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

EDR zacznij z mocniejszą ochroną

Reakcja na incydent z przewodnikiem

Dodaj ekspertyzę, przy obecnej liczbie pracowników

Źródło: Ankieta bezpieczeństwa Sophos Q1 2019 na bazie 3100 decydentów IT w 12 krajach na pięciu kontynentach

Najlepsza ochrona punktów końcowych

Intercept X

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

MRG Effitas
Efficacy Assessment & Assurance

#1 Malware Protection
#1 Exploit Protection

SE Labs AAA APR-JUN 2018 SMALL BUSINESS ENDPOINT PROTECTION

#1 Small Business Protection

SE Labs AAA APR-JUN 2018 ENTERPRISE ENDPOINT PROTECTION

#1 Enterprise Protection

NSS LABS RECOMMENDED

#1 Endpoint Protection

Gartner

Leaders Quadrant

FORRESTER®

Endpoint Security Leader

SOPHOS

Sophos Intercept X: Inteligentny EDR

Spostrzeżenie
Czynnik ludzki, z priorytetem, i możliwe do działania

Badaj
Szukaj, śledź, i poluj

Dane
Skorelowanie, określone i zorganizowane

AI Expert Insights

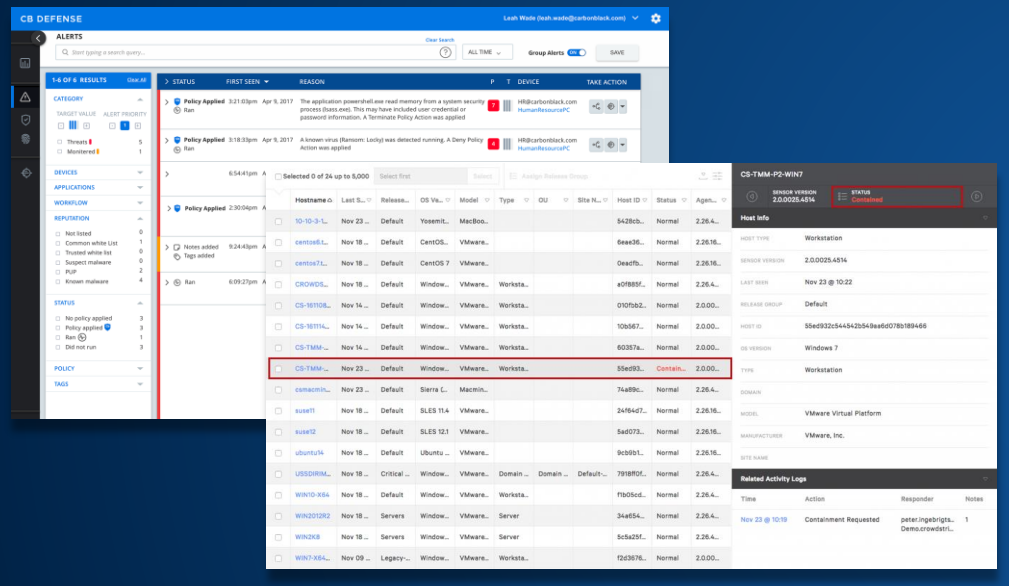
- ***EDR Zacznij z najsilniejsza ochroną***
  Zatrzymaj naruszenie polityki bezpieczeństwa zanim oni zaczną
- ***Dodaj ekspertyzę, przy obecnej liczbie pracowaników***
  “Eksperci z pudełka”
- ***Guided Incident Response***
  Respond with the Click of the Button

Cyberbezpieczeństwo Experts-in-a-Box

SOPHOS

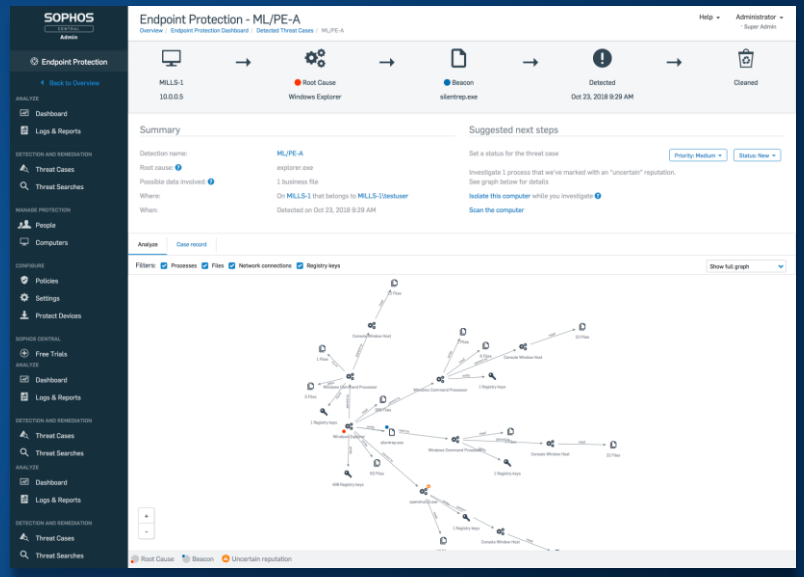
Ewolucja EDR

Pierwsza generacja



- Niekończące się dane
- Ręczne Polowanie
- Zasobochłonne

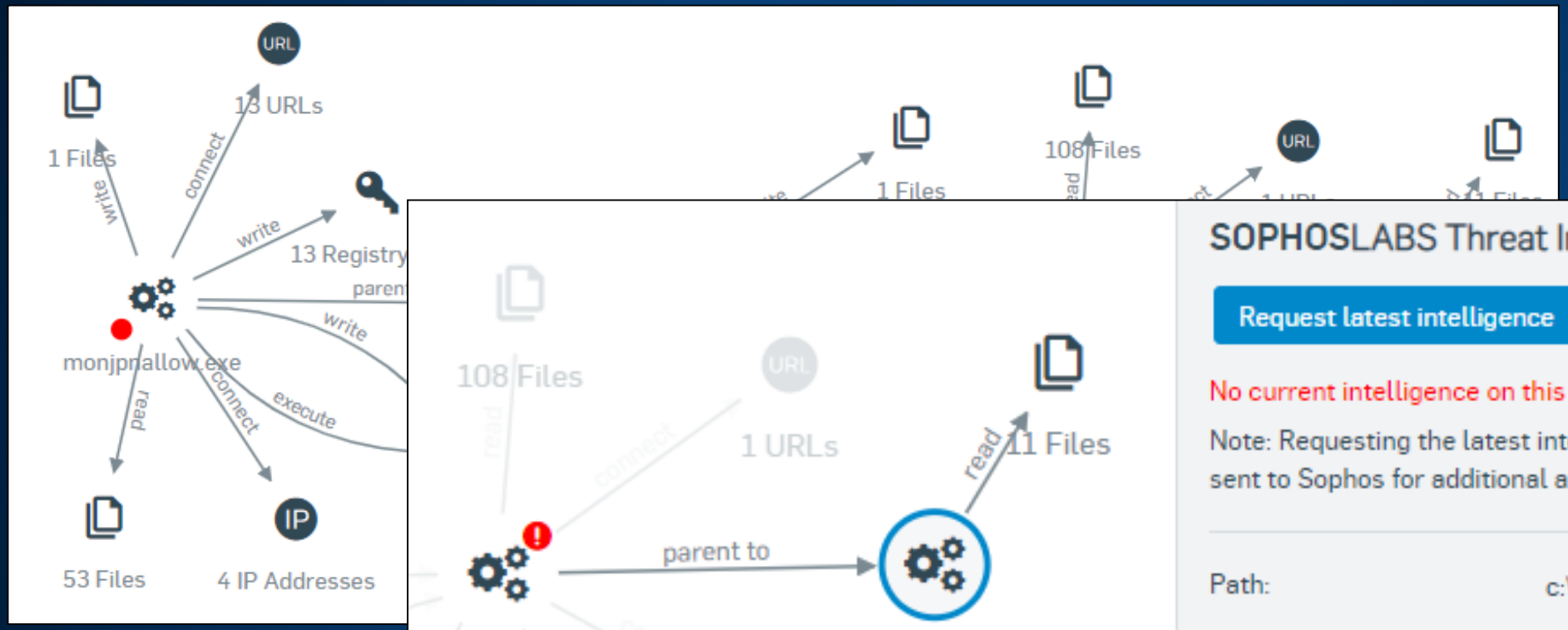
Druga generacja



- Inteligenta Informacja
- AI Automatyzacja
- Skalowalna ekspertyza

SOPHOS

Threat Cases



SOPHOSLABS Threat Intelligence

Request latest intelligence

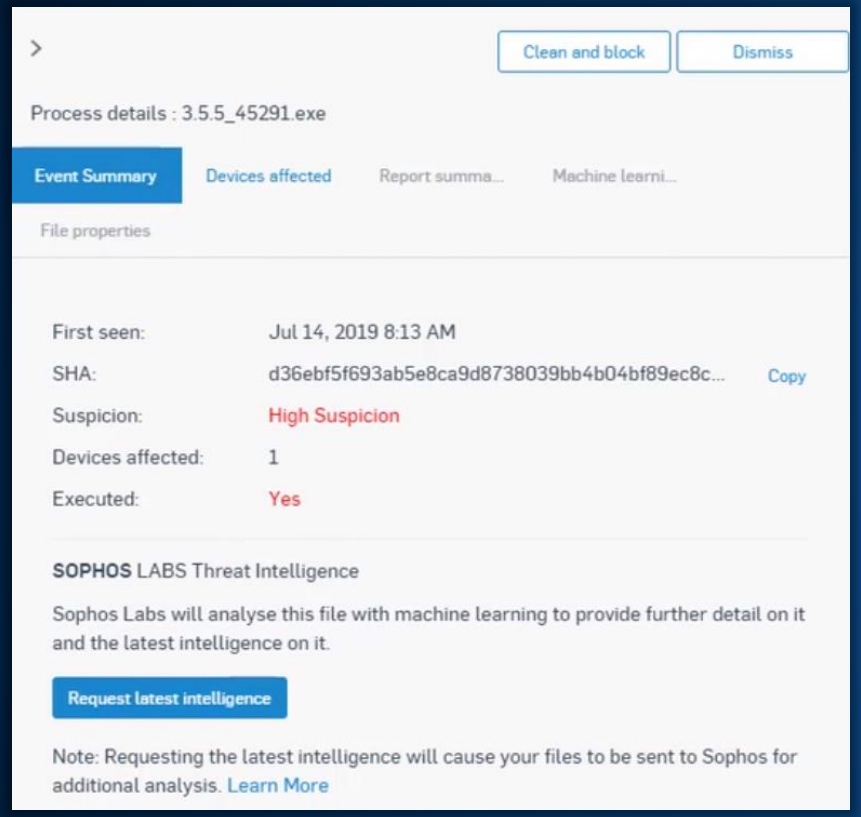
No current intelligence on this file.

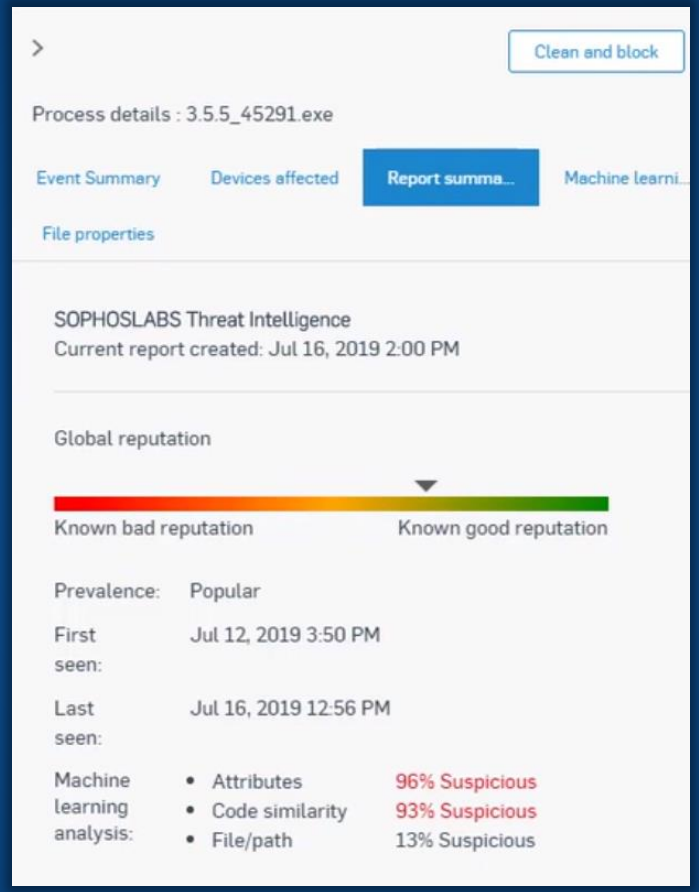
Note: Requesting the latest intelligence will cause your files to be sent to Sophos for additional analysis. Learn More

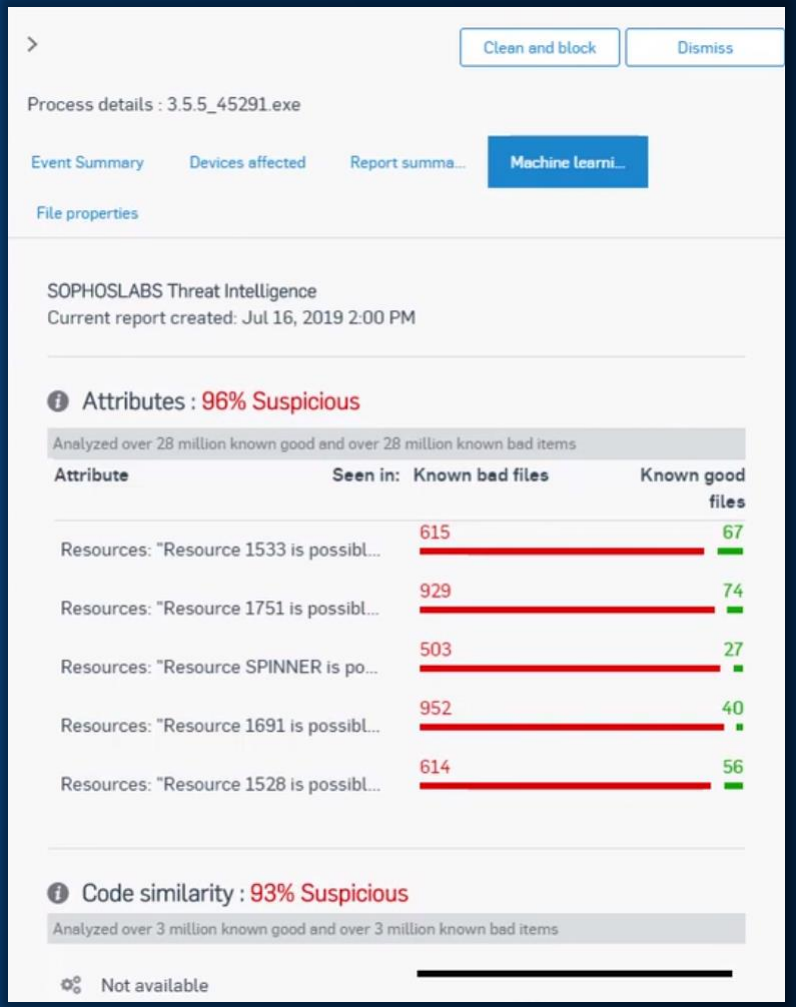
Path:	c:\windows\syswow64\netsh.exe
Name:	netsh.exe
Command line:	netsh.exe advfirewall firewall delete rule name="Remote Assistance (50383)"
Process ID:	4352
Process executed by:	NT AUTHORITY\SYSTEM

SOPHOS

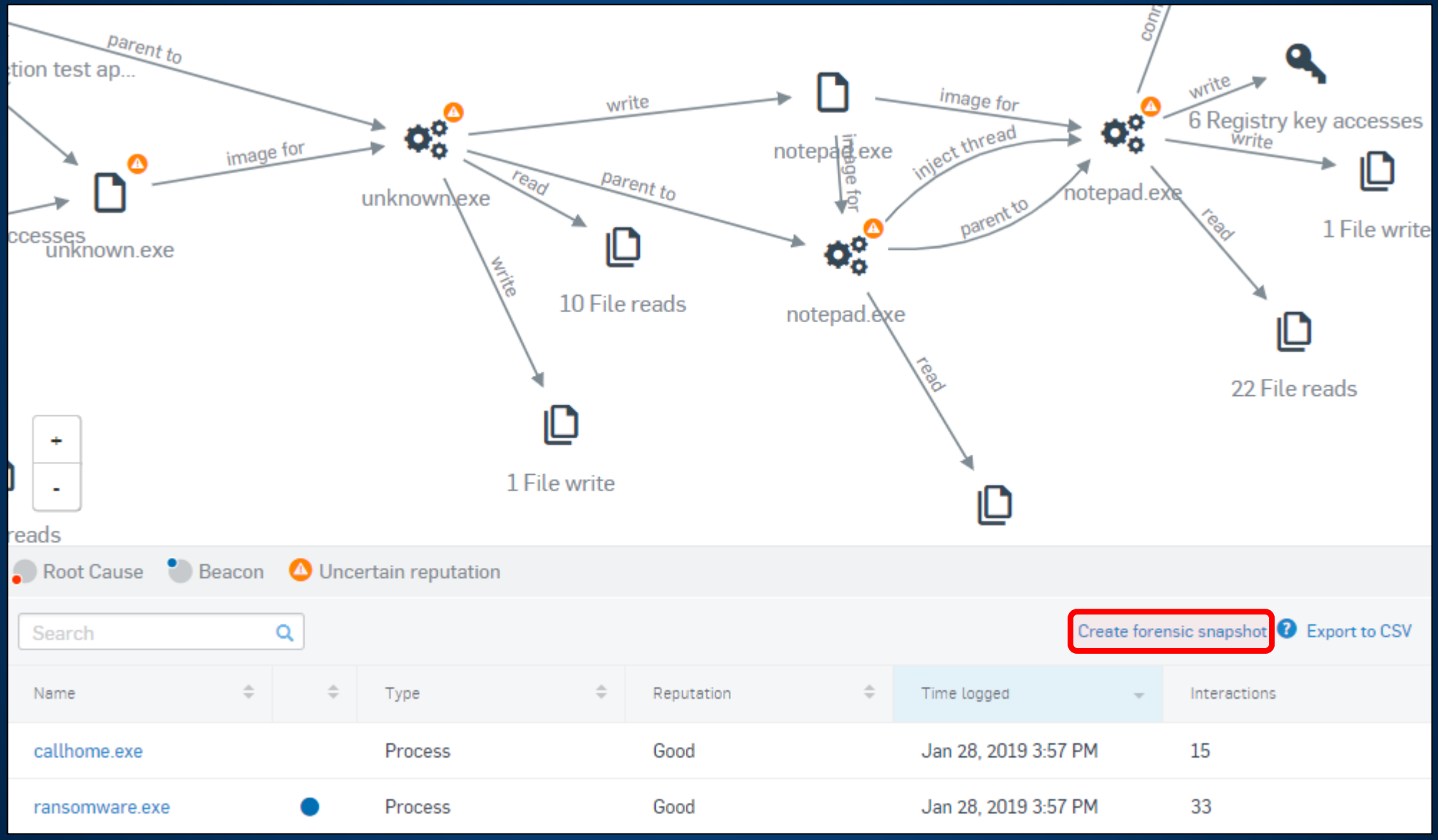
Machine Learning Threat Indicators







Forensic Snapshots



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_157d1dddb3784e82.tgz -o MyThreatcase.db
Using latest output version: 1
Conversion complete.

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

DB Browser for SQLite - C:\ProgramData\Sophos\Endpoint Defense\Data\Saved Data\201901cryptoguard.db

File Edit View Help

New Database | Open Database | Write Changes | Revert Changes

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: Process | New Record | Delete Record

	rt	path_id	cl	sha1	sha25
	Filter	Filter	Filter	Filter	c7f3282e6
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 --l...	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

1 - 9 of 9 | Go to: 1

Edit Database Cell

Mode: Text | Import | Export | Set as NULL

"C:\mydata\notepad.exe" --injection-target --initialized-event=528 --log-sync-mutex=508

Type of data currently in cell: Text / Numeric
87 char(s) | Apply

Remote

Identity

Name	Commit	Last modified	Size

SQL Log | Plot | DB Schema | Remote

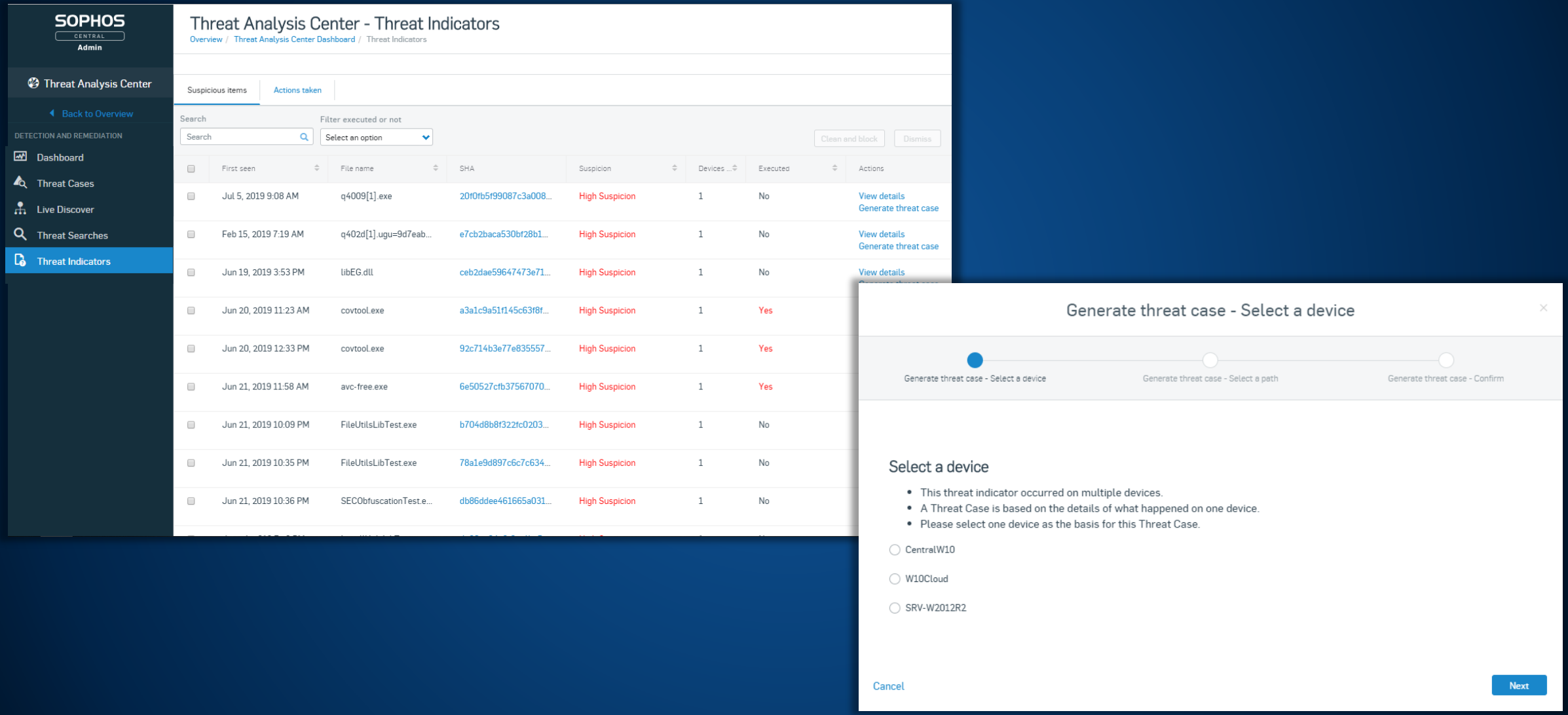
UTF-8

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

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

SOPHOS

Machine Learning Threat Indicators



Dlaczego serwery są głównymi celami?!

Cele o wysokiej wartości

Serwery zawierają cenne dane i utrzymują działalność firmy

Przestoje są kosztowne

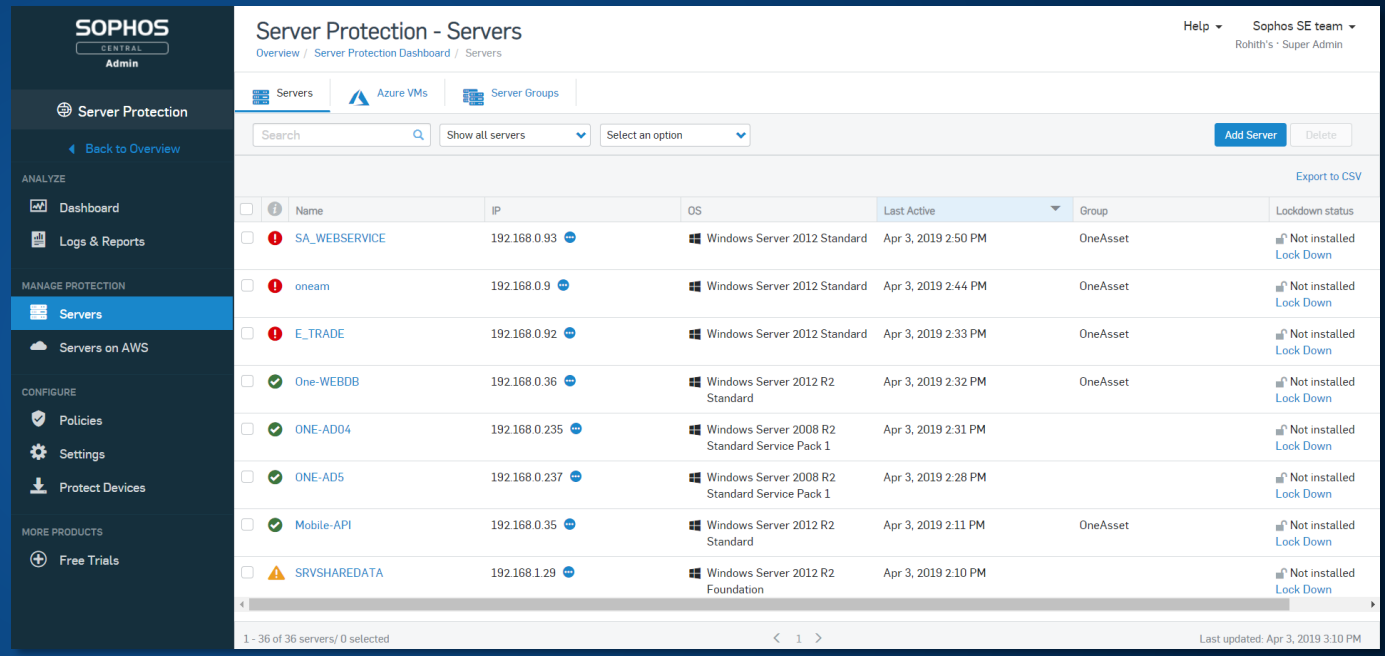
Przestoje na serwerze mogą zniszczyć efektywność pracy

Idealne miejsce postoju

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

Najważniejsze funkcje

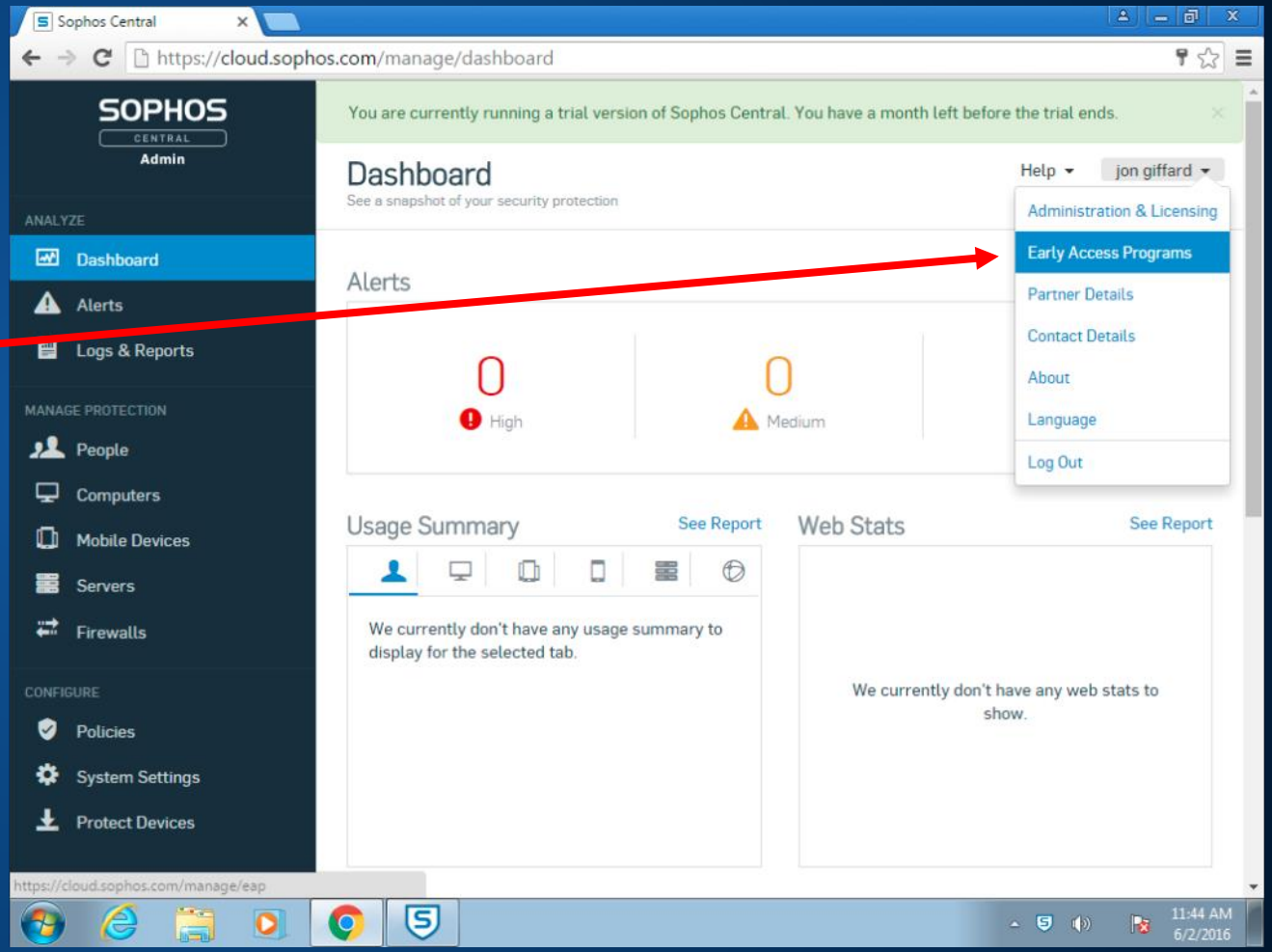
- Ochrona serwera typu „wszystko w jednym”
  - Zatrzymaj zaawansowane złośliwe oprogramowanie
- Automatyczne wykrywanie zagrożeń i reagowanie
  - Złap nieuchwytne zagrożenia
- Przejmij kontrolę nad swoimi serwerami
  - Wykorzystaj unikalną funkcjonalność Server Lockdown



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

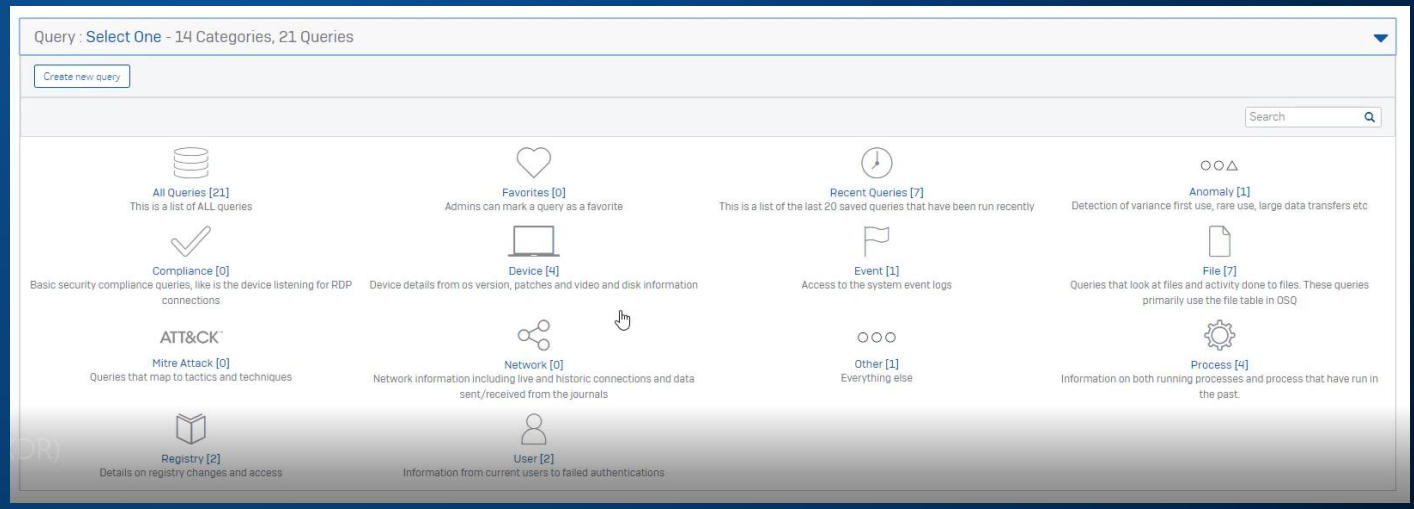


Odkryj więcej informacji

Live Discover

- Bogate możliwości wyszukiwania punktów końcowych
  - IT insight
  - Threat hunting
  - Look beyond malware
- Zapytania SQL dla wiekszej szczegółowości
  - Pre-konfigurowane zapytania
  - Mofyfikowalne zapytania
  - Dostęp do community
- Dane na żywo i histryczne (do 90 dni)

- EAP: Win Endpoint & Server kwiecień
- Windows i Linux GA w Czerwcu
- Wsparcie dla komputerów Mac wkrótce

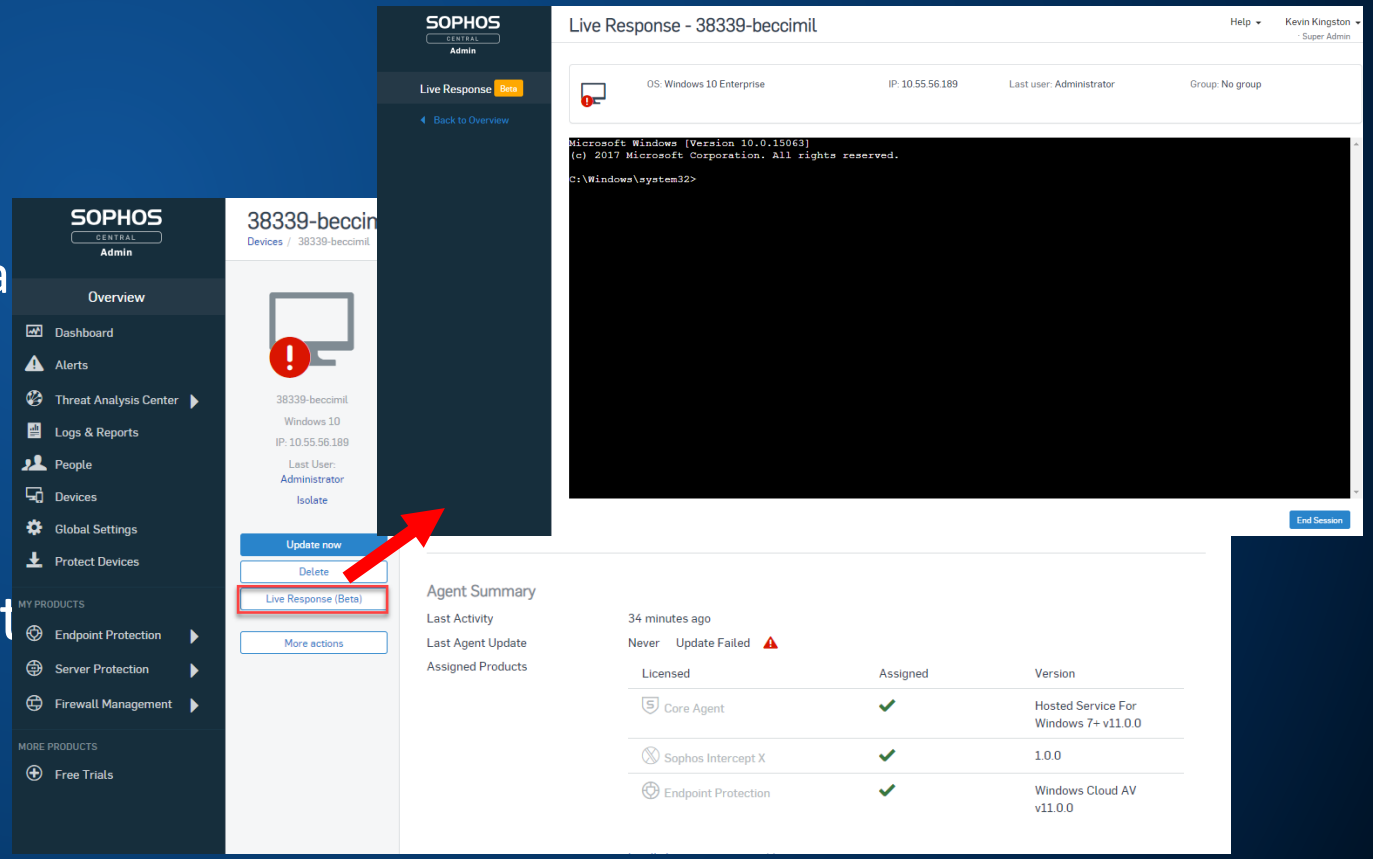


*Uwaga: daty i funkcje mogą ulec zmianie * Może pojawić się wkrótce po GA*

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 wkrót
- Audit logs and MFA



Uwaga: daty i funkcje mogą ulec zmianie

Automatyczne wykrywanie zagrożeń i reagowanie

Endpoint Detection and Response (EDR)

- Aktywnie ścigaj wyrafinowane zagrożenia
- Zrozumieć spektrum incydentów bezpieczeństwa

Wykryj i zabezpiecz chmurowe mijesca 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 nieznane aplikacje komunikujące się na zewnątrz

Live demo

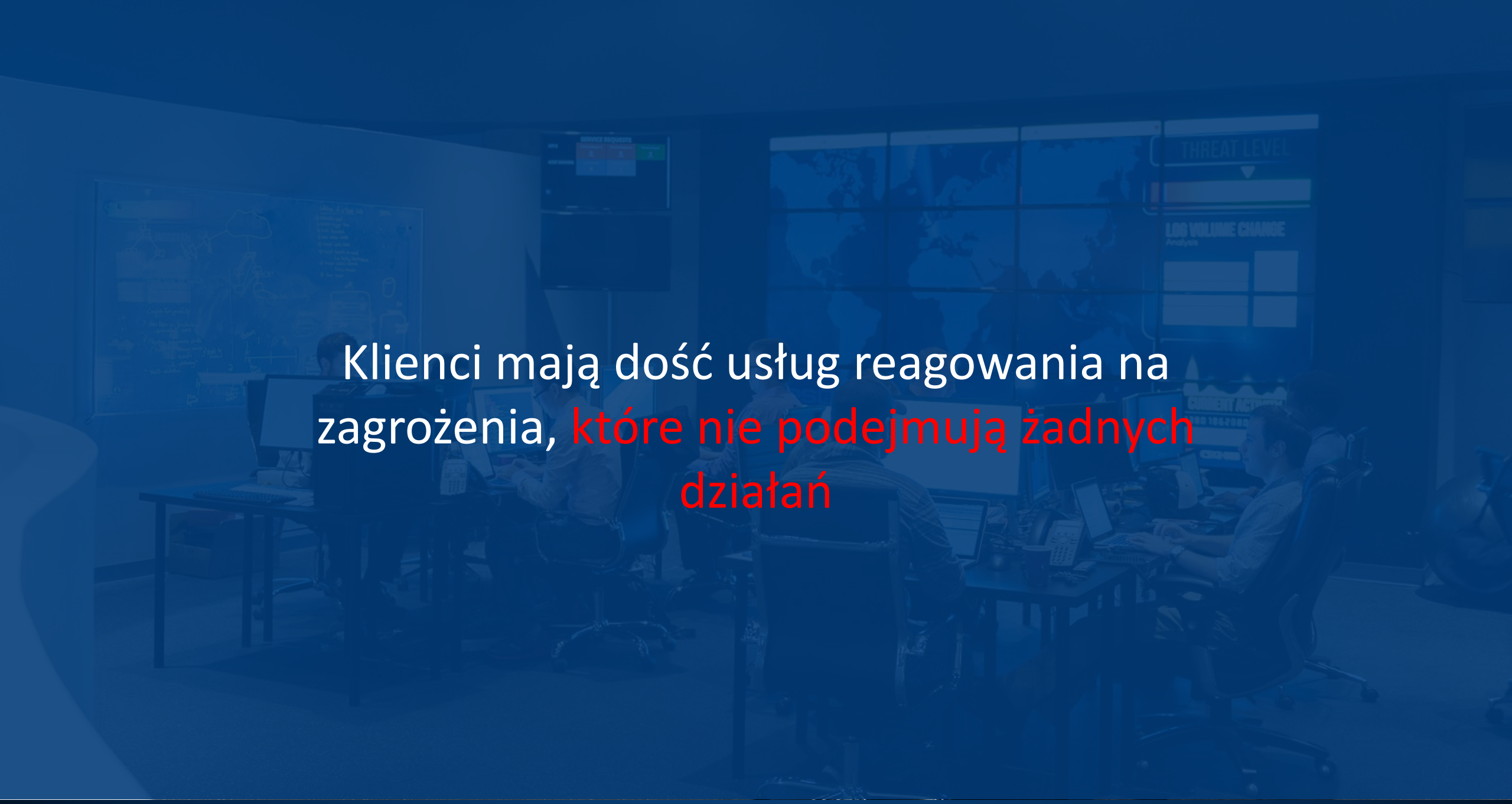
SOPHOS

Sophos Endpoint Protection (User Licensing)

	Central Endpoint Protection	Intercept X	Intercept X Advanced	Intercept X 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 X for Server	Sophos Intercept X for Server with EDR
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

Ochrona

Wykrycie

\+

EDR

odpowiedź

\+

EDR

\+

MTR

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

1. Intercept X with EDR Monitors for Threats
2. Machine Learning Prioritizes Suspicious Activities
3. Confirmed Malicious Activities are Automatically Terminated

HUMAN THREAT HUNTERS AND RESPONSE EXPERTS

4. Human Analysts Investigate Suspicious Events
5. Threat Hunts are Conducted to Find New Threats
6. Response Experts Take Action to Neutralize Threats

SOPHOS

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 podejrzane 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 podejrzane zachowanie

Odpowiedź

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

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

Analityk 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

Analityk prowadzący poszukiwania zagrożeń odkrywa nowy wskaźnik (IoC)

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

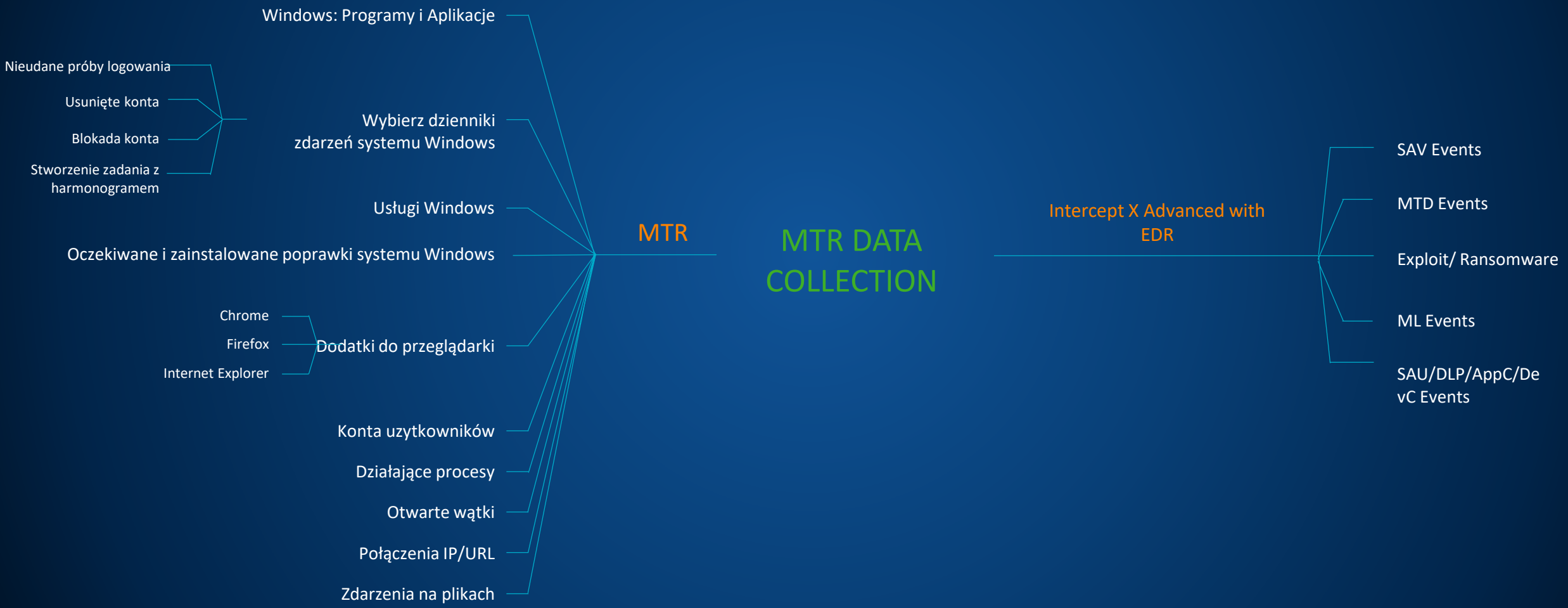
Analityk określa, jakie działania należy podjąć i które wykonuje w ramach tego planu

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

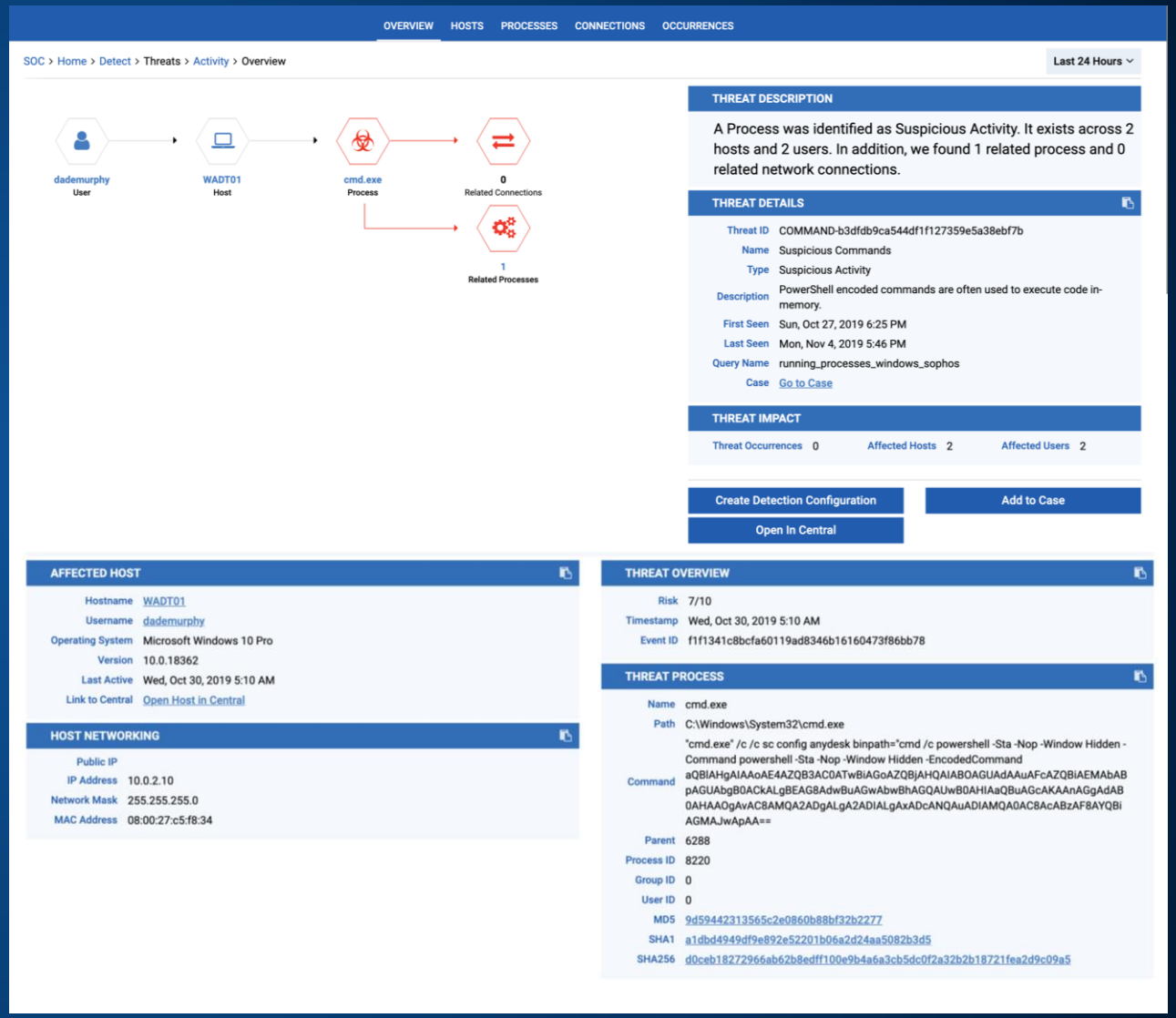
Zbieranie danych



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)

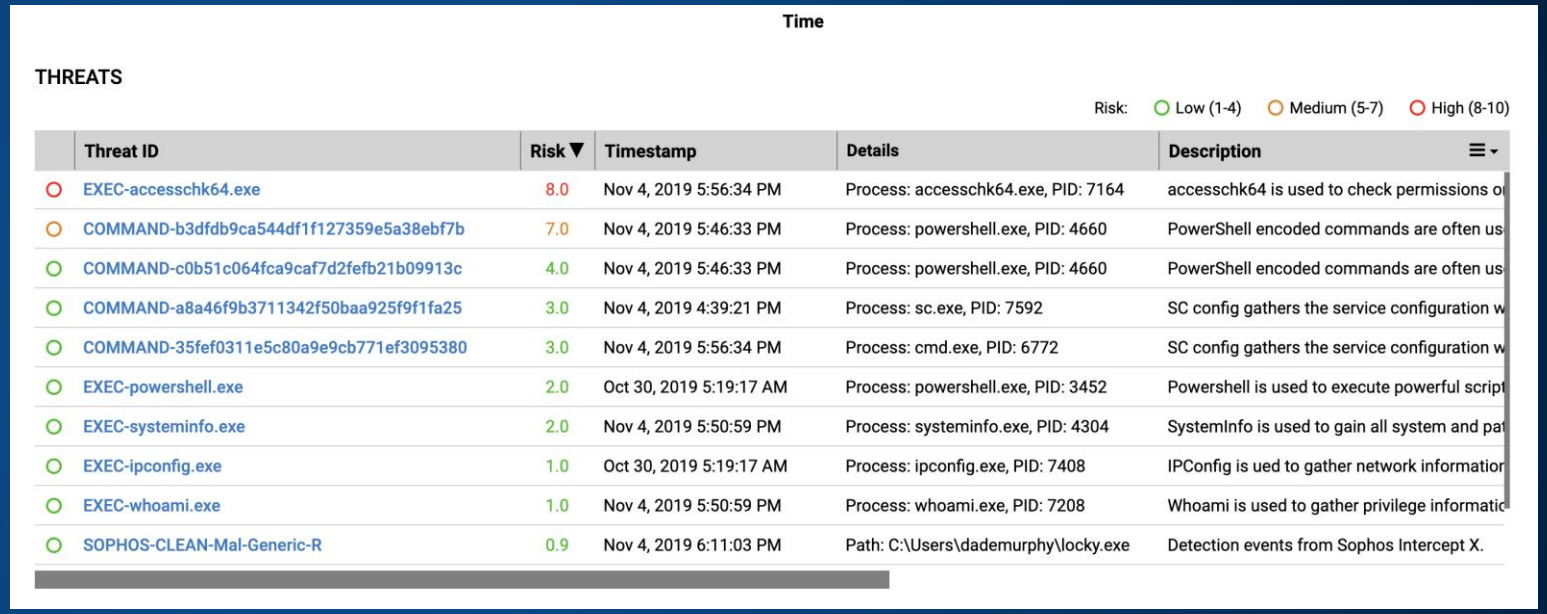


Jak tego używamy ??

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 o
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 ued to gather network information
EXEC-whoami.exe	1.0	Nov 4, 2019 5:50:59 PM	Process: whoami.exe, PID: 7208	Whoami is used to gather privilege informatic
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 wyszukiwnaie zagrożeń

Dedykowany specjalista ds. Reagowania na incydenty

Bezpośrednie wsparcie telefoniczne

Cykliczne omówienie przeprowadzanych działań

Proaktywna poprawa postawy

Analiza zasobów

Rozszerzona telemetria

Managed Threat Response Report

Dec 21, 2019 - Jan 21, 2020

SOPHOS

Overall Protection Rating

Yellow

See Health Check recommendations for steps to enhance your posture

1280

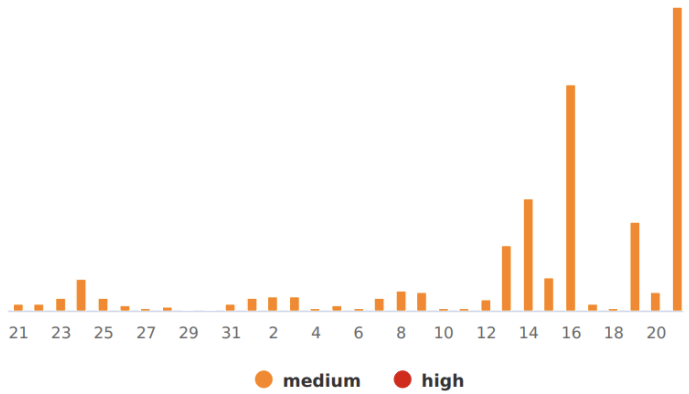
Protected With MTR

0 MTR Not Deployed

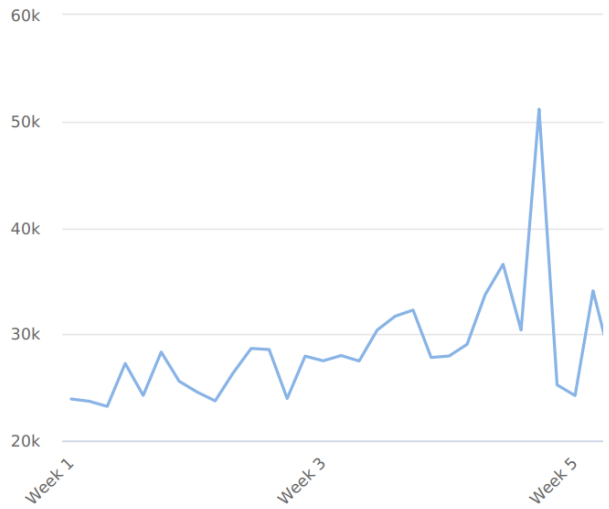
57809 After Hour Detections

(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	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
0 -	1 -	1 -	0 -	0 -	0 -

Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
0 -	1 -	0 -	0 -	1 -	0 -

Sophos MTR Connectors

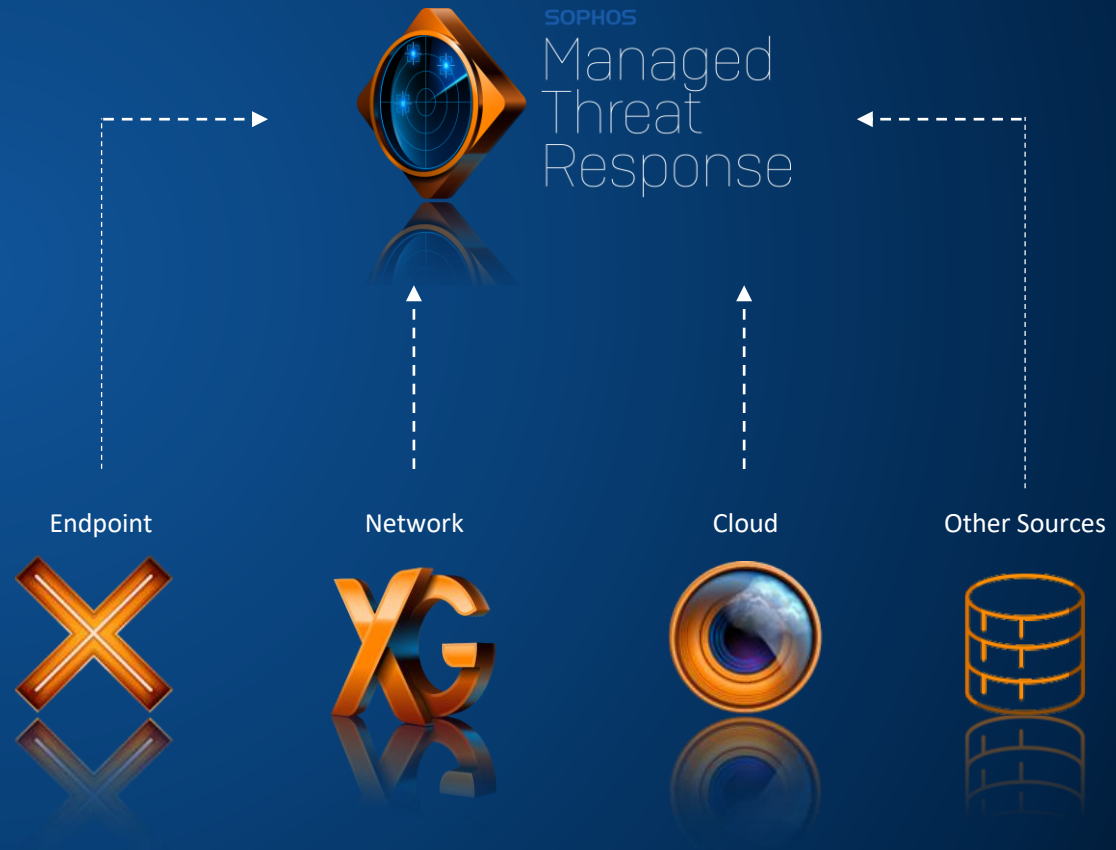
Dokładniejsze możliwości działania w celu zapobiegania zagrożeniom, wykrywania ich i reagowania na nie

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

Rowiązanie

- 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 kientów, którzy zarządzają swoimi XG Firewall poprzez Sophos Central i korzystaja 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

SOPHOS INTERCEPT X
Advanced with EDR

Pytania?

SOPHOS

Cybersecurity evolved.