

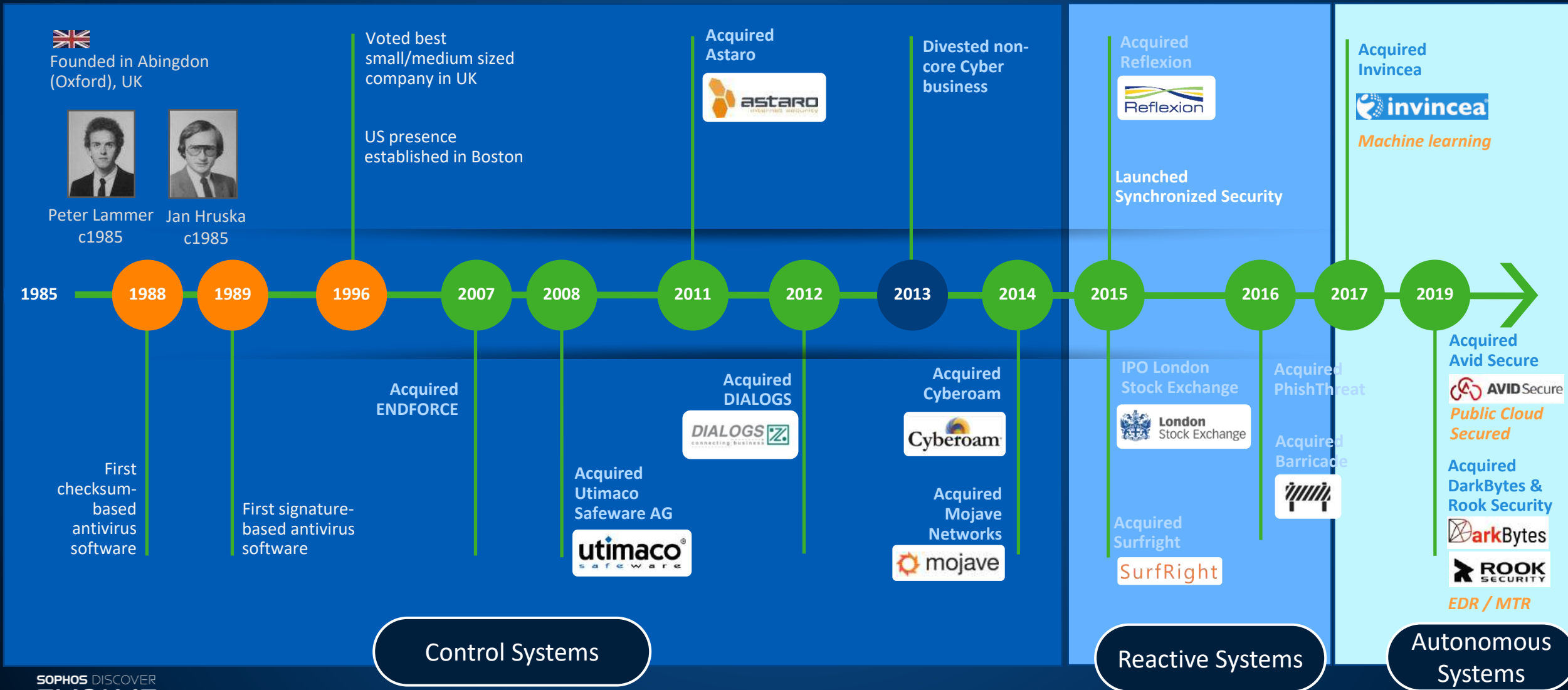
SOPHOS - Soluzioni di deep learning ed EDR, utilizzate per creare report in ambito forense

Giovanni Giovannelli
Senior Sales Engineer
Amelia, 18 Ottobre 2019

SOPHOS DISCOVER 2019
EVOLVE

Sophos History

Evolution to Synchronized Security Evolved





INTERCEPT

NOW WITH EDR

THE BEST JUST GOT BETTER

Endpoint Technologies

BANK
\$£€



Synchronized Security

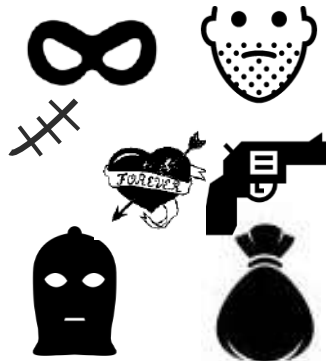
Anti
Virus

WANTED!



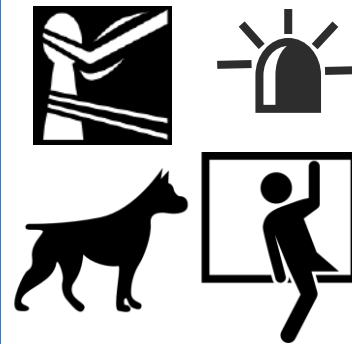
Deep
Learning

Suspicious!



Exploit
Prevention

Techniques!



Behavior
Monitoring

Actions!



Pre-Execution

Post-Execution

Anatomy of an Attack – The Cyber Kill Chain



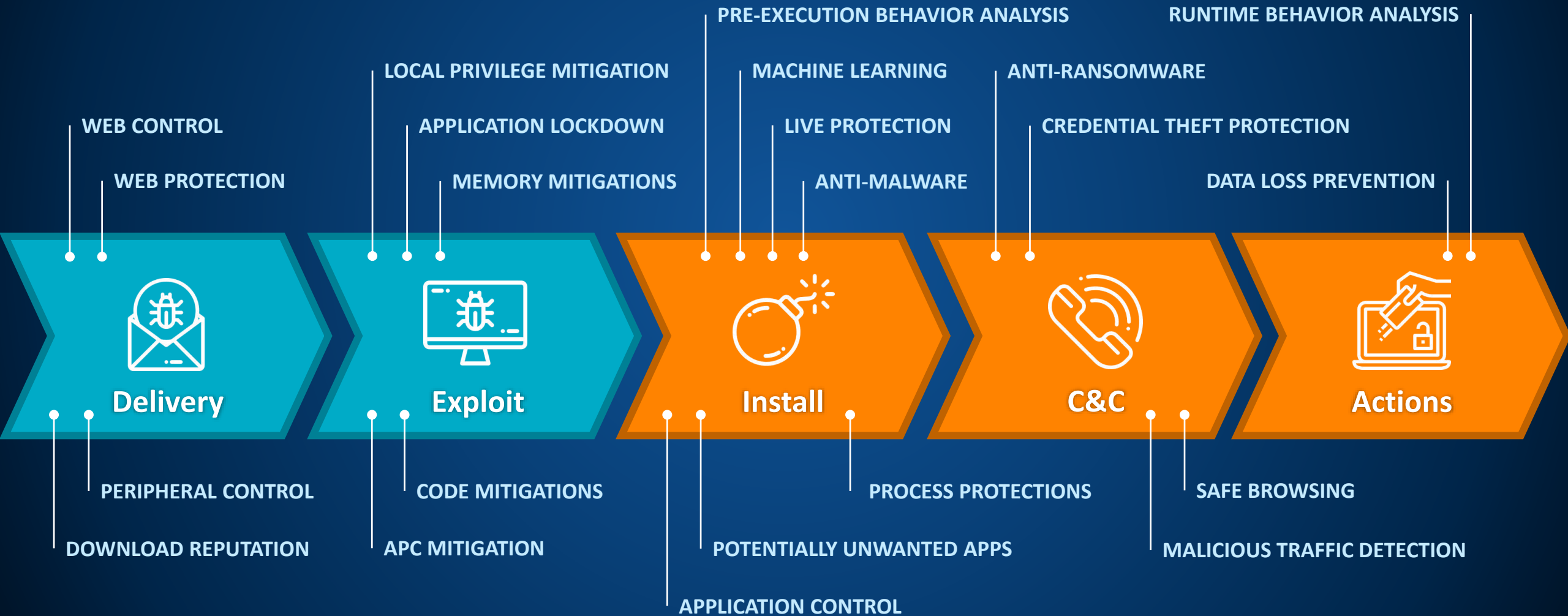
Layered Defense

Intercept X Advanced with EDR

SYNCHRONIZED SECURITY
Heartbeat

INVESTIGATE & REMOVE
Threat Cases
Sophos Clean M with SafeStore

DETECT & RESPOND
AI Expert Insights
Cross-Estate Hunting
SophosLabs Threat Intelligence



Power of the Plus

1.

Delivery and Instruction

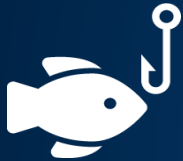
2.

Exploit and Execution

3.

BOOM!

\$\$\$



Phishing



Malicious URL



Command & Control



Code Cave



Weaponized Doc



Credential Theft



Privilege Escalation



Malicious Executable



Data Exfiltration



Ransomware



Server Attack



Application Exploit

Anti-Exploit

Web Control

Malicious Traffic

Anti-Exploit

Deep Learning

Hashes

DLP

EDR

Server

Phishing Training

Behavior

Anti-Ransomware

SOPHOS

Sophos Deep Learning Malware Detection Features

- Prevents both known and never-seen-before malware
- Blocks malware before it executes
- Does not rely on signatures
- Classifies files as malicious, potentially unwanted apps (PUA), or benign
- Extremely small footprint (under 20MB) with infrequent updates
- Detects malware in approximately 20 milliseconds
- Protects even when the host is offline
- Works out of the box, no additional training needed



BANK
\$£€

Synchronized Security



◀◀ REW

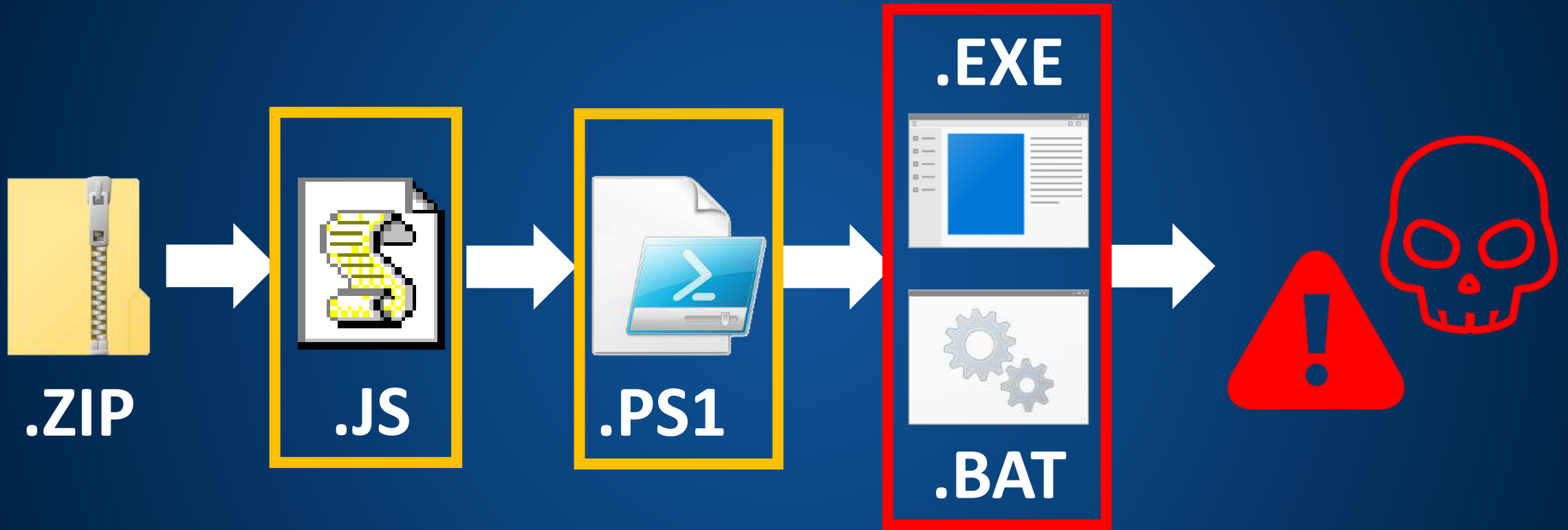
BANK
\$£€

Endpoint Detection
& Response

SophosLabs
Threat
Intelligence



Infection chain



Intercept X w/ EDR: Detect

SOPHOS
CENTRAL
Admin

Endpoint Protection
[Back to Overview](#)

ANALYZE

Dashboard

Logs & Reports

DETECTION AND REMEDIATION

Threat Cases

Threat Searches

Suspicious Events

MANAGE

People

Computers

CONFIGURE

Policies

Dashboard
[Overview](#) / Endpoint Protection Dashboard

Marcus Jones
ABC Corp - Primay Admin

?

Most Recent Threat Cases [See all cases](#)

Sophos generated

Admin generated

CREATED ON ▼	PRIORITY	TYPE	NAME	CONDITION	USER	DEVICE
Apr 18, 2016 12:23PM	High	Malware detected	Mal/ML-PE	Blocked and cleaned	William Morris	WMorrisPC
				Cleaned up	Brian Jones	BrianJComp
				Blocked	Brian Jones	BrianLaptop
				Running	Eryn Havers	ErynMac
				Clean up needed	Gina Baker	Gina Comp

Machine learning identifies top suspicious events to investigate

Top Suspicious Events [See all events](#)

NAME	DETECTED ON	THREAT SCORE	ENDPOINTS AFFECTED
Dropper.exe	July 31, 2018 09:01 AM	31	12
Quiver.exe	July 29, 2018 12:04 PM	25	3
DancingCats.exe	July 20, 2018 10:57 AM	23	23
Tweetbot.exe	July 04, 2018 09:07 AM	22	46
Adware.WPSOffice	July 03, 2018 5:37 PM	19	54
Packed.Generic.533	June 28, 2018 2:19 PM	17	11

Threat Search

Search for potential threats on your network

Enter one or more SHA 256 files hashes or file names,

192.151.42.1, Beef_Wellington.exe, c84c361b7f5dbaeac93828e60d2b5470fa

Searches on hashes or file names will return portable executable files with uncertain reputation.

Search

SOPHOS

Intercept X w/ EDR: Detect

Endpoint Protection

Back to Overview

ANALYZE

Dashboard

Logs & Reports

DETECTION AND REMEDIATION

Threat Cases

Threat Searches

Suspicious Events

MANAGE

People

Computers

CONFIGURE

Policies

Dashboard

Overview / Endpoint Protection Dashboard

Marcus Jones
ABC Corp - Primay Admin

Most Recent Threat Cases

See all cases

Sophos generated

Admin generated

CREATED ON ▼	PRIORITY	TYPE	NAME	CONDITION	USER	DEVICE
Apr 18, 2016 12.23PM	High	Malware detected	Mal/ML-PE			
Apr 17, 2016 12.23PM	Medium	Exploit	Exploit Lockdown			
Apr 16, 2016 12.23PM	Low	Malicious traffic	Troj/PDFJs-AIA			
Apr 15, 2016 12.23PM	High	Ransomware	Exploit Cryptogua			
Apr 14, 2016 12.23PM	High	PUA	Troj/Loic-A	Clean up needed	Gina Baker	Gina Comp

Easily search by IP address, file name, hash, etc.

Top Suspicious Events

See all events

NAME	DETECTED ON	THREAT SCORE	ENDPOINTS AFFECTED
Dropper.exe	July 31, 2018 09:01 AM	31	12
Quiver.exe	July 29, 2018 12:04 PM	25	3
DancingCats.exe	July 20, 2018 10:57 AM	23	23
Tweetbot.exe	July 04, 2018 09:07 AM	22	46
Adware.WPSOffice	July 03, 2018 5:37 PM	19	54
Packed.Generic.533	June 28, 2018 2:19 PM	17	11

Threat Search

Search for potential threats on your network

Enter one or more SHA 256 file hashes or file names,

192.151.42.1, Beef_Wellington.exe, c84c361b7f5dbaeac93828e60d2b5470fa

Searches on hashes or file names will return portable executable files with uncertain reputation.

Search

Threat Search

Campagna Ransomware FTCODE veicolata in Italia

02/10/2019

ftcode powershell ransomware

Osservato in Italia a partire da settembre 2019, il ransomware denominato **FTCODE** ha lo scopo di cifrare i file e, rinominarli con estensione .FTCODE, al fine di ottenere un riscatto dalle potenziali vittime.

Il CERT-PA ha avuto evidenza della campagna odierna grazie alle segnalazioni pervenute da parte di comuni e di PA centrali. Nel caso specifico il malware viene veicolato attraverso l'invio di mail, sia PEO che PEC precedentemente compromesse, contenenti in allegato un archivio compresso all'interno del quale è presente un file .doc con macro malevola. Di seguito uno screenshot della mail utilizzata per la campagna in oggetto.

Da responsabilesettorellpp.comune.cassanoalloionio.cs@asmepec.it ☆

Oggetto **Fatture scadute 2019 2644199**

A pec@pec.comune.madignano.cr.it ☆

In allegato trova la fattura. 611608

Cordiali saluti

DOMAIN

connect.simplebutmatters.com
home.southerntransitions.net
connect.southerntransitions.com
home.selltokengarff.com
home.ktxhome.com
home.goteamrob.com
twitter.crtcostruzionisrl.com
my.mylifeamongthewomen.com
home.hopedaybook.com
getpdfreader.13stripesbrewery.com
getpdfreader.lilupicks.com
home.artdietfitness.com
home.parkandhome.com
home.mmaut.com
aweb.theshotboard.info
cofee.theshotboard.net
home.tith.in
donald.tilmonday.com

SHA256

7E458B1FB5CD1D6AA33663FD6E749C8C3FBEC152AC279B22C5FE4461FD2CBD13
EBFC3CF4A57981B84F6E651D3A5DC145EB1B54D41D75BD94F15ECB0E5826D56C
1D59F58777358E769E8C943BDF27801B77D5FC43057D2C02DEFCCC8A4730128C
0E88623431DA59C1A953D025A37E9737C1F256FF523189FE5CB20974B4125284
5995d9e63de7336713cfd5d6aad4955f0f0700835e9a3def625a880f6b62c08e
417f0316d938f659d91049d8f0985ef41dca140f712be51b44b131a9fe96e74b
1222299c4796779f3b29ddd8e28d6515e85ba42935c74c94e63c571e3e80d246
636aef37fb54cc2d979079a4d30aaf3a6e2865359486a98dea65def695e25839
7f870083a645d47078484ee78a9f6f65c9b426e595f4d9a5af6ed839e283c086
24d6087d2f32e88bedde34e81bad584dfb54643557e8134d341514949c5eae95
e02a49ad6b6dfcfbd33ddb53725421700e6fe2acd4205c46b42409df9d58473d

Guided Incident Response

Security analysis: Cross-estate threat hunting

Endpoint Protection

Back to Overview

ANALYZE

Dashboard

Logs & Reports

DETECTION AND REMEDIATION

Threat Cases

Threat Searches

Suspicious Events BETA

MANAGE

People

Computers

CONFIGURE

Policies

System Settings

Protect Devices

ENHANCED PROTECTION

Explore Products

Endpoint Protection - Threat Searches

Overview / Endpoint Protection Dashboard / Threat Searches

Marcus Jones
ABC Corp - Primary Admin

?

New threat search

Search for potential threats on your network

Enter one or more SHA 256 file hashes or file names.

Searches on hashes or file names will return portable executable files with uncertain reputation.

Search

Saved searches

Search Type: All

Delete

<input type="checkbox"/>	NAME ▼	CREATED ON ▼	CREATED BY ▼	TYPE ▼	STATUS ▼
<input type="checkbox"/>	Wannacry	Apr 12, 2016 12.39PM	Glen	From threat case	Running
<input type="checkbox"/>	mw9h234t8hz0927g....	Apr 12, 2016 12.36PM	Glen	Direct search	Running
<input type="checkbox"/>	5a8d62350ee811aeb08470d56...	Apr 12, 2016 12.35PM	Glen	Direct search	Complete
<input type="checkbox"/>	d2fd908365cd489de4a4dc711...	Apr 12, 2016 12.34PM	Eric	From threat case	Complete
<input type="checkbox"/>	Wannacry	Apr 12, 2016 12.33PM	Glen	From threat case	Complete
<input type="checkbox"/>	Dodgydropper	Apr 12, 2016 12.32PM	Glen	From threat case	Complete
<input type="checkbox"/>	www.commandandcontrol.com	Apr 12, 2016 12.31PM	Eric	Direct search	Complete
<input type="checkbox"/>	badthing.exe	Apr 12, 2016 12.30PM	Eric	Direct search	Complete
<input type="checkbox"/>	8f6afac9a7b42fb5a8e75e96b...	Apr 12, 2016 12.29PM	Eric	From threat case	Complete
<input type="checkbox"/>	Glen's search for malware	Apr 12, 2016 12.28PM	Eric	Direct search	Complete

Threat Analysis Center

- EDR Across Endpoint and Server

The screenshot displays the Sophos Threat Analysis Center interface. On the left is a dark sidebar with the 'SOPHOS CENTRAL Admin' logo and navigation links: 'Threat Analysis Center', 'Back to Overview', and a 'DETECTION AND REMEDIATION' section containing 'Dashboard', 'Threat Cases', and 'Threat Searches'. The main content area is titled 'Threat Analysis Center - ML/PE-A' and includes a breadcrumb trail: 'Overview / Threat Analysis Center Dashboard / Detected Threat Cases / ML/PE-A'. In the top right corner, there are links for 'Help' and 'Administrator' (Super Admin). A horizontal timeline illustrates the threat's progression: RDS (IP 192.168.50.135) → Root Cause (Windows Explorer) → Beacon (highscore.exe) → Detected (Jan 21, 2019 6:49 PM) → Cleaned. Below this, the 'Summary' section lists: Detection name: ML/PE-A; Root cause: explorer.exe; Possible data involved: 1 business file; Where: On RDS; When: Detected on Jan 21, 2019 6:49 PM. The 'Suggested next steps' section includes: 'Set a status for the threat case' (with 'Priority: Medium' and 'Status: New' dropdowns), 'Isolate this device while you investigate', and 'Scan the device'.

All threat cases, alerts and searches, across all device types

Hardest part of EDR: Knowing where to start

#1

Desired EDR feature

**Identification of
Suspicious Events**

AI Driven Threat Hunting

Groundbreaking machine learning from SophosLabs data science team (coming soon)

Automated Hunting

Prioritized Cases

Endpoint Protection - Suspicious Events

Overview / Endpoint Protection Dashboard / Suspicious Events

Help

Administrator

Super Admin

Suspicious Events

Suspicious Events History

Search

All categories

Executed or not

Clean and block

Dismiss

	Date detected	Event name	SHA	Category	Threat ...	Endpoint...	Executed	Latest t...
<input type="checkbox"/>	Oct 08, 2018 10:28 AM	Recipeaddictstool.exe	546ec58d0134ea64611e12d7e3a867793e...	Malware	93	12	Yes	View
<input type="checkbox"/>	Sep 19, 2018 5:01 AM	PasswordRevealer!g1	FA2F1C8562FC59584F79835F6F803382...	Malware	87	1	Yes	View
<input type="checkbox"/>	Sep 25, 2018 11:12 AM	Packed.Generic.533	038CA04BA7E930DA3F83DD1DBDA150B...	Malware	82	7	No	View
<input type="checkbox"/>	Sep 28, 2018 1:37 PM	Tweetbot.exe	25B293193D0B4362CE46F7AD6A9C346...	PUA	67	2	Yes	View
<input type="checkbox"/>	Oct 05, 2018 6:57 AM	Quiver.exe	0F4E5BE14ED5650F2F03522DEAD34FC...	Malware	58	6	No	View
<input type="checkbox"/>	Oct 06, 2018 8:04 AM	Dropper.exe	0078AF329DAEEE0B41A5E7CA069A3E4...	PUA	50	8	Yes	View

1 - 6 of 6 < >

Threat intelligence analysis: Access on-demand threat intelligence curated by SophosLabs

[>](#)

SearchClean and block

[What does this do?](#)

Process details : recipeaddictstool.exe

Process details

Report summary

Machine learning analysis

File properties

File breakdown

Reputation at time case was created:Uncertain

▼

Known bad reputationKnown good reputation

Detection status: Not detected at time case was created
You should investigate this item to determine whether it is harmful.

SOPHOSLABS Threat Intelligence
Current report created: Sep 25, 2018 7:32 PM

Request Latest Intelligence

Note: Requesting the latest intelligence will cause your files to be sent to Sophos for additional analysis. [Learn More](#)

Path:
c:\users\martynroberts\downloads\recipeaddictstool new 25 09 2018\recipeaddictstool.exe

Name:recipeaddictstool.exe

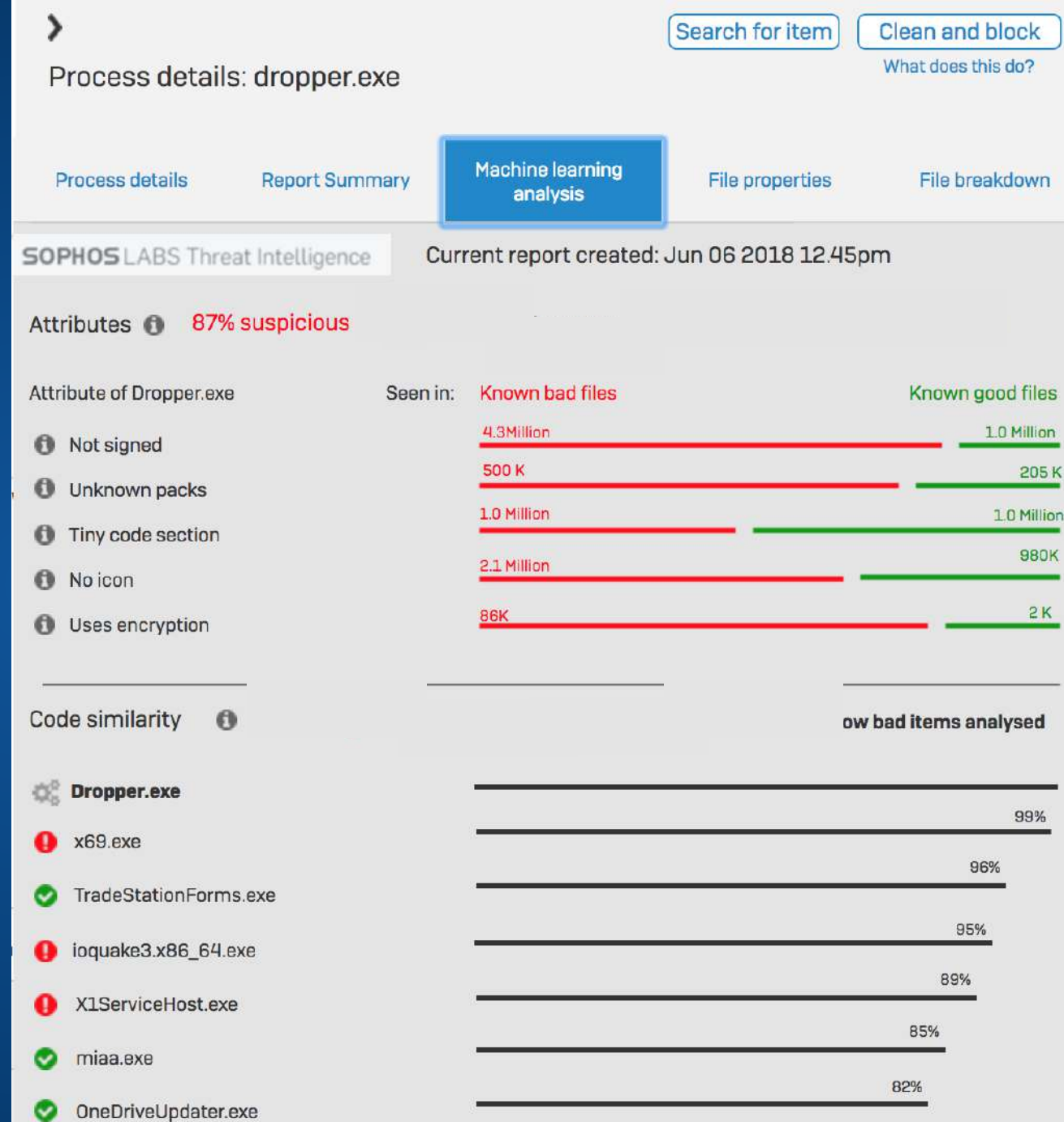
Process ID:592

SHA-256:5e147d105b93a01b0f756f2afd2f44a8a27914c42d948c0e3051a2db3657c453

Start Time:Sep 26, 2018 2:49 AM

Malware Analysis

Analyze files using deep learning



SOPHOS

Details

Analyze | Activity record

Showing ☒ Processes [4] ☒ Files [21] ☒ Network connections [1] ☒ Registry keys [0]

[Click here for IX only version](#)

The graph illustrates the activity of **Chrome.exe** as the central process. It shows the following connections:

- Parent to:** Outlook.exe
- Child:** 20 Files
- Read:** 1 business file
- Write:** Dropper.exe, which in turn **Writes** to Bedthing.exe.
- Network:** A connection to the Internet (represented by a globe icon).

A legend in the top left corner shows a gear icon with an orange triangle, labeled **Dropper.exe**.

Respond with the click of a button

SOPHOS
CENTRAL
Admin

Endpoint Protection

Back to Overview

ANALYZE

Dashboard

Logs & Reports

DETECTION AND REMEDIATION

Threat Cases

Threat Searches

Suspicious Events

MANAGE

People

Computers

Endpoint Protection - Search Details

Overview / Endpoint Protection Dashboard / Threat Searches / Threat Search Results / Search Details

Marcus Jones
ABC Corp - Primary Admin

3 of 3 items found on Athomson Mac belonging to Anna Thomson

Create forensic snapshot

SHA256 Hash	Name	Reputation	Type	Cleaned	Path	Actions
e92e02d1f752778c13c1d7883c0781a335b88fcd4158b8e89810623a390c12	Installer.exe	Uncertain	Process	No	c:\program files\path name	<div>Actions</div> <div>Clean and block</div>
2bf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824	Updater.exe	Uncertain	Process	No	c:\program files\path name	<div>Actions</div>
					c:\program files\second path name	<div>Actions</div>
					c:\program files\third path name	<div>Actions</div>
					c:\program files\fourth path name	<div>Actions</div>
3cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824	Keylogger.exe	Bad: Malware	Process	No	c:\program files\path name which is long and will wrap in the table row	<div>Actions</div>

Clean and block

You're about to clean up this item on any computer where we've found it and block it on all your computers.

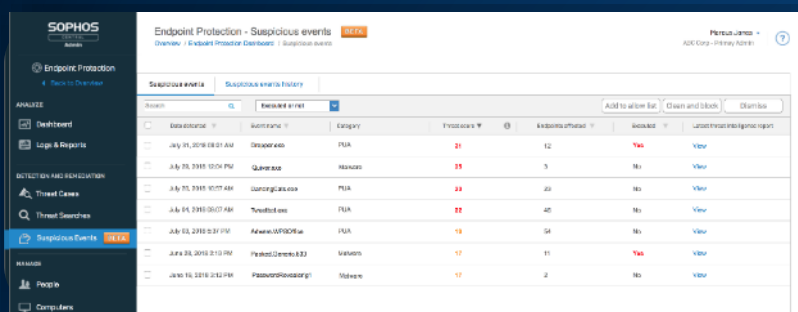
Why are you blocking this item?

Clean and remove this suspicious file and block it

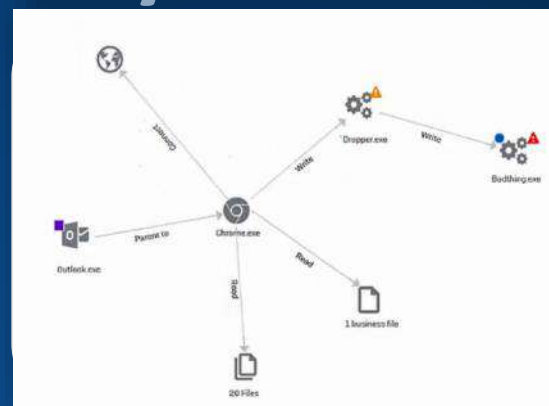
Note: You can see the items you've blocked or unblock them again in your Blocked Items list.

Cancel Confirm

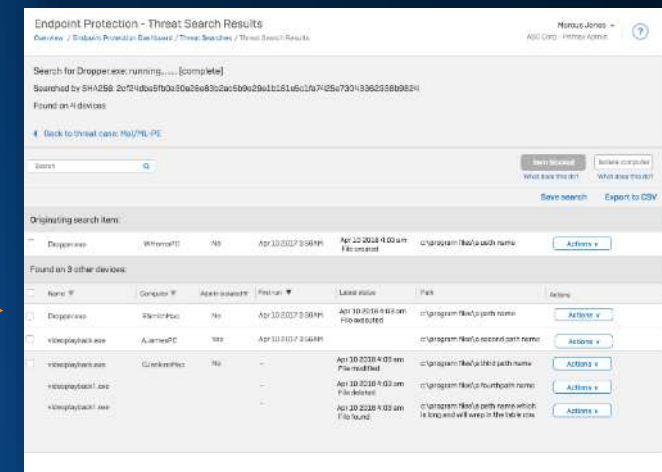
Day in the Life of an Analyst



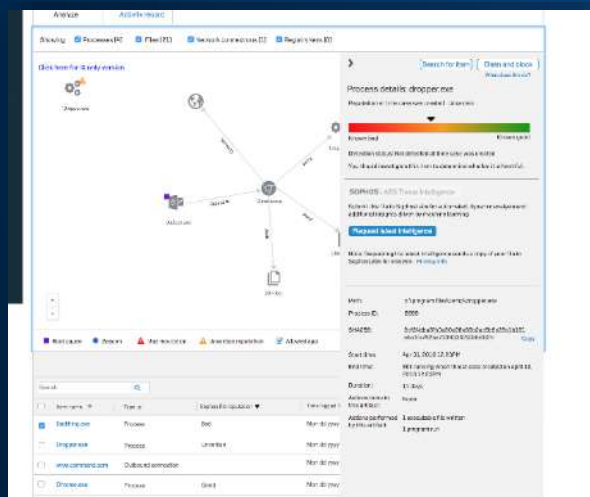
Identifies top incident as Dropper.exe via Threat Indicators



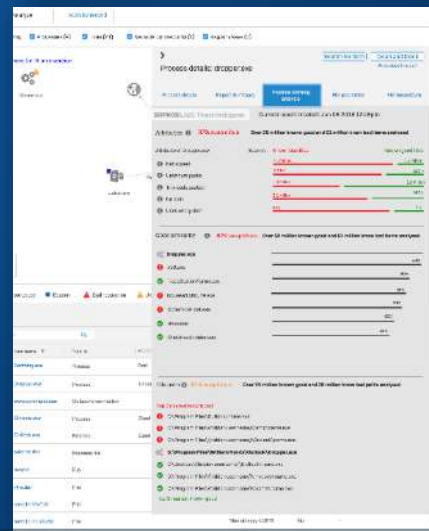
Sees Dropper.exe distributed malware (which was blocked)



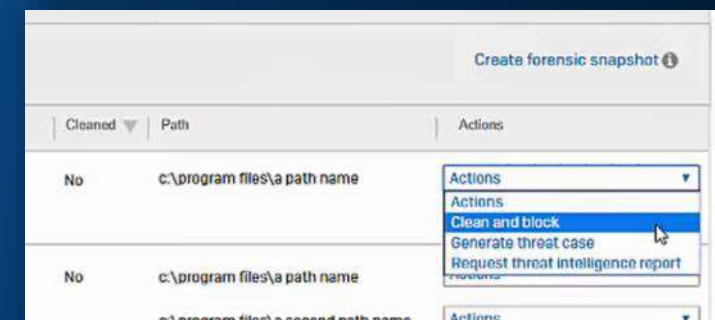
Determines where else Dropper.exe exists



Requests more details from SophosLabs



Uses Deep Learning to determine file is malicious



Remediates threat "Clean and block"

Intercept X w/ EDR: Respond

Respond to incidents with a click of a button

- Full disclosure of potential threat activity
- Isolate machine(s)
- Clean file, blacklist or whitelist
- Investigate further, create forensic snapshots

The screenshot shows the Sophos EDR console interface. On the left is a sidebar with navigation options: 'Endpoint Protection', 'Back to Overview', 'ANALYZE' (with 'Dashboard' and 'Logs & Reports'), 'DETECTION AND REMEDIATION' (with 'Threat Cases', 'Threat Searches', and 'Suspicious Events'), and 'MANAGE' (with 'People' and 'Computers'). The main area displays a table of threat events. The table has columns for 'SHA256 Hash', 'Name', 'Reputation', 'Type', 'Cleaned', and 'Path'. A red arrow points to the 'Actions' column of the first row, which is expanded to show options: 'Actions', 'Clean and block', 'Generate threat case', and 'Request threat intelligence report'.

SHA256 Hash	Name	Reputation	Type	Cleaned	Path	Actions
e92e02d1f752778c13c1d788ac0781a339b86c04158b5e8f9810623a390c12	Installer.exe	Uncertain	Process	No	c:\program files\...	Actions Clean and block Generate threat case Request threat intelligence report
2bf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824	Updater.exe	Uncertain	Process	No	c:\program files\... path name	Actions
					c:\program files\... second path name	Actions
					c:\program files\... third path name	Actions
					c:\program files\... fourth path name	Actions
3cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824	Keylogger.exe	Bud. Malware	Process	No	c:\program files\... path name which is long and will wrap in the table row	Actions

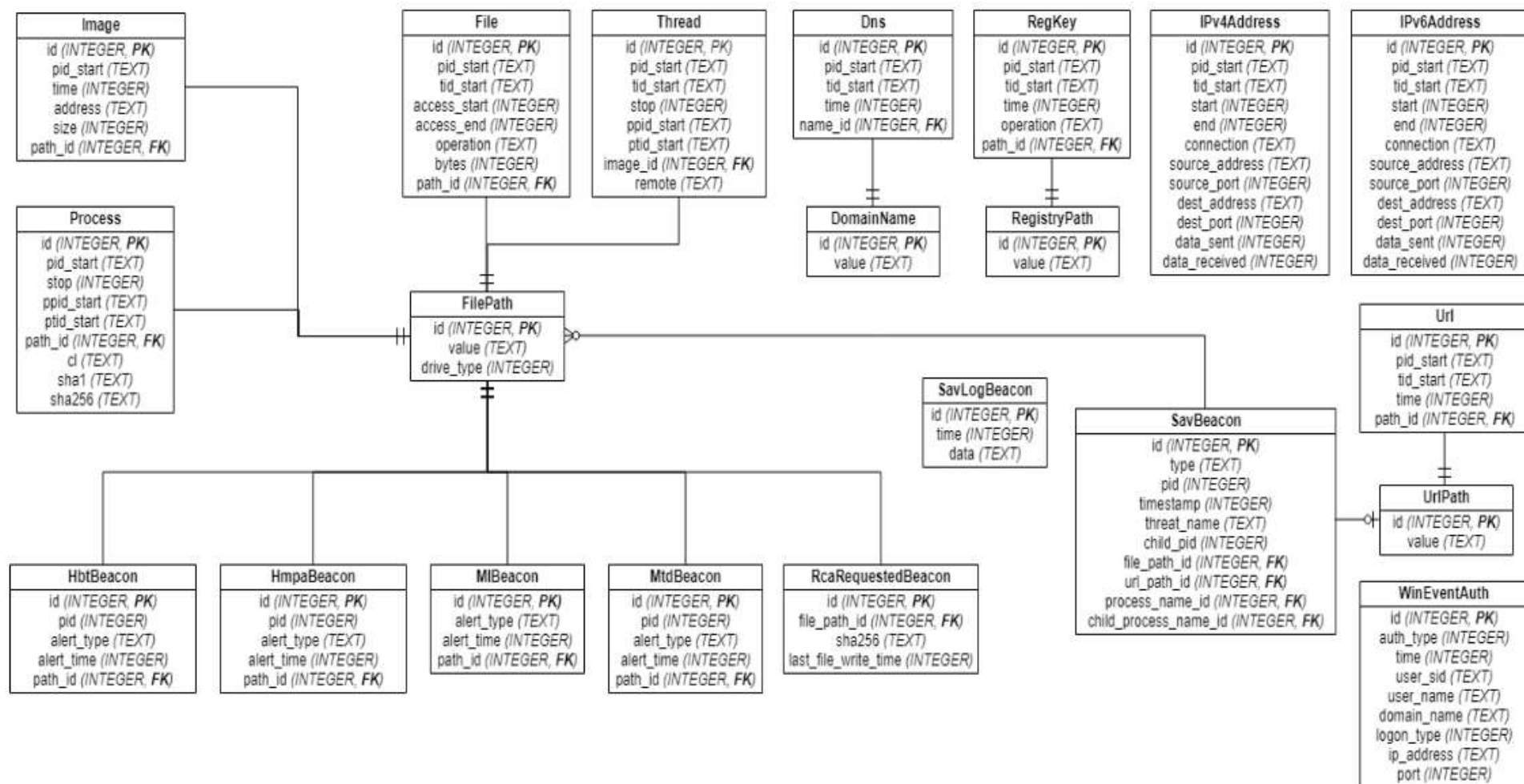
The 'Clean and block' dialog box contains the following text: 'You're about to clean up this item on any computer where we've found it and block it on all your computers.' Below this is a text input field with the value 'Clean and remove this suspicious file and blacklist it'. A note at the bottom states: 'Note: You can see the items you've blocked or unblock them again in your Blocked Items list.' At the bottom right are 'Cancel' and 'Confirm' buttons. An orange arrow points from the 'Clean and block' option in the table's actions menu to this dialog box.

The 'Suggested next steps' panel lists the following actions:

- Set status and priority for the case (New High)
- Investigate 1 process we've marked with an "uncertain" reputation. See graph below for details
- Isolate the computer while you investigate.
- Scan the computer

The Forensic Snapshot

Database Model



The Forensic Snapshot

The screenshot displays the 'DB Browser for SQLite' application window. The title bar indicates the file path: 'C:\Users\sophos.SOPHOS\Desktop\snapshot.sql'. The menu bar includes 'File', 'Edit', 'View', and 'Help'. The toolbar contains icons for 'New Database', 'Open Database', 'Write Changes', and 'Revert Changes'. The main interface has four tabs: 'Database Structure', 'Browse Data', 'Edit Pragma', and 'Execute SQL'. The 'Database Structure' tab is active, showing a tree view of 22 tables. The table list includes: Dns, DomainName, File, FilePath, FileReputation, HbtBeacon, HmpaBeacon, IPv4Address, IPv6Address, Image, IpsBeacon, MlBeacon, MtdBeacon, Process, RcaRequestedBeacon, RegKey, and RegistryPath. Each table entry shows its name, type, and schema. The 'Edit Database Cell' dialog is open on the right, showing a text input field and buttons for 'Import', 'Export', and 'Set as NULL'. Below the input field, it states 'Type of data currently in cell: NULL' and '0 byte(s)'. The 'Remote' tab is also visible, showing a table with columns: Name, Commit, Last modified, and Size. The bottom status bar shows 'UTF-8' encoding.

DB Browser for SQLite - C:\Users\sophos.SOPHOS\Desktop\snapshot.sql

File Edit View Help

New Database Open Database Write Changes Revert Changes

Database Structure Browse Data Edit Pragma Execute SQL

Create Table Create Index Modify Table Delete Table

Name	Type	Schema
Tables (22)		
Dns	CREATE TABLE "Dns" ("id" INTEGER PRIMARY KEY,"pid_start	
DomainName	CREATE TABLE "DomainName" ("id" INTEGER PRIMARY KEY	
File	CREATE TABLE "File" ("id" INTEGER PRIMARY KEY,"pid_start	
FilePath	CREATE TABLE "FilePath" ("id" INTEGER PRIMARY KEY,"value	
FileReputation	CREATE TABLE "FileReputation" ("id" INTEGER PRIMARY KEY	
HbtBeacon	CREATE TABLE "HbtBeacon" ("id" INTEGER PRIMARY KEY,"p	
HmpaBeacon	CREATE TABLE "HmpaBeacon" ("id" INTEGER PRIMARY KEY,	
IPv4Address	CREATE TABLE "IPv4Address" ("id" INTEGER PRIMARY KEY,"	
IPv6Address	CREATE TABLE "IPv6Address" ("id" INTEGER PRIMARY KEY,"	
Image	CREATE TABLE "Image" ("id" INTEGER PRIMARY KEY,"pid_st	
IpsBeacon	CREATE TABLE "IpsBeacon" ("id" INTEGER PRIMARY KEY,"pi	
MlBeacon	CREATE TABLE "MlBeacon" ("id" INTEGER PRIMARY KEY,"ale	
MtdBeacon	CREATE TABLE "MtdBeacon" ("id" INTEGER PRIMARY KEY,"p	
Process	CREATE TABLE "Process" ("id" INTEGER PRIMARY KEY,"pid_s	
RcaRequestedBeacon	CREATE TABLE "RcaRequestedBeacon" ("id" INTEGER PRIMA	
RegKey	CREATE TABLE "RegKey" ("id" INTEGER PRIMARY KEY,"pid_s	
RegistryPath	CREATE TABLE "RegistryPath" ("id" INTEGER PRIMARY KEY,"	

Edit Database Cell

Mode: Text Import Export Set as NULL

Type of data currently in cell: NULL
0 byte(s)

Apply

Remote

Name	Commit	Last modified	Size
------	--------	---------------	------

SQL Log Plot DB Schema Remote

UTF-8

Core Security Capabilities

Protect



Prevent attacks and proactively
secure known vulnerabilities

Detect



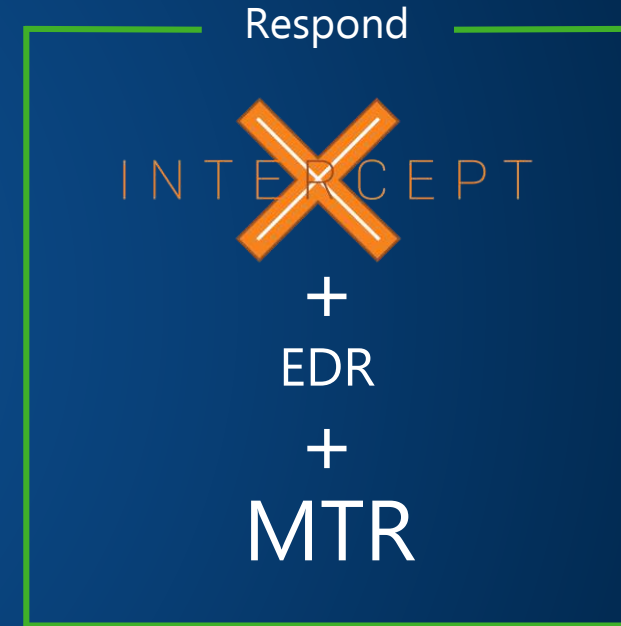
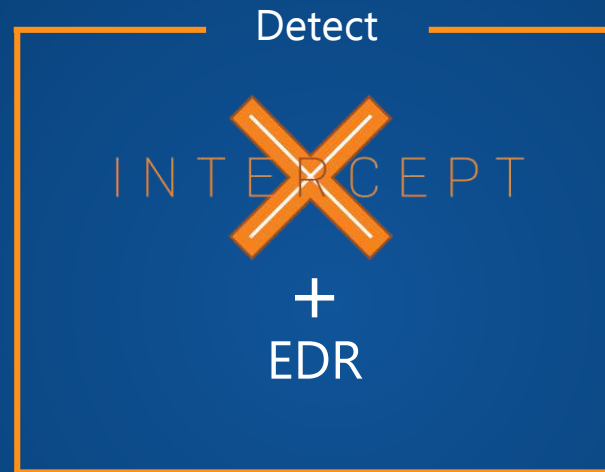
Detect active attacks and identify
potentially malicious behaviors

Respond



Rapidly investigate and remediate
incidents to minimize impact

Core Security Capabilities



Response Modes

You choose the best way for our MTR team to work alongside you

Notify

We notify you about the detection and provide detail to help you in prioritization and response

Collaborate

We work with your internal team or external point(s) of contact to respond to the detection

Entrust


We handle containment and neutralization actions and will inform you of the action(s) taken

PARTNER SOPHOS: S.O.S. COMPUTER 2000

www.soscomputer2000.eu/?page_id=155

Intercept X + EDR

SOPHOS PRODOTTI BUSINESS ▾ PRODOTTI HOME ▾ PARTNER ▾ SUPPORTO ▾ ☰

 Intercept X Endpoint [Funzionalità](#) [Prova gratuita](#) [Specifiche tecniche](#) [Demo](#) [Preventivo](#) [Informazioni sull'acquisto](#)

The Best Just Got Better. Sophos Intercept X – Ora con EDR. [Ulteriori informazioni](#)



PARTNER SOPHOS: S.O.S. COMPUTER 2000

www.soscomputer2000.eu/?page_id=155

Sophos MTR



The screenshot displays the Sophos Managed Threat Response (MTR) website. The top navigation bar is blue with the 'SOPHOS' logo on the left and links for 'PRODOTTI BUSINESS', 'PRODOTTI HOME', 'PARTNER', and 'SUPPORTO' on the right. Below this, a white sub-header contains the 'Managed Threat Response' title with a circular icon, and links for 'Features', 'How to Buy', 'Get Pricing', and 'Contact Us'. The main content area features a dark background with a central graphic of a glowing orange and blue lens or sensor. Below the graphic, the text 'Managed Threat Response' is written in a large, white, sans-serif font. The bottom left corner of the image shows the 'SOPHOS' logo in white.

SOPHOS

Cybersecurity made simple.