measure performance.
* Be a member of the Incident Response Team.
* Other duties as assigned. Management reserves the right to assign or reassign duties and responsibilities at any time.
* Perform network security audits and testing and evaluate system security configurations to ensure efficacy and compliance with policies and procedures.
* Adheres to organization Policies and Procedures and drives compliance within the team.
* Takes ownership for own development and career management, seeking opportunities to develop personal capability and improve performance contribution.
* Enable out of the box monitoring use cases, develop runbooks/playbooks, and tune false positives alerts to improve the detection capabilities.
* Monitor Open Source and Commercial Threat Intel feeds and integrate those IOCs, TTPs into various security technologies.
* Monitor, Detect and Respond security alerts within defined SLAs.
* Participate in Incident Response Activity by collaborating with cross functional teams to minimize the impact of security incidents.
* Drive cyber investigations through to eradication, feedback and lessons learned phase to improved cyber resilience.
* Work on assigned cases, perform detailed investigations, and escalate in a timely manner to senior analyst.
* Strategize and deliver on immediate and long-term goals through teamwork and collaboration within the infosec group.