cybereason®

We are DEFENDERS

Jens Peter Höhner

Enterprise Sales Director

Marcus Stahlhacke

Enterprise Sales Engineer

WHO WE'RE ARE

Undefeated in the fight against ransomware

1. Gegründet 2012
2. 1400 Mitarbeiter
3. über 2000 Kunden

MITRE ATT&CK™ Gartner® NSS LABS

Herausforderungen für die Unternehmen

- Underground Economy
- Ransomware as a service
Fileless Angriffe
- Zu viele Alarme + Blind Spots
- Wenige Spezialisten
- Komplexität der Angriffe

Erwartungshaltung

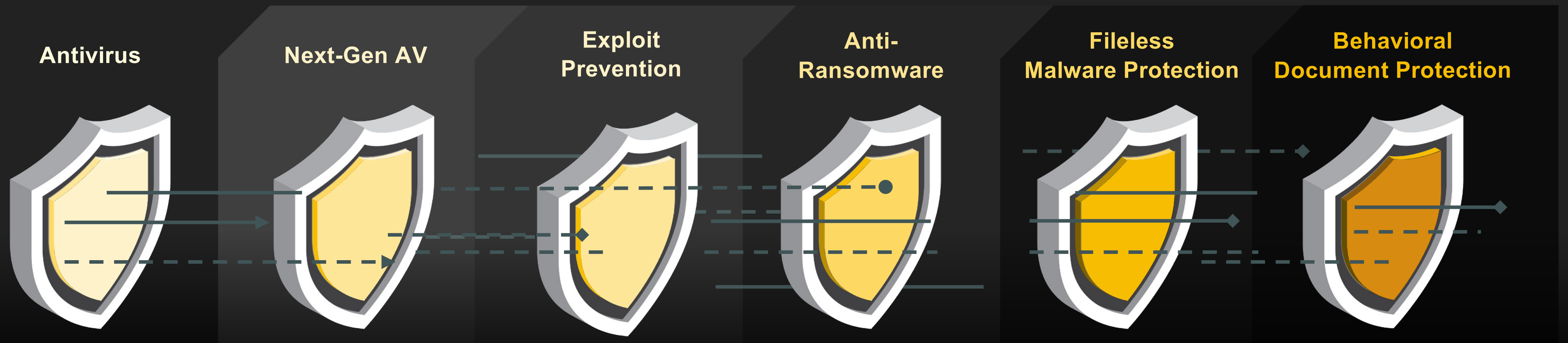
MTTD
Meantime to detect

MTTI
Meantime to investigate

MTTR
Meantime to respond

Der Prevention Stack

Ungeschlagen gegen Ransomware



Antivirus

Next-Gen AV

Exploit Prevention

Anti-Ransomware

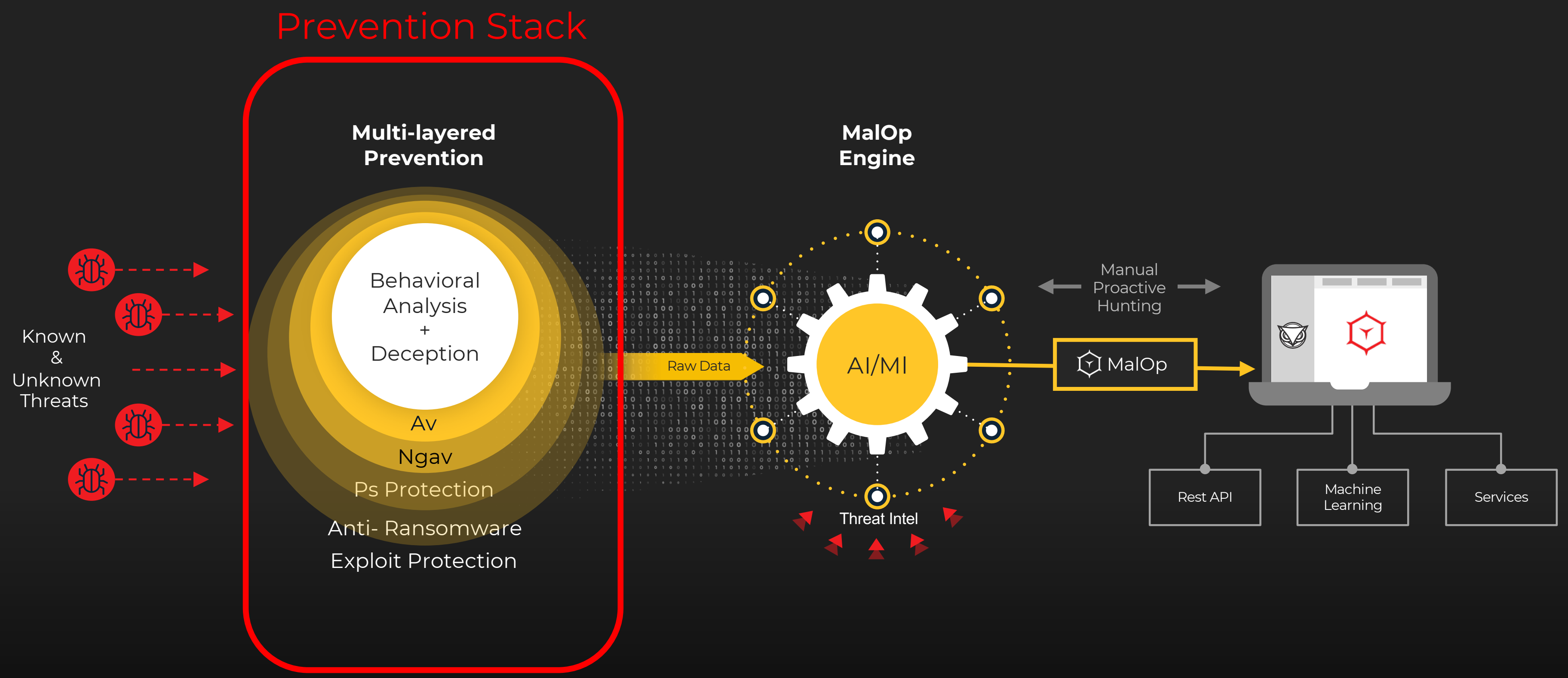
Fileless Malware Protection

Behavioral Document Protection

NSS LABS Highest Overall ‘AA’ Rating

MITRE | ATT&CK® Highest Score Real-Time Coverage

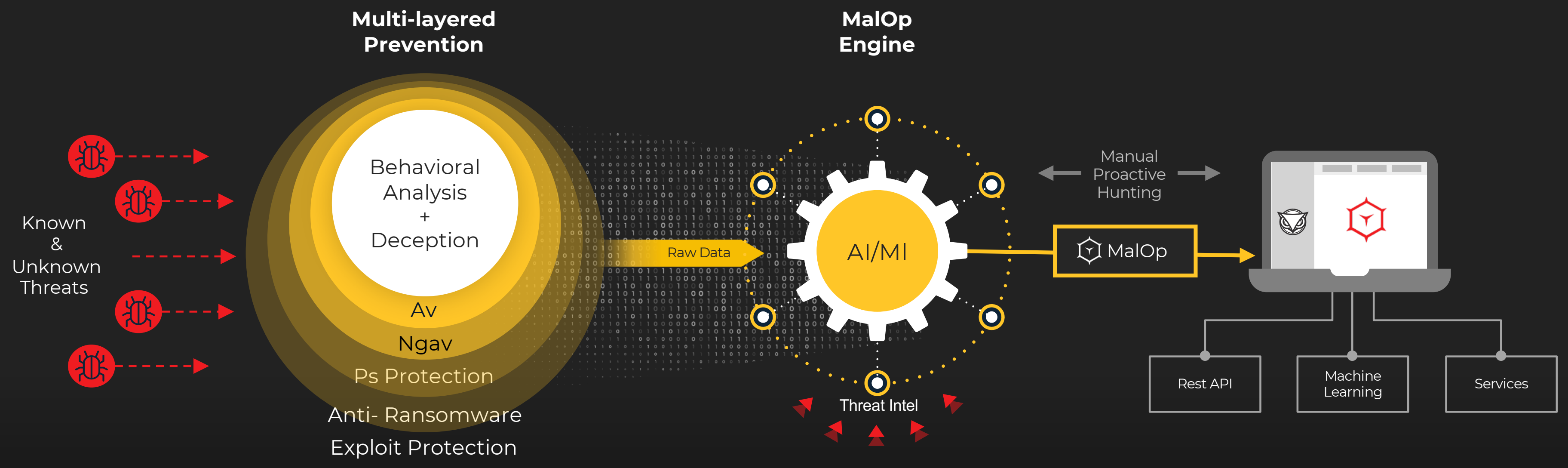
Operation-centric: MalOp Engine



Weniger Fehlalarme (<1%) → **Weniger "dwell time" (98%)** → **Schnellere Response (93%)**

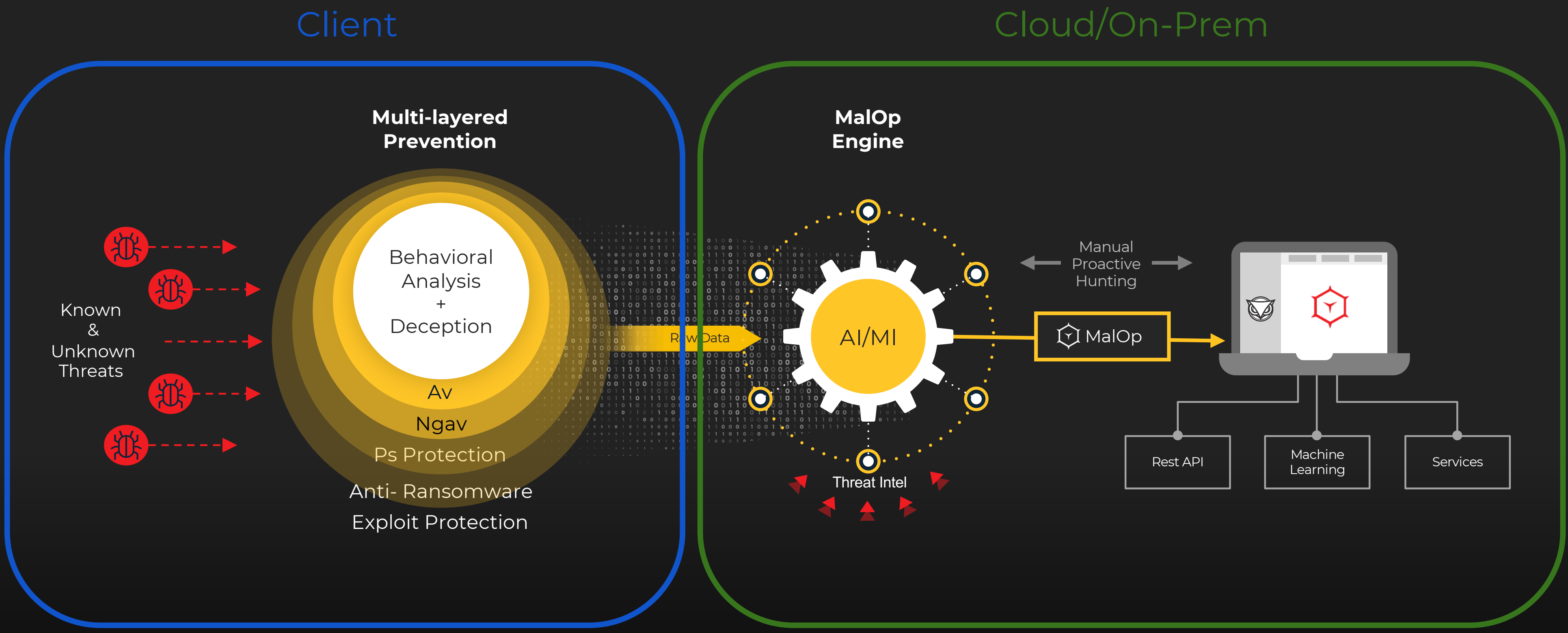
Cybereason

Operation-centric: MalOp Engine



Weniger Fehlalarme (<1%) **Weniger "dwell time" (98%)** **Schnellere Response (93%)**

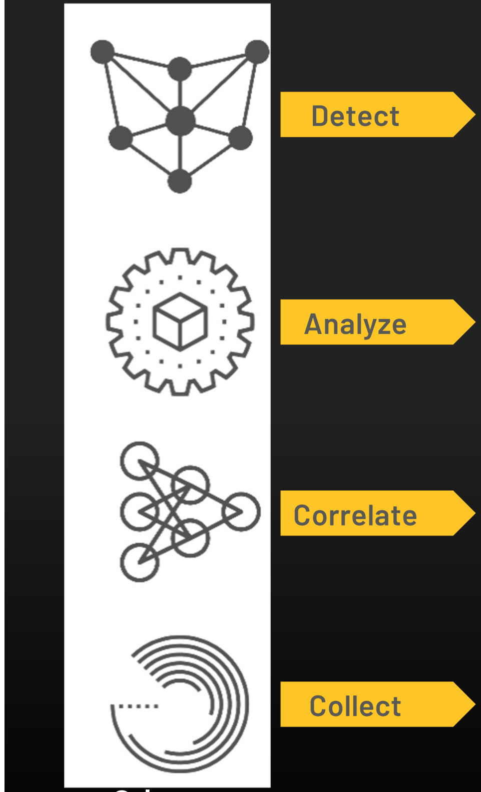
Operation-centric: MalOp Engine



Weniger Fehlalarme (<1%) → **Weniger “dwell time” (98%)** → **Schnellere Response (93%)**

CYBEREASON ANALYSIS MODEL

Dynamic, persistent, real-time



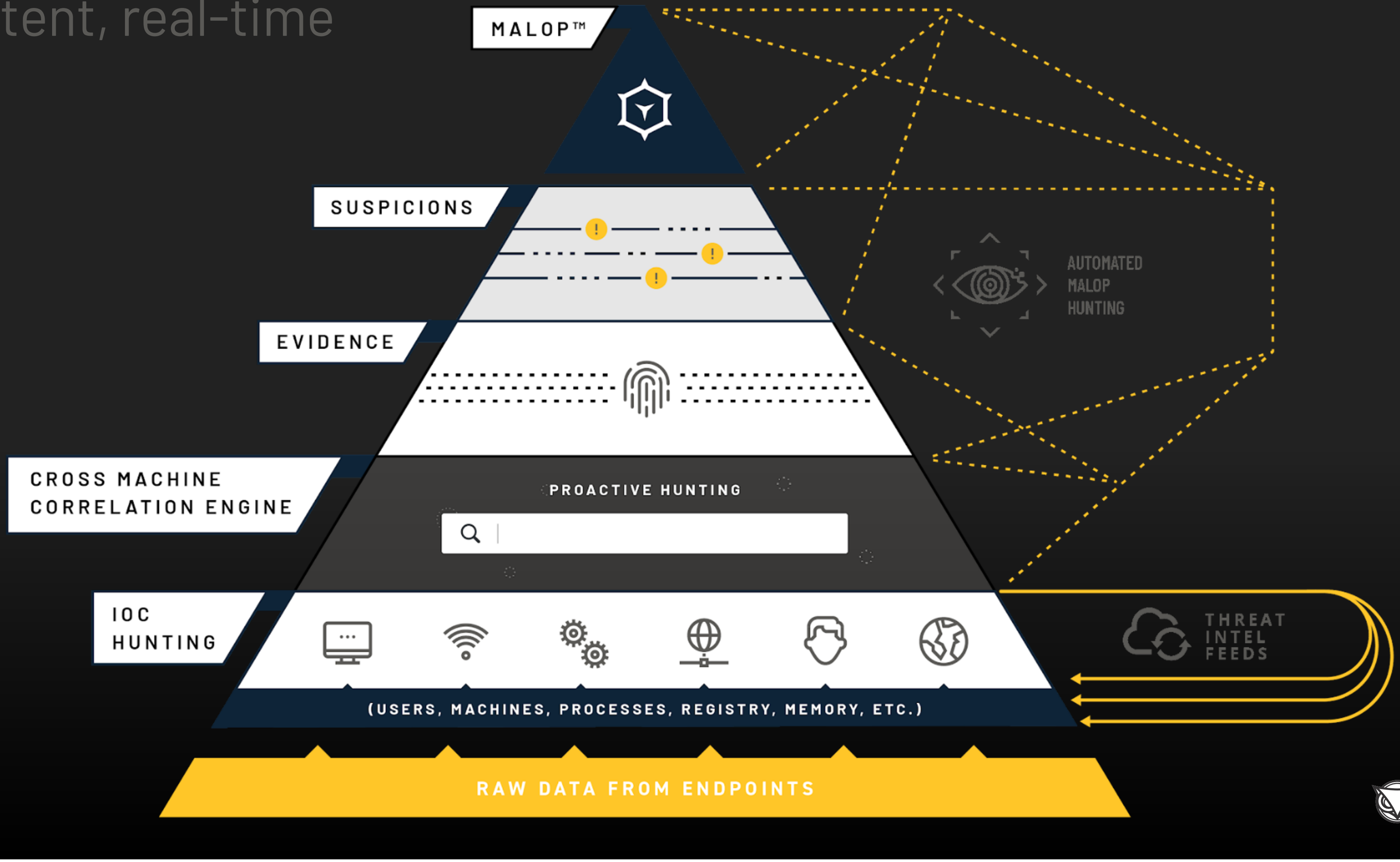
Detect

Analyze

Correlate

Collect

Cybereason



MALOP™

SUSPICIONS

EVIDENCE

CROSS MACHINE CORRELATION ENGINE

PROACTIVE HUNTING

IOC HUNTING

(USERS, MACHINES, PROCESSES, REGISTRY, MEMORY, ETC.)

RAW DATA FROM ENDPOINTS

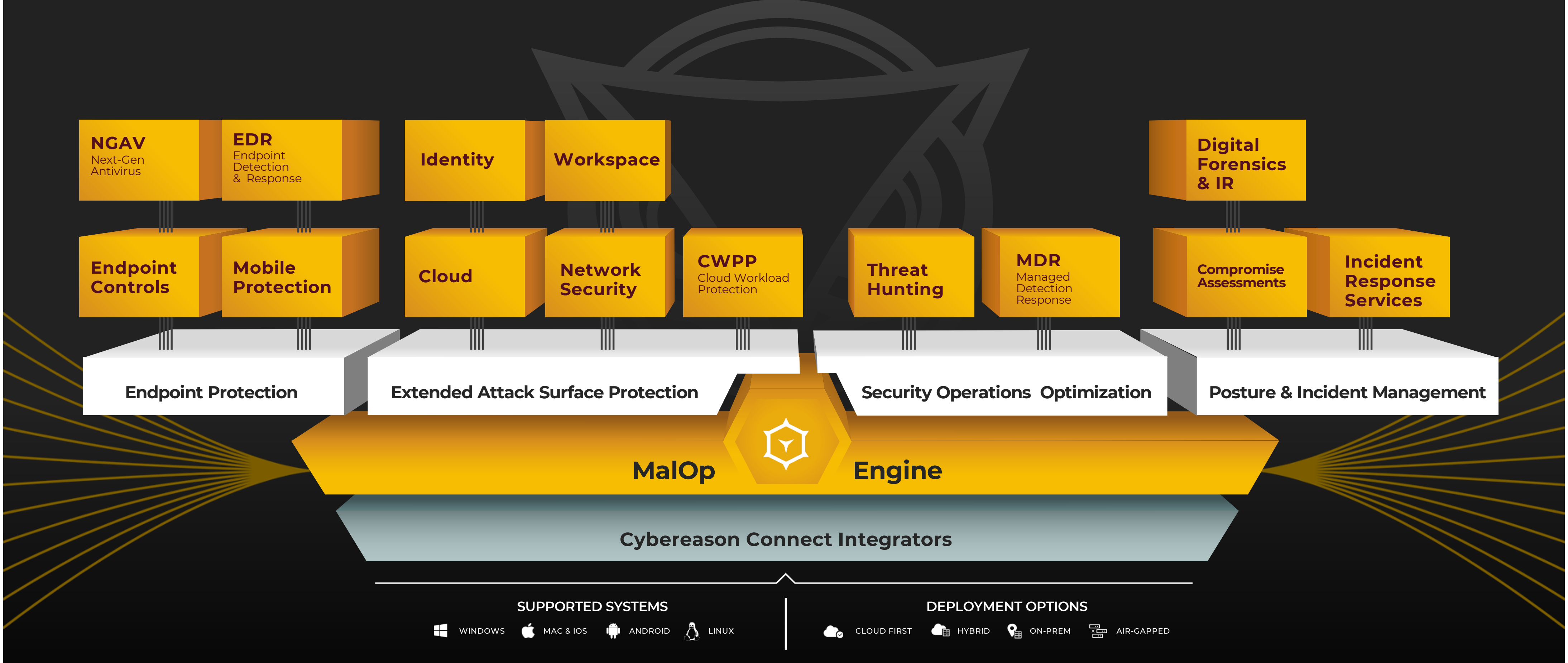
AUTOMATED MALOP HUNTING

THREAT INTEL FEEDS

cybereason®

THIS IS XDR

CYBEREASON XDR PLATFORM



NGAV
Next-Gen Antivirus

EDR
Endpoint Detection & Response

Endpoint Controls

Mobile Protection

Endpoint Protection

Identity

Workspace

Cloud

Network Security

CWPP
Cloud Workload Protection

Extended Attack Surface Protection

Threat Hunting

MDR
Managed Detection Response

Security Operations Optimization

Digital Forensics & IR

Compromise Assessments

Incident Response Services

Posture & Incident Management

MalOp Engine

Cybereason Connect Integrators

SUPPORTED SYSTEMS

WINDOWS · MAC & IOS · ANDROID · LINUX

DEPLOYMENT OPTIONS

CLOUD FIRST · HYBRID · ON-PREM · AIR-GAPPED

XDR Integrations

ENDPOINT

iOS

WORKSPACE

Office 365

Exchange

slack

proofpoint.

IDENTITY

Microsoft Active Directory

Azure Active Directory

okta

CLOUD

AWS

Azure

netskope

zscaler

NETWORK

FORTINET.

paloalto® NETWORKS

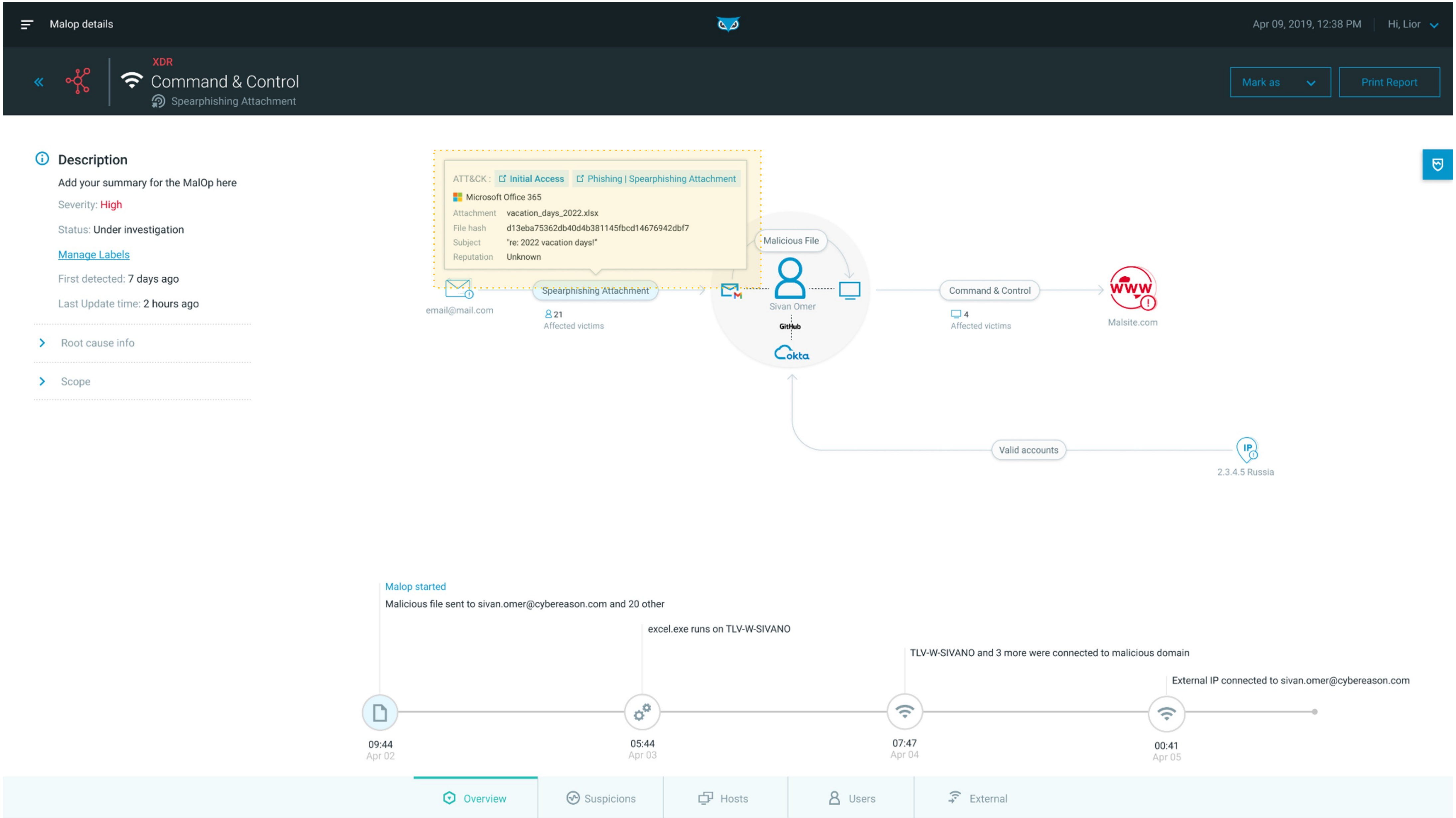
cisco

Check Point SOFTWARE TECHNOLOGIES LTD.

zscaler

EDR Demo

XDR Demo



Description

Add your summary for the MalOp here

Severity: High

Status: Under investigation

Manage Labels

First detected: 7 days ago

Last Update time: 2 hours ago

ATT&CK : Initial Access | Phishing | Spearphishing Attachment

Microsoft Office 365

Attachment	vacation_days_2022.xlsx
File hash	d13eba75362db40d4b381145fbcd14676942dbf7
Subject	"re: 2022 vacation days!"
Reputation	Unknown

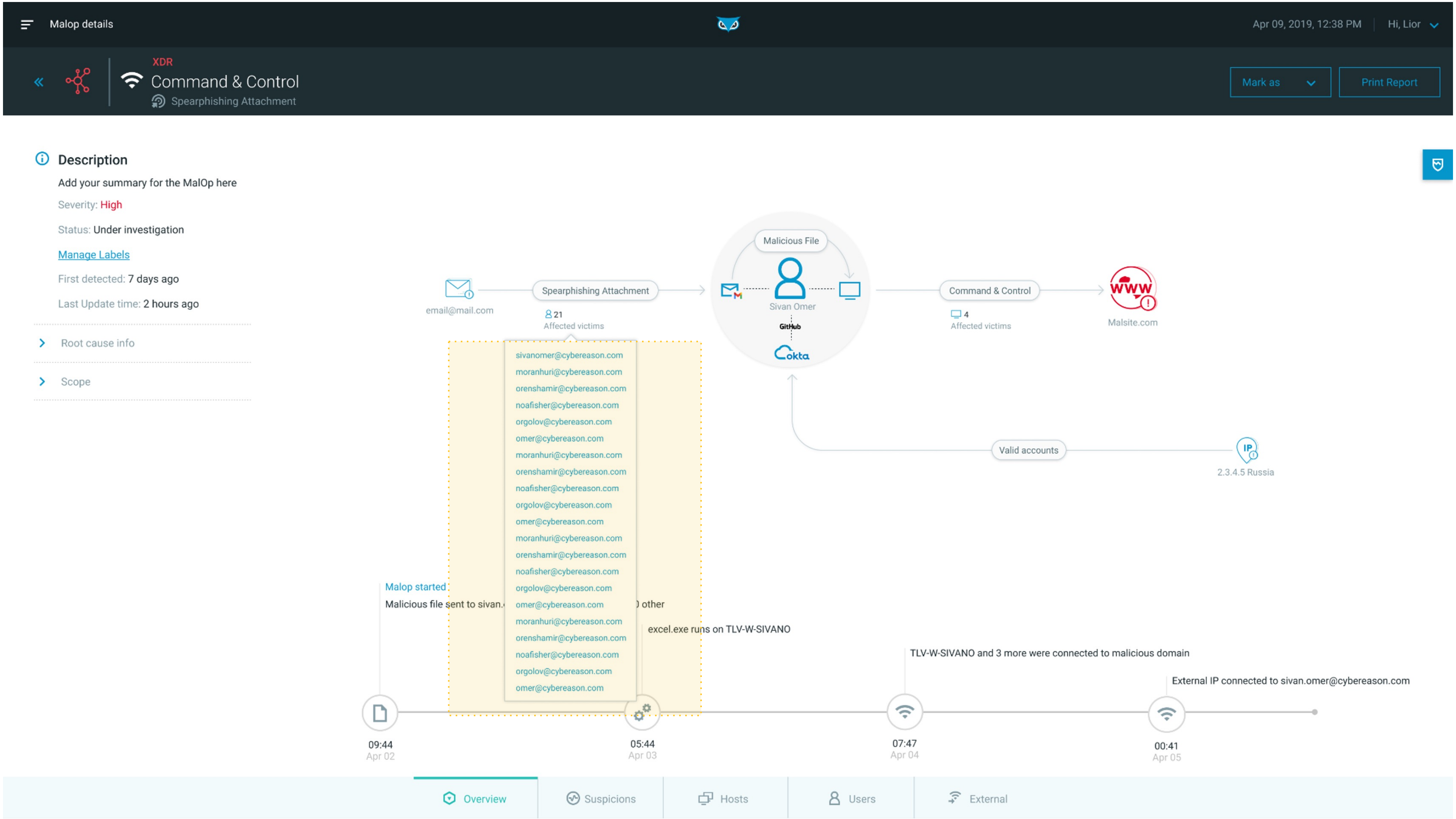
Malop started

Malicious file sent to sivan.omer@cybereason.com and 20 other

excel.exe runs on TLV-W-SIVANO

TLV-W-SIVANO and 3 more were connected to malicious domain

External IP connected to sivan.omer@cybereason.com



Description

Add your summary for the MalOp here

Severity: High

Status: Under investigation

Manage Labels

First detected: 7 days ago

Last Update time: 2 hours ago

sivanomer@cybereason.com
moranhuri@cybereason.com
orenshamir@cybereason.com
noafisher@cybereason.com
orgolov@cybereason.com
omer@cybereason.com
moranhuri@cybereason.com
orenshamir@cybereason.com
noafisher@cybereason.com
orgolov@cybereason.com
omer@cybereason.com
moranhuri@cybereason.com
orenshamir@cybereason.com
noafisher@cybereason.com
orgolov@cybereason.com
omer@cybereason.com
moranhuri@cybereason.com
orenshamir@cybereason.com
noafisher@cybereason.com
orgolov@cybereason.com
omer@cybereason.com

Malop started

Malicious file sent to sivan.( ) other

excel.exe runs on TLV-W-SIVANO

TLV-W-SIVANO and 3 more were connected to malicious domain

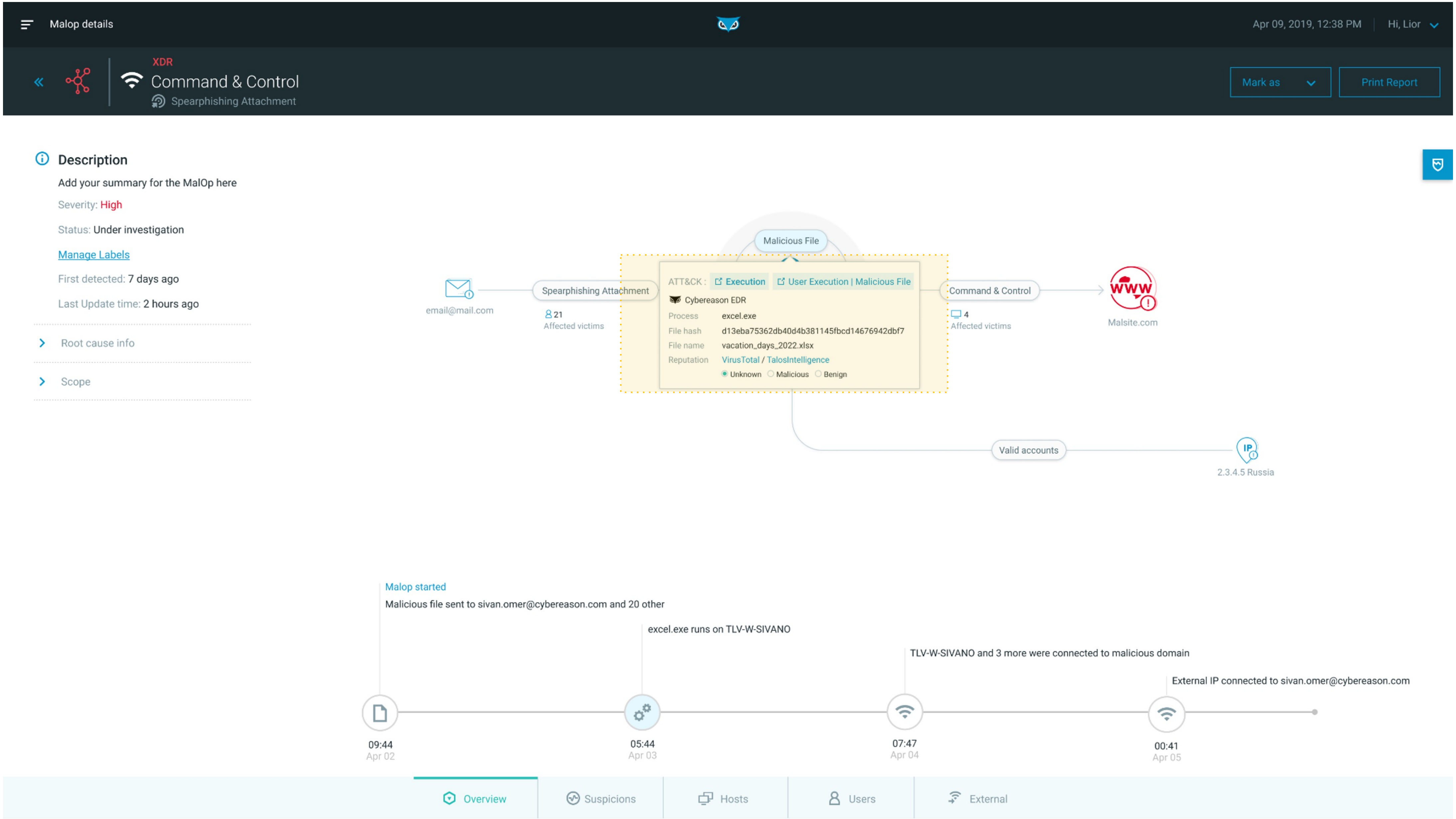
External IP connected to sivan.omer@cybereason.com

09:44 Apr 02

05:44 Apr 03

07:47 Apr 04

00:41 Apr 05



XDR

Command & Control

Spearphishing Attachment

Description

Add your summary for the MalOp here

Severity: High

Status: Under investigation

Manage Labels

First detected: 7 days ago

Last Update time: 2 hours ago

› Root cause info

› Scope

21 Affected victims

ATT&CK : Execution User Execution | Malicious File

Cybereason EDR

Process	excel.exe
File hash	d13eba75362db40d4b381145fbcd14676942dbf7
File name	vacation_days_2022.xlsx
Reputation	VirusTotal / TalosIntelligence
	● Unknown ○ Malicious ○ Benign

4 Affected victims

Malop started

Malicious file sent to sivan.omer@cybereason.com and 20 other

excel.exe runs on TLV-W-SIVANO

TLV-W-SIVANO and 3 more were connected to malicious domain

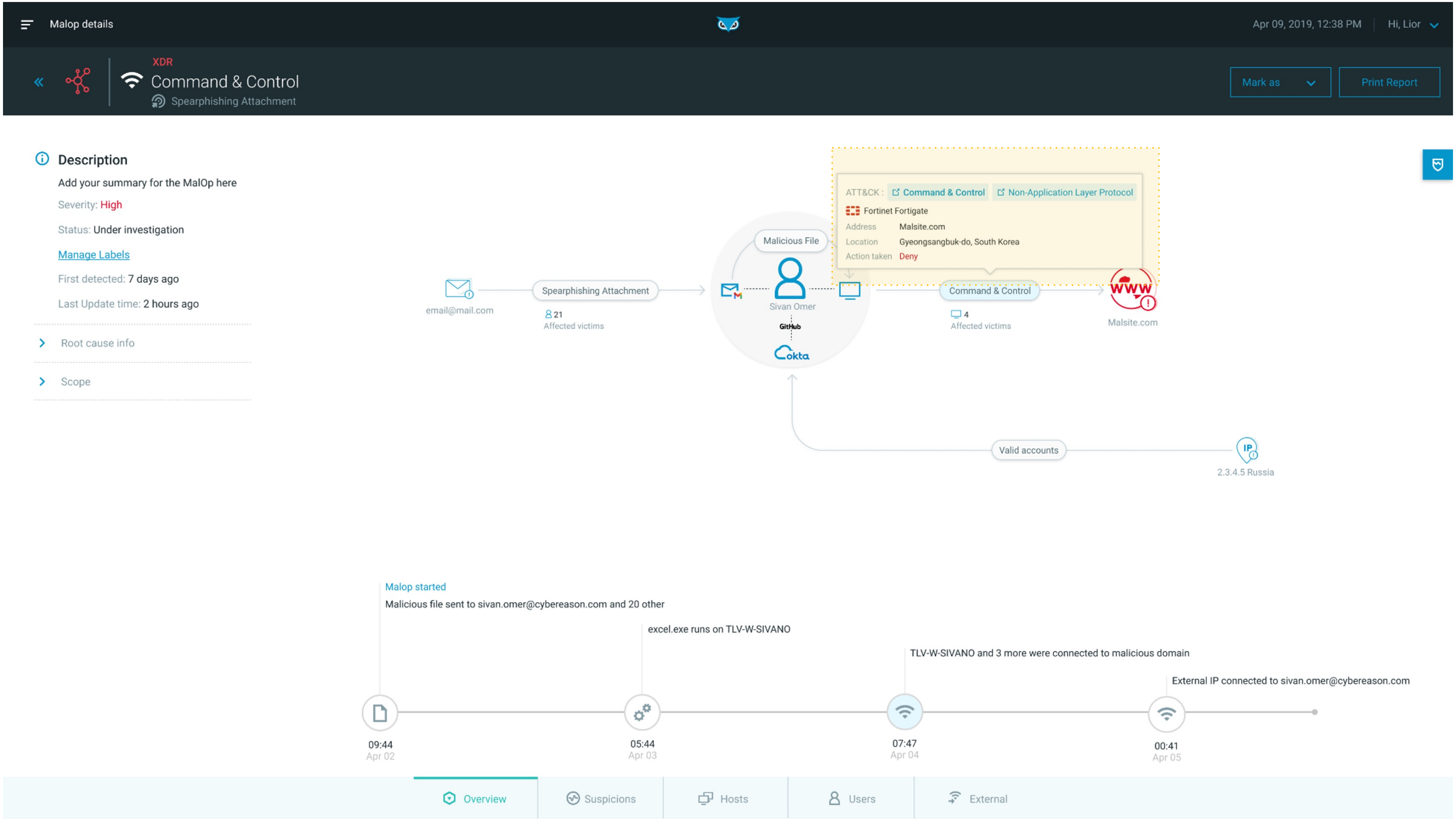
External IP connected to sivan.omer@cybereason.com

09:44 Apr 02

05:44 Apr 03

07:47 Apr 04

00:41 Apr 05



Malop details

Apr 09, 2019, 12:38 PM | Hi, Lior

XDR

Command & Control

Spearphishing Attachment

Mark as

Print Report

Description

Add your summary for the MalOp here

Severity: High

Status: Under investigation

Manage Labels

First detected: 7 days ago

Last Update time: 2 hours ago

Root cause info

Scope

ATT&CK : Command & Control | Non-Application Layer Protocol

Fortinet Fortigate

Address	Malsite.com
Location	Gyeongsangbuk-do, South Korea
Action taken	Deny

Malop started

Malicious file sent to sivan.omer@cybereason.com and 20 other

excel.exe runs on TLV-W-SIVANO

TLV-W-SIVANO and 3 more were connected to malicious domain

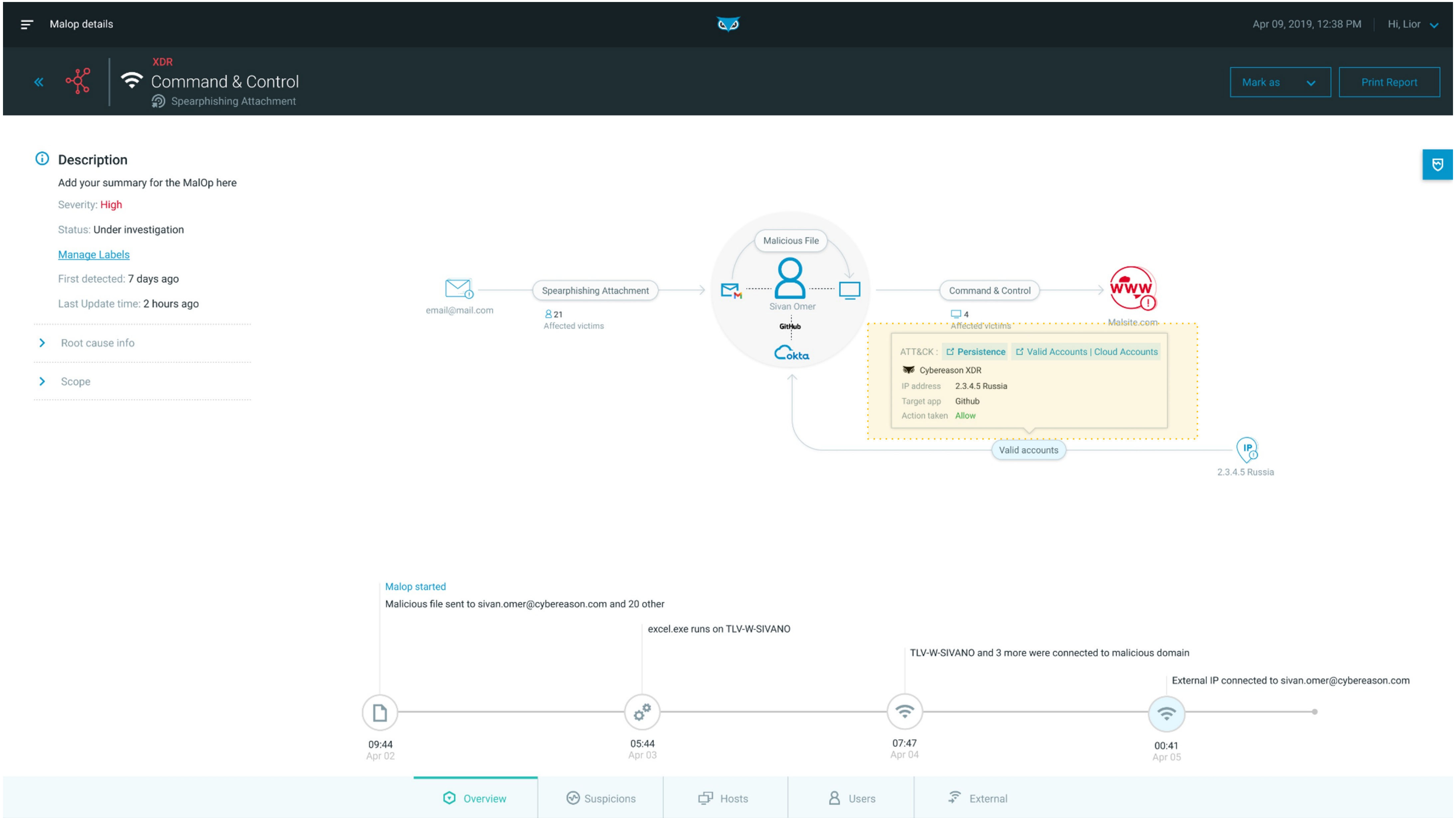
External IP connected to sivan.omer@cybereason.com

09:44 Apr 02

05:44 Apr 03

07:47 Apr 04

00:41 Apr 05



Description

Add your summary for the MalOp here

Severity: High

Status: Under investigation

Manage Labels

First detected: 7 days ago

Last Update time: 2 hours ago

ATT&CK : Persistence | Valid Accounts | Cloud Accounts

Cybereason XDR

IP address 2.3.4.5 Russia

Target app Github

Action taken Allow

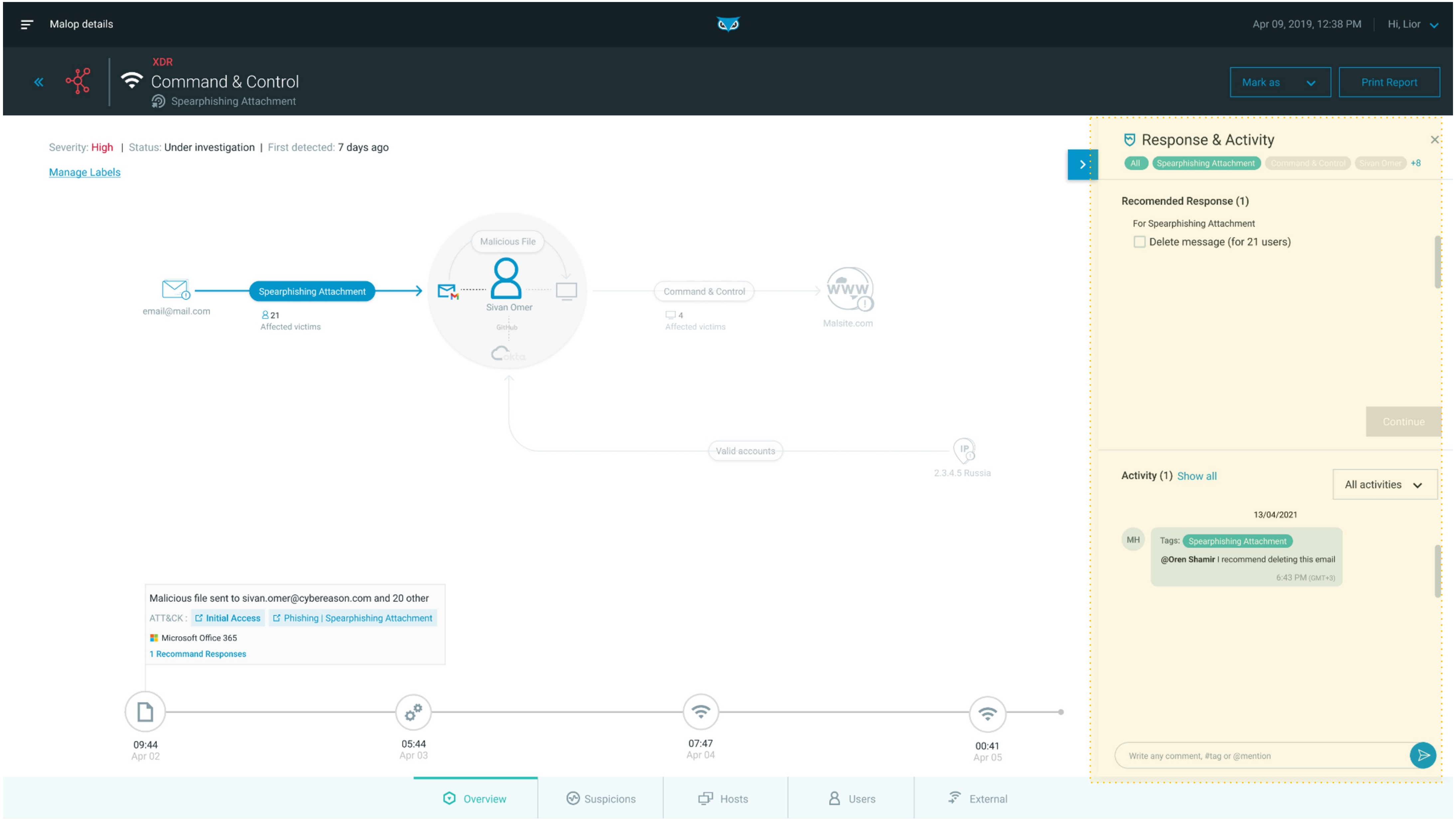
Malop started

Malicious file sent to sivan.omer@cybereason.com and 20 other

excel.exe runs on TLV-W-SIVANO

TLV-W-SIVANO and 3 more were connected to malicious domain

External IP connected to sivan.omer@cybereason.com



Severity: High | Status: Under investigation | First detected: 7 days ago

Malicious file sent to sivan.omer@cybereason.com and 20 other

ATT&CK : Initial Access | Phishing | Spearphishing Attachment

Microsoft Office 365

1 Recommand Responses

Response & Activity

Recomended Response (1)

For Spearphishing Attachment

□ Delete message (for 21 users)

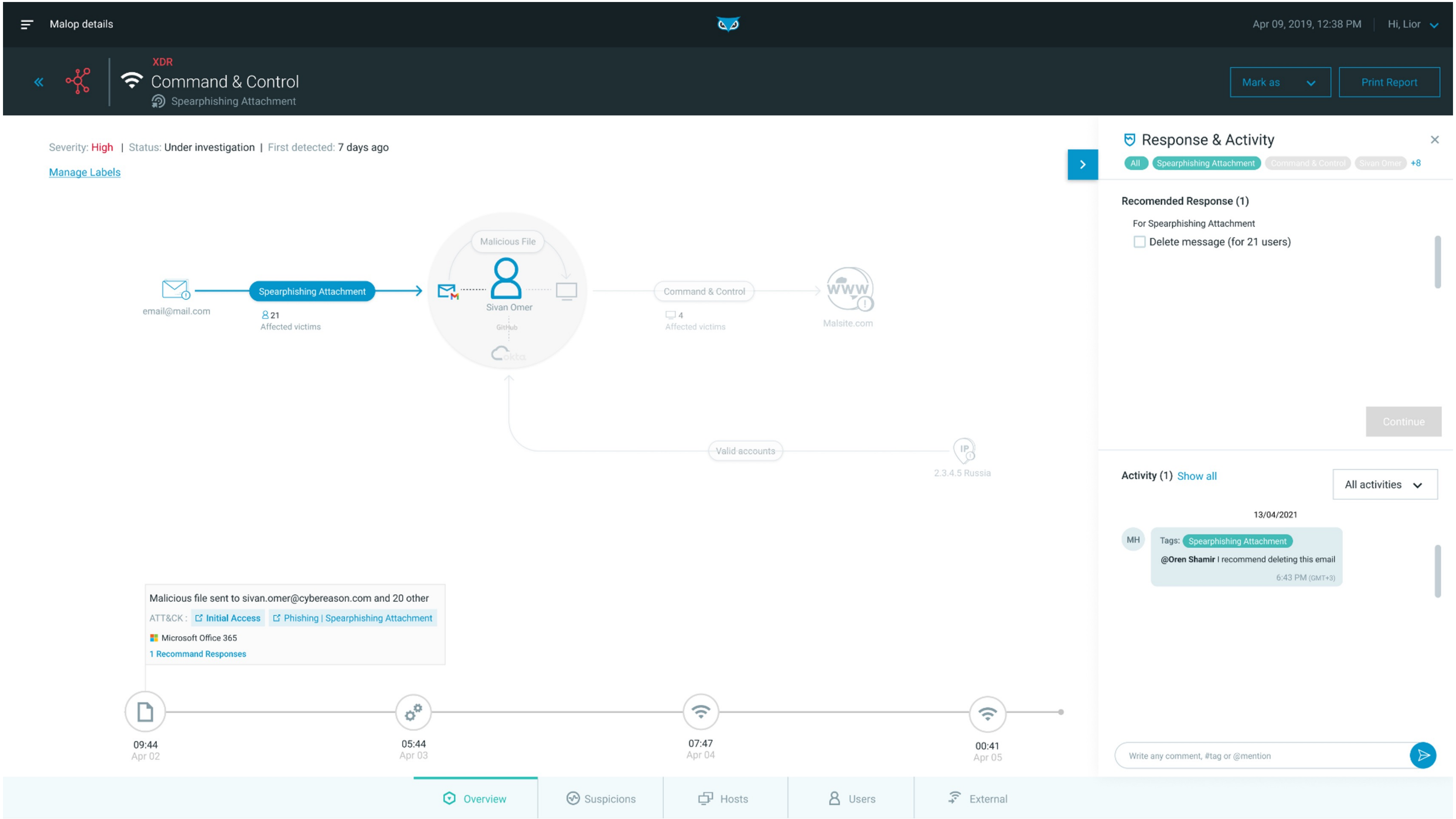
Activity (1) Show all

13/04/2021

MH Tags: Spearphishing Attachment

@Oren Shamir I recommend deleting this email

6:43 PM (GMT+3)



Command & Control

Spearphishing Attachment

Severity: High | Status: Under investigation | First detected: 7 days ago

Manage Labels

Malicious file sent to sivan.omer@cybereason.com and 20 other

ATT&CK : Initial Access | Phishing | Spearphishing Attachment

Microsoft Office 365

1 Recommand Responses

Response & Activity

Recomended Response (1)

For Spearphishing Attachment

☐ Delete message (for 21 users)

Activity (1) Show all

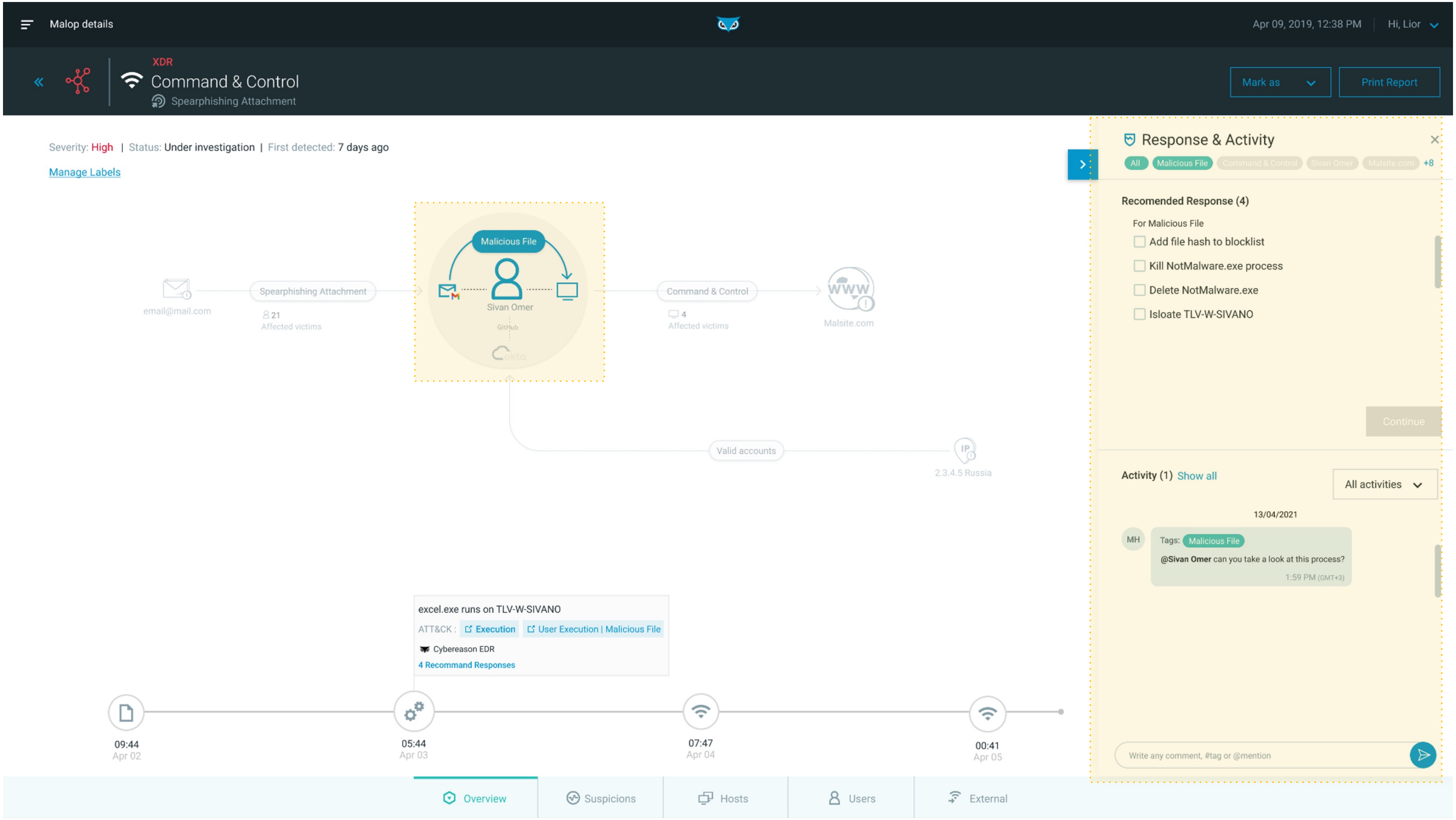
13/04/2021

MH

Tags: Spearphishing Attachment

@Oren Shamir I recommend deleting this email

6:43 PM (GMT+3)



Severity: High | Status: Under investigation | First detected: 7 days ago

excel.exe runs on TLV-W-SIVANO

ATT&CK : Execution User Execution | Malicious File

Cybereason EDR

4 Recommand Responses

Recomended Response (4)

For Malicious File

□ Add file hash to blocklist

□ Kill NotMalware.exe process

□ Delete NotMalware.exe

□ Isloate TLV-W-SIVANO

Activity (1) Show all

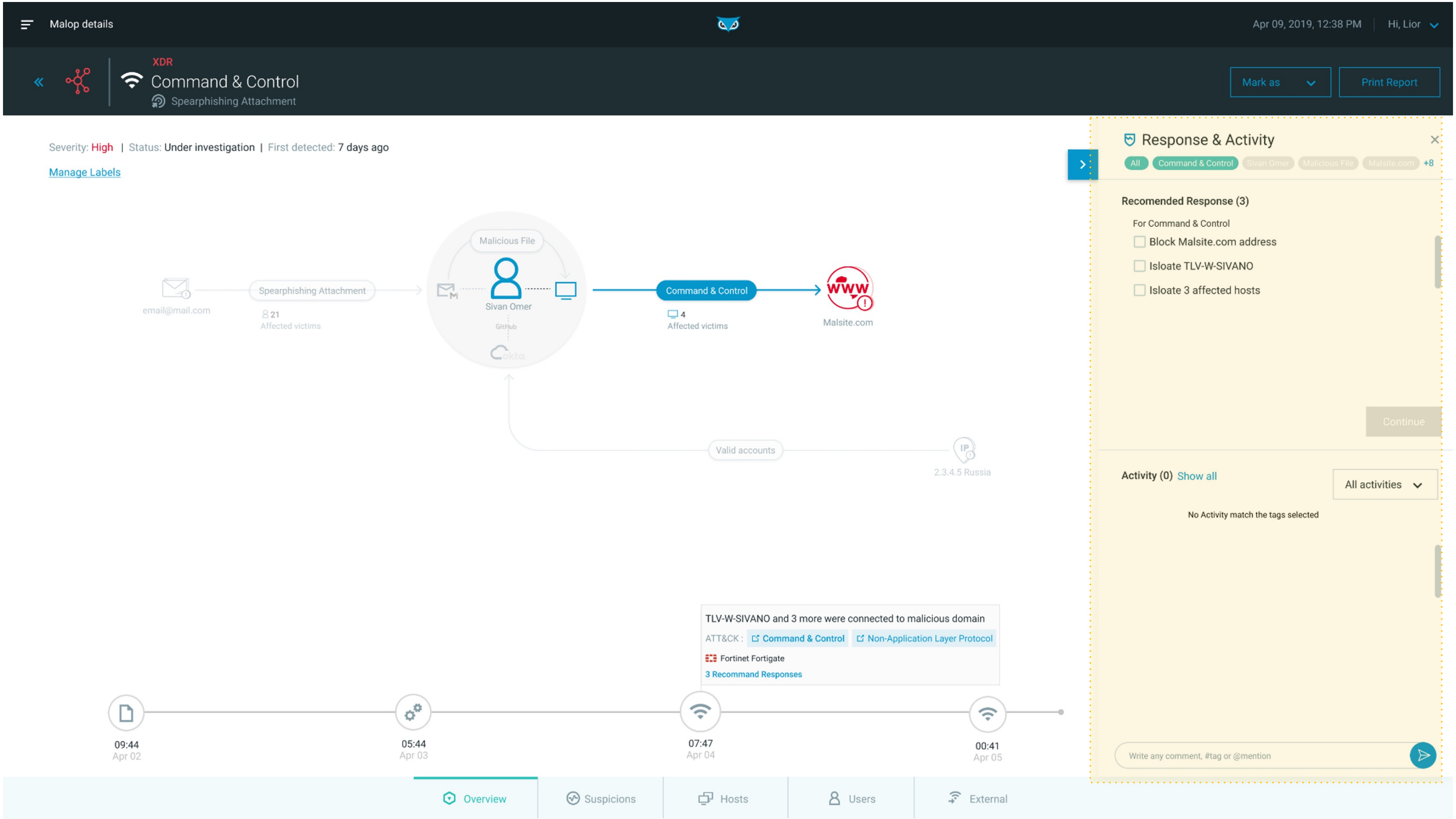
13/04/2021

MH

Tags: Malicious File

@Sivan Omer can you take a look at this process?

1:59 PM (GMT+3)



Severity: High | Status: Under investigation | First detected: 7 days ago

TLV-W-SIVANO and 3 more were connected to malicious domain

ATT&CK : Command & Control | Non-Application Layer Protocol

Fortinet Fortigate

3 Recommand Responses

Response & Activity

Recomended Response (3)

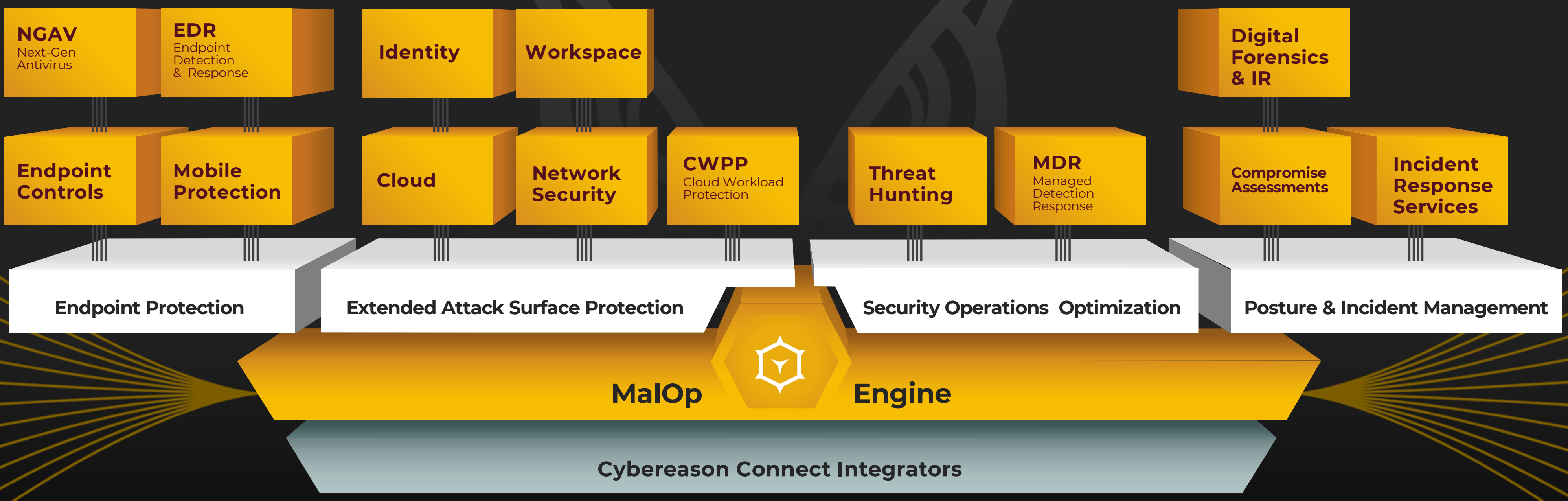
For Command & Control

- □ Block Malsite.com address
- □ Isloate TLV-W-SIVANO
- □ Isloate 3 affected hosts

Activity (0) Show all

No Activity match the tags selected

CYBEREASON XDR PLATFORM



NGAV Next-Gen Antivirus

EDR Endpoint Detection & Response

Identity

Workspace

Digital Forensics & IR

Endpoint Controls

Mobile Protection

Cloud

Network Security

CWPP Cloud Workload Protection

Threat Hunting

MDR Managed Detection Response

Compromise Assessments

Incident Response Services

Endpoint Protection

Extended Attack Surface Protection

Security Operations Optimization

Posture & Incident Management

MalOp Engine

Cybereason Connect Integrators

SUPPORTED SYSTEMS

WINDOWS · MAC & IOS · ANDROID · LINUX

DEPLOYMENT OPTIONS

CLOUD FIRST · HYBRID · ON-PREM · AIR-GAPPED

Let’s DEFEND