**Sindhuja Thirupalani**

**SUMMARY:**

* Security professional with 10+ years of experience in Security GRC (Governance, Risk & Compliance), IAM Security, SailPoint IIQ, Linux, and SIEM tools, including Splunk and QRadar. Skilled in vulnerability management, network security, and handling access control to limit security threats.
* Proven ability to establish task priorities, work independently, and collaborate effectively as part of a team. Excellent communication and problem-solving skills.
* Expertise in identifying security threats, generating threat findings reports, and implementing corrective actions to mitigate vulnerabilities.
* Assess and manage information technology risk across a range of areas, including cybersecurity, IT strategy and governance, regulatory compliance, and business continuity.
* Experience in selecting third-party suppliers, drafting executive summaries, and delivering final reports to clients.
* Implemented policies for training, patching, vulnerability management, and continuous monitoring to minimize attack vectors in organizations.
* Collaborated with cross-functional teams to address security issues and provide support on projects from vision to development.
* Experience in Splunk and QRadar SIEM operations and implementation, administration, and monitoring, including log analysis of Firewall, Network, Host, and IDS logs to identify potential threats.
* Well-versed in IAM and Multifactor authentication, with training in AWS IAM by an employer-sponsored program.
* Experience in threat intelligence and malware analysis, performing advanced cyber threat detection and integrating security advisories with QRadar and Splunk.
* Knowledgeable in SCAP, vulnerability scanning, system hardening, and using tools like Nmap, Wireshark, Burp suite and Metasploit.
* Expertise in identifying and evaluating technology risks, internal controls, and related opportunities for improvement.
* Proficient in performing vulnerability scans using Nessus for improper configurations, missing patches, insecure credentials, and accounts.
* Completed regular security awareness training, including Information security awareness, Business continuity management, and HIPAA Privacy and Security.
* Strong knowledge of industry-standard frameworks and regulations, including NIST, PCI DSS, and ISO 27001, and experience in aligning security programs with these frameworks.
* Expertise in managing security incidents, responding to cyber-attacks, and conducting root cause analysis to prevent future incidents.
* Experience in conducting security risk assessments and developing risk management plans to ensure the confidentiality, integrity, and availability of critical assets.
* Experience in performing security assessments on cloud platforms, including AWS and implementing security controls to mitigate cloud security risks.
* Experience in designing and implementing security controls for network infrastructure, including firewalls, IDS/IPS, and VPNs.

**SKILLS:**

|  |  |
| --- | --- |
| * Governance Risk and Compliance Security * IDaaS (Identity-as-a-service), RBAC (Role Based Access Control) * SIEM Enterprise Security * IAM (Identity and Access Management) Security * Vulnerability Management * Security Risk Management Strategies * NIST, PCI DSS, HIPAA, GDPR Regulatory Requirements, and SOX Compliance * Security logs | * Internal Audits * ITIL - AD-HOC Queries, Ticket handling with SLA, Helpdesk * Packet filtering * Threat Detection * Security Implementation * Designing Security Controls * Implementation of Policies & Procedures * Preparation of policy documents & SOPs |

**CERTIFICATIONS:**

* CISCO Cybersecurity certified professional, **CISCO**.
* NIST Security Compliance Certifications completed by the American Bankers Association (**ABA**).
* Masters in information systems security (**CISSP Modules**), University of the Cumberlands.
* Master of Business Administration, Bharathiyar University.
* Bachelor of computer science, Bharathiyar University.

**PROFESSIONAL EXPERIENCE:**

**United Parcel Services (UPS) – Parsippany, NJ Oct 2022 - Till date**

**Information security Analyst**

**RESPONSIBILITIES:**

* Defining security requirements and security assurance tasks for network architecture, firewall management, security monitoring, user identification/authentication, and system hardening in a Confidential process control network.
* 4Security assessment and assurance on Cyber-Ark deployment - for privilege account management, non-personal account management, and service account management.
* Act as the security consultant on projects related to Confidential automation systems and control networks, advising projects on the security level of automation systems and security controls for safety systems.
* Conducting comparative risk assessments of Public Cloud threats versus traditional IT deployment models, giving the insight to control selection (network segmentation/segregation, security monitoring, SIEM, IAM, CM, platform security, encryption).
* Developed methodology for Cloud Service Provider assessment leveraging NIST, ENISA, and CSA guidance.
* Defining protections that enable trust and data protection in the cloud and developing a roadmap for implementation. Examples of such protections are CASB and security as a service suite.
* IaaS hardened Infrastructure build reviews, including the use of secured verified software - manually or based on infrastructure as a code.
* Risk assessment of IAM solutions - SAML, ADFS, OAUTH, IWA
* Guiding data owners on the impact of GDPR on Cloud security and current data handling practices. Planning data discovery and information classification tooling and road map.
* Data protection policy definition and testing enforcement using Sky High Cloud Access security broker.
* Developed hash and PCI - DSS relevant hardening guide for internet IPSEC VPN routers.
* Application vulnerability and patch management for environments under PCI-DSS scope. Use of Fortify and Checkmarks for SAST scans and prioritization of remediation activities after risk and control analysis.

**Vizio – Dallas -Tx Mar 2020 – May 2022**

**Security GRC Consultant**

**RESPONSIBILITIES:**

* Conduct security risk governance activities, assign risk owners, document remediation action plan in the enterprise risk register, and follow up to closure.
* Producing various IT security and risk artifacts such as security requirements specification documents, statements of work, Technical Vulnerability Assessments (TVA), and Assessments of Risk and Control.
* Testing of technical control implementation against control objective. Assessing the implementation of internal and SOX controls in multiple IS domains –
* Foundation (BIA, CIA, TVA) IAM, Security Monitoring, Platform Security, IT resilience, Change Management, and record retention.
* Interpreting controls and guiding application DevOps teams in collecting and uploading objective evidence for the Confidential Internal Audit function’s review.
* Advised IT custodians and asset owners on the importance of having the technology and processes in place to achieve the RPO and RTO recorded in Business Impact Assessments (BIA).
* Conducting UNIX and database infrastructure build reviews, assessing the use and vaulting of passwords for the high privilege and root accounts.
* Evaluating SOC2 reports for application functions outsourced to third parties.
* Maintained network security infrastructure globally including routing architecture, firewalls, IPS/IDS tuning, WAN optimization, distributed denial-of-service (DDOS) mitigation, virtual private network (VPN), and remote access.
* Escalate complex cases to the Detection team and the system owners.

**Wells Fargo, India Feb 2018-Oct 2019**

**Security GRC Consultant**

**RESPONSIBILITIES:**

* Worked under NIST 800 -53; PCI -DSS; HIPAA, FACTA, and CIS standards and have a good understanding of security compliance controls and their implementations.
* Develop and implement customer Data security governance, risk management, and compliance (GRC) framework, including conducting risk assessments, creating security policies and standards, and tracking compliance with regulatory requirements.
* Coordinated with a team to develop a risk mitigation plan and prioritize remediation accordingly.
* Assisted the GRC team in maintaining and validating security control catalogs.
* Assessed proper protections, physical, and technical controls are implemented as Per NIST Standards.
* Looked for daily software vulnerabilities from and Us-cert and then looks for those vulnerabilities available in our environment through Nessus (Tenable).
* Monitored health and logs of Applications and their components using SIEM tools and methodologies.
* Automated various alerts to business owners as per their requirements related to their applications and its errors.
* Configured alerts and automated those alerts as per requirements.
* Provided management recommendations for remediation and mitigation of vulnerability scan results.
* Analyze threat and vulnerability alerts, determine current impacts, and coordinate remediation actions as necessary.
* Have a keen understanding of threat vectors as well as exfiltration techniques.
* Worked on minimizing the attack vectors in the organization by policies of training; patching; vulnerability management and continuous monitoring.
* Identifying and working with cross-functional teams on security issues.
* Worked on preparing documentation, reviewing and assessing security controls for NIST Compliance.
* Scan the system for any vulnerability before authorizing to operate in environment.
* Reviewed, modified, and updated procedures documents as per policies.
* Assisted with internal and external audits to confirm compliance with applicable laws and regulations to customer data according to the Data Protection Act.
* Expertise in identifying gaps between existing control environments and security requirements.
* Develop and document risks and severity levels associated with identified vulnerabilities within risk matrices and security assessment reports.
* Proficiency in applying NIST security controls guidance to Enterprise IT systems and applications.
* Used the SIEM tool to assess the audit logs by monitoring security controls and their vulnerabilities.
* Reviewing & Validating Testing spreadsheets, Scripts, Review work papers, Retention & Archiving.
* Identified gaps in existing compliance processes and recommended updates.
* Developed security risk assessment models and controls to identify potential compliance risks.

**CITI, INDIA Aug 2015 – Feb 2017**

**security - SOC- Senior Analyst**

**RESPONSIBILITIES:**

* Work collaboratively with business owners to maintain NIST 800-171/CMMC, ISO-27001 compliance by performing risk and control maturity assessments; targeting information systems that process, store, and transmit company and customer information.
* Conducting risk assessments of vendor services or products, including but not limited to software, hardware, or other professional services as applicable.
* Provide cybersecurity risk consultation to internal teams focused on the alignment of information system design and implementation to the underlying cybersecurity control requirements.
* Document third-party cybersecurity risks supporting corporate information systems.
* Opened incident tickets and tracked them from start to completion following closely on its lifecycle stages prepare, identify, contain, eradicate, recover and lessons learned.
* Collected evidence for future use on similar cases, lesson learned, training and awareness.
* Develop and continually improve incident response runbooks to ensure we efficiently and effectively analyze and respond to security alerts and prioritize alerts.
* Assess new security technologies, assist in selecting third party suppliers and create solutions to mitigate security threats.
* Acted as a SOC analyst working on the second line of defence by implementing controls and regular monitoring of vulnerabilities, alerts etc.
* Establish categorization of third-party applications by criticality, track risks requiring remediation and set recurring risk reviews accordingly.
* Investigated and resolved incidents of unauthorized access to sensitive information.
* Administered and monitored firewalls, intrusion detection systems and anti-virus software to detect risks.
* Analyzed network traffic and system logs to detect malicious activities and work as a SOC Analyst in 24/7/365 environment with 12 Hours shifts both day and Night on rotation based.
* strong network understanding of TCP/IP protocol stack, HTTP/HTTPS, TLS security features and protocols.
* Worked with other teams to enforce security of applications and systems and monitored computer virus reports to determine when to update virus protection systems.
* Performed risk analyses to identify appropriate security countermeasures.
* Implemented security measures to reduce threats and damage related to cyber-attacks.
* Drafted security reports and metrics to track security performance and strategize improvements.
* Conducted security audits to identify vulnerabilities.
* Executed penetration testing to identify security weaknesses and develop disaster recovery plans.

**Royal Bank of Scotland, RBS Jun 2012 – Aug 2015**

**IAM Security - Senior Process Associate**

**RESPONSIBILITIES:**

* ITIL – Service Now - Supporting access provisioning, modification and deprovisioning to many key banking business systems.
* Deep knowledge and experience with various industry wide access management systems (SailPoint, Active Directory).
* Conducted training and applied change management to achieve desired outcomes.
* Developed standard operating procedures (SOP) and document workflows to drive current and future processes.
* RBAC (Role-Based Access control), MFA (Multi-Factor Authentication), PowerShell, and GUI tools to manage user accounts.
* Review and test user access to avoid unauthorized access, Segregation of duties (SOD), or detect any policy violation.
* Focus and maintain the CIA Triad and AAA security.
* Familiar with Active Directory domain controller, Windows accounts and OU, the configuration of windows file system permissions, and remote access VPN. Zero-trust model.
* Lifecycle approach of Identity, Assess, Remediate and Validate the AD domain controller by undertaking scanning methodologies to find out any vulnerabilities that occurred.
* Having a piece of Significant SailPoint product knowledge and experience, including developing and implementing certifications and IIQ policy-based controls.
* Coordinate with implementing and modifying new and existing access controls by industry and compliance standards.
* Audit for the unsuccessful logons and User Entitlement Reviews (UER) to make sure that only authorized user is having right access to the system/application.
* Implementing privilege access permissions and methodologies such as R/W/X.
* Password policies & Practices, Provisioning of Access, Monitoring, reviewing, and terminating user permissions & Groups.