SOC Analyst (Internship)

To analyse any incidents escalated by the Level 1 Security Engineer and undertake the detailed investigation of the Security Event.
Shall determine whether the security event will be classified as an incident.
Coordinating with the customer IT and Security team for resolution of the Security Incident.
This role reports to the SOC Team Lead.

Duties

- Perform proactive monitoring for security log events in 24x7 mode. (Splunk, SIEM, TrendMicro (EDR/IPS/etc) and others 3rd Party software)
- Escalate validated and confirmed incidents to designated incident response team.
- Notify Client of incident and required mitigation works.
- Fine-tune SIEM rules to reduce false positive and remove false negatives / analysis and response to previously unknown hardware and software vulnerabilities.
- Collect global threat intelligence and internal threats then inject actions based on analysis and recommendation.
- Provide advisories and threat intelligence based on new trends, threats, emerging campaigns, malicious attacks, hacker group.
- Proactively research and monitor security information to identify potential threats that may impact the organisation.
- Develop and distribute information and alerts on required corrective actions to the organisation.
- Learn new attack patterns, actively participate in security forums.
- Perform threat intel research.
- Track and update incidents and requests based on client's updates and analysis results.
- Investigating, documenting, and reporting on any information security (InfoSec) issues as well as emerging trends.
- Assist the Level 1 or Level 2 with monthly and ad-hoc reporting - responsible for completing statistical and status reports, as well as providing fast and timely responses.
- Perform as an escalation point for all incidents relating to potential security