JOB DESCRIPTION

Job Title: Cybersecurity Specialist
Job Level: Senior / Specialist
Department: IT
Position Type: Full-time
Job Location: Hybrid
Reports To: CEO
Supervisory Responsibilities: IT

Job Summary:
The Cybersecurity Specialist's purpose is to protect the confidentiality, integrity, and availability of sensitive information, systems, and data. The Cybersecurity Specialist shall employ technologies, processes, structures, and practices to protect PayCare Limited's networks, computers, programs, and data from unauthorized access or damages. The Cybersecurity Specialist must ensure secure storage, control access, and prevent unauthorized processing, transfer, or deletion of data.

Job Focus:
The Cybersecurity Specialist (CSS) is entrusted with the duties of security intelligence that include identifying, protecting, detecting, responding, and recovering systems, data, and information in increasing PayCare Limited's resilience to cyberthreats, attacks, and vulnerabilities. The Cybersecurity Specialist shall monitor systems and networks for attacks, intrusions, and vulnerabilities. Implements security audits across computer hardware and software systems. The CSS recommends hardware and software solutions necessary in reducing risks. The CSS creates and updates security processes, systems, and policies. The CSS trains employees in security procedures and best practices, and ensures security standards are met and up-to-date. The CSS supports PayCare Limited in adhering to security regulatory requirements.

Job Duties and Responsibilities:

- **Threat Protection:** Protect the organization's systems and networks from cyber threats by implementing security measures and protocols.
- **Risk Assessment:** Conduct regular risk assessments and security audits to identify vulnerabilities and recommend remediation strategies.
- **Security Protocol Implementation:** Implement security protocols such as firewalls, intrusion detection systems, and encryption to safeguard sensitive data and systems.
- **Incident Response:** Respond to security incidents, investigating breaches, and coordinating response efforts to mitigate risks and prevent future occurrences.

- **Compliance Management:** Ensure compliance with industry standards and regulations (such as GDPR, PCI DSS) by regularly reviewing policies and procedures.
- **Training and Awareness:** Conduct security awareness training for employees to educate them on best practices and emerging threats, fostering a culture of security.
- **Collaboration with IT Teams:** Collaborate with IT and development teams to integrate security measures into the development lifecycle, ensuring secure application deployment.

Expected Outcomes:

- The CSS must ensure the readiness of PayCare Limited against cyber incidents and attacks.
    - Accurate and on-time detection of risks, threats, and vulnerabilities.
    - Zero number of outdated devices or non-fully patched devices.
- The number of security incidents; the number of times hackers attempted to gain access or breached PayCare Limited's network should be Zero or a minimum of **5 over 12 months**.
- Minimum **10** number of intrusion attempts over **6 months**; (the intensity and frequency of cyber threats; efficient implementation of threat detection/prevention systems, and proactive identification and detection of various attack vectors), **20** number of reviews of firewall logs to see if anyone has unauthorized access to the network.
- There shall be **zero** incorrectly configured SSL Certificates.
- The CSS shall detect a threat or data breach within **30 minutes** (Mean Time to Detect).
- The CSS shall respond to a known cyberthreat within **1 hour** (Mean Time to Resolve).
- The CSS shall close or contain an identified attack vector across all PayCare's endpoints within **2 hours** (Mean time to contain).
- The CSS shall recover products or systems after a failure within **12 hours** (mean time to recover).
- The number of vulnerabilities in PayCare Limited's system (patching cadence) should be zero or a minimum of **2 over 6 months**.
- The cost per incident should be a minimum of **$5,000**; the cost of responding to and resolving a cyberattack (the cost per incident covers employee overtime, reduction of employee productivity, suspension of specific activities, potential loss of communication with customers, system downtime, and the cost of investigating the attack).
- The CSS must prevent malware and botnets that can breach the firewall and security systems by tracking the volume of data transferred via PayCare's network **5 times over 6 months**.
- The CSS must implement effective security audits that lead to the identification of vulnerabilities and recommendations for improvements.
- The CSS shall ensure the reliability and durability of PayCare's cybersecurity systems; the Mean Time Between Failure (the average time a system or component operates before failing shall be **6 months** or zero).
- The CSS shall conduct a profound risk assessment **4 times over 12 months** that results in identifying, assessing, and prioritizing potential threats and vulnerabilities, and informed decision-making about security measures.
- The CSS must implement cloud security best practices and monitoring of potential risks.

- The CSS shall demonstrate ethical performance in security processes, e.g., obtaining proper authorization, respecting privacy, maintaining confidentiality, responsible disclosure of findings, and avoiding harm to individuals and organizations.
- The CSS shall ensure timely and up-to-date compliance with international data protection laws.
- The CSS shall update security policies **3 times over 12 months**.
- The CSS shall train employees in security policies and compliance **2 times over 6 months**.

Quantifiable metrics or milestones (daily/weekly/monthly/percentage/ratio?) to be provided for gauging success in meeting these expectations.

Required Knowledge:

- **Threat Protection:** Proven experience in implementing security measures and protocols to protect systems and networks. Familiarity with security frameworks (e.g., NIST, CIS).
- **Risk Assessment:** Experience conducting risk assessments and security audits to identify vulnerabilities.
- **Security Protocol Implementation:** Strong knowledge of firewalls, intrusion detection systems, and encryption methods. Experience with SIEM tools for threat detection and response.
- **Incident Response:** Experience in investigating security incidents and coordinating response efforts.
- **Compliance Management:** Knowledge of industry regulations (e.g., GDPR, PCI DSS) and ensuring compliance through regular reviews.
- **Training and Awareness:** Experience in conducting security awareness training for employees.
- **Collaboration with IT Teams:** Ability to work with IT and development teams to integrate security into the development lifecycle.

Education:

- Bachelor's Degree in Cybersecurity, Information Technology, Computer Science, or a related field.
- Master's Degree (optional) in a relevant field (e.g., Cybersecurity, Information Assurance, or Computer Science).
- Additional Training (Optional): Certifications in cybersecurity (e.g., CISSP, CISM, CompTIA Security+) or specialized training in security tools and practices can be beneficial.

Required Competencies (Skills and Abilities):

Technical Skills:

- Domain Name System (DNS) monitoring, Cryptographic Principles (Asymmetric and Symmetric Encryption), Patch Deployment, Rate Limiting, Load Balancing, IP Blacklisting, Parameterized Queries, Parameter Security, Network Segmentation, and Message Authentication Code (MAC).

Technologies/Software:

- Firewalls (Next-generation firewalls, web application firewalls, etc.), Wi-Fi Protected Access 3, and Honeypots.

Methodologies:

- ISO 27001/27002 and Security Information and Event Management System (SIEM).

Programming Languages and Frameworks:

- Java, JavaScript, C++, Python, HTML5, SQL, and Elixir.

Security Tools and Platforms:

- VPN, Intrusion Detection Systems (IDS) e.g., network-based (NIDS) and host-based (HIDS) systems, Intrusion Prevention Systems (IPS), Vulnerability Scanner, Project Management Tools (e.g., Jira, etc.).

Security Management:

- DDoS Protection, e.g., LevelBlue, etc.

Protocols:

- Strong Encryption (e.g., Secure Sockets Layer, Transport Layer Security, etc.), HTTPS, and Wireless Security Protocols.

Behavioral Competencies:

Transferable Skills:

- **Analytical Skills:** Strong analytical skills for assessing security risks and developing effective mitigation strategies.
- **Communication Skills:** Ability to communicate complex security concepts to nontechnical stakeholders clearly and concisely.
- **Attention to Detail:** Vigilance in identifying potential threats and vulnerabilities within systems and networks.
- **Problem-Solving Skills:** Strong problem-solving abilities to address and resolve security incidents effectively.
- **Team Collaboration:** Ability to collaborate with IT and development teams to integrate security measures throughout the development lifecycle.
- **Continuous Learning:** Commitment to staying updated on the latest cybersecurity trends, threats, and technologies.

What is Your Salary Expectation? Please state your salary expectations in figures:

1. _____ Per Annum
2. _____ Per Month

Apply Now:

To apply, click the Link: https://paycaretech.world/application-form

Thank you for your interest in PayCare, and good luck!
