Security Events vs. Security Incidents

Security Events and Security Incidents sound pretty similar, but they are both different terms in the security environment. Cybersecurity professionals use these terms to determine the severity of potential data breaches. This blog is curated to explain the difference between Security Events and Security Incidents.

What is a Security Event?

A security event is a change in regular operations of a network or service representing a security policy that can violate. It includes an attempted attack that creates security vulnerabilities. Organization undergoes thousands of events every day, and most of these events can be resolved by security specialists with the best security practices.

Examples of Security Events

- The user is unable to access files in the system, and the system does not respond properly.
- The file server runs slow.
- The files do not open, and a suspicious notice or an alert message displays on the screen.

- The content on the website has changed to something obscene.

What is a Security Incident?

A security incident is an event that further leads to potential risks for the organization's information security. It includes any event that threatens the Confidentiality, Integrity, and Availability of information.

Examples of Security Incidents

- Security Management finds a virus in the system.
- Network security finds a suspicious activity network port scan.
- A Ransomware virus is on the user's computer and has a notification that files are encrypted, and a Bitcoin payment is required to decrypt.
- An employee downloads the attachments shared through phishing emails.
- A brute force attack compromises the password on the system.

Difference between Security Event and Security Incident

A Security event can encompass various issues that impact an organization. Security events occur in the hundreds of thousands if not millions. It rarely leads to a data breach that can potentially affect the organization.

Security incidents differ from security events and result in a higher risk to an organization. Security events indicate that a system can be compromised but can also result in other cases, such as a suspicious login attempt or a misconfiguration.

For example, a phishing email is a security event. Still, an employee clicking on a link in the email might result in an incident that further exposes credential theft, malware, or a phishing attempt.

Events are easy to resolve, and they represent isolated risks. Organizations may experience thousands of security events in a day, which they resolve using automated tools such as SIEM.

SOC Training at InfosecTrain

InfosecTrain offers Security Operation Center (SOC) Analyst training curated for aspiring and current SOC Analysts who want to know how to identify, assess, respond, and prevent cybersecurity threats and incidents. This training would also help you to get a complete understanding of security solutions such as digital forensics, threat intelligence, and SIEM. Also, you can crack the certification exam seamlessly.