EDR

By Dr. Ashu Sharma

Intro to EDR: Landscape

- Today's organizations face huge challenges securing and protecting servers, networks, and digital assets.
- This goes double for mobile users, as they — and their laptops, tablets, and other devices — traipse all over the place.
- Also, more organizations are moving IT workloads to the cloud, leveraging hosted and SaaS models.
- With an expanded definition of endpoints that includes any connected device, physical or virtual, it's good that cybersecurity solutions are available to help IT security organizations cope.
- Such solutions offer protection, monitoring, and support to secure business-critical assets and quickly respond to a breach.

Intro to EDR: Landscape

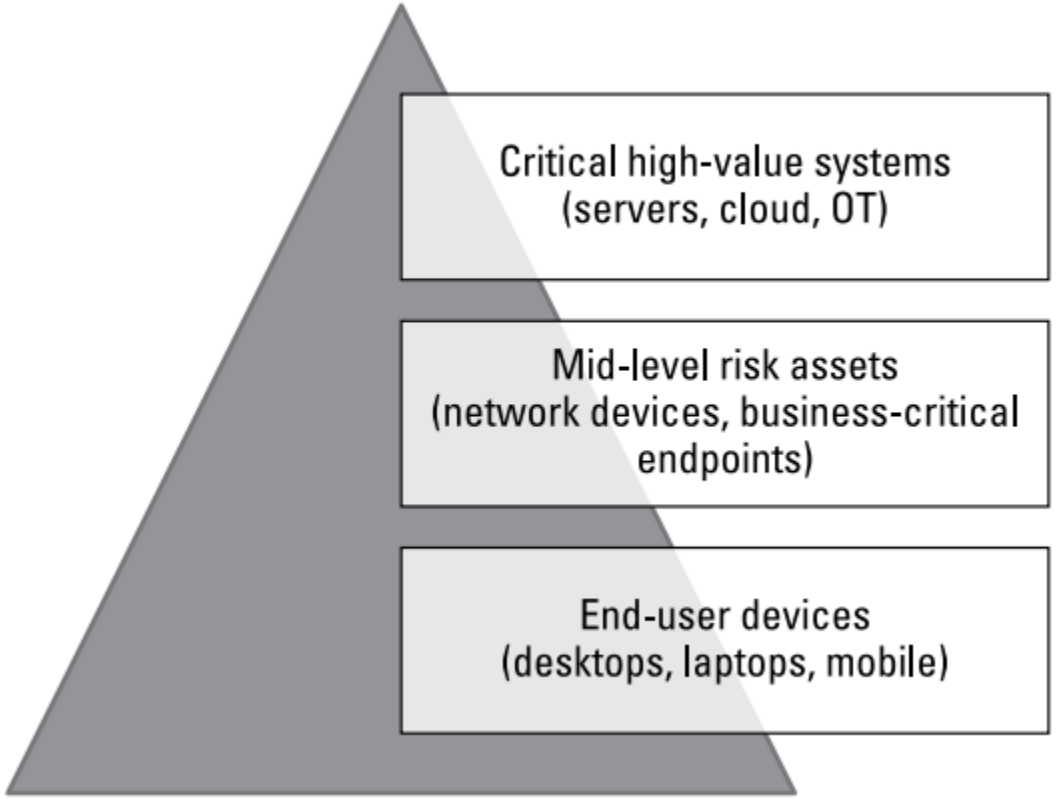
- An endpoint is any connected device used to access an organization's data and network. Traditionally, IT pros interpreted this as "anything with a CPU and a keyboard."
- we need to expand our definition of an endpoint to include servers, mobile devices, ATMs, medical gear, industrial systems, cameras and, yes, even cars.
- With more systems
  - — physical or virtual, on-premises or in the cloud
  - — accessing organizational data and networks,
  - the definition will be stretched even further — soon!

Intro to EDR: focus to secure

Security experts often talk about four elements when describing the security landscape.

- Asset: An organization's hardware, software, apps, and information that should be tracked and audited.
- Threat: A person, agent, or thing likely to inflict evil, damage, or loss.
- Risk: A characteristic or situation that involves exposure to disruption, damage, or loss.
- Exposure: A quality or characteristic in a system, service, or software that increases its vulnerability to attack or unauthorized access.

Intro to EDR: Pyramid of asset count and business value



EndPointSecurity

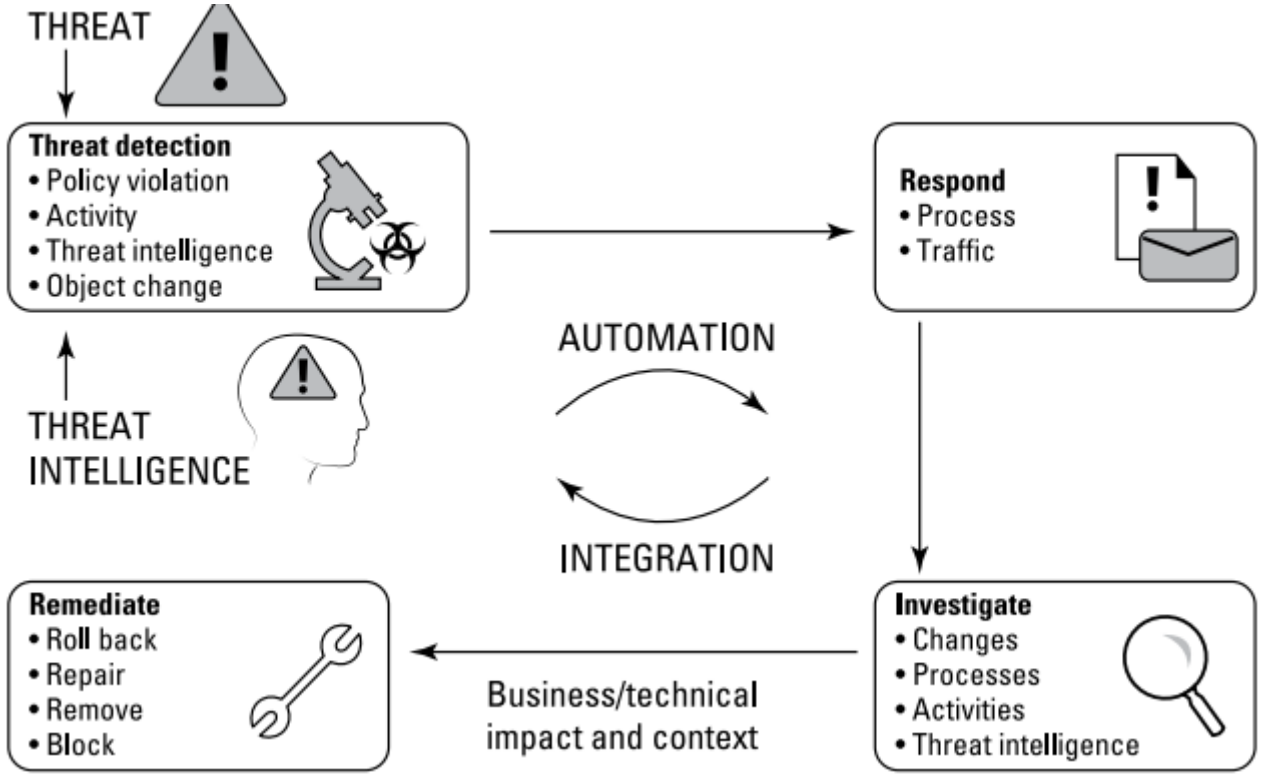
- Endpoint security starts with protecting and hardening devices — the endpoints — but doesn’t stop there.
- Broad, effective protection means endpoint security must also include ongoing
  - endpoint discovery,
  - monitoring,
  - assessment,
  - and prioritization to minimize the means and probable success of attacks on endpoint systems. This is called “the attack surface” in cybersecurity-speak.

Threat Intelegence

- Threat intelligence consists of evidence-based knowledge about an existing or emerging threat to assets designed to help guide a considered response to that threat.
- The knowledge can include security context data, indicators or signatures, implications, and actionable advice.
- Threat intelligence usually comes from security feeds that may also include actionable advice on how to automate an appropriate response to a threat.

Requirements for EDR

- Endpoint Detection and Response (EDR) systems demand at least four types of capability



Requirements for EDR

- Endpoint Detection and Response (EDR) systems demand at least four types of capability
- . Systems must
  - ✓ Be able to detect security incidents as they occur.
  - ✓ Contain the incident at the endpoint.
  - ✓ Support investigation of the incident.
  - ✓ Provide mechanisms to remediate affected endpoints.

Cyberthreat Gap

- The Detection Gap: The amount of time that passes from when a breach occurs until the organization discovers its presence and identifies it conclusively. Industry reports say this gap can sometimes be as long as 18 months.
- The Response Gap: The amount of time an organization takes to identify the scope of a breach and to contain its damage. Industry reports indicate that this gap can take four months or longer to be closed.
- The Prevention Gap: The time needed to implement measures that avoid a repeat of the breach, or a similar breach. This is an open-ended time frame, and can take months or years to close, depending on the nature of threat involved.

Detection and Response: Needs

- IOC detection: This method identifies changes in the system state and compares it to internal IOC (Indicator of Compromise). Sometimes it may be necessary to send the state changes or a suspect file to a threat intelligence service for analysis and evaluation.
- Anomaly detection: Changes to a system from a known good base configuration can also help to identify threats.
- Behavior detection: Identifying bad, odd, or illicit behavior on a system can indicate a threat. Logging such events helps with threat identification and may identify the time when an incident occurred or began.
- Policy violations: System changes (for example, scheduled maintenance or upgrades, new software installs, new users, or account changes) outside approved configuration windows may indicate a threat actor at work

RDR:The value of speed and accuracy

- Case study 1: A firm implemented an EDR solution to reconcile changes on its endpoints. When a pen-test team exploited a vulnerability on a web server to drop an exploit kit, the change was detected by the EDR system, reconciled with ticketing (as a “bad” change) within minutes, and escalated to an incident response team. Case closed (before it really got going, in fact)!

RDR:The value of speed and accuracy

- Case study 2: A gaming company's SIEM received "404, page not found" logs from approximately 20 percent of all transactions on its web servers. At first, the company thought it was a DDoS attack, but their firewalls and network intrusion detection system's events didn't support that theory. Then they thought it was an exploited vulnerability, but their vulnerability scanner revealed nothing relevant. Finally, using EDR with configuration management, they determined that a patch had been deployed improperly on two systems in a ten-server cluster by looking at the system state history. The patch was redeployed and the error disappeared!

Automate Threat Protection

- a top-notch EDR system can detect, analyze, and verify threats, include brand-new ones (called zero-day threats), and truly nasty ones (called advanced persistent threats).
- Changes to system state can be compared automatically to IOCs, and suspicious files can be automatically uploaded and “detonated” in isolated test areas called “sandboxes.”
- Another key component in a capable EDR system is called proactive discovery. Such a component continuously monitors the network to discover all endpoint assets and applications. Security analysts can then automatically classify the assets or applications by examining their attributes, which come from the ongoing inventory. Analysts can scan those assets for vulnerabilities, which may then be remediated. For example, patches or updates may be needed, or malware protection can be added or updated.

What is threat intelligence?

- Threat intelligence provides data that you did not already have (such as reputation scoring, attack tools, threat actors, and so on).
- It provides data (or analysis of that data) that helps you make more and better decisions about defense and helps you figure out what else to look for, or what proactive measures to take.

Making best use of threat intelligence

- Automate what you can: Automated attacks need automated defenses.
- Save analyst resources for subtle, complex data that helps you pinpoint threats that are most likely to affect your organization negatively.

Making best use of threat intelligence

- Threat intelligence is widely available from many commercial and community sources — for example, Cisco, Check Point, Palo Alto Networks, Lastline, Blue Coat, iSIGHT Partners, CrowdStrike, Soltra, and ThreatStream, among many others. Every organization needs to decide which threat intelligence services are most suitable for it, based on criteria such as origin, freshness, speed and scale, relevance, accuracy, confidence, completeness, and consumability

Making best use of threat intelligence

- Advanced EDR systems integrate with multiple independent threat intelligence services and support concurrent feeds for automated threat detection and validation. Because threat intelligence drives EDR (and much of enterprise security defenses), these decisions are vitally important. Intelligence feeds should be an important part of the conversation with any prospective EDR system vendor.

Making best use of threat intelligence

- By itself, threat intelligence is interesting and provides a sense of context. But it’s what one does with threat intelligence that really counts, and that’s where the rubber meets the road with EDR.

- A recent report from the Enterprise Strategy Group (ESG) identified a lack of integration of threat intelligence programs into enterprise collaboration, communication, and IT workflows as a chief shortcoming for in-house security intelligence programs.

- Prioritize the threat intelligence that’s relevant to your endpoints — and the rest of your security infrastructure — and act on high priority items ASAP!

Advanced Detection

- Metadata based ML: using meta data about samples
- Behaviour-based ML: identify new threats with process trees and suspicious sequences
- AMSI- pared ML: Detect fileless and in memory attack used paired client and cloud ML
- File classification ML: Detect new malware by machine learning known malwares
- Detonation-based ML: Catches new malware by detonating unknown files
- Reputation ML: detect by bad reputation whether direct or by association
- SMART Rules: Blocks threats using expert-written rules

Advanced Detection

- Correlated Post-breach detection
- Investigation experience incident
- Advanced hunting
- Response actions (+edr blocks)
- Deep File Analysis
- Live Response
- Threat analytics