Incident Management Analysis

By: Ryan Stewart

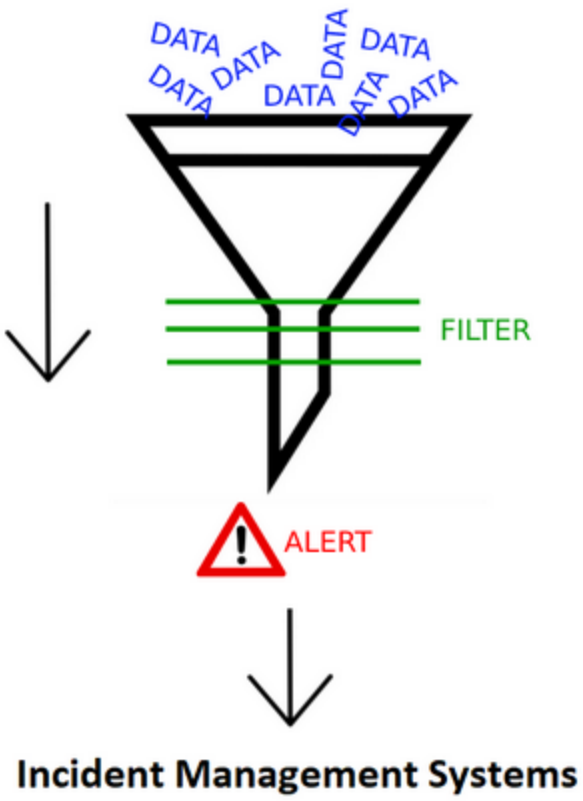
Basic Definitions About Incident Management

In this section, we will elucidate fundamental concepts crucial for understanding incident management. These concepts will be encountered frequently in your educational journey and daily work routine, making it essential to thoroughly grasp their meanings:

- **Alert**
- **Event**
- **Incident**
- **True Positive**
- **False Positive**

Alert

In the SIEM training module (accessible [here](https://app.letsdefend.io/training/lessons/siem-101)), we previously discussed how alerts are generated. Briefly, an alert results from data collection and processing (parsing, enriching, etc.) in SIEM, initiating the analysis process by sending the generated alarms to the Incident Management System.



Event

An event refers to any observable occurrence in a system or network. Essentially, events encompass activities such as a user connecting to a file share, a server receiving a request for a web page, a user sending electronic mail (e-mail), or a firewall blocking a connection attempt.

Incident

The definition of a computer security incident has evolved over time. Initially perceived as a security-related adverse event involving the loss of data confidentiality, disruption of data or system integrity, or denial of availability, the term "incident" has expanded. Broadly, an incident now encompasses any violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices ([NIST Special Publication 800-61](https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final)).

True Positive Alert

A True Positive alert occurs when the detected situation aligns with the situation intended to be identified. For instance, a positive COVID-19 test result accurately reflects the condition it aims to detect – the presence of COVID-19. In the context of security, if a rule designed to detect SQL Injection attacks triggers due to a genuine attack, it is classified as a "True Positive."

False Positive Alert

In contrast, a False Positive Alert is essentially a false alarm. Imagine a security camera in your home alerting you to your cat's movements – this is a false positive alert. Similarly, if an SQL injection alert is triggered by a harmless URL containing the word "Union" used in a sports context, it is considered a false positive alert.