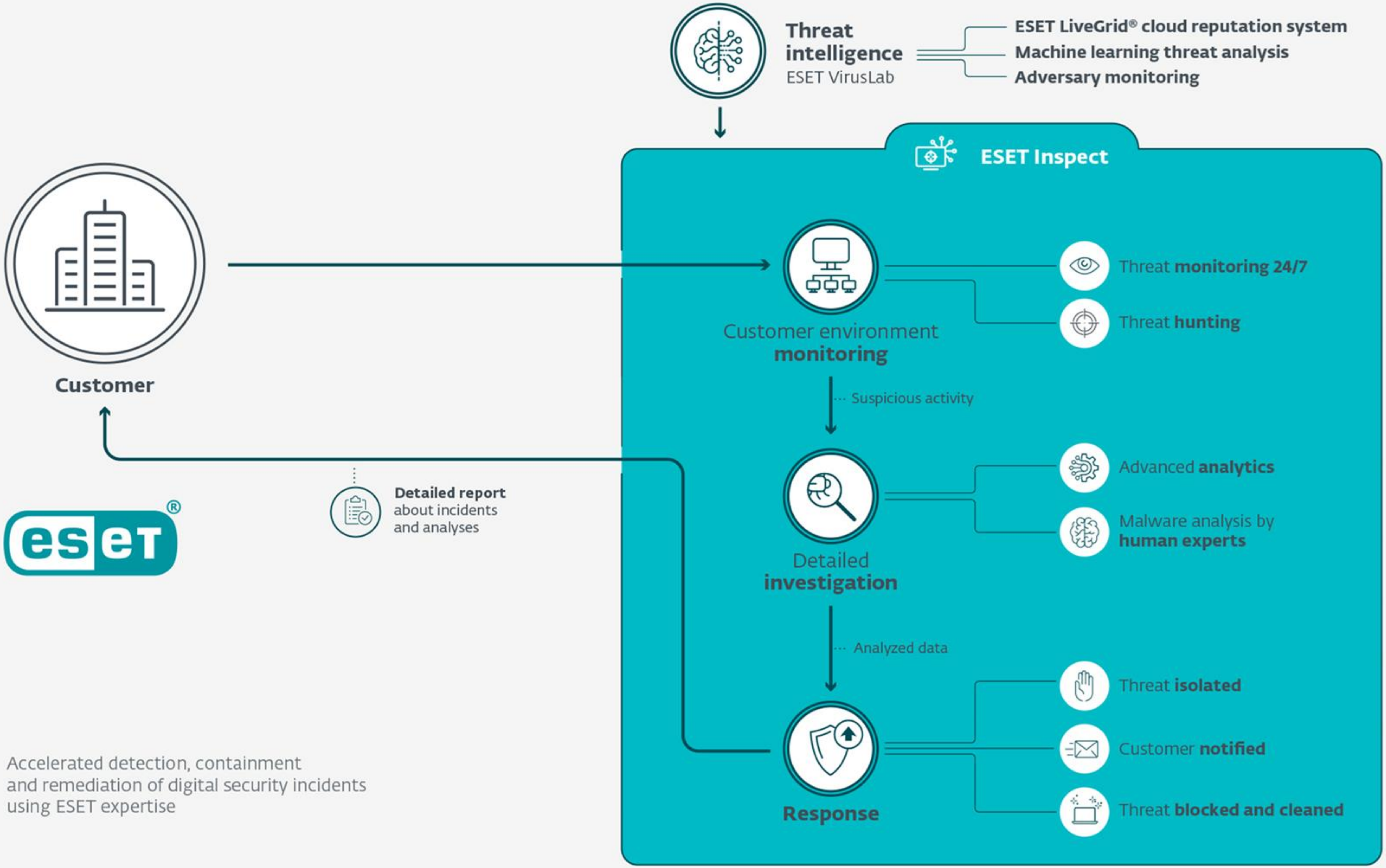
ESET Inspect

Filip Maliarik
Senior sales engineer
filip.maliarik@eset.com



Accelerated detection, containment
and remediation of digital security incidents
using ESET expertise

ESET OUTBOUND INTEGRATIONS

SIEM

Splunk

elastic
The Search AI Company

Microsoft
Microsoft Sentinel

wazuh.

IBM QRadar

XDR

wazuh.

STELLAR
CYBER®

ARCTIC
WOLF

SOAR

BLOCKAPT™

mindflow

THREAT INTEL

ANOMALI

THREATQUOTIENT™
A SECURONIX COMPANY

IBM QRadar

OpenCTI
Filigran

elastic
The Search AI Company

MSP: PSA/RMM

ATERA

CONNECTWISE
PSA

HALOPSA

ConnectWise
Automate™

Kaseya®

datto

N-ABLE

ninjaOne

SuperOps

eset® INSPECT

Highly customizable
Endpoint Detection & Response

FOR PARTNERS

ESET INSPECT

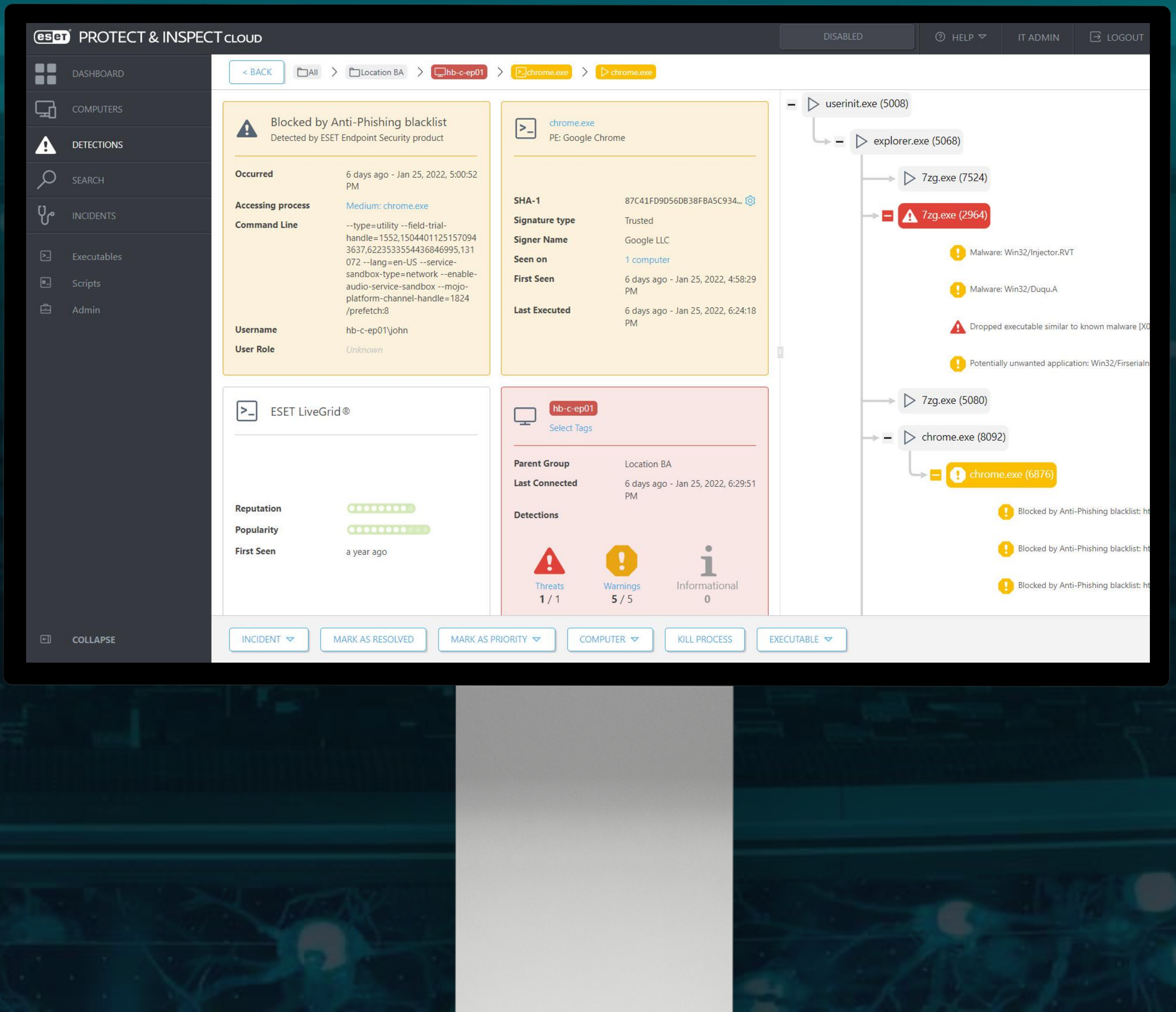
This session

What is ESET Inspect and what does it do

1. Main capabilities
2. Dashboards

Incident investigation

- triage
- investigation
- response
-



Blocked by Anti-Phishing blacklist
Detected by ESET Endpoint Security product

Occurred: 6 days ago - Jan 25, 2022, 5:00:52 PM
Accessing process: Medium: chrome.exe
Command Line: --type=utility --field-trial-handle=1552,15044011251570943637,6223533554436846995,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1824 /prefetch:8
Username: hb-c-ep01\john
User Role: Unknown

chrome.exe
PE: Google Chrome

SHA-1: 87C41FD9D56DB38FBA5C934...
Signature type: Trusted
Signer Name: Google LLC
Seen on: 1 computer
First Seen: 6 days ago - Jan 25, 2022, 4:58:29 PM
Last Executed: 6 days ago - Jan 25, 2022, 6:24:18 PM

ESET LiveGrid®

Reputation: ●●●●●●●●
Popularity: ●●●●●●●●
First Seen: a year ago

hb-c-ep01
Select Tags

Parent Group: Location BA
Last Connected: 6 days ago - Jan 25, 2022, 6:29:51 PM
Detections

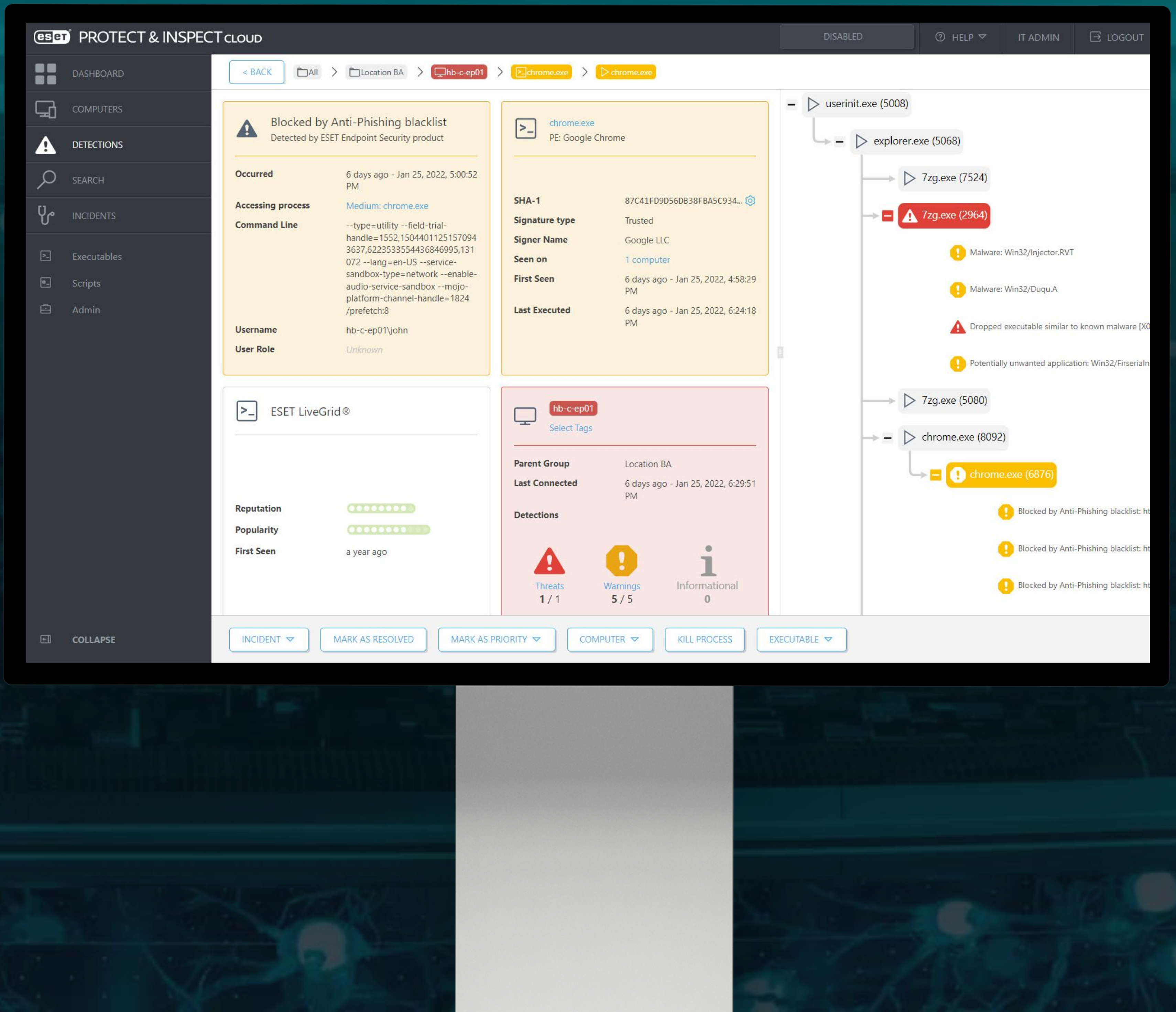
Threats 1 / 1
Warnings 5 / 5
Informational 0

userinit.exe (5008)
explorer.exe (5068)
7zg.exe (7524)
7zg.exe (2964)
Malware: Win32/Injector.RVT
Malware: Win32/Duqu.A
Dropped executable similar to known malware [X0
Potentially unwanted application: Win32/FirserialIn
7zg.exe (5080)
chrome.exe (8092)
chrome.exe (6876)
Blocked by Anti-Phishing blacklist: ht
Blocked by Anti-Phishing blacklist: ht
Blocked by Anti-Phishing blacklist: ht

ESET INSPECT

Key features

- Collects real time events
- Provides extensive filtering and sorting
- Uses ESET reputation system
- Custom notification rules
- Blocking and remediation
- Designed for threat hunting



Blocked by Anti-Phishing blacklist
Detected by ESET Endpoint Security product

Occurred	6 days ago - Jan 25, 2022, 5:00:52 PM
Accessing process	Medium: chrome.exe
Command Line	--type=utility --field-trial-handle=1552,15044011251570943637,6223533554436846995,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1824 /prefetch:8
Username	hb-c-ep01\john
User Role	Unknown

chrome.exe
PE: Google Chrome

SHA-1	87C41FD9D56DB38FBA5C934...
Signature type	Trusted
Signer Name	Google LLC
Seen on	1 computer
First Seen	6 days ago - Jan 25, 2022, 4:58:29 PM
Last Executed	6 days ago - Jan 25, 2022, 6:24:18 PM

ESET LiveGrid®

Reputation	
Popularity	
First Seen	a year ago

hb-c-ep01
Select Tags

Parent Group	Location BA
Last Connected	6 days ago - Jan 25, 2022, 6:29:51 PM

Detections

Threats	Warnings	Informational
1 / 1	5 / 5	0

```
userinit.exe (5008)
  explorer.exe (5068)
    7zg.exe (7524)
    7zg.exe (2964)
      Malware: Win32/Injector.RVT
      Malware: Win32/Duqu.A
      Dropped executable similar to known malware [X0
      Potentially unwanted application: Win32/Firserialn
    7zg.exe (5080)
    chrome.exe (8092)
      chrome.exe (6876)
        Blocked by Anti-Phishing blacklist: ht
        Blocked by Anti-Phishing blacklist: ht
        Blocked by Anti-Phishing blacklist: ht
```

FOR PARTNERS

ESET INSPECT

The ESET Difference

Complete Prevention, Detection, and Response

Solution from a Security First Vendor

Prevention is better than cure

Detailed Network Visibility

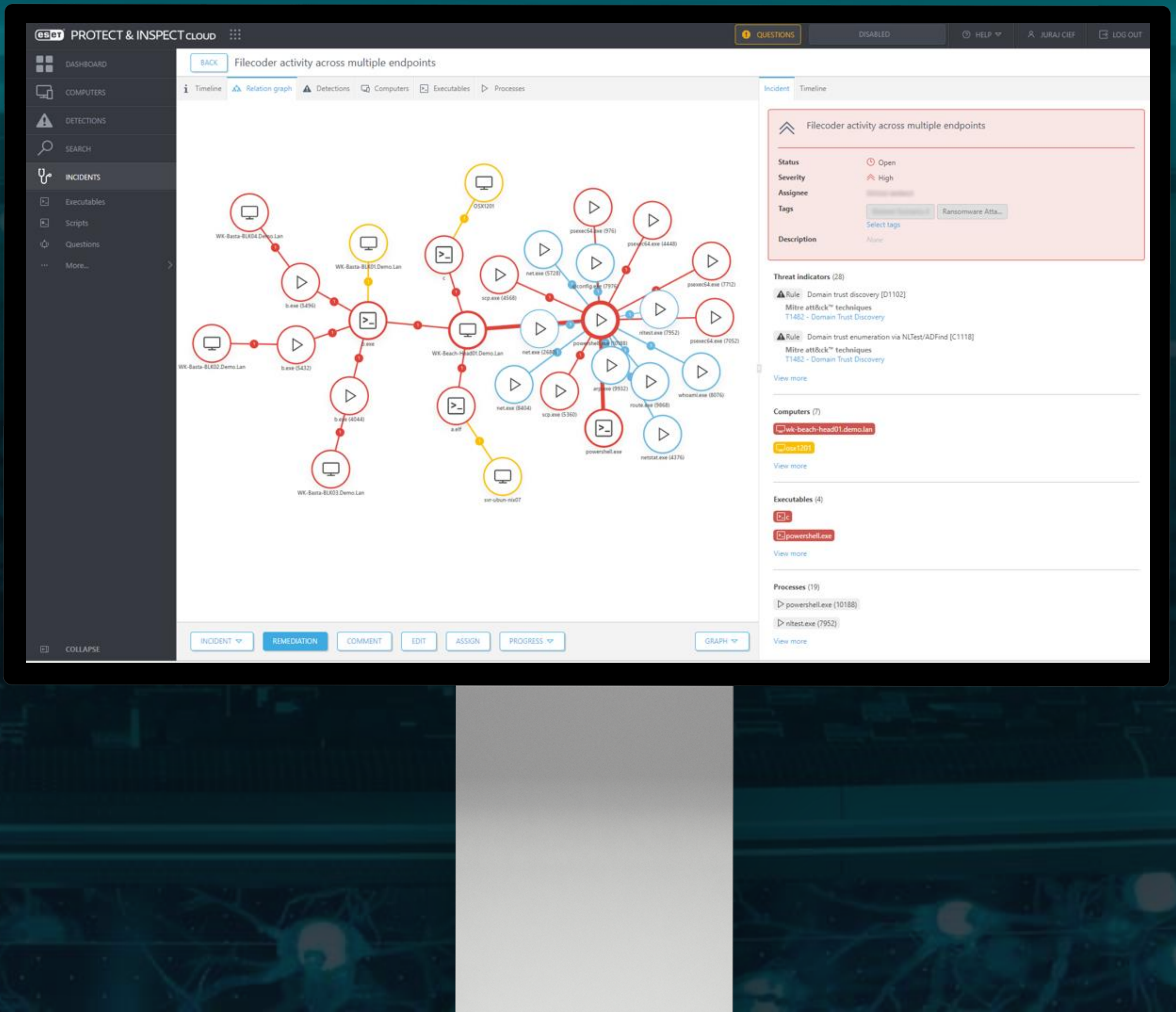
Flexibility of Deployment

Automated Incident Creation

Ready to Start Work Now

Reputation System

Automation and Customization



Filecoder activity across multiple endpoints

Filecoder activity across multiple endpoints

Status: Open
Severity: High
Assignee: [redacted]
Tags: [redacted] Ransomware Atta...
Select tags
Description: None

Threat indicators (28)

Rule Domain trust discovery [D1102]
Mitre att&ck™ techniques
T1482 - Domain Trust Discovery

Rule Domain trust enumeration via NLTest/ADFind [C1118]
Mitre att&ck™ techniques
T1482 - Domain Trust Discovery

View more

Computers (7)
wk-beach-head01.demo.lan
osx1201
View more

Executables (4)
c
powershell.exe
View more

Processes (19)
powershell.exe (10188)
nltest.exe (7952)
View more

FOR PARTNERS

ESET INSPECT

DETECTION

Find malicious anomaly

VISIBILITY

What is affected?

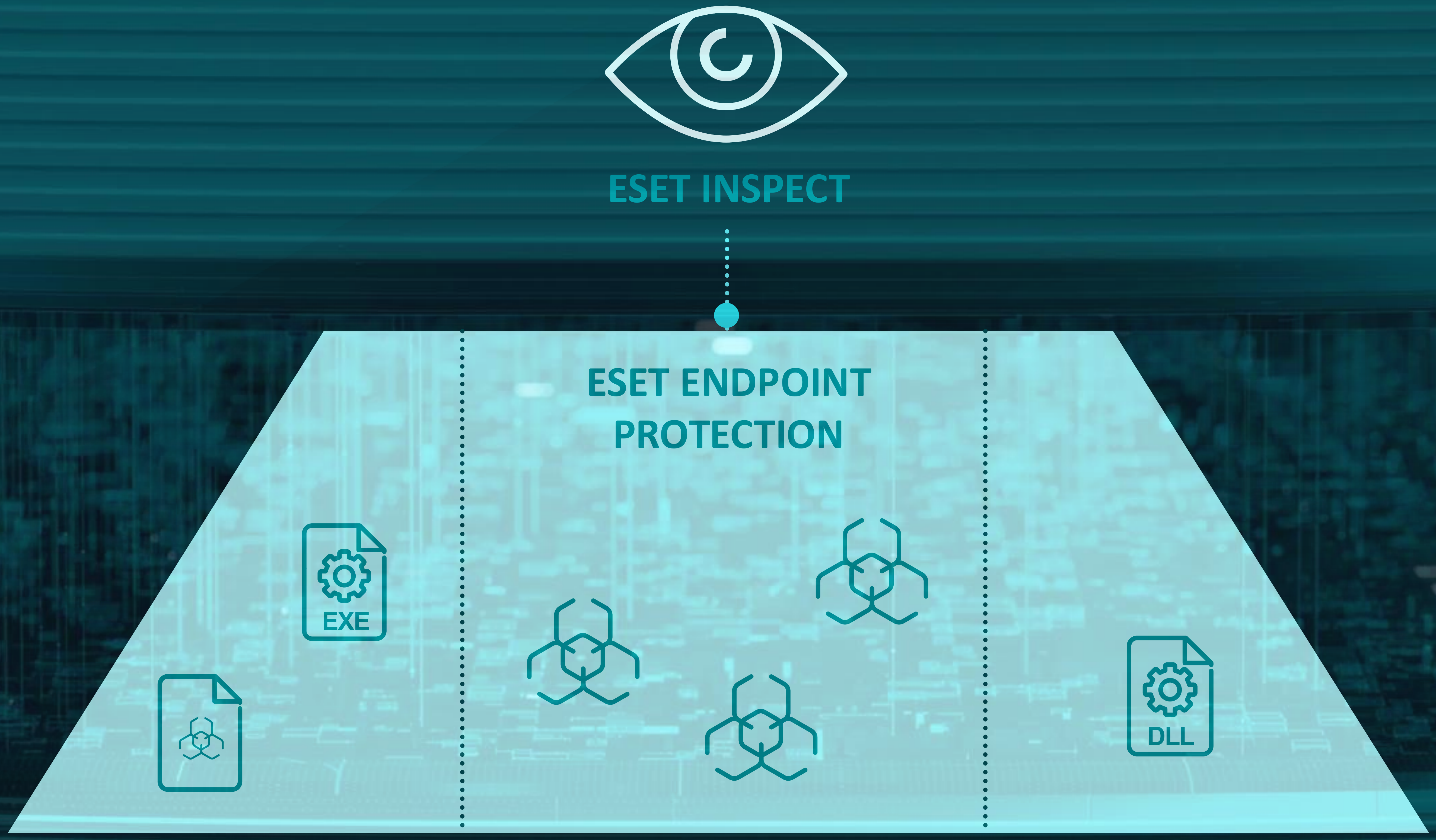
When it happened?

How it happened?

RESPONSE

Block it

Remove it



ESET INSPECT

ESET ENDPOINT PROTECTION

Visibility into what is happening on endpoints

Active Components

Fileless Attacks

Root Cause

Lateral Movement

Data Affected

Techniques Used

Allowing you to control how to respond

Block
Execution

Isolate
Computer

Kill
Process

Clean
File

Incident investigation with ESET Inspect

There are 2 basic approaches to investigation

Detection centric

Operator reacts to triggered detections within set threshold

Lateral Movement

Incident centric

Operator reacts towards incidents created based on behavioral rules and AI model

Live presentation will be in place here with comments (I will pre-record it as well)

Lateral Movement

Digital Security
Progress. Protected.