**Jithendra.Popuri**

**LinkedIn:-** [**linkedin.com/in/jithendra-chowdary-p**](linkedin.com/in/jithendra-chowdary-p)

[**jithendra30.popuri@gmail.com**](mailto:jithendra30.popuri@gmail.com)

**+1 940-315-0 913**

**Sr. Cyber Security Analyst**

Work Summary:

* Around 9+ years of experienced Professional as an IT Security Professional in IT Infrastructure, Threat Intelligence, Risk Management, SOC Analyst, SIEM, Vulnerability Management, Penetration Testing, Validation, Information Security, and Cyber Security.
* Proficient in leveraging SIEMs (Security Information and Event Management) to collect, correlate, and analyze security logs and events from various sources, enabling proactive threat detection and incident response.
* Experience in utilizing proxy solutions to monitor and analyze network traffic, identify suspicious patterns or anomalies, and detect potential threats or malicious activities.
* Skilled in sandboxing techniques and tools to analyze and detonate suspicious files, URLs, or email attachments in a controlled environment, uncovering advanced malware and zero-day threats.
* System Security and Administration Professional with expertise in Information Security Management, Firewalls, IDS, SIEM, Penetration Testing, DLP, and industry security standards e.g. ISO 27001:2013, NIST 800 series, NISPOM, COBIT, HIPAA, SOC, SOX, etc.
* Proficient in implementing and adhering to NIST 800-53v5 guidelines and controls.
* Extensive experience in conducting security assessments and audits based on NIST 800-53v5.
* Skilled in developing and maintaining system security plans (SSPs) in accordance with NIST 800-53v5.
* Skilled in identifying and mitigating security risks by applying NIST 800-53v5 controls.
* Proficient in utilizing the Diamond Model, Cyber Kill Chain, and MITRE ATT&CK framework to analyze and mitigate cyber threats effectively.
* Experience in applying the Diamond Model to understand threat actors, their capabilities, and their motives, enabling proactive threat intelligence and incident response.
* Knowledgeable in the Cyber Kill Chain methodology, allowing the identification and analysis of the different stages of a cyber-attack, from reconnaissance to exfiltration.
* Skilled in leveraging the MITRE ATT&CK framework to map and analyze adversary tactics, techniques, and procedures (TTPs) to enhance threat detection and response capabilities.
* Hands on experience with SAST and DAST using tools like HP Fortify, Burp suite, HP Web Inspect, Check Marx and IBM AppScan.
* Utilized Digital Guardian to protect most valuable assets with an on-premises deployment or an outsourced managed security program (MSP).
* System Security and administrator Professional, Facility Security Officer (FSO), Information Systems Security Officer (ISSO), Information Security Management, Firewalls, IDS, Penetration Testing, and industry security standards e.g. ISO 27001:2013, NIST 800 series, HITRUST, HIPPA, GDPR and CCPA, and NISPOM regulations.
* Resolved vulnerabilities in the WebEx and Fed RAMP GRC environments, POA&M & NIST, using automated scripts created in Python, PowerShell, Bash.
* Worked on GRC policies like - ISO Standards - Planning, Implementation and Management of ISO 27001:2013 Information Security Management System (ISMS) and ISO 20000-1:2011 Service Management System (SMS).
* Experience in Splunk-friendly regex expressions and optimizing Splunk search queries with optimal performance.
* Getting different log sources to send data to Splunk along with creating and tuning Technical Add-Ons for proper field extractions using regex
* Build threat intelligence capability and integrated 200+ threat intelligence feeds supporting STIX/TAXII. integrated with security controls, enhanced investigations and build threat connections to external partners

Technical Skills:

* Antivirus: McAfee Virus Scan Enterprise, Symantec, Endpoint Protection Suite
* DLP: Websense, Symantec & McAfee
* SIEM: Splunk ES, McAfee, ArcSight, Qradar, Log Rhythm
* PEN TESTING TOOL: BurpSuite, CheckMarx SAST, Red Team, HP Fortify, IBM AppScan, Contrast Security, OWASP Zap, Nmap, Kali Linux, Postman, Rapid7 Nexpose, ReconNG
* End Point Security: McAfee Suits (VSE, HIPS & HDLP), McAfee MOVE AV, Safeboot
* IPS/IDS: McAfee IPS, HP Tipping Point, Cisco IDS, SecureWorks IDS/IPS
* DAST and SAST tools: IBM AppScan Enterprise (ASE), Standard & Source editions, HP Web Inspect, BurpSuite Pro, Acunetix, Fortify SCA, SQLMAP, Burp Suit
* Threat Intelligence Platforms - MISP, YETI, CRITs
* Cloud Security: AWS, Azure, OpenStack, Docker, Ansible, Chef, Ansible, CI/CD, Terraform
* Proxies/Sniffers Tools: Burp Suite, Web scarab, Wireshark, DirBuster
* Vulnerability Management Tools: Foundstone, QualysGuard, Nessus, Nmap, Nexpose, Wireshark
* Security Tools: Splunk ES, McAfee Vulnerability management solutions, Burpsuite, OpenVAS, Nessus, Qualys, SolarWinds, ForeScout, IBM – ICS

|  |  |
| --- | --- |
| Technical Skills: | |
| Risk, Compliance, Architecture, Vulnerability, Threat Modeling, Threat Hunting, Audit & Testing | Information security, Cloud Security, IT / Cyber GRC & Certification Program, Network & Infrastructure Security, 3rd Party / Vendor risk, IT & Cyber Audits, IT Service Management, data governance, resiliency, windows and iso/LINUX |
| Assurance Standards & Frameworks | NIST CSF, CIS, ISO 27001/2, SOC 1&2, ENISA, GDPR, HITRUST, SANS ICS, SANS 20, CompTia+, FedRamp, PCI, HIPAA, SAMA CSF, NCA, .NET, COBIT, TOGAF, ISA/IEC 62443, OWASP, SOX 1 & 2, MITRE- ATTACK Framework, CMMC |

CERTIFICATIONS

|  |  |
| --- | --- |
| * C.E.H | * Introduction to Cyber security |
| * AWS-Architect | * Incident Response Handler |
| * Endpoint security | * Data Analytics Essentials |
| * Operating systems | * Palo Alto Network Cyber security |
| * AWS-Cloud Security | * Cyber Security IT Professional-Google |
| * Python Essentials-1&2 | * SOC (Security Operation Center Level-1) |
| * Cyber threat management | * Vulnerability Assessment & Penetration Testing |
| * Cyber Security Essentials | * Network Defense & Addressing Troubleshooting & Configuration |
| * Red Hat Enterprise Linux | * CISA IT Components and Industrial Control Systems (U.S.A Homeland security) |
| * Java Script Essentials -1&2 * Creating Complains Reports * Splunk * Qradar SIEMs | * CISA IOT & ICS Domains & Communication (U.S.A Homeland security) * ISIE(Imperial Society of Innovative Engineers Drive Dream India) * Networking with Cisco Packet Tracer |

EDUCATION

* Bachelors in CSE klef Koneru Lakshmaiah Education Foundation (Deemed to be University):-2014.

Speclization In Cyber Security

PROJECT

As a professional in information security, I have led and participated in multiple Data Loss Prevention (DLP) initiatives that protect confidential data and guarantee adherence to regulations. The establishment of strong data protection procedures within the company was made possible in large part by these efforts. This project encompassed the implementation of Symantec Data Loss Prevention (DLP) across all endpoints, ensuring secure data management and preventing unauthorized access. Additionally, I orchestrated the migration from McAfee EPO to Carbon Black, integrated cloud-native security services, and configured robust encryption protocols for data at rest and in transit. Collaborating closely with compliance teams, I ensured adherence to industry standards, while also implementing and maintaining security controls on AWS. This project not only strengthened our overall security framework but also demonstrated my proficiency in orchestrating complex security measures, particularly in cloud environments, and my commitment to maintaining a resilient cyber security landscape.

“The Holistic Cloud Security Enhancement project was undertaken to fortify our cloud environment against evolving threats, integrating cloud-native security services, compliance measures, and robust threat detection capabilities. By implementing encryption for data at rest and in transit, enforcing IAM controls and RBAC mechanisms, and conducting regular risk assessments and forensic analysis, we bolstered our defenses and ensured adherence to industry standards. Collaborating closely with vendors, optimizing security tools, and prioritizing continuous improvement initiatives, we enhanced incident detection and response capabilities while maintaining a resilient and secure infrastructure. Through these efforts, we safeguarded our critical assets and data, demonstrating our commitment to proactive security measures in an ever-evolving digital landscape.

WORK EXPERIENCE

**Client: UBS, Weehawken, NJ Duration: June 2022 to Present**

**Sr. Cyber Threat Intelligence Analyst (RISK MANAGEMENT)**

**Responsibilities:**

* Implemented Symantec DATA Loss prevention to secure all end points. Configured and instrumented Symantec management console, Symantec management server and Symantec database on Oracle.
* Experienced in analyzing McAfee DLP events and reports, as well as migrating from McAfee EPO to Carbon Black.
* Coordinate and conduct event collection, log management, event management, compliances automation, and identity monitoring activities using SIEM platform.
* Delivering DLP implementation project including full PLM deliverables: requirements, designing, testing, pilot and global implementation.
* Creating new certificates in Venafi, renewing the PKI certificates in Venafi and revoking and replacing the certificates.
* Provided security audits for Oracle and Sybase installations.
* Review System and firewall logs based on individual preset client policies, rules, and standards; also review all host activity for specified timeframe.
* Utilized cloud-native security services and APIs to protect cloud workloads and data, and configured encryption for data at rest and in transit using cloud provider APIs.
* Collaborated with compliance and audit teams to ensure both cloud security and IAM compliance with industry standards and regulations.
* Provided support for privileged access management (PAM) solutions within the IAM framework.
* Implemented IAM controls for identity lifecycle management to automate user provisioning and deprovisioning.
* Conducted RBAC training and awareness programs to educate employees on their access rights and responsibilities.
* Performed RBAC audits to identify and remediate excessive or unauthorized access permissions.
* Collaborated with compliance and audit teams to ensure RBAC compliance with industry standards and regulations.
* Lead multiple engagements specific to industrial control systems (ICS), IT and OT cybersecurity convergence, Internet of Things (IoT) and supply chain management. Minimizing risk and ensuring business continuity by limiting the impact of a security breaches.
* Provided technical support and troubleshooting for Imprivata solutions, resolving issues promptly and ensuring high levels of customer satisfaction.
* Architect the holistic security design related to the SAP implementation covering Infrastructure, network, encryption, SSO, SAP User security, SAP GRC and security models
* Provided ICS cyber security advice in client engagements (including assessment, design and implementation of security in Linux environments and security infrastructure for IT/OT risk solutions) Provided professional analysis through trusted expertise
* Configuring rules and Maintaining Palo Alto Firewalls& Analysis of firewall logs using various tools
* Establish standard operating procedures for embedding Cyber security driven processes into the agile Software Development Life Cycle (SDLC).
* Conducted regular risk assessments and vulnerability scans to identify potential threats and vulnerabilities in systems and networks.
* Build relationships with enterprise - wide customers and Oracle representatives to create clear and effective communications and to address customer needs across the systems we support.
* Utilizes NIST 800-53A and NIST 800- 53 rev-4 to review implemented controls and enter information into the Requirements Traceability Matrix (RTM) and findings into the Security Assessment Report (SAR).
* Build Inbound and Outbound Security Assertion Markup Language (SAML) Services on F5 Local Traffic Manager (LTM).
* Implement strong authentication mechanisms to ensure that only authorized users or devices can access the embedded system.
* Employed authorization controls to define and manage access levels for different users or components, and utilized encryption techniques to protect sensitive data both at rest and in transit..
* Secure communication channels using protocols like TLS/SSL to prevent eavesdropping and tampering.
* the cloud platforms proficient in, such as AWS, Azure, Google Cloud Platform (GCP),
* Implemented and maintained security controls on AWS, ensuring a secure cloud environment for critical applications and data.
* Designed and implemented IAM policies, reducing unauthorized access incidents by 70%.
* Led the implementation of data encryption protocols, improving the security of sensitive information both during transfer and while stored.
* Coordinated the response to security incidents, including escalation, investigation, resolution, and reporting, demonstrating strong leadership and decision-making abilities.
* Forensic analysis of end user systems and servers to identify indicators of compromise (IOCs) and determine the root cause and impact of security incidents.
* Administered and optimized a wide range of security tools, including Security Information and Event Management (SIEM) systems, log management, intrusion detection/prevention systems, antivirus, and other security technologies, enhancing incident detection and response capabilities.
* Collaborated with server owners, system custodians, and IT contacts to conduct security incident response activities, obtain access to systems, collect digital artifacts, and implement containment and remediation actions in a timely manner.
* Implemented continuous process improvement initiatives, including updating and improving system forensics process documentation, protocols, and standard operating procedures (SOPs) to enhance the efficiency and effectiveness of incident response operations.

**Client: WellCare Health Plans, Newburgh, NY Duration: June 2021 to May 2022**

**Network Security Engineer**

**Responsibilities:**

* Engaged with new acquisitions to design network taps for their core data centers.
* Create and manage VMware virtual server environments to support various tools including Palo Alto, EIS, Rapid7, Fire Eye and Net brain VMs that are deployed in new acquisition space.
* Review existing Ixia network tap solution and recommend new solutions for network taps and network traffic discovery to support M&A integration agenda.
* Reviewed existing NetBrain network traffic analyzer, Palo Alto virtual firewall solution, and internet network hub, recommending new solutions for network discovery, perimeter security, and meeting enterprise security requirements.
* Co-ordinate with Project Managers of the work being done and stay on top of the deployment and cutover schedules.
* Recommend efficient solutions to speed up the Ixia network tap solution deployment.
* Co-ordinate and Collaborate with the Network Engineers on-site at Business Partner location on piecing together the information required for the deployment.
* Troubleshooting as required during outages and device failures.
* Documentation of all the changes made, information gathered and providing them during the hand-over to the Operations team.
* Implement new Meraki Security Appliance, like MX84, MX100 at the end offices of the Acquired Entities to replace their existing firewalls and route their traffic through Regional Hubs which has the head end like MX250 or MX400.
* Configuring the various tools part of the Pathfinder kit and get it ready to be deployed based on the Customer's requirements.
* Design and implement Cisco ACI Multisite Fabric across two data centers in an active-active state. Utilized the ACI default blacklist model to implement L4 segmentation with the help of EPG, Contracts and filters
* Implemented Cisco ACI multi-site design with Multi-site orchestrator acting a central hub for policy control
* Performed software upgrades on Cisco ACI Fabric and Multisite controller to remediate vulnerabilities and to avail new features
* Designed and created a dedicated service block for the client environment with Nexus 9K switches and used VX-LAN BGP EVPN to extend L2 across the data centers using multicast/anycast-gateway
* Implemented network segmentation across DTE network using Next Gen Firewalls to protect all the data center infrastructure from user traffic
* Implemented service graphs within the ACI fabric to implement L7 inspection via an external Palo Alto firewall for key and critical enterprise applications to filter East-West traffic within the ACI environment
* Installed a new Palo Alto firewall to protect datacenter resources and implement North-South traffic filtering
* Experience in working with various regulated DMZ environments such as PCI, SOC, DCS & PCN networks
* Write technical documentation for the newly designed and installed networks, to facilitate quick troubleshooting and enhanced support in future
* Troubleshooting application issues with various network packet captures and examining the data flow by observing the TCP, UDP, HTTP, HTTPS etc., communications over LAN/WAN.

**Thomson Reuters, Eagan, MN June 2019 – May 2021**

**Sr. Cyber Engineer**

**Responsibilities:**

* Worked on SIEM, as well as solar winds, Symantec end to end point security for malware detection and threat analysis
* Perform vulnerability assessments of Systems/Network device. Working knowledge of some Security tools like Cyber Ark, IDS/IPS, SIEM, PIM, and Cisco ASA Firewalls.
* Assessed threats, risks, and vulnerabilities from emerging security issues and also identify mitigation requirements.
* Support IT teams based on latest risks and possible remediation. Involved in integration of Splunk with Service Now, Active directory and LDAP authentication
* Used Splunk Deployment Server to manage Splunk instances and analyzed security-based events, risks & reporting.
* Configured and deployed Azure Office 365 DLP HIDS on Windows Server 2008 and 2012 and desktops.
* Provided physical and logical designs for Oracle, Sybase and Informix databases using ER/Win.
* Administered various shell and Python scripts for monitoring and automation.
* Generated reports and metrics to measure DLP effectiveness, track incidents, and demonstrate compliance with data protection regulations.
* Collaborated with cloud governance teams to define and enforce cloud security policies and standards.
* Assisted in the development of disaster recovery and business continuity plans for cloud environments.
* Provided guidance on securing serverless functions and APIs in cloud-based microservices architectures.
* Conducted IAM risk assessments to identify vulnerabilities and potential security gaps.
* Managed IAM exception handling and request processes to address unique access needs.
* Assisted in IAM change management and control procedures to ensure secure policy updates.
* Provided support for RBAC-based threat detection by monitoring and alerting on unusual role access patterns.
* Conducted RBAC policy reviews and updates to adapt to changing business requirements.
* Implemented automated RBAC provisioning and de-provisioning to streamline user lifecycle management.
* Stayed updated with the latest features, updates, and best practices related to Office 365 DLP to ensure proactive protection and mitigation of data loss risks.
* Hands on experience to manage Palo Alto and check point with including set up new infrastructure, adding new route-based policy, NAT, site to site VPN, Global Protect.
* Deliver operational efficiencies and enhance GRC efficacy and control by delivering a system of engagement and real time actionable insights about the enterprises' risk and compliance operations
* Proficient in configuring and maintaining Imprivata solutions, including SSO, multi-factor authentication (MFA), and secure communications.
* Implemented various efficiencies solutions for all locations including Disaster Recovery site such as Nagios, Dell Kace, Imprivata, MPLS and Dell SecureWorks (IPS/ IDS), SAN, Virtualization, UPS Solutions, Email Encryption, Cisco and 3rd Party Connections.
* Managed logical and physical data structures, resolved errors from database links, snapshots and table space fragmentation.
* Developed Stored Procedures and Triggers in Oracle and Sybase.
* Actively participated in incident response activities related to Office 365 DLP, investigating and mitigating data breaches and policy violations.
* Generated detailed reports and dashboards to provide visibility into data exposure, access patterns, and compliance violations.
* Integrated Varonis Data Discovery with other security solutions such as SIEM and DLP systems for centralized monitoring and incident response.
* Actively monitoring and analyzing threat intelligence feeds, open-source intelligence (OSINT), and industry reports to stay updated on emerging threats and evolving attack techniques.
* Conducting threat assessments and risk analyses using the Diamond Model, Cyber Kill Chain, and MITRE ATT&CK framework to identify critical assets and potential impact from specific threat actors.
* Familiarity with the NIST Risk Management Framework (RMF) and its integration with NIST 800-53v5.
* Strong understanding of NIST 800-53v5 control implementation strategies, including technical and non-technical approaches.
* Performed Static and Dynamic Analysis and Security Testing (SAST and DAST) for various applications as per firm’s security standards (i.e., OWASP, SANS 25).
* Implemented risk mitigation measures, such as implementing security controls, patch management, and incident response plans.
* Monitored and reported on key risk indicators, providing senior management with actionable insights to make informed decisions.
* Led incident response activities, including root cause analysis and the development of corrective and preventive actions to address identified risks.
* Conducted security awareness training to educate employees on risk management principles and best practices.
* Conducted security control assessments and provided recommendations for control enhancements based on NIST 800-53v5 guidelines.
* Developed and delivered training programs to educate employees on NIST 800-53v5 compliance and best practices.
* Worked closely with external auditors to ensure successful completion of NIST 800-53v5 compliance audits.
* Stayed up-to-date with the latest updates and revisions of NIST 800-53v5 and incorporated them into the organization's security framework.
* Conducted security assessments on networks and Industrial Control systems (ICS), designed cyber security solutions, supported the implementation of those solutions, and identify security trends and practices.
* Configuring and Troubleshooting Cisco Firewall/ASA, Checkpoint FW, Bluecoat Proxy SG.
* Worked on the OWASP top 10, CIS CSC, DLP, Data classification, and Encryption standards for Contractors and employees and experience with object-oriented programming (OOP) concepts using Python, C++, C#, and PHP.
* Deployed Azure IaaS virtual machines (VMs) and AWS Cloud services (PaaS role instances) into secure VNets and subnets.
* Providing fixes & filtering false findings for the vulnerabilities reported in the scan reports.
* Performed Static and Dynamic Analysis and Security Testing (SAST and DAST) for various applications as per firm’s security standards (i.e., OWASP TOP 10).
* Developed security policies and baselines for web applications. Performed compliance audits to ensure security policies and baselines have been adequately implemented.
* Documented security findings, recommendations and presented to the business users, executive committee and Compliance departments.
* Implemented and managed security appliances such as Imperva WAF, Splunk SIEM, and custom solutions designed to block, log and alert on potential security issues.
* Experience in conducting in-depth analysis of security events, alerts, and logs from SIEMs, proxy solutions, sandboxing, and endpoint detection systems to identify patterns, trends, and potential indicators of compromise.
* Familiarity with security incident response procedures and the ability to collaborate with incident response teams to investigate and mitigate identified threats or security incidents.
* Skilled in generating actionable threat intelligence reports and alerts based on analysis findings, providing recommendations for enhancing security controls and mitigating identified risks.
* Strong understanding of enterprise, network, system/endpoint, and application-level security issues and risks
* In securing in-vehicle networks (CAN, LIN, Ethernet) against cyber threats.
* Highlight any hands-on work with intrusion detection, network segmentation, and secure communication protocols in automotive systems.
* In conducting security assessments and penetration testing for automotive systems.
* Provide examples of vulnerabilities discovered and mitigated during assessments.
* Emphasize your work in ensuring the security of firmware in automotive embedded systems.
* Detail any efforts to secure boot processes, firmware updates, and integrity verification.
* Understanding and adherence to cybersecurity standards and regulations in the automotive industry (e.g., ISO/SAE 21434, UN R155).
* Developed and implementing incident response plans for automotive cybersecurity incidents.

**E-Trade, Financial, NYC, NY Mar 2017 to May 2019**

**Threat Intelligence Security Engineer (RISK MANAGEMENT)**

**Responsibilities:**

* Installing, Configuring, Administering and supporting the Windows 2003 Server, Windows 2003 Server, Windows 2000 Server, Windows 2000 Advanced Server, IDS server, SQL Server and Active Directory
* Worked on different networking concepts and routing protocols like RIP, BGP, EIGRP, OSPF and other LAN/WAN technologies.
* Experience with Symantec DLP and RSA DLP architecture and implementation for enterprise level. Designed Symantec DLP architecture, implemented Symantec DLP. Worked with Symantec DLP upgrades and patches. Implemented Symantec DLP Policy and Content Blade creation and tuning. Provided input into customer's operational and processes and procedures.
* Provided training and guidance to users and administrators on the usage and administration of Varonis Data Discovery tools and features.
* Stayed updated with the latest data protection regulations and industry best practices to ensure compliance and proactive data risk management.
* Actively participated in the evaluation and selection of additional Varonis modules and enhancements to enhance DLP capabilities and strengthen data security posture.
* Experienced with RSA DLP, Symantec DLP versions 12.5, 14.0, 14.5, and 14.6, Symantec DLP or native GPO controls and other tools.
* Worked on Symantec Data Loss Prevention (DLP) upgrading and migration to 14.6
* Worked on the latest industry standards and frameworks related to risk management, such as NIST Cybersecurity Framework and ISO 27001.
* Collaborated with internal and external stakeholders, such as auditors and regulators, to ensure compliance with applicable regulations and standards related to risk management.
* Collaborative team player with excellent communication skills, able to effectively communicate NIST 800-53v5 requirements to stakeholders and team members.
* Collaborating with cross-functional teams, including incident response, vulnerability management, and security operations, to develop and refine threat hunting strategies based on threat intelligence and adversary behaviors.
* Participating in red team exercises and simulated attacks to evaluate the effectiveness of existing security controls and enhance the organization's defensive capabilities.
* Implemented NIST 800-53v5 controls to enhance the organization's overall cybersecurity posture.
* Conducted regular security assessments and audits to ensure compliance with NIST 800-53v5 standards.
* Developed and maintained a comprehensive inventory of system assets and their associated security controls in alignment with NIST 800-53v5.
* Contributing to the development and improvement of threat management processes and procedures based on industry best practices and lessons learned from the Diamond Model, Cyber Kill Chain, and MITRE ATT&CK framework.
* Implemented Application Security program (DAST and SAST) at the enterprise level to identify, report and remediate security vulnerabilities from applications deployed in DEV, PRE-PROD and PROD environments.
* Created a case for the suspicious issue and forwarded it to the Onsite SOC team for further investigation.
* Conducted Vulnerability assessment for a network using Tenable Nessus
* Provided support in life service security and network solutions (Checkpoint, Bluecoat, Cisco ASA)
* Conduct Burp Suite AppScan Source for Analysis DAST and SAST testing on WWB Applications.
* Utilized Splunk SIEM to solve active threats and alarms for over 40 client accounts
* Tested various threat vectors and presented evidence of intent to create signatures/rules to mitigate specific threats.
* Performed Static Application Security Testing (SAST) using tools such as HP Fortify and Dynamic Application Security Testing (DAST) using tools such as IBM AppScan.
* Documenting and reporting threat analysis findings, including identified TTPs, IOCs, and recommended countermeasures, to stakeholders and senior management.
* Keeping abreast of the latest developments in threat intelligence, threat modeling, and adversary techniques to continuously enhance threat management strategies and stay ahead of evolving threats.
* Proficient in using threat intelligence platforms and tools to manage, analyze, and share threat intelligence information with stakeholders and external partners.
* Knowledgeable in applying threat intelligence frameworks, such as the Diamond Model, Cyber Kill Chain, and MITRE ATT&CK, to enrich analysis and provide contextual information on observed threats.
* Familiarity with regulatory requirements and industry standards related to threat intelligence and incident response, such as GDPR, NIST Cybersecurity Framework, or ISO 27001.
* Strong analytical and investigative skills to identify patterns, trends, and correlations in data, and to conduct root cause analysis of security incidents or breaches.
* Collaborating with cross-functional teams, including security operations, vulnerability management, and threat hunting, to share intelligence insights, align security strategies, and improve overall cyber defense posture.
* , event categorization, and Incident reporting).
* Troubleshoot Symantec DLP Issues and provided support remotely for DLP issues.
* Customized and fine-tuned DLP policies to reduce rate of false positives in alerts and align them with business needs incident response. Configure HIPPA, HITECH, PKI, PCI, SOX, and PHI policies and rules.
* Configuring, implementing and maintaining all security platforms and their associated software, such as routers, switches, firewalls, intrusion detection/intrusion prevention, anti-virus, and SIEM.
* Deployed Splunk Enterprise on AWS to gain real-time visibility across AWS and entire IT environment.
* Experience with Windows, Linux, vulnerability assessment tools, firewalls, IDS/IPS, Nessus, NMAP, SIEM, DLP, Active directory user's attribute bulk modification in PowerShell, query user's details in PowerShell and export reports.

**Client: Ishir Infotech, Hyderabad, India Apr 2014 – Aug 2016**

**Network &Systems security Administrator**

**Responsibilities:**

* Responsible for maintaining network availability and reliability by proactive monitoring of network alarms.
* Monitoring, assuring network connectivity and security over connections to the systems and Internet.
* Administration, designing, planning, developing documentation and establishing policies for networks, network security and access controls.
* Serve as the first line contact for the Security Operations Center. Participate in incident handling processes such as incident discovery, analysis and verification, incident tracking, containment and recovery, incident response coordination, escalation, and notification. Assist in coordinating with other teams to remediate detected incidents.
* Successfully configured ESX servers for HA and DRS capabilities and managed DNS, DHCP, Remote Desktop Session Host, DFS, and Microsoft Failover Clusters.
* Performed L1 &L2 troubleshooting and escalating system issues to OEMs, vendors, 3rd line support for quick incident resolution.
* Identified potential causes of disruptions to network services including hardware failure, software failure, access issues, weather conditions etc. by analyzing health-check and preventive maintenance reports.
* Oversight purchasing of LAN, WAN equipment, ATMs, servers, PCs, printers, routers, switches and firewalls.
* Excellent experience in installation, configuration and administration of Active Directory and Domain with Windows server2003.
* Configuration of Network Printers, Plotters and installing of the same on user machines.Troubleshooting general IT Issues on user workstations.
* Provide support to end users relating to hardware and software, computer applications, LAN components and peripherals.
* Plan, build and configure network infrastructure within VPC with public and private subnets, configure routing tables and internet gateway.
* Performed general preventative maintenance tasks on computers, laptops, printers, and other authorized equipment.
* Rectify security risks on network printers by applying security applications and certificates.
* Active Directory and Group Policy administration, hardware configuration. User Support for VPN, MS Office, applications.
* Performed regulated changes to network live environment by adhering to standard Change management process.
* Configured Cisco Catalyst 2950T-24-port Switch and modems.Complete planning, building and administering LAN and troubleshooting the network.Applying Firewall using IP chains and Iptables.
* Work directly with ESM engineers and Account Information Security Officers to adjust alert criteria. Coordinated escalations to Forensic Analyst Team with recommendations for remediation.
* Evaluated and fulfilled requests from the Account Information Security Risk & Compliance Officers for each client and aligned with the appropriate runbook procedures to attain Client Service Level Objectives and Agreements
* Adjusted network alerts temporarily to suppress excessive alerts prior to engineers making permanent threshold changes.
* Aided management with administration and configuration of critical enterprise security systems and software such as McAfee ePO, McAfee DLP, McAfee Complete Endpoint Protection-Enterprise, Proofpoint, etc.