Acronis

Glossary

#CyberFit

Glossary

Endpoint protection platform (EPP)	An endpoint protection platform (EPP) is a solution deployed on endpoint devices to prevent file-based malware attacks, detect malicious activity and provide the investigation and remediation capabilities needed to respond to dynamic security incidents and alerts. Detection capabilities will vary, but advanced solutions will use multiple detection techniques, ranging from **static IOCs (signature-based detection) to behavioral analysis**. Desirable EPP solutions are primarily cloud-managed, allowing the continuous monitoring and collection of activity data, along with the ability to take remote remediation actions, whether the endpoint is on the corporate network or outside of the office. In addition, these solutions are cloud-data-assisted, meaning the endpoint agent does not have to maintain a local database of all known IOCs, but can check a cloud resource to find the latest verdicts on objects that it cannot classify. Note: According to Gartner EDR and EPP tools are merging to address new threats. Leading vendors have created holistic tools in a single portal. These platforms can displace existing endpoint toolsets with faster detection and optional automated response.
Endpoint Detection and Response (EDR)	Solutions that record and store endpoint-system-level behaviors, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity and provide remediation suggestions to restore affected systems. EDR solutions must primarily provide the following four capabilities: ▪ Detect security incidents ▪ Contain the incident at the endpoint ▪ Investigate security incidents ▪ Provide remediation guidance

Glossary

Term	Description
Extended Detection and Response (XDR)	The evolution of EDR, which optimizes threat detection, investigation, response, and hunting in real time. XDR unifies security-relevant endpoint detections with telemetry from security and business tools such as network analysis and visibility (NAV), email security, identity and access management, cloud security, and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation.
Managed Detection and Response (MDR)	Managed detection and response (MDR) is an outsourced service that provides organizations with threat hunting services and responds to threats once they are discovered. It also involves a human element: Security providers provide their MDR customers access to their pool of security researchers and engineers, who are responsible for monitoring networks, analyzing incidents, and responding to security cases.
Security Operations Center (SOC)	A Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents. A SOC acts like the hub or central command post, taking in telemetry from across an organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside.
Security analyst / SOC analyst	The security analyst is an expert in tracking down active threats in an environment and their efforts are primarily focused on what's happening in the present. In traditional detection of threats, SOC analysts use a large quantity of tools that will automatically generate alerts for investigation and mitigation.
Threat analyst	A threat analyst specializes in monitoring and analyzing active as well as potential cyber security threats, while gathering useful intelligence throughout time. In contrast with the security analysts who are mostly reactive, threat analysis proactively hunt for threats.

Glossary

Term	Description
Cyber risk	An effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation.
Cyber threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
Attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses sensitive information; or an authorized user accesses sensitive information for another than authorized purpose.
Living-Off-The-Land Attack	Cyberattack which intruders use legitimate software and functions available in the system to perform malicious actions on it.

Glossary

Term	Description
IOCs (Indicators of Compromise)	IOCs are pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network. These bread crumbs can help Service Providers to detect malicious activity early in an attack sequence Let's take an example: • A publicly know malware that has been seen in the wild is identified by a specific hash, or connectivity to a specific IP, or does a change in a specific registry key, etc. Such information you can find over internet while researching any specific threat that you are interested in. • All of these artefacts, are called indicators of compromise and any trace of them found on a system hints that a workload is compromised and actions need to be taken. Finding an IOC on an workload can mean either that an attack is preparing or that an attack has taken place
Event	Occurrence or change of a particular set of circumstances within a system.
Incident	An event or series of events that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Alert	A brief, usually human-readable, technical notification regarding current security-relevant issue such as vulnerabilities, exploits, etc. Also known as an advisory, bulletin, or vulnerability note.
MITRE ATT&CK framework	The MITRE ATT&CK™ framework is a comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk. The aim of the framework is to improve post-compromise detection of adversaries in enterprises by illustrating the actions an attacker may have taken.

Glossary

Term	Description
NIST framework	The National Institute of Standards and Technology (NIST) framework is a best market standard framework that focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. More information: https://www.nist.gov/cyberframework
False positive	Incorrect flagging of something as malicious when it's not. **Analogy**: Mistaking a real bank client for a robber and discovering the truth after the guard catches him.
False negative	When a security system fails to identify a threat, something malicious is flagged as non-malicious. (Analogy: Not understanding that someone was a robber until after they leave the bank with the money.)
Detection types: Signature vs behavior vs intent	Signature-based technologies – Having a predefined repository of static signatures (fingerprints/hashes) that represent known threats. These threats are different from one another because of their unique coding. A threat is detected by the technology creating signatures for each file and comparing with the database of known bad signatures. Behavior technologies – Concerned with looking at known bad behaviors but blind to the intent of the attackers. Most of the time, they are associated with the techniques by which an attacker achieves it's goal/intent. Intent - Concerned with what is the objective of the attacker (regardless of the techniques used to achieve them)

Glossary

Term	Description
Known malware	Malware that is actively exploited in the wild, and therefore is part of antivirus databases. Can be detected with signature-based detection.
Unknown malware	New, previously unseen form of malware. Can be detected only with behavioral heuristics.
Advanced Persistent Threats (APTs)	Attacks that use continuous, sophisticated and highly evasive hacking techniques to gain unauthorized access to system and stay undetected for a prolonged period of time, with potentially destructive consequences
Zero-day malware	Malware that infiltrates the system through a zero-day vulnerability (a vulnerability that is exploitable, but the software vendor has not released a patch for it yet – the vulnerability can be known or unknown). Can be detected with behavioral heuristics.
Fileless attack	Fileless malware is a type of malicious software that uses legitimate programs to infect a computer. It does not rely on files and leaves no footprint, making it challenging to detect and remove. Can be detected with exploit prevention.
Polymorphic malware	A type of malware that constantly changes its identifiable features in order to evade detection
Obfuscation technique	Obfuscation techniques entail making malware more complex by design in order to mask identifiable features and evade detection
Exploit kit	An exploit kit or exploit pack is a type of toolkit cybercriminals use to attack vulnerabilities in systems so they can distribute malware or perform other malicious activities.