Endpoint Protection : Last line of defense?

First TC
Noumea, New Caledonia 10 Sept 2018

Raja Azrina Raja Othman
Independent Information Security Advisor

MSc Information Security & Computer Crime
BSc Computer Engineering
Co-founder of MyCERT
Date: 10 Sept 2018

OVERVIEW

UNDERSTANDING ENDPOINT SECURITY AND THE BIG PICTURE

- Rapid development in **security technology** requires understanding on how the many solutions **work together**, **not against each other**.

- Good understanding of technology allows better design and implementation when:
  - Integrating Security Controls in a new infrastructure, or
  - Incorporating new or optimizing existing security controls in response to recent threats.

- Understanding the role of **Endpoint Security Controls** as the last line of defense.

CYBER SECURITY IS A CEO, NOT CIO ISSUE

THE BUSINESS IMPACT OF CYBER CRIME IS OVERWHELMING

Cyber threats are a material risk to your business

200+ DAYS

Median number of days attackers are present on a victims network **before detection**

Source Microsoft Advanced Threat Analytics

$3 TRILLION

Impact of loss of **productivity and growth by 2020**

Source : McKinsey Risk and Responsibility in Hyperconnected World Report 2014

$4 MILLION

Average **cost of a data breach** (up 29% since 2013) [383 Org in 12 countries]

Source : 2016 Ponemon Institute Cost of Data Breach Study

Attacks are fast, efficient, and easier to implement

50%

of those who open phishing messages, click attachments **within the first hour**

Source Microsoft Advanced Threat Analytics

CHANGES IN CYBER THREAT ?

MALWARE | SELF PROPAGATE | DISRUPT | PERSISTENT

Blaster Worm
Discovered: **August 11, 2003**

- Propagates via network (**network worm**)
- **Scans** and connect on TCP port 135
- **Exploit** MS Windows DCOM RPC Interface Buffer Overrun Vulnerability.
- **Date trigger payload** that launches DDoS SYN flood against windowsupdate.com
- Sends large amount of data sufficient to overrun the buffer
- Gain shell on TCP port 4444 - **backdoor**
- Invoke 'tftp.exe' download
- System to reboot in order to launch

Created by an 18-year-old from Minnesota, sentenced to 18mo prison term.

Wannacry Ransomware
Discovered: **May 12, 2017**

- Propagates via network (**network worm**)
- **Scans** and exploit SMB protocol
- Eternal Blue **exploit**
- Install **backdoors** (Double Pulsar)
- **Encrypting data and demanding ransom** payments in Bitcoin
- Includes Kill switch – (prevented infected computers from spreading WannaCry further).
- Affected more than 200,000 computers across 150 countries (manufacturing plants, hospitals)
- System reboot/bluescreen on certain platform.

Created by a North Korean computer programmer , claimed to be state-sponsored attack.

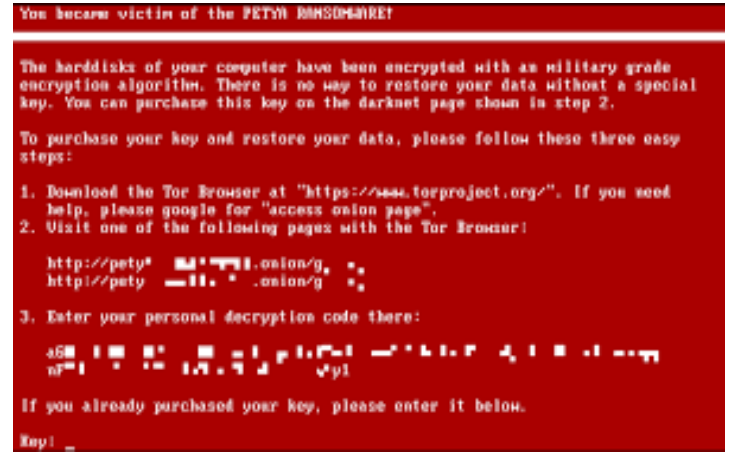
DOJ Charges North Korean in Sony Hack, Wanna Cry Attack
(September 6, 2018)

The US Department of Justice (DOJ) has charged Park Jin Hyok, a North Korean computer programmer, in the 2014 attack against Sony Pictures, a 2016 theft from Bangladesh Bank, and the 2017 Wanna Cry malware attack. The complaint alleges that Park carried out the attack against Sony Pictures on behalf of the North Korean government; it also links Park to the Lazarus Group, which is believed to be involved in the Wanna Cry attack and a Bangladesh Bank theft.

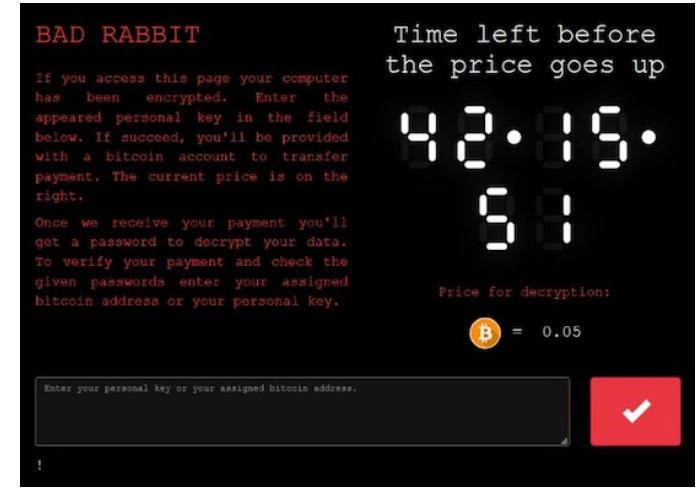
RECENT INCIDENTS/VULNERABILITY HIT ENDPOINTS

RANSOMWARE | HARDWARE LEVEL VULNERABILITY

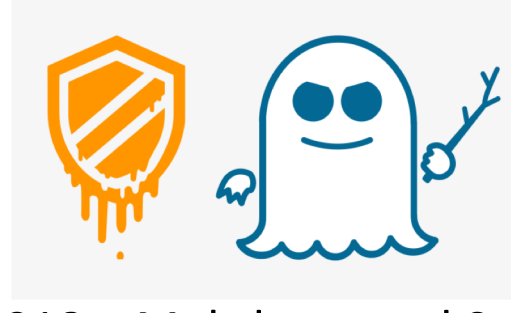
May 2017 - Wannacry Ransomware



June 2017 - NotPetya



Oct 2017 – Bad Rabbit

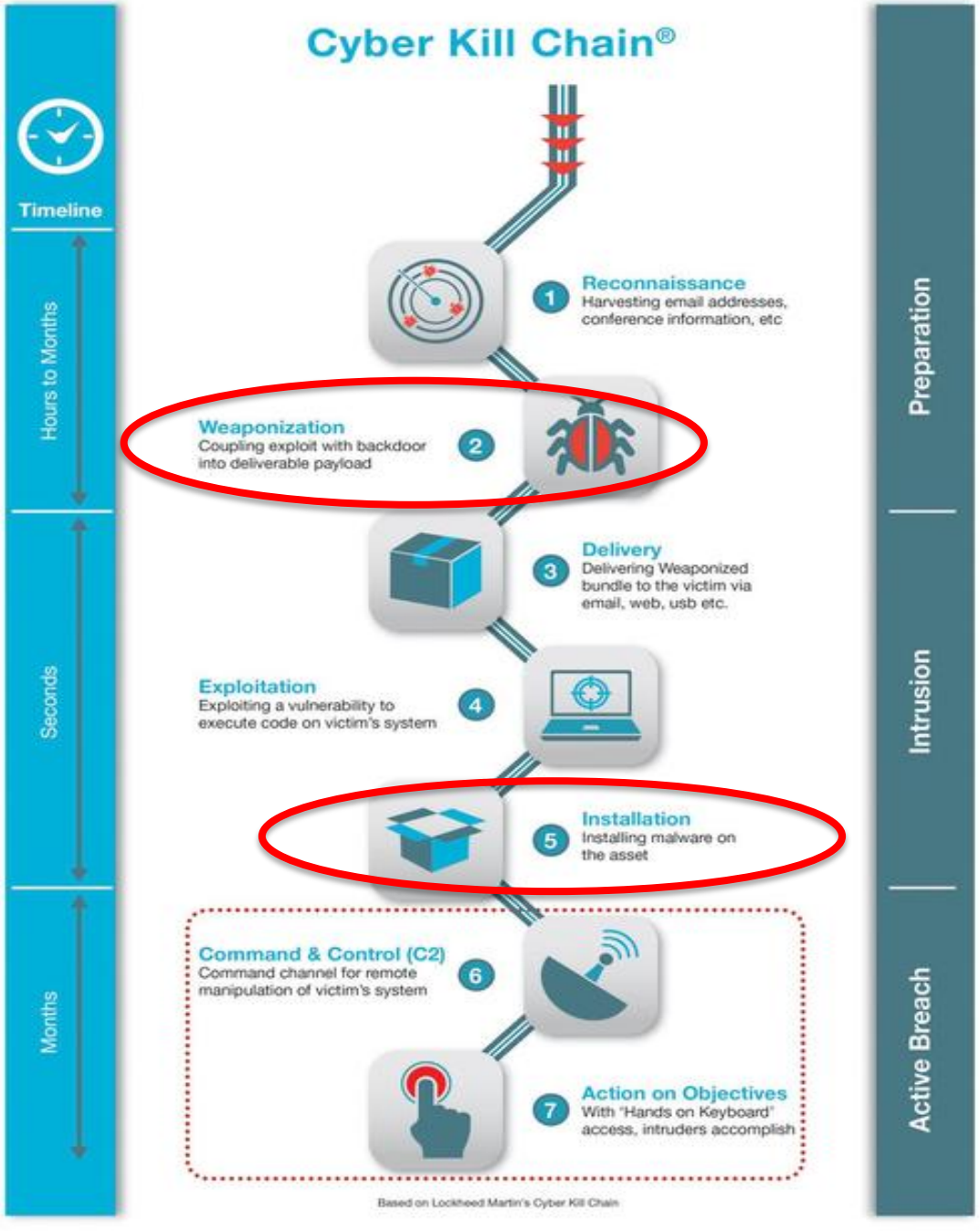


Jan 2018 – Meltdown and Spectre

Kernel memory vulnerability allow memory exploit at hardware level

ANATOMY OF A HACK

AND WHAT'S AT STAKE

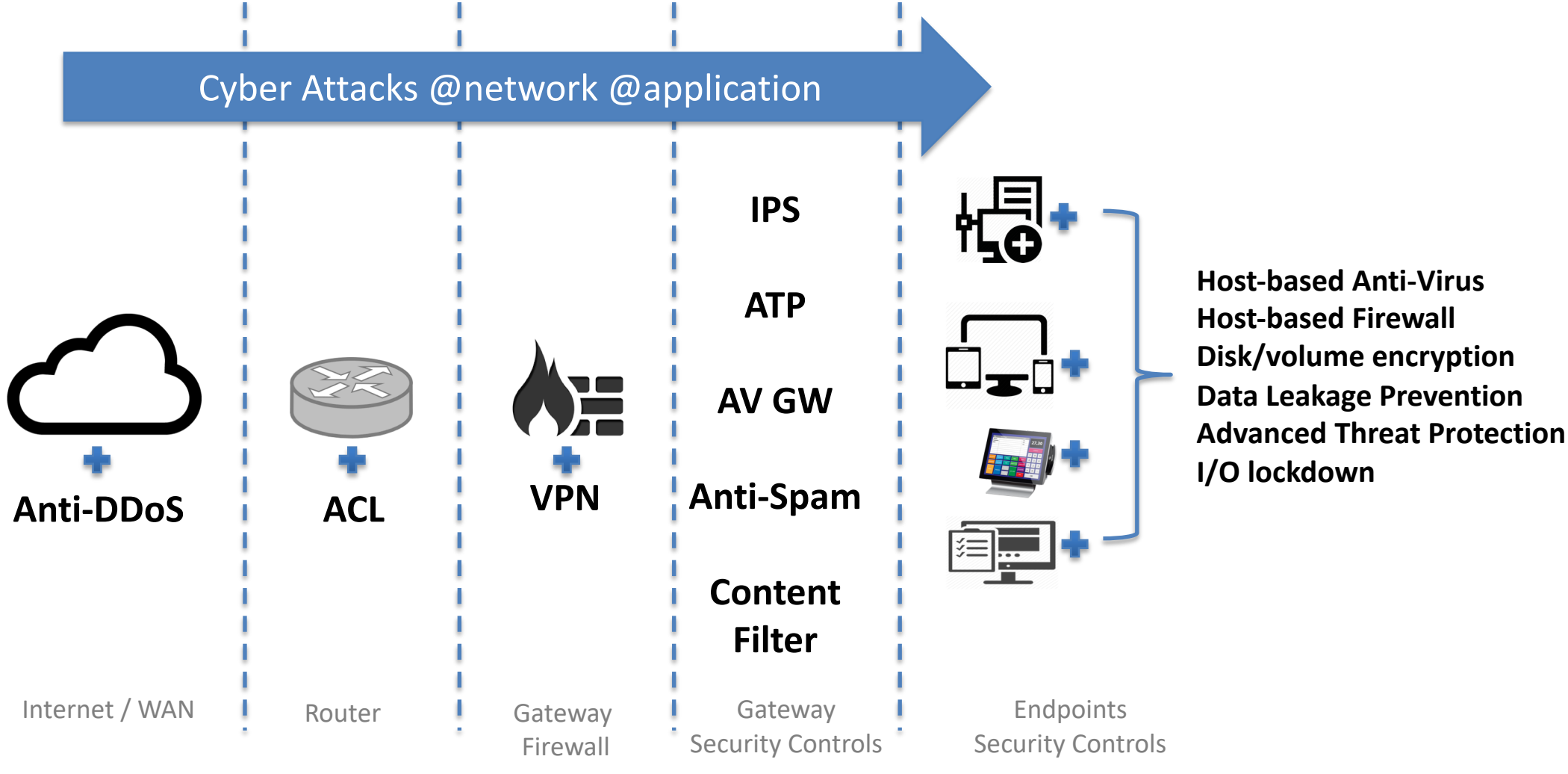


Objective of compromise:

- To **steal** information, credentials.
- To **weaponize** a compromised host as launching pad, man in the middle.
- To **ransom** the victim.
- To gain **unauthorized use** of computing resources – crypto mining, spam relay, malware hosting

MULTI LAYERED ATTACK MITIGATION

MULTI-LEVEL SUBVERSION TO ULTIMATELY TARGET ENDPOINTS



BLACKLISTING | WHITELISTING | LEARNING

SECURITY CONTROLS

Blacklist: allows everyone access except those listed in the blacklist

Whitelist: denies everyone access except those listed in the whitelist

Blacklisting Technology

- Block/Blacklist selected files/applications/URL/domain/content based on certain known fact/signature.
- IPS, Firewall, Content Filter, DLP, Anti Malware

Whitelisting Technology

- Application Whitelist - Allow installation of only selected files/application based on certain known criteria that is set as policy.
- Network Traffic Whitelist – Access Control List

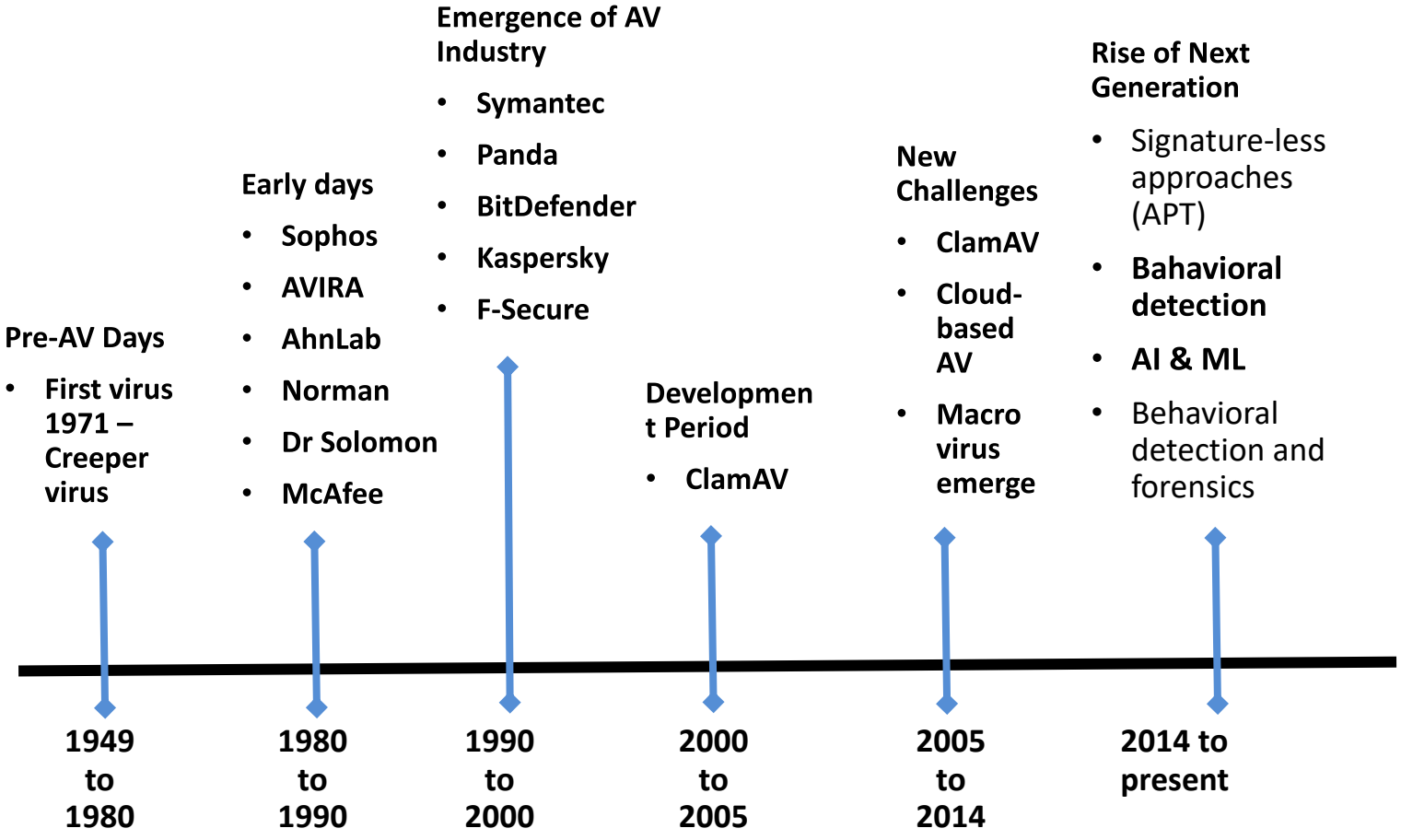
Learning Technology

- Conduct analysis to determine anomaly, based on algorithms such as behavioral, heuristic, Artificial Intelligence, Machine Learning and more
- Example: Anti-spam, ATP, Anti-DDoS

ANTI MALWARE EVOLVED INTO ENDPOINT PROTECTION

DETECTING THE KNOWN AND UNKNOWN (ZERO-DAY)

The anti malware technology had over decades relied on **signature based detection**. The next generation Endpoint Protection includes **Behavioral Detection, Artificial Intelligence (AI) and Machine Learning (ML)**. These require heavy processing. Most desktops in critical sector are running End of Life systems.



Challenges

- Viruses, Worms, Trojans **mutate** - polymorphic code change every time it runs –signature fails.
- Gartner and Forrester has described AV as **ineffective** and **outdated**.
- **False Positive** when doing app updates
- **Performance degrade** due to size of heavy processing.
- **Conflict with encryption software**.

ENDPOINT TARGETS

INTERNET FACING SERVERS | END USER COMPUTERS

SERVERS

- WEB Server Injection Attacks
- Mail Server
- AV Server
- Directory Service
- Domain Name Server

END USER

- Via Phishing /Spam
- Via Web Drive-by attacks
- Via Network Scanning
- Via Folder Sharing
- Via File Transfers
- Via Tech Support Advertisement

METHODS OF APPLICATION WHITELISTING

WHAT TO LOOK FOR IN APPLICATION WHITELISTING

- Critical systems require only limited function to conduct daily operations and should operate based on trusted applications.

- Implementing Top 4* security controls at endpoints will mitigate at least 85% of the intrusion techniques. Application whitelisting is one of the Top 4 controls.

Methods used by most application whitelist solution:

- **File Hash** - maintaining **hash** of the whitelisted files

- **Digital Certificates** - trust certain publishers of software. Most software vendors digitally sign their applications. This digital signature can be used by many whitelisting vendors to automatically approve software from a specific vendor into the whitelist.

- **Trusted updaters** – e.g. predefined accounts, processes or network locations which are automatically trusted. Automatic trust means that an application can be installed and automatically added to the enterprise whitelist.

- **Monitoring mode | Incident Response -** This provides visibility into the executables which are running on end user systems and can be used to detect, confirm and respond to attacks.

*TOP 4 STRATEGIES TO MITIGATE TARGETED CYBER INTRUSIONS: MANDATORY REQUIREMENT EXPLAINED by Australian Signals Directorate (ASD) assesses that https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

BRINGING IT ALL TOGETHER

TOWARDS EFFECTIVE SECURITY CONTROLS AGAINST PAST, CURRENT AND EMERGING THREATS

- Make security controls **work together**, **not against each other**.

- Don’t just settle – **Measure effectiveness** of Endpoint controls and **make improvements**.


Thank you