Glossary terms

Terms and definitions

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