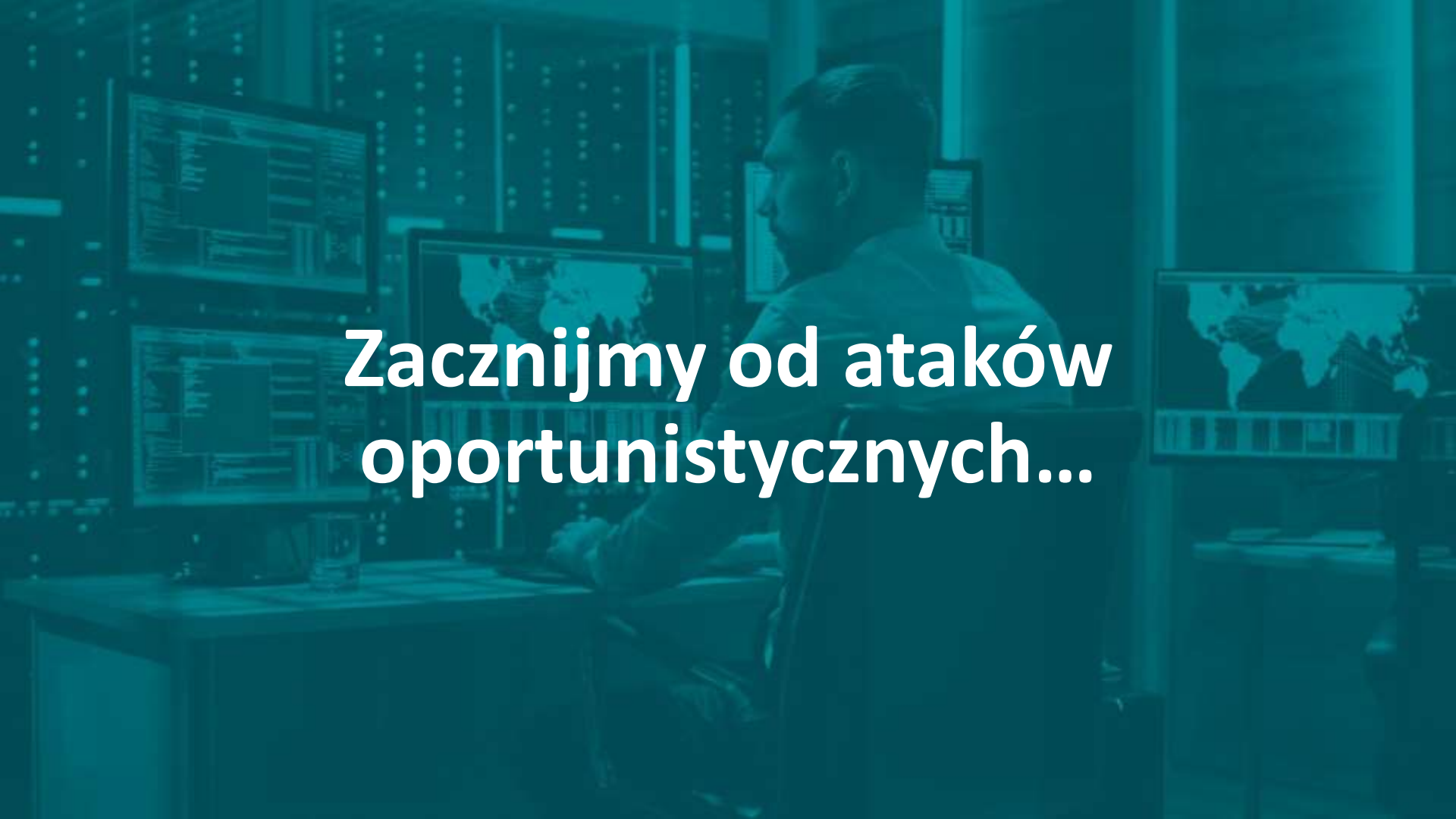
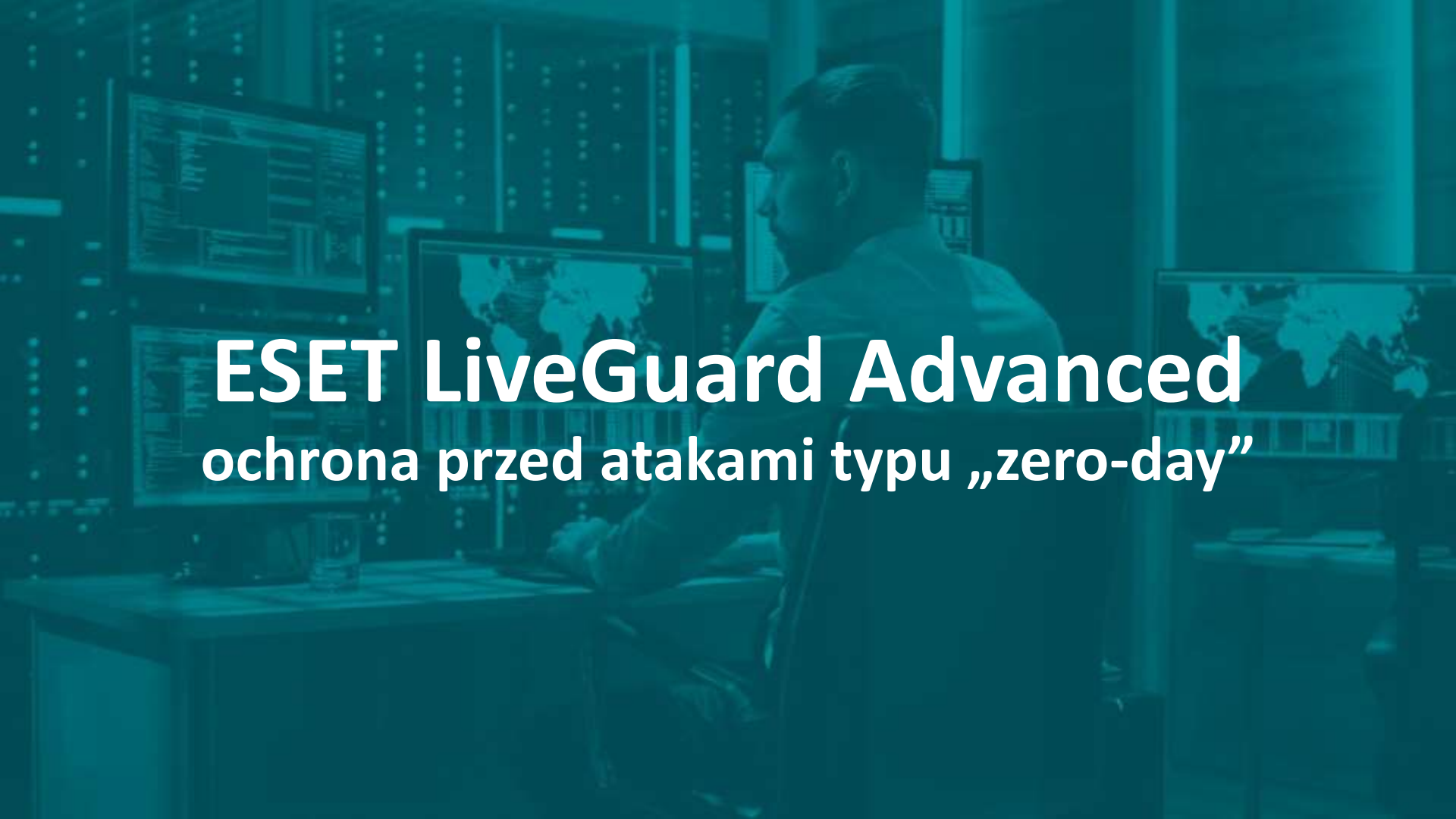
JAK CHRONIĆ SIĘ PRZED UKIERUNKOWANYM ATAKIEM TYPU APT I PRZEPROWADZIĆ SKUTECZNĄ ANALIZĘ POWŁAMANIOWĄ

Robert Łęczycki – Product Manager ESET
Mateusz Laber – Inżynier systemowy

Ataki celowane
vs
Ataki oportunistyczne


Zacznijmy od ataków
oportunistycznych…



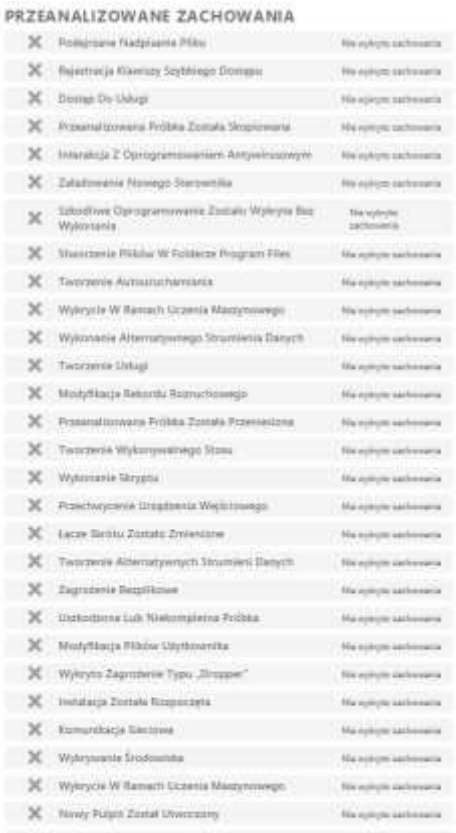
ESET LiveGuard Advanced

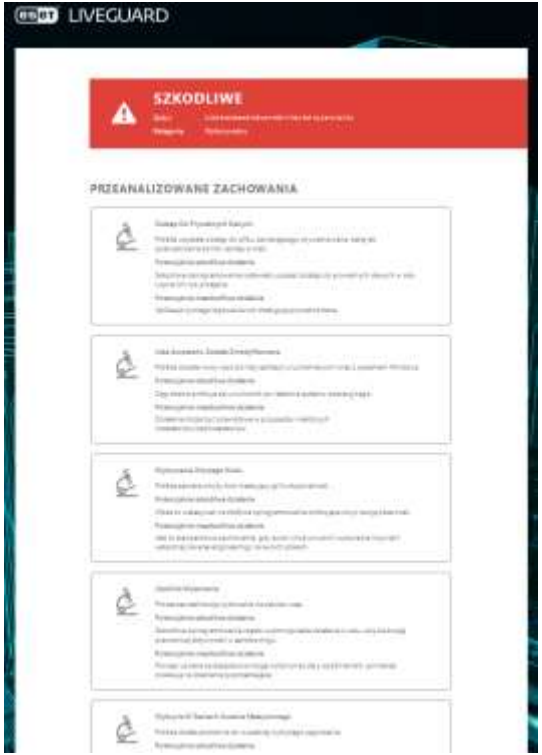
ochrona przed atakami typu „zero-day”

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?



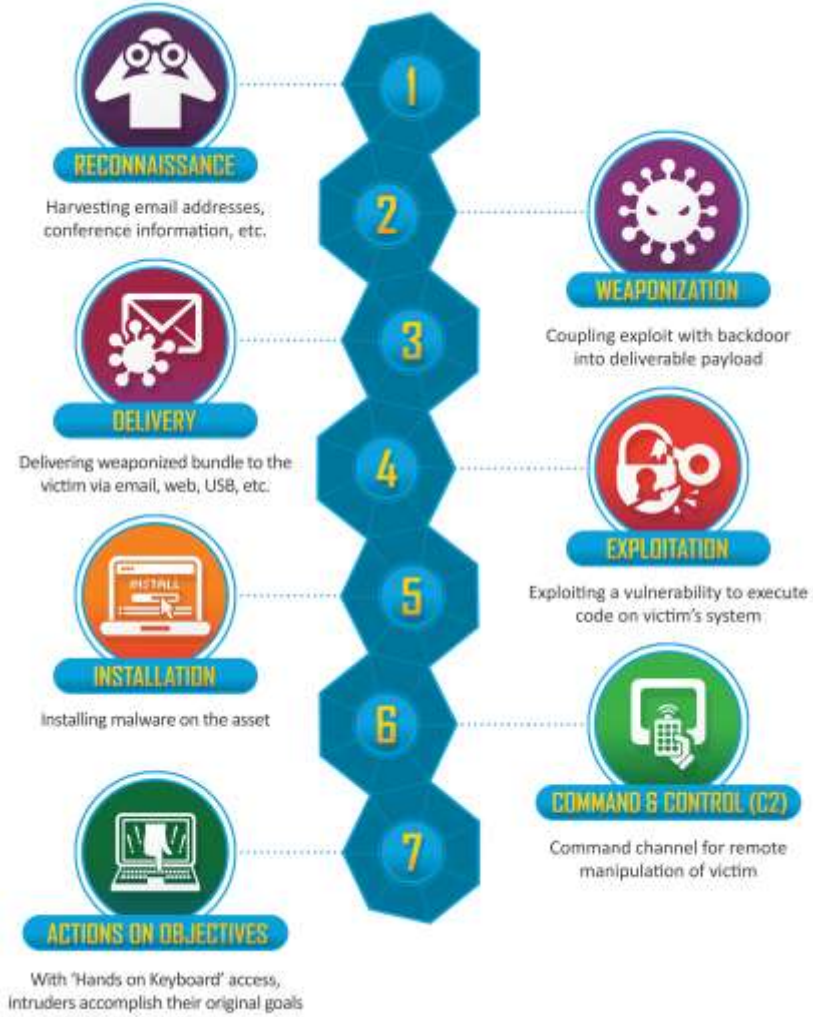


Pokaz praktyczny ESET LiveGuard Advanced

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…**



https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Co się stało?

Jak się rozpoczął?

Gdzie się rozpoczął?

Kiedy się rozpoczął?

Jak przebiegał?

Jak uniknąć w przyszłości?

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

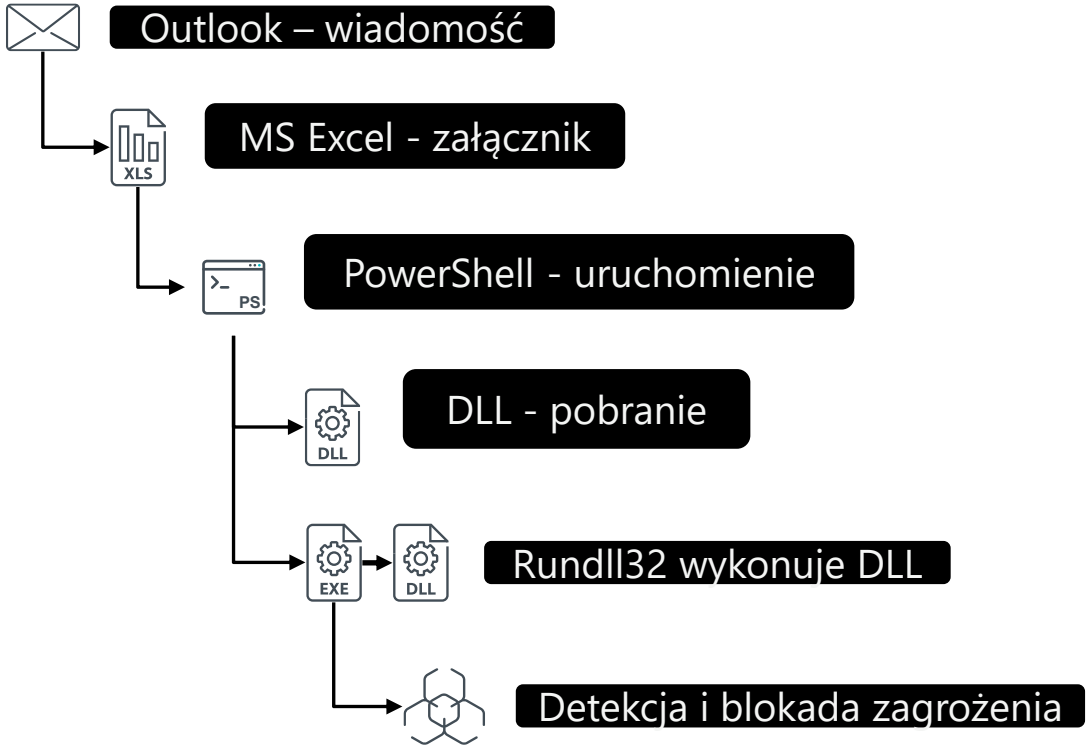
narzędzie klasy XDR
Extended detection and response

Co da mi ESET Inspect?

Detekcja

Widoczność

Reakcja



Przykładowe alarmy

- Wykonanie podejrzanego skryptu PowerShell (Mitre att&ck T1059.001 / T1555.003)
- Czytnik PDF zrzucił podejrzany 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

https://attack.mitre.org

Techniki Taktyki Procedury

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)

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 produkcie 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	✗	✗	✗	✗	✓	✗

Digital Security
Progress. Protected.