SOMPO
INTERNATIONAL

Sompo International is the trade name for the global specialty property and casualty insurance and reinsurance operations of Sompo Holdings, Inc. ("Sompo"), established in March 2017 as the result of Sompo's acquisition of Endurance Specialty Holdings Ltd.

Sompo is a financial services holding company organized under the laws of Japan whose shares are listed and posted for trading on the Tokyo Stock Exchange. Sompo, through various operating subsidiaries, is one of the top three insurers in Japan and is engaged in the provision of insurance services as well as other related services through its global network of businesses operating in 32 countries around the world.

Sompo International is the international operation of Sompo and, through its operating subsidiaries, writes agriculture, casualty and other specialty, professional lines, property, marine/energy and aviation lines of insurance and catastrophe, property, casualty, professional lines and specialty lines of reinsurance.

As a leading global provider of insurance and reinsurance, we recognize that our success is derived directly from those whose contributions matter most: our people. Sompo International's headquarters is in Bermuda and we currently have offices in the United States, the United Kingdom, Continental Europe, and Asia. A shared commitment to integrity, accountability, collaboration and agility define our culture, and we strive to create exceptional value for our clients and shareholders and maintain Sompo International as a desirable place to work.

We are seeking a **Senior Security Analyst** to join our **Information Technology** team in our **Purchase, NY, Florham Park, NJ** or **Charlotte, NC** office. The Senior Security Analyst is responsible for Incident Response, Vulnerability Mitigation, Log Analysis/Correlation, and Security Control Design. The analyst will also lead the investigation of complex security incidents and forward-looking process and tool implementations. This role will continuously enhance the accuracy and efficiency of all Sompo International security tools. The analyst will collaborate with infrastructure operations teams, application owners, vendors, and management to actively manage our security risks.

Main areas of responsibility:

- Identify and investigate security incidents, develop and implement mitigation and response plans.
- Lead incident response efforts including investigation and cooperation with legal and law enforcement as required.
- Implement and manage analysis tools by:
    - Configuring and tuning data sources, rules, and alerts
    - Ensuring service capacity and availability
    - Identifying analysis visibility gaps and developing recommendations to address them
- Use vulnerability data and indicators of compromise to quantify our exposure to newly-discovered threats.
- Interface with other IT disciplines including the networking engineering, storage, monitoring, and platform support teams to provide and coordinate resolution of security issues.
- Provide technical guidance and implementation support for the mitigation of issues discovered by in-house discovery and forensic tools. A successful candidate will have familiarity and understanding of a range of potential issues including:
    - Web application vulnerabilities

SOMPO
INTERNATIONAL

- Windows and Unix system vulnerabilities
- Database security weaknesses
- Malware indicators

Desired Skills & Experience:

- Familiarity with online sources for reliable analysis of emerging threats.
- BS or MA in Computer Science, Information Security, or a related field.
- 5+ years of experience in information security, especially on a Computer Incident Response Team (CIRT), Computer Emergency Response Team (CERT), Computer Security Incident Response Center (CSIRC) or a Security Operations Center (SOC).
- 10+ years of experience in Windows-centric applications and technologies, including:
  - Scripting, OS management tools, and ad-hoc reporting
  - Core OS security
  - Active Directory
  - Certificates and cryptography
  - SMTP and SIP messaging
  - HTTP applications
  - Relational databases
- Experience with a range of vulnerability reporting and management toolsets including Tenable SecurityCenter, Qualys QualyGuard, Varonis DATAdvantage, NMAP, and other ad hoc discovery/forensic tools.
- Hands-on experience with IDS/IPS, SIEM, and web filtering solutions, specifically analyzing, crafting and tuning detection techniques.
- Expert understanding of TCP/IP principles and LAN technology, including network capture utilities, and detailed packet analysis.
- Understand common cyber-attack methods such as SQL Injection and Cross Site Scripting attacks (XSS).
- SANS GCFA, GCED, GMON, and Splunk certifications are a plus.
- Ability to react quickly, decisively, and deliberately in high-stress, high-impact situations.
- Strong decision-making capabilities, weighing the relative costs and benefits of potential actions.
- An ability to collaborate with others to understand and influence their opinions, plans, or behaviors.
- An understanding of business needs and commitment to delivering high-quality, prompt, and efficient service to the business.
- An understanding of organizational mission, values, and goals and consistent application of this knowledge.
- Self-directed knowledge gathering from a combination of public and internal sources – able to answer questions that haven't been asked before.

Sompo International offers a competitive compensation and benefits package commensurate with experience. The minimum salary for this position is: $90,000. For consideration, please e-mail your resume along with your Minimum Salary Expectations as well as your Minimum Total Compensation Expectations to: achimera@sompo-intl.com.

SOMPO
INTERNATIONAL

Sompo International is an equal opportunity employer committed to a diverse workforce. M/F/D/V

Visit our website at www.sompo-intl.com