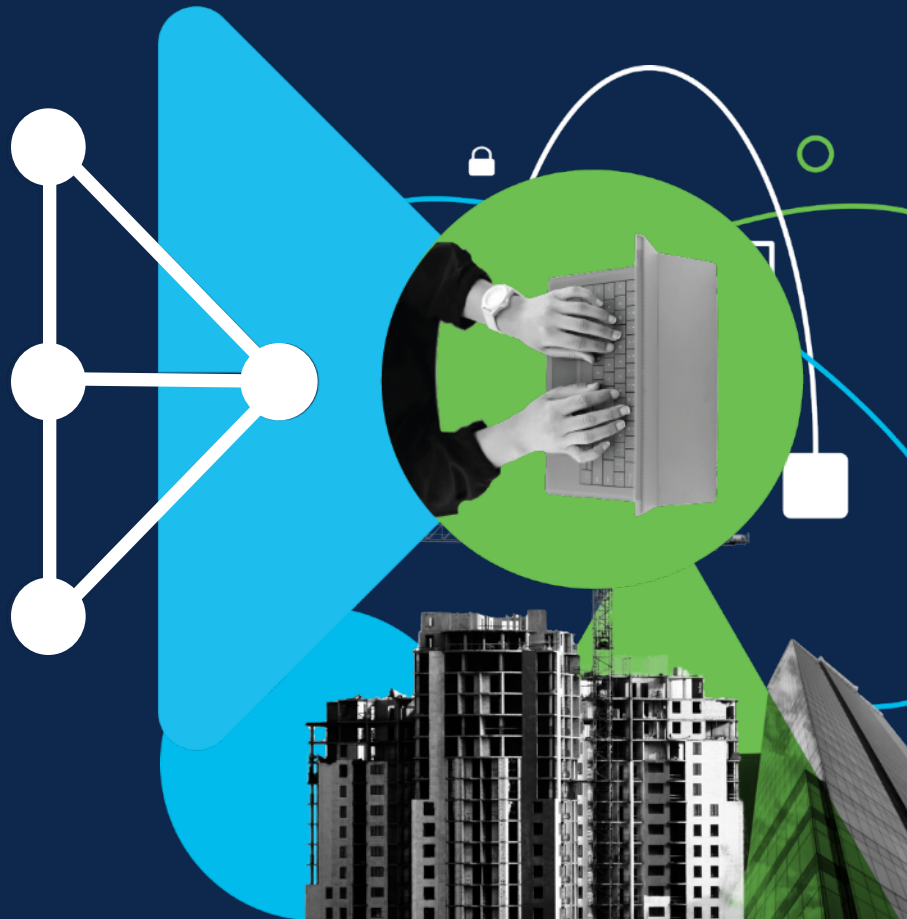
CISCO SECURE

CISCO The bridge to possible

Endpoint Detection and Response (EDR)



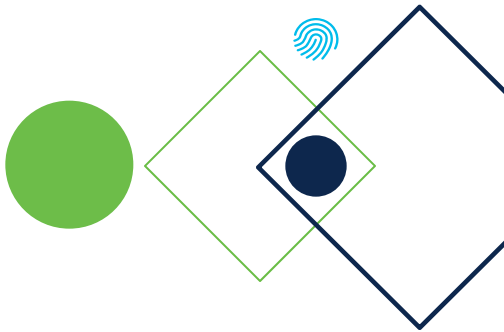
Mac Tetreault
Technical Solutions Architect - Security
January 2023

Agenda

- What is it?
- Endpoint Security in the Healthcare
- EPP/EDR as part of XDR
- Considerations when evaluating
- Questions

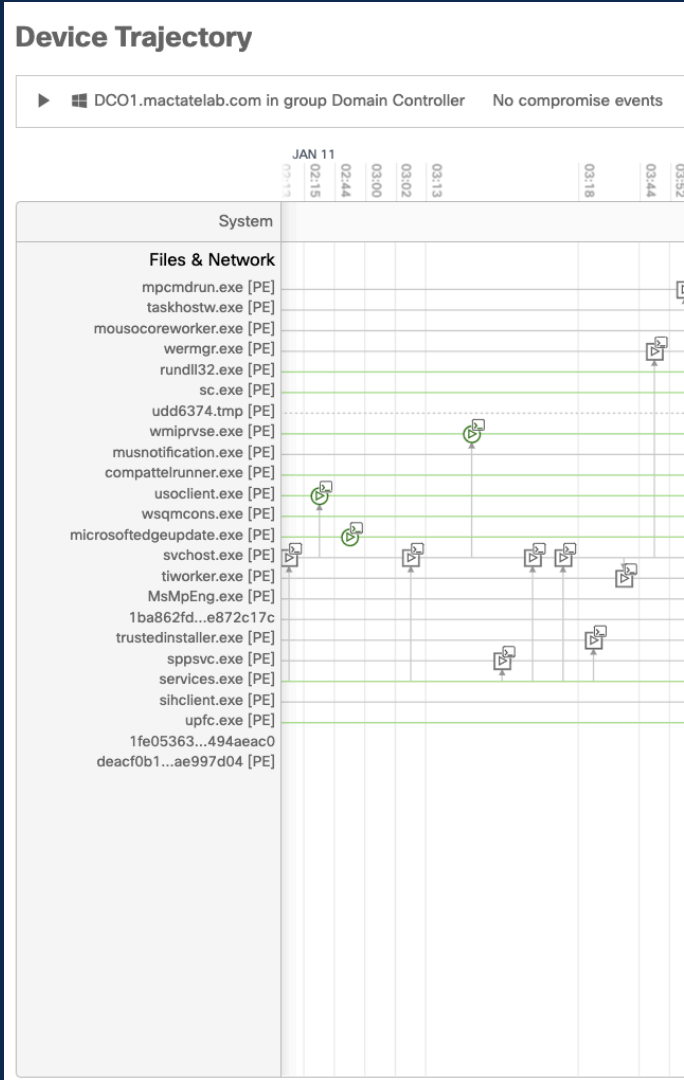
A quick history on endpoint security…

- 1990's - Antivirus is born - The rise of the internet era
- Early 2000's - Antivirus gets some help – patch management, encryption, Data Loss Prevention, host-based firewalling
- 2010-ish – Next Generation AV– Using artificial intelligence/Machine Learning methods to identify malware without relying on signatures
- 2013 – EDR concept is born – Gartner coins the term



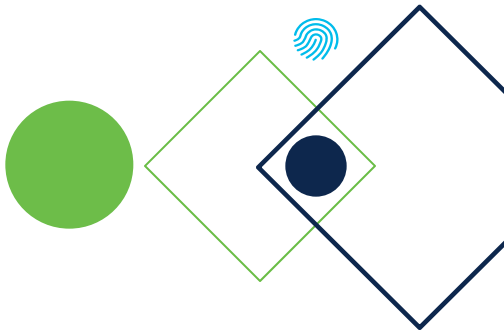
How is EDR different?

- Designed to detect, alert, and contain advanced threats
  - Behavior analysis and tracking
  - Detecting file-less attacks
  - Terminating or blocking malicious processes, shell commands, or network activity
- Deep insights into device-level forensic data
  - Process Visibility
  - Network Connections
- Response Actions
  - Device Quarantining/Isolation



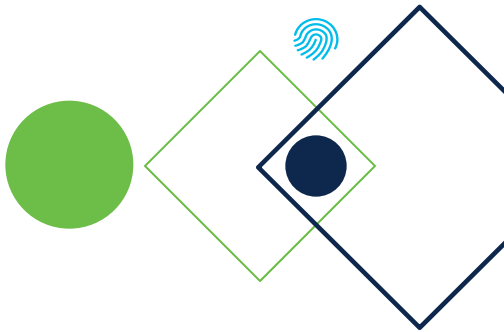
EDR in Healthcare Environments

- The standard for workstation, laptop, mobile and server endpoint security. (Anything that can accept a software agent - Windows, Mac, Linux, mobile)
- Many devices are mission critical and are used to access sensitive EMR data – protection is critical
- Devices commonly leave the network (Staff bringing devices home or to other facilities)
- Many devices in Healthcare CAN NOT accept a software agent - EDR is a piece of the healthcare security puzzle.



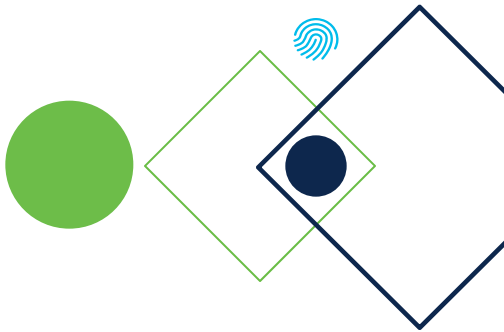
Don’t get confused - EDR is not XDR! (eXtended detection and response)

- XDR is the combination of EDR, Network Detection and Response (NDR), Email Security, Identity and Access Management (IAM) activity, Firewall, and more.
- XDR brings data from multiple sources together to provide cross-platform detections and response functionalities via product integrations
- XDR is highly valuable in Healthcare environments as it provides visibility, detection, and response for areas of the environment not protected by EDR

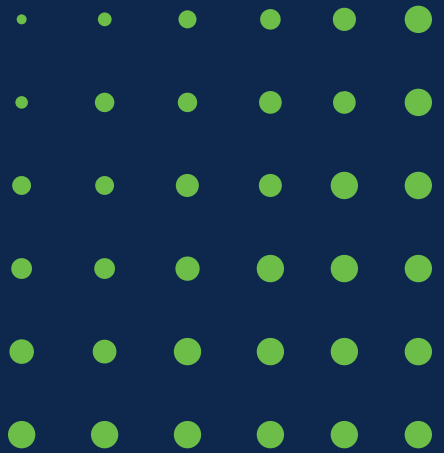


Considerations

- Would your organization benefit from Managed Detection and Response (MDR) or Managed EDR (MEDR)?
  - 24x7 ”eyes on glass”
  - Expert assistance with monitoring on your behalf
- How does EDR fit into you existing architecture?
  - Ingestion into your SIEM (Security Incident/information and Event Management) if applicable
  - Integration with other products to form an XDR architecture
  - Supportability for your OS-types and versions
- Incident Response (IR)
  - Do you pay for an IR retainer? Is the IR firm able to leverage your EDR or choice?



Questions?



Contact Info:

Mac Tetreault
matetrea@cisco.com
www.linkedin.com/in/mackenzietetreault/