    

**Vishal Renigunta**

**Sr. Cyber security analyst**

**2485877195 | vishalrenigunta38@gmail.com**

**SUMMARY:**

* Cyber Security Analyst/Engineer with 8+ years of experience in system security planning (SSP) development, compliance documentation, and vulnerability management.
* Expertise in NIST 800-53, 800-37, and 800-53A compliance, risk assessments, and security control implementation.
* Proven ability to collaborate with system owners, automation managers, and security administrators to align applications with Secure Application Development Life Cycle and accreditation processes.
* A solid understanding of IT operations and conversant in cybersecurity solutions operations.
* Working experience with Qualys, Tenable, Tanium, Nessus, or Rapid7.
* Experienced in security assessment, documentation of compliance, implementation of controls.
* Experience with common information security management frameworks, such as ISO 2700X NIST, PCI and HIPPA.
* Excellent knowledge of Identity & Access Management (IAM) and Role Based Access Control (RBAC)
* Excellent understanding of Governance, Risk and Compliance.
* Responsible for applying the latest Symantec standards on various platforms (Windows, UNIX, Middleware, AIX, etc.) through the Symantec control compliance suite tool.
* Provide onsite Symantec DLP technical service and support to a Large Enterprise customer base.
* Expert in Implementing & Managing Symantec tools like Data Loss Prevention (DLP) and Secure Web Gateway.
* Highly skilled in Splunk to build, configure and maintain different environments and in-depth knowledge of log analysis generated by various operating systems.
* Good communications skills, both verbal and written, as well as the ability to communicate well with people in a variety of positions, roles, and levels.
* Served as a subject matter expert for vulnerability assessment, response, management, scanning, and identification.
* Worked analytically to solve both tactical and strategic problems within the vulnerability management and remediation programs.
* Researched, planed, developed, and oversee the implementations and configurations of vulnerability solutions using industry standard tools, such as, Rapid7, NMAP, and Prisma Cloud application scanners, and other vulnerability scanners on a wide variety of business information systems both on prem and cloud based.
* Experience managing security information and event management (SIEM) systems, threat intelligence platforms, security automation and orchestration solutions, and other network and system monitoring tools.
* Knowledge of and implementation experience with security technologies and architecture, including but not limited to, encryption, network security, firewall configuration, two factor authentication and intrusion detection.
* Demonstrated experience functioning in an Incident Response Team during a rapidly evolving security incident.
* Experience of information security tools and techniques (including incident response, cloud security, security operations, vulnerability scanning and reporting, NIST standards, and best practices associated with digital asset protection.
* Working knowledge & understanding of compliance obligations such as SOC 1/2, ISO 27001, PCI-DSS, NIST 800-53, NIST 800-171, Cyber Essentials, NIST CSF and CIS.
* Proficiency in IT Systems and understanding of Networking and Computer Information Systems.
* Good knowledge of the kill-chain model, ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework, and modern red team tactics and techniques.
* Knowledge of systems hardening and other risk mitigation factors on multiple technologies and operating systems (Window, Linux, Mac, routers, switches, Kubernetes).

**CERTIFICATION:**

* Fortinet Network security expert Level 1 & 2
* CompTIA Security Plus
* Microsoft Azure Administrator certification (AZ-104)
* Certified Software Asset Manager
* Rapid 7 Certified Nexpose Administrator
* Qualys VMDR Certified
* ISC2 Certified in Cybersecurity

**EDUCATION DETAILS:**

B.Tech in Computer Science, Gokaraju Rangaraju Institute of Engineering & Technology , 2016

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| **SIEM** | Splunk, Sumo Logic, IBM QRadar |
| **Vulnerability Management Tools** | Rapid-7 Nexpose & InsightVM, Qualys, Tenable Nessus, Nmap, Wireshark, OWASP |
| **Security Tools** | GuardiCore, McAfee Vulnerability management solutions, SolarWinds, LogRhythm, Tenable, Proofpoint |
| **IPS/IDS** | McAfee IPS, Secure Works IDS/IPS, SNORT |
| **Firewall** | Palo Alto, Panorama, Checkpoint Firewall |
| **Network Management** | Wireshark, SNMP, SolarWinds NCM+NPM |
| **Platforms/Applications** | Continuous Monitoring Vulnerability Management, Web Application Scanning, Threat Protect, Policy Compliance, Cloud Agents, Asset Management, Governance, Risk Management, and Compliance, SolarWinds, Burp suit, NMAP, Wireshark, Kali, Extra hop, Confluence, Nagios, SQL Server Management |
| **Ticketing Tools** | Service Now, Alloy Navigator, My-Cherwell, Jira |

**PROFESSIONAL EXPERIENCE:**

**Baxter, Chicago, IL**  September 2023 to Present

**Sr. Incident Response Analyst**

**Responsibilities:**

* Contributed to incident response and business continuity planning efforts, ensuring alignment with NIST guidelines and organizational security policies.
* Lead the discussions with Application Analysts, Development, and Infrastructure to implement security guidelines and standards.
* Function as a central third-party risk management subject matter expert looking to involve third parties in processes that interact with data.
* Support completion of information security review process for all new third parties, and annual reviews for all other relationships, that receive and/or interact with data.
* Maintain inventory of third parties who possess and/or interact with data, including key risk information about the relationship, data attributes involved, and regulatory compliance.
* Monitor open third-party security issues and remediation actions associated with security control gaps to ensure timely closure.
* Monitor, collect, and organize a high volume of incoming and outgoing communications, directives, requests, and reports with a clear security imperative.
* Triage information for dissemination to relevant security stakeholders and organization management.
* Examine security monitoring use cases and develop and tune supporting content for security tools such as dashboards, alerts, reports, rules including but not limited to the configuration and monitor security information and event management (SIEM) platform and endpoint detection tools for security alerts.
* Oversee data analysis in support of security event management processes, including root cause analysis.
* Implement automation and orchestration to improve efficiency and effectiveness of security monitoring and response processes, document processes and procedures in the form of playbooks and reference guides.
* Act as a primary point of security risk management activities, including analyzing, quantifying, and tracking identified information security risks and reviewing and documenting risk exception requests.
* Create dynamic dashboards and scorecards for visibility of Information Security Governance activities.
* Developed, maintained, and managed cloud security controls (e.g., MCAS, Conditional Access), ensuring compliance with security frameworks and regulatory requirements.
* Ensure that the identity & access management program protects the entire environment, including cloud services and high-performance compute environment.
* Assist with the management and operation of information security tools and processes, including security information and event management (SIEM) and endpoint AV and malware defense (EDR).
* Attend regular technical project and implementation meetings and serve as a security consultant to help guide secure application and infrastructure configurations.
* Understand potential and emerging information security threats, vulnerabilities, and control techniques and communicate this information to appropriate team members throughout the company on a timely basis.
* Deploy, integrate, and configure of all new security solutions and or any enhancements to existing security solutions in accordance with standard best operating procedures generically and the organization security documents specifically.
* Continually investigate and introduce security processes improvement measures, metrics, and present suggestions.
* Conduct periodic reviews to ensure compliance with established policies and procedures ensuring all events/incidents are executed and documented as required by current standards.
* Incorporate external threat intelligence sources related to zero-day attacks, exploit kits and malware into detection tools. conduct forensics such as host-based disk and memory, as well as network and analysis.

**T-Mobile, Atlanta, GA** Jan 2021 to Aug 2023

**Sr. Cyber Security Analyst**

**Responsibilities:**

* Conducted comprehensive security audits of IT infrastructure, identifying vulnerabilities and providing risk assessment reports aligned with NIST, ISO 27001, and PCI-DSS standards.
* Developed security recommendations to improve the company’s cybersecurity posture.
* Collaborated with cross-functional teams to develop and maintain System Security Plans (SSPs) for key applications, ensuring alignment with the Secure Application Development Life Cycle.
* Assisted in third-party security assessments and vendor security compliance.
* Researched and explored new security threats, vulnerability trends, alerts and recommends and implements remedial monitoring and actions.
* Drive the implementation of new information security technologies or integration of existing technologies including initial configuration, installation, change management, and operational handoff.
* Conducted tabletop exercises with Automotive SOC stakeholders and recommend changes, improvements in the security processes, and technologies.
* Formulated detailed technical and procedural documentation describing various components of the vulnerability management program; design reports and metrics; investigate areas of concern to be communicated to management.
* Build and maintained system documentation for security tools, perform system health checks, create test cases, and lead the upgrade of security tools.
* Lead incident response activities for highly complex events. Conduct technical investigation of incidents to identify causes and recommend future mitigation strategies.
* Responsible for creating technical/engineering documentation and design, develop and implement automation for manual processes via scripting and other automation tools.
* Design, document, test, maintain, and provide issue resolution recommendations for highly complex security and other technology solutions.
* Utilize subject matter knowledge in industry leading security solutions and best practices to implement one or more components of information security such as availability, integrity, confidentiality, risk management, threat identification, modeling, monitoring, incident response, access management, and business continuity.
* Work with partner engineering teams on identification and remediation of security vulnerabilities and conduct risk assessments of infrastructure to ensure compliance with corporate security policies and adherence to best practices.
* Develop, administer, and maintain phases of the security program, projects, and initiatives.
* Implement security tools, assess security status, monitor systems, and respond to incidents or breaches.
* Liaise with internal support teams to coordinate ease of daily operations as well as participate in team procedures to drive successful GSOC (Global Security Operations Center) operations.
* Assess information systems, collect information on potentially threatening activity to inform stakeholders of emerging security situations, risks, or threats accurately and efficiently.
* Prepare and present security reports based on intelligence data.
* Serve as the focal point for analysis and distribution of operative information that affects the clients’ employees, properties, or operations.
* Distribute incident reports, situation briefings and after-action reviews to client organizations and their partners for crisis management purposes, as well as business resiliency or disaster recovery.
* Maintain records, logs, and case management files related to security operations, intelligence, investigations, and alarm monitoring performance for use by clients in business reviews.
* Support and maintain organizational identity governance initiatives and the firm’s Privileged Access Management (PAM) platform. Ensure proper access controls and compliance with regulations and industry standards.
* Create solutions that balance business requirements with information and cybersecurity best practices.

**American Express, Pheonix, AZ**  August 2019 – Dec 2020

**Information Security Analyst - II**

**Responsibilities:**

* Developed and maintained System Security Plans (SSPs) for applications requiring Authority to Operate (ATO) and system enhancements, collaborating with system owners to ensure compliance with NIST 800-53 security controls.
* Collaborated with system owners to ensure compliance with NIST 800-53 security controls.
* Conducted security risk assessments, provided control recommendations, and assisted teams with artifact collection to support assessment requirements, aligning with NIST guidelines.
* Performed system Data Classifications as part of the SSP/ATO process, ensuring compliance with organizational policies and regulatory requirements."
* Coordinated vulnerability scanning activities and validated compliance with security frameworks.
* Assisted teams with artifact collection to support assessment requirements.
* Managed security incidents and monitored corrective action plans for security gaps.
* Evaluate existing detection rules and facilitate the development and tuning of AV, EDR, and SIEM rules to ensure high fidelity alerting.
* Perform in-depth security risk assessments and audits, both in-house and with external parties, establishing IT security audit frameworks.
* Lead comprehensive security strategy, ensuring robust data protection, risk management, and adherence to product security standards.
* Simplify complex security data into actionable reports for decision-makers, regulatory bodies, and stakeholders, enhancing transparency and understanding of our cybersecurity efforts.
* Enhance cybersecurity operations by identifying improvement areas, standardizing processes, and integrating cutting-edge security tools.
* Collaborate closely with business leaders to address and mitigate information security risks, ensuring timely and effective solution implementation.
* Develop and maintain a centralized dashboard for leadership, providing a clear and concise overview of cybersecurity risks and statuses across the organization.
* Planned, coordinated, and executed regular incident response preparedness, including tabletop exercises.
* Configured and administered complex cybersecurity systems, including vulnerability management, SIEM detection and alert development, EDR detections and exclusions, SOAR playbooks, and writing scripts for automations.
* Collaborated with the network team to ensure secure configuration and management of firewalls and security groups to prevent unauthorized access and monitor traffic.
* Identify and analyze new requirements for policy impacts; develop and update policies, procedures, and guidelines. Improve compliance with security standards and policies across the enterprise.
* Designed and documented best-practice security procedures, standards, and guidelines for other teams or business units.
* Assessed and provided gap analysis of existing tools and controls to determine areas of increased risk and action those items through remediation.
* Performed technical risk assessments, triage security testing results and manage security response actions.
* Assisted in compliance activities such as external audits from customers, regulatory compliance projects, and overall information security reviews.
* Actively monitored, analyzed, and correlated activities, evaluated security events, conducted research, and provided in-depth incident analysis.

**Colruyt Group, Hyderabad, India** July 2016 – Dec 2018

**Security Analyst**

**Responsibilities:**

* Improved and automated internal capabilities for identifying, investigating, and responding to security events, aligning with industry best practices and NIST guidelines.
* Lead and participated in incident response tabletop exercises to validate processes, document lessons learned, and enhance procedures.
* Contributed to the creation and refinement of incident response runbooks.
* Developed and adjusted automations, scripts, and security tool configurations to drive efficiencies and enhance investigations.
* Hunted for malicious activity and provided feedback to the threat intelligence and signal development teams.
* Communicated incident details clearly and concisely to key stakeholders, both technical and non-technical, in written and verbal forms.
* Researched security technologies and drive proof-of-concept evaluations to improve network and production system security.
* Configured, installed and maintained security technologies such as firewalls, IDS/IPS, antivirus, endpoint protection, WAF, wireless security, and network access control.
* Performed security event monitoring & analysis related to security violations, potential vulnerabilities and alerts from detection systems.
* Assisted in defining application security policies and guidelines and lead implementation within a multi-team; develop performance indicators to ensure policy compliance.
* Collaborated and partnered with Engineering and Operations teams to drive remediation of security issues, while balancing prioritization of those security issues within SLA and teams’ respective backlogs.
* Performed security reviews and identified gaps in security monitoring and response architectures.
* Supported and managed cybersecurity compliance demands and engagements, supported team prioritization.
* Supported risk register maintenance. Followed up on outstanding remediation with related stakeholders.
* Assisted internal audit requirements with preparing and presenting written and oral reports and other technical or process related information in a pertinent, concise, and accurate manner for distribution to management.
* Analyzed threat information gathered from logs, Intrusion Detection Systems (IDS), intelligence reports, vendor sites, and OSINT.
* Collaborated with appropriate response partners, assisted with determining the root cause of incidents and work with stakeholders and responsible parties to remediate any identified control gaps or failures.
* Escalate issues to management in a timely manner with appropriate information regarding severity, exposure, and action items.
* Applied critical thinking and investigative mindset coupled effective written, and verbal communication skills.