NETWORK SECURITY ANALYST

Summary

Solid background in organizational cyber security, documentation and proactively monitoring and managing the ever changing landscape of cyber security within an IT enterprise ecosystem. Consistently met and exceeded customer and supervisor expectations through adapting practical industry technologies and solutions. Good technical documentation and pragmatic management skills. Works well in team settings as well as on individual projects. Experience in analysis, implementation, compliance and evaluation of operational policies and risk assessment. *High level knowledge of Project Management, compliance legislation (HIPAA, FERPA, SOX, PCI-DSS, FISMA, GLBA). *Knowledge in Information Systems Security, Network Security and Security Posture. Internal control framework (ISO 27001) *Hands on security management software (Mcafee ePO, IPS, Nexpose Rapid7, Proofpoint, VPN, Cisco ISE) *Strong Access Management, testing and regulatory operational risk management. *In-depth knowledge of the different steps of Risk Management Framework (RMF), System Development Life Cycle (SDLC), NIST 800-Series, Security Assessment & Authorization. *Experience in the development of System Security Plan (SSP), Contingency Plans, Disaster Recovery Plans, Incident Response. Knowledge of Plan of Action and Milestones (POA&M), Security Assessment Report (SAR), Risk Assessment Report (RAR), Policy and Process Development. *Penetration Testing, Vulnerability Scanning, Anti-virus and Malware, Application Code Scanning and Secure Coding Practices, Configuration Management, File Integrity Monitoring, Multi-Factor Authentication, Encryption and Key Management, Hardening of servers and network devices.

Work History

Asrc Federal Holding Company

Experience

02/2017 to 08/2017

Network Security Analyst Vista Equity Partners ï¼ Layton , MN

- Oversaw operational activities and lead security migration project to enhance compliance, mitigate risk and Data aggregation (Trifacta).
- Responsible for developing security policies and reports necessary to validate systems that meet security and privacy requirements in accordance to the Risk Management Framework (RMF) authorization process.
- Work with IT personnel, Application Owners, Operational and Business Analysts, vendors to ensure stability in our Identity and Access Management (IAM) Systems.
- SailPoint, NetIQ, OIM).
- Support security tests and evaluations (ST&Es) and generate security documentation including Security Assessment Report; Requirement Traceability Matrix(RTM); Contingency Plans; Disaster Recovery Plans; Risk Assessment (RA); Privacy Impact Assessment (PIA).
- Manage, deploy, report in (McAfee ePO) manage Intrusion prevention (IPS) email filtering (Proofpoint) to meet compliance requirements and secure environment.
- Perform regular penetration testing with Rapid7 Metasploit to determine weaknesses in the infrastructure (hardware), application (software) and users in order to develop recommendations for mitigating vulnerabilities and exploits in the system.
- Conduct the role of Security Control Assessor by reviewing the artifacts and implementation statements provided by the ISSO on a system to determine if the security controls are being met.
- Conduct weekly information security reviews based on the clients implementations of frameworks such as, NIST 800.53r4, FISMA, FedRAMP and NIST 800.171.

12/2013 to 12/2016

Compliance Analyst 900Lbs Of Creative

- Coordinated PCI assessments -related tasks to ensure the readiness of managers and their teams for assessment testing and facilitating the timely resolution of any findings.
- Created agent files in Mcafee ePO, deployed agents, synchronized agents in AD, managed policies, configured products update, created custom event and table queries, managed repository.
- Configured sensors and signatures, managed components, dashboard, policies, reports and devices.
- Managed radius servers, authorization, and audit log parameters in IPS/NSM.
- Managed progresses of remediation steps to identified control deficiencies.
- Created hyper-personalized engagements for customer Identity and Access Management (CIAM) platforms to break traditional identity and access management (IAM) solutions .that aligns with customer expectations, met privacy concerns and complied with multiple third party privacy policies and government regulations.
- OneLogin, IBM).
- Analyzed and assessed incident response activities to ensure that appropriate actions were taken to minimize the potential of future occurrences.
- Reviewed and updated remediation on (POA&Ms), in the organization's Cyber Security Assessment and Management (CSAM) system.
- Worked with system administrators to resolve POA&Ms, gathering artifacts and creating mitigation memos, residual risk memos and corrective action plans to assist in the closure of the POA&M.
- Assisted with Incident Response training and testing.

06/2003 to 06/2013

Account Executive Company Name ï¼ Bloomington , State

- Determined prospective customers' needs for credit card processing and other service through negotiation to present First Data services that meet those needs.
- Prepared and presented proposals and provided appropriate follow-up throughout the sales process.
- Completed and obtained documentation required for the conversion of data from previous merchant service provider to the First Data

system.

- Worked directly with internal departments to insure the client has a smooth transition to their new merchant service provider.
- Developed prospects through cold calling, referrals, professional and personal contacts and other sources.
- Maintain contact with existing customers to determine needs for additional services.
- Exceeded quarterly and annual sales quota with a proven successful track record of phone based sales.
- Software / Artifacts / Platform & Methodologies: Identity Management System (IDMS), Physical Access Control Service System (PACS), UNIX, Microsoft Tools - Word, Project, Excel, PowerPoint, Security Assessment and Authorization.
- Confidentiality, Integrity, Availability, Vulnerability Scans, Contingency Planning, Policies and Procedures, Access Control, Risk Assessment, Implementation, Incident Response, Implementation RMF Tools CSAM, Risk Vision, TAF, Xacta, Remedy, Nessus, E-Authorization, Checkpoint, Rapid7, Websense, McAfee, IPS/IDS, EPO, NIST SP 800-18, 800-37, 53A rev4, 800-30, VMWare ESXi 6 Microsoft Server: 2003, 2008, 2012 Active Directory, GPO, DNS, DHCP, WSUS, Exchange Server 2007, 2010, 2013, Backups, VPN client configurations, Documentation, Vendor Management, Hardware Support (Server - Client).

Education and Training

February 2017

Bachelor of Science : Computer Information Systems Information Security DeVry University ï¼ City , State Computer Information Systems Information Security Dean's List Spring 2014, Fall 2014, Spring 2015, Fall 2016)

Skills

Active Directory, AD, cold calling, hardware, conversion, credit, Client, clients, DHCP, Disaster Recovery, Documentation, DNS, email, government regulations, Hardware Support, IBM, IDMS, IDS, information security, McAfee, Access, Excel, Exchange Server, PowerPoint, Word, migration, negotiation, network, PACS, PCI, personnel, Policies, proposals, Requirement, Risk Assessment, Risk Management, sales, servers, phone, UNIX, Vendor Management, VPN, Vision