Hari Priya Edupuganti

harie2070@gmail.com   |   469-319-3550 | www.linkedin.com/in/hari2070

Summary

Experienced Professional Experience as an IT Security Professional in IT Infrastructure, Cloud, Risk security, Information Security, and Cyber Security. Installed, configured, and provided oversight of SEPM and SQL servers, Symantec Endpoint Protection client configuration, troubleshooting, (SEPM) Server management, design, build, and infrastructure. Hands on experience in standing up AWS accounts, migrating workloads, enforcing security and automation best practices. Involved in Cloud Security Infrastructure and design for clients in - house Azure Applications Deployed in the cloud and on-premises using Amazon Web Services (AWS) and Single- Server Support. Information-security expert with a diverse technical background in enterprise networking, server infrastructure, database technologies, and system security. Experience in configuration management and policy implementation. Experience in managing Network infrastructure security using HPE ArcSight ESM/ Splunk for monitoring and classifying and responding to incidents and threats. Experienced with Symantec DLP Policies (DLP templates) compliance and regulation standards such as SOX, PCI, and HIPAA. Supporting for Enterprise customers on Microsoft Azure (IAAS, PAAS, and SAAS). Experience configuring and deploying McAfee modules and products like McAfee epos, McAfee VSE, McAfee HIPS, McAfee Endpoint Encryption, McAfee Network DLP, McAfee DLP Endpoint, McAfee SIEM. Performed System Administration Tasks for Symantec Data Centre Security (DCS). Knowledge of distributed Splunk installation with Forwarders, Clusters, Search head cluster. Experience with network monitoring with SIEM IBM QRadar and Wireshark, Information Security & Network security configuration and functions. Experience in configuring deployment server, Splunk Apps and add-ons. Hands on experience with several vulnerability forms i.e., SQL injection, XSS etc. Hands on Experience with Security frameworks such as NIST, HIPAA Experience with NIST SP A and NIST SP. Perform vulnerability scan with Nessus for improper configurations, missing patches, hosts, network, and insecure credentials and accounts. Having hands on experience for Documentation and log analysis.

Skills

|  |  |
| --- | --- |
| * TCP/IP * OWASP * Firewall * IDS * IPS * Vulnerability Management * Web Application Scanning * Threat Protect * Policy Compliance * Cloud Agents * Asset Management * Governance * Risk Management and Compliance * Sourcefire * Nexpose * Forcepoint | * Rapid7 * AWS * Splunk * LogRhythm * HP ArcSight * Metasploit * NMAP * Wireshark * Kali * Symantec DLP * MacAfee epos * Nessus * Ethereal * Snort * RSA Authentication * Kali Linux |

Professional Experience

|  |  |
| --- | --- |
| **Maximus** | Denver, CO  Cyber Security Analyst  *04/2023 - Current* | * Responsible for monitoring and, providing analysis in a 24x7x365 using various SIEM, IDS/IPS tools * Leveraging AWS Native Security services for Cloud Security Operations Also using External tools and integrates with AWS environments and accomplishes the desired objective of Compliance and Audit * Worked on IDS/IPS Controls operation and monitoring, Endpoint Security and Control, Vulnerability Management, WAF, DDOS, File integrity, Advanced Endpoint Malware Protection, Email Security, Threat Intel, Secure Web Gateway, SIEM and Log Management * AWS Cloud Operations 24/7 support Lead * Involved in security product assessments such as Palo Alto, Twist lock, Azure Firewall * Development of Cloud Formation template automating the creation of VPC and associated AWS resources for the application * Part of security team and performing analyzing VAPT assessment and closing loop holes in AWS Infra * Developed an AWS security roadmap which included the AWS services and 3rd party tools to be utilized in the AWS cloud for security monitoring * Developed an AWS security group strategy, determined naming conventions, owners and approval process for security group changes requests in a promote-to production environment * Verify that the Windows Virus Definitions on the SEPM are within 24hours from those reported by Symantec * Experienced in administering, upgrading, and troubleshooting problems with McAfee ePO, McAfee ENS, McAfee NDLP and McAfee NDLPE * Schedule scans on Symantec and reviewing results and quarantine risk data * Perform and maintain SAST, DAST, IAST and RASP best practices * Manage Splunk configuration files like inputs, props, transforms, and lookups * Upgrading the Splunk Enterprise to 6.2.3 and security patching * Deploy, configure and maintain Splunk forwarder in different platforms * Ensuring that the application website is up and available to the users * Continuous monitoring of the alerts received through mails to check if all the application servers and web servers are up * Create Splunk Search Processing Language (SPL) queries, Reports, Alerts and Dashboards * Perform technical analysis on data de-identification tools * Perform data de-identification implementation in the non-production environment * Scan and identify using data discovery for sensitive data containing PII, PHI, PCI, and GDPR information * Ensuring the database refresh containing any sensitive data is detected and masked as defined in the policies * Installing and Troubleshooting McAfee 8.8, ePO 4.5 * Working closely with Appscan, Symantec and Rapid7 for any malware activity on environment * Ensuring Symantec DLP policies are in place and scanning the environments for incidents * Assisting in DLP policy development for the non-production environment * Monitoring the enforce console for incidents and troubleshooting * Provide real time intrusion detection host-based monitoring services using Symantec Endpoint * Assist with the development of process and procedures to improve incident response times, analysis of incidents, and overall functions * Provide network intrusion detection expertise to support timely and effective decision making of when to declare an accident * Actively monitored and responded to activity impacting various enterprise endpoints facilitating network communication and data handling (McAfee End Point Security, DLP, Splunk) * Data Loss Prevention suit, Symantec DLP Product - Implementation and deployment as the champion team * Gained experience with Symantec DLP Software: DLP Cloud Prevent for Microsoft Office 365, DLP * Assisted engineers with Splunk troubleshooting * Created Splunk dashboards for investigations * Monitor and investigate SOC incidents and alerts with McAfee EPO * Document all activities during an incident with status updates during the life cycle of the incident * Analyze network and host-based security appliance logs (Firewalls, NIDS, HIDS, Sys Logs, etc.) |

|  |  |
| --- | --- |
| **Centene Corporation** | St Louis, Missouri  Cloud Cyber Security Analyst  *10/2021 - 03/2023* | * Implement and maintain NGA Amazon Cloud Service (AWS) security instances and deploy security infrastructure * Deploy Palo firewall, Panorama, Cisco FTD, FMC and F5 on AWS east and west regions VDSS (Virtual Data Center Security Stack) with redundant availability zones * Advice and Recommendation to management for AWS security posture improvement * Enabled and configure cloud trail logs for all VPC's in all AWS accounts * Monitored cloud environments (AWS) for potential threats and vulnerabilities using security tool, Redlock, to process logs and generate alerts based on rule criteria * Installed and managed detection servers and cloud detectors * Deliver the implementation, setup, and management of Symantec DLP * Provide a solutions-driven, customer-centric approach to clients' data-security challenges * Performed Single Tier Installation of Symantec DLP for test purpose * Also performed two tier and three tier installation * Performed activities including requirement analysis, design and implementations of various client server-based applications using Splunk 5.x, Splunk 6.x * Experience implementing an operational Splunk environment * Review, recommend changes and improvements * Responsible for monitoring and, providing analysis in a 24x7x365 Security Operation Center (SOC) using various SIEM (Splunk), IDS/IPS software tools * Worked with Symantec DLP version 14.6 and 15.0 * Provide DLP support to end users remotely and Onsite * Manage and deployed 3000+ endpoints and 100+ detection servers * Managed DLP Users and their roles * Analyze network attacks, blocks, detects, and regular Health checkups in environment * Tuned policies for HIPPA, HITECH, PII, PCI, PHI and SOX * Scanned File servers, Distributed machines, documents and email repositories, web content, applications, and databases * Manage system events and messages * Worked with saved system reports, configure event thresholds and triggers, enable syslog server, log review, configure system alerts, and configure enforce server to send email alerts * Involved in firewall deployment and management in Azure such as Palo Alto, Azure Firewall * Developed incident management module to automate the existing incident Management and Incident response process thereby reducing the manual effort of incident analyst by 40% * Configure response rule for endpoint detection, Network Prevent detection, Cloud storage detection, and data at rest detection * Created and managed 50+ agent groups * Assign appropriate policy and response rules to agent group * Investigated new DLP technologies, Software, patches, and security packages, which improve system performance and system procedures * Become a trusted advisor in Symantec DLP with our customers and clients |

|  |  |
| --- | --- |
| **CBRE** | Dallas, TX  Cyber security Analyst  *02/2019 - 09/2021* | * Provided necessary designs and implemented security solutions for egress/ingress points using IDS/IPS sensors across the networks to provide better incident handling and event monitoring * Developed cyber security standards on NIST frameworks and ensured their proper implementation to reduce risk of vulnerabilities to IT assets * Developed various functions including identifying, protecting, detecting, responding and recovering for performing concurrent and continuous operation of dynamic security risk * Reported compliance and operational metrics for network security infrastructure * Worked with vendors, IT personnel and various departments to deploy new or updated technologies * Conducted routine hardware and software audits of all supported systems to ensure compliance with established standards, policies, procedures and other requirements * Periodic security assessment of firewall, routers, switches, VPNs and other network components' security configurations * Provided support in investigating any actual and potential information security incidents * Experience with deployment of Symantec DLP- Endpoint Prevent, Network Prevent for Email, and Network Prevent for Web, Network Discover, and ITA * Installed and applied Qualys Guard appliances and ran various standard reports * Responsible for supporting customers with Symantec products including Ghost Solution Suite, Deployment Solution, and Symantec Endpoint Protection * Provided real time intrusion detection host-based monitoring services using Symantec Endpoint * File Integrity Monitoring - Infrastructure Operations and Administration of Symantec Data Center Security Server * Deploying and Managing Symantec Endpoint Protection |

|  |  |
| --- | --- |
| **Amigos Software Solutions** | Hyd, India  Cyber Security Analyst  *06/2016 - 11/2018* | * Responsible for tracking insider threat alerts involving PHI/PII information * Performed risk analysis and led remediation efforts for threats and vulnerabilities in response to industry news and vulnerability assessment tool results * Responsible for information security: Vulnerability management, scanning and remediation of all networked systems * Tested and created the mobile hardening policy for all cellular devices; Company owned and BYOD * Researched and documented briefings on threat reports and assessments * Created the Security Operations Center runbook, a concise procedural guide to handling common security events * Assisted in the researching of new security toolsets to include: next generation firewalls, Endpoint protection, Security Automation and threat intelligence collection/collaboration tools * Designed and initiated Insider threat monitoring policies and procedures for databases containing PHI/PII * Assisted with Social media exercises including the coding and development of security applications * Assisted the Special Investigations Unit (SIU) with internal employee fraud and misconduct investigations * Conducted forensic investigations for both employee fraud and malware analysis * Proactively protected PHI/PII through use of Data Loss Prevention (DLP) * Monitored for access and exfiltration of sensitive data * Built active content and logic in SIEM for existing and emerging monitored applications * Assisted with Symantec DLP Operational alerts, policies, monitoring, investigations and creating Reporting * Delivered onboarding and security training to new employees * Delivered weekly and monthly Security Metrics for the CEO and IT Stakeholders |

|  |  |
| --- | --- |
| **Avon Technologies Pvt Ltd** | Hyd, India  Information Systems Security Analyst  *08/2015 - 05/2016* | * Provided computer security incident response support to the Confidential bureau of Confidential * Collaborated with the Computer Technology Officer (CTO) to maintain and operate HBSS, which includes generating custom reports, host system monitoring, configuration, and maintenance * Established and maintained safeguards against unauthorized access, destruction, and loss or alteration of data * Researched and documented briefings on threat reports and assessments * Established network software parameters used for insider threat analysis; e.g., ArcSight security authorization tables, configuration definitions, and file access tables * Assist staff in defending assets from unauthorized and malicious activity & provide knowledge/expertise in personnel transfers * Monitored and evaluated system's compliance with IT security requirements in accordance with Intelligence Community Directives (ICDs) 502/503, Committee on National Security Systems Instruction (CNSSI) 1253, and National Institute of Science and Technology (NIST) * Configured and monitored Intrusion Detection Systems (IDS): read, interpret and analyze network traffic and related log files * Correlated data from multiple sources (IDS, IPS, HIDS, HIPS, ArcSight Logger & ESM, HBSS, DMZ logs), data acquired through computer forensics & situational awareness data sources, vulnerability repositories, cyber threat reports & prioritizes events for incident handling * Created network diagrams based on site topologies for use in identifying security flaws * Implemented policy and procedural controls covering physical security, application and data security, system software security, contingency planning, and compliance with personnel clearance procedures |