Name: Sai Kiran

Sr. Cyber security analyst

Email: lsaikiran0708@gmail.com

Phone: 7077671396

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SUMMARY:**

* Cyber Security Analyst/Engineer with 9+ experience in Implementation, Administration, Operation and troubleshooting of enterprise data networks.
* Experience in planning, developing, implementing, monitoring, and updating security programs, and advanced technical information security solutions.
* Experience within security vulnerability management(Qualys, Rapid7, Tenable Nessus), including familiarity with managing and deploying vulnerability management tools within technology organizations.
* Knowledge of security controls for multiple security domains including access management, data loss prevention, encryption methods, network security, and endpoint security
* Experience as a Splunk Engineer configuring, implementing, and supporting Splunk Server Infrastructure across Windows, UNIX, and Linux environments.
* Knowledge of firewall/IPS devices and understanding of encryption and VPN technologies (IPSEC, TLS/SSL, SSH, SNMP).
* Strong understanding of network concepts including TCP/IP protocol stack, HTTP and TLS, DDoS detection/prevention, Intrusion detection and prevention.
* Design, implement and document the Microsoft Defender Endpoint Protection solution in corporate environments according to the specific enterprise architecture and compliance requirements.
* Monitored, maintained, and troubleshoot issues with Microsoft Defender for Endpoint Protection, and BitLocker Encryption.
* Knowledge in Application Security and identifying and fixing OWASP Top 10 and SANS 25 security vulnerabilities.
* Valuable experience in analyzing IAM logs, IAM application server logs, provisioning server logs to troubleshoot various authentication/endpoint related issues.
* Experience in Identity and Access Management (IAM) security operations, policy, governance, development, testing and access control provisioning.
* In depth knowledge of AWS cloud services like Compute, Network, Storage and Identity and Access Management.
* Provide IT Governance, Risk, and Compliance (GRC) service to fulfil client requirements.
* Worked with Infrastructure team to deploy crowd strike agent to all assets.
* Utilize cloud-based APIs when appropriate to write network/system level tools for securing cloud environments.
* Facilitate implementations of information security policies, account security policies and standards for logical and physical security.
* Good experience to provide remediation consultation to organizations and system owners, ensuring vulnerabilities are remediated.
* Modernize assessment tools by researching emerging technologies and outlining their procurement to increase productivity and effectiveness.
* Knowledge of Process Explorer, JAVA, Python, HTML.
* Hands on experience on End point Security using Symantec products.
* Monitor the network traffic using tools like Wireshark and Panaseer.
* Having good understanding and knowledge for implementation of FISMA guidance/governance.
* Lead 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.
* Experienced in handling IT infrastructure Network administration.
* Dedicated, multifaceted, and detail-oriented professional with progressive experience in Cyber security operations; complimented with wide-ranging knowledge of networking technologies such as firewalls, switches, and routers.
* Analyzed the Policy rules, monitor logs and documented the Network/Traffic flow diagram of the Palo Alto firewalls placed in the Data Center with MS Vision.

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| **SIEM** | Splunk, LogRhythm, IBM QRadar |
| **Vulnerability Management Tools** | Qualys, Rapid7, Tenable Nessus, Nmap, Nexpose, Wireshark, OWASP |
| **Security Tools** | GuardiCore, McAfee Vulnerability management solutions, Nessus, SolarWinds, LogRhythm, Tenable, Proofpoint |
| **IPS/IDS** | McAfee IPS, Secure Works IDS/IPS, SNORT |
| **Firewall** | Cisco ASA, Firepower Module (context firewalls), ACLs, IPSEC, Palo Alto, Panaroma, Checkpoint Firewall, Fortinet Firewall (Traffic Shaping) |
| **Network Management** | Wireshark, SNMP, SolarWinds NCM+NPM, Live NX |
| **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, App Dynamics, Extra hop, Observium, Confluence, Nagios, Zabbix, SQL Server Management |
| **Ticketing Tools** | Service Now, Alloy Navigator, My-cherwell |

**EDUCATION DETAILS:**

B.Tech ,2013

**CERTIFICATION:**

* CompTIA Security+ Certified
* Fortinet Network security expert Level 1& 2.
* Checkpoint cybersecurity jumpstart certified.
* Rapid 7 Certified Nexpose Administrator

**PROFESSIONAL EXPERIENCE:**

**Client –HP ENTERPRISE, Denver, CO** Mar 2022 to Present

**Role: Sr. Cyber Security Analyst**

**Responsibilities:**

* Responsible for ensuring the confidentiality, integrity, and availability of enterprise-wide assets. Work with business units for security assessments to identify vulnerabilities, remediation strategies, and implement effective safeguards.
* Conduct incident response activities from detection, analysis, remediation, and mitigation, to lessons-learned documentation.
* Configuring and supporting security tools like vulnerability scanner, SIEM, Firewall policies and content filtering, IDS/IPS, EDR and Email gateways.
* Responsible for monitoring of security alerts from various security controls implemented in the environment.
* Work with the business units for implementation and monitoring of various security alerts for internal and external environments.
* Monitor threat alerts from sources including DHS-CISA, Threat Connect, Shodan, and SANS and analyze the environment for vulnerabilities and risks related to new threats.
* Develop plans and implement solutions to mitigate risks in the environment. Coordinate with the technology team to determine solutions, priorities, and schedules for remediation work of identified issues.
* Support security operations and infrastructure teams with the analysis of operational issues related to security controls and processes.
* Strong understanding of the OWASP TOP 10, showcasing your ability to identify and mitigate common web application security vulnerabilities, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).
* Perform ad-hoc reporting in support of various initiatives. Maintain individual records for departmental metric reporting and compile metrics reporting data as necessary.
* Develop and maintain good relationships with other teams, system owners, business units, and users to ensure communication is customer focused and professional.
* Performing vulnerability assessments and implementing remediation measures based on the OWASP TOP 10 guidelines, demonstrating your commitment to securing web applications.
* Develop security standards and best practices for the organization. Plan and carry out an organization’s incident response plan.
* Prepare reports that document security incidents and the extent of the damage caused by the incident.
* Provide technical support for a comprehensive risk management program identifying mission critical processes and systems.
* Partner with Product Managers, Business System Analysts, Engineering and other groups in Enterprise Security and Customer Success organization to understand what products are being worked on, what risks are involved, and what security controls need to be implemented to detect or prevent security fraud.
* Lead security risk assessments of organization ecosystem, platforms, and products as it relates to data security, access management, fraud detection/prevention and recommend controls commensurate with the risks identified, develop mitigation plans, and work with internal stakeholders to mitigate the risks
* Demonstrate ability to balance between strategic initiatives and tactical activities required to run information risk response and remediation efforts.
* Create dashboards to quantify the impact of risks, monitor KRIs, and identify opportunities for improvement; Identify emerging security and fraud trends and design new security/fraud controls.
* Responsible for providing data analysis that helps to identify, prioritize, and mitigate risks that surface organization ecosystem to resolution.
* Build strong relationships and become a trusted advisor within BU and technology owners to influence change and drive ownership and accountability.
* Serve as a technical liaison between the IT Security and other organizational units to ensure production facilities, operations and systems are following security best practices.
* Lead cyber threat and security incident identification, protection, detection, response, and remediation activities impacting the operations environment and escalating to management.
* Define and ensure compliance with security policies, processes, and standards to build a comprehensive security program.

**Client- VISA, San Fransico, CA** Nov 2020 to Feb 2022

**Cyber Security Analyst**

**Responsibilities:**

* Act as a liaison between the assigned area and Information Security Strategy. Provides support for proposing, coordinating, implementing, and enforcing information systems security policies, standards, and methodologies.
* Recommend logging/monitoring rules and provides configuration management (CM) support for information system security software, hardware, and firmware.
* The GIAC Security Essentials (GSEC) or another relevant one, make sure to mention it. This showcases your expertise in information security.
* Review the quality of the threat intelligence information received from the CTI Cyber Threat Intel team and provide constructive feedback to the Information Security organization based on the needs of the assigned area.
* Communicate and translate information security policies, standards, and procedure requirements, and serves as a subject matter resource for organization policies and standards.
* Assist in the assigned area with regulatory compliance assessments, security risk assessments, findings analysis and remediation.
* Support the implementation and communication of security training and awareness activities.
* Train individuals within the assigned area on how to incorporate security into job functions and processes.
* Guide partners on a broad range of specific Technology Controls and Information Security programs, policies, standards, and incidents.
* Conduct risk assessment, required controls definition, control procedure appropriateness, vulnerability assessments and any other relevant areas.
* Lead or contribute to the completion of risk and control design assessments for an assigned business application, business portfolio, and overall enterprise, as well as risk mitigation and remediation plans and remediation strategy.
* Contribute to the definition, development, and oversight of a global security management strategy and framework using NIST CSF.
* Ensure technology, processes, and governance are in place to monitor, detect, prevent, and react to both current and emerging technology and security threats against organization.
* Develop on-going technology risk reporting, monitoring key trends and defining metrics to regularly measure control effectiveness for own area.
* Adhere to internal policies and procedures, technology control standards, and applicable regulatory guidelines.
* Contribute to the review of internal processes and activities and assist in identifying potential opportunities for improvement.
* Adhere to, advise, oversee, monitor, and enforce enterprise frameworks and methodologies that relate to technology controls / information security activities.
* Implementing security controls based on the SANS TOP 20 Critical Security Controls framework. Explain how you've applied these controls to enhance the security of systems, networks, and data in your previous roles.
* Influence behavior to reduce risk and foster a strong technology risk management culture throughout the enterprise.
* Maintain a roadmap for the Information Security Engineering program and lead efforts to mature and evolve it over time.
* Assist in setting the information security methodology, implementation standards, and tactics. Evolve programs over time to achieve desired results and conduct compliance assessments to evaluate design controls and mitigate risk.
* Coordinate security related activities between application, data, infrastructure and security architects and engineers. Lead product and operational workstreams through the threat modeling process ensuring risks are understood and navigated as early as possible in the development cycle.
* Arm workstreams with information to understand how the program can impact and enable them with effective mitigation strategies.
* Ensure the confidentiality, integrity and availability of the data residing on or transmitted to/from/through enterprise workstations, servers, and other systems and in databases and other data repositories.
* Ensure the enterprise security and implementation strategies are aligned with business strategy. Provide input to technical designs in enterprise security solutions, specifically around tools and systems that would best support the design.
* Recommend improvements to company's security posture through technological, administrative, or physical controls. Work with project teams regarding security architecture and technical implementation.
* Perform analysis to identify critical data, assets, and processes in the assigned area.

**Client- TikTok, Los Angeles, CA** June 2018 – Oct 2020

**Cyber/Network Security Engineer**

**Responsibilities:**

* Responsible for the development & implementation of the organization specific Security policies & procedures.
* Configure, test, document, and implement changes or upgrades to security processes, controls, or products as directed.
* Work closely within the Security Operations Center (SOC) performing incident response activities when an incident has been discovered, participating in investigations to determine root cause of security incidents, and ensuring that proper protection or corrective measures have been taken.
* Provide operational support, troubleshooting, and maintenance of Security-related processes, controls, or products.
* Responsible for assessing systems, processes, and projects against compliance requirements, control objectives, and security best practices.
* Report status on activities, issues, projects, etc. to senior staff/management, including the effectiveness and efficiency of security activities.
* Propose new standards, tools, policies, and procedures to improve security, compliance and risk management activities based on security operations findings, or security events or incidents
* Present changes at the Change Advisory Board (CAB) as needed. Works with cross-organizational teams to address alert deficiencies.
* Collaborate with IT teams and security colleagues to ensure audit readiness, and to prepare for internal and external audits. Making BIA/RA also Pen Testing Procedures.
* Analyze enterprise network for indicators of network breaches and present findings and recommendations to Senior leadership management.
* Formulate and implement comprehensive cybersecurity strategy for the organization, using external vendors and consulting firms.
* Work with IBM X-Force and Threat connect for open-source threat intelligence to monitor APT activities, Threat actors.
* Collect STIX & TAXII from multiple sources like DHS-CISA, FBI PIN and MS-ISAC and create alerts in SIEM.
* Collect, correlate, and categorize to determine analytics on threats, tactics, and procedures [TTP’s] by using Cyber kill chain framework.
* Perform intermediate threat management, threat modeling, threat vector identification and develop use cases for security monitoring.
* Process indicators of compromise and threat actor TTPs for correlation, detection and alerting in appropriate security tools.
* Configure and troubleshoot McAfee ePO policies for managed systems on production networks and provide system administrator support.
* Monitoring for alerts and suspicious activity on hosts by using end point solutions like **McAfee ePo** and Crowdstrike.
* Investigate and address alerts generated by network security controls, to ensure the integrity of corporate data and information.
* Analyze implemented security measures, identifying gaps in monitoring and alerting.
* Consult other groups within the organization on used third-party technologies to identify and prevent security gaps
* Continuously evaluate current trends in Information Security, especially as related to the financial sector, identifying, and implementing relevant security initiatives at organization.
* Implement industry-standard best practices and continually adapt, refine, and enforce the organization technology security policy while working with stakeholders to balance cybersecurity, convenience, and business information requirements.
* Collaborate with other team members to design and deploy new network capabilities, improve performance, fault tolerance, security, and efficiency
* Prepare security assessment plan, secure resources, and hold kick-off meetings prior to assessment.
* Follow information security policies, methods, standards, NIST standards, and practices to organize information systems, IT reference material, and interpret regulations.
* Determined the classification of information systems to aid in selecting appropriate controls for protecting the system.
* Threat intelligence collection using open-source networks. Performed network and host DLP monitoring and logging using vendor tools.
* Used remediation techniques for all collected vulnerabilities and if it is very high severe vulnerability then ticket escalate to the higher authority.
* Investigate security incidents and recommend actions needed to resolve situations.

**Client: HDFC BANK, DELHI** Jan 2016 – Sep 2017

**Role: Information Security Engineer**

**Responsibilities:**

* As part of the IT Security team, develop and implement CLS IT Strategy in consultation with the CLS IT teams, ensuring that all initiatives are mirrored in respective strategies including the overall CLS Strategy
* Provide security advice and support for information technology projects
* Research new security related products and services to ensure that CLS is equipped with appropriate industry best tools and solutions
* Operate and maintain IT Security controls related to SIEM, DLP, Vulnerability Management, Cyber Threat Intelligence, Endpoint Protection, etc. with an emphasis on cloud deployments and implementations.
* Conduct IT Security risk assessments for all high impact projects, defining security mitigating controls that impact the technology architectures of CLS, service providers, and business partners
* Support 24 x 7 Security Monitoring and Response on a 1/8 rotation
* Review and update IT Security procedures to reflect best practice and mitigate current and emerging threats
* Assigned ownership of IT Security Monitoring and Response related FRB and Internal Audit finding(s) and effective / timely resolution with IT Security
* Maintain relationships with all third-party IT security vendors and strategic partners
* Planned and implemented security systems and standards by evaluating network and security technologies, developing security requirements for the enterprise infrastructure, and maintaining overall user access in support of enterprise objectives and client service delivery.
* Researched and provided recommendations on methods, software, and technologies to mitigate risk exposures.
* Performed security log event analysis taking appropriate action as directed or required to address security risk issues or event/incidents.
* Lead the development, deployment, and management of Samsara’s vulnerability management and code analysis program, including tool identification, integration, and ongoing operations.
* Work closely with teams within Security Operations, Security Engineering, Risk & Compliance, IT, and Product Security to integrate vulnerability management into all elements of Samsara’s technology portfolio.
* Drive ongoing reporting and awareness around vulnerability response, SLA alignment, and risk acceptance.
* Work with a variety of cross-functional teams to ensure compliance with laws, regulations, and policies.
* Support Audit Readiness during external and internal Audit Activities.
* Ensure compliance of business continuity management policies and process in accordance with applicable regulatory requirements.
* Create security assessment of security controls on Information Systems by interviewing, examining, and testing methods using NIST 800-53A rev4 as a guide.
* Review and update System Security Plan (SSP) based on findings from Assessing controls using NIST SP 800-18 rev1, NIST SP 800-53A rev4 and NIST SP 800-53
* Develop and maintain information security standards, guidelines, and procedures. Align with industry guidelines to implement secure design policies and procedures.
* Determine security violations and inefficiencies by conducting periodic reviews. Implement and maintain security controls.
* Conduct threat and risk analysis and analyze the business impact of new and existing systems and technologies to eliminate risk, performance, and capacity issues.
* Assist with incident response as events are escalated, including triage, remediation, and documentation.
* Implements security improvements by assessing current situation; evaluating trends; anticipating requirements.
* Maintain quality service by following organization standards. Contribute to team effort by accomplishing related results as needed.
* Attend regular project and implementation meetings and serve as the security consultant to help guide secure practices.
* Keep up to date with the current and proposed security changes impacting regulatory, privacy and security industry best practice guidance.

**Client- HSBC Financial, HYD** July 2013 – Nov 2015

**Jr. Security Analyst**

**Responsibilities:**

* Worked on OWASP Top 10 critical vulnerabilities.
* Maintain confidentiality with sensitive information.
* Work with Devops team to integrate on CI/CD Pipeline edition to integrate SAST tool.
* Deliver continuous improvement year over year by providing accurate information, timely case entry, enhancing problem solving skills, and sound decision making.
* Build solid peer-to-peer relationships in a team environment to meet operational needs.
* Communicate effectively and clearly on a daily, weekly, monthly basis to provide exceptional customer service regarding routine and escalated requests.
* Responsible for answering alarms in the access control system, reviewing video, and entering service request when necessary.
* Evaluate potential security products, technical solutions, and capacity requirements to meet business needs and recommend changes to mitigate risk.
* Support quality control and compliance programs to include weekly camera audits, documenting PCI sites according to procedures, accurate case classification, and tracking of physical security issues.
* Utilize specialized tools to search social media and the internet for potential threats against the company, associates, contractors, and visitors.
* Ability to conduct in depth research on various entities as request by our business partners.
* Respond promptly to requests and complete concise and timely reports.
* Ability to handle both common and crisis situations calmly and efficiently.