

5.1. Incident Identification and Classification

Effective incident identification and classification are pivotal components of the Spectra360 Security Operations Center (SOC) platform, ensuring prompt detection and appropriate prioritization of security events. This process enables the SOC to allocate resources efficiently and implement suitable response strategies.

Incident Identification:

The identification phase involves the continuous monitoring of systems and networks to detect potential security incidents. Key activities include:

- **Monitoring Systems and Networks:** Utilizing tools to observe system activities and network traffic for signs of anomalies or malicious behavior.
- **Collecting and Analyzing Security Logs and Alerts:** Gathering data from various sources to identify patterns indicative of security threats.
- **Triage and Prioritization:** Assessing detected events to determine their significance and urgency.

Incident Classification:

Once an incident is identified, it is classified based on predefined criteria to determine its severity and impact. This classification guides the response process. Factors considered in classification include:

- **Number of Affected Parties:** Assessing how many clients or organizations are impacted.
- **Reputational Impact:** Evaluating potential damage to the organization's reputation.
- **Duration and Downtime:** Considering how long systems are affected.
- **Geographical Spread:** Determining the extent of the incident's reach.
- **Data Loss:** Assessing the extent of data loss concerning confidentiality, integrity, and availability.
- **Criticality of Services Affected:** Identifying which essential services are impacted.
- **Economic Impact:** Estimating the financial consequences of the incident.