**Sr. Cyber Security Engineer**

**Preethi Pakala  **

**Contact: +1 475-319-9 819**

**Mail: preethipakala99@gmail.com**

**Professional Career Profile:**

* Around 10yr of experience as Cyber Security Engineer with good experience in Implementation, Administration, Operation and troubleshooting of enterprise data networks.
* Proficient in utilizing the MITRE ATT&CK framework to analyze and assess potential security threats and vulnerabilities within an organization’s network and systems.
* Proficient in implementing, configuring and managing Cisco Stealth watch, a comprehensive network visibility and security analytics platform.
* Skilled in creating and managing firewall policies on FortiGate devices. Able to define access control rules, NAT (Network Address Translation) rules, and virtual IP mappings to control traffic flow and secure network perimeters.
* Led the implementation and integration of CASB solutions (e.g., Microsoft Defender for Identity, Netskope, McAfee MVISION) to provide visibility and control over cloud services and applications used by the organization.
* Coordinated with cross-functional teams to integrate CASB with existing security tools (SIEM, IAM, DLP) to enhance threat detection, data loss prevention, and compliance enforcement in cloud environments.
* Developed and led the organization's incident management process, ensuring that all security incidents were promptly identified, reported, and resolved in line with CISM best practices.
* Proficient in using load balancing techniques such as round-robin, weighted round-robin, least connections, and session persistence.
* Expertise in working with Meraki MX series firewalls, including configuration, monitoring, and troubleshooting.
* Implemented firewall rules, ACLs, and encryption mechanisms to secure database traffic and mitigate threats.
* Performed regular patch updates, troubleshooting, and fine-tuning of DAM solutions for optimal performance.
* Integrated Bit bucket with other development tools such as JIRA, Confluence, and Jenkins to enable seamless integration and traceability across the development lifecycle.
* Spearheaded the design and implementation of secure architecture for large-scale enterprise systems, ensuring alignment with organizational security policies, regulatory requirements, and industry best practices.
* Conducted comprehensive threat modeling and risk assessments for enterprise applications, identifying vulnerabilities and ensuring that the security architecture mitigated potential risks and threats.
* **Implemented and managed Cisco ISE solutions**
* **Configured and deployed Cisco ISE for policy-based access control**, enabling dynamic device authentication and guest network management to enhance security and compliance with organizational policies.
* for network access control, ensuring secure authentication, authorization, and accounting (AAA) policies for users and devices across enterprise environments.
* Developed and implemented Zero Trust Architecture (ZTA) for the enterprise, enhancing the security posture by enforcing strict access controls, least privilege policies, and continuous verification of users and devices.
* Developed and enforced security policies based on the principles of Zero Trust Architecture, including least-privilege access, micro-segmentation, and continuous authentication for all network users and devices.
* Designed and implemented robust cybersecurity strategies to protect sensitive taxpayer data and ensure compliance with IRS security protocols and federal regulations.
* Implemented and managed Microsoft Information Protection (MIP) policies across enterprise environments to safeguard sensitive data and comply with data privacy regulations.
* Developed and deployed Data Loss Prevention (DLP) policies in Office 365 to prevent the accidental sharing of sensitive data, ensuring compliance with industry standards (e.g., GDPR, HIPAA).
* Integrated Azure Information Protection (AIP) labels with DLP policies in Office 365 to automatically classify and protect sensitive data based on content type, such as financial reports or personally identifiable information (PII).
* Designed and implemented CI/CD pipelines to automate the building, testing, and deployment of secure code, ensuring faster and more reliable software delivery with integrated security checks.
* Integrated security testing tools (e.g., SAST, DAST, SCA) into CI/CD workflows to identify vulnerabilities early in the development lifecycle and mitigate risks before deployment.
* Developed and maintained Python-based data pipelines to automate the extraction, transformation, and loading (ETL) of large datasets, ensuring seamless integration across multiple databases and cloud storage solutions.
* Built efficient, scalable ETL workflows using Python libraries like pandas, Dask, and PySpark to process large datasets and integrate with relational (SQL) and NoSQL (MongoDB) databases.
* Designed custom data ingestion pipelines with Python to extract data from diverse sources including REST APIs, CSV, JSON, and XML files, as well as cloud platforms like AWS S3, Google Cloud Storage, and Azure Blob Storage.
* Implemented automated security scans using tools like OWASP ZAP, SonarQube, and Checkmarx in the CI/CD pipeline to enforce secure coding standards and reduce vulnerabilities in production code.
* Designed secure cloud architectures (AWS, Azure, Google Cloud) for enterprise systems, incorporating strong encryption, identity and access management (IAM), and security monitoring to ensure data protection and compliance.
* Performed regular audits using Microsoft Information Protection tools to identify and mitigate risks associated with sensitive data handling across cloud and on-premises systems.
* Designed, deployed, and managed enterprise-level Data Loss Prevention (DLP) solutions such as Symantec DLP, Digital Guardian, or McAfee DLP, reducing data breach incidents by [percentage].
* Integrated security controls such as firewalls, intrusion detection/prevention systems (IDS/IPS), data loss prevention (DLP), and multi-factor authentication (MFA) into the enterprise systems architecture, strengthening overall defense-in-depth strategies.
* Implemented code review workflows using pull requests in Bitbucket to ensure code quality and foster collaboration.
* Provide operational support for security tools, troubleshooting issues and ensuring ongoing system integrity.
* Collaborate with cross-functional teams, including development, operations, and risk management, to address security vulnerabilities and compliance gaps.
* Identified risks and vulnerabilities in the organization’s IT infrastructure, systems, and processes, and provided actionable recommendations to mitigate risks based on audit findings and CISA guidelines.
* Audited internal systems for compliance with industry standards and regulations, including GDPR, HIPAA, PCI-DSS, and SOX, ensuring appropriate controls were in place and functioning effectively.
* Delivered clear, concise audit reports to senior management and stakeholders, outlining findings, risks, and actionable recommendations for improvement based on CISA standards.
* Suggested improvements in IT processes, controls, and procedures to increase efficiency, reduce risk, and enhance security based on audit results and industry benchmarks.
* Managed the planning, execution, and reporting of IT audits, covering areas such as risk management, IT governance, system controls, and compliance with regulatory requirements (e.g., SOX, GDPR).
* Perform risk analyses, recommending strategies to mitigate risk and enhance organizational security posture.
* Expertise in executing and enhancing technology risk programs and conducting self-assessments for various lines of business.
* Development, review, and maintenance of operational and technology risk programs, ensuring compliance with PNC risk standards.
* Performing risk and control self-assessments to ensure adherence to business and regulatory expectations.
* Experienced in configuring and managing Palo Alto Networks firewalls to ensure network security. Skilled in rule creation, policy enforcement, VPN setup, and threat prevention using Palo Alto's security features.
* Successfully implemented and configured Akamai Web Application Firewall to protect web applications against a wide range of cyber threats, including OWASP Top 10 vulnerabilities, DDoS attacks, and application-layer attacks.
* Developed and customized Akamai WAF rules and policies to suit specific application security requirements.
* Designed and implemented cloud security architectures for federal clients, ensuring alignment with FedRAMP requirements and federal security frameworks, including NIST 800-53.
* Led the implementation and validation of NIST 800-53 security controls within cloud environments, ensuring compliance with FedRAMP Moderate and High impact levels for federal contracts.
* Ensured compliance with FDA and other federal data acquisition standards such as FISMA (Federal Information Security Modernization Act) and NIST (National Institute of Standards and Technology) guidelines for the protection of sensitive data.
* Experience in Identity and Access Management (IAM) security operations, policy, governance, development, testing and access control provisioning.
* In depth knowledge of AWS cloud services like Compute, Network, Storage and Identity and Access Management.
* Monitored access logs to ensure compliance with RBAC policies, identifying and investigating instances of unauthorized access or privilege escalation.
* Leveraged RBAC as part of security incident investigations, identifying roles with excessive permissions and recommending adjustments to minimize security risks.
* Worked with IAM and systems administrators to audit and review RBAC assignments, ensuring correct permissions were granted, and invalid access was promptly revoked.
* Worked with Infrastructure team to deploy crowd strike agent to all assets.
* Reduced the overall application vulnerability footprint by implementing a combination of **SAST**, **DAST**, and **SCA**, addressing issues proactively at both the code and runtime levels.
* Conducted regular training for development teams on secure coding practices, emphasizing the importance of **SAST**, **DAST**, and **SCA** in mitigating security risks across both in-house and third-party code.
* Automated data protection workflows in MCAS to ensure that all sensitive data uploaded to cloud apps is encrypted and classified according to company security standards.
* Created and Cribl enforced DLP policies to protect sensitive information (e.g., PII, intellectual property, financial data) by defining data classification, encryption, and access control measures.
* Utilize cloud-based APIs when appropriate to write network/system level tools for securing cloud environments.
* **Implemented network automation solutions** using tools like **Ansible**, **Python**, and **Netmiko** to automate repetitive network configuration tasks, reducing deployment time by 40% and minimizing human errors.
* Strong analytical background in data mapping, data-driven insights, and risk trend analysis.
* **Deployed and managed network intrusion detection systems (IDS)** such as **Snort** and **Suricata**, configuring custom rule sets to monitor and detect malicious network traffic, improving threat detection capabilities by 30%.
* Integrated threat intelligence feeds and services into the Akamai WAF platform, enhancing the ability to identify and block malicious IPs, user agents, and emerging attack patterns.

**Professional Skills**

* Cyber Security Design, Operations and Management
* Cyber security Incident and Offensive Management
* Cyber Security Disaster / Continuity Management
* Cyber Security Threat Intelligence
* Cyber Security Professional Trainings and Awareness
* Cyber Security Project, Program and Change Management
* Cyber Security Audit
* Application security / Vulnerability Management
* Cloud Security, Routers, Switches, Firewalls, Endpoints Protection
* CISO Management
* Information Security Policies, Controls, Governance and Compliance
* NIST, ISO, MITRE ATTACK, PCI DSS,SABSA and TOGAF
* SIEM (Security Event and information Management)
* IOT (Internet of Things)
* College Teaching, specialized in Cyber Security / Information Security Domain
* **Risk Management Tools:**
  + GRC Tools (Governance, Risk, and Compliance)
  + ServiceNow (Risk Management Functions)
  + Microsoft Office Suite (Excel, PowerPoint, SharePoint)
  + Tableau, Visio (Data Visualization and Process Mapping)
* **Technology Risk Management in Financial Institutions**
  + KY3P (Know Your Third Party)
  + 1st Line of Defense Risk Experience

**Key Skills**

* **Veracode**: Expert in conducting SAST and DAST.
* **Container Security**: Proficient in securing containers in **ROSA**, **Tekton**, and **OpenShift** pipelines.
* **CI/CD Orchestration**: Hands-on experience with **Jenkins**, **Tekton**, **GitLab**, and **Bamboo**.
* **Container Security Tools**: Operational support for **Palo Alto Prisma**, **Aqua**, or equivalent tools.
* **Baseline Image Validation**: Perform baseline image validation of new container templates.
* **Vulnerability Scanning**: Conduct vulnerability scans and maintain container security.
* **OWASP Top 10**: Strong understanding of common vulnerabilities and mitigations.
* **Secure Coding**: Apply secure coding practices using **Java**, **C#.NET**, and **JavaScript**.
* **Pen Testing**: Perform penetration testing on internally developed applications.
* **API Security**: Conduct security assessments against web applications and APIs.
* **Security Assessments**: Ensure security and privacy by design in all architecture/infrastructure.

**TECHNICAL SKILLS:**

**SIEM**: Splunk, LogRhythm, IBM QRadar

**Vulnerability Management Tools**: Nessus, Nmap, Nexpose, Wireshark, OWASP

**Security Tools**: GuardiCore, McAfee Vulnerability management solutions, Nessus, SolarWinds, LogRhythm, Tenable, Proof point.

**IPS/IDS**: McAfee IPS, Secure Works IDS/IPS, SNORT

**Firewall**: Cisco ASA, Firepower Module (context firewalls), ACLs, IPSEC, Palo Alto, Panaroma, Checkpoint Firewall, Fortinet Firewall (Traffic Shaping)

**Network Management**: Wireshark, SNMP, SolarWinds NCM+NPM, Live NX

**Platforms/Applications**: Continuous Monitoring Vulnerability Management, Web Application Scanning, Threat Protect, Policy Compliance, Cloud Agents, Asset Management, Governance, Risk Management, and Compliance, SolarWinds, Burp suit, NMAP, Wireshark, Kali, App Dynamics, Extra hop, Observe, Confluence, Nagios, Zabbix, SQL Server Management

**Ticketing Tools**: Service Now, Alloy Navigator, My-cherwell

**Education:** Bachelor’s in CSE, JNTU, Hyd, India.

**Certifications:**

* Certified Information Systems Security Professional (CISSP)
* Cisco Certified Internetwork Expert (CCIE)
* Certified information security Manager (CISM)
* Certified information security Auditor (CISA)
* Certified Cloud Security Professional (CCSP)
* Certified in Microsoft Azure Architect .

**Professional Experience:**

**WSFS, New Fairfield, CT** **Duration: Sep 2023 – Till Date**

**Sr. Cyber Security Lead Engineer**

**Responsibilities:**

* [Responsible for planning, studying, and designing robust security architectures for clients.](https://www.infosectrain.com/blog/roles-and-responsibilities-of-a-security-architect/)
* Created and maintained security dashboards and metrics to track and report on the status of security tests, vulnerabilities, and remediation efforts throughout the SDLC.
* Utilized RBAC to support Zero Trust architecture by continuously verifying the roles and permissions of users and devices before granting access to enterprise applications.
* Integrated **SAST**, **DAST**, and **SCA** tools into the organization’s DevSecOps pipeline, enabling continuous security testing throughout the software development, testing, and deployment processes.
* Led the implementation of automated RBAC policy enforcement using Identity and Access Management (IAM) solutions to ensure ongoing adherence to organizational security requirements.
* **Monitored network traffic and analyzed IDS alerts** to identify potential security threats, reducing false positives and improving response times to network intrusions through the use of advanced filtering and correlation techniques.
* Worked with project stakeholders and system SME’s to guide them through all phases of the certification and accreditation process.
* Manage CSAM Inquiries and Troubleshooting Process (CSAM SME).
* Performed comprehensive security assessments on data platforms to identify risks and gaps in protection.
* Administered security measures for federal data systems in alignment with FDA requirements, ensuring proper encryption, access control, and data masking for sensitive information.
* Conducted risk assessments and audits on FDA-regulated data systems to ensure adherence to federal guidelines for secure data handling and minimize the risk of data breaches.
* Assisted in the development and enforcement of cloud security policies by leveraging CASB solutions to define acceptable use, access controls, and data protection standards for cloud-based applications.
* Worked closely with security and compliance teams to design policy enforcement rules that govern access to and data handling within SaaS, IaaS, and PaaS environments.
* Led incident response efforts, identifying and mitigating potential cyber threats to IRS systems, ensuring minimal disruption and safeguarding critical financial data.
* **Led the integration of Cisco ISE with Active Directory and LDAP**, streamlining user authentication and identity management processes while strengthening network security through role-based access control (RBAC).
* **Configured Cisco ISE to support 802.1X authentication**, enhancing wired and wireless network security by ensuring only authorized devices could access the network.
* Led and conducted comprehensive audits of information systems to assess their effectiveness in achieving security, compliance, and operational objectives, ensuring alignment with CISA standards and best practices.
* Designed policies and reporting mechanisms for monitoring unauthorized access, improving overall database security posture.
* Design and Implement Cyber Security policies, standards, procedures, and Cyber security controls.
* Provided SME Level 3 support and direction for production related issues.
* Integrated Multi-Factor Authentication (MFA) as a core component of Zero Trust Architecture, ensuring secure user authentication across all access points, applications, and devices.
* **Integrated IDS with SIEM solutions** (e.g., **Splunk, ArcSight**) to centralize alert management and improve incident detection, enabling quicker responses to critical network security events.
* Conducted **comprehensive penetration tests** on client networks, identifying vulnerabilities in **routers, firewalls, switches**, and **VPNs** using manual and automated testing tools (e.g., **Nessus, Qualys, OpenVAS**).
* Implemented CrowdStrike Falcon Endpoint Protection to enhance threat detection and prevention capabilities, reducing security incidents by X% in the first quarter.
* Monitored and analyzed endpoint security using CrowdStrike's EDR capabilities, identifying and mitigating advanced persistent threats (APTs) in real time.
* Collaborated with the threat intelligence team to incorporate CrowdStrike's intelligence feeds into the security operations center (SOC), improving proactive defense measures.
* Integrated Microsoft Information Protection with Microsoft Defender for Identity, enabling a comprehensive security approach that protected sensitive data while mitigating advanced threats.
* Automated data workflows using Python-based scheduling tools like Apache Airflow, enabling efficient, recurring data loads from various sources into centralized data repositories.
* Integrated Python with cloud scheduling services such as AWS Lambda and Google Cloud Functions to trigger automated data pipeline executions based on events and changes in data sources.
* Completed the ATO process as both Infrastructure and Security SME for Thales and Vormetric products.
* Conducted regular vulnerability assessments and penetration testing of IRS systems to identify security gaps, improving overall system resilience.
* Ensured adherence to IRS cybersecurity policies and procedures, including compliance with federal regulations such as FISMA, NIST, and the Privacy Act to safeguard taxpayer data.
* Partnered with government agencies (FBI, DHS, etc.) and financial institutions to enhance threat intelligence and collaborate on cybersecurity initiatives, strengthening IRS defenses against cyberattacks.
* Designed, implemented, and administered Data Access Management (DAM) solutions using IBM Guardium and Imperva, ensuring robust data security across Oracle, MS SQL, PostgreSQL, and cloud-hosted databases (AWS RDS, Azure SQL).
* Applied DevSecOps principles by incorporating security into the CI/CD pipeline, automating security reviews, compliance checks, and vulnerability scanning at each stage of the software development lifecycle.
* Worked closely with software development, infrastructure, and IT teams to ensure that security was embedded at every stage of the enterprise systems' lifecycle, from design to deployment.
* Led the FedRAMP authorization process for cloud service providers (CSPs), ensuring that all security controls were implemented to meet federal government standards and guidelines.
* Enterprise Security Standards Compliance: Ensured enterprise systems architecture met security standards and frameworks, including ISO 27001, NIST, SOC 2, GDPR, and PCI-DSS, achieving compliance and reducing security risks.
* Configured DLP rules to monitor and protect sensitive data across O365 applications (Outlook, SharePoint, OneDrive, Teams), reducing the risk of data breaches due to misconfigured sharing settings or employee error.
* Deployed DLP policies for data protection in SharePoint and OneDrive for Business, restricting the sharing of sensitive files externally and ensuring data retention policies were in place to protect organizational assets.
* Security Architecture Roadmap: Developed a multi-year security architecture roadmap to align with business goals, incorporating emerging security technologies and ensuring scalability and resilience for future growth.
* Developed and maintained comprehensive security documentation for FedRAMP compliance, including Security Authorization Packages (SAP), System Security Plans (SSPs), and Continuous Monitoring Plans.
* Performance Optimization Cribl and Balanced security requirements with system performance, ensuring that the secure architecture design did not hinder system performance or user experience while maintaining compliance with security policies.
* Performed installations, configurations, patch management, and troubleshooting of security agents and appliances to maintain optimal performance.
* Delivered educational sessions on ISO 27001’s principles, best practices, and how they contribute to the organization's security objectives.
* Created, tested, and fine-tuned policy rules and reports to monitor unauthorized data access and anomalies.
* [Design and provide technical advice on the implementation of security controls, Cyber security Policies, frameworks implementation such as, MITRE ATTACK, NIST, ISO 27001, PCI DSS, SABSA and TOGAF across corporate and business systems.](https://www.velvetjobs.com/job-descriptions/principal-security-architect)
* Provided regular reports and insights on vendor risk exposure to senior leadership, recommending mitigation strategies to reduce organizational risk.
* Facilitated vendor audits and assessments, ensuring adherence to contractual agreements and industry best practices for data protection and cybersecurity.
* Developed network architecture solutions utilizing Cisco products such as Cisco Nexus, Catalyst, and ASR routers to meet organizational performance, security, and scalability needs.
* Designed and implemented SAML-based Single Sign-On (SSO) solutions to provide secure, seamless access to multiple cloud and on-prem applications, reducing password fatigue and improving user experience.
* Integrated SAML authentication with third-party identity providers (IdPs) such as Active Directory Federation Services (ADFS), Okta, and Azure AD to streamline user authentication across enterprise systems.
* Led incident response efforts involving third-party vendors, coordinating with external partners to remediate security incidents and minimize impact.
* Successfully implemented IBM Guardium DAM across multi-regional database infrastructure, improving data governance and compliance.
* Reduced unauthorized data access incidents by 30% through proactive monitoring and policy fine-tuning.
* Streamlined patching processes, achieving zero downtime for critical database systems.
* Led the implementation of a multi-layered application security strategy, utilizing SAST, DAST, and SCA to ensure comprehensive security coverage across the software development lifecycle.
* Developed and enforced security best practices for developers, including the integration of SAST in the CI/CD pipeline, regular DAST assessments, and continuous monitoring of third-party components using SCA tools.
* Integrated Zscaler with existing SIEM systems to streamline threat detection and response, enabling more efficient real-time alerts and enhancing incident response capabilities.
* Configured Zscaler ZPA (Private Access) for seamless, secure remote access to internal applications, supporting remote workforce security initiatives without compromising performance.
* Led the deployment of PingID as part of a Zero Trust architecture to enforce continuous verification of user identity and device security before granting access to enterprise resources.
* Collaborated with cross-functional teams to integrate PingID MFA across various enterprise platforms, ensuring a unified approach to access control and enhancing overall security posture.
* Conduct vulnerability scans on container environments and perform baseline image validation of new container templates.
* Led cross-functional teams to implement comprehensive information security programs, aligning with business needs while managing risk and protecting critical assets.
* Established and maintained security metrics and reporting mechanisms, providing clear, actionable insights to executive leadership based on CISM guidelines.
* Led the response to DLP incidents by investigating data leakage events, identifying vulnerabilities, and providing actionable remediation steps to prevent future data losses.
* Developed CI/CD processes to ensure that all security and compliance requirements (e.g., GDPR, HIPAA, PCI-DSS) were met during automated deployments, reducing the risk of non-compliance.
* Automated audit logging and security monitoring within CI/CD pipelines to provide continuous security monitoring and compliance tracking for deployed applications, ensuring that security posture was maintained.
* Conducted training sessions for staff on best practices for data security, emphasizing the importance of DLP controls and responsible data handling.
* Spearheaded security awareness programs for employees, emphasizing the importance of adhering to security policies and practices outlined in the CISM framework.
* Communicated security issues, risks, and mitigation strategies effectively to the executive team, leveraging CISM methodologies to highlight risks and propose strategic solutions.
* Troubleshoot connectivity and operational issues in containerized environments, ensuring uninterrupted security operations.
* Validate and remediate vulnerabilities identified through static and dynamic analysis tools.
* Develop and present detailed findings and remediation reports to cross-functional teams and senio

**CISCO, San Jose, CA** **Duration: Jan 2022 – Aug 2023**

**Cyber Security Engineer**

**Responsibilities:**

* Responsible for Intellectual Assets Protection Management (Cyber Security) 65 Security and IT Infrastructure and Builds.
* Supervise Global Security architects in build Existing security infrastructure, Remediation, and hardening process.
* Lead Risk Assessment process and operations of 65 Security infrastructure and Build Environments GRC.
* Led the integration of **security controls** throughout all phases of the SDLC, from planning and design to development, testing, deployment, and maintenance, ensuring security was a foundational aspect of every project.
* Led **threat modeling** sessions during the design phase of the SDLC to identify potential security threats and plan mitigations before development started.
* Collected and analyzed external and internal threat intelligence from multiple sources (e.g., threat feeds, open-source intelligence, dark web, and vendor-specific reports) to identify emerging threats and vulnerabilities.
* Conducted comprehensive analysis of cyber threat data to identify indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs) used by adversaries, improving proactive defenses.
* Utilized threat intelligence platforms (TIPs) like ThreatConnect, Anomali, or IBM X-Force to aggregate, analyze, and visualize threat data.
* Led incident response efforts related to FDA-regulated data, identifying and mitigating security threats to ensure rapid containment and reporting in compliance with federal data protection regulations.
* Coordinated with government agencies and internal teams to address and report any FDA-compliant data breaches, ensuring regulatory obligations were met and appropriate mitigation actions were implemented.
* Conducted risk assessments and vulnerability scanning on cloud systems to identify security gaps, ensuring continuous FedRAMP compliance and adherence to federal cybersecurity standards.
* Leveraged CrowdStrike's machine learning algorithms to automate incident response and threat hunting, reducing response times.
* Deployed and configured Zscaler's Secure Web Gateway (SWG) to enhance cloud-based web filtering and real-time threat protection, reducing malware incidents by X% in the first quarter.
* Conducted risk assessments and security audits using CASB tools to monitor and identify risky behavior or unapproved cloud applications (Shadow IT) being used within the organization.
* Developed and implemented real-time monitoring and alerting for cloud environments, enabling proactive risk mitigation and ensuring compliance with regulatory frameworks such as GDPR, HIPAA, and SOC 2.
* Implemented Zscaler’s Zero Trust Architecture (ZTA) And Cribl for secure application access, ensuring consistent policy enforcement and reducing the risk of unauthorized access by X%.
* Monitored Zscaler’s cloud security platform to detect and mitigate potential threats, providing continuous protection against data breaches, ransomware, and malicious web traffic.
* Performed security assessments and vulnerability management by using CrowdStrike’s vulnerability scanning tools and techniques to identify and remediate potential risks.
* Monitored and responded to authentication-related security incidents using PingID analytics, investigating and mitigating suspicious activity such as credential stuffing or phishing attempts.
* Automated user provisioning and de-provisioning workflows with PingID to enforce least privilege access principles and reduce insider threat risks.
* Automated data loss prevention workflows for monitoring and blocking unauthorized access or transmission of sensitive data across endpoints, networks, and cloud services.
* Led initiatives to ensure compliance with regulations like GDPR, HIPAA, and PCI-DSS using Azure and O365 DLP capabilities, ensuring data privacy and security controls were effectively enforced.
* Manage Teams of Cyber security / Build Security for Upgrading and design new security infrastructure.
* Integrated automated vulnerability management tools into CI/CD pipelines, such as Nexus IQ and Qualys, to continuously monitor for vulnerabilities in third-party libraries, container images, and infrastructure.
* Deployed RBAC across cloud platforms (AWS, Azure, Google Cloud) to enforce granular access policies and ensure secure, role-based permissions to cloud resources.
* Configured RBAC with multi-factor authentication (MFA) to strengthen access control for critical systems and ensure access is granted based on least privilege principles.
* Conducted training sessions for employees on best practices for handling sensitive information and using MIP tools, significantly reducing instances of non-compliance.
* Developed and maintained user awareness programs on data protection and security, including training on Microsoft Information Protection policies and tools.
* Administered and managed database security solutions for relational databases (Oracle, MS SQL, MySQL) and cloud-hosted services (AWS PaaS/DBaaS, Azure SQL).
* Collaborated with stakeholders to identify security gaps and implemented policies to address vulnerabilities and improve data security compliance.
* Designed secure data architectures, ensuring scalability, cost-efficiency, and alignment with HIPAA, FISMA, and CPRA regulations
* Worked Application Security process and operations.
* Involved in New Cyber Security infrastructure design and deployment phases.
* Developed and deployed automated data quality checks in Python to detect anomalies, validate data integrity, and flag errors during the ETL process, ensuring clean and reliable datasets.
* Implemented logging and monitoring mechanisms using Python libraries such as Loguru and Celery to track pipeline execution, identify bottlenecks, and ensure data processing stability.
* Collaborated with IT and security teams to implement end-to-end data protection strategies, including encryption, access controls, and DLP to safeguard against both insider and outsider threats.
* Manage cyber–Security Risk Assessment, Compliance, Audit and Program Management
* GRC Policies using MITRE ATTACK, NIST, ISO 27001, PCI DSS, SABSA and TOGAF.
* Establish and maintain the Cyber Security program management guidelines.
* Routine Trainings to team lead include new security infrastructures andSecurity Awareness Trainings.
* Actively monitored DLP alerts, generated comprehensive reports for management, and recommended actions to minimize exposure of sensitive data across various endpoints and communication channels.

**Ascena retail group, Patskala, OH** **Duration: Sep 2019 – Dec 2021**

**Cyber Security / Information Security**

**Responsibilities:**

* Assist with the overall business technology planning, providing current knowledge and future vision of technology and systems.
* Implements security controls, risk assessment framework, and program that aligns to regulatory requirements.
* Evaluates risks and develops security standards, procedures, and controls to manage risks. Improves PCC’s security positioning through process improvement, policy, automation, and the continuous evolution of capabilities.
* Performed **security risk assessments** and vulnerability scans at key stages of the SDLC, helping to prioritize and address the highest risks early in the project lifecycle.
* Integrated **Static Application Security Testing (SAST)** and **Dynamic Application Security Testing (DAST)** tools into the SDLC, automating security testing and vulnerability detection throughout development.
* Implemented automated rollback mechanisms in CI/CD pipelines to quickly revert deployments in case of security breaches or vulnerabilities, ensuring business continuity and minimizing downtime.
* Developed and maintained incident response playbooks that integrate with CI/CD pipelines, enabling rapid identification, mitigation, and resolution of security incidents.
* Developed custom DLP templates for specific compliance needs (e.g., financial data, medical records) in O365 and Azure, ensuring that organizational policies met both internal security and regulatory requirements.
* Led incident response efforts using Microsoft Information Protection and Security & Compliance Center to investigate and remediate potential data breaches and unauthorized access incidents.
* Deployed Microsoft Cloud App Security (MCAS) to monitor and analyze cloud-based applications, identifying and mitigating suspicious activities and potential threats across the organization’s cloud infrastructure.
* Designed and implemented Identity and Access Management (IAM) strategies for cloud and on-premises environments to ensure secure, scalable, and efficient management of user identities and access permissions.
* Developed IAM architectures that support role-based access control (RBAC), least privilege principles, and multi-factor authentication (MFA) to enhance security across the enterprise.
* Configured and maintained DLP policies within CASB tools to monitor, control, and prevent sensitive data from being accessed, shared, or leaked across cloud applications.
* Integrated CASB DLP capabilities with other data protection systems to ensure a comprehensive and unified data security strategy for cloud-based applications and services.
* Leveraged MCAS to monitor user activity, file access, and data sharing in real-time, proactively identifying abnormal behaviors and reducing potential security breaches by X%
* Review and Update CISO Policies twice a year.
* Implements processes, such as GRC (governance, risk, and compliance), to automate and continuously monitor information security controls, exceptions, risks, testing. Develops reporting metrics, dashboards, and evidence artifacts, using frameworks MITRE ATTACK, ISO 27001, PCI DSS, SABSA and TOGAF
* Updates security controls and provides support to all stakeholders on security controls covering internal assessments, regulations, protecting Performs and investigates internal and external information security risk and exceptions assessments. Assess incidents, vulnerability management, scans, patching status, secure baselines, penetration test result, phishing, and social engineering tests and attacks.
* Designed and executed organization-wide training programs to raise awareness of ISO 27001 standards, ensuring that all employees understand their role in maintaining information security.
* Develop, implement, and monitor a strategic, comprehensive enterprise information security and IT risk management program.
* Work directly with the business units to facilitate risk assessment and risk management processes.
* Documents and reports control failures and gaps to stakeholders
* Provides remediation guidance and prepares management reports to track remediation activities.
* Supervise Application owners for application security requirements and approvals.
* Set up real-time monitoring and alerting for DLP policy violations across O365 services (Exchange Online, SharePoint, OneDrive), enabling prompt responses to potential data leaks or breaches.
* Facilitate IT auditors and Perform internal ISD audit.

**Client: Klazigo Pvt Ltd, Hyd, India.** **Duration: May 2017 to Apr 2019**

**Cyber & Information Security**

**Responsibilities:**

* Administer and maintain Cyber Security policies to assure the safety and Security of Cyber Security Infrastructure
* Develop policies and procedures to protect enterprise communications, systems, and assets from internal and external threats.
* Create disaster and/or crisis preparedness plans.
* Responsible for overseeing an organization's overall cyber security.
* Supervises aspects of Cyber security including design, development
* Cyber Security Governance, Risk and Compliance.
* Cyber Security Project Management
* implementation, incident response and Threat Intelligence
* Budgets, and adherence to various regulations.
* Assist in building relationships with vendors and creating cost-efficient contracts.
* Integrated Microsoft Cloud App Security with Microsoft Defender for Identity and other Microsoft security solutions to create a unified security ecosystem, enhancing the ability to detect and respond to advanced threats.
* Configured MCAS policies to integrate with Microsoft Defender for Office 365, ensuring seamless protection of cloud applications and email systems against phishing and malicious activity.
* Configured and delivered detailed DLP violation reports to leadership and compliance teams, providing insights into sensitive data activity and risk areas for continuous improvement.
* Utilized MCAS Cloud App Discovery to gain insights into shadow IT by identifying unsanctioned applications, providing recommendations for mitigating risks associated with unauthorized cloud apps and improving compliance.
* Analyze the business requirements of all departments to determine their technological needs.
* Coordinate IT managers and supervise computer scientists, technicians, and other professionals to provide guidance.
* Recruit, train, and schedule security personnel.

**Client: Wide Business solutions, Hyderabad- India Duration: June 2015 to May 2017**

**Cyber Security / IT Security**

**Responsibilities:**

* Worked and Provided security guidance on a constant stream of new backend/core infrastructure and technologies.
* Worked on Analyze, assess, and respond to various internet threats.
* Interact directly with the security community regarding infrastructure security vulnerabilities and threats.
* Used Routine Operations of Firewalls and Proxy Servers
* Deliver ultra-high availability of Alcatel Telecommunications switching system security and access management.
* Participated in requirements/control definition, implementation design, build and staging, Verification and transition to maintenance and support.
* Developed and implemented conditional access policies in MCAS to enforce strict access controls for cloud-based applications, reducing unauthorized access and strengthening security for remote workers.
* Design, configure, and support security deployments including Firewalls, Proxy servers and Windows servers. Routine meeting with Clients related to Network and system Security related issues.