

# Terms and definitions from Course 6, course 6 glossary

## A

**Advanced persistent threat (APT):** An instance when a threat actor maintains unauthorized access to a system for an extended period of time

**Analysis:** The investigation and validation of alerts

**Anomaly-based analysis:** A detection method that identifies abnormal behavior

**Array:** A data type that stores data in a comma-separated ordered list

## B

**Broken chain of custody:** Inconsistencies in the collection and logging of evidence in the chain of custody

**Business continuity plan (BCP):** A document that outlines the procedures to sustain business operations during and after a significant disruption

## C

**Chain of custody:** The process of documenting evidence possession and control during an incident lifecycle

**Command and control (C2):** The techniques used by malicious actors to maintain communications with compromised systems

**Command-line interface (CLI):** A text-based user interface that uses commands to interact with the computer

**Common Event Format (CEF):** A log format that uses key-value pairs to structure data and identify fields and their corresponding values

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

**Configuration file:** A file used to configure the settings of an application

**Containment:** The act of limiting and preventing additional damage caused by an incident

**Crowdsourcing:** The practice of gathering information using public collaboration

## D

**Data exfiltration:** Unauthorized transmission of data from a system

**Data packet:** A basic unit of information that travels from one device to another within a network

**Detection:** The prompt discovery of security events

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

## E

**Endpoint:** Any device connected on a network

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

**Eradication:** The complete removal of the incident elements from all affected systems

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

## F

**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

**Final report:** Documentation that provides a comprehensive review of an incident

## H

**Honeypot:** A system or resource created as a decoy vulnerable to attacks with the purpose of attracting potential intruders

**Host-based intrusion detection system (HIDS):** An application that monitors the activity of the host on which it's installed

## I

**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

**Indicators of attack (IoA):** The series of observed events that indicate a real-time incident

**Indicators of compromise (IoC):** Observable evidence that suggests signs of a potential security incident

**Internet Protocol (IP):** A set of standards used for routing and addressing data packets as they travel between devices on a network

**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

## K

**Key-value pair:** A set of data that represents two linked items: a key, and its corresponding value

## L

**Lessons learned meeting:** A meeting that includes all involved parties after a major incident

**Log analysis:** The process of examining logs to identify events of interest

**Log management:** The process of collecting, storing, analyzing, and disposing of log data

**Logging:** The recording of events occurring on computer systems and networks

## M

**Media Access Control (MAC) Address:** A unique alphanumeric identifier that is assigned to each physical device on a network

## N

**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

**Network-based intrusion detection system (NIDS):** An application that collects and monitors network traffic and network data

**Network data:** The data that's transmitted between devices on a network

**Network Interface Card (NIC):** Hardware that connects computers to a network

**Network protocol analyzer (packet sniffer):** A tool designed to capture and analyze data traffic within a network

**Network traffic:** The amount of data that moves across a network

## O

**Object:** A data type that stores data in a comma-separated list of key-value pairs

**Open-source intelligence (OSINT):** The collection and analysis of information from publicly available sources to generate usable intelligence

## P

**Packet capture (p-cap):** A file containing data packets intercepted from an interface or network

**Packet sniffing:** The practice of capturing and inspecting data packets across a network

**Playbook:** A manual that provides details about any operational action

**Post-incident activity:** The process of reviewing an incident to identify areas for improvement during incident handling

## R

**Recovery:** The process of returning affected systems back to normal operations

**Resilience:** The ability to prepare for, respond to, and recover from disruptions

**Root user (or superuser):** A user with elevated privileges to modify the system

## S

**Search Processing Language (SPL):** Splunk's query language

**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

**Signature:** A pattern that is associated with malicious activity

**Signature analysis:** A detection method used to find events interest

**Standards:** References that inform how to set policies

**Sudo:** A command that temporarily grants elevated permissions to specific users

**Suricata:** An open-source intrusion detection system and intrusion prevention system

## T

**tcpdump:** A command-line network protocol analyzer

**Telemetry:** The collection and transmission of data for analysis

**Threat hunting:** The proactive search for threats on a network

**Threat intelligence:** Evidence-based threat information that provides context about existing or emerging threats

**Triage:** The prioritizing of incidents according to their level of importance or urgency

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

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

## V

**VirusTotal:** A service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content

## W

**Wildcard:** A special character that can be substituted with any other character

**Wireshark:** An open-source network protocol analyzer

## Y

**YARA-L:** A computer language used to create rules for searching through ingested log data

**Zero-day:** An exploit that was previously unknown

---

---

Revision #1

Created 6 November 2023 16:39:17 by naruzkurai

Updated 6 November 2023 16:40:54 by naruzkurai