AT A GLANCE

2012

- CYBEREASON FOUNDED

2013

- $4.8 M SERIES A
- FIRST OFFICE

2014

- FIRST CUSTOMER
- EDR

2015

- $25 M SERIES B
- $59 M SERIES C
- NEW GLOBAL BOSTON HQ

2016

- 50+ CUSTOMERS
- CYBEREASON JAPAN, LONDON
- ANTI RANSOMWARE

2017

- 100+ CUSTOMERS
- $100M SERIES D

2018

- 200+ CUSTOMERS
- NSS LABS EDR 'RECOMMENDED'
- MITRE ATT&CK EVALUATION

2019

- $200 M SERIES E
- NEW EMEA HQ
- EPP
- MITRE ATT&CK EVALUATION

2020

- 1900+ CUSTOMERS
- MOBILE
- NSS LABS AEP 'AA' RATED AND AV-COMPARATIVE CERTIFIED
- XDR

2021

- ANTI RANSOMWARE 2.0
- CWPP
- INCIDENT RESPONSE

LOCKHEED MARTIN

SoftBank Group

SoftBank Group

SoftBank Group

LIBERTY Strategic Capital

Google

Industry Challenges

- Ransomware, Fileless & other Advanced Attacks
- Too Many Alerts
- Triage & Investigations Take Too Long
- Limited Security Staff
- Lack of Visibility

Why Cybereason

75%

Reduction in platform management via a single LW agent

1:200,000

Analyst-to-Endpoint Ratio

100:1

Event consolidation hundreds of events to a single MalOp

- Full Telemetry Data Collection
- Support all OS (including Legacy)
- Alerts to Operations Centric Security
- Roadmap to XDR — Chronicle part of Google Cloud
- Detect: 1 **Triage:** 5 **Remediate:** 30

The Most Validated Endpoint Solution

The Cybereason Defense Platform

Gartner

Cybereason Named a **LEADER** in Gartner's 2022 EPP Magic Quadrant Report

Gartner Peer Insights

60+ stellar reviews in the last 12 months

MITRE ATT&CK

Cybereason Achieved the **Highest Ever Recorded Score** in MITRE ATT&CK Enterprise testing

Undefeated against ransomware. Proven to stop hundreds of strains of known and novel ransomware

fubo bugaboo PINNACLEGROUP

Defending customers large and small, **from 500,000 endpoints to 50**

GARTNER MAGIC QUADRANT LEADER.

THE REASON?

Undefeated against ransomware

Highest ever recorded score in the **MITRE ATT&CK testing**

Only Cybereason **reduces alerts by 10X**

cybereason

MITRE 2023: Key Metrics to Consider

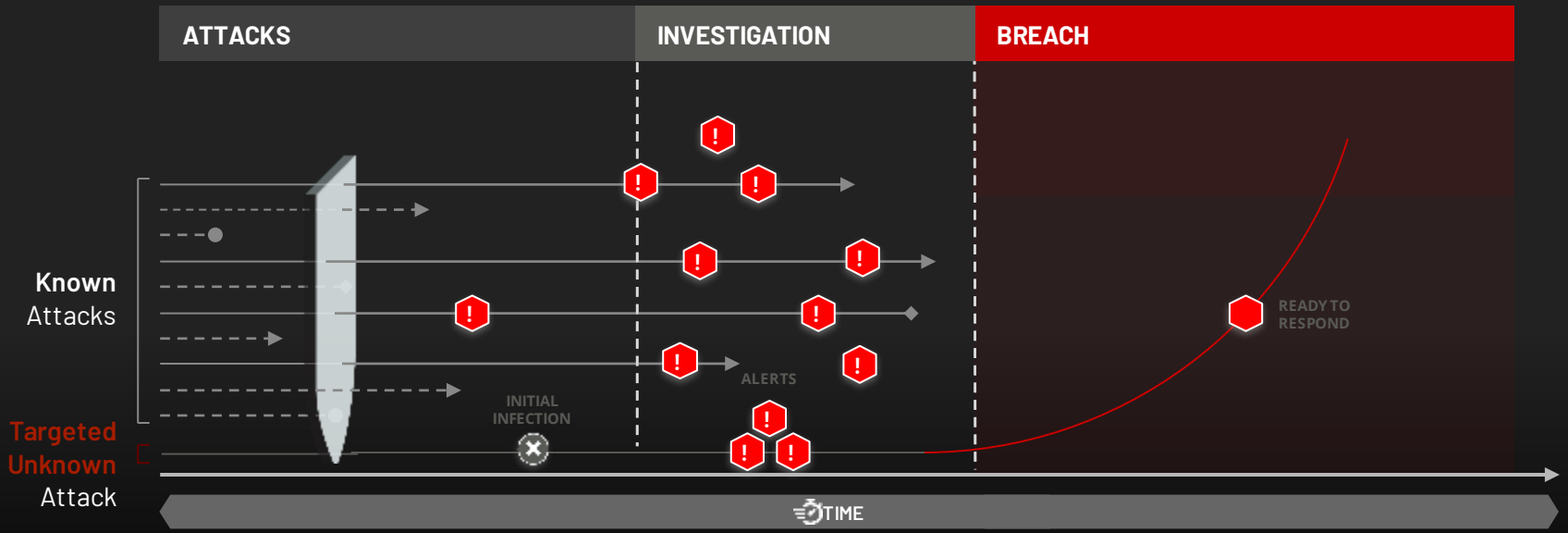
Vendor	Protection (out of 13 tests)	Detection* (out of 19 steps)	Visibility (out of 143 substeps)	Technique* (out of 143 substeps)	Out of the Box Capability	Real Time Detections
Palo Alto Networks	100%	100%	100%	99%	100%	100%
Cybereason	100%	100%	100%	97%	100%	100%
Cynet	92%	100%	100%	92%	98%	100%
CrowdStrike	100%	100%	98%	80%	97%	91%
SentinelOne	100%	95%	88%	77%	100%	100%
Microsoft	100%	100%	87%	68%	73%	100%
Broadcom Symantec	100%	95%	76%	40%	100%	100%
Trend Micro	100%	100%	84%	50%	78%	91%
Sophos	85%	100%	83%	61%	82%	96%
Elastic	85%	100%	79%	30%	97%	100%
Check Point	92%	95%	78%	56%	76%	100%
Trellix	85%	100%	78%	42%	83%	97%
VMware Carbon Black	77%	100%	68%	31%	100%	99%
Malwarebytes	54%	95%	58%	39%	67%	100%
Rapid7	0%	95%	68%	19%	92%	97%

MITRE 2022 Evaluation - Key Metrics to Consider

Vendor	Prevention (Out of 9 attacks)	Visibility Coverage % (Out of 109 substeps)	Analytic Coverage % (Out of 109 substeps)	Delayed Detections %	Configuration Changes %	Linux Detections %
Cybereason	100%	100%	99%	0%	3%	100%
SentinelOne	100%	99%	99%	0%	2%	100%
Cynet	100%	98%	94%	0%	22%	84%
Check Point	78%	94%	94%	0%	23%	95%
CrowdStrike	100%	96%	86%	10%	2%	84%
Microsoft	100%	90%	90%	0%	12%	95%
Trend Micro	89%	96%	92%	13%	19%	100%
McAfee	67%	98%	77%	0%	10%	37%
Broadcom Symantec	67%	84%	80%	5%	2%	74%
FireEye	67%	82%	78%	1%	8%	84%
Cylance	100%	82%	65%	0%	14%	53%
Cisco AMP	78%	83%	68%	6%	17%	58%
Elastic	0%	90%	65%	0%	11%	63%
VMware CarbonBlack	89%	83%	52%	0%	0%	32%
Sophos	44%	81%	61%	2%	8%	68%
Qualys	0%	61%	46%	0%	17%	0%
Rapid7	0%	57%	21%	7%	8%	21%

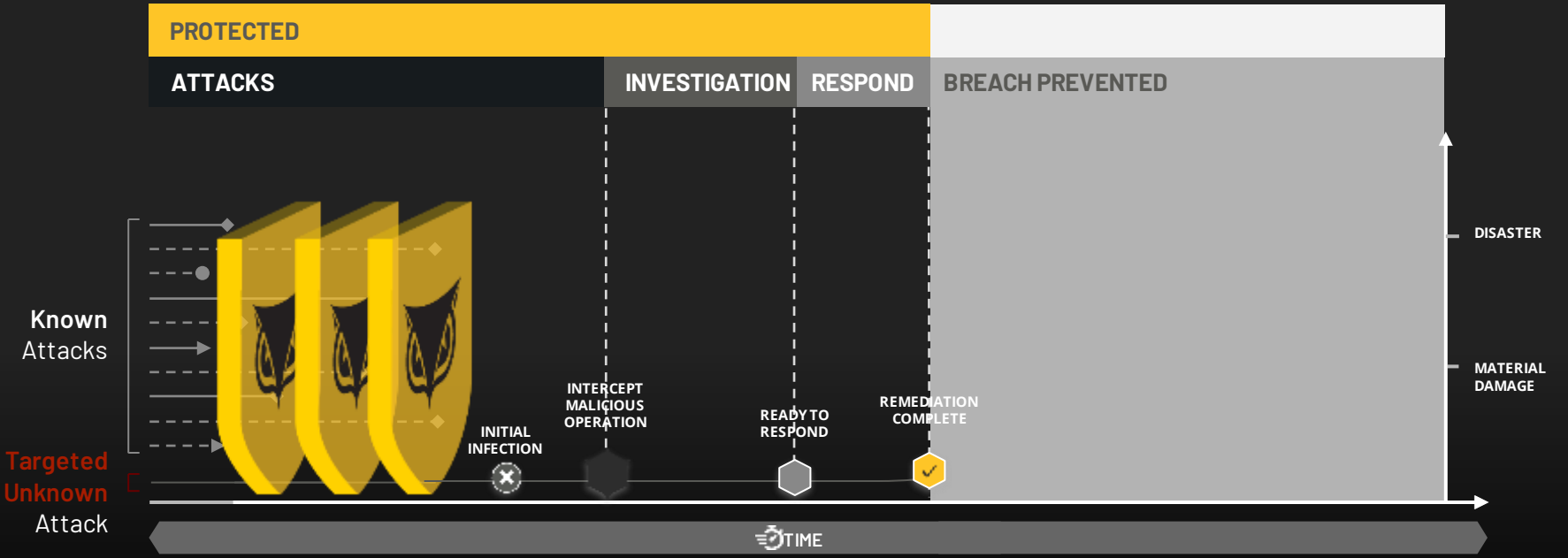
Alert-Centric Security

Slow, Inefficient, Costly

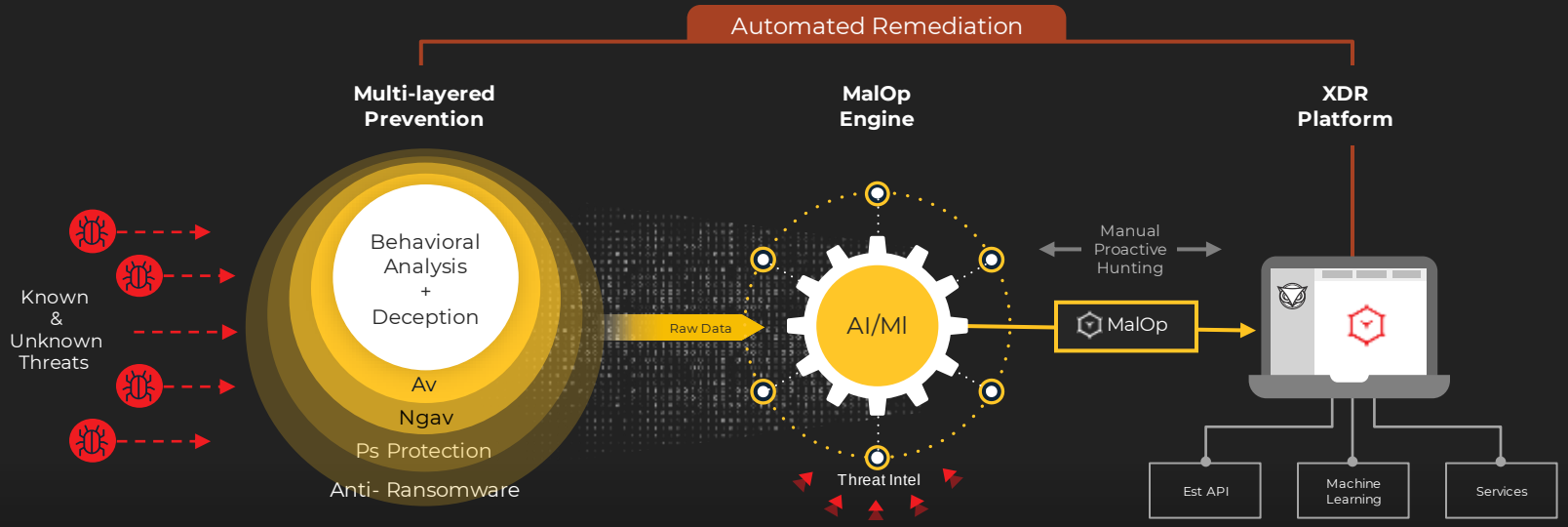


Operation-Centric Security

The Ideal State



Operation-centric: MalOp Engine



Reduces false positives (<1%) **Reduces attacker dwell time (98%)** **Improves monitoring scale (308% ROI)** **Accelerates response (93%)**

The MalOp™ (Malicious Operation)

Providing the Complete Story of an Attack

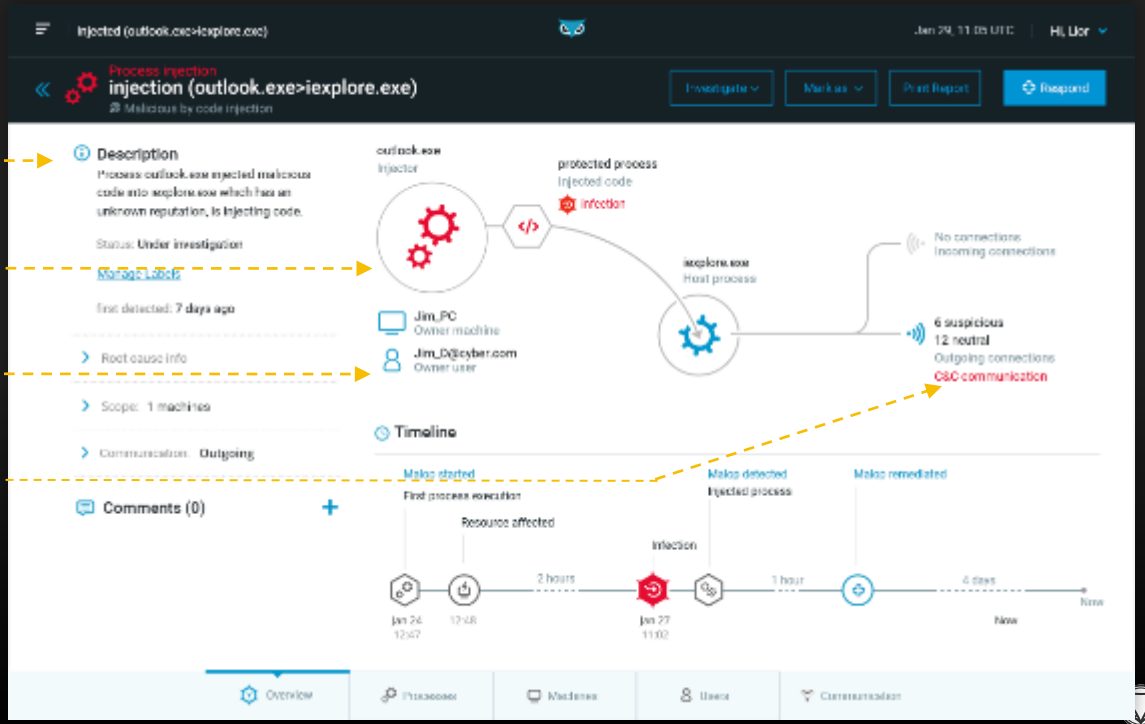
Root cause

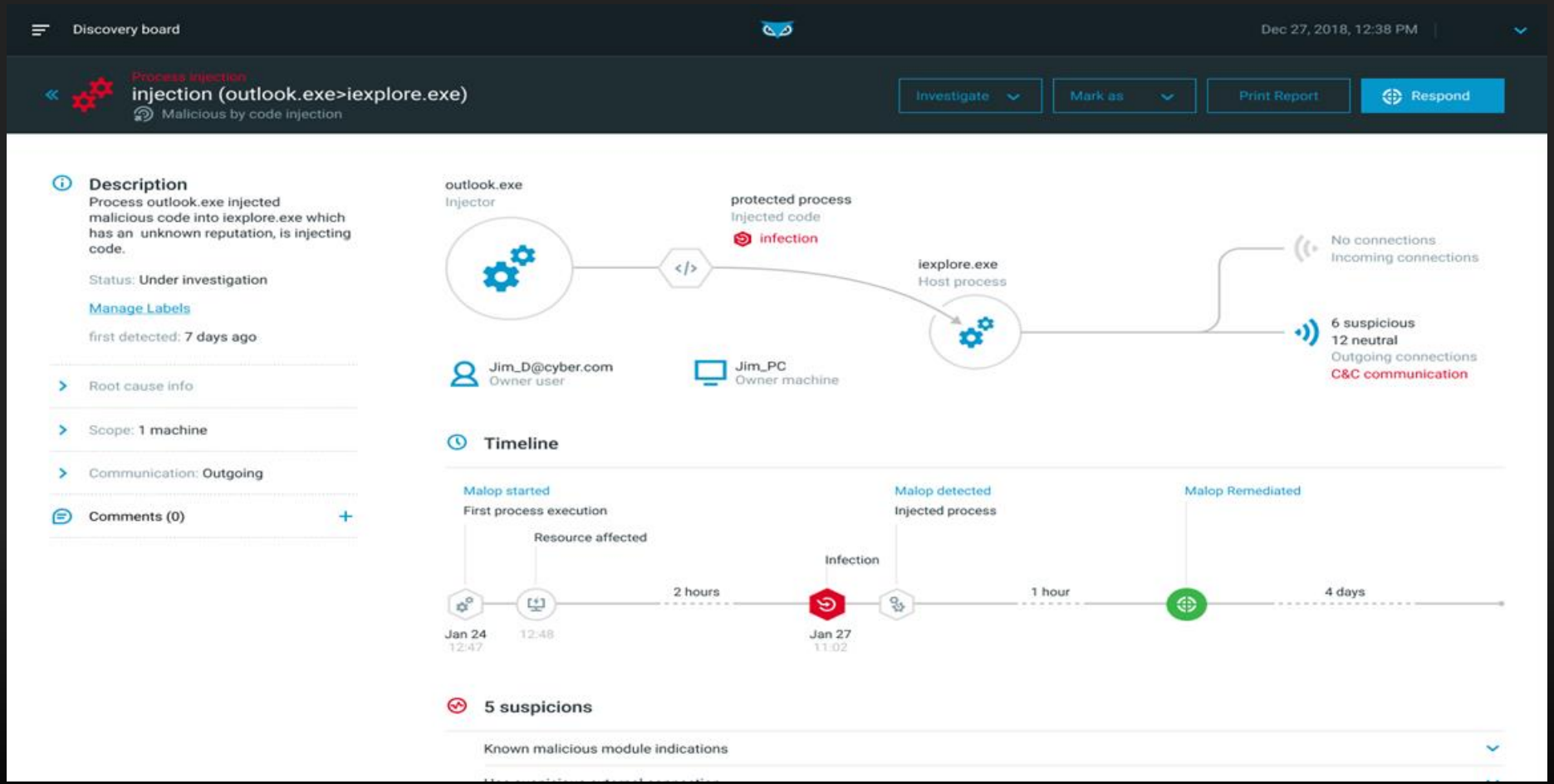
Tools leveraged

Affected users & machines

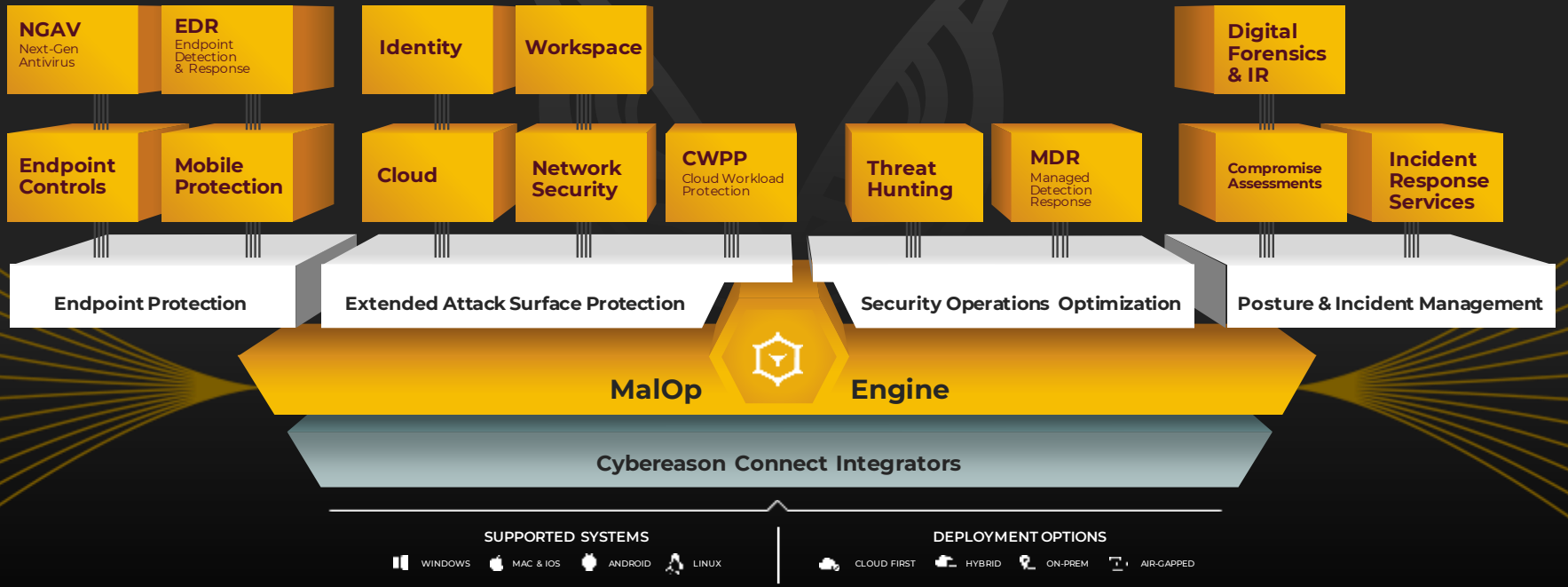
Attacker communications

Attack timeline




Discovery board
Dec 27, 2018, 12:38 PM
Process injection
injection (outlook.exe>iexplore.exe)
Malicious by code injection
Investigate
Mark as
Print Report
Respond
Description
Process outlook.exe injected malicious code into iexplore.exe which has an unknown reputation, is injecting code.
Status: Under investigation
Manage Labels
first detected: 7 days ago
Root cause info
Scope: 1 machine
Communication: Outgoing
Comments (0)
outlook.exe
Injector
protected process
Injected code
infection
iexplore.exe
Host process
No connections
Incoming connections
6 suspicious
12 neutral
Outgoing connections
C&C communication
Jim_D@cyber.com
Owner user
Jim_PC
Owner machine
Timeline
Malop started
First process execution
Resource affected
Malop detected
Injected process
Infection
Malop Remediated
2 hours
1 hour
4 days
Jan 24
12:47
12:48
Jan 27
11:02
5 suspicions
Known malicious module indications

CYBEREASON XDR PLATFORM



TECHNOLOGY PARTNERS

XDR Integrations

ENDPOINT



iOS

WORKSPACE


Office
Exchange
proofpoint

IDENTITY

Active Directory
Azure Active Directory
okta
DUO
onelogin

CLOUD


aws
zscaler
Azure

NETWORK

FORTINET
paloalto
zscaler
CHECK POINT

References

- Largest customer in Defense industry
- Executive Government Entity
- Largest Investment holding Government Group
- Retail Customer
- One of Airline Management Companies