ROD VIAL
Systems Security Administrator
Information Technology Infrastructure and Operations

Tasks Description

The Systems Security Administrator at Spring Financial is responsible for the protection and integrity of the organization's IT infrastructure, focusing on identifying and mitigating security threats, maintaining security protocols, and ensuring compliance with regulatory standards.

- Security Monitoring: Regularly monitor and audit server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity.
- System Administration: Administer and maintain security systems, ensuring all necessary updates, patches, and preventive measures are implemented.
- Incident Response: Develop and implement incident handling procedures and respond to security incidents promptly.
- Policy Development: Create and update IT security policies, standards, procedures, and protocols.
- Threat Mitigation: Identify, document, and assess risks, and work on detecting and mitigating cyber security threats.
- Compliance: Ensure compliance with applicable regulatory requirements and maintain data security strategies and programs.
- Technical Support: Provide support for security analytic systems, such as log monitors and IDS/IPS deployments, and troubleshoot antivirus and endpoint deployments.
- Training: Provide technical guidance and training to end-users and IT staff on security-related matters.
- Audit and Reporting: Prepare and coordinate audit activities, document management, and handle action and deadline management.

Key Interfaces

1. Internal IT Team:
   - Collaborate closely with IT Security, Tech and DevOps engineers to ensure system security protocols are integrated into daily operations and new projects.
   - Work with network administrators to monitor and secure network traffic and infrastructure.
   - Coordinate with software development teams to integrate security best practices into the development lifecycle.
2. Executive and Management Team:
   - Report to the Chief Information Officer (CIO) or Chief Technology Officer (CTO) regarding security posture, incidents, and compliance status.
   - Provide security-related insights and recommendations to senior management for strategic decision-making.
3. Compliance and Risk Management:
   - Interface with compliance officers to ensure adherence to regulatory requirements and industry standards.
   - Work with risk management teams to identify and mitigate potential security threats and vulnerabilities.
4. End-Users:
   - Engage with employees across various departments to promote security awareness and best practices.
   - Provide training and support to end-users on security tools, policies, and incident reporting procedures.
5. External Vendors and Partners:
   - Coordinate with third-party vendors for the implementation and maintenance of security solutions.
   - Manage relationships with SaaS providers to ensure security requirements are met and integrated effectively.

6. Audit and Regulatory Bodies:
    - Liaise with external auditors and regulatory bodies during security audits and compliance reviews.
    - Prepare and submit required documentation and reports to demonstrate compliance with security standards and regulations.
7. Incident Response Teams:
    - Collaborate with incident response teams to address security breaches and threats promptly.
    - Participate in the development and execution of incident response plans and drills.
8. Human Resources (HR):
    - Work with HR to implement security protocols related to employee onboarding, offboarding, and access control.
    - Coordinate with HR on security-related training and awareness programs.

Internal Collaboration Tasks

1. Security Protocol Integration:
    - Collaborate with IT administrators and engineers to ensure that security protocols are seamlessly integrated into daily operations and ongoing projects. This involves regular meetings to review current security measures and plan for upcoming implementations.
2. Network Security Monitoring:
    - Work with network administrators to monitor network traffic and infrastructure. This includes setting up and managing security tools like firewalls, intrusion detection/prevention systems, and VPNs.
3. Development Security Practices:
    - Coordinate with software development teams to embed security best practices into the software development lifecycle (SDLC). Participate in code reviews, provide input on secure coding standards, and ensure that security testing is part of the CI/CD pipeline.
4. Incident Reporting and Response:
    - Engage with end-users across departments to ensure prompt reporting of security incidents. Provide clear guidelines on what constitutes a security incident and the steps to report it.
5. Security Awareness Training:
    - Provide training sessions and materials to educate employees on security best practices. This includes creating training programs for phishing awareness, password management, and secure data handling.
6. Regulatory Compliance and Documentation:
    - Liaise with compliance officers to ensure that all security measures meet regulatory requirements. This involves maintaining up-to-date documentation and preparing reports for compliance audits.
7. Vendor Management:
    - Coordinate with third-party vendors to manage and maintain security solutions. This includes overseeing vendor performance, ensuring that security requirements are met, and integrating external solutions with internal systems.
8. Policy Development and Review:
    - Work with risk management and compliance teams to develop and update security policies and procedures.
    - Regularly review and revise policies to address emerging threats and changing regulatory requirements.
9. Security Audits and Assessments:
    - Prepare for and participate in security audits by collaborating with internal teams to gather necessary information, document security practices, and address any findings or recommendations.
    - Technical Support and Guidance:
    - Provide technical support and guidance to internal IT staff and end-users. This includes troubleshooting security-related issues, offering advice on secure practices, and mentoring junior staff members.

Key Platforms, Systems and Software Tools

1. Platforms

Cloud Platforms:
- AWS (Amazon Web Services): For cloud infrastructure and services.
- Microsoft Azure: For cloud solutions and enterprise services.
- Cisco Meraki: For Centrally Managed Network and Security Cameras

On-Premises Systems:
- Windows Server: For managing and securing server environments.
- Unix/Linux: For managing and securing UNIX/Linux-based systems.

Cloud Servers:

Windows 2019/2022:
- Windows Server 2022 WSUS Deployment
- Windows Server 2022 Active Directory Domain Service

Windows Server 2022

Linux Ubuntu 22.04.4/20.04.6 Servers:
- Apache Servers with Jenkins and Ansible automations
- Wazuh – Index, Server, Dashboard Servers
- LAMP (Linux, Apache, MySQL, PHP) – SimpleRisk

2. Software Tools

Security Management:
- Splunk/Wazuh: For security information and event management (SIEM).
- SimpleRisk: For fully integrated Governance, Risk Management and Compliance GRC platform
- Palo Alto Networks Cortex XDR: For security analytics and threat detection.
- AWS Inspector/Microsoft Wiz/Nmap: For vulnerability scanning.

Identity and Access Management:
- Okta: For identity management and single sign-on (SSO)
- Microsoft Active Directory: For managing user accounts and permissions.

Network Security:
- Palo Alto Networks: For firewall and network security.
- GlobalProtect: For advanced firewall protection and VPN services endpoints.

Endpoint Protection:
- Palo Alto Networks Cortex XDR: For antivirus and endpoint detection and response (EDR) security.

Backup and Recovery:
- AWS Storage Gateway: For data backup and disaster recovery.
- SolarWinds: For data protection and management.

Configuration Management:
- Jenkins: For continuous integration (CI) tool for building and testing software projects.
- Ansible: For automating configuration management and deployment.
- Puppet: For managing system configurations.

Monitoring and Management:
- Nagios: For system and network monitoring.
- SolarWinds: For IT infrastructure monitoring.
- PRTG: For Network Monitoring

Database Security:
- Oracle Database Vault: For securing database environments.
- Microsoft SQL Server Management Studio: For managing databases

Inventory and Deployment Management:
- PDQ Inventory: For managing and auditing software and hardware inventory.
- PDQ Deploy: For automating software deployment across multiple systems.

3. Development Tools

As a Systems Security Administrator at Spring Financial, I interacted with various development tools, ensuring they are secure and compliant with security policies. Here are some key development tools I worked with:

Version Control:
- Git: For source code management and version control.
- GitHub/GitLab/Bitbucket: Platforms for hosting and managing Git repositories.

Continuous Integration/Continuous Deployment (CI/CD):
- Jenkins: For automating the build, test, and deployment processes.
- CircleCI: For CI/CD automation.
- Travis CI: For continuous integration and delivery.

Containerization:
- Docker: For containerizing applications and services.
- Kubernetes: For orchestrating containerized applications.

Configuration Management:
- Ansible: For automating IT configuration management and deployment.
- Puppet: For managing infrastructure as code.

Code Quality and Security:
- SonarQube: For continuous inspection of code quality.
- Checkmarx: For static application security testing (SAST).
- Veracode: For securing software through automated vulnerability testing.

Integrated Development Environments (IDEs):
- Visual Studio Code: A widely used code editor for various programming languages.
- IntelliJ IDEA: For Java development and other languages.

Collaboration and Project Management:
- Jira: For project tracking and issue management.
- Confluence: For team collaboration and documentation.
- Trello: For task management and project planning.

Testing:
- Selenium: For automated testing of web applications.
- JUnit: For unit testing Java applications.

Scripting and Command-Line Tools:
- PowerShell: For task automation and configuration management on Windows.
- Bash Scripts: For automating tasks and managing configurations on Linux/Unix systems.
- CMD Windows Command: For Managing and configuring Windows environments
- Linux Commands: For managing and configuring Linux environments