SOPHOS INTERCEPT X

Advanced with EDR

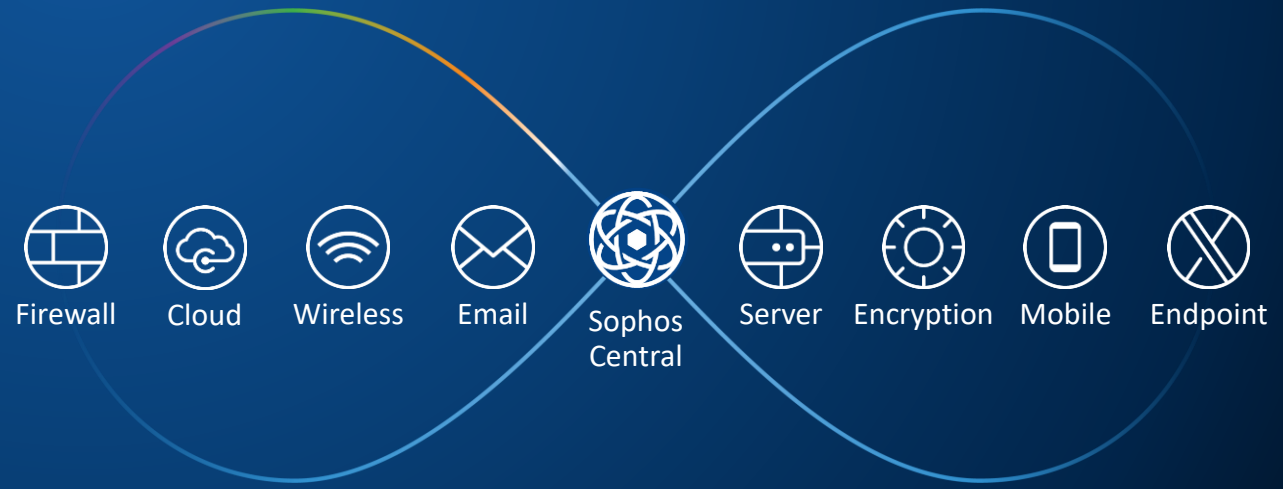
Sesja techniczna

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**

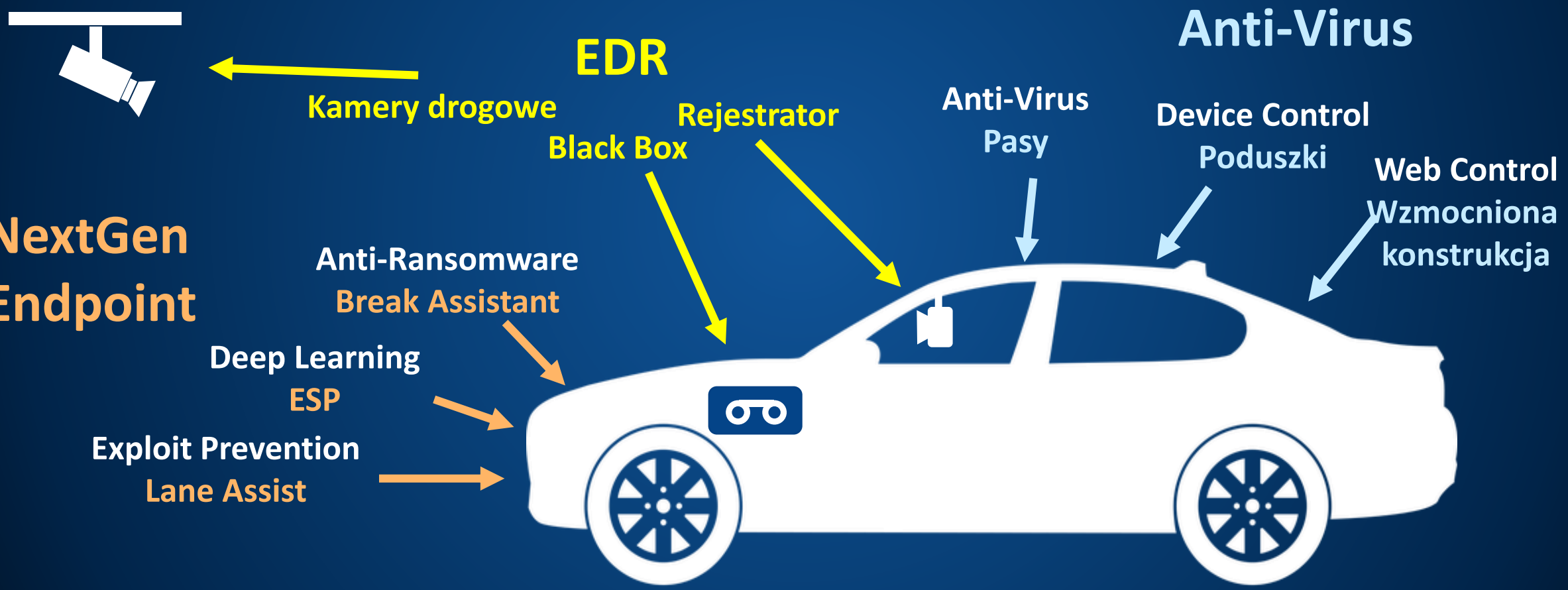
Czech Republic's Second-Biggest Hospital is Hit by Cyberattack

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-lorganisation-poised-for-work-on-Coronavirus

Od Anti-Virus do EDR



SOPHOS

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)
	excepStructuredtion handler overwrite(SEHOP)
	Import address table filtering (IAF)
	Load library
	Reflective DLL injection
	Shellcode
	VBScript god mode
	WOW64
	Syscall
	Hollow process
	DLL jacking
	Squibdlydoo 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

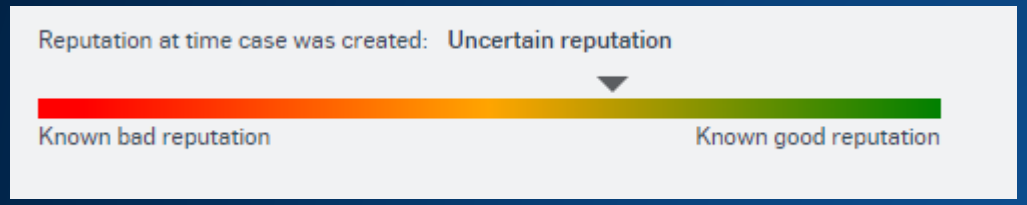
- RODO, POPI, PCI, SOX, Basel III, HIPAA, ...
- Ochrona danych wymagana zgodnie z najnowszym stanem wiedzy (program antywirusowy NIE jest najnowocześniejszy)
- Obowiązek udowodnienia, czy dane zostały wyciekły podczas incydentu
- Zarządzanie ryzykiem

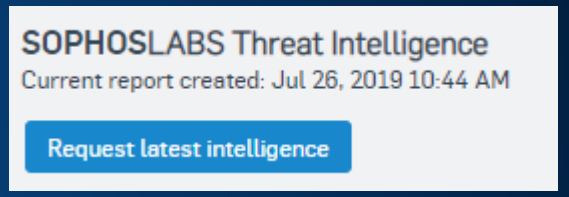
Koszt incydentu <-> koszt ochrony

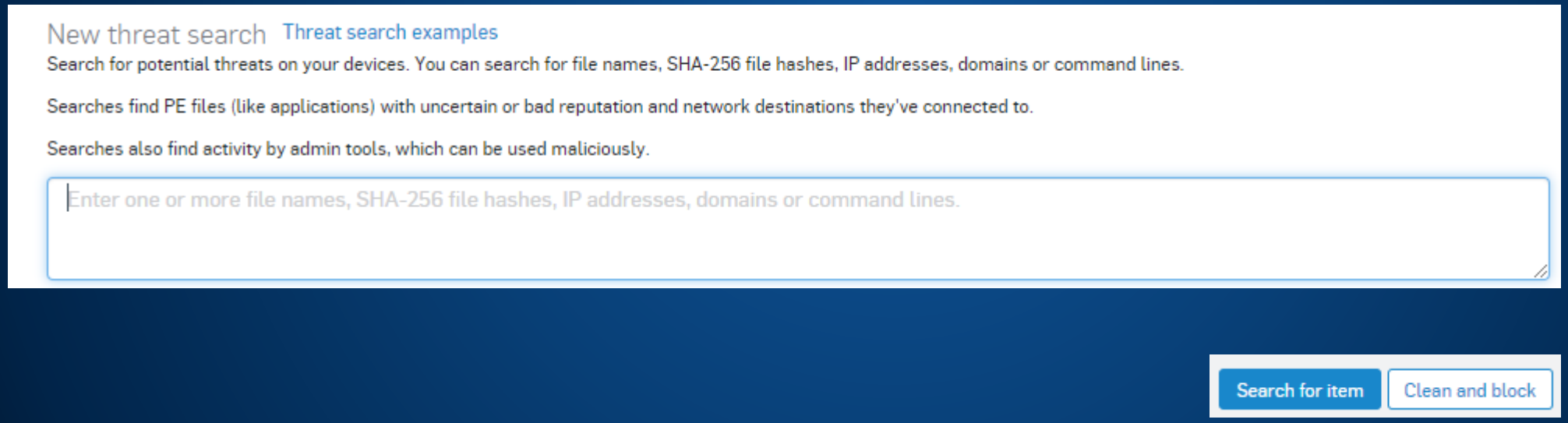
Widoczność

- 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?

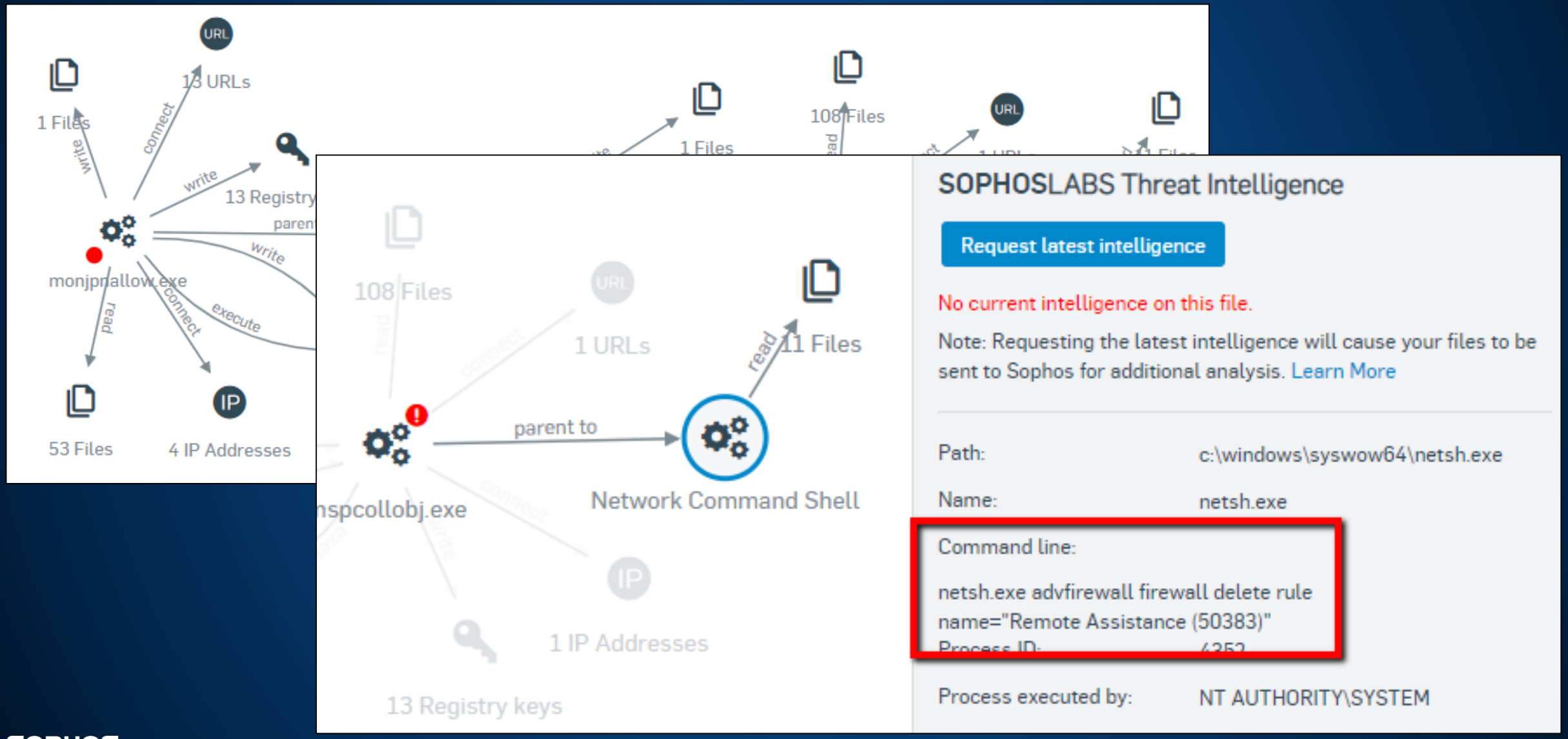
Widoczność


Reputation at time case was created: Uncertain reputation
Known bad reputation
Known good reputation

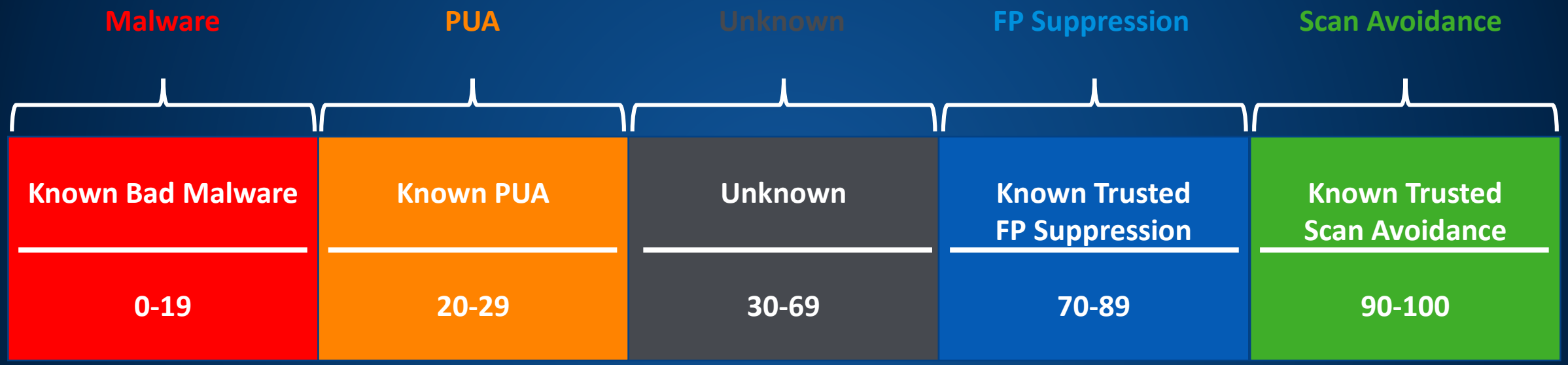

SOPHOSLABS Threat Intelligence
Current report created: Jul 26, 2019 10:44 AM
Request latest intelligence


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



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

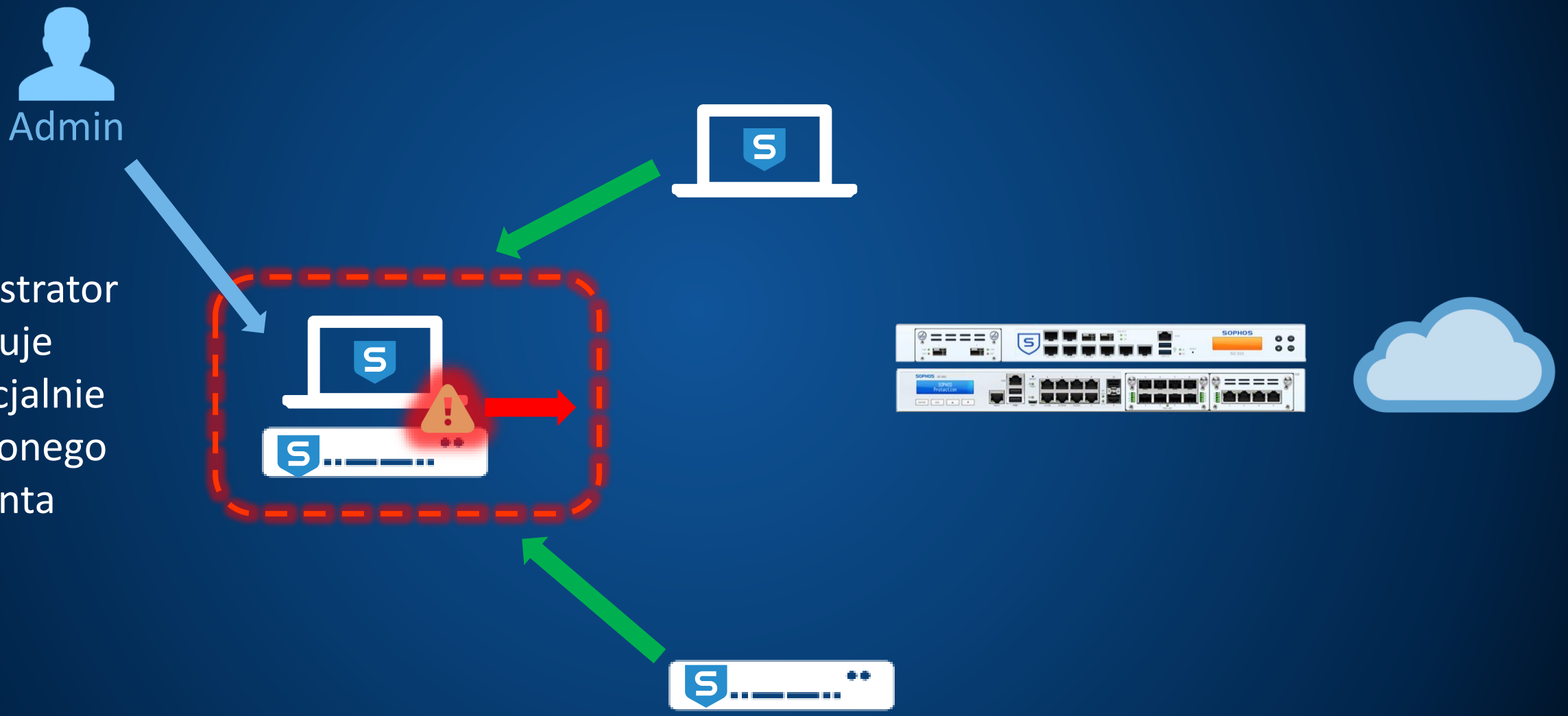
Trickle Feed

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

Reakcja / Zatrzymanie

SOPHOS

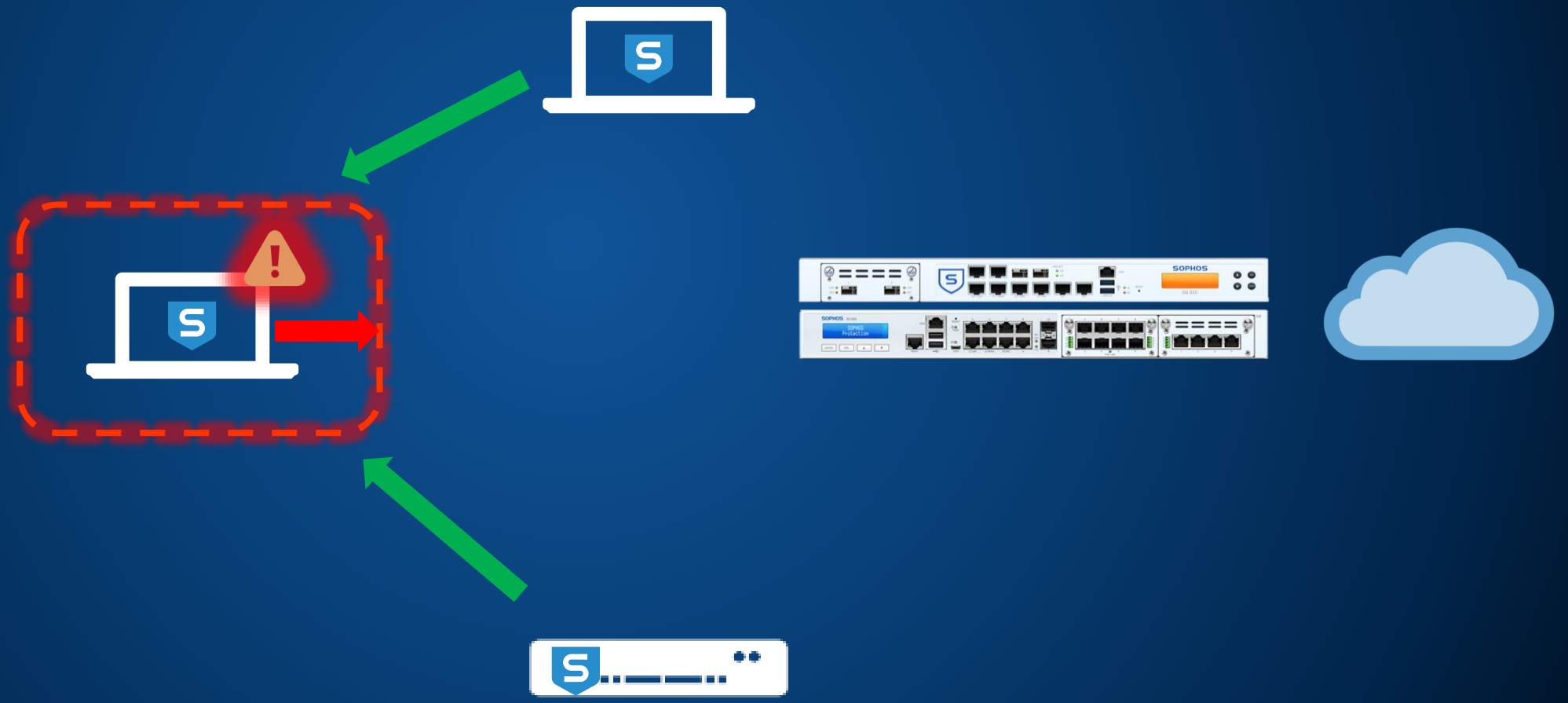
Admin Isolation



Administrator izoluje potencjalnie zagrożonego klienta

Self Isolation

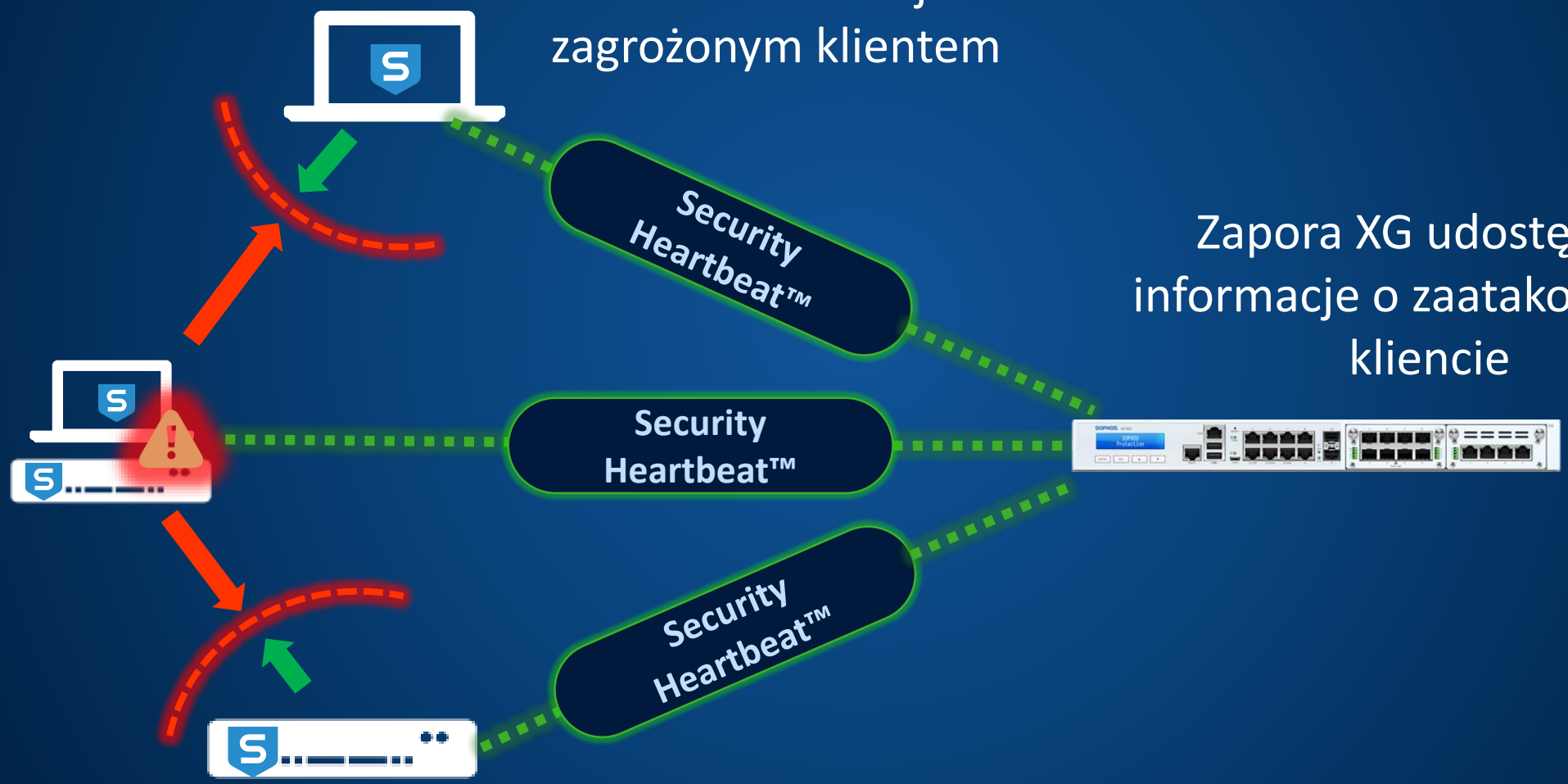
Zainfekowany komputer izoluje się sam



Automatyczna kwarantanna sieciowa z XG Firewall

Zapora XG poddaje kwarantannie zainfekowanego klienta

Lateral Movement Protection

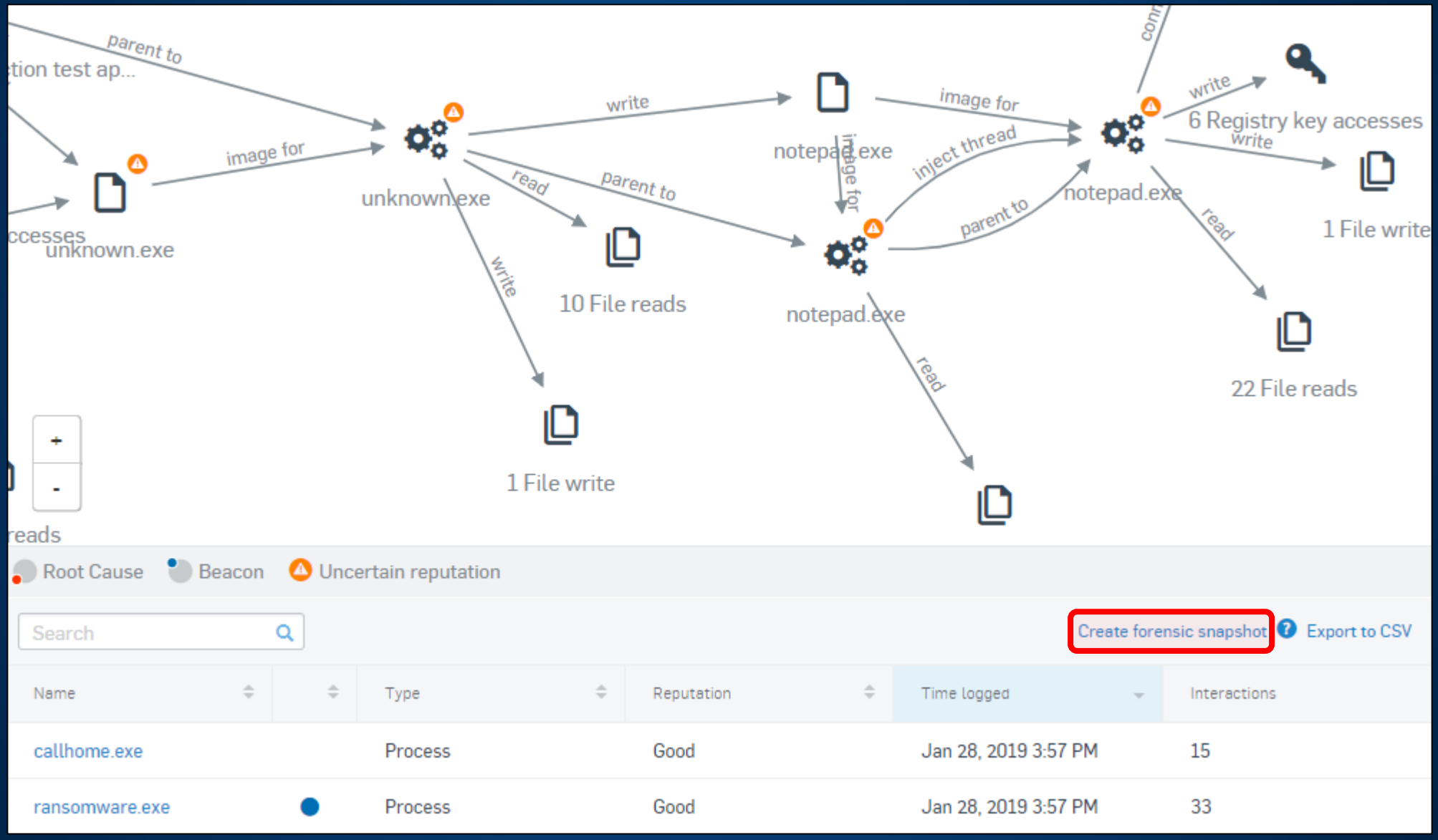


Live Demo

Advanced z EDR

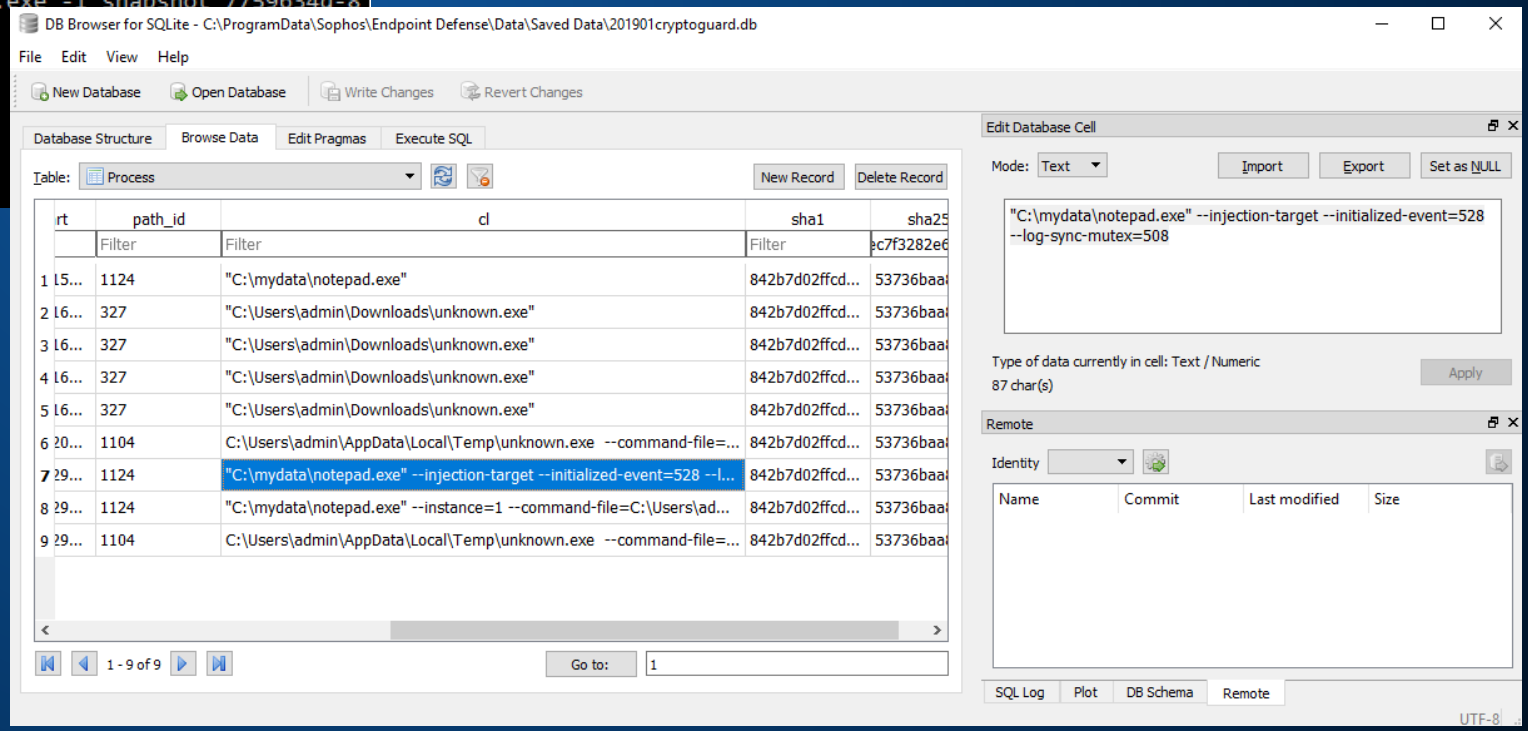
SOPHOS

Forensic Snapshots



Konwersja snapshot przy pomocy SDRExporter do formatu DB

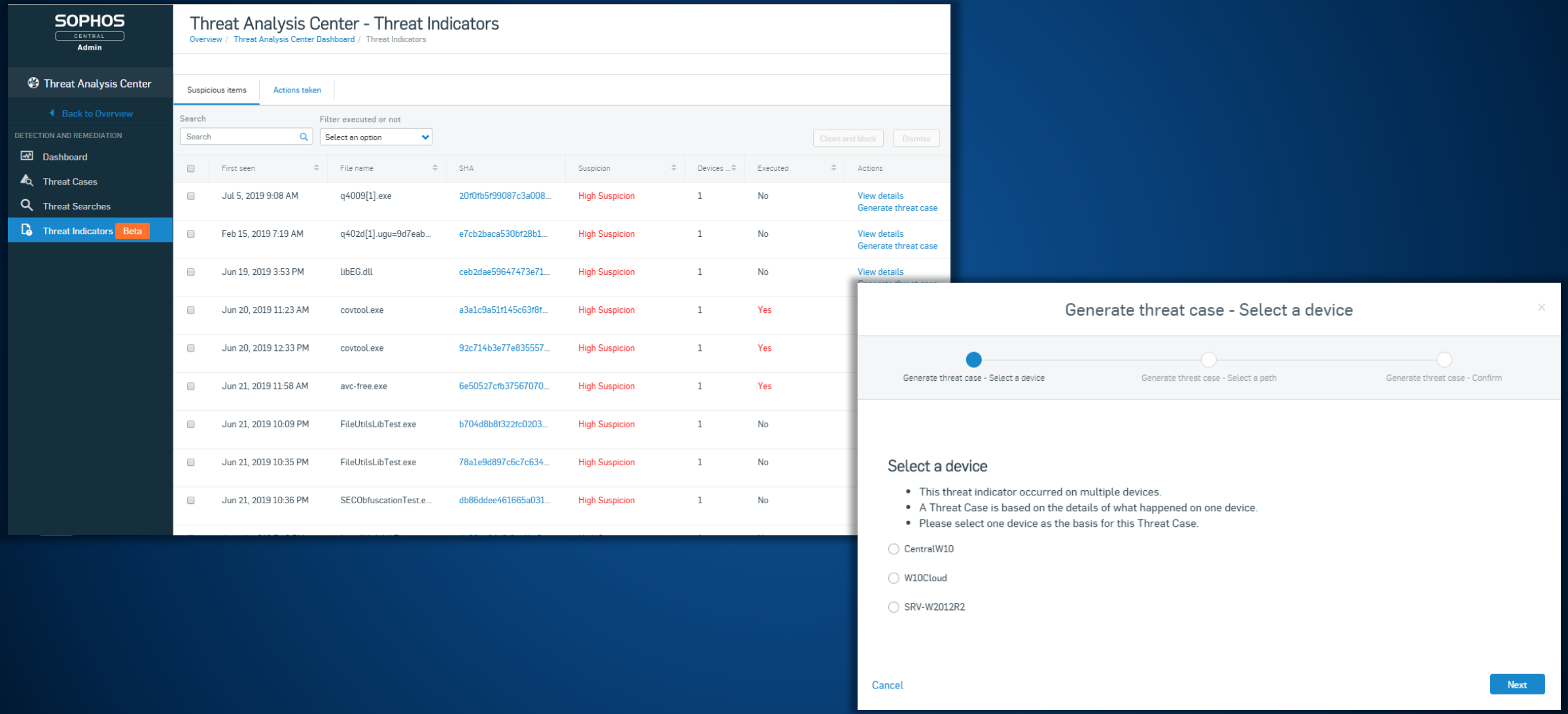
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

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>
```



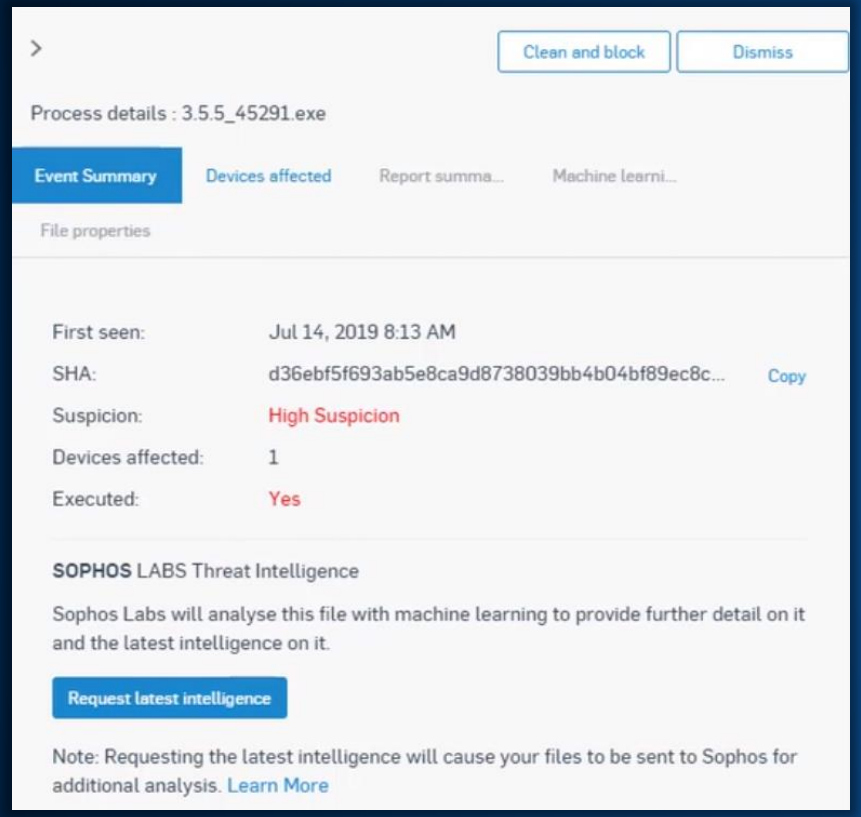
https://community.sophos.com/kb/en-us/132861

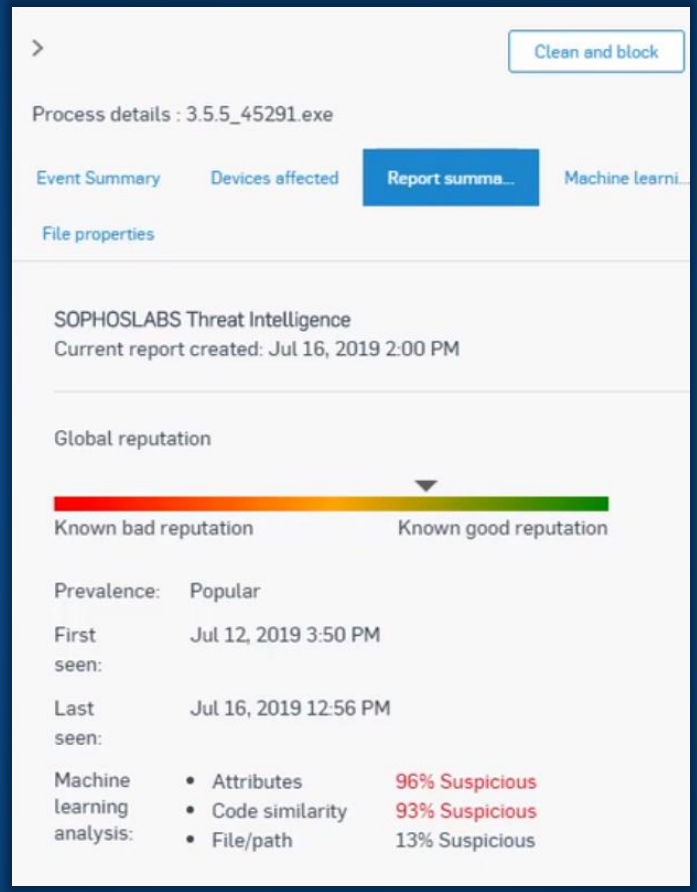
https://community.sophos.com/kb/en-us/133141

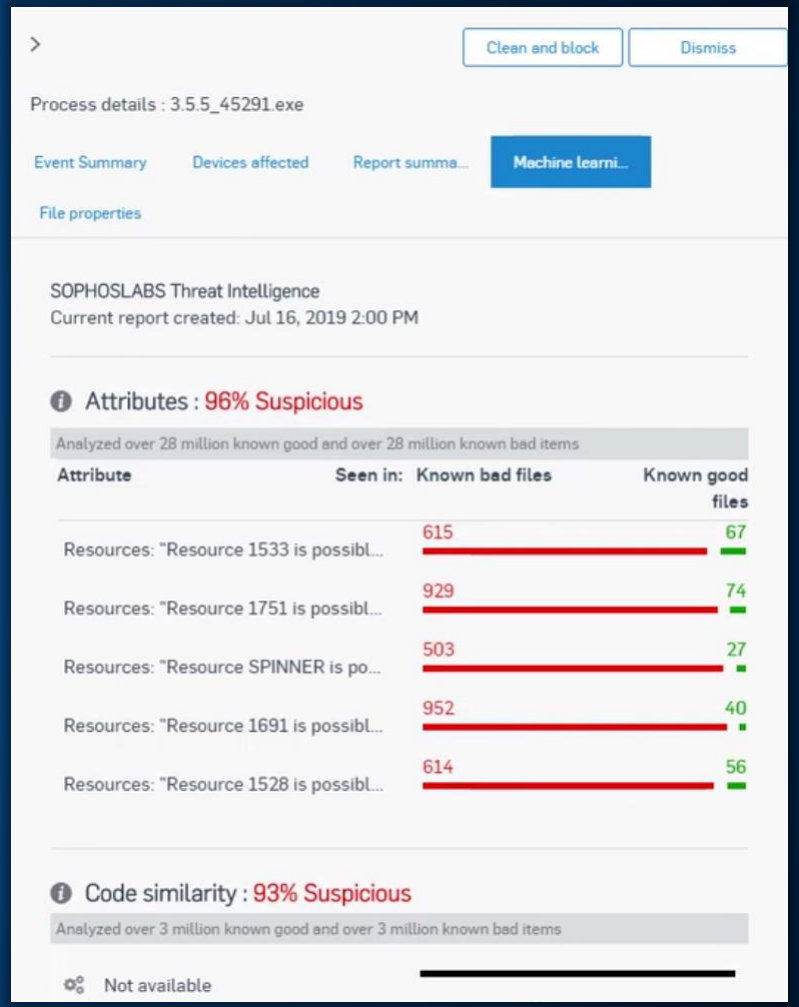
Wskaźniki zagrożenia uczenia maszynowego



Wskaźniki zagrożenia uczenia maszynowego







Advanced

Advanced with EDR

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	Intercept X Advanced	Intercept X 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 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			✓

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.