



IS SECURITY ANALYST

DEPARTMENT:	Information Systems	REPORTS TO:	Global IS Security Manager
DIVISION:	Corporate	FLSA STATUS:	Exempt
JOB CODE:	2345	EFFECTIVE DATE:	10/14/2024

JOB SUMMARY

Protect, monitor, and maintain the Pyrotek Information System (IS) network security system. Investigate security incidents and implement robust security measures. Partner with the IS Global Security Manager to ensure compliance with regulatory standards.

QUALIFICATIONS

Education/Experience

Bachelor's Degree in Information Systems, Computer Science, or related field; plus, a minimum of five (5) years of experience in system security; or equivalent combination of education and related experience.

Certified Information Systems Security Professional (CISSP), CompTIA Security+, and other relevant security certifications preferred.

Knowledge/Skills/Abilities

IS Security. Knowledge of IS security principles, best practices and tools used to protect data and systems. Demonstrated ability to identify security threats, mitigate IS risks and ensure compliance with security standards.

Core People Skills. Ability to positively interact and work collaboratively with a diverse group of people at all levels of the organization. Genuine with high ethical standards and values and personal integrity and honesty. Ability to apply a large measure of common sense to a variety of situations.

Communication Skills. Ability to speak clearly and persuasively in positive or negative situations, listen and obtain clarification, and respond well to questions. Proficiency in writing clearly and concisely and editing work for spelling and grammar. Ability to vary writing style to meet business needs.

Computer/Applications Skills. Proficient in Windows server and desktop operating systems and Microsoft 365 product applications. Working knowledge of Internet Protocol (IP), Transmission Control Protocol (TCP/IP), and other network administration protocols. Working knowledge of firewalls and secure network access platforms/solutions. Experience with Fortigate firewall, Aruba Clearpass and Sophos a plus.

Core Business Skills. Ability to exercise sound judgement and discretion in handling of proprietary and confidential information. Ability to work independently, without significant direction and to use resources effectively to "figure it out". Strong critical thinking skills, judgment and keen attention to detail and accuracy. Exceptional prioritization, time management and organizational skills. Ability to write routine reports and correspondence.

Professional Investment. Demonstrated commitment to own personal professional development and learning.

Travel. Ability to travel by land and air, both domestic and international, up to 10%. Valid driver's license and US passport or ability to obtain.



ESSENTIAL FUNCTIONS/RESPONSIBILITIES

1. Actively monitor the IS security network for threats and vulnerabilities, ensuring prompt action against any potential breaches through these functions:
 - a. Monitor security and data using Security Information and Event Management (SIEM) tools to analyze security events and identify patterns.
 - b. Analyze security events and identify suspicious activities that could compromise the organization.
 - c. Respond to incidents, investigate security breaches, determine root causes, and implement corrective actions to prevent future occurrences.
2. Effectively implement and maintain robust security measures to safeguard data and systems, while ensuring compliance with regulatory standards to include, but not limited to:
 - a. Plan, configure, and maintain security tools such as firewalls, intrusion detection systems, and encryption technologies.
 - b. Develop, enforce, and regularly update security policies and procedures to ensure data protection.
 - c. Ensure compliance with security frameworks such as, National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO 27001) through regular audits, assessments, and updates to security practices.
3. Regularly promote security best practices and implement measures to prevent data loss and maintain data integrity. Collaborate with the IS team and other departments to integrate and promote security best practices. Implement data loss prevention (DLP) strategies to safeguard sensitive information.
4. Stay current on emerging security threats, trends, and technologies to improve defense strategies. Prepare detailed reports on security incidents, findings and actions taken. Maintain accurate documentation for audits and compliances purposes.
5. Promote positive team member and customer relations by supporting Pyrotek's commitment to a working environment of tolerance, acceptance, and civility. Respond appropriately to inquiries, concerns, and complaints by being professional, courteous, and respectful at all times.
6. Maintain regular, consistent, reliable, punctual, and predictable attendance, as required to achieve internal and external customer satisfaction.
7. Actively and positively participate in problem resolution, demonstrating constructive communication, timely response, and effective resolution skills. Work effectively within team environments both within your department and across the organization.
8. Cooperate and comply fully with all Pyrotek policies and procedures. Actively support and follow the Pyrotek Safety Program.
9. Participate in company/department meetings, training activities, continuing education programs and other associated activities.
10. Consistently promote and communicate Pyrotek's core values through work performance and excellent customer service.
11. Perform other tasks as assigned.

PHYSICAL/SENSORY REQUIREMENTS

Must be able to sit for long periods-of-time, bend, and reach, use stairs, lift up to 25 pounds occasionally and communicate effectively in English by telephone, in person and in writing. Effectively use a personal computer, office equipment and telephone.



WORKING ENVIRONMENT

While performing the essential responsibilities of this position, team member generally will work in an office environment.

Team Member's Signature

Date

Manager's Signature

Date