Sai Raj Pinnapureddy

CISM, Network+, AWS Architect

Email id: sairajreddy29@gmail.com

Number: 9403209180

PROFESSIONAL SUMMARY

Experienced Cybersecurity Professional around 8 years of expertise in safeguarding enterprise environments through advanced threat detection, incident response, and vulnerability management. Proficient in deploying and managing enterprise-grade security tools, including SIEM platforms (Splunk SOAR, IBM QRadar, Microsoft Sentinel), EDR solutions (CrowdStrike Falcon, FireEye, Carbon Black), and IAM/PAM systems (Okta, SailPoint, Azure AD). Skilled in implementing Data Loss Prevention (DLP) strategies, managing encryption protocols, and configuring Cloudflare for secure content delivery and web application firewall (WAF).

Certified Information Security Manager (CISM) with strong hands-on experience in vulnerability assessments using tools like Tenable Nessus, Qualys, and Rapid7, as well as compliance with ISO 27001, PCI DSS, GDPR, and HIPAA standards. Adept at automating security workflows with Python and Bash scripting, developing custom SIEM use cases, and creating actionable dashboards and reports for real-time threat insights.

SKILLS & EXPERTISE

* Cybersecurity Tools: Splunk, IBM QRadar, Microsoft Sentinel, CrowdStrike Falcon, FireEye, Carbon Black, Tenable Nessus, Qualys, Rapid7, OpenVAS.
* Identity and Access Management: Okta, SailPoint, CyberArk, Azure AD.
* Governance & Compliance: ISO 27001, PCI DSS, GDPR, HIPAA, Third-Party Risk Management (TPRM).
* Network Security: Firewalls (Palo Alto, SonicWALL), VPNs, Secure Protocols (IPSec, BGP, MPLS).
* Cloud Security: AWS, Azure, Cloudflare (WAF, SASE, DDoS Protection).
* Programming & Automation: Python, Bash, PowerShell, ServiceNow, Jira.
* Endpoint Protection: DLP (Symantec, McAfee, Forcepoint), Microsoft Defender.
* Encryption & Cryptography: TLS/SSL, SHA-256, PKI Management.

CERTIFICATIONS

CISM- Certified Information Security Manager, 2022 [Link](https://www.credly.com/badges/6b73edb1-4a84-4f12-951f-31b764c07bff/public_url) (DoD certified)

AWS solutions Architect 2024 [Link](https://www.credly.com/badges/649c7479-9a9a-4e53-ad71-d1a51f04756b/public_url)

CompTIA Network + 2020 [Link](https://www.credly.com/badges/f0d49ca9-7eba-432d-939a-c29d61ad7abb/public_url)

EXPERIENCE

* Information security Engineer

Citi Bank, Dallas, TX Oct 2024 – Till date

* + Performed analysis and recommendations for IDS/IPS systems, firewalls, antivirus, and anomaly detection tools, improving threat detection by at least 25%.
  + Configured and managed Microsoft Azure sentinel SIEM for numerous data sources, improving security event correlation and reducing response time.
  + Administered SonicWALL firewalls across 3 multiple remote sites, enhancing network security and uptime.
  + Implemented and managed Microsoft Purview DLP policies across Microsoft 365, securing sensitive data and ensuring compliance with regulations like GDPR and HIPAA.
  + Configured and optimized Microsoft Defender for Cloud Apps (MCAS) to detect and mitigate cloud security risks, enforce access controls, and prevent data exfiltration.
  + Monitored and responded to DLP and MCASalerts, investigating policy violations, automating remediation workflows, and enhancing cloud security posture.
  + Collaborated with SecOps to monitor and respond to 50+ security incidents per month, improving response efficiency
  + Developed Bash and Python scripts for automation and deployed them on hundreds of Linux servers, reducing manual workload.
  + Deployed IDS/IPS to monitor 1,000+ network traffic sources, improving detection accuracy and reducing false positives by 20%.
  + Conducted monthly vulnerability scans using Qualys, addressing crucial vulnerabilities and ensuring compliance with PCI DSS, HIPAA, and GDPR.
  + Managed vulnerability assessments, automating patch management and improving patch compliance by 30%.
  + Configured Cloudflare for DDoS protection and WAF, securing web applications and reducing threats by half.
  + Authored and maintained information security policies aligned with ISO 27001 and GDPR, reducing non-compliance incidents by 25%.
  + Managed Jira and ServiceNow, tracking 200+ incidents and automating workflows, improving team efficiency by 30%.
* Security Risk Analyst

Johnson & Johnson, NJ Sept 2023 – Sept 2024

* + Prepared and presented regular reports to senior management on vendor risk profiles and mitigation efforts effectively leading the third-party risk assessment.
  + Analyzed SOC performance metrics to evaluate and enhance the effectiveness of incident response.
  + Monitored Qualys dashboards for emerging threats and took swift action to mitigate risks.
  + Developed and delivered training materials on IDS/IPS best practices for staff.
  + Managed firewall configurations and access logs to ensure compliance with PCI DSS.
  + Generated and analyzed Splunk SIEM reports to identify trends and improve threat detection capabilities and created playbooks using Splunk Phantom.
  + Automated report generation using Python to streamline security metrics updates.
  + Led SecOps drills and simulations to test and improve incident response strategies.
  + Managed data subject access requests (DSARs) in compliance with GDPR.
  + Assisted in third-party risk assessments using NIST and SIG frameworks.
  + Integrated Splunk with security tools to enhance threat detection and response.
  + Implemented malware scanning with Cloudflare to block malicious content at the edge.
  + Managed SharePoint migrations and ensured minimal disruption during transitions.
  + Created and optimized SQL-based alerts to monitor changes in critical security configurations.
  + Collaborated with IT teams to remediate security incidents and enhance overall security posture.
  + Ensured compliance with HIPAA, ISO 27001 and GDPR through regular audits and assessments.
  + Reported third-party risk management metrics to senior leadership to guide decision-making.
  + Coordinated the development of security policies in line with industry standards and regulatory requirements.
* Cyber Security Engineer/Analyst

Maintec Technologies Pvt Ltd June 2022 – Apr 2023

* + Designed, deployed, and optimized Enterprise Security solutions, including Cyber Threat Management, Security Analytics, SIEM, and Malware Detection.
  + Automated centralized detection of security vulnerabilities using scripts for Vulnerability Assessment tools like ArcSight.
  + Designed and implemented secure network architecture, including firewalls, intrusion prevention system (IPS), and virtual private networks (VPNSs) for clients.
  + Monitored network traffic and security events through SIEM tools (e.g., Splunk, ArcSight) to detect potential threats and take proactive measures.
  + Established a strong GRC (Governance, Risk and Compliance) practice to ensure adherence to ISO 27001 and regulatory requirements.
  + Performed enterprise security and Cloud security specific solutions such as: IAM, Identity Governance, SIEM, Key Management & Encryption access keys, Public, Private and Hybrid cloud solutions.
  + Involved in Security Operation, Vulnerability and Risk Assessment, altering report generation, and analysis with various security tools (Splunk, McAfee ePO, Symantec DLP, Bluecoat Proxy).
  + Conduct threat intelligence analysis on key areas of the Enterprise Defense-in-depth analytics, incident statistics, and other relevant information in the creation of periodic threat intelligence reports.
  + Managed log sources for Splunk and created technical add-ons for field extractions using regex.
  + Deployed and installed Checkpoint, Fortigate, and Palo Alto NGFW.
  + Collaborated with Splunk professional services to maintain performance best practices for Splunk Enterprise Security.
  + Utilized Splunk GRC standards for OWASP Top 10, CIS CSC, and DLP.
  + Created GRC policy in compliance with HIPAA and educated departments on compliance requirements.
  + Strong understanding of enterprise, network, system/endpoint, and application-level security issues and risks.
  + Created Jira workflows to streamline incident response procedures, facilitating real-time visibility and progress of vulnerabilities and security incidents.
  + Experienced with Windows, Linux, and various security tools including Nessus, NMAP, and SIEM.
* Network Security Analyst

Alstom, India May 2018 – June 2021

* + Ensured security compliance across servers and network devices within the information security department.
  + Administered major operating systems, ensuring optimal performance and security.
  + Managed and resolved Health Management alerts (performance, connectivity, configuration) to prevent operational disruptions.
  + Deployed containerized applications on Linux servers using Docker and Kubernetes for enhanced scalability.
  + Provided technical support for on-premise hardware and software, ensuring rapid incident resolution.
  + Configured and maintained WatchGuard firewalls, including High Availability, VPN, and Next Generation features.
  + Assisted in change management processes for firewalls and proxies, including Zscaler.
  + Monitored and analyzed security technologies (IDS, IPS, firewalls) using ArcSight SIEM to detect and mitigate IT security incidents.
  + Followed operational processes and procedures to analyze, escalate, and remediate critical security incidents.
  + Managed Scrum ceremonies, driving continuous team improvement and operational efficiency.
  + Integrated storage systems with virtualization platforms to streamline data access and enhance security.
  + Assisted in vulnerability assessments and risk testing of the network using Nessus and other security tools.
  + Conducted troubleshooting and resolved technical issues to maintain system integrity and security.
* Network Engineer

Carrier, Hyderabad, India Aug 2016 – Apr 2018

* + Planned, designed, configured, and maintained LAN, WAN, Wireless, Data Center, and Firewall technologies to ensure network reliability.
  + Implemented and supported LAN/WAN solutions for seamless connectivity.
  + Created RFCs, TDRs (Technical Design Reviews), and LLDs (Low-Level Designs) for network infrastructure projects.
  + Conducted wireless network implementations and passive surveys to assess and optimize coverage.
  + Documented network surveys and implementation processes for future reference and compliance.
  + Provided advanced troubleshooting, configuration, and maintenance of complex networks using protocols such as BGP, MPLS, OSPF, and EIGRP across Core and Distribution layers.
  + Led the replacement of EOS (End of Support) switches, upgrading from Cisco 6500 to 6500E, and from 3550 to 3750X and 3850 models.
  + Transitioned data and WAN networks to adhere to industry standards, ensuring operational efficiency.
  + Collaborated on LAN network integration projects, optimizing network performance and scalability.
  + Managed CATOS to NATIVE IOS migrations and performed hardware upgrades to enhance LAN and wireless infrastructure.
  + Provided oversight and support for successful WAN and LAN implementations, ensuring compliance with requirements.
  + Reviewed Statement of Works (SOW) and Bill of Materials (BOM) for LAN/WAN projects, ensuring alignment with technical specifications.