**Cyber Security Analyst / Incident Responder**

**Job Description**

We are looking for a **Cyber Security Analyst / Incident responder** who will repert to the Head of CSIRT and will analyze the alerts raised by the SIEM and other Security systems and manage the potential incidents escalated by the SOC and by other activators.

CSIRT Unit is responsibe for the end to end management of Cyber Security Incidents from its detection to the containment eradication and recovery. The CSIRT is also in charge to execute threat hunting activities and to improve, strength and evolve the Incident management process. The Unit manages the SOC (Security Operation Center) service, the IR (Incident Response) service and the phishing analysis processes in close coordination with the other security and IT teams within GOSP.

The Cyber Security Analyst / Incident Responder will be in charge of executing all the incident management activities, from the containment of the threat to its eradication (directly or coordinating other IT department of the company).

The resource will also deepen the analysis on emerging threats and will perform threat hunting activities with the tools and resources at his disposal.

The candidate is also asked to support the other team within the CSO Division performing tasks such as:

* Support SIEM Use Cases definition and alerts engineering
* Support the Vulnerability management and prevention unit
* Review the effectiveness of the EDR’s detections
* Support the other teams within the GOSP CSO Division

**Main tasks**:

* Analyze the security incident identified by SOC and other activators, assess and assign the appropriate severity and priority, contain the threat, define and monitor the remediation activities
* Proactively identify possible threats performing threat hunting activities
* Define the priority of incidents to determine the appropriate response and course of action that has to be taken to effectively manage the incident lifecycle
* Identify events that could lead to loss or disruption of operation, service or function within the organization, leveraging OSINT sources and early warning received by the Group Security Intelligence Team
* Limit disruption and its consequences and returning back to business as usual
* Support, monitor and control the mitigation / resolution activities undertaken
* Execute the escalation process when incident becomes a crisis / emergency
* Provide structured ex post analysis to the detection or resolution of the event
* Perform forensic analysis on infected assets
* Report and present the results of the analysis in both oral and written form to different stakeholders
* Manage and evolve the tools supporting the Incident management process

It could be also requested to support the team performing the other tasks of the Unit:

* Monitor all the security events, detecting, containing, managing and mitigating through the SOC
* Perform Intelligence activities in order to develop and manage the Security Intelligence tools, feeds and platforms of the CSIRT
* Evaluate and scout new tools to increase the CSIRT response capability
* Support GHO IT Security to define a set of possible attacks (use cases), assessing the probability, the potential harm and the priority of identified attacks and thus minimizing the risk involved
* Manage, test and evolve the Security Operation Center
* Support the other teams within the GOSP CSO division

**Requirements**

Our ideal candidate will meet the following requirements:

* STEM degree-level (Science, Technology, Engineering or Mathematics) with strong passion on cyber security
* Knowledge of SIEM technologies (QRadar, Splunk, … ) and Big Data tools for analytics
* Strong understanding of attackers tactics techniques and procedures;
* Strong understanding of the security implications and investigation methods for the most common IT components: network infrastructure (routing, switching and firewalls), security infrastructure (IPS, WAF, AV), OS knowledge (Linux/UNIX and Microsoft Windows, client and server), core infrastructures (Active Directory, Exchange, DNS, DHCP), full stack web services infrastructure and technologies involved (front-end to back-end). Analysis of network captures and knowledge of TCP/IP and network protocols
* Forensic analysis experience
* Threat hunting activities experience
* Experience in at least one of the following programming languages: Python, C, C++, Java

Nice to have:

* Certifications on Information Security (e.g. GIAC GCFE, GSEC, CEH, CSX, CHFI etc.) would be a plus

Soft Skills:

* Strong passion on cyber security
* Ability to work in large international organization, in multicultural contexts and to deal with different scenarios
* Analytical and communication skills
* Demonstrated ability to work effectively as part of a team sharing and parallelizing tasks and knowledges
* Excellent written and oral English language skills
* Advanced problem solving and analytical
* Great attention to privacy and confidentiality managing critical information. Great sense of information classification and ability to understand the right level of disclosure in each situation
* Pugnacity, tenacity, imagination, judgment and the resistance to stress are also key qualities in that job

Company Profile

Generali is a major player in the global insurance industry – a strategic and highly important sector for the growth, development and welfare of modern societies. Over almost 200 years, we have built a multinational Group that is present in more than 60 countries, with 470 companies and nearly 80,000 employees.

GOSP - Generali Operations Service Platform is a joint-venture between Generali and Accenture and provides IT and Procurement services to Generali Group companies. Our purpose is to accelerate the Group's innovation and digitization strategy through the Cloud and shared platforms. Based in Italy it has 5 branches across Europe and employs about 1.000 people.