Security Events vs Security Incidents

This lesson will explain the key differences between security events and security incidents. It is important to establish why these are different and why different measures are taken to address them. By the end of this lesson, you should be able to explain the difference and provide examples of each category. **It's important to remember that all security incidents are security events, but not all events become incidents.**

SECURITY EVENTS

A Security event is anything that ***could*** have a security implication, such as causing damage or disruption. Examples of this include:

- **Spam emails –** as they could potentially include hyperlinks to malicious websites such as credential harvesters or malware downloads.
- **A malicious actor performing a vulnerability scan –** as this could identify a vulnerability that can later be exploited.
- **A malicious actor performing reconnaissance scans –** as this helps them to build up a better idea of the systems used by the organization, which can be researched to identify vulnerabilities and weaknesses.
- **An explained anomaly –** an unusual circumstance, but the cause is identified and it is not malicious (such as disruption on the network caused by a misconfiguration).
- **A user downloads software from the internet –** to a company-owned device. There is always a risk with downloaded files from the internet. Users that are not very tech or security-savvy may inadvertently download malicious software or legitimate software that is bundled with malware such as trojans.
- **A malicious actor begins a brute-force attack –** against a login portal on a web server. This is an event until the attacker gains access.

Security events are happening constantly, and are typically dealt with automated security controls or simply logged in case they evolve into security incidents.

SECURITY INCIDENTS

Security incidents are security events that have resulted in damage to the organization. Revisiting the examples of security events, let's cover how they could turn into incidents.

- **The spam email –** contained a malicious URL which downloads Maze ransomware to the system, encrypting all of the organization's files. The email being delivered is the **security event**, and the ransomware encrypting files is the **damage** as it causes operational disruption.
- **The vulnerability scan –** showed a number of easily-exploited vulnerabilities, which the malicious actor proceeded to exploit giving them remote access to a server in the DMZ, where the actor then exfiltrated data from a database. The vulnerability scan is the **security event**, and the data breach is the **damage**.
- **An unexplained anomaly –** an unusual circumstance, where the root cause has not yet been identified. This is classed as an incident, as until this has been properly scoped, there is the potential for malicious activity.
- **A user downloads software from the internet –** to a company-owned device. This turned out to be a piece of malware, which infected the system and began beaconing to its command-and-control server to retrieve instructions. The operators tell the malware to collect common files (such as .docx, .xlsx, .pptx) and send them to the malicious actors. The user downloaded software is the **security event**, and the data exfiltration is the

damage.

- **A malicious actor is successful with their brute-force attack –** against a login portal on a web server. They can now browse files, edit web pages, and view the contents of a MySQL database. The brute-force attack is the **security event**, and the intrusion and access of private information is the **damage**.

EVENTS vs INCIDENTS

Security events will typically be dealt with by security analysts (often within a Security Operations Center, or SOC) whereas security incidents are often handled by specialist incident responders (depending on the size of the organization and security team) who can perform advanced analysis and investigation into what exactly has occurred, and how to contain and respond to the incident. If there is a high risk to the organization, either an internal or external Computer Security Incident Response Team (CSIRT) may be activated to respond.

Not every SIEM or IDS alert is an incident. It is more likely to be an event that is manageable, such as an IP scanning the organization's public IP range, or it could even be a false positive, where an alert is generated, but no malicious activity has taken place. It's important to look into every alert that is generated, and use knowledge and experience to determine what this alert is representing, and how to respond to it appropriately.

Previous Topic | Mark Complete | Next Topic

Back to Lesson