

IT Security Analyst

Deadline:

01-11-2026

General Overview of the Job:

We are looking for a skilled Security Operations Center (SOC) Analyst with experience in cyber threat intelligence (CTI), threat hunting, analytic rule creation, and incident response. This role will be responsible for day-to-day security operations, proactive threat detection, and threat intelligence analysis to help strengthen the organization's overall security posture.

Job Duties and Responsibilities:

- Perform day-to-day monitoring, investigation, triage, containment, and handling of security incidents and alerts.
- Conduct proactive threat hunting activities to identify suspicious, anomalous, or malicious activities across the environment.
- Create, tune, and maintain analytic/detection rules within SIEM and security monitoring platforms.
- Analyze cyber threat intelligence feeds, indicators of compromise (IoCs), emerging threats, and attacker behaviors to improve detection and response capabilities.
- Perform threat actor profiling, TTP (Tactics, Techniques, and Procedures) analysis, and mapping using frameworks such as MITRE ATT&CK.
- Manage IoC lifecycle activities including validation, enrichment, tracking, tuning, and operationalization.
- Utilize threat intelligence platforms such as Recorded Future or similar CTI solutions for threat research and analysis.
- Investigate phishing, malware, endpoint, identity, cloud, and network-related security incidents.
- Correlate logs, telemetry, and intelligence data to identify attack patterns and security gaps.
- Present findings, discuss risks, and provide security recommendations to technical teams, management, and stakeholders.
- Coordinate with internal teams during incident response and remediation activities.
- Continuously improve SOC processes, use cases, playbooks, and detection coverage.

Minimum Qualifications:

- At least 3–5 years of experience in SOC operations, incident response, threat hunting, or cyber threat intelligence.
- Hands-on experience with SIEM platforms such as Microsoft Sentinel
- Experience creating and tuning analytic rules, detections, correlation logic, and alerting mechanisms.

Strong knowledge of cyber threat intelligence concepts including:

- Threat actor profiling
- TTP analysis
- IOC management
- Threat landscape monitoring
- MITRE ATT&CK mapping
- Experience using CTI platforms such as: Recorded Future
- Experience investigating phishing, malware, account compromise, insider threats, and advanced attack activities.
- Knowledge of KQL, SPL, or similar query languages.
- Strong analytical, investigative, documentation, and communication skills.
- Ability to present technical findings clearly to stakeholders and management.

Contact person:

Jose Manuel Catindig

Office:

Manila, Alabang (SSC),
Philippines

Location:

Alabang–Zapote Road, 1780,
Muntinlupa

