Glossary terms

Terms and definitions

Analysis: The investigation and validation of alerts

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

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

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

Crowdsourcing: The practice of gathering information using public input and collaboration

Detection: The prompt discovery of security events

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

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

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

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

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

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

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

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

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

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

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

Standards: References that inform how to set policies

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

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