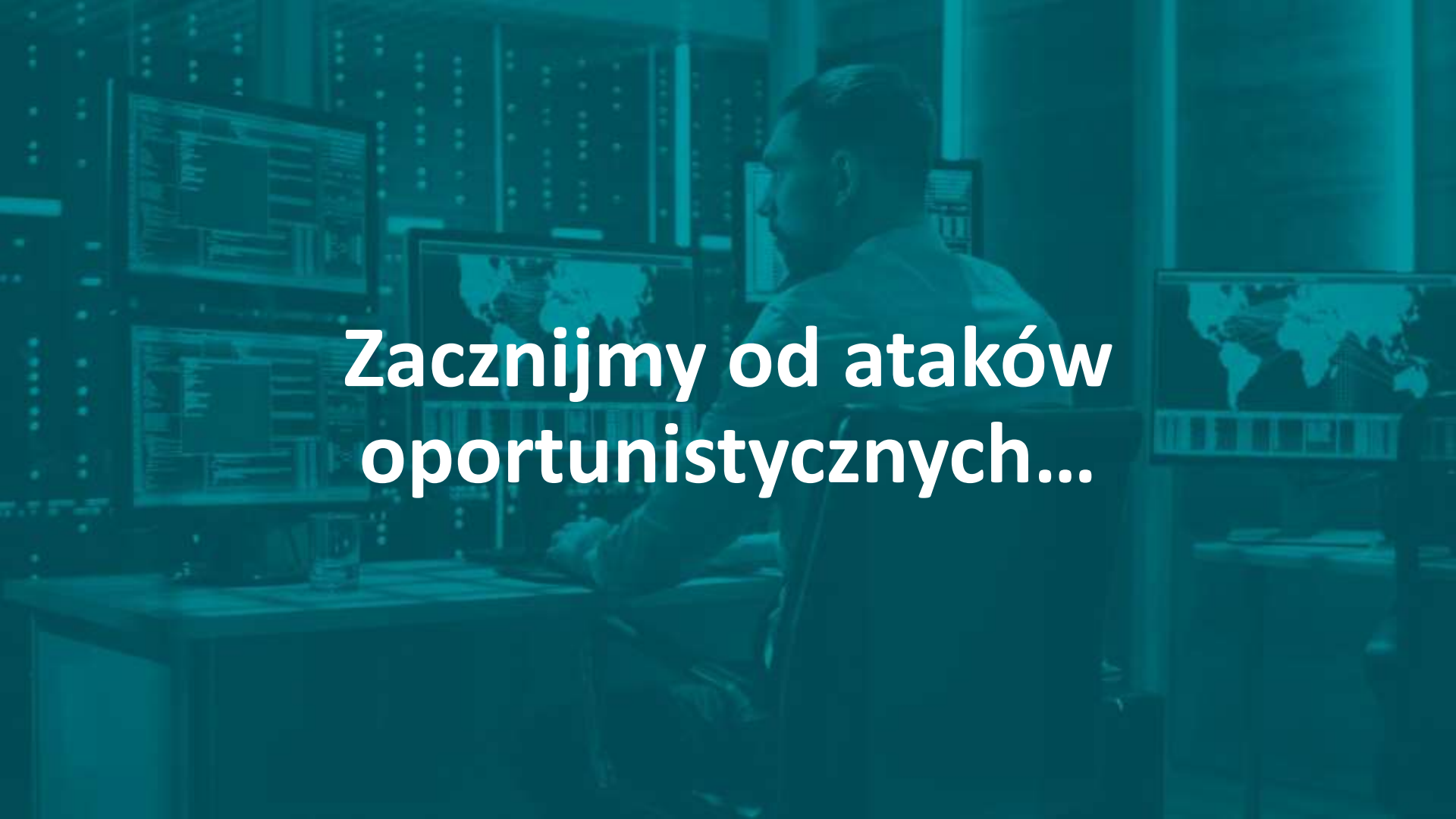


JAK CHRONIĆ SIĘ PRZED UKIERUNKOWANYM ATAKIEM TYPU APT I PRZEPROWADZIĆ SKUTECZNĄ ANALIZĘ POWŁAMANIOWĄ

Robert Łęczycki – Product Manager ESET
Mateusz Laber – Inżynier systemowy



Ataki celowane
vs
Ataki oportunistyczne

A person is seated at a desk in a server room, viewed from the side. They are looking at several computer monitors. The monitors display various data visualizations, including a world map and charts. The room is dimly lit with a strong blue/teal color cast. The text "Zacznijmy od ataków oportunistycznych..." is overlaid in white on the image.

**Zacznijmy od ataków
oportunistycznych...**



ESET LiveGuard Advanced
ochrona przed atakami typu „zero-day”

Najmocniejsze punkty ESET LiveGuard Advanced

- ✓ Blokowanie plików przed uruchomieniem
- ✓ Transparentne dla użytkownika końcowego
- ✓ Prosta konfiguracja, którą robisz tylko raz
- ✓ Błyskawiczne skanowanie do 5 minut
- ✓ Pełna kontrola wysyłanych plików
- ✓ Szczegółowe raporty z analizy
- ✓ Praktycznie bezobsługowa

Jak wyglądają raporty?

PRZEANALIZOWANE ZACHOWANIA

✗	Roślinne Naczynie Piłki	Nie wykryto zachowań
✗	Rejestracja Kluczy Szybnego Domogu	Nie wykryto zachowań
✗	Domag Do Usługi	Nie wykryto zachowań
✗	Wpisanie Zestawu Próbki Zostało Skopnowane	Nie wykryto zachowań
✗	Interakcja Z Oprogramowaniem Antywirusowym	Nie wykryto zachowań
✗	Założenie Nowego Sercowika	Nie wykryto zachowań
✗	Szkodliwe Oprogramowanie Zostało Wykryte Bez Wykrycia	Nie wykryto zachowań
✗	Wskazanie Piłki W Folderze Program Files	Nie wykryto zachowań
✗	Tworzenie Alternatywności	Nie wykryto zachowań
✗	Wyjście W Ramach Uczenia Maszynowego	Nie wykryto zachowań
✗	Wykonanie Alternatywnego Strumienia Danych	Nie wykryto zachowań
✗	Tworzenie Usługi	Nie wykryto zachowań
✗	Modyfikacja Rejestru Rozruchowego	Nie wykryto zachowań
✗	Przeanalizowana Próbka Została Przeniesiona	Nie wykryto zachowań
✗	Tworzenie Wykorzystanego Stosu	Nie wykryto zachowań
✗	Wykonanie Skrypty	Nie wykryto zachowań
✗	Poczwyczenia Usługami Wejściowego	Nie wykryto zachowań
✗	Łącze Serwu Zostało Zmienione	Nie wykryto zachowań
✗	Tworzenie Alternatywnych Strumieni Danych	Nie wykryto zachowań
✗	Zagrożenie Receptorem	Nie wykryto zachowań
✗	Uszkodzona Lub Niekompletna Próbka	Nie wykryto zachowań
✗	Modyfikacja Piłki Użytkownika	Nie wykryto zachowań
✗	Wyjście Zagrożenie Typu „Zrzepnię”	Nie wykryto zachowań
✗	Instalacja Została Rozpozczona	Nie wykryto zachowań
✗	Komunikacja Sercowa	Nie wykryto zachowań
✗	Wyjście Środowiska	Nie wykryto zachowań
✗	Wyjście W Ramach Uczenia Maszynowego	Nie wykryto zachowań
✗	Nawy Pulpki Został Utworzony	Nie wykryto zachowań

CS-OT LIVEGUARD

NIE ZNALEZIONO ZAGROZEŃ

ZAAWANSOWANE SILNIKI SKANOWANIA

- Skanywanie Rozszerzenia Systemowa**
Skanywanie rozszerzenia systemowego - sprawdzanie plików rozszerzenia i konfiguracji rozszerzenia w katalogach Systemowa rozszerzenia.
- Skanywanie Rozszerzenia Programu**
Skanywanie rozszerzenia programu - sprawdzanie plików rozszerzenia i konfiguracji rozszerzenia w katalogach Systemowa rozszerzenia.
- Skanywanie Rozszerzenia Usługi**
Skanywanie rozszerzenia usługi - sprawdzanie plików rozszerzenia i konfiguracji rozszerzenia w katalogach Systemowa rozszerzenia.

PASKOWNICA ANALIZY ZACHOWANIA

- Skanywanie Usługi Systemowej**
Skanywanie usługi systemowej - sprawdzanie plików rozszerzenia i konfiguracji rozszerzenia w katalogach Systemowa rozszerzenia.
- Skanywanie Usługi Systemowej**
Skanywanie usługi systemowej - sprawdzanie plików rozszerzenia i konfiguracji rozszerzenia w katalogach Systemowa rozszerzenia.
- Skanywanie Usługi Systemowej**
Skanywanie usługi systemowej - sprawdzanie plików rozszerzenia i konfiguracji rozszerzenia w katalogach Systemowa rozszerzenia.

PRZEANALIZOWANE ZACHOWANIA

- ✗ Wykonanie Usługi Systemowej
- ✗ Wykonanie Usługi Systemowej
- ✗ Wykonanie Usługi Systemowej
- ✗ Wykonanie Usługi Systemowej
- ✗ Wykonanie Usługi Systemowej
- ✗ Wykonanie Usługi Systemowej
- ✗ Wykonanie Usługi Systemowej

CS-OT LIVEGUARD

SZKODLIWE

PRZEANALIZOWANE ZACHOWANIA

- Skanywanie Rozszerzenia Systemowego**
Skanywanie rozszerzenia systemowego - sprawdzanie plików rozszerzenia i konfiguracji rozszerzenia w katalogach Systemowa rozszerzenia.
- Skanywanie Rozszerzenia Programu**
Skanywanie rozszerzenia programu - sprawdzanie plików rozszerzenia i konfiguracji rozszerzenia w katalogach Systemowa rozszerzenia.
- Skanywanie Rozszerzenia Usługi**
Skanywanie rozszerzenia usługi - sprawdzanie plików rozszerzenia i konfiguracji rozszerzenia w katalogach Systemowa rozszerzenia.
- Skanywanie Usługi Systemowej**
Skanywanie usługi systemowej - sprawdzanie plików rozszerzenia i konfiguracji rozszerzenia w katalogach Systemowa rozszerzenia.
- Skanywanie Usługi Systemowej**
Skanywanie usługi systemowej - sprawdzanie plików rozszerzenia i konfiguracji rozszerzenia w katalogach Systemowa rozszerzenia.
- Skanywanie Usługi Systemowej**
Skanywanie usługi systemowej - sprawdzanie plików rozszerzenia i konfiguracji rozszerzenia w katalogach Systemowa rozszerzenia.

A person is seated at a desk in a server room, viewed from the side. They are looking at several computer monitors. The monitors display various data visualizations, including a world map and technical charts. The room is filled with server racks in the background, and the entire scene is bathed in a blue light. The text 'Pokaz praktyczny ESET LiveGuard Advanced' is overlaid in white on the image.

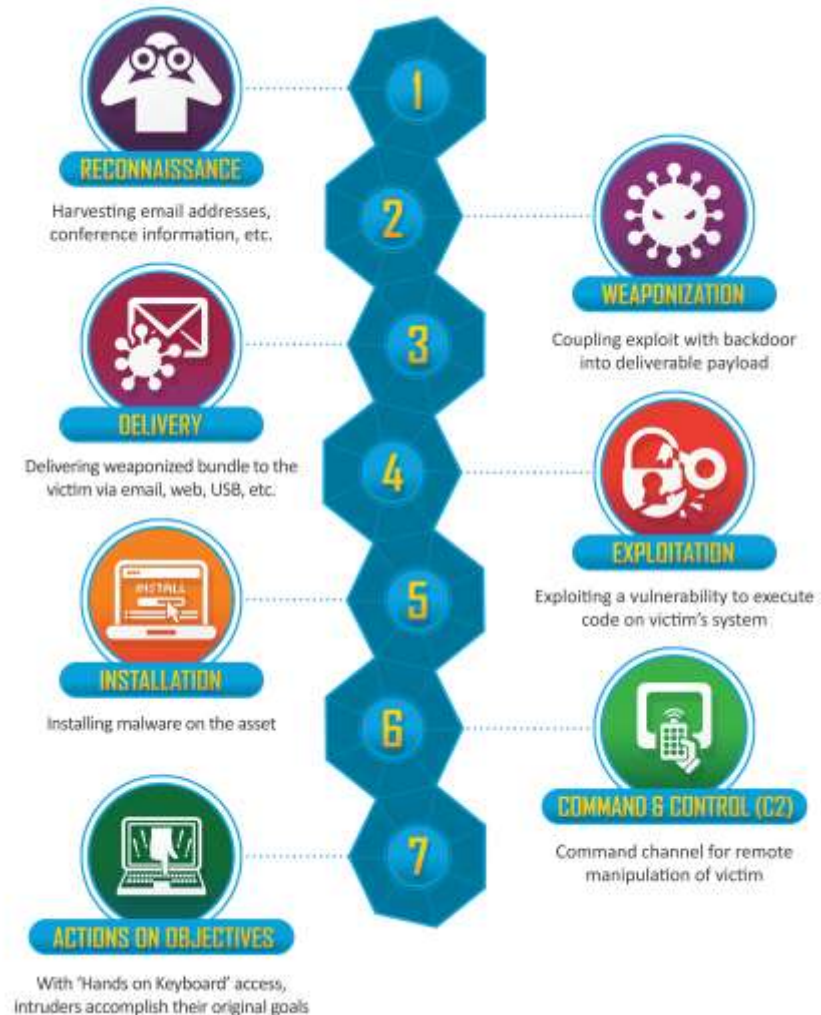
Pokaz praktyczny ESET LiveGuard Advanced

A person is seated at a desk in a server room, looking at several computer monitors. The monitors display various data visualizations, including maps and charts. The room is dimly lit with a blue tint, and server racks are visible in the background.

Przejdźmy do ataków celowanych

Cyber Kill Chain

- Rekonesans
- Techniki, taktyki, procedury opisane przez MITRE ATT&CK (Attack.mitre.org)
- Dystrybucje Kali Linux i ParrotOS
- Framework Metasploit
- Narzędzia systemowe (powershell.exe, certutil.exe, rundll32.exe...)
- Czas...





Recycle Bin



Microsoft
Edge

Co się stało?

Jak się rozpoczął?

Gdzie się rozpoczął?

Kiedy się rozpoczął?

Jak przebiegał?

Jak uniknąć w przyszłości?



Type here to search



ENG

2:02 PM

INTL

06-Jul-20



Co to jest XDR?

- ✓ Monitorowanie sieci i systemów.
- ✓ Szczegółowa analiza zdarzeń i zachowań.
- ✓ Analiza wielu platform.
- ✓ Łączenie danych w alarmy bezpieczeństwa.
- ✓ Wykrywanie i analiza anomalii.
- ✓ Proaktywne wykrywanie zagrożeń.
- ✓ Widoczność i możliwość reakcji.



ESET Inspect

narzędzie klasy XDR

Extended detection and response

Co da mi ESET Inspect?



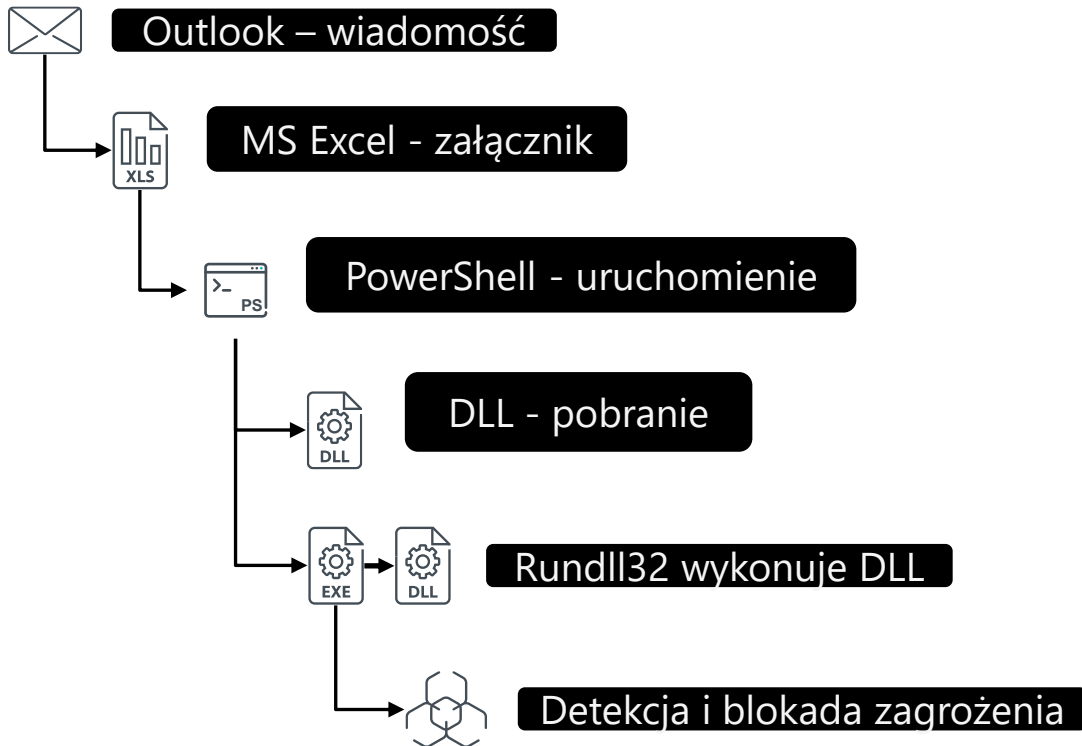
Detekcja



Widoczność



Reakcja



Przykładowe alarmy

- Wykonanie podejrzanego skryptu PowerShell (Mitre att&ck [T1059.001](#) / [T1555.003](#))
- Czytnik PDF rzucił podejrzaną plik wykonywalny (Mitre att&ck [T1203](#))
- **Plik zmodyfikowany w katalogu systemowym startup** (Mitre att&ck [T1547.001](#))
- Proces explorer.exe wykonany spoza katalogu %WINDIR% (Mitre att&ck [T1036.005](#))
- **Microsoft Office zapisał plik *.exe** (Mitre att&ck [T1059.005](#))
- Proces szyfrowania plików (Mitre att&ck [T1486](#))
- Czyszczenie event logs (Mitre att&ck [T1070.001](#))
- Modyfikacja ustawień Windows Firewall (Mitre att&ck [T1562.004](#))
- Uruchomienie pliku z podejrzanym rozszerzeniem (Mitre att&ck [T1036](#))
- **Potencjalne wykorzystanie luki Log4Shell (CVE-2021-44228)** (Mitre att&ck [T1210](#))

- **Ponad 900 innych + możliwość tworzenia własnych**

Framework MITRE ATT&CK

ATT&CK Matrix for Enterprise

[layouts](#)
[show sub-techniques](#)
[hide sub-techniques](#)

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Fulfillment	Impact
18 techniques	8 techniques	7 techniques	18 techniques	14 techniques	12 techniques	27 techniques	19 techniques	22 techniques	7 techniques	17 techniques	14 techniques	8 techniques	13 techniques
Active Scanning (T)	Acquire Infrastructure (S)	Drive-by-Compromise (X)	Desktop and Laptop Hijacking (S)	Account Manipulation (S)	Host Execution Control Mitigation (S)	Abuse Windows System Mechanisms (S)	Drive Filing (S)	Account Enumeration (S)	Administrative UI Access (S)	Active Directory Data (S)	Application Layer Protocol (S)	Hardware Hijacking (S)	Account Access Retention (S)
...

Techniki Taktyki Procedury

TECHNIQUES

Registry Run Keys / Startup Folder

Authentication Package

Time Providers

Winlogon Helper DLL

Security Support Provider

Kernel Modules and Extensions

Re-opened Applications

LSASS Driver

Shortcut Modification

Port Monitors

Print Processors

XDG Autostart Entries

Active Setup

Login Items

Boot or Logon Initialization Scripts

Browser Extensions

Compromise Client Software Binary

Create Account

Create or Modify System Process

Event Triggered Execution

External Remote Services

Hijack Execution Flow

Implant Internal Image

Home -> Techniques -> Enterprise -> Boot or Logon Autostart Execution -> Registry Run Keys / Startup Folder

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Other sub-techniques of Boot or Logon Autostart Execution (14)

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. ^[1] These programs will be executed under the context of the user and will have the account's associated permissions level.

Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in. The startup folder path for the current user is `%localappdata%`.

The startup folder path for all users is `%allusersprofile%\startup`. The startup folder path for all users is `%allusersprofile%\startup`.

The following run keys are created by default on Windows systems:

- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce`

Run keys may exist under multiple hives. ^[2] The

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx` is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency. ^[3] For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx: `reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx\001\Depend" /v "C:\Program Files\logon\logon.dll" /t REG_SZ` ^[4]

The following Registry keys can be used to set startup folder items for persistence:

- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell\Folders`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell\Folders`

ID: T1547.001

Sub-technique of: T1547

- Tactics: Persistence, Privilege Escalation
- Platforms: Windows
- Permissions Required: Administrator, User
- CAPEC ID: CAPEC-270
- Contributors: Oddvar Moe, goddvmoe
- Version: 1.1
- Created: 23 January 2020
- Last Modified: 12 May 2022

Version Permalink

Jaką wartość wnosi XDR ESET?

- Platforma bezpieczeństwa oparta o ESET PROTECT
- Jest proste we wdrożeniu i zarządzaniu
- Nie wymaga dedykowanego zespołu Security
- Zbiera dane z systemów Windows, Linux i MacOS
- Elastyczne wdrożenie lokalnie lub chmurowo
- Działa w tle, zużywa minimum zasobów stacji końcowej
- Dane są przetwarzane wewnątrz organizacji (on-prem) lub w ramach chmury (region UE w AWS i Azure)

A person is seated at a desk in a server room, viewed from the side. They are looking at a computer monitor. The room is filled with server racks and multiple monitors. The scene is dimly lit with a strong blue/teal color cast. The text 'Pokaz praktyczny ESET Inspect' is overlaid in white on the image.

Pokaz praktyczny ESET Inspect

Jak można zoptymalizować pracę z XDR?

Perfekcyjny **POC w 3 krokach:**

Krok 1: Otrzymujesz licencje testowe, instruktaż wdrożenia

Krok 2: Uruchamiasz konsolę, wdrażasz konektory, zbierasz dane

Krok 3: Masz już alarmy a nasz inżynier nieodpłatnie pomaga Ci :

- przeanalizować alarmy i zdarzenia
- zoptymalizować konfigurację
- utworzyć wyjątki przydatne w Twojej sieci
- zmodyfikować reguły tak aby alarmowały w punkt

EFEKT: Działający, zoptymalizowany i w pełni funkcjonalny XDR

Dodatkowo w produkcji ustawisz:

Tryb uczenia | Typ użytkownika | Zakres danych | Retencję danych

Pakiety biznesowe ESET



Cloud

	 PROTECT ESSENTIAL	 PROTECT ENTRY	 PROTECT ADVANCED	 PROTECT COMPLETE	 PROTECT ENTERPRISE	 PROTECT MAIL PLUS
Konsola ESET PROTECT Cloud	✓	✓	✓	✓	✓	✓
ESET Server Security / ESS	✓	✓	✓	✓	✓	✗
ESET Endpoint Antivirus / EEA	✓	✓	✓	✓	✓	✗
ESET Endpoint Security for Android / EES AND	✓	✓	✓	✓	✓	✗
ESET Endpoint Security / EES	✗	✓	✓	✓	✓	✗
Sandboxing w chmurze / ELGA	✗	✗	✓	✓	✓	✓
Szyfrowanie dysków / EFDE	✗	✗	✓	✓	✓	✗
Ochrona serwera pocztowego / EMS	✗	✗	✗	✓	✗	✓
Ochrona Microsoft 365 / ECOS & ELGA	✗	✗	✗	✓	✗	✗
Extended Detection & Response / EI	✗	✗	✗	✗	✓	✗



DZIĘKUJEMY ZA UWAGĘ