UW HEALTH JOB DESCRIPTION

IS Cybersecurity Engineer Principal

Job Code: 340026	**FLSA Status: Exempt**	**Mgt. Approval: E. Thiesenhusen**	**Date: March 2022**
Department: 1007422 IS - Risk & Compliance		**HR Approval: N. Lazaro**	**Date: March 2022**

JOB SUMMARY

The UW Health Cybersecurity Engineer Principal is the guardians of all enterprise data, including data subject to the HIPAA Security Rule, and other sensitive or restricted electronic information, for which UW Health is the custodian. The Cybersecurity Engineer is responsible for the confidentiality, integrity, and availability of the network and systems that store data.

The Principal Cybersecurity Engineer independently maintains and troubleshoots a variety of technologies, cybersecurity problems, and network issues. The Principal Cybersecurity Engineer has a wealth of knowledge across many of the technologies in the security domain, as well as being a member of a team that supports deterrent, detective, and responsive systems. Some of these technologies include vulnerability assessment, security information and event management (SIEM), cloud security tools, encryption, identity access management and identity governance (IAM/IG), endpoint detection and response (EDR), URL filtering, firewall security controls, intrusion detection and prevention systems (IDS/IPS), and modern/mobile device management (MDM). The Principal Cybersecurity Engineer participates in the design and building of Zero Trust environments, incident response, disaster recovery and business continuity.

The Principal Cybersecurity Engineer independently leads the proposal, development, deployment and support of highly complex, enterprise class solutions consistent with established security best practices, and corporate values and standards. The Principal Cybersecurity Engineer leads the development and implementation of new procedures and mentors and teaches less experienced Cybersecurity Engineers along with others throughout UW Health. The Principal Cybersecurity Engineer develops and leads large-scale projects, maintains organizational-level responsibilities, and collaborates with employees and leaders across UW Health, the UW School of Medicine and Public Health, and our partners and affiliates.

MAJOR RESPONSIBILITIES

- Evaluates, leads, plans, and implements security technologies for the protection of UW Health's data, systems, and infrastructure.
- Champions cybersecurity technologies, practices, processes, techniques, risks, and trends to UW Health based on industry research.
- Leads evaluation of modern technologies and ongoing risk assessments.
- Ensures that the organization's data and infrastructure are protected by researching, recommending, and enabling security controls.
- Troubleshoots complex cybersecurity and network problems in collaboration with other Information Systems teams and stakeholders.
- Responds to system and/or network security incidents in collaboration with a managed security services provider. Actively participates in efforts to contain and remediate breaches along with preventing future breaches.
- Follows change management process when designing, implementing, and updating security controls.
- Tests and identifies network and system weaknesses through vulnerability scanners, penetration testing, and other methodology.
- Guides owners on remediation strategies to better protect and secure their systems.
- Completes daily standard work, reporting, and communication as needed to maintain operations and security technologies.
- Acts as the subject matter expert for many topics and technologies in the security domain, while maintaining working knowledge of other technologies supported by the cybersecurity team for cross coverage while on call.
- Evaluates organizational security needs and establishes standards and best practices accordingly.
- Provides security advice to other teams and departments throughout UW Health.
- Actively participates and contributes to the planning of the organizational Information Security strategy.
- Takes part in a 24x7 on-call rotation 365 days a year to assure ongoing operations and security for a facility that operates continuously to provide the best possible care to the patients we serve.
- Mentors and teaches, formally and informally, less experienced Cybersecurity Engineers in addition to other IS colleagues and UW Health staff and affiliates on relevant cybersecurity topics.

ALL DUTIES AND REQUIREMENTS MUST BE PERFORMED CONSISTENT WITH THE UW HEALTH PERFORMANCE STANDARDS.

JOB REQUIREMENTS

Education	Minimum	Associate Degree in Healthcare, Information Technology, Business, or related field (2 years of relevant experience may be considered in lieu of degree in addition to experience below)

	Preferred	Bachelor's or Master's degree in Computer Science, Information Systems, Healthcare, Cybersecurity, Information Technology, Engineering, Business, or related field strongly preferred.
Work Experience	Minimum	Demonstrated success leading the use and implementation of vulnerability scanners, SIEM, cloud security tools, identity access management systems, encryption technologies, firewall management, IDS/IPS, URL filtering, or endpoint detection and response tools. Demonstrated success leading the assessment, testing, and implementation of enterprise grade security systems and controls Demonstrated success mentoring and teaching others on cybersecurity protocols and topics. Demonstrated success leading enterprise projects and processes
	Preferred	15 or more years of progressively responsible experience in a healthcare setting, using technologies such as Microsoft 365, Azure Cloud, Active Directory, Cisco and Palo Alto Product Lines, VPN, Intrusion Prevention, Detection and Response, IAM & IG, PAM, LogRhythm/SIEM, Federation/SAML, or Qualys/Vulnerability Management.
Licenses & Certifications	Minimum	None.
	Preferred	Advanced certifications such as CISSP, CEH, CISM, CISA, CRISC, CCSP, and/or specific training and certification in Cloud, Microsoft 365, SIEM, MDM, Federation, IAM & IG, PAM, or other information security specialty.
Required Skills, Knowledge, and Abilities		Advanced competency in the following areas: • Leadership including leads with integrity, maintains strategic orientation, demonstrates business & financial acumen, champions innovation, manages execution, leads & develops people • Technical leadership of applicable products or platforms • Leading without direct authority • Communication • Effective team member • Critical thinking • Mentoring and teaching • Organizational Awareness / Understanding • Technology Awareness & Strategic Planning • Security infrastructure, including three or more Firewalls, VPN, Data Loss Prevention, IDS/IPS, URL filtering, Security Audits, SIEM, endpoint detection and response, federation, vulnerability management Intermediate competency in the following areas: • Leading highly empowered, self-directed teams including cross-functional teams • Applying lean management tools • Applying agile methodologies Advanced competency in two of the following areas: • Application Security • Enterprise Security, Privacy, & Info Sharing • Identity Management • Legal, Government, and Compliance • Threat Analysis Other Knowledge, Skills and Abilities • Ability to analyze data and information with a wide-ranging understanding of cybersecurity methodologies. • Meticulous attention to detail • Outstanding problem-solving skills • Ability to work comfortably under pressure and deliver on tight deadlines • Effectively handle changes in direction and provide guidance and support to the rest of the team

PHYSICAL REQUIREMENTS

Indicate the appropriate physical requirements of this job in the course of a shift. *Note: reasonable accommodations may be made available for individuals with disabilities to perform the essential functions of this position.*

UW HEALTH JOB DESCRIPTION

	Physical Demand Level	Occasional Up to 33% of the time	Frequent 34%-66% of the time	Constant 67%-100% of the time
X	**Sedentary:** Ability to lift up to 10 pounds maximum and occasionally lifting and/or carrying such articles as dockets, ledgers and small tools. Although a sedentary job is defined as one, which involves sitting, a certain amount of walking and standing is often necessary in carrying out job duties. Jobs are sedentary if walking and standing are required only occasionally and other sedentary criteria are met.	**Up to 10#**	**Negligible**	**Negligible**
	Light: Ability to lift up to 20 pounds maximum with frequent lifting and/or carrying of objects weighing up to 10 pounds. Even though the weight lifted may only be a negligible amount, a job is in this category when it requires walking or standing to a significant degree.	**Up to 20#**	**Up to 10#** or requires significant walking or standing, or requires pushing/pulling of arm/leg controls	**Negligible** or constant push/pull of items of negligible weight
	Medium: Ability to lift up to 50 pounds maximum with frequent lifting/and or carrying objects weighing up to 25 pounds.	**20-50#**	**10-25#**	**Negligible-10#**
	Heavy: Ability to lift up to 100 pounds maximum with frequent lifting and/or carrying objects weighing up to 50 pounds.	**50-100#**	**25-50#**	**10-20#**
	Very Heavy: Ability to lift over 100 pounds with frequent lifting and/or carrying objects weighing over 50 pounds.	**Over 100#**	**Over 50#**	**Over 20#**
List any other physical requirements or bona fide occupational qualifications:				

Work/Environmental: Moderate noise level consistent with an office environment