HITACHI
Inspire the Next

JOB DESCRIPTION

Title of Position	**Information Security Specialist**
Department	**SOC (Security Operations Centre)**
Immediate Supervisor	**Director, Global Security Operations**
Location	**Blainville**

Summary of the Role:

As an Information Security Specialist, you will join a team of Information Security professionals in support of Hitachi Systems Security Inc. clients by providing Information Security services in various market sectors. Duties will include delivery of security advice and guidance, services, reports and other deliverables to meet client needs.

Primary Responsibilities:

- Assist customers with security related issues;
- Review and validate alerts escalated by Security Analysts;
- Assist Security Analysts on the complex cases and provide guidance during and after a security incident;
- Reviewing customer reports to ensure that quality and accuracy are meet;
- Working with customers to create use cases, correlations rules, filters, …. etc.;
- Creation and tuning IDS rules;
- Fine tuning alerts;
- Reacts to customer's escalations;
- Mentor and Train security analysts in both technical and process areas.;
- Create incidents and support the customers of such incidents to not only mitigate the current threat but also prevent future occurrence;
- Provide support and recommendations to customers in the interest of promoting and maintaining an appropriate security posture;
- Perform vulnerability Management and Penetration tests;
- Be part of on-call rotation team for off-shift escalations;
- Participates in security investigations;
- Provide feedbacks for improvement;
- Follow the incident response process to ensure all security incidents are created and escalated within SLA;
- Participates in organizational projects, as required;
- Excellent analytical skills and having the mentality of a problem solver;
- Excellent communication skills that translate into the ability to effectively handle security incidents;

- Insure that all the security controls in scope are deployed and are working properly; and are meeting the customer needs;

Qualifications Required:

- Expert analytical and problem solving skills;
- Self-driven leader and highly motivated;
- Ability to work independently and in a team environment
- Ability to mentor and train junior SOC analysts on technical and process related areas
- Willingness to work flexible hours and support on-call;
- Experience working with SIEM tools and able to identify tuning recommendations for improved detection and accuracy
- Experience performing security analysis and incident response
- In-depth experience performing packet captures and analyzing output;
- Strong understanding of networking and associated protocols;
- Strong understanding of security threats and vulnerabilities;
- Strong understanding of general cybersecurity concepts;
- Strong understanding of security tools and technologies;
- Customer service skills;
- Excellent verbal and written communication skills in language to be supported;
- Minimum of 3 years of experience in an operations environment as a security analyst and/or engineer;
- Bachelor's degree or equivalent experience in a related field.
- Certified: GCIA, CEH, CISM or CISSP;

We offer:

- Professional environment in cutting-edge technology
- Dynamic work setting in new and modern office
- Employee Referral Bonus
- Group insurance plan
- Team spirit and dedication to service excellence
- Sense of belonging to a global, brand-name organization