**Bhargav Kumar Muvva**

**Senior Cyber Security Engineer**

**+1 812-263-3024 bhargavkumar0812@gmail.com**

**Professional summary:-**

* Experienced Cybersecurity Professional with 8+ years of IT experience with a focus on designing, implementing, and managing comprehensive security programs across enterprise environments, including regulated industries such as healthcare.
* Skilled & technically proficient with multiple security domains including network security, endpoint protection, identity management, security operations, and governance, risk, and compliance.
* Hands-on experience in managing VMware vCenter, VMware ESXi (v7.0/v8.0), Site Recovery Manager, and Veeam Backup & Replication for enterprise backup and disaster recovery solutions across on-prem and cloud environments
* Extensive experience in **managing the full lifecycle of security incidents**, including **detection, analysis, containment, eradication, and recovery** in enterprise environments.
* **Primary incident handler** responsible for real-time monitoring, event triage, and forensic analysis, ensuring **timely response and resolution** of security threats.
* Expert in **incident escalation, triage, and remediation coordination**, collaborating with SOC, IT, and compliance teams to **minimize impact and ensure regulatory adherence**.
* Strong ability to **communicate complex security risks** to **non-technical stakeholders**, ensuring executive leadership understands risk impact and mitigation strategies.
* Committed to **mentoring cybersecurity professionals**, fostering an **inclusive security culture**, and leading security awareness training to **strengthen enterprise-wide security posture**.
* Perform ongoing security assessments, vulnerability management, threat detection, and incident response to protect critical business assets and sensitive data.
* Skilled in network protocol analysis using Wireshark and NetScout nGeniusOne to troubleshoot network communication issues and optimize application performance.
* Conduct threat modeling using frameworks such as STRIDE, DREAD, and PASTA to proactively identify and mitigate potential security risks in enterprise environments**.**
* Manage SOX and PCI compliance programs, security controls implementation, and remediation efforts across enterprise environments.
* Knowledge and experience in standard security and regulatory frameworks including ISO 27001/31000, NIST 800-53, HITRUST CSF, PCI DSS, HIPAA, and SOX.
* Served as Security SME for Centers for Medicare and Medicaid Services (CMS) major applications and enterprise security initiatives.
* Establish roadmaps for implementing security policies, standards, and controls to align with COBIT and industry best practices.
* Data leakage prevention using Symantec, McAfee, and endpoint encryption solutions with comprehensive key management strategies.
* Implementing and administering SIEM tools like IBM QRadar, Splunk, and Microsoft Sentinel for comprehensive security monitoring.
* Experience in Security Information and Event Management using IBM QRadar, Splunk, RSA Archer, and other leading security monitoring platforms.
* Knowledge on PKI Certificate Management, Vulnerability Management using Qualys, Tenable, and Rapid7 scanning solutions.
* Implementing and administering endpoint protection platforms including Sophos, McAfee, Microsoft Defender, and CrowdStrike for comprehensive threat prevention.
* Performing internal security audits based on ISO 27001, SOX compliance, HIPAA requirements, and CCPA regulations
* Knowledge on managing IDS/IPS Systems, Network Access Control (NAC), and Identity and Access Management solutions across enterprise environments.
* Experience in Change, Release, and Incident Management as per ITIL framework with focus on security operations and risk management.
* Expert in enterprise networking security, specializing in secure architecture design, segmentation, and defense-in-depth strategies.
* Experience with HPE Synergy, C7000 Compute Modules, HPE 3PAR, and Alletra Storage arrays, including SAN switches for enterprise storage solutions, backup management, and high availability infrastructure
* Extensive experience in managing and securing networks using next-generation firewalls including Palo Alto, Cisco ASA, and Check Point with advanced threat prevention capabilities.
* Experience managing Citrix NetScaler, Azure Load Balancers, and OCI Load Balancers for high-performance application delivery and security, including traffic optimization and firewall rule configurations
* Implemented comprehensive Intrusion Prevention Systems for both perimeter protection and internal network monitoring.
* Creating and troubleshooting secure remote access solutions including VPN platforms, zero trust network access, and privileged access workstations.
* Experience of executing security projects and implementing tasks under ITIL standards with comprehensive documentation and change management.
* Expertise in gathering and analyzing security metrics, key risk indicators, and maintaining scorecards to ensure information security program effectiveness and efficiency.
* Been a focal contact for departments during client Policies and Standards based Audit for ISO/IEC27001:2013 Standard.
* Experienced in design, installation, configuration, administration, and troubleshooting of secure network infrastructure using enterprise-grade security controls.
* Monitored and researched Cyber Threats with a direct & indirect impact to the organization through threat intelligence platforms and security research.
* Worked with threat intelligence platforms including FireEye, Recorded Future, and MISP for enhanced threat detection and proactive defense.
* Advanced knowledge in secure network design principles, implementation of defense-in-depth strategies, and security architecture reviews.
* Advanced knowledge in network protocols, common attack vectors, and security control implementation across enterprise technology stacks.
* Conducted Security Awareness training programs for employees across different roles, enhancing organizational security posture through education.
* Experienced in conducting Disaster Recovery drills, implementing business continuity plans, and ensuring resilience of critical security systems.
* Commendable experience in auditing, implementing & managing security controls to satisfy HIPAA, SOX, GLBA, FFIEC, ISO, NIST, PCI DSS, FISMA, and SAS 70 & 11 requirements.
* Hands-on experience in implementing Zero Trust security models using modern security solutions and Multi-Factor Authentication (MFA) across enterprise environments.
* Assisted in the migration from traditional perimeter-based security to zero trust architecture, implementing secure application access without exposing services to the internet.
* Supported multi-tenant security architectures for global enterprise clients with over 20,000 users, ensuring secure and scalable security controls across diverse environments.
* Specialized security experience includes solutions for clients in the financial, retail, healthcare, and technology services domains.
* Collaborate with cross-functional security teams to integrate access controls with SIEM and other security monitoring tools for comprehensive threat detection.
* Managed encryption solutions for data protection, secure communications, and regulatory compliance across enterprise environments.
* Extensive experience in balancing Information Security requirements with business objectives, implementing appropriate controls based on risk analysis.
* Hands-on skills include end-to-end security management (from policy development to implementation and monitoring) and security integration throughout the system development lifecycle.
* Experienced in leading **security incident response efforts**, serving as the **primary incident owner** for threat detection, containment, escalation, and resolution across enterprise environments.
* Strong background in **security policy enforcement and compliance**, ensuring alignment with **ISO 27001, NIST 800-53, PCI DSS, HIPAA, and SOX** frameworks.
* Expertise in **security intelligence reporting**, working closely with cross-functional teams and executive leadership to **translate cybersecurity risks into actionable insights** for informed decision-making.
* Skilled in **incident tracking, forensic investigation, and post-incident remediation** to strengthen organizational security posture and prevent reoccurrence of threats.

**TECHNICAL SKILLS:-**

* Vulnerability Management: Qualys Vulnerability Management, Tenable Nessus, Rapid7 InsightVM, OpenVAS, Web Application Scanning, Policy Compliance, Asset Management
* Security Monitoring & SIEM: IBM QRadar, Splunk Enterprise Security, Microsoft Sentinel, LogRhythm, ArcSight, ELK Stack, Sumo Logic, Google Chronicle
* Security Tools: Metasploit, NMAP, Wireshark, Kali Linux, Burp Suite, OWASP ZAP, SolarWinds, Nessus, InsightIDR, PowerShell, Python Security
* Security Frameworks: NIST Cybersecurity Framework, NIST 800-53, NIST 800-171, ISO 27001/31000, HIPAA, HITRUST CSF, PCI DSS, SOX, FISMA, COBIT
* Threat Intelligence: FireEye, Recorded Future, ThreatConnect, MISP, VirusTotal, AlienVault OTX, IBM X-Force, ThreatGrid, MITRE ATT&CK,IOC/IOA Analysis
* Network Security: Cisco, Palo Alto, Check Point, Fortinet, Juniper, F5, Cisco ISE, Aruba ClearPass, VLANs, Segmentation, IDS/IPS, WAF, NetScout nGeniusOne, Wireshark (for network protocol analysis), Citrix NetScaler, Azure Load Balancers, OCI Load Balancers, Application Firewalls
* Endpoint Security: Microsoft Defender ATP, CrowdStrike Falcon, Carbon Black, Symantec, McAfee, SentinelOne, Cylance, Trend Micro, Sophos
* Identity & Access Management: Active Directory, Azure AD/Entra ID, Okta, Ping Identity, ForgeRock, Role-Based Access Control, Privileged Access Management
* Multi-Factor Authentication: Duo Security, RSA SecurID, Microsoft Authenticator, YubiKey, FIDO2, Passwordless Authentication
* Data Protection: DLP, Encryption, Digital Rights Management, Email Security, Data Classification, Database Security, S/MIME, PGP
* Cloud Security: AWS Security, Azure Security, GCP Security, Cloud Security Posture Management, CASB, CSPM, CWPP, Cloud Native Security
* Compliance & GRC: RSA Archer, MetricStream, ServiceNow GRC, Compliance Management, Risk Assessment, Control Testing, Audit Management
* Application Security: SAST, DAST, IAST, SCA, Secure SDLC, DevSecOps, API Security, Code Signing, Mobile App Security, Secure Coding Practices
* Security Architecture: Zero Trust, Defense-in-Depth, Secure Design Principles, Security Reference Architecture, Threat Modeling, Risk Assessment
* Incident Response: Digital Forensics, Malware Analysis, Threat Hunting, Incident Handling, SOAR, Playbooks, Chain of Custody, Evidence Collection, Triage, Escalation, Root cause identification, Post-incident remediation
* Infrastructure Security: Server Hardening, OS Security, Container Security, Virtualization Security, IoT Security, OT/ICS Security, Wireless Security, HPE Synergy, HPE C7000 Compute Modules, HPE 3PAR & Alletra Storage Arrays, HPE SAN Switches, HP5100 / 5260 Backup Storage Arrays
* Cryptography: PKI, TLS/SSL, Certificate Management, Key Management, Hash Functions, Digital Signatures, Encryption Algorithms, HSM
* Security Awareness: Phishing Simulations, Security Training, Social Engineering, Security Culture, Compliance Training, Metrics and Reporting
* Governance & Documentation: Security Policies, Standards, Procedures, Guidelines, Security Controls Documentation, Compliance Documentation
* Privacy & Data Governance: GDPR, CCPA, CPRA, Data Mapping, Privacy Impact Assessments, Privacy by Design, Data Subject Rights Management
* **Virtualization & Backup Solutions:** VMware vCenter, VMware ESXi (v7.0/v8.0), Site Recovery Manager, Veeam Backup & Replication, Immutable Backup, Scale-Out Repository, Azure Storage Accounts

**Education:-**

* Bachelor’s in Electronics and Communications Engg. (Veltech University -Chennai, India) 2015
* Master’s in Computer Science (Michigan State University -Michigan, US) 2018

**PROFESSIONAL EXPERIENCE:-**

**Client: Penske Truck leasing Reading, PA Jan 2023 -present**

**Role: Sr Cyber Security Network Engineer**

Roles & Responsibilities: -

* Perform real-time security log and event analysis and take action to contain and mitigate information security threats. the events will originate from SIEM, DLP, IDS/IPS, and antivirus, firewalls, and system security logs.
* Assisted in implementing network devices, including routers, switches, and firewalls across infrastructure environments.
* Collaborated with network and infrastructure teams to support design and implementation of network security controls.
* Developed infrastructure documentation, including network topology diagrams and inventory reports.
* Managed VMware vCenter and ESXi (v7.0/v8.0) configurations, Site Recovery Manager, and Veeam Backup & Replication, ensuring secure and optimized virtualization, backup, and disaster recovery solutions across on-prem data centers.
* Evaluate enterprise risks, document processes and systems in flowchart and narrative form, and design audit programs.
* Planning and implementing overall risk management process.
* Conducted security assessments and penetration testing on access control mechanisms to identify potential risks.
* Assisted in security incident management, focusing on access control-related events and working with cross-functional teams to implement remediation.
* Provide strategic recommendations for the integration of PKI and KMS to manage and secure encryption keys for various applications and communications.
* Oversee encryption audits and assessments, identifying vulnerabilities and ensuring encryption strength meets evolving security threats.
* Developed and implemented security best practices across all stages of the product development lifecycle, ensuring compliance with secure coding principles, DevSecOps methodologies, and industry security standards such as ISO 27001 and NIST 800-53
* Led security design reviews, penetration testing, and secure architecture assessments for software and hardware products to proactively identify vulnerabilities and enforce security-by-design principles.
* Collaborated with systems engineering, software development, and regulatory teams to document and implement cybersecurity controls in alignment with industry best practices and regulatory requirements.
* Supervised a team of helpdesk technicians, providing guidance and technical support for resolving IT issues across the organization.
* Worked with internal security teams to enhance SIEM capabilities and improve the accuracy of incident detection.
* Maintained detailed documentation of SIEM processes and security event investigations for future reference and compliance audits.
* Managed enterprise-wide vulnerability remediation, collaborating with engineering, IT, and compliance teams to ensure consistent security baselines and risk mitigation strategies across different sites
* Created and optimized saved searches and reports to monitor system health, performance metrics, and security events.
* Implemented and managed Veeam Backup & Replication for critical server backups, leveraging Immutable Backup and Scale-Out Repository strategies to enhance enterprise storage resilience and cloud backup integration with Azure Storage Accounts.
* Configured and maintained network switches, routers, firewalls, and VPN connections to secure and optimize the organization’s network.
* Performed advanced network traffic analysis using Wireshark and NetScout nGeniusOne to diagnose latency, protocol anomalies, and optimize network performance for critical applications at SCC.
* Implemented IPS for hosted websites and incoming traffic filtering using Palo Alto firewalls.
* Monitored system performance and network traffic using monitoring tools like Nagios, SolarWinds, and PRTG, addressing potential issues before they impacted operations.
* Provided timely updates to security teams on zero-day vulnerabilities, outlining the risk and mitigation steps.
* Monitored threat intelligence feeds and security bulletins to stay ahead of new vulnerabilities and security advisories.
* Regularly updated threat hunting playbooks to reflect new attack tactics, techniques, and procedures (TTPs).
* Assisted in the development and tuning of threat detection rules and alerts to minimize false positives and enhance detection accuracy.
* Trained and mentored junior analysts on digital forensics methodologies, ensuring adherence to best practices and forensic tools.
* Prepare detailed forensic reports for use in legal contexts, maintaining chain of custody throughout investigations.
* Provided support for MFA systems such as Duo, RSA SecurID, and Microsoft Authenticator, resolving issues related to authentication failures.
* Assisted in the development of a zero trust security model, enforcing least privilege access with MFA as a critical security layer.
* Manage and optimize Carbon Black Protection and ThreatLocker for enterprise-wide endpoint security, ensuring robust protection against malware, ransomware, and insider threats.
* Deployed and configured Carbon Black Protection to secure endpoints across multiple environments, creating security policies to block unauthorized software and prevent fileless malware attack.
* Implement Google Chronicle to enhance security analytics and threat detection, utilizing its scalable data storage and advanced analytics capabilities for long-term data retention and insights.
* Led **tier-2 security incident response**, investigating threats using **Microsoft Sentinel and Google Chronicle**, coordinating rapid containment, escalation, and forensic analysis.
* Owned **end-to-end security incidents**, leading **incident detection, forensic investigation, containment, and executive-level reporting** to ensure rapid response and risk mitigation
* Developed **SOC incident management workflows,** ensuring seamless coordination between **security teams, IT operations, and compliance teams** to mitigate risks
* Enhanced **incident tracking and response efficiency** by optimizing **SIEM correlation rules and detection mechanisms**, reducing false positives and improving response times by **30%.**
* Provided **security briefings to key stakeholders**, ensuring transparent communication of emerging threats, risk impact assessments, and mitigation strategies
* Led **post-incident forensic analysis**, ensuring proper documentation, **chain of custody**, and compliance with **industry regulations.**
* Performed vendor due diligence, assessing the security posture and reputation of software providers before making purchasing decisions.
* Managed enterprise DNS and DHCP services using Infoblox, improving scalability and security of network configurations.
* Supported incident response activities by providing expertise on CIS hardening practices and their impact on security incidents.
* Create technical and managerial level reports and risk assessments for Cloud based applications and infrastructure.
* Identify processes/procedures for how to handle a cloud security event, including forensic isolation and mitigation with Digital Forensics and Incident Response (DFIR/IR) teams.
* Develop ISO-based controls that address regulatory requirements associated with PCI, HIPAA and SOX.
* Deliver security awareness training to employees focused on PCI DSS compliance and safe handling of payment card data.
* Create/ enhance tools for Risk Management. Also create tools to help partners to better manage project and funds.
* Direct and perform reviews of internal control procedures and security for systems under development and/or enhancements to current systems Preparing, Implementing and Testing of Project specific Business Continuity Plan (BCP).
* Conducting Full Interruption Test to ensure the BCP preparedness.
* Participated in all kind of BCP Activities (Business Continuity Plan).
* Investigate the security logs, mitigation strategies and responsible for preparing Generic Security incident report.
* Reported the status of projects the ISSM/ISSO office was working, to local management.
* Review and updated System Security Plan (NIST SP 800-18), Risk Assessment (NIST SP 800-30), and Security Assessment Report (NIST SP 800-53А).
* Evaluates POA&M activities to ensure identified.
* Designed and deployed Zero Trust security solutions using Zscaler ZIA/ZPA for over 25,000+ users, ensuring secure remote access.
* Configured and managed MFA solutions (Duo, RSA, Microsoft Authenticator) to enhance security posture.
* Led enterprise security operations for infrastructure spanning 1,000+ servers and 200+ locations, managing comprehensive security stack including Zscaler Private Access (ZPA) infrastructure supporting 25,000+ users across multiple tenants, achieving 99.9% uptime and reducing security incidents by 40%.
* Established and executed comprehensive security frameworks for multi-tenant environment serving 20,000+ users, ensuring compliance with NIST, PCI, CIS, and IRS standards while maintaining zero security breaches Developed and implemented automated security monitoring protocols.
* Monitored, analyzed, and resolved security issues related to Zscaler services, ensuring optimal performance and security posture.
* Provided training to IT staff and end-users on ZIA/ZPA configurations, best practices, and troubleshooting techniques.
* Worked with cross-functional teams to implement Zscaler and troubleshoot network-related issues, providing comprehensive technical support and maintenance.
* Managed daily operations of Zscaler ZIA, including configuration of URL filtering, bandwidth control, and security policies for remote workers and on-site employees.
* Managed web proxy solutions, including Zscaler, to enforce internet security policies, control traffic, and prevent unauthorized access to web resources.
* Conduct FISMA complaint security control assessments to ascertain the adequacy of management, operational, technical and privacy controls.
* Other responsibilities: Site ISSM/ISSO. Ensured site systems were compliant with required local and national security standards.
* Compliance standards and frameworks such as PCI, NIST 800-53, HIPAA, HITRUST and Privacy standards and frameworks such as Generally Accepted Privacy Principles (GAPP).
* Reviewing and documenting Risk Assessment mitigation strategies Perform system and information control reviews to include system development standards, operating procedures, system security, programming controls, communication controls, backup and disaster recovery, and system maintenance.
* Identify gaps and area of opportunities in the process followed and suggest ways to fix them.
* Configure network scans, schedule network scans to run with bandwidth usage and ensure accurate vulnerability assessment analysis results are generated and disseminated to system owner/ISSM/ISSO.
* Security SME for new interface between CMS and private insurance community.
* Worked with independent auditing firms (EY, Deloitte) on SOX audits.
* Perform direct assist for the external auditor for SOX testing.
* Replaced the external auditor hired to perform SOX ITGC testing for SEC.
* Responsible for real time proactive monitoring of complex systems and response to known and emerging threats against the EY network via intrusion detection software Familiar with Splunk, Fidelis XPS, IP Address Management (IPAM), Microsoft Active Directory Application Mode (ADAM), Firewalls, SEP, and Stealth-watch knowledge base.
* Conduct security assessments on networks and Industrial Control System (ICS), design cyber security solutions, support implementation of those solutions, and identify security trends and practices.
* Creates and maintains authentication records for all flavours of UNIX (Linux, AIX, and Solaris) and Windows, as well as for databases using Basic and Cyber-Ark Vault authentication records. Scope includes entire Novartis global data centers and work sites using QualysGuard.
* Experience with security tools from various vendors to include: Cisco, CheckPoint, IronPort, McAfee, Symantec, Sourcefire, Sophos, ArcSight, Tenable, Juniper, Imperva, BlueCoat, Encase, Fire Eye, Bitlocker.
* Conduct operational, compliance, financial and investigative audits.
* Monitored Security Management Console for Security Operation Centre (SOC) for ensuring confidentiality, Integrity and Availability of Information systems Provided leadership in architecting and implementing security solutions towards Qualys and SIEM tools like Splunk, Solutionary and LogRhythm.
* 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).
* Led **end-to-end security incident resolution**, ensuring proper escalation, tracking, and mitigation of security threats in alignment with NIST 800-53.
* Worked closely with **SOC analysts, IT teams, and compliance to escalate high-severity incidents**, ensuring timely resolution and minimal business impact.
* Performed **real-time log correlation and analysis** using **Splunk, IBM QRadar, and Microsoft Sentinel**, identifying malicious activity and mitigating risks proactively
* Developed **incident reporting dashboards**, providing key stakeholders with detailed insights into cyber threats and risk posture.
* Responsibilities for CSIRT included SIEM, Context Filtering, Web Security, Incident Tracking, IPS/IDS and Malware Analysis.
* Developing customized Shell scripts in order to install, manage, configure multiple instances of Splunk forwarders, indexers, search heads, deployment servers.
* Used SPLUNK forwarders to provide reliable and secure collection and delivery of data to the Splunk platform for indexing, storage and analysis.
* Managed enterprise-wide Splunk deployment including index configuration, capacity planning, and performance optimization across multiple departments.
* Implemented and maintained Splunk Universal Forwarders across distributed environments, ensuring efficient data collection and transmission.
* Configured and optimized Citrix NetScaler, Azure Load Balancers, and OCI Load Balancers, managing firewall rule sets, secure application routing, and load balancing policies to enhance enterprise network security and availability.
* Conducted thorough research and testing of Splunk add-ons to enhance data parsing and visualization capabilities.
* Integrated Splunk with SIEM and security tools to create comprehensive security monitoring and alerting framework.
* Implemented role-based access control (RBAC) in Splunk environment to ensure secure data access and compliance.
* Provide regular support guidance to Splunk project teams on complex solution and issue resolution.
* Assisted administrators to ensure whether SPLUNK is actively and accurately running and monitoring on the current infrastructure implementation Responsible to check the SPLUNK logs for web server so as to avoid server time down during production.
* Managing TCP hosts through SPLUNK deployment server. Pushing configurations and grouping servers to push similar configurations at the same time.
* Worked on setting up Splunk to capture and analyze data from various layers Load Balancers, Web servers and application servers.
* Device Vulnerability and Threat management with Cyber Security Team.
* DLP- Data Loss Prevention monitoring and investigations using Risk Fabric & Symante Enforcer.
* Stealth Watch for Net Flow and Network Security Monitoring.
* Training new Employees in Security Incident Management Procedures.
* Monitor security functionality (IDS/IPS and Endpoint) and report daily operational metrics; provide scheduled management reports on risk status of network infrastructure, applications, internet activity, email filtering, vulnerability management and security metrics.
* Designed core scripts to automate Splunk Maintenance and alerting tasks.
* Expert in Analyzing the Security Related Logs from various sources using SIEM system which creates alerts whenever it detects Anamolous Transactions and also blocks malicious activities.
* Designed core scripts to automate Splunk Maintenance and alerting tasks.
* Provided necessary designs and implemented security solutions for egress/ingress points using the IPS/IDS sensors across the networks to provide better incident handling and event monitoring.
* Managed a Vulnerability Remediation Team (VRT) for reporting all the scan reports and guided them to fix the vulnerabilities and patches using the QID’s, Bugtraq ID’s and CVE ID’s from knowledge base from vendors.
* Managed to secure the devices across entire network by using the ThreatProtect Module from Qualys. Measured the level of Severity of devices to fix the issues arising from them by providing solution.

**Client: Collins Aerospace Aguadilla, PR Jul 2019 – Dec 2022**

**Role: Cyber Security/ Information Security and Compliance Analyst**

As a member of Infrastructure security team, responsible for configuration, implementation & maintenance of various cyber security technologies like Forcepoint web proxy, O365 Security, McAfee IPS, ArcSight SIEM.

Roles & Responsibilities:-

* Developed Cyber Security Standards on NIST Frameworks and insured their proper implementation to reduce the risk of vulnerability to IT assets.
* Provided support for network performance and troubleshooting, ensuring high availability of critical infrastructure services.
* Assisted in the implementation and deployment of network security devices (Cisco, Palo Alto, and Check Point firewalls).
* Worked with cross-functional teams to understand infrastructure requirements and provide network security solutions.
* Developed various functions including identifying, protecting, detecting, responding and recovering for performing concurrent and continuous operation of dynamic security risk.
* Worked closely with systems engineering, software development, and regulatory compliance teams to develop and implement cybersecurity controls in embedded systems, ensuring secure software and hardware development in accordance with regulatory security standards.
* Provided suggestions and inputs for Global Security Council and Privacy as a part of project consulting towards Information Security and Cyber Intelligence.
* Designed and implemented methods to discover risk in in-house products and services and track them to resolve by providing solutions.
* Planning audit activities, including coordination, scheduling, reporting results, and follow up.
* Supported cybersecurity compliance initiatives for regulated industries, ensuring alignment with HIPAA security controls.
* Worked with cross-functional teams to integrate cybersecurity requirements into enterprise security solutions, ensuring adherence to ISO 27001, NIST 800-53, and HITRUST CSF
* Administered HPE Synergy Compute Modules, HPE 3PAR, and Alletra Storage arrays, including SAN switch configurations for enterprise storage optimization, high availability, and backup data replication strategies
* Manage access control configurations for various systems, ensuring that roles, permissions, and entitlements adhere to the principle of least privilege (PoLP).
* Develop and enforce encryption policies that align with organizational security objectives and compliance requirements.
* Implemented robust encryption solutions to secure financial data and critical business communications.
* Monitor and analyze security logs and reports to detect and address suspicious activity in real-time.
* Monitored security events using SIEM tools, correlating log data from firewalls, IDS/IPS, antivirus, and endpoint security solutions.
* Spearheaded **incident response operations**, leading **incident triage, threat containment, and crisis management** for security incidents impacting enterprise infrastructure
* Designed and implemented **SOC playbooks**, standardizing **incident response procedures, escalation handling, and post-incident remediation**
* Handled **high-severity security incidents**, working with **SOC, compliance, and forensic teams** to conduct **deep-dive investigations, malware analysis, and regulatory remediation**
* Created **SOC playbooks and automated threat hunting workflows**, reducing **false positives by 30%** and improving **SOC efficiency in detecting and escalating advanced threats**
* Conducted **post-incident forensics**, analyzing malware artifacts and compromised endpoints to determine **root cause and corrective actions.**
* Led **security awareness programs** for employees, educating teams on **incident handling, phishing awareness, and regulatory compliance** (PCI DSS, HIPAA)
* Collaborated with **legal and compliance teams** to ensure incident response protocols adhered to **SOX, HIPAA, and PCI DSS** regulatory requirements
* Conducted **forensic investigations** on security breaches, ensuring **detailed incident reports** were developed for **root cause analysis and security control improvements**
* Led **security awareness programs** focused on **incident response best practices, escalation workflows, and compliance enforcement**, reducing **security breaches by 40%.**
* Designed and deployed Arista-based Spine-Leaf architecture, utilizing BGP-EVPN and VXLAN to optimize data center networking.
* Implemented enterprise-wide PKI infrastructure for securing internal communications and digital certificates.
* Configured and optimized Palo Alto firewall policies to enforce strict security controls and prevent intrusion attempts.
* Configured network services such as DNS, DHCP, and file/print sharing, maintaining consistent uptime and efficient operation.
* Oversee the deployment and management of Active Directory, DNS, DHCP, and network file shares, providing secure and efficient user access to resources.
* Leveraged threat intelligence and indicators of attack (IoAs) to uncover malicious behavior and reduce dwell time of attackers.
* Led daily threat hunting operations, analyzing network and endpoint data for suspicious activity and potential threats.
* Recover deleted or encrypted data using advanced forensic tools, ensuring integrity and accuracy of evidence for legal proceedings.
* Worked closely with legal teams to provide expert testimony and detailed forensic reports for litigation and regulatory purposes.
* Performed risk assessments and gap analyses, evaluating existing authentication methods and identifying areas for MFA implementation.
* Integrated MFA with identity providers and single sign-on (SSO) systems, providing seamless and secure authentication for users.
* Monitor threat activity using behavioral analytics, leveraging Carbon Black’s advanced threat detection capabilities to proactively detect and respond to suspicious activities.
* Worked closely with IT operations to ensure seamless deployment of Carbon Black and ThreatLocker agents across Windows and Linux endpoints.
* Implemented Microsoft Defender’s suite of security tools across the organization, providing protection against malware, ransomware, and other advanced threats.
* Conduct security assessments using Microsoft Defender’s built-in threat intelligence and Google Chronicle’s analytics to identify potential vulnerabilities and threats.
* Implemented and managed CIS hardening benchmarks for a range of operating systems, applications, and network devices, improving security posture and reducing attack surfaces.
* Supported the implementation of financial controls and processes to ensure accurate budgeting and reporting.
* Provided technical support and training to IT staff on the use of ZIA and other web proxy tools, ensuring effective utilization and compliance with security standards.
* Develop, implement, and review security policies and procedures to enhance organizational adherence to PCI DSS and data security best practices.
* Worked with clients to implement multi-factor authentication (MFA), encryption, and other critical PCI DSS requirements.
* Monitored RSA Archer as a Security Management Console to see Data Loss Prevention Events, ePO Detections, SourceFire Events Classifications, Bluecoat Malware Detections and Analysis of WhiteHat Web Application security scanning.
* Implement necessary security controls and enhancements on the ICS.
* RSA Archer used as an audit management tool for inputting various information and dashboards to showcase to improve the risk and control functions against Risk, IT Governance and Compliance.
* Opened, Assigned and closed the tickets assigned in SOC Security Management Console towards Qualys for various Remediation Process and Patch Management Process.
* Support security compliance initiatives and assessments including responses to client security organization audits, questionnaires.
* Created & Managed Lifecycle Plan for proper usage of the scanners all over the network and planned future deployments Experienced working on Solarwinds SIEM to instantly improve security and compliance.
* Vulnerability Management: Configured Qualys Guard Tool for Vulnerability Analysis of Devices and Applications. Monitored them constantly through the dashboard by running the reports all the time.
* Created Asset Groups, scheduled Scans/Reports for smooth remediation process and assigned the correct sensors to those scanners placed in the network.
* Managed all the scans including discovery maps, authentication scans to ensure proper scheduling, reporting and smooth functioning of IP’s.
* Managed Qualys Cloud Agents. Assisted in installing them over the devices, servers or also for remote users.
* Scanned the entire devices using the cloud agents whenever needed for employees working from home and provided the solutions to fix the vulnerability.
* Configured and optimized Private and Public Service Edges within Zscaler to enhance application connectivity and ensure seamless, secure access for large enterprise environments with 20,000+ ZPA users.
* Implemented advanced troubleshooting and problem resolution for high-availability network setups, managing multiple firewalls, switches, routers, and load balancers across 1,000+ servers and over 200 locations to maintain optimal security.
* Implemented Zscaler dashboards and analytics to monitor traffic, security events, and performance metrics, ensuring continuous optimization of Zscaler services.
* Regularly provided reports on Zscaler performance, detailing security threats blocked, bandwidth usage, and compliance to executives and stakeholders.
* Worked on Qualys Web Application Scanning for monitoring the Web Applications, filtering and crawl scoping to detect the vulnerabilities in the web applications and fix them.
* Log analysis from various devices such as proxies, firewalls, IPS/IDS, Desktops, laptops, servers, SIEM tool logs, routers, switches, AD servers, DHCP servers, Access Control Systems, etc.
* Perform user administration, Active Directory user management functions like Identity Management, Access Management, Directory Management, Single Sign-On, Federation, and Role Based Access systems.
* Work on technical examination, analysis and reporting of computer-based evidence.
* Utilize forensic tools and investigative methods to find electronic data, including Internet use history, word processing documents, images, and other files.
* Created and maintained Splunk correlation rules for detecting security anomalies in aerospace manufacturing systems.
* Implemented automated Splunk data ingestion for critical aerospace control systems and security appliances.
* Developed custom Splunk apps and dashboards for real-time monitoring of aerospace systems and security metrics.

**Client: Volkswagen Credit, NY Nov 2018 - Jun 2019**

**Role: Network & Security engineer**

High-risk system access reviews for CCPA scoped applications, data centers, and domain user accounts using Termination, provisioning review methods, encryption, Vulnerability management and Penetration testing Access reviewer tool to review High privileged accounts & highly sensitive application that contains PCI & PII Data.

Roles & Responsibilities:-

* Experience on conducting full interruption test to test the BCP preparedness.
* ⁠Extended my support to Transition Risk Management team in reviewing RAD.
* Developed and documented network configurations and policies in collaboration with security and IT teams.
* Assisted in the implementation and optimization of network services, including VPNs, routing, and switching.
* Coordinate the VA testing in advance with the system ISSO and the Government SOC TM to assure coordination with network maintenance, availability, and operations. Coordinate with system owner/ISSM/ISSO any necessary changes to the schedule Investigate the security logs, mitigation strategies and Responsible for preparing Generic Security incident report.
* Conducted **incident triage and analysis,** escalating security breaches and containing active threats through **firewall, SIEM, and EDR** integrations.
* Created **incident escalation workflows**, ensuring that high-priority threats were promptly communicated to **senior leadership and IT response teams.**
* Ensured **incident response alignment** with regulatory requirements, including **SOX, PCI DSS, and NIST standards,** mitigating compliance risks.
* Assisted in PCI DSS assessments by preparing documentation, supporting audits, and working with security vendors to address vulnerabilities.
* Utilize Qualysguard as primary tool to monitor tickets and vulnerabilities.
* Utilize Qualysguard as primary tool to monitor and report Policy Compliance, based on NIST, ISO2007 and CIS Benchmarks.
* Conduct Business Impact Analysis (BIA) to analyze mission-critical business functions, and identify and quantify the impact those functions if these are interrupted.
* Provided leadership in architecting and implementing security solutions towards Qualys and SIEM tools like Splunk, Solutionary, LogRhythm, SCCM, Altiris, LanDesk, BigFix, McAfee/Symantec, Cabon Black, NXlo.
* Deploy and support information security systems and solutions such as key management, IPS/IDS, SIEM, MDM, NAC, APT detection, and endpoint management for remote user.
* Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention.
* Perform and document audit activities in accordance with professional standards such as COBIT, COSO and SOX internal control frameworks Audit Project.
* Conducted PCI DSS compliance assessments, ensuring all systems handling PII and payment data met regulatory requirements.
* Designed and optimized **incident tracking dashboards and response workflows, reducing MTTR (Mean Time to Resolution) by 25%** and ensuring seamless security operations.
* Acted as the **primary point of contact for high-severity security incidents**, coordinating **remediation efforts between IT, security, and compliance teams**
* Acted as the **primary point of contact for high-severity security incidents**, coordinating **remediation efforts between IT, security, and compliance teams**
* Designed and implemented **incident tracking dashboards**, improving **incident visibility and resolution efficiency across the organization**
* Implemented and optimized Zscaler ZIA/ZPA solutions for securing cloud-based web applications and remote access.
* Coordinate special projects such as Segregation of Duties (SOD) and SOX Compliance audit.
* Provide a security review of system documentation, audit logs, rule set and configuration to validate policy compliance, Report IT security incidents in accordance with established procedures.
* Plan, develop, implement, and maintain an Incident Response and Audit Program for events of interest and address Plan of Action and Milestones (POA&Ms) in continuous monitoring with various point of contact.
* Audit risk-based Quarterly Account Provisioning, and Role Change/Job Transfer Reconciliations.
* Prepare project scorecards and provide status updates in granular level to SSE IT Controllership team on a weekly basis and key stakeholders on a bi-weekly basis.
* Prioritize remediation of gaps based on internal and external audits.
* Prepare security and compliance reports by collecting, analyzing, and summarizing data.
* Assist in providing support of the enterprise vulnerability management program.
* Collect and present detailed status at a granular level (trackers, reports, documentation).
* Consolidate the IT inventory of systems in scope (App/DB/OS).
* Identify reviewers and map in the inventory.
* Create assets in Access Reviewer Tool if required for performing the review.
* Monitor and track the responses for the review of timeline.
* Extract ‘after list’ and validate the change implementation.
* Review and validate the review document for completeness and accuracy.
* Experience with EndPoint management software, such as Tanium, Sophos, Altiris, Avast, Symantec, Gravityzone, Avira, Kaspersky, Webroot, F-Secure.
* Configured Splunk Universal Forwarders across 1000+ endpoints for comprehensive log collection and analysis.
* Developed custom Splunk dashboards for monitoring financial transaction security and fraud detection.

**Plus91 Technologies Pvt Ltd Pune India. July 2015 to Aug 2017**

**Role: Security Engineer**

Configuring Qualys scans and creating accounts for the business security team to verify the vulnerabilities and remediation procedures. Providing the base line option profiles for businesses to scan their devices and monitor traffic logs using Accelops SIEM tool.

Roles & Responsibilities:-

* Monitored and triaged security events using AccelOps SIEM, correlating logs from IPS, firewalls, and endpoint security solutions.
* Worked closely with network teams to document and analyze network vulnerabilities and performance.
* Handled **security alerts and event triage** using **SIEM tools (AccelOps, Splunk, ArcSight)** to identify potential cyber threats.
* Conducted **IOC analysis, malware forensics, and security log reviews** to detect and respond to APTs and insider threats.
* Conduct Security Risk Assessment on all new applications, IT Systems or changes to existing IT systems to verify if they satisfy established security baseline before adoption into Corporate.
* Assist management in authorizing the IT Systems for operation on the basis of whether the residual risk is at an acceptable level or whether additional compensating controls should be implemented. plans, training and testing were executed appropriately and discuss lessons learnt.
* Monitor and respond to Qualys incidents which couldn’t be resolved by L2’s.
* Creation of baseline policies with all the QID’s for business to use.
* Helped to research open-source intelligence feeds for current and emerging threat information.
* Ability to conduct manual Penetration Tests on sensitive systems.
* Handling the compatibility issues that arises due to Qualys scans.
* Preparing the Standard operating procedures and basic documentation for known issues.
* Coordination with the Qualys vendor for new(unknown) issues.
* Created and supported security awareness programs to inform and educate employees.
* Testing source code and running code.
* Participate in meetings to discuss system boundaries for new or updated systems to help determine information types for categorization purposes. Determine the classification of information systems to aid in selecting appropriate controls for protecting the system.

**PROJECTS**

**Enterprise Security Program Implementation** - Designed and implemented comprehensive security program for global enterprise - Developed security policies, standards, and procedures aligned with ISO 27001 framework - Implemented security controls across network, endpoint, application, and data domains - Created security metrics dashboard for executive reporting and program effectiveness measurement

**Security Operations Center Transformation** - Led initiative to enhance security monitoring and incident response capabilities - Implemented SIEM solution with custom use cases aligned with MITRE ATT&CK framework - Developed automated playbooks for common security incidents to improve response time - Created tiered SOC model with defined escalation paths and specialized security roles

**Identity Governance and Privileged Access Management** - Implemented enterprise-wide identity governance solution - Developed role-based access control framework with automated provisioning workflows - Created privileged access management solution with just-in-time access and session recording - Established regular access certification process with automated reviews and attestation

**Security Awareness and Culture Program** - Developed comprehensive security awareness program targeting different employee roles - Created phishing simulation campaign with targeted education for susceptible users - Implemented security champions program to promote security culture across departments - Developed security metrics to measure effectiveness of awareness initiatives and behavior