The triage process

Previously, you learned that triaging is used to assess alerts and assign priority to incidents. In this reading, you'll explore the triage process and its benefits. As a security analyst, you'll be responsible for analyzing security alerts. Having the skills to effectively triage is important because it allows you to address and resolve security alerts efficiently.

Triage process

Incidents can have the potential to cause significant damage to an organization. Security teams must respond quickly and efficiently to prevent or limit the impact of an incident before it becomes too late. **Triage** is the prioritizing of incidents according to their level of importance or urgency. The triage process helps security teams evaluate and prioritize security alerts and allocate resources effectively so that the most critical issues are addressed first.

The triage process consists of three steps:

1. Receive and assess
2. Assign priority
3. Collect and analyze

Receive and assess

During this first step of the triage process, a security analyst receives an alert from an alerting system like an **intrusion detection system** (IDS). You might recall that an IDS is an application that monitors system activity and alerts on possible intrusions. The analyst then reviews the alert to verify its validity and ensure they have a complete understanding of the alert.

This involves gathering as much information as possible about the alert, including details about the activity that triggered the alert, the systems and assets involved, and more. Here are some questions to consider when verifying the validity of an alert:

- **Is the alert a false positive?** Security analysts must determine whether the alert is a genuine security concern or a **false positive**, or an alert that incorrectly detects the presence of a threat.
- **Was this alert triggered in the past?** If so, how was it resolved? The history of an alert can help determine whether the alert is a new or recurring issue.
- **Is the alert triggered by a known vulnerability?** If an alert is triggered by a known vulnerability, security analysts can leverage existing knowledge to determine an appropriate response and minimize the impact of the vulnerability.
- **What is the severity of the alert?** The severity of an alert can help determine the priority of the response so that critical issues are quickly escalated.

Assign priority

Once the alert has been properly assessed and verified as a genuine security issue, it needs to be prioritized accordingly. Incidents differ in their impact, size, and scope, which affects the response efforts. To manage time and resources, security teams must prioritize how they respond to various incidents because not all incidents are equal. Here are some factors to consider when determining the priority of an incident:

- **Functional impact:** Security incidents that target information technology systems impact the service that these systems provide to its users. For example, a ransomware incident can severely impact the confidentiality, availability, and integrity of systems. Data can be encrypted or deleted, making it completely inaccessible to users. Consider how an incident impacts the existing business functionality of the affected system.
- **Information impact:** Incidents can affect the confidentiality, integrity, and availability of an organization's data and information. In a data exfiltration attack, malicious actors can steal sensitive data. This data can belong to third party users or organizations. Consider the effects that information compromise can have beyond the organization.
- **Recoverability:** How an organization recovers from an incident depends on the size and scope of the incident and the amount of resources available. In some cases, recovery might not be possible, like when a malicious actor successfully steals proprietary data and shares it publicly. Spending time, effort, and resources on an incident with no recoverability can be wasteful. It's important to consider whether recovery is possible and consider whether it's worth the time and cost.

Note: Security alerts often come with an assigned priority or severity level that classifies the urgency of the alert based on a level of prioritization.

Collect and analyze

The final step of the triage process involves the security analyst performing a comprehensive analysis of the incident. Analysis involves gathering evidence from different sources, conducting external research, and documenting the investigative process. The goal of this step is to gather enough information to make an informed decision to address it. Depending on the severity of the incident, escalation to a level two analyst or a manager might be required. Level two analysts and managers might have more knowledge on using advanced techniques to address the incident.

Benefits of triage

By prioritizing incidents based on their potential impact, you can reduce the scope of impact to the organization by ensuring a timely response. Here are some benefits that triage has for security teams:

- **Resource management:** Triaging alerts allows security teams to focus their resources on threats that require urgent attention. This helps team members avoid dedicating time and resources to lower priority tasks and might also reduce response time.
- **Standardized approach:** Triage provides a standardized approach to incident handling. Process documentation, like playbooks, help to move alerts through an iterative process to ensure that alerts are properly assessed and validated. This ensures that only valid alerts are moved up to investigate.

Key takeaways

Triage allows security teams to prioritize incidents according to their level of importance or urgency. The triage process is important in ensuring that an organization meets their incident response goals. As a security professional, you will likely utilize triage to effectively respond to and resolve security incidents.