japannexts JNXS

Senior Security Engineer

Location

Tokyo, Japan

About us

Established as the premier Proprietary Trading System (PTS), Japannexts Co., Ltd. stands at the forefront of Japan's trading infrastructure landscape. Our cutting-edge matching engine delivers a low-latency, high-capacity trading platform that ensures stability and reliability, distinguishing us as the industry leader. Our comprehensive suite of services extends beyond trading, encompassing IT solutions such as Smart Order Routing (SOR), proficient data center management, and top-tier co-location services.

Central to our operation is a diverse team of English-speaking IT enthusiasts from over 30 countries. Our collaborative spirit is fostered under the guidance of experienced professionals in the FinTech sector. As we embark on thrilling new ventures, we are eagerly seeking individuals of exceptional talent to add their expertise to our innovative and forward-thinking team.

Your role

You will monitor and respond to security alerts, perform triage and investigations, manage client tickets, collaborate with teams on incident response, and engage in security projects. You will stay updated on emerging threats, conduct risk assessments, and implement security strategies to protect systems and data. As a key leader and technical focal point for security solutions, you will provide strategic guidance, mentorship, and direction to team members ensuring our security posture remains robust and aligned with industry standards. Strong communication, teamwork, and problem-solving skills are essential for success in this role.

Responsibilities:

- Monitor the SIEM/SOAR platform and respond promptly to suspicious or abnormal alerts.
- Perform initial triage and investigation of alerts, documenting findings appropriately.
- Utilize multiple data sources and apply critical thinking skills to effectively triage alerts.
- Manage and resolve client tickets submitted through the ticketing system.
- Collaborate with the Incident Response team to provide insights and support during investigations.
- Document and follow up on open or ongoing security incident tickets.
- Maintain strong communication skills and work effectively within a team.
- Stay informed on emerging threats, such as CVEs and known exploits.

- Work alongside other security staff and engineers on ongoing issues and projects.
- Engage in continuous self-learning and professional development.
- Serve as the technical focal point for security solutions, including firewalls, WAF, remote access, NAC, vulnerability assessment solutions, TLS/SSL interception, and DNS security.
- Demonstrate proficiency in web security, patch management, and foundational knowledge of security domains, such as firewalls, email security, and IPS.
- Conduct risk assessments to identify and prioritize security risks and vulnerabilities related to security solutions.
- Perform security audits and assessments to identify risks, address vulnerabilities, and ensure compliance with regulatory and industry standards.
- Develop and implement security strategies, policies, and procedures to safeguard client systems, servers, networks, and data.
- Provide guidance on security best practices and align with industry standards.
- Offer technical leadership and mentorship to other members of the security team.
- Take ownership of critical security initiatives, driving them from concept to successful implementation.
- Collaborate with cross-functional teams to ensure effective communication and coordination of security initiatives.
- Monitor, assess, and secure cloud environments (AWS, Azure, and GCP) to identify and mitigate risks.
- Implement and manage cloud security tools such as CSPM, CIEM, or CWPP to enhance cloud security posture.
- Ensure compliance with cloud security best practices, frameworks, and regulatory requirements.
- Respond to cloud-specific security incidents and assist in forensic investigations.
- Work with DevOps and cloud engineering teams to integrate security into CI/CD pipelines.

Requirements:

- A degree in Computer Science or a related field, or a minimum of five years of relevant experience with demonstrated ability to perform the required job functions.
- 5+ years of experience in infrastructure security.
- Hands-on experience in an IT Security Operations Center (SOC).
- Experience in mentoring or managing junior security staff.
- Extensive knowledge and experience with Security Information and Event Management (SIEM) systems.
- Expertise with Intrusion Detection and Prevention Systems (IDS/IPS).
- Strong understanding of SSL/TLS, DNS, TCP/IP, computer networking, routing, and switching.
- System administration experience with Windows and Linux/UNIX devices.
- Proficiency in system log forensics (e.g., Syslog and Event Viewer).
- Proven experience securing cloud environments (AWS, Azure, or Google Cloud) and familiarity with cloud-native security tools.
- Experience with cloud security tools such as CSPM, CIEM, or CWPP.
- Knowledge of DevOps practices and integrating security into CI/CD pipelines.

- Exceptional troubleshooting, analytical, and problem-solving abilities.
- Strong organizational skills and ability to work independently while adhering to established processes.
- Excellent verbal and written communication skills for engaging with peers, management, and clients.
- Proven ability to create clear, concise, and professional technical documentation.
- Fluency in English, both spoken and written.
- Experience with Palo Alto, Darktrace, Security Onion, or other relevant tools is considered an asset.
- Familiarity with compliance frameworks (e.g., ISO 27001, SOC 2, NIST, and CIS Benchmarks) is highly desirable.

Benefits

- English-speaking work environment
- Health insurance covered by Kanto IT Software Health Insurance Association
- 401(k)-style defined-contribution retirement plan (after the probation period)
- Life Insurance (after the probation period)
- Sumitomo Seimei Group Three Major Illness Insurance (after the probation period)
- Reimbursement of job-related certifications (subject to conditions)
- Casual dress code
- Self-directed continuous learning programs