EDR Exploits to Indicators
Staying at the forefront of Cybersecurity protection
What drives the desire for EDR products

Endpoint Detection and Response enables the discovery of unknown threats and provides the ability to respond in real-time.
What are customers so afraid of?

- **Data Breaches**
  - 67% over 5 years

- **Ransomware**
  - $20 Billion

- **146 Billion Records**
  - Will be exposed in the next 5 years

- **86% of Phishing Attacks**
  - Target the United States

- **60%**
  - Of Americans have been exposed to fraud

- **540 Million**
  - Facebook users exposed in breach

- **Microsoft Office**
  - Microsoft office files accounted for 48% of all malicious email attachments in 2018

Is my AV good enough? What more should I be doing?

Understanding the Attack Lifecycle

- **Initial Compromise**: The attacker successfully execute malicious code on one or more systems.
- **Establish Foothold**: The attacker ensures remote access to a recently compromised system.
- **Escalate Privileges**: The attacker gains greater access to systems and data than was initially available.
- **Complete Mission**: The attacker accomplishes their goal.

**Maintain Persistence**: The attacker ensures continued access to the victim environment.

**Move laterally**: The attacker uses the established foothold to move from system to system.

**Internal Recon**: The attacker explores the victims environment.

**Critical system recon**
- System, active directory and user enumeration
What does an EDR product do

Protect

Prevent attacks and proactively secure known vulnerabilities

Detect

Detect active attacks and identify potentially malicious behaviors

Respond

Rapidly investigate and remediate incidents to minimize impact
## How does it work

<table>
<thead>
<tr>
<th>Endpoint Observation</th>
<th>Anomaly and Threat Detection</th>
<th>Investigation Tools</th>
<th>Containment and Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process activity</td>
<td>Threat intel feeds</td>
<td>Situational awareness</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>Confirmed attacks</td>
<td>Who/What/Where/When</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Suspect executables</td>
<td>Assets at risk</td>
<td></td>
</tr>
<tr>
<td>File system</td>
<td>Admin hunting</td>
<td>Scope of attack</td>
<td></td>
</tr>
<tr>
<td>Registry</td>
<td>Suspect activities</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Activity map</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deep insight</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>File and Device Forensics</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reputation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Isolation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quarantine</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Removal</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process Kill</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Blocking</td>
<td></td>
</tr>
</tbody>
</table>
Top 5 Reasons your customers need EDR

They don’t know their current security risks
They can not see the suspect activity that is happening
They have very limited response actions to threats
Existing staff are already overloaded and lack deep security skills
They can’t improve if they don’t understand what happened and why
Having confidence in your Security Posture

Are we secure right now?
What are our blind spots?

EDR should provide a clear view into the current situation and ongoing risks
Detecting attacks that have gone unnoticed

What are the top indicators of compromise that I should look at first

- Suspect executables
- Use of administration tools
- Persistence events
- Data transfers
- Suspect Authentications
The ability to respond to active threats

Fast response requires powerful but easy to use tools

- Insight should be easy to acquire
- Actions should be intuitive
- Do no harm
Augment existing staff skills

Complex tools will not be used or understood to their potential
The cost of ‘expert staff’ is prohibitive
Any solution must be usable by the staff already available

Figure 5: Staff knowledge was cited as the top reason why organizations have not adopted an endpoint detection and response (EDR) solution (Source: Sapio study in conjunction with Sophos, October 2018)
Understanding how an attack happened

Deep forensics knowledge of an attack must be available for the experts and still usable by the novice
The Gap

BENIGN
[Allow]

MALICIOUS
[Block]
SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.