Position #NEW
IS Technical Services Specialist
Security Analyst
DMS/BISM

POSITION SUMMARY

Working under the general review of the Chief Information Security Officer (CISO) in the Bureau of Information Security Management (BISM) this position provides the Department of Employee Trust Funds (ETF) with professional-level IS work including; technical design, implementation, maintenance, and ongoing operation of security controls for all aspects of ETF's information technology enterprise, such as applications, endpoints, sensitive data and including those systems and services hosted by the Wisconsin Department of Administration (DOA) Department of Enterprise Technology (DET) such as network and servers.

This position assists the BISM Team Lead to ensure that ETF successfully manages information security risk with its technical initiatives, tools, and processes. To that end, the incumbent provides advanced technical support in the development and implementation of security controls designed to support ETF's information security strategy and applies comprehensive knowledge to technical security projects for the development, testing and implementation of major platforms in the ETF application portfolio.

This position requires strong oral and written communication skills, advanced information security (INFOSEC) knowledge in: network security, information system design, computer application design and operation, active directory, penetration testing methodologies and exploitation mitigation techniques. This position should have mastery of common administrative tools in Windows and Linux and working knowledge of penetration tools and techniques. This position independently resolves conflicts and problems through the skilled application of theoretical and practical knowledge of information security best practices as well as the application of ETF policies and standards.

The incumbent performs security administration tasks, as directed. The incumbent may also serve as a BISM representative at committees, meetings, and other forums.

Goals and Worker Activities

35% GOAL A. Mitigation and remediation of hardware, software, and framework vulnerabilities

A1. Analyze network configuration and monitor Security Event and Incident Management (SIEM) and tools to ensure only approved devices and software have presence on ETF local and remote VPN network.

A2. Work with Security + Operations (SecOps) BISM staff to ensure hardware patching and software version are kept current for all network infrastructure.

A3. Collaborate with DET to harden network infrastructure and create secure network segments that limit the ability for malicious code to laterally spread from endpoint to endpoint within our network.

A4. Perform technical reconnaissance of all network segments, using common hacking tools available in Kali Linux, on software versions, open ports, and services to determine a point of attack. Lead the technical efforts in closing holes that exist.

A5. Routinely conduct vulnerability assessments on network infrastructure. Rate-risk vulnerabilities and advise other IS staff and leadership through remediation and risk mitigation tactics.

A6. Assist in the development standard operational procedures addressing the cyber security practices of common processes, infrastructure setup, admin, and service account privileges.

A7. Maintain installed enterprise security (Endpoint Detect and Response tools, QRADAR, Z Scaler, NXLog, or similar) systems on an ongoing basis while maintaining system stability.

A8. Contribute to the development of information security-related strategic, tactical and operational plans.

35% GOAL B. Detection and analyzation of anomalies and threats

B1. Monitor enterprise security tools and investigate alarms. Lead in the investigative efforts to determine root cause for the alarm. Determined the most appropriate course of action; dismiss or tune the alarm or risk mitigation efforts.

B2. Configure and tune Security Event and Incident Management (SEIM) software to alarm on network anomalies found by deep packet inspections (port mismatching, viruses, spam, protocol non-compliance, poor reputation score, etc.).

B3. Establish a standard operating procedure for case and incident reporting and handling; account for the incident lifecycle (logs, events, alarms/alerts, cases, and incidents)

B4. Institute active security defenses throughout the organization. Utilize honey pots, honey ports, honey documents as tripwires that will alarm and provide details information to assist in attribution and threat intelligence gathering.

B5. Stay current on emerging threats and industry trends. Subscribe to and read INFOSEC whitepapers, blogs, intelligence feeds from Whitehat and Blackhat sources.

15% GOAL C. Investigation, response, and resolution of incidents

C1. Actively monitor ETF data networks to identify probable source of problem.

C2. Communicate incident detail with BISM leadership immediately. Escalate incident details to WSIC, FBI, DET and vendor contacts as directed.

C3. Work with sys admins, other BISM staff, and vendors to capture forensic data, analyze, perform diagnostics and attempt to resolve the incident.

C4. Isolate infected hosts and bring up systems at COOP location as operational needs dictate.

C5. Prepare incident report capturing pertinent incident details to communicate out to ETF leadership.

10% GOAL D. Development, implementation and maintenance of information security standards and procedures

D1. Collaborate with Bureau of Information Technology Services (BITS) personnel to ensure BITS operations comply with security principles, policy, standards, and procedures.

D2. Collaborate with internal and external stakeholders, to develop and implement standards, procedures and technology that supports ETF's information security strategy.

D3. Develop and perform information security-related procedures for continuous monitoring of ETF's business applications.

D4. Collaborate with the ETF Office of Communications to ensure quality information security-related messaging to the ETF user community and other relevant stakeholders.

5% GOAL E. Performance of miscellaneous duties related to standards, communications, and special assignments

E1. Work with other BITS staff on new and developing technologies and their impact on agency system security.
E2. Read books and periodicals to improve knowledge of information security and system design principles.
E3. Attend training sessions and workshops to increase knowledge of information security.
E4. Read security reports published by various public and private organizations, to stay current on newly discovered computer security vulnerabilities.
E5. Maintain knowledge and an ongoing awareness of Department values. Actively embrace the Department's values and fully incorporate them into the way you approach your tasks and perform your job.
E6. Carry out special assignments as directed.

(Dev. 11/04/2021)

KNOWLEDGE, SKILLS, and ABILITIES

KNOWLEDGE OF:

1. Information security control framework theory
2. Individual security controls as outlined in the CIS Top 20 or equivalent framework
3. Common adversary tactics, techniques, and procedures in assigned area of responsibility
4. Different classes of attacks (e.g., passive, active, insider, close-in, distribution, etc.)
5. General attack stages (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks, etc.) MITRE ATT&CK Framework
6. New and emerging IT and information security technologies
7. Application vulnerabilities
8. Linux command line (e.g., mkdir, mv, ls, passwd, grep, etc.)
9. Hacking methodologies in Windows or Unix/Linux environment (metasploit)

SKILLED IN:

10. Information system security-related planning, selection, implementation, and documentation processes and best practices
11. Information technology training methods and techniques
12. Communication of technical information effectively, either orally or in writing, to technical and non-technical users, technical teams, and senior management
13. Use of information technology operating systems
14. Coordinating and providing expertise related to the security and maintenance of network infrastructure
15. Analyzing problems and developing solutions
16. Working independently or collaboratively with a variety of persons at technical and non-technical peer, consultant, and manager levels
17. Coordinating or leading the work of IT professionals or project teams
18. Providing expertise and problem resolution across multiple platforms and software
19. Conducting vulnerability scans and recognizing vulnerabilities in security systems
20. Performing packet-level analysis (e.g., Wireshark, tcpdump, etc.)
21. Network mapping and recreating network topologies

ABILITY TO:

22. Perform advanced work on security controls, with immediate impact or potential impact on ETF systems
23. Coordinate the delivery of ETF security services to customers
24. Coordinate and lead teams in planning and implementation of security controls, including testing and roll-back planning
25. Provide technical direction for security systems and supporting technologies across multiple platforms
26. Develop comprehensive operational procedures for documented, consistent use of security controls
27. Work with end-users to remediate compliance issues related to security policies and practices
28. Operate vulnerability scanning tools such as Qualys, Nessus, or equivalent
29. Operate SIEM tools such as QRadar, Splunk, SolarWinds LEM, or equivalent
30. Operate anti-malware tools such as Symantec, Norton, McAfee, or equivalent
31. Operate web filter tools such as ZScaler, Forcepoint, Bluecoat, or equivalent

SPECIAL REQUIREMENT:

Due to the nature of this position, some non-standard work hours may be required.