Position # 512320
IS Technical Services Specialist
Division of Technology, Security & Data Services
Bureau of Information Security Management

POSITION SUMMARY

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 the technical design, implementation, maintenance, and ongoing operation of security controls for all aspects of ETF's information technology enterprise. This includes applications, endpoints, sensitive data, as well as 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 cybersecurity 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 cybersecurity strategy. This position applies comprehensive knowledge to technical security projects for the development, testing, and implementation of major platforms in the ETF application portfolio.

This position independently resolves problems through the implementation of information security best practices and the application of ETF policies and standards. This position performs security administration tasks, as directed. The incumbent may also serve as a BISM representative at committees, meetings, and other forums.

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.

ETF is a medium sized, non-shared services agency administering the Wisconsin Retirement System and related benefit programs to over 630,000 members receiving $5.6 billion in retirement benefits and $1.6 billion in health benefits annually. This position directly supports the agency strategic goal focused on building a talented and agile workforce necessary for achieving the department's mission to develop and deliver quality benefits and services to our members while safeguarding the integrity of the Trust. As an employee of ETF, the incumbent will support and create a diverse and inclusive work force.

GOALS AND WORKER ACTIVITIES

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

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

A2. Work with Security + Operations (SecOps) BISM staff to ensure hardware patching and software versioning 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, software versions, open ports, and services to determine a point of attack. Lead technical efforts in closing the 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. Maintain installed enterprise security systems (e.g., Endpoint Detect and Response tools, SIEM, Web Filtering, Log Aggregators, etc.) on an ongoing basis while ensuring system stability.
A7. 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 investigative efforts to determine the root cause for the alarm. Determine the most appropriate course of action; dismiss or tune the alarm or perform risk mitigation efforts.
B2. Configure and tune SIEM software to alarm on network anomalies found by deep packet inspections (e.g., 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, and honey documents as tripwires that will alarm and provide detailed information to assist in attribution and threat intelligence gathering.

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 system administrators, other BISM staff, and vendors to capture and analyze forensic data, 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.

D5. Assist in the development and implementation of standard operational procedures addressing cybersecurity practices, common processes, infrastructure setup, admin, and service account privileges.

5% GOAL E. Performance of miscellaneous duties and special assignments

E1. Work with other BITS staff on new and developing technologies and their impact on agency system security.
E2. Read articles and other resources and attend training sessions and workshops to increase knowledge of information security and system design principles.
E3. Read security reports published by various public and private organizations to stay current on newly discovered computer security vulnerabilities.
E4. 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.
E5. Stay current on emerging threats and industry trends. Subscribe to and read INFOSEC whitepapers, blogs, intelligence feeds from Whitehat and Blackhat sources.
E6. Carry out special assignments as directed.

(Revised 1/2024)

KNOWLEDGE, SKILLS, AND ABILITIES

KNOWLEDGE OF:

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

SKILLED IN:

11. Performing cybersecurity functions (e.g., detection, validation, remediation, analysis, implementing security controls, etc.)
12. Developing, implementing, and documenting information security processes and best practices
13. Communicating technical information effectively, either orally or in writing, to technical and non-technical users, technical teams, and senior management
14. Use of information technology operating systems
15. Analyzing problems and developing solutions. Providing expertise and problem resolution across multiple platforms and software.
16. Working independently and collaboratively with a variety of persons at technical and non-technical peer, consultant, and manager levels
17. Conducting vulnerability scans and recognizing vulnerabilities in security systems using scanning tools such as Qualys, Nessus, or equivalent
18. Performing packet-level analysis (e.g., Wireshark, tcpdump, etc.)
19. Network mapping and recreating network topologies

ABILITY TO:

20. Implement security controls with immediate impact or potential impact on ETF systems
21. Coordinate the delivery of security services to customers
22. Coordinate and lead teams in the planning and implementation of security controls, including testing and roll-back planning
23. Provide technical direction to security teams on security systems and supporting technologies across multiple platforms
24. Work with end-users to remediate compliance issues related to security policies and practices
25. Operate SIEM tools such as QRadar, Splunk, SolarWinds LEM, Elastic, or equivalent
26. Operate anti-malware tools such as Symantec, Norton, McAfee, or equivalent
27. Operate web filter tools such as ZScaler, Forcepoint, Bluecoat, or equivalent
28. Operate Endpoint Detect and Response tools such as CrowdStrike
29. Collaborate with cross-functional teams on the planning and implementation of security controls
30. Understand and comply with all ETF and enterprise security standards, policies, processes, and procedures.
31. Maintain confidential information in accordance with policies, guidelines, and direction from manager.

SPECIAL REQUIREMENT:

On very rare occasions, some non-standard work hours may be required as security events arise.