Incident triage involves rapidly assessing and categorizing security incidents to determine their severity and priority. It's the first step in responding to a potential threat and helps allocate resources efficiently.

INCIDENT TRIAGE PROCESS

Initial Assessment:

- Quickly gather information about the incident, such as the nature of the threat, affected systems, and potential impact.
  - Determine if the incident is a false positive or a genuine security threat.

Classification

- Categorize incidents based on their severity and potential impact on the organization.
  - Classify incidents to prioritize responses and allocate resources effectively.

Prioritization

- Prioritize incidents based on their criticality and the level of risk they pose.
  - Consider factors such as data sensitivity, potential financial loss, and impact on business operations.

Escalation

- If needed, escalate the incident to higher levels of management or specialized teams for further investigation and resolution.
  - Establish clear communication channels for efficient escalation.
A

Documentation

- Thoroughly document all aspects of the incident, including initial findings, actions taken, and the resolution process.
  - Accurate documentation is crucial for post-incident analysis and compliance purposes.

INCIDENT TRIAGE CHALLENGES

Time Sensitivity

Triage must be swift to minimize the impact of security incidents. Balancing speed with accuracy is a constant challenge.

Limited Information

Initial information may be limited, making it essential to adapt to new details as the incident unfolds.

False Positives

Sorting genuine threats from false positives requires a discerning eye to avoid unnecessary panic and resource allocation.

INCIDENT TRIAGE BEST PRACTICES

Regular Training

Stay updated on the latest threats and practice incident response scenarios regularly Ato enhance triage skills.

Collaboration

Work closely with other SOC team members, IT departments, and relevant stakeholders to gather comprehensive information.

Automation:

Leverage automation tools for quick data analysis and to streamline the initial stages of incident assessment.

Continuous Improvement

Conduct post-incident reviews to identify areas for improvement in the triage process.