**Karthik**

**Cyber Security Engineer**

**Email: Karthik75287@gmail.com**

**A red and white logo

Description automatically generatedA logo for security company

Description automatically generated**A circular logo with a cloud in the center

Description automatically generated

**Profile Summary:**

* Having **10+ years** of experience in multiple cloud environments. Identified security risks, threats and vulnerabilities of networks, systems, applications, and new technology initiatives.
* Experienced Cyber Security Engineer proficient in designing, implementing, and maintaining enterprise data networks with a focus on security.
* Skilled cybersecurity professional adept in developing and updating security programs to meet SOX and PCI standards, while ensuring compliance with NIST and ISO guidelines.
* Experienced in establishing robust GRC practices, collaborating on accreditation packages, conducting risk assessments, and implementing ISO 27001, NIST 800-series, DIACAP, and FISMA standards.
* Experienced Splunk Engineer adept at configuring and supporting Splunk Server Infrastructure in diverse environments.
* Very good experience in Installation and configuration of CyberArk Vault, Vault Client, Active CPM, Network load balanced CyberArk PVWA and Clustered CyberArk PSM Architecture and design.
* Proficient in log monitoring and analysis utilizing SIEM tools such as Splunk, QRadar, Azure Sentinel, and HP ArcSight, with expertise in threat detection and response.
* Proficient in configuring and managing network security solutions including firewalls (Checkpoint, Juniper, Cisco ASA, Fortinet), IDS/IPS (Cisco, Checkpoint, Sourcefire), VPN, ACLs, and Web Proxy.
* Expert in configuring Layer 2 technologies including VLANs, Trunking, STP, RSTP, PVST, MST, VTP, and port-security.
* Involved Upgrade on CyberArk component on various servers and Setup Privileged password management Policies for CPM component.
* Experienced in Proxy and Malware-mitigation technologies (Bluecoat, Radware/ApplXcel/Alteon, FireEye) and Data Leakage Protection (DLP).
* Hands-on experience in operating Aruba-based wireless networks for DoD users and deploying Imperva web application firewall for attack mitigation.
* Managed McAfee ePolicy Orchestrator (ePO), configured HIPS 8.0 policies, and supported deployment of HBSS point products.
* Provided consultation for vulnerability remediation and researched emerging technologies to enhance assessment tools.

**Technical Skills:**

* **Threat Intelligence:**STIX, TAXII, TruSTAR
* **DLP:**Websense, Symantec & McAfee
* **SIEM:**Splunk, Netforensics, Qradar, Azure Sentinel
* **Load balancer:**BigIP F5 LTM and GTM
* **Network:**Cisco Routers, Switches
* **Network Security:**Snort
* **Database:**My SQL
* **Programming Languages:**Python, Ruby and Perl
* **Operating Systems:**Windows, Linux
* **Cloud Technologies:**Amazon Web Services (AWS): SDK, Dynamo DB, Lambda, Elastic Beanstalk
* **Application Servers:**Apache Tomcat, AWS Lambda, AWS Elastic Beanstalk
* **Virtualization Services & Technologies:**Amazon EC2, GITHub

**WORK EXPERIENCE:**

**Client: NYC OTI, NYC Oct 2022 – Till date**

**Role: Sr. Cyber Security Consultant**

**Responsibilities:**

* Design, develop, implementation, tuning and testing of standard and nonstandard content for Splunk and QRadar.
* Analyze, recognize, correlate, and report any potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information from SIEM, Snort logs and Checkpoint FW logs.
* Good understanding of policies in CyberArk Central Policy Manager (CPM).
* Perform Digital forensics and Incident Response (IR) using tools Autopsy, Magnet, Stinger, etc. 28 DOL agencies.
* Served as the primary SME for RSA SecurID and all multi-factor authentication products including Azure MFA.
* Maintained GIT repositories, branches and tags and Experience in Administering GITHUB repository.
* Played a key role in deploying Symantec Endpoint Protection Manager and clients on a closed network.
* Worked as a PCI-DSS consultant to perform a 3rd party audit.
* Establish and maintain an IT Compliance program for Financial Security Infrastructure team that minimize risks to IT objectives through effective, efficient, scalable, and cost-effective design and operation of controls, including NIST, ISO 27001, COBIT 5.0, FFIEC, GLBA, SOX, PCI & PII, and other domestic and international compliance requirements. Performed risk analysis using State approved risk analysis methodology based on NIST SP and ISO IEC 17799 methodologies.
* Performing system auditing using audit reduction tools; following up on audit findings; maintaining authorization documents; and supporting the local Information Systems Security Manager (ISSM) as needed to maintain system authorization.
* Installation and configuration of CyberArk Vault, Password Vault Web Access (PVWA), Central Password
* Manager (CPM) and Privileged Session Manager (PSM) in Prod and DR
* Involved in DLP data encryption, monitoring/reporting and remediation of internal and external threats/vulnerabilities.
* Configurations including AD integration and Management of Cyber Ark Enterprise Password vault
* Ensured Azure Government system was compliant to meet a FedRAMP Provisional Authority to Operate (P-ATO) and DoD Provisional Authorization (PA).
* Understand the threat landscape as related to vendors and perform vendor risk assessments.
* Works with Encase, FTK, Cellebrite, Gargoyle, IEF, tools, plus dozens of utilities for ripping, extracting, repairing, copying, de-duplicating data.
* Collaborate with Internal audit, External Audit, SOX PMO in a regular cadence, discuss changes to the control environment and prepare effective, efficient compliance and substantive test plans and SOX Calendar.
* Work closely with the Risk and finance teams to associate a monetary value to security risks within the User Behavior Analytics (UBA) tool.
* Interacted with Cloud Service Provider (CSP) to conduct Incident Response (IR) and Contingency Plan (CP) exercises for Disaster Recovery Plan (DRP) and procedures.
* Worked extensively in Configuring, Monitoring Elk, Extrahop.
* Consulted with business and technology partners to create and provide security recommendations and best practices.
* Assisted CSO with completion of established goals, objectives, and streamlining of internal office procedures.
* Conducted onsite penetration tests from an insider threat perspective.
* Performed host, network, and web application penetration tests.
* Support the reporting and outputs from cross-functional teams related to the vendor risk assessment process.
* Provide IT Governance, Risk, and Compliance (GRC) service to fulfil client requirements.
* Managed Cyber Security threats through prevention, detection, response, escalation and reporting in effort to protect Enterprise IT Assets through Computer Security Incident Response Team (CSIRT).
* Responsibilities for CSIRT included SIEM, Context Filtering, Web Security, Incident Tracking, IPS/IDS and Malware Analysis.
* Responsible for troubleshooting and resolving firewall software and hardware issues, including VPNs, connectivity issues, logging, cluster configurations, and hardware installations for Checkpoint and Palo Alto firewalls.
* Increased productivity by fine-tuning their IPS security policies allowing analysts to quickly identify threats on the network. Tune HIPS and VirusScan policies to support mission requirements as needed.
* AWS CLI Auto Scaling and Cloud Watch Monitoring creation and update.
* Participate in design efforts for network security related portions of new applications along with application development areas and the network design for disaster recovery efforts.
* Advise and implement Symantec Best Practices and configuration management in the environment.
* Initiated a vendor risk assessment program.
* Used virtualization tools such as VMWARE and VIRTUAL BOX to build server infrastructure for security solutions.
* Coach and mentor new analysts in our Third-Party Vendor Risk Assessment Program.
* Design and implement a vendor risk assessment scorecard - to establish a risk benchmark, identify areas needing improvement, and as a periodic tool to assess overall risk status.
* Configuring and implementing F5 BIG-IP, LTM, GTM load balancers to maintain global and local traffic.

**Client: Bright Horizons**, **Watertown, MA Jan 2021 – Sep 2022**

**Role: Cyber Security Engineer**

**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.
* Administration experience of Cyber Ark vault with Safe creation, integration with LDAP and other
* authentication methods.
* Provide expertise with incident response, security event monitoring, vulnerability management, asset security compliance and data loss prevention utilizing McAfee Nitro (SIEM), McAfee ePO, McAfee DLP.
* Monitoring and remediating daily security alerts generated by end users with the tools like Intel/McAfee SIEM, Forcepoint’s Websense, and Intel/McAfee EPO 5.X and responsible for effectiveness of tools and scans, as well as assessing and tracking risk of exposure.
* Create and run routine reports and data analytics in Excel and Tableau. Audit and validate data/reports.
* 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.
* 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.
* 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.
* Providing proper remedy to fix vulnerability in the client network after analyzing security incident queries alerted by ArcSight Performing Vulnerability Assessments and taking the required counter actions and measurements to ensure the security of the IT infrastructure / systems.
* Analysis and documentation of network & information security requirements and define security policy for enterprise client and business critical servers.
* Configurations including AD integration and Management of Cyber Ark Enterprise Password vault.
* Perform daily duties supporting and trouble-shooting digital rights management on a Windows and Linux Platform, while defining and implementing patching
* Build and operate a security & awareness program relating to vendor risk management program.
* Experience implementing/architecting cloud-based Active Directory solutions for Azure and AWS
* Implementation of Symantec Mail Security for SMTP and Symantec Endpoint Protection.
* Experienced with tools like Metasploit/Qualys/Network forensics technologies.
* Respond to inbound security monitoring alerts, emails, and inquiries that arose from various monitoring tools that included Symantec DLP.
* Perform vendor risk assessments as assigned. Work with vendors and business owners to gather documentation and develop vendor remediation plans.
* Primary responsibilities include Installation and configuration of CyberArk Vault, Vault Client, Active CPM,
* Network load balanced CyberArk PVWA, Clustered CyberArk PSM and PSM SSH proxy Architecture and design.
* Addressed critical areas of potential information security risks and opportunities with gap analysis for Data protection, Cloud Security and Data Classification.
* Used Microsoft Azure Security center to monitor the cloud environment.
* Worked on AWS designing and followed Info security compliance related guidelines.
* Design, Deploy, support and maintain Splunk cluster infrastructure in a highly available, geo-redundant configuration Develop, implement, and execute standard procedures for the administration, content management, change management, version/patch management, and lifecycle management of the firm’s enterprise security platforms.
* Worked on projects moving to cloud services such as Azure, Office 365 and Amazon Web Services (AWS).
* Knowledge and experience in IT risk or compliance disciplines including risk assessment.
* Websense, Symantec Endpoint Protection and Active Directory (User Account Management specific) events monitoring and analysis.
* Infrastructure security design and implementation expertise (Firewall, IDS/IPS, SIEM, Proxy services, Antivirus, Vulnerability Management, Key management, Web application firewall and PKI).
* Management of Cloud security, Vulnerability assessment, and security audits.
* Reducing Proofpoint Digital Risk to defend impersonation of the brand to harm current market.
* Perform personnel interviews during assessments and review proper analysis of testing results.
* Review documentation as applicable to controls for compliant/non-compliant status.
* Ability to provide an independent assessment per control and ensure security controls are implemented correctly; operating as intended; and producing the desired outcome.
* Designed and documented Compliance logging & auditing strategy, provide analysis and trending of security log data from security devices, provide threat and vulnerability analysis as well as security advisory services.
* Co-ordinating pen testing and application security testing audits with PenTest Tools like Metasploit, NMAP, Wireshark and Kali on Linux/Unix operating system.
* Respond to security incidents and follow through to resolution, reporting, and lessons learned phases.
* Cisco ASA/Palo alto firewall troubleshooting and configuring policy based on change request, allowing/denying communication between different segment of the network based on requested ports.
* Conduct vulnerability scans to support our risk/threat/vulnerability management program including resolving risks and the documentation of any residual risks.
* Maintain serviceability of assessment tools with latest software and firmware resulting in zero equipment failure during assessments
* Identifying flaws and weaknesses in information systems that may be exploited to impact the confidentiality, integrity and availability of a system.
* Prioritize vulnerabilities/assets that should be patched during maintenance cycles.
* Analyze vulnerability assessment results, identify remediation strategies and provide timely reports to management for review.
* Configured AWS Identity Access Management (IAM) Group and users for improved login authentication.
* Solution partner product compatibility validation with Cisco UCS servers. Functional and Feature testing of various datacenter and IT solutions and extracting test results for the quarterly marketing press release for Cisco partners.

**Client: Cisco, San Jose, CA Feb 2019 – Dec 2020  
Role: Cyber Security Engineer**

**Responsibilities:**

* Utilize Nessus/Tenable, Nmap, OWSAP and Web Inspect to scan all ports, access points, devices, software, and Servers.
* Utilize PowerShell, SCCM for scripting, patching, Application Testing and Imaging Windows OS, 7 & 10 machines.
* Monitored, Configured, Scan/Patch Network TCP/IP, DNS, Telnet and DHCP.
* Managed/Secured and Scanned devices, software, Web applications following NIST protocol & FIPS 140-2
* Auditing and documenting systems using DISA auditing tools, Assured Compliance Assessment Solution (ACAS), DISA STIG, and SCAP tools.
* Responsible for monitoring and, providing analysis in a 24x7x365SecurityOperation Center (SOC) using Splunk SIEM, IDS/IPS tools.
* Lead in implementing security solutions towards SIEM tool using Splunk, and work on setting up the dashboard. Operate closely with data security teams.
* Used Splunk Deployment Server to manage Splunk instances and analyzed security-based events, risks & reporting.
* Provide support of Splunk integration and deployment, configuration, and maintenance.
* Integration of data feeds (logs) into Splunk.
* Managing various industries standard IPS, PIA, CASB, Firewalls, Gateways, VBlock, Rapid7 Virus and Endpoint Managers
* Audit and validate configurations of network devices based on DISA STIGs
* Utilize RSA Archer platform 6.1.
* forensics, sniffers, and malware analysis tools.
* Participate supporting RSA Archer version upgrades.
* Managed, configured, account creation and supported CDM Dashboard within eGRC Archer platform.
* Managed, Configured of 3rd party applications data feeds.
* Conducts complex security architecture analysis to evaluate and mitigate issues. Develops policies and procedures for securing the system infrastructure and applications.
* Develops complex technical and programmatic assessments, evaluates engineering and integration initiatives, and provides complex technical support to assess security policies.
* Utilize Wireshark, Nessus to Pen-test and analyze the network and software’s.
* Utilize McAfee ePolicy/End Point Protection Suite administration including virus protection, HIDS/HIPS, firewall, encryption, and other workstation security technologies.
* Address known exploits using the Host Intrusion Prevention System (HIPS) also, configured, monitored, installed, and updated the application as well.
* Denied/Approved Software applications after testing the software for vulnerabilities and malware.

**Client: Microsoft, India Oct 2015 – Apr 2018**

**Role: Information Security Analyst**

**Responsibilities:**

* Develop and recommend security controls, identify key security objectives to maximize software and system security while minimizing disruption to plans and schedules.
* Assessing the enterprise architecture and identifying the critical assets.
* Discovering the vulnerabilities and sorting the application domain user groups.
* Perform Penetration Testing and conduct critical server, security administration and infrastructure architecture diagnostic to conduct Network Security Assessment
* Perform Black Box application testing and review of application architecture and secure code.
* Strong familiarity with OWASP Top Ten, NIST, and MITRE ATT&CK
* Understanding of both application and network layer security considerations and how to fix them such as: buffer overflow, ToC vs.
* ToU, input validation, encapsulation, insecure protocols, MITM attacks, SQLi, etc.
* Educating the users on 'Social Engineering' such as Tail Gaiting, Password Sharing, and information
* Sharing, Strolling, Dumpster diving etc.
* Mentor and train others in information security in addition to training for other technical groups.
* Participated in forensic recovery and analysis.

**Client: Avaya, India May 2012 – Sep 2015**

**Role: Security Analyst**

**Responsibilities:**

* Resolved all LAN/WAN connectivity other issues.
* Analyze Vulnerabilities reports from various scans and assessments by acting on high risk / critical Vulnerabilities to other Vulnerabilities.
* Management of system security and file system security policies and analyzing systems to determine ways of improving performance.
* Conducting routine checks, warranty claims, hardware failure, replacement, software up-gradation, download patches and hotfixes.
* Infrastructure deployment from the very basis to complete function and Information Security Policy as per PCI-DSS Audit Compliance.
* Performing OS updates and upgrading applications.

Top of Form