Wrap-up; Terms and definitions from Course 6, Week 1

Way to go! You made it through a new section, and you've learned a lot.

As a refresher, we first covered the incident response lifecycle as a framework to support incident response processes.

You were also given your very own incident handler's journal for your incident investigations, which you'll continue to use throughout this course.

You explored how incident response teams operate together to respond to incidents using incident plans.

You also learned about the documentation, detection, and management tools used during incident response.

Congrats on making it through the first part of your incident response journey.
Coming up, we'll explore network monitoring.
You'll also have the opportunity to apply your learning through the activities.
I'll meet you in the next section.

Glossary terms from week 1

Terms and definitions from Course 6, Week 1

Computer security incident response teams (CSIRT): A specialized group of security professionals that are trained in incident management and response

Documentation: Any form of recorded content that is used for a specific purpose

Endpoint detection and response (EDR): An application that monitors an endpoint for malicious activity

Event: An observable occurrence on a network, system, or device

False negative: A state where the presence of a threat is not detected

False positive: An alert that incorrectly detects the presence of a threat

Incident: An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies

Incident handler's journal: A form of documentation used in incident response

Incident response plan: A document that outlines the procedures to take in each step of incident response

Intrusion detection system (IDS): An application that monitors system activity and alerts on possible intrusions

Intrusion prevention system (IPS): An application that monitors system activity for intrusive activity and takes action to stop the activity

National Institute of Standards and Technology (NIST) Incident Response Lifecycle: A framework for incident response consisting of four phases: Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and Post-incident activity

Playbook: A manual that provides details about any operational action

Security information and event management (SIEM): An application that collects and analyzes log data to monitor critical activities in an organization

Security operations center (SOC): An organizational unit dedicated to monitoring networks, systems, and devices for security threats or attacks

Security orchestration, automation, and response (SOAR): A collection of applications, tools, and workflows that uses automation to respond to security events

True negative: A state where there is no detection of malicious activity

True positive An alert that correctly detects the presence of an attack

---

Revision #1
Created 2023-09-06 11:42:48 UTC by naruzkurai
Updated 2023-11-01 01:10:46 UTC by naruzkurai