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 **Purchase, NY, Florham Park, NJ** or **Charlotte, NC** locations.

The Senior Analyst is responsible for Incident Response, Log Analysis/Correlation, Threat Mitigation, and Security Control Implementation. The analyst will respond to complex security incidents starting with either a system-generated alert or a user-reported suspicious activity. When not actively handling incidents, this role will help improve the security of our computing environment by collaborating with application and infrastructure teams or improving our set of internal security tools and processes.

**Main areas of responsibility:**

- Investigate security incidents, develop and implement a response to neutralize the threat. Work with other IT disciplines including the networking, server, database, and application support teams to resolve security issues.
- Design new controls and procedures to prevent future occurrences of common threats. Work with other IT disciplines to implement.
- Exchange threat data with other Sompo companies, ISACs, and regulatory/law enforcement agencies as required.
- Implement and manage security tools:
    - Configure and tune data sources (vendor-provided/third-party/open-source), rules, and alerts
    - Identify visibility gaps and develop options to address them
    - Provide security guidance/implementation support for vulnerability management: work with other IT disciplines to develop a technical mitigation
    - Secure deployment: formulate firewall, IPS, and other rules based on vendor-provided requirements.
    - Public key cryptography: ensure that certificates and keypairs are being used appropriately in devices, applications, etc.
    - Ongoing system hardening: maintain awareness of new security capabilities in our platforms and contribute to the design and implementation. Identify new tactics, techniques, and procedures that threaten our existing controls.

**Desired Skills & Experience:**

The ideal candidate will possess an understanding of business needs and commitment to delivering high-quality, prompt, and efficient service to the business. He/she will react quickly, decisively, and deliberately in high-stress, high-impact situations and collaborate with others to understand and provide guidance surrounding these circumstances. The Senior Security Analyst will also have strong decision-making skills and the ability to implement and measure processes to show effectiveness and consistency.

**Minimum Qualifications:**

- SOC/CIRT incident handling protocols and SIEM tools
- Windows authentication and internals; Kerberos, LDAP, groups, ACLs, and GPOs
- Public key infrastructure and cryptographic fundamentals
- Discovery/reconnaissance/OSINT tools; e.g. nmap, Bloodhound, shodan.io, etc.
- Hands-on experience with IDS/IPS, web filtering, and EDR solutions (Carbon Black), specifically with the creation of access and logging rules
- Online sources for reliable analysis of emerging threats

**Preferred Qualifications:**

- Scripting with PowerShell and Python
- Integration with services via REST and JSON APIs
- Pattern matching using regular expressions (YARA, snort, or similar)
- SAML, OAUTH, and other web authentication mechanisms
- SQL Server security and activity monitoring
- Vulnerability scanning, both tools and workflows for operating systems, web applications, etc.
- Cyber Kill Chain, MITRE ATT &CK, or other frameworks
- Experience in penetration testing
- SANS GCFA, GCED, GMON, or Splunk certification
- BS or MA in Computer Science, Information Security, or a related field

Sompo International offers a competitive compensation and benefits package commensurate with experience. For immediate consideration, please e-mail your resume along with your Minimum Salary Expectations as well as your Minimum Total Compensation Expectations to: abenincaso@sompo-intl.com.

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