CareerCross by JAC Recruitment

PR/117183 | IT Security Infrastructure

Job Information

Recruiter
JAC Recruitment Thailand

Job ID
1540356

Industry
Other (Manufacturing)

Job Type
Permanent Full-time

Location
Thailand

Salary
Negotiable, based on experience

Refreshed
June 18th, 2025 07:00

General Requirements

Minimum Experience Level
Over 3 years

Career Level
Mid Career

Minimum English Level
Business Level

Minimum Japanese Level
Business Level

Minimum Education Level
Associate Degree/Diploma

Visa Status
No permission to work in Japan required

Job Description

Position: IT Security Infrastructure

Location: Amata city, Chonburi

Salary Package: 40,000 - 45,000 (Bonus 5-6 mths)

Working day: Monday to Friday

Job Description

- Configure and maintain network security controls, including access rules, firewall policies, and segmentation, adhering to best practices.
- Configure and maintain secure settings for virtual machines and other cloud services, following best practices.
- Provide recommendations to the team for the secure design of applications and/or solutions.
- Collaborate with infrastructure and cybersecurity teams to plan and execute patch management across operating

systems, applications, and network devices.
- Provide support for internal and external audits regarding IT security measure performance.
- Provide timely updates on incident status, escalate when necessary, and ensure remediation efforts.
- Coordinate with the relevant teams to detect, investigate, and resolve security incidents.
- Handle cyber-attack and malicious activity detection.
- Ensure the detection, analysis, and combating of advanced and emerging threats, including identifying vulnerabilities and mitigating associated cybersecurity risks proactively.
- Proactively search for cyber threats and risks within data before attacks occur.
- Gather comprehensive information on threat behavior, goals, and methods.
- Organize and analyze collected data to identify trends in the organization's security environment.
- Make predictions for future threats and eliminate current vulnerabilities.
- Perform Security Incident Handling procedures.
- Manage and define proactive rules for the cyber defense perimeter and endpoint security, including WAF, IPS, Anti-DDoS, Anti-Phishing, and other security controls.

Qualifications

- Bachelor’s degree in Computer Engineering, Computer Science, Information Security, or a related engineering discipline, or equivalent practical experience.
- A minimum of 3 years of experience in cybersecurity or a similar field.
- Hands-on experience with security tools (e.g., firewalls, WAF, SIEM, EDR), patch management processes, and incident response procedures.
- Strong understanding of network protocols, firewall configurations, and vulnerability management principles.
- Excellent analytical and problem-solving skills with the ability to quickly adapt to changing priorities.
- Ability to work effectively under pressure, demonstrating diligence and patience.
- Security certifications are considered a plus.
- A strong enthusiasm for staying current with emerging cybersecurity technologies and practices.

Company Description