

SOPHOS
INTERCEPT

Advanced with EDR

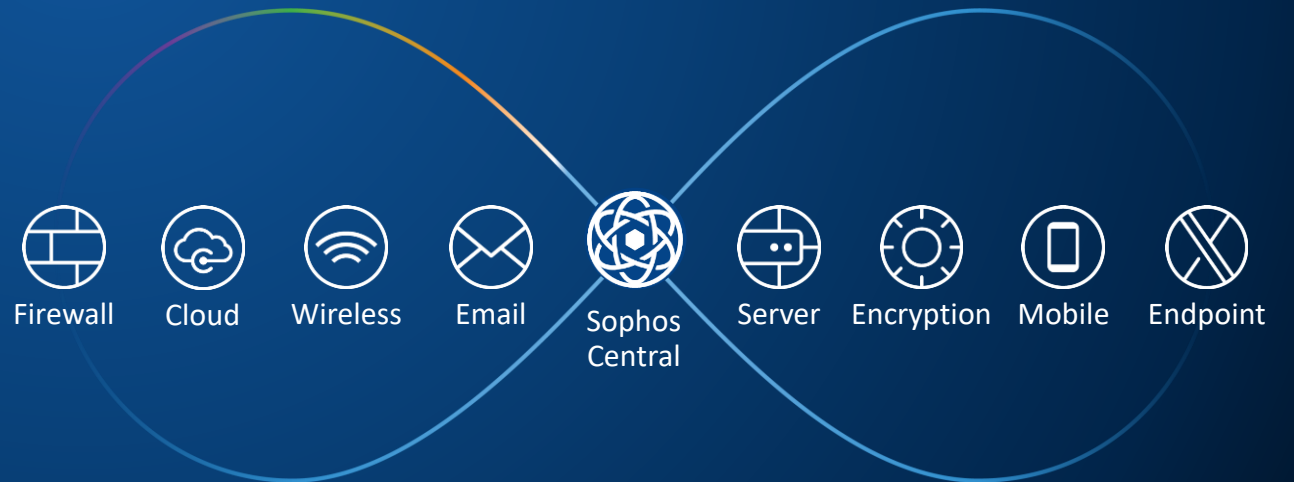
Sesja techniczna

Damian Przygodzki
System Engineer

SOPHOS

Sophos

- Założona w Oxford w 1985
- 3,500 pracowników
- 350,000 klientów
- 100 milionów użytkowników w 150 krajach
- 47,000 partnerów



Ataki w dobie epidemii nie ustają...

Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack

The Maze ransomware group has published personal and medical details of thousands of former patients of a London-based medical research company after a failed attempt to disable the firm's computer systems



By **Bill Goodwin**, Computer Weekly

Published: 22 Mar 2020 15:40

Czech Republic's Second-Biggest Hospital is Hit by Cyberattack



BY PRAGUE MORNING
MARCH 13, 2020

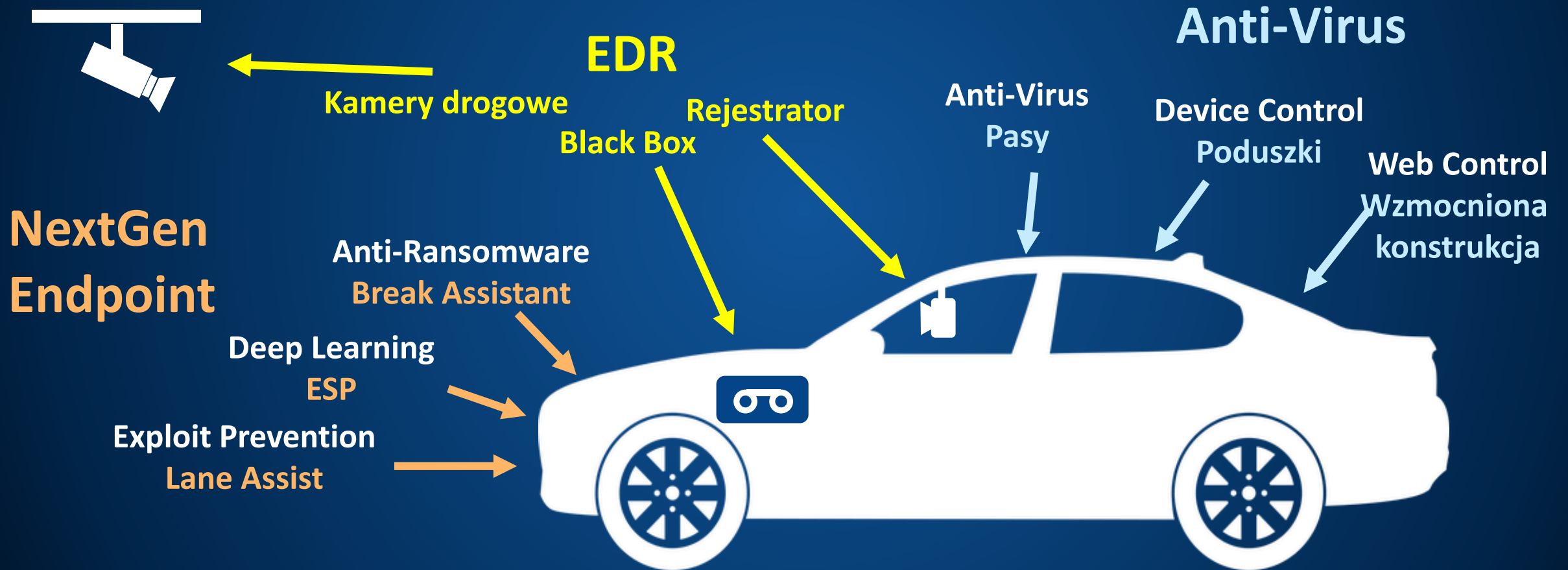


<https://www.praguemorning.cz/czech-republics-second-biggest-hospital-is-hit-by-cyberattack/>

<https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-organisation-poised-for-work-on-Coronavirus>

SOPHOS

Od Anti-Virus do EDR



Dlaczego używamy narzędzi EDR?



Co to jest EDR (Endpoint Detection and Response)?

- EDR to holistyczne podejście do bezpieczeństwa punktów końcowych
- **Detekcja** incydentów
- **Reakcja** na incydenty bezpieczeństwa
- **Poszukiwanie** zagrożeń
- **Badanie kryminalistyczne** po zaistniałym incydencie



integruje wszystkie komponenty EDR

Technologia NextGen w



Exploit Prevention	Enforce data execution prevention
	Mandatory address space layout randomization
	Bottom-up ASLR
	Null page(Null Deference protection)
	Heap spray allocation
	Dynamic heap spray
	Stack pivot
	Stack pivot (memory protection)
	Stack-based ROP mitigations(caller)
	exceptStructuredtion handler overwrite(SEHOP)
	Import address table filtering (IAF)
	Load library
	Reflective DLL injection
	Shellcode
	VBScrip god mode
	WOW64
	Syscall
	Hollow process
	DLL jacking
	Squibldydo applocker bypass
APC protection (Double pulsar/AtomBombing)	
Process privilege escalation	

Anti-Hacker	Credential theft protection
	Code cave prevention
	Man-in-the-browser protection (Safe browsing)
	Malicious traffic detection
	Meterpreter shell detection
Anti-Ransomware	Ransomware file protection (CryptoGuard)
	Automatic file recovery (CryptGuard)
	Disk and boot record protection (WipeGuard)
Application Lockdown	Web browsers (including HTA)
	Web browser plugins
	Java applications
	Media applications
	Office applications
Deep Learning	Deep learning malware detection
	Deep learning PUA detection
	False positive suppression
	Live protection
Analysis & Reaction	Root Cause Analysis
	Sophos Clean
	Synchronized Security
	Cross-estate search and containment

Najlepsza ochrona



Wymagania

- RODO, POPI, PCI, SOX, Basel III, HIPAA, ...
- Ochrona danych wymagana zgodnie z najnowszym stanem wiedzy (program antywirusowy NIE jest najnowocześniejszy)
- Obowiązek udowodnienia, czy dane zostały wyciekły podczas incydentu
- Zarządzanie ryzykiem

Koszt incydentu <-> koszt ochrony

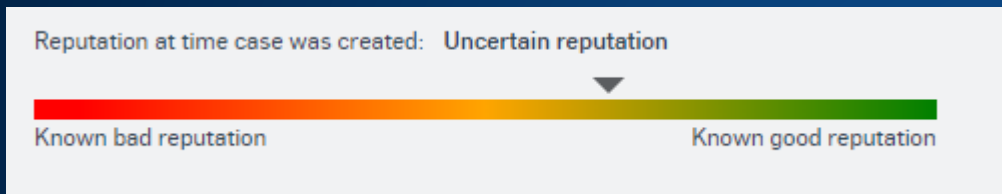


Widoczność

- Czy jesteśmy chronieni przed zagrożeniem XY z wiadomości?
- Czy jesteśmy atakowani?
- Mieliśmy incydent, ale
 - czy rozprzestrzeniło się zagrożenie?
 - czy atak jest nadal w toku?
 - czy straciliśmy dane?



Widoczność



SOPHOSLABS Threat Intelligence
Current report created: Jul 26, 2019 10:44 AM

[Request latest intelligence](#)

New threat search [Threat search examples](#)

Search for potential threats on your devices. You can search for file names, SHA-256 file hashes, IP addresses, domains or command lines.

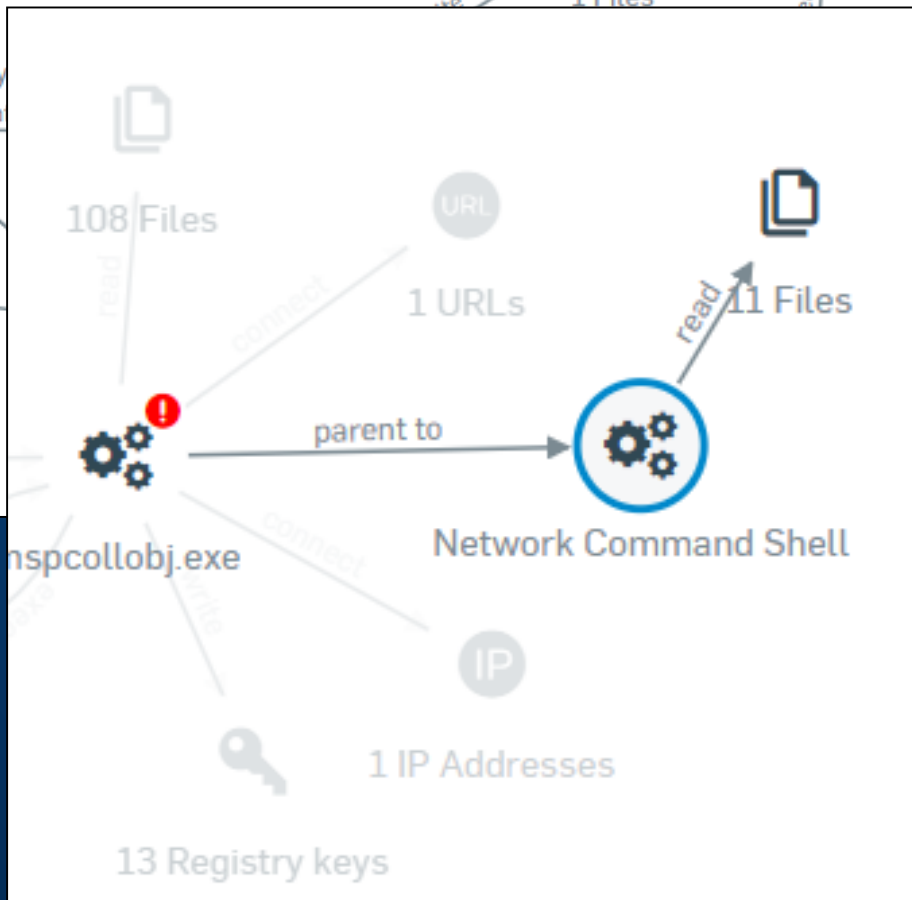
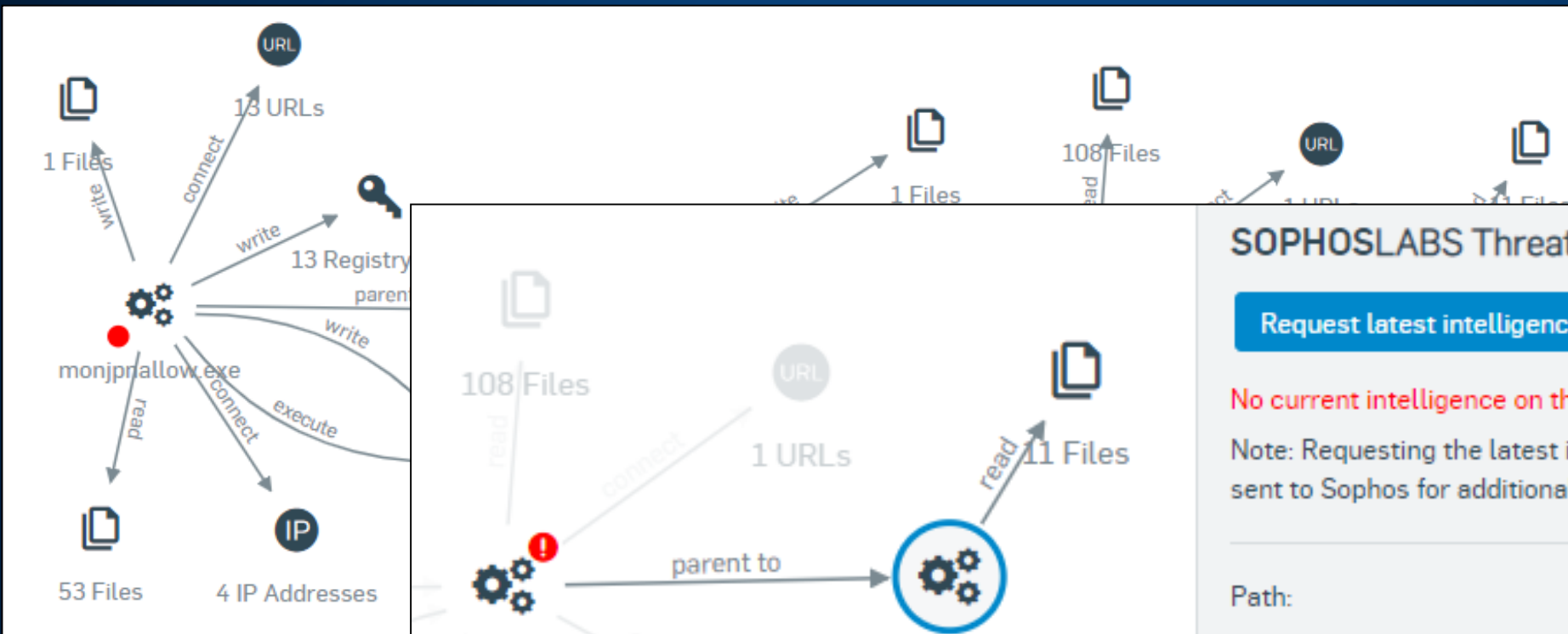
Searches find PE files (like applications) with uncertain or bad reputation and network destinations they've connected to.

Searches also find activity by admin tools, which can be used maliciously.

Enter one or more file names, SHA-256 file hashes, IP addresses, domains or command lines.

[Search for item](#) [Clean and block](#)

Przykład klienta EMOTET



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

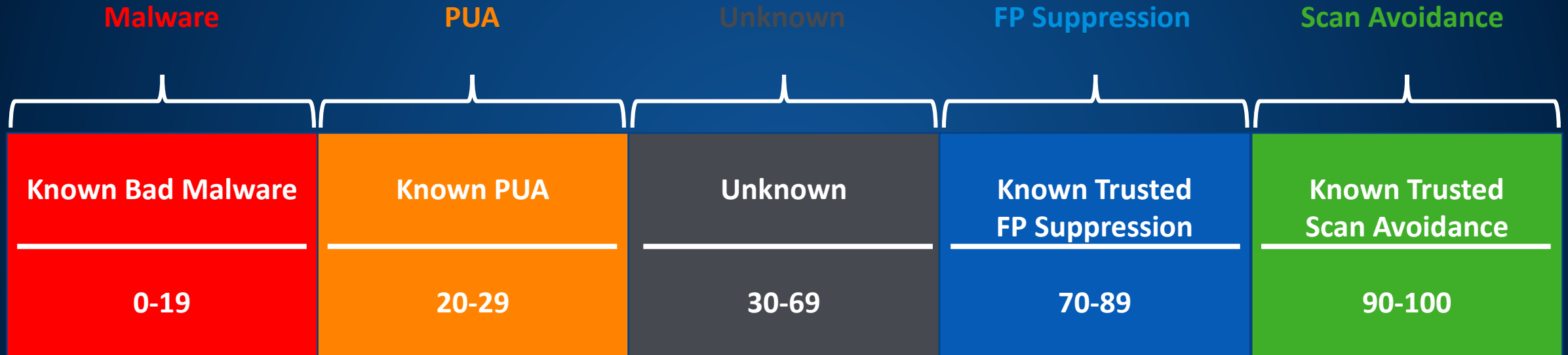
Command line:

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

Process ID: 6352

Process executed by: NT AUTHORITY\SYSTEM

PE Reputacja



Snapshot vs. Threat Case vs. Trickle Feed

Snapshot

- Kilka tygodni
- Operacje na plikach
- Operacje rejestru
- Połączenia sieciowe
- Rozpoczęcie procesu / rozgałęzienie



Threat Case

- Tylko dane między „Root Cause” a „Beacon”
- Operacje na plikach
- Operacje rejestru
- Połączenia sieciowe
- Rozpoczęcie procesu / rozgałęzienie



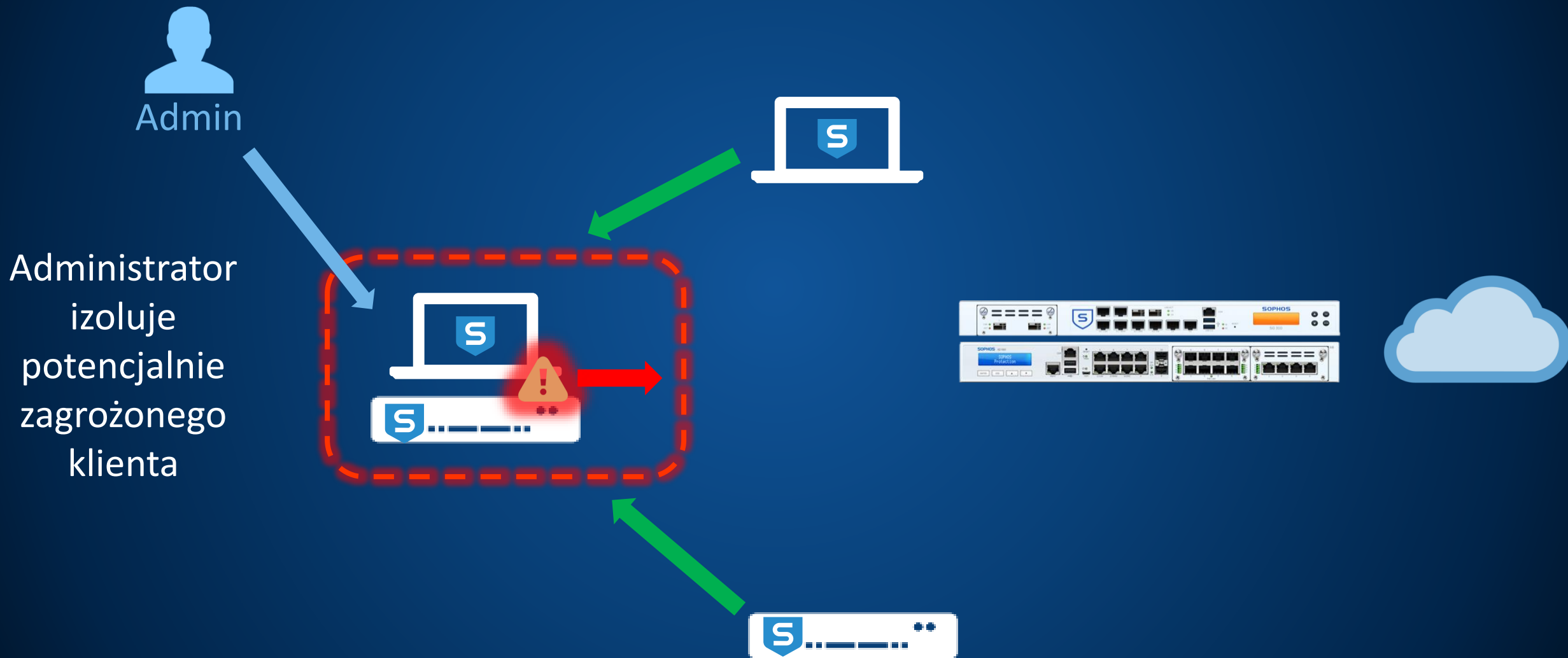
Trickle Feed

- Kilka miesięcy
- <70 Reputacja PEs:
 - Wykonanie, operacje zapisu itp.
 - Zmiany ścieżki i reputacji
 - Porozumiewanie się



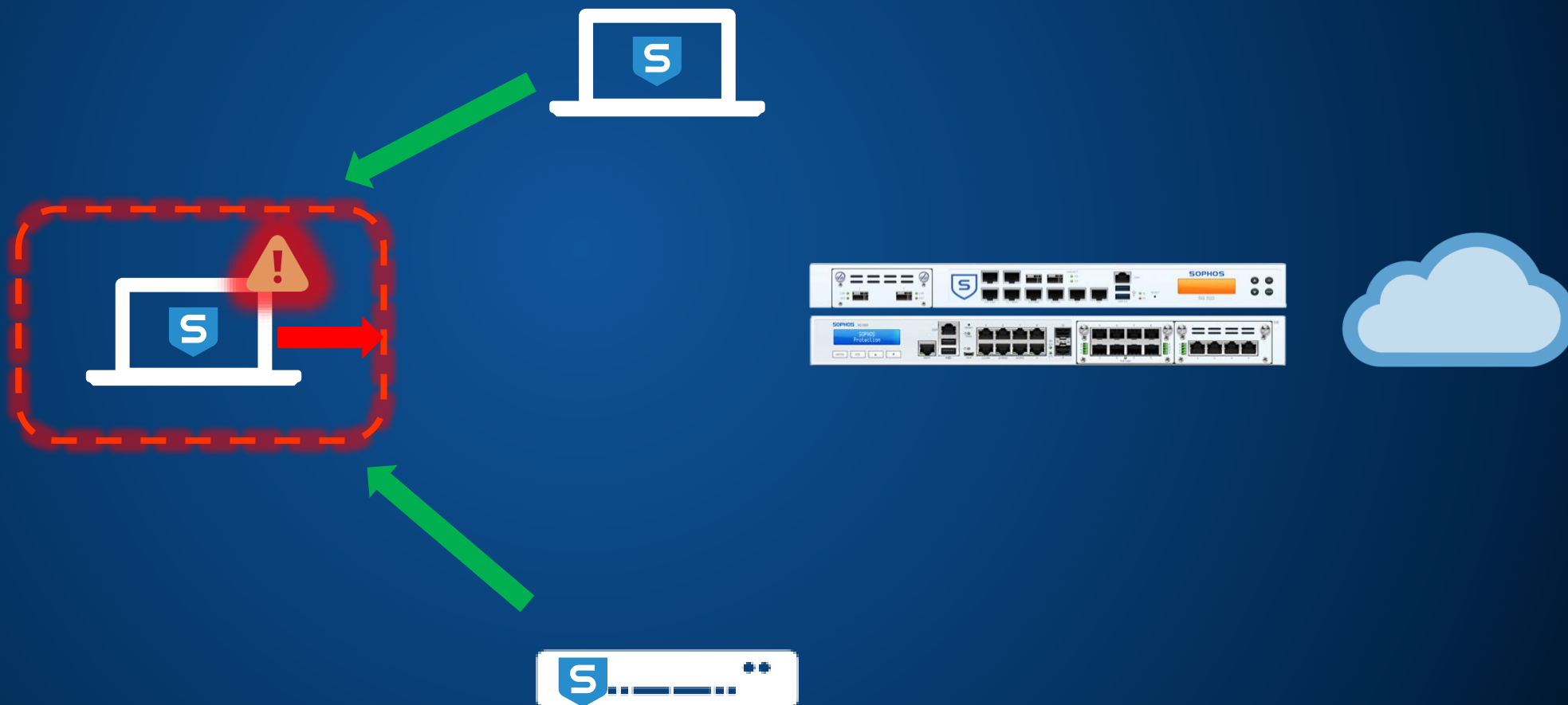
Reakcja / Zatrzymanie

Admin Isolation



Self Isolation

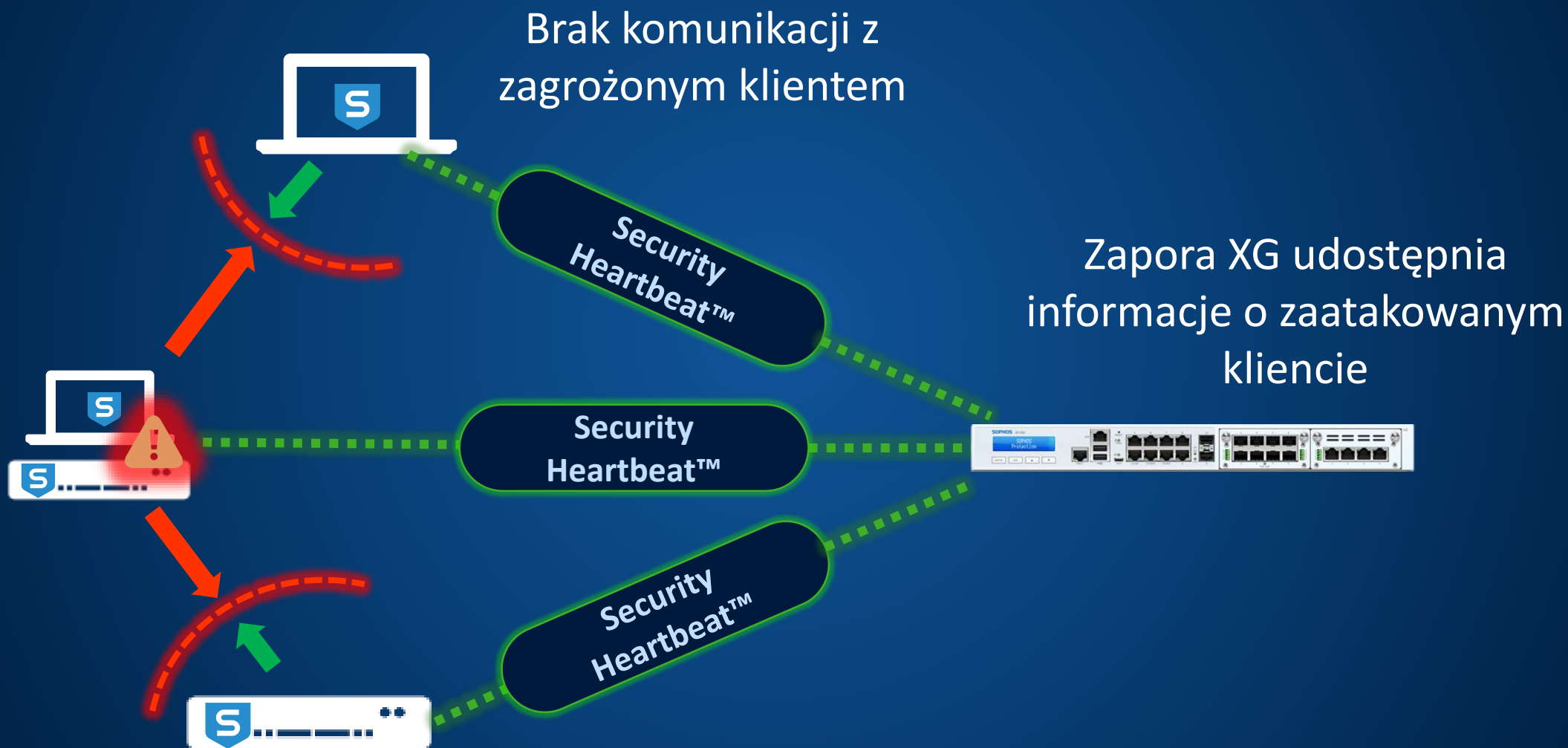
Zainfekowany komputer izoluje się sam



Automatyczna kwarantanna sieciowa z XG Firewall



Lateral Movement Protection



Live Demo



Advanced z EDR

Forensic Snapshots

The diagram illustrates a forensic snapshot of system activity. It shows a hierarchy of processes and their interactions:

- unknown.exe** (Uncertain reputation) is the parent of another **unknown.exe** and a **notepad.exe**. It performs 1 File write and 10 File reads.
- The **notepad.exe** child of **unknown.exe** is the parent of another **notepad.exe**. It performs 1 File write and 22 File reads.
- The **notepad.exe** child of the second **notepad.exe** performs 6 Registry key accesses and 1 File write.
- Other interactions include 'inject thread', 'image for', and 'parent to' relationships between processes.

Below the diagram is a control panel with a search bar, a legend for Root Cause, Beacon, and Uncertain reputation, and buttons for 'Create forensic snapshot' (highlighted in red) and 'Export to CSV'.

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

Konwersja snapshot przy pomocy 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 Pragas Execute SQL

Table: Process

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...

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>

Wskaźniki zagrożenia uczenia maszynowego

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, Threat Searches, and Threat Indicators (Beta). The main content area is titled 'Threat Analysis Center - Threat Indicators' and includes a search bar, a filter dropdown for 'Filter executed or not', and a table of suspicious items. The table has columns for 'First seen', 'File name', 'SHA', 'Suspicion', 'Devices', 'Executed', and 'Actions'. The 'Suspicion' column for all items is 'High Suspicion'. The 'Executed' column shows 'No' for most items and 'Yes' for some. The 'Actions' column includes links for 'View details' and 'Generate threat case'.

First seen	File name	SHA	Suspicion	Devices	Executed	Actions
Jul 5, 2019 9:08 AM	q4009[1].exe	20f0fb5f99087c3a008...	High Suspicion	1	No	View details Generate threat case
Feb 15, 2019 7:19 AM	q402d[1].ugu=9d7eab...	e7cb2baca530bf28b1...	High Suspicion	1	No	View details Generate threat case
Jun 19, 2019 3:53 PM	libEG.dll	ceb2dae59647473e71...	High Suspicion	1	No	View details
Jun 20, 2019 11:23 AM	covtool.exe	a3a1c9a51f145c63f8f...	High Suspicion	1	Yes	
Jun 20, 2019 12:33 PM	covtool.exe	92c714b3e77e835557...	High Suspicion	1	Yes	
Jun 21, 2019 11:58 AM	avc-free.exe	6e50527cfb37567070...	High Suspicion	1	Yes	
Jun 21, 2019 10:09 PM	FileUtilsLibTest.exe	b704d8b8f322fc0203...	High Suspicion	1	No	
Jun 21, 2019 10:35 PM	FileUtilsLibTest.exe	78a1e9d897c6c7c634...	High Suspicion	1	No	
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 bar 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.' Below the text are three radio button options: 'CentralW10', 'W10Cloud', and 'SRV-W2012R2'. At the bottom left is a 'Cancel' button and at the bottom right is a 'Next' button.

Wskaźniki zagrożenia uczenia maszynowego

> Clean and block Dismiss

Process details : 3.5.5_45291.exe

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](#)

> Clean and block

Process details : 3.5.5_45291.exe


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

> Clean and block Dismiss

Process details : 3.5.5_45291.exe

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





Najlepsza ochrona na rynku

- Deep Learning
- Anti-Ransomware
- Anti-Exploit
- Web/Device/AppControl
- Root Cause Analysis
- Synchronized Security



Dodatkowo

- Odpowiedzi na pytania
 - Czy jestem chroniony przed zagrożeniem X?
 - Czy atak jest w toku?
 - Czy dane zostały skradzione? -> RODO / Zgodność!
- Wyszukiwanie w całym przedsiębiorstwie + ograniczanie zagrożeń

Sophos Endpoint Protection (User Licensing)

	CENTRAL ENDPOINT PROTECTION	 Advanced	 Advanced with EDR
AV Signatures / HIPS / Live 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			✓

Pytania?



Co dalej ?!

Date	Topics	Link
06-05-2020	Inteligentny EDR & MTR - wszystko, co powinieneś wiedzieć	https://attendee.gotowebinar.com/register/5441771524148448268

Co dalej ?!

Inteligentny EDR & MTR - wszystko, co powinieneś wiedzieć

Niektóre zaawansowane cyberzagrożenia infekują system, nie wykazując natychmiastowych oznak naruszenia bezpieczeństwa. W tym webinarium w j .polskim podpowiemy, jak zwiększyć odporność cyberbezpieczeństwa na ataki dzięki Endpoint Detection and Response - funkcji wykrywania i reagowania na incydenty bezpieczeństwa opartej na sztucznej inteligencji oraz Managed Threat Response - zespołowi ekspertów wyszukujących cyberzagrożenia i reagujących na nie w trybie całodobowym.

SOPHOS
Cybersecurity evolved.