Welcome to module 3 ; The detection and analysis phase of the lifecycle

Welcome back!
I want to commend you on such a fantastic job you're doing so far.
The skills you are learning will create a solid foundation as you begin your security career.

In the previous section, you applied your networking knowledge to deepen your understanding of network traffic.
You practiced some skills that security analysts use on the job like capturing network traffic and dissecting packets.
Next, we'll examine the life cycle of a security incident from beginning to end.
You'll focus on how to detect, respond, and recover from an incident.
Coming up, you'll learn how to investigate and verify an incident once it's been detected.
You'll explore the plans and processes behind incident response.
Finally, you'll learn about the post-incident actions that organizations take to learn and improve from the experience.

At the end of this section, you'll gain a comprehensive understanding of an incident's lifecycle.
You ready?
Let's begin!

The detection and analysis phase of the lifecycle

Incidents happen, and as a security analyst, you'll likely be tasked with investigating and responding to security incidents at some point in your career.
Let's examine the Detection and Analysis phase of the incident response lifecycle.
This is where incident response teams verify and analyze incidents.

Detection enables the prompt discovery of security events.

Remember not all events are incidents, but all incidents are events.
Events are regular occurrences in business operations, like visits to a website or

password reset requests.
IDS and SIEM tools collect and
analyze event data from different sources to identify potential unusual activity.
If an incident is detected, such as a malicious actor successfully gaining
unauthorized access to an account, then an alert is sent out.
Security teams then begin the Analysis phase.

Analysis involves the investigation and validation of alerts.
During the analysis process, analysts must apply their critical thinking and
incident analysis skills to investigate and validate alerts.
They'll examine indicators of compromise to determine if an incident has occurred.
This can be a challenge for a couple of reasons.

The challenge with detection is it's impossible to detect everything.
Even great detection tools have limitations in how they work, and automated
tools may not be fully deployed across an organization due to limited resources.
Some incidents are unavoidable, which is why it's important for
organizations to have an incident response plan in place.

Analysts often receive a high volume of alerts per shift,
sometimes even thousands.
Most of the time, high alert volumes are caused by misconfigured alert settings.
For example, alert rules that are too broad and
not tuned to an organization's environment create false positives.
Other times, high alert volumes can be legitimate alerts caused
by malicious actors taking advantage of a newly discovered vulnerability.

As a security analyst, it's important that you're equipped to effectively analyze
alerts and coming up, you'll do just that.

Revision #4
Created 2023-09-13 14:57:33 UTC by naruzkurai
Updated 2023-11-01 01:10:46 UTC by naruzkurai