Roles of a Cyber Security Analyst

Cyber Security Analyst

Are you a problem solver? Do have good analytical skills and like to get to the bottom of an issue? Cyber security analysts help to protect an organisation by employing a range of technologies and processes to prevent, detect and manage cyber threats. This can include protection of computers, data, networks and programmes.

Analysts are the guardians of the networks and with the largest share of the job market as well. A Cyber Analyst comes in primarily three forms and will typically wear multiple hats; performing different positions than regulated to one specific task.

Job titles vary and may include information security analyst, security analyst, information security consultant, security operations centre (SOC) analyst and cyber intelligence analyst.

So what is it like during a day for an Analyst?

The primary duty is to actively defend a network by utilising security tools and policies. The primary security tool is a SIEM; however, some organisations may use a managed Host Intrusion Detection System (HIDS) or a Host Intrusion Prevention System (HIPS) to manage and monitor the network. They are similar to use, with the exception that a HIDS/HIPS can manage the end points while a SIEM can only provide data.

An end point is a remote computing device that communicates back and forth with a network to which is it connected. Examples of endpoints include:

- Desktops
- Laptops
- Smartphones
- Tablets
- Servers
- Workstations

When using such systems, analysts determine if there are anomalies that need further investigation, or further observe for any suspicious activity or attacks. Investigation involves checking with other security tools and the log files. The investigation may also involve the human aspect to determine if a non-technical situation occurred.

Analysts normally operate within four common tiers of support:

- Tier 1 Alert Analysts are the front line fighters, which go through the hordes of alerts and logs and determine what is suspicious for further investigation by the Tier 2 Analysts or can be removed the queues.
    - Monitor for events and alerts and prune the log queue
    - Escalate security alerts to Tier 2
    - The rule of thumb is to make a decision of an alert in approximately 5 minutes. Thus if the analyst believes that a given alert can be resolved in under 5 minutes, then the Analysts can take action to solve for it; otherwise up it goes to the next Tier.

- Tier 2 Incident Response, these analysts investigate the alerts that the Tier 1 Analysts has referred to them.
    - Respond to the alerts sent from Tier 1 Analysts
    - May need to institute the Incident Response Plan if the situation warrants it.
    - Perform deep data dive by gather data from multiple sources.
    - Determine if a critical component or data has been impacted
    - Advisory support for Tier 1 Analyst

- Tier 3 Subject Matter Experts, these are specialised roles which can cover Hunting, Threat Intelligence, System Engineering, etc.
    - Expertise with networking, endpoints, threat intelligence and forensics
    - Usually of reviewing and proposing changes for the rulesets
    - When there are incidents occurring, will then take active actions such as hunting within the network to find possible incidents.
    - Involved in developing, tuning and implementing threat detection analytics.

- Tier 4 Management; this is the management rank that leads the security team. This includes the common management tasks such as:
    - Manages resources to include personnel, budgeting, and scheduling
    - Manages the technology strategies to meet Service Level Agreements (SLA)
    - Coordinates and communicates with senior and peer management
    - Works with the ultimate goal of detecting, investigating and mitigating incidents that impacts business.

The core duty of the Analyst is the same for all; to monitor for signs of suspicious activity and to take action to stop or limit the activity in order to protect the data. Overall with most career opportunities, working as Analyst is about 90% routine and with a 10% dealing with incidents and attacks.

Broadly, you can work in one of the following areas:

- working to protect the security of the organisation you work for; or
- consulting, offering technical advisory services to clients