**PARTH TRIVEDI || US CITIZEN**

**Senior Cyber Security Engineer**

**Cell: 609-498-6709**

* Experienced Professional with over 10+ years of experience as an IT Security Professional in IT Infrastructure, SOC, Information Security, and Cyber Security.
* Managed information security assessments for three agencies within the Department of Transportation DOT.
* Experience of risk management and computer forensic tools, technologies, and methods. Experienced in IT security design and implementation with a solid understanding of disaster recovery, intrusion detection systems (IDS), intrusion protection systems (IPS), and web application firewalls (WAF). Analytical problem solver adept at managing network changes and troubleshooting network issues to ensure maximum up time.
* IT experience in Application Security, Security Life Cycle, SDLC, Penetration Testing, and Vulnerability Assessment using OWASP, NIST and CWE/SANS Special Publications.
* Experience with Windows, Linux, vulnerability assessment tools, firewalls, IDS/IPS, Nessus, NMAP, SIEM, Splunk, ArcSight, Rapid7, Routers, Switches, LAN/WAN, TCP/IP protocols, VMware, Endpoint Security, Cloud Security.
* Support and assist the CSOC in their investigations of cyber security events to identify potential security incidents.
* Generated notification based on different templates on record content values using RSA Archer.
* Execute Identity and Access Management (IAM) services, including, but not limited to Provisioning, Authentication, Authorization and Monitoring.
* Involved in vulnerability assessment, Patch management and penetration testing using various tools like Metasploit, Burp Suite, DirBuster, OWASP ZAP proxy, NMAP, Nessus, SQL Map, IBM AppScan enterprise, Kali Linux, Wireshark.
* Knowledge and experience in standard security and regulatory frameworks including ISO 27001/31000 , NIST 800 - 71, HITRUST CSF and PCI DSS.
* Developed security strategy and performing risk assessment, vulnerability assessment and working with the business to mitigate risks.
* IoT/ Cloud Solution Services Consultant
* In-depth understanding of Information Security Concepts, Vulnerability Assessment and Penetration testing.
* Expertise in improving the Risk and Control functions against Governance, Risk Management and Compliance.
* Maintained security infrastructure, including IPS, IDS, log management, and security assessment systems.
* Assessed threats, risks, and vulnerabilities from emerging Security issues.
* Expertise in improving the Risk and Control functions against Governance, Risk Management and Compliance (GRC).
* Experience analyzing cyber threats, as a malware analyst, incident responder, and digital forensics investigator.
* Strong understanding of malware analysis, data recovery, information security assurance, network forensics, hacking techniques, and digital forensics experience
* Experienced in performing analysis of the results from penetration test to identify the risks that need to be taken care of immediately.
* Perform ongoing gap analysis of policies, procedures, and practices as they relate to established guidelines outlined by NIST, OMB, and FISMA.
* Provide tactical leadership during incident response for products within team portfolio, coordinating with executive committee, production support, cyber-security operations center (CSOC), and enterprise fraud management teams.
* Involved in Cloud Security Infrastructure and design for client's in - house Azure Applications
* Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS/ IPS), Data Loss Prevention (DLP), forensics, sniffers and malware analysis tools.
* Advanced Knowledge in IPSEC VPN design connection and protocols, IPSEC tunnel configuration, encryption and integrity protocols.
* Commendable experience in auditing, implementing & managing HIPAA, SOX, GLBA, FFIEC, ISO, NIST, PCI DSS, FISMA, SAS 70 I & II Standards/Guidelines.
* Incidence responder, Offensive and defensive information security SME with skills on Web penetration testing, network penetration testing, network security assessment, and vulnerability assessment.
* Adept in penetration testing and forensic analysis. Certified in Cisco Network Associate, Kali Linux, PCI DSS Auditing, and worked on VoIP, HTTPS, SNMP, FTP, RDP, TCP, RTP etc.
* Monitored and investigated suspicious network activities, endpoints and threats utilizing a variety of tools such as ArcSight, Splunk, Carbon Black, FireEye, Cisco Talos, WireShark and Nessus
* Use of LogRhythm SIEM for investigations.
* Incident response and threat detection using Tanium.
* Experience on Fireeye for Management Systems and for Threat Intelligence.
* Experience deploying in the cloud and on-premises using Amazon Web Services (AWS) and Single- Server support
* Using network monitoring and IDS tools such as Wireshark and Snort.
* Support and implement information security projects for the enterprise to include SSL decryption, application filtering, and LogRhythm SIEM solution for the enterprise.
* Provided leadership in architecting and implementing security solutions towards Qualys and SIEM tools like Splunk, ArcSight, Solutionary, LogRhythm create logrhythm rules.

**Technical Skills:**

**Security Software:** Nessus, NMap, Metasploit, Snort.

**Web Application:** Manual SQL Injection, Manual Cross Site Scritping(XSS), Cross site request forgery(CSRF), SQLmap

**Frameworks:** NIST SP, ISO 27001/31000 , HIPPA, HITRUST CSF, PCI DSS.

**Security Technologies:** Symantec DLP, McAfee EPO, QRadar, Splunk, Cybereason, Trend Micro TippingPoint

**Qualys Continuous Monitoring:** Vulnerability Management, Web Application Scanning, Policy Compliance, Asset Management, Governance, Risk Management and Compliance.

**Frameworks:** NIST SP, ISO 27001/31000 , HIPPA, HITRUST CSF, PCI DSS

**Operating Systems:** Windows, Server 2012 R2, Linux

**Professional Overview**

**Senior Cyber Security Engineer**

**Quarterspot, Fairfax, VA May 2017 to Present**

* Analyze, investigate and respond to security events and incidents from IDS/IPS, SIEM, Firewall, Splunk, Log analysis, DLP, malware analysis and forensics tools (FireEye, Bit9, Security Analytics, Fidelis XPS and Wireshark).
* Schedule and initiate automated vulnerability scans in Nessus and IBM Scan, and manual verification of the vulnerabilities by conducting penetration testing to quantify the impact and calculate time frame for the patching.
* Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS/IPS), Data Leakage Prevention (DLP), forensics, sniffers and malware analysis tools.
* Analyzed threats to corporate networks by utilizing SIEM products (QRadar and Splunk) to assess the impact on client environments.
* Participate in ST&E Kick-off Meeting and populate the Requirements Traceability Matrix (RTM) per NIST SP 800-53A. Also done IDAM.
* Cyber Security readiness related to 5G Mobil network for Smart Cities, IoT and V2X devices Critical Infrastructure Protection (CIP) and CIS controls mapping to NIST framework as it relates to gas & oil, power grid and transportation industries.
* Develops cyber security solutions for transportation Industrial Control Systems and Supervisory Control and Data Acquisition (SCADA) systems in accordance with NIST 800 - 82.
* Assist in responses to external audits, penetration tests and vulnerability assessments.
* Aggregate and analyze all source information to include intelligence reporting, network security device logs, and host based security solutions to identify and mitigate advance threat activity
* Develop CSOC, NOC and CSIRT capabilities and manage daily events
* Expertise in improving the Risk and Control functions against Governance, Risk Management and Compliance (GRC).
* Performed functional testing of security solutions like RSA two factor authentication, Novel single sign on, DLP and SIEM
* Utilized various project management methodology & PMI process to enhance various cyber security programs within the Department. Managed the 24x7 DoT SOC/CIRT.
* Involved in vulnerability assessment, Patch management and penetration testing using various tools like Metasploit, Burp Suite, DirBuster, OWASP ZAP proxy, NMAP, Nessus, SQL Map, IBM AppScan enterprise, Kali Linux, Wireshark.
* Installed and configured IBM QRadar Network Insights appliance to enables attack prediction through real-time network traffic analysis.
* Analyzed threats to corporate networks by utilizing SIEM products (Arcsight and LogRhythm) to assess the impact on client environments.
* Discover, identify, mitigate and report intentional or unintentional unauthorized use of customer information and information systems.
* Monitored, managed and closed existing internal and external audit issues, and ensuring that internal systems are compliant with security Confidential security standards and controls including regulatory requirements.
* Anti-virus alert response due to alerts by Logrhythm (SIEM), McAfee, Cylance.
* Worked with IBM QRadar SIEM Integration and responsible for integrating the log sources with IBM QRadar.
* Configuring log generation and collection from a wide variety of products distributed across categories of servers, network devices, security devices, databases, and apps.
* Generate, review and update System Security Plans (SSP) against NIST 800-18 and NIST 800 53 requirements.
* Performed pen testing of both internal and external networks. The pen testing scope included O/S (Windows and Linux) and external facing web apps and database servers that store customer confidential information.
* Participated in Web Application Security Testing including the areas covering Mobile, Network, security, WIFI.
* Deploy and manage multiple global sensors to collect threat intelligence
* Experienced in performing analysis of the results from penetration test to identify the risks that need to be taken care of immediately.
* Perform analysis on security incidents using Splunk, Tanium, Windows Event and Symantec logs.
* Perform analysis of host or user activities using Tanium Dashboard and Tanium Trace for evidence gathering.
* Work as per of SOC team to briefing on emerging threats and events in accordance to run book
* Assist with the development of processes and procedures to improve incident response times, analysis of incidents, and overall SOC functions.
* Performing quantitative research design as it relates to IoT and V2X devices.
* Analyze Cyber Intelligence threats (advanced persistent threats) by investigating of cyber security incidents, assisting the DOT Inspector General, FBI, NSA, ARL (Army Research Lab), AFRL (Air Force Research Lab), and other law enforcement agencies with forensic analysis (Malware/shellcode analysis via. tools Encase, IDApro)
* Supports to generate all kinds of reports and extensively used in the workspace dashboards using RSA Archer and Forcepoint.
* Executed examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4
* Monitored and analyzed Intrusion Detection Systems (IDS) to identify security issues for remediation
* Perform cyber threat intelligence analysis, correlate actionable security events, perform network traffic analysis using raw packet data, net flow, IDS, IPS and custom sensor output as it pertains to the cyber security of communications networks, and participate in the coordination of resources during incident
* Performed manual security testing (Penetration Testing) on critical client applications.
* Conduct analysis, cyber threats, the discovery of its vulnerabilities, monitoring for cyber intrusions, troubleshoot and response to security incidents detected from hp arcsight or related SIEM. IDS/ IPS, and other security applications
* Extensive Experience with Symantec DLP and RSA DLP architecture and implementation for enterprise level.
* Installed and configure Enforce Server Administration console to manage Endpoints, policies, policy rules, Agent groups, Incidents, manage DLP servers, and etc.
* Installed and Configure Endpoint Prevent and Discover detection server to protect Data in use.
* Performed vendor File share scan with Symantec DLP by setting up Site-to-site VPN.
* 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 PCI, SOX rules.
* IT Experience in Application Security Testing particularly focused on performing technical activities such as Penetration testing, Code review, Secure Application Testing, Vulnerability Analysis based on OWASP.
* Served as Tier 1 support in area of network intrusion prevention and detection in CSOC under SMT.
* Worked in Security Incident and Event Monitoring SIEM platform - IBM QRadar, and Splunk.
* Tested various threat vectors and present evidence of intent to create signatures/rules to mitigate specific threats.
* Installed and configured IBM QRadar Network Insights appliance to enables attack prediction through real-time network traffic analysis.
* Monitor SIEM tool and triage all alerts as they come in to assure the network is safe
* Services monitored include, but are not limited to SIEM, IDS/IPS, Firewall, Cloud Environments, and Data Loss Prevention (DLP) SMTP and Web.
* Collaborated with internal Line of Business (Information Security, Supplier Manager, and Risk Management, Audit) and provided risk assessment disposition reports; evaluations and recommendations.
* Conduct tuning engagements with security engineers to develop/adjust SIEM rules and analyst operating procedures.
* Monitor critical infrastructure including firewalls, IDS/IPS devices, virtual networks, vulnerability scanners, VPNs, WANs, and disaster recovery sites.
* Performed scoping engagements, vulnerability assessments, web application penetration testing, network penetration testing, and phishing campaigns to test security controls and policies.
* Worked closely on Data Privacy control frameworks and related laws and regulations (ISO 27000 series, NIST).
* Investigated alerts created by IDS/IPS including malicious file uploads compromised servers, SQL-injections, and port scanning.
* Authored recommendations associated with findings on how to improve the customer's security posture in accordance with NIST controls
* Conducted Security Scans using Security Center (NESSUS) to identify System Vulnerability, risk assessment and technical report submission detailing the vulnerabilities, risk, and remediation action and review assessment results.
* Implemented ArcSight Logger within organization's syslog enclave for long-term data retention and analysis (SIEM).
* Developed Vulnerability Scanning process for all environment builds, and on-going monthly scanning reporting using Nessus.
* Monitoring of events from Data Loss Prevention (DLP) and other information security tools and determined appropriate next steps using knowledge of Corning businesses or processes.
* Utilized Security Information and Event Management (SIEM), Data Leakage Prevention (DLP), Intrusion Detection and Prevention (IDS / IPS), forensics, sniffers and malware analysis tools.
* Performed investigation, analysis, reporting and escalations of security events from multiple sources including events like intrusion detection, Firewall logs, Proxy Logs, Web servers.

**Cyber Security Engineer**

**Method 360, Northville, MI Oct 2015 to Mar 2017**

* Responsibilities includes supporting 24/7 SOC environment to ensure real time information security and prevent any cyber-attack from inside and outside network.
* Designs and implementation in all aspects of Information Assurance and Information Security (InfoSec) Engineering. Guidance on ISCM (Information Security Continuous Monitoring), assess and mitigate system security threats/risks throughout the program life cycle by validating system security requirements definition and analysis.
* Scheduled a Penetration Testing Plan throughout the organization and completed all the tasks in the given time frame.
* Conducted penetration tests on systems and applications using automated and manual techniques with tools such as Metasploit, Burp Suite, Kali Linux, and other open source tools as needed and report the findings.
* This included the design, development, and implementation of multiple independent Splunk instances that would be able to monitor SCADA environments and CDAs and also be able to forward alerts and logs to an independent off-site CSOC.
* Security Engineer for Transportation Security Administration
* Experience with 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.
* Designed & implemented the department SIEM (Arcsight) to monitor the DOT enterprise (over 20,000 assets). Administration of the DOT security infrastructure consisting of IDS/IPS systems (Snort, ISS, IDSM2, IPS, NFR, Checkpoint IPS1), Vulnerability Assessment tools (Foundscan and Nessus).
* Monitor compliance and ensure enforcement with all SOX, PCI DSS, HIPAA/HITECH, COBIT, and NIST requirements as applicable to the organization.
* Worked with tools like Burp Suite, DirBuster, HP Fortify, Nmap, Acunetix, Webinspect, Nessus, IBM app scan as part of the penetration testing, on daily basis to complete the assessments.
* Skilled using Burp Suite, Checkmarx, HP Fortify, SecureAssist, WAS, NMAP, Havij, DirBuster for web application penetration tests.
* Involved in Security Operation, Vulnerability and Risk Assessment, alerting 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.
* Implemented quality assurance review processes to ensure audit work conforms to the Standards for the Professional Practice of Internal Auditing and the standards established by ISACA.
* Perform compliance checks against industry standard and regulatory mandates such as FISMA, DISA, HIPAA, SCAP. Develop POA&M for mitigation as required by Risk Management Framework (RMF)
* Network Admin, logging and securing network data using RSA Archer (TCP/IP data analysis).
* Used McAfee ePolicy Orchestrator to monitor and identify potential intrusions and attacks for the Cyber Security Operations Center (CSOC).
* Conducted penetration testing on our web applications using some tools.
* Hunting within the network for potential threats based on intelligence reporting.
* Monitoring logRhythm dashboard for the suspicious alerts and provide efficient write-up for each alert.
* Using tools like LogRhythm in analyzing network, DLP email monitoring, Symantec SEP logs, firewall and proxy logs to determine the risk level of the alarms.
* Hadoop, Cloud AWS, Enterprise Risk Management, sox2, 404, pci, NIST, cobit, others.
* Delivering comprehensive prevention, detection and response status using FireEye, Symantec, and Qualys software.
* Vulnerability Assessment of various web applications used in the organization using Burp Suite, and Web Scarab, HP Web Inspect.
* Monitored IT audit activities with internal auditors, external auditors and third-party examiners and prepared management responses and remediation planning;
* Utilized Tanium for Deployments, monitor, and analyze data throughout various networks.
* Administer Controls & Permissions to files using PowerShell commands through SCCM.
* Performing periodic vulnerability testing and assisting in remediation efforts.
* Identified, documented and investigated suspicious events in intrusion detection systems (IDS) and SIEM tools.
* Monitoring and analyzing network traffic, Intrusion Detection Systems (IDS) and Instruction Prevention Systems (IPS), security events and logs.
* Performed penetration testing over the enterprise systems to audit the standards to comply with PCI DSS regulations.
* Project managed Project, Gantt charts, risk registries, Creation of templates. Guided and trained 8 analysts in Risk and compliance in NIST 800, PCI-DSS and other Frameworks. Work flow charts Change management. Risk management.
* Configuration of the RSA Archer platform with effective solutions and applications that support variety of business needs and to achieve organizational objectives
* Involved in firewall deployment and management in Azure such as Palo Alto, Azure Firewall
* Analyzed threats to corporate networks by utilizing SIEM products (QRadar, Splunk) to assess the impact on client environments.
* Assist with their global DLP program including multiple DLP solutions / Cloud Access Security Broker (CASB) security deployment.
* Worked in Security Incident and Event Monitoring SIEM platform - IBM QRadar, and Splunk.
* Provide proactive APT hunting, incident response support, and advanced analytic capabilities.
* Run vulnerability scans and reviews vulnerability assessment reports.
* Coordinates and assists with team on assigned daily SOC operations.
* Analyze and escalate events and incidents to SOC Analyst Level for response and resolution.

**Information Security Engineer**

**Department of Labor, Washington D.C Sep 2012 - Sep 2015**

* Managed DLP solution which included configuring and fine tuning DLP filters. Took action on alerts generated off of DLP.
* Conducting Web Application Vulnerability Assessment & Threat Modeling, Gap Analysis, secure code review on the applications.
* Development of IoT Solutions based on Industry Security Requirements.
* Review and updated System Security Plan (NIST SP 800-18), Risk Assessment (NIST SP 800-30), and Security Assessment Report (NIST SP 800-53A).
* Performing onsite & remote security consulting including penetration testing, application testing, web application security assessment, onsite internet security assessment, social engineering, wireless assessment, and IDS/IPS hardware deployment.
* Preparing and conducting IT Audits and IT General Controls Reviews, Internal IT Audits, Operational Audits
* Imported existing information from legacy systems into RSA Archer Applications and questionnaire. Integrated the RSA Archer with External data sources with WebAPI.
* Creates and implements new insider threat processes as appropriate
* Remains current on cyber security best practices, news, issues, vulnerabilities and threats
* Supports activities related to the implementation and use of tools for insider threat intelligence gathering, analysis, and reporting.
* Recognized areas of improvement for CSOC visibility, incident management and Threat Hunting use cases
* Performed Vulnerability Assessments using - Kali Linux / Metasploit / BurpSuite / Paros / SQLmap and many open source tools.
* Evaluation of threats and risk to business operations resulting in security solutions that appropriately balance cost and risk mitigation.
* Proficient in detecting application level vulnerabilities like XSS, SQL Injection, CSRF, authentication flaws etc both through automation and manual testing.
* Explanation of the security requirements to the design team in initial stages of SDLC to minimize the efforts to rework on issues identified during penetration tests.
* Identified issues on session management, Input validations, output encoding, Logging, Cookie attributes, Encryption, Privilege escalations
* Carrying out and preparing for compliance audits for SOX, PCI, HIPAA, ISO 27001, SOC \SAS70\SSAE16, Fed Regulations, etc.
* Developed this web application to store all system information in a central location. This was developed using Spring MVC, Struts, jQuery, JSP, Servlet, Oracle 10g, HTML and CSS
* Analyze the results of penetrations tests, design reviews, source code reviews and other security tests.
* Combining threat and vulnerability analysis, forensic analysis, mitigation assessment, threat intelligence & research, signature database building, knowledge sharing, IDS technologies, patch management technologies and more to develop a security profile & cyber defense strategy specific to the client’s environment that minimizes collateral damage and does not affect their line of business
* Provide tactical leadership during incident response for products within team portfolio, coordinating with executive committee, production support, cyber-security operations center (CSOC), and enterprise fraud management teams
* Participating during major incidents to support the primary Incident Manager with outage communications and logging incident timeline and other key information during an incident.
* Configures Smart Connectors on ArcSight Connector Appliance.
* Configuring and administering Arcsight loggers, ESM, and database systems.
* Processes vulnerability and threat data from a variety of internal and external sources to provide actionable intelligence to internal consumers.
* Worked on different types of vulnerability assessments reports both application generated and manual penetration testing and presented it.
* Create and implement Splunk Enterprise Security use cases for the Insider Threat team.
* Monitor network traffic off of QRadar SIEM and Sourcefire IDS tools for any suspicious activity.
* Experience in handling security events that affect VMware systems, applications, infrastructure, information and users using Splunk Enterprise Security.
* SIEM: Building software & application to enhance SOC operations and cohere Threat Intel interactions. Creating custom data visualization tools to interpret data correlated from event logs. Designing & implementing security content/use-cases on SIEMs, utilizing various event log sources. Delivering solutions, maintenance and support to currently deployed SIEM engines.
* Performed information security incident response and incident handling based on Working with multiple clients on Real time threat management using SIEM and solutions. Categorization and in accordance with established procedures
* Integration of different devices/applications/databases/ operating systems with SIEM.
* Monitors agencies sensors and SOC (Security Operation Center) systems for incidents and malicious activity.
* Analyze escalated email events including phishing and malware, and escalate as necessary
* Understanding and evaluating the cyber threat landscape, and assess what threats are most relevant to respective client
* Supplying actionable recommendations to other teams within the Cyber Security Center, to bolster cyber security efforts
* Managing indexes and cluster indexes, Splunk web framework, data model and pivot tables.
* Performed troubleshooting and/or configuration changes to resolve Splunk integration issues.
* Used burpsuite, dirbuster, IBM Appscan on daily basis for vulnerability assessments followed by manual penetration tests on applications.
* Writing Splunk Queries, Expertise in searching, monitoring, analyzing and visualizing Splunk logs.
* Experience in alert handling, standard availability and performance report generation.
* Configured and scheduled Qualys Scanner in QRadar to perform scan on regular intervals
* Vulnerability Management by scanning, mapping and identifying possible security holes using Qualys Guard and Nessus scanner.

**Security Engineer**

**CIT Group Inc, Livingston NJ Jan 2010 –July 2012**

* Assisted as a technical security analyst as part of a team responsible for assessing and ensuring NIST 800-53 Rev 4 management, operational, technical, and privacy security control implementation compliance for large apparel
* Manage the Security Incident and Event Management (SIEM) infrastructure.
* 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.
* Compliance standards and frameworks such as PCI, NIST 800-53, HIPAA, HITRUST and Privacy standards and frameworks such as Generally Accepted Privacy Principles (GAPP)
* Experience in conducting penetration testing for web applications and servers using Burp Suite and Metasploit Pro, and document the results to the senior management.
* Collaborate across the entire organization to bring Splunk access to product and technical teams to get the right solution delivered and drive future innovation gathered from customer input.
* Fine tuning existing correlation rules to reduce noise and false positives.
* Monitor the performance of Splunk via the Splunk Monitoring Console.
* Push configurations and updates to multiple Splunk Enterprise instances via the Splunk Deployment Server.
* Develop reports/alerting to meet SOC, clients and leadership requirements.
* Improved and expanded SOC L1 and L2 process documents.
* Risk analysis and security control gap analysis from information & network security perspective.
* Managing security incidents in the organization, key member of Incident Response Team