Przemysłowy antywirus dla Energetyki – możliwości i zastosowanie

Mirosław Zwierzyński

Email: miroslaw.zwierzynski@elmark.com.pl

Elmark Automatyka S.A., ul. Niemcewicza 76, 05-075 Warszawa, Polska

Elmark Automatyka w pigułce

Przemysłowa komunikacja i Cyberbezpieczeństwo

ELMARK Automatyka

Obszary działania:

- Kompletna infrastruktura komunikacyjna dla OT
- Rozwiązania do budowa przemysłowych sieci Ethernet
- Wykorzystanie IEC 62443 w budowie sieci
- Segmentacja sieci
- Ochrona assetów na poziomie sieciowym z wykorzystaniem systemów IPS
- Ochrona assetów końcowych opartych o systemy Windows
- Inspekcja assetów opartych o systemy Windows

Przemysłowa komunikacja i Cyberbezpieczeństwo

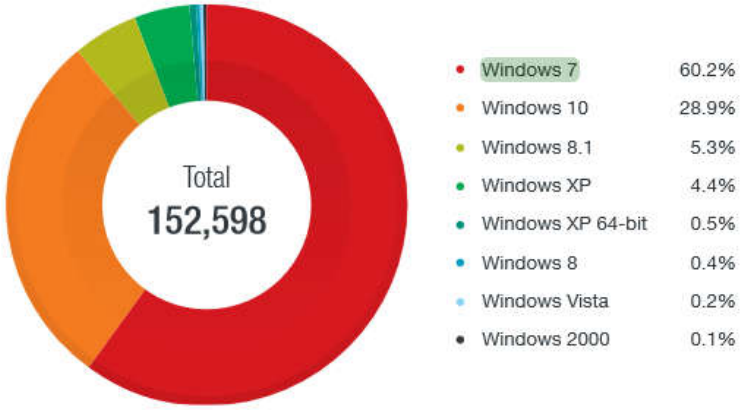
Nasi partnerzy

Systemy operacyjne w aplikacjach OT

Systemy Windows w środowiskach przemysłowych

Systemy operacyjne Windows w środowiskach przemysłowych (dane z 2020 roku)

Starsze wersje Windows dalej mają znaczący udział



Źródło:
Trend micro securing smart factories threats to manufacturing environments in the era of industry 4.0
https://documents.trendmicro.com/assets/white_papers/wp-threats-to-manufacturing-environments-in-the-era-of-industry-4.pdf

50% użytkowników ma zaimplementowany antywirus w środowisku OT

Na bazie odpowiedzi około 500 respondentów – właścicieli fabryk

Źródło
The State of Industrial Cybersecurity
Converging IT and OT with people, process, and technology
https://resources.trendmicro.com/rs/945-CXD-062/images/WP00_State_Industrial_Cybersecurity_White_Paper_210319US_web.pdf

Jakie widzimy potrzeby i wyzwania?

- Brak pełnej wiedzy o stanie, statusach oraz wykorzystaniu posiadanych komputerów w obszarze OT
- Brak pełnej kontroli nad działaniami użytkowników
- Ryzyko nieautoryzowanego wykorzystania fizycznych portów
- Nieświadoma ingerencja w pliki systemowe oraz aplikacji
- Ryzyko transferu niebezpiecznego oprogramowania przez „zewnętrznych" użytkowników
- Brak dedykowanych narzędzi do realizacji polityk bezpieczeństwa

Zabezpieczenie stacji inżynierskich i komputerów przemysłowych przed nieautoryzowanym oprogramowaniem oraz łatwe monitorowanie ich wykorzystania

Istniejące rozwiązania vs wymagania OT

Po prostu nie pasują - rozwiązania IT nie biorą pod uwagę trudnych warunków w sieciach OT:

- Mała tolerancja na opóźniania sieci
- Przestarzałe systemy operacyjne (brak wsparcia dla starszego systemu niż Windows 7)
- Ograniczone zasoby obliczeniowe – min. Wymaganie na 1 GB RAM
- Brak internetu = nie da się pobrać aktualizacji sygnatur

Istotne ograniczenia – brak informacji na temat środowisk przemysłowych w rozwiązaniach bezpieczeństwa IT

- Różne protokoły sieciowe
- Aplikacje od różnych dostawców
- Podatności specyficzne dla OT
- Taktyki i techniki atakujących stosowane w OT

Sama widoczność nie jest wystarczająca – brak osób odpowiedzialnych za bezpieczeństwo OT

- Zmęczenie ilością zdarzeń
- Potrzeba technik blokujących 99% znanych zagrożeń

TXOne Stellar

TXOne Stellar

ELMARK Automatyka

Przemysłowy antywirus nowej generacji

Zaawansowane skanowanie w poszukiwaniu zagrożeń zabezpiecza zasoby OT bez przerywania pracy

Ochrona aplikacji przemysłowych

Wykrywanie i rozpoznawanie aplikacji ICS/OT oraz ich ochrona

Inteligentne wykrywanie anomalii

Wykrywanie nieprawidłowych operacji, które nie pasują do wzorca zachowania użytkownika

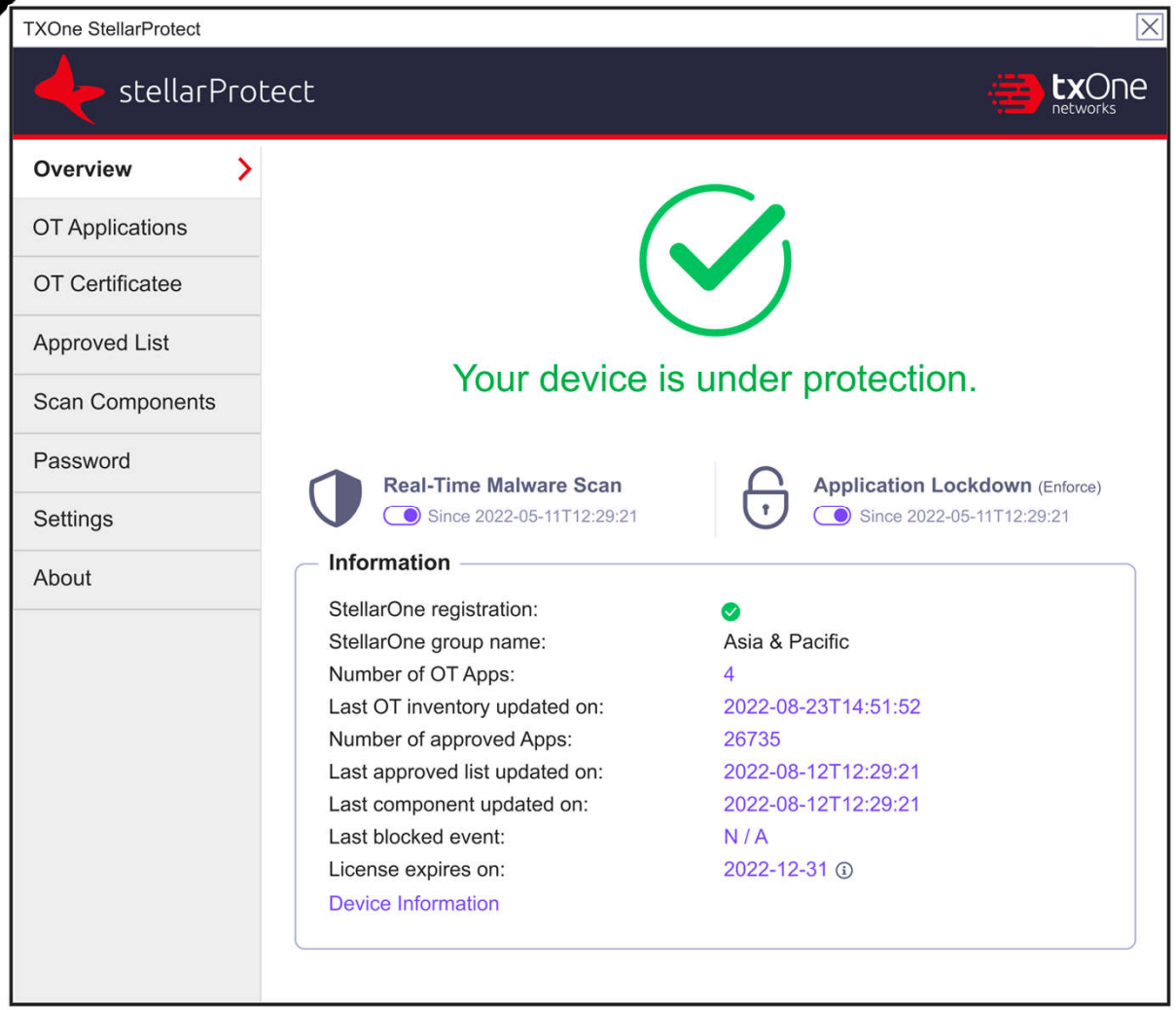
Blokowanie niezaufanych procesów

Tylko zaufane i zatwierdzone procesy mogą być uruchamiane przez użytkownika oraz inne aplikacje

Kontrola portów USB

Zapobieganie zagrożeniom wewnętrznym i szkodliwym działaniom

Stellar Protect – lekki agent na systemy Windows



- OT EDR+
- Next-gen AV
- Lockdown
- Device control
- Support legacy

Stellar Protect – systemy operacyjne

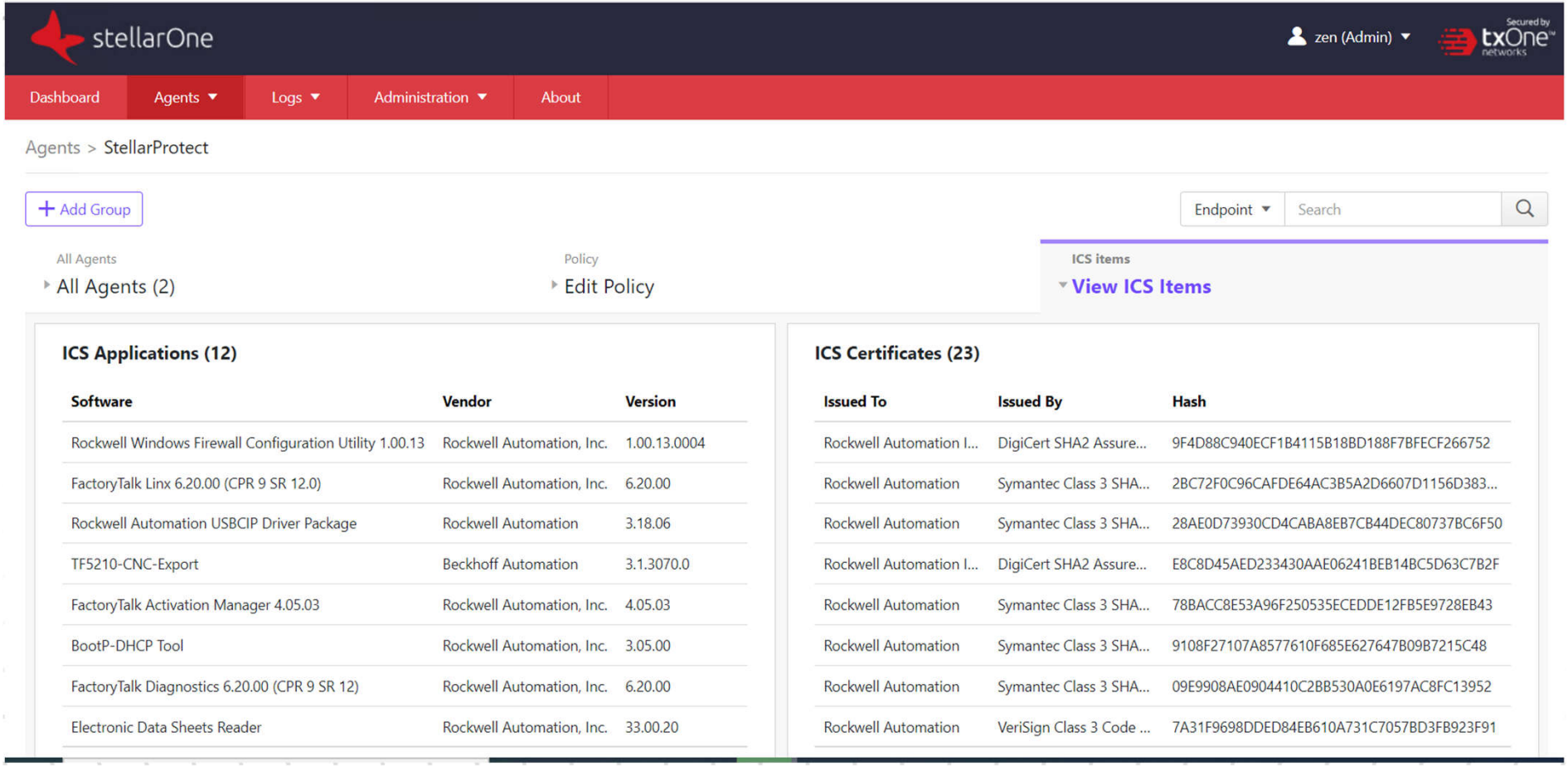
ELMARK Automatyka

Wspierane systemy operacyjne

OS	Client OS	Server OS
	- Windows 2000 (SP4) [Professional] (32bit) **- Windows XP (SP1/SP2/SP3) [Professional/Professional for Embedded Systems] (32bit)** **- Windows Vista (NoSP/SP1/SP2) [Business/Enterprise/ Ultimate] (32bit)** **- Windows 7 (NoSP/SP1) [Professional/Enterprise/Ultimate/ Professional for Embedded Systems/Ultimate for Embedded Systems] (32/64bit)** - Windows 8 (NoSP) [Pro/Enterprise] (32/64bit) - Windows 8.1 (NoSP) [Pro/Enterprise/with Bing] (32/64bit) - Windows 10 [Pro/Enterprise/IoT Enterprise] (32/64bit) Anniversary Update, Creators Update, Fall Creators Update, April 2018 Update, October 2018 Update*, May 2019 Update, November 2019 Update, May 2020 Update, October 2020 Update, May 2021 Update, November 2021 Update, 2022 Update - Windows 11 (NoSP) [Pro/Enterprise] (64bit) 2022 Update - Windows XP Embedded (SP1/SP2) (32bit) - Windows Embedded Standard 2009 (NoSP) (32bit) - Windows Embedded POSReady 2009 (32bit) - Windows Vista for Embedded Systems (NoSP/SP1/SP2) (32bit) - Windows Embedded Standard 7 (NoSP/SP1) (32/64bit) - Windows Embedded POSReady 7 (NoSP) (32/64bit) - Windows Embedded 8 Standard (NoSP) (32/64bit) - Windows Embedded 8 Industry (NoSP) [Pro/Enterprise] (32/64bit) - Windows Embedded 8.1 Industry (NoSP) [Pro/Enterprise/Sideloading] (32/64bit) - Windows Embedded POSReady (32bit)	**- Windows 2000 Server (SP4) (32bit)** **- Windows Server 2003 (SP1/SP2) [Standard/Enterprise/ Storage] (32bit)** **- Windows Server 2003 R2 (NoSP/SP2) [Standard/Enterprise/ Storage] (32bit)** **- Windows Server 2008 (SP1/SP2) [Standard/Enterprise/ Storage] (32/64bit)** **- Windows Server 2008 R2 (NoSP/SP1) [Standard/Enterprise/ Storage] (64bit)** - Windows Server 2012 (NoSP) [Essentials/Standard] (64bit) - Windows Server 2012 R2 (NoSP) [Essentials/Standard] (64bit) - Windows Server 2016 (NoSP) [Standard] (64bit) - Windows Server 2019 (NoSP) [Standard] (64bit) - Windows Server 2022 (NoSP) [Standard] (64bit) - Windows Storage Server 2012 (NoSP) [Standard] (64-bit) - Windows Storage Server 2012 R2 (NoSP) [Standard] (64-bit) - Windows Storage Server 2016 (NoSP) (64bit) - Windows Server 2003 for Embedded Systems (SP1/SP2) (32bit) - Windows Server 2003 R2 for Embedded Systems (NoSP/SP2) (32bit) - Windows Server 2008 for Embedded Systems (SP1/SP2) (32/64bit) - Windows Server 2008 R2 for Embedded Systems (NoSP/SP1) (64bit) - Windows Server 2012 for Embedded Systems (NoSP) (64bit) - Windows Server 2012 R2 for Embedded Systems (NoSP) (64bit)
CPU	Equivalent to minimum system requirements of operating system (only Intel 64 and IA-32 Architectures supported)	
Memory	Equivalent to minimum system requirements of operating system	
Free HDD space	Minimum 300MB	

StellarOne - Wykrywanie i rozpoznawanie aplikacji ICS/OT

ELMARK Automatyka



StellarOne – Wykrywanie i rozpoznawanie aplikacji ICS/OT

- ABB
- Acronis
- Autonics
- Baker Hughes
- Bürkert
- Codesys
- Delta electronics
- Druck limited
- Emerson
- Epson Robots
- Fanuc
- Fisher controls
- Fuji
- GE
- Idec
- Keyence
- Hitachi
- Honeywell
- Lovato electric
- Micromeritics
- Mitsubishi
- Motorola
- National instruments
- Omron
- Pactware
- Phoenix contact
- Red lion
- Roboticsware
- Rockwell
- Seiko Epson
- Schneider
- Siemens
- Verif-I
- YASKAWA
- Yokogawa
- Yamaha

StellarOne – ochrona aplikacji ICS oraz ich zasobów

ELMARK Automatyka

Ochrona aplikacji ICS

Group
Nagoya Horita (5)

Policy
Edit Policy

ICS Application Safeguard

Protect files and folders from unauthorized changes.

Protect the ICS Applications

K-254-A23	10.1.192.36		South Area	Omron	S7-400	Metee

ICS Applications (4)

Software	Vendor	Version	Install Path
ROBOT Studio	ABB	7.0	C:\Program Files (x86)\ABB Indu
Factory Talk	Rockwell	6.1	C:\Program Files\Rockwell Software\Factory
Roof Station	Siemens	2.12.0.1	C:\Program Files\Rockwell Software\Factory
Citect	Schneider	10.12.93	C:\Program Files\Rockwell Software\Factory

Ochrona krytycznych plików/folderów

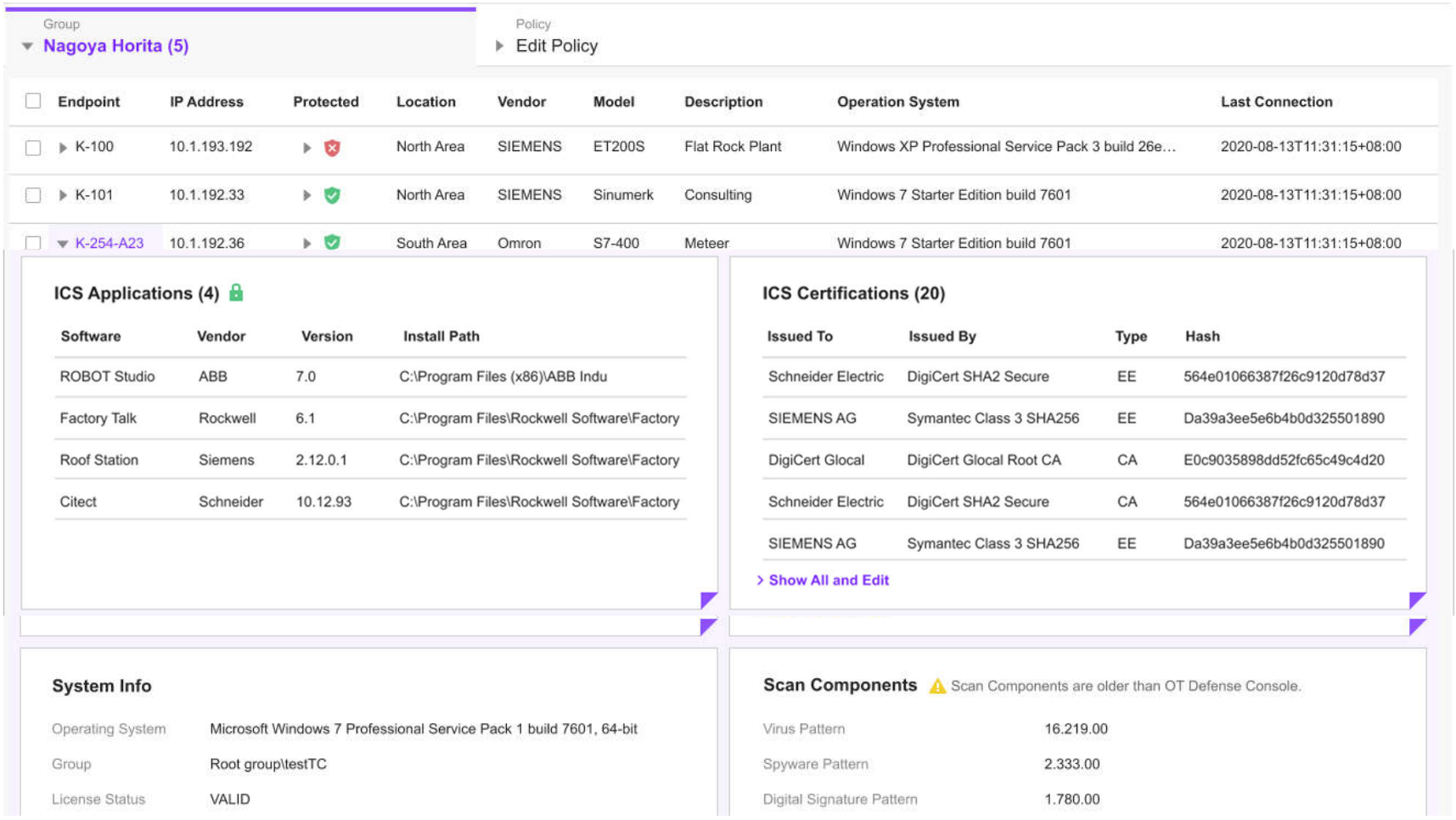
ICS Application Safeguard

+ Add

Protection Path	Type	Exception Process	Actions
All ICS Applications	All ICS Applications	C:\Windows\explorer.exe	
HKEY_LOCAL_MACHINE\SOFTWA	Registry Key	C:\Windows\explorer.exe	
C:\MyFolder	Folder	No Process can write	
C:\MyFolder\MyFile.exe	File	-	
HKEY_LOCAL_MACHINE\SOFTWA	Registry Key	-	

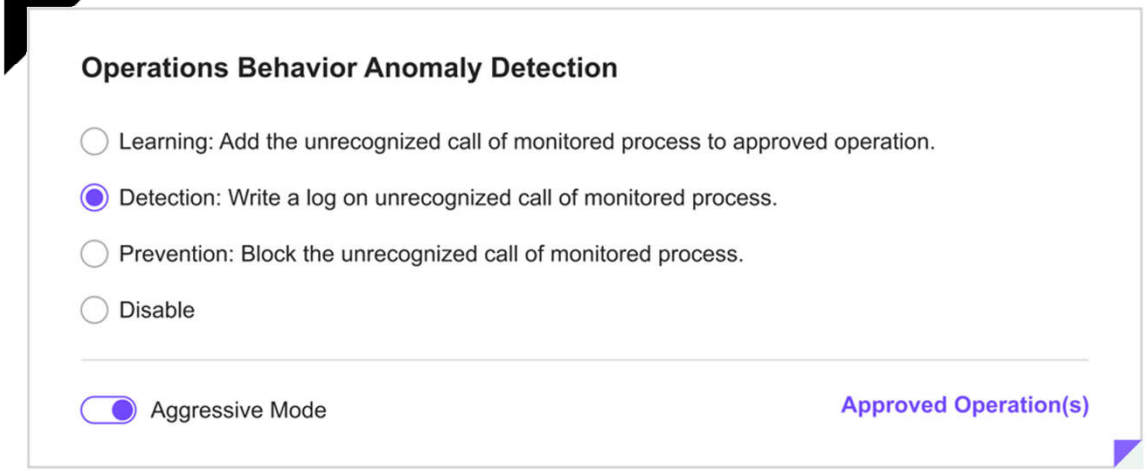
StellarOne – zarządzanie aplikacjami/certyfikatami

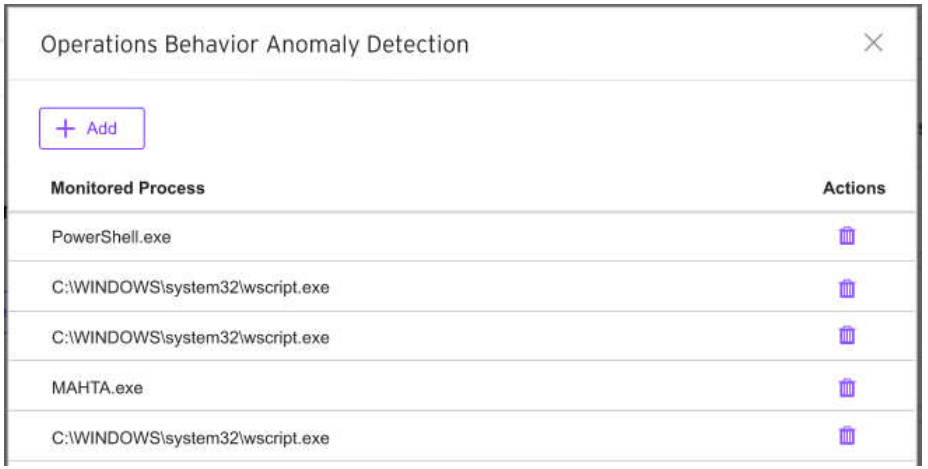
ELMARK Automatyka



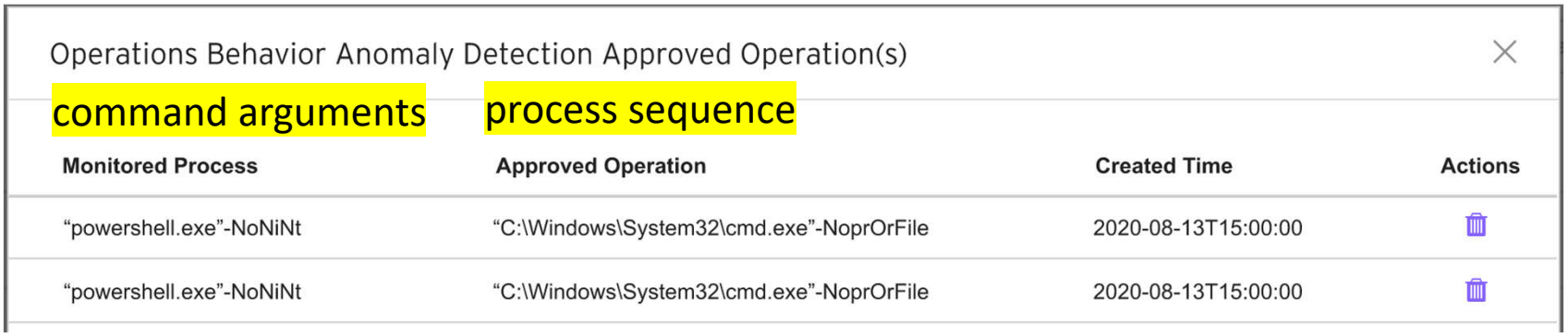
StellarOne – Wykrywanie anomalii

Monitorowanie wrażliwych procesów – np. PowerShell





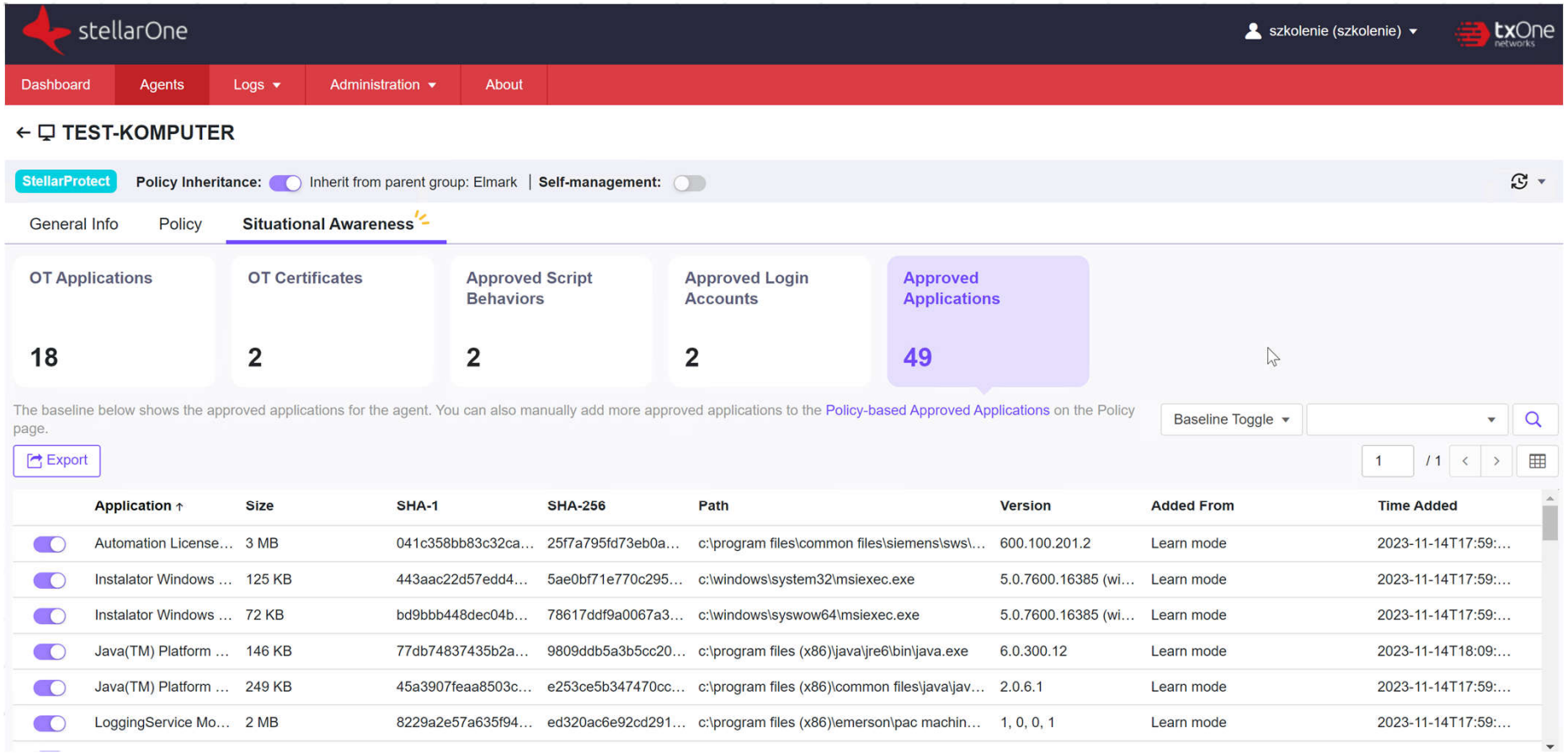
Nauka i akceptowanie prawidłowego zachowania użytkownika



https://www.txone.com/blog/how-flax-typhoon-hack-weaponized-legitimate-software/

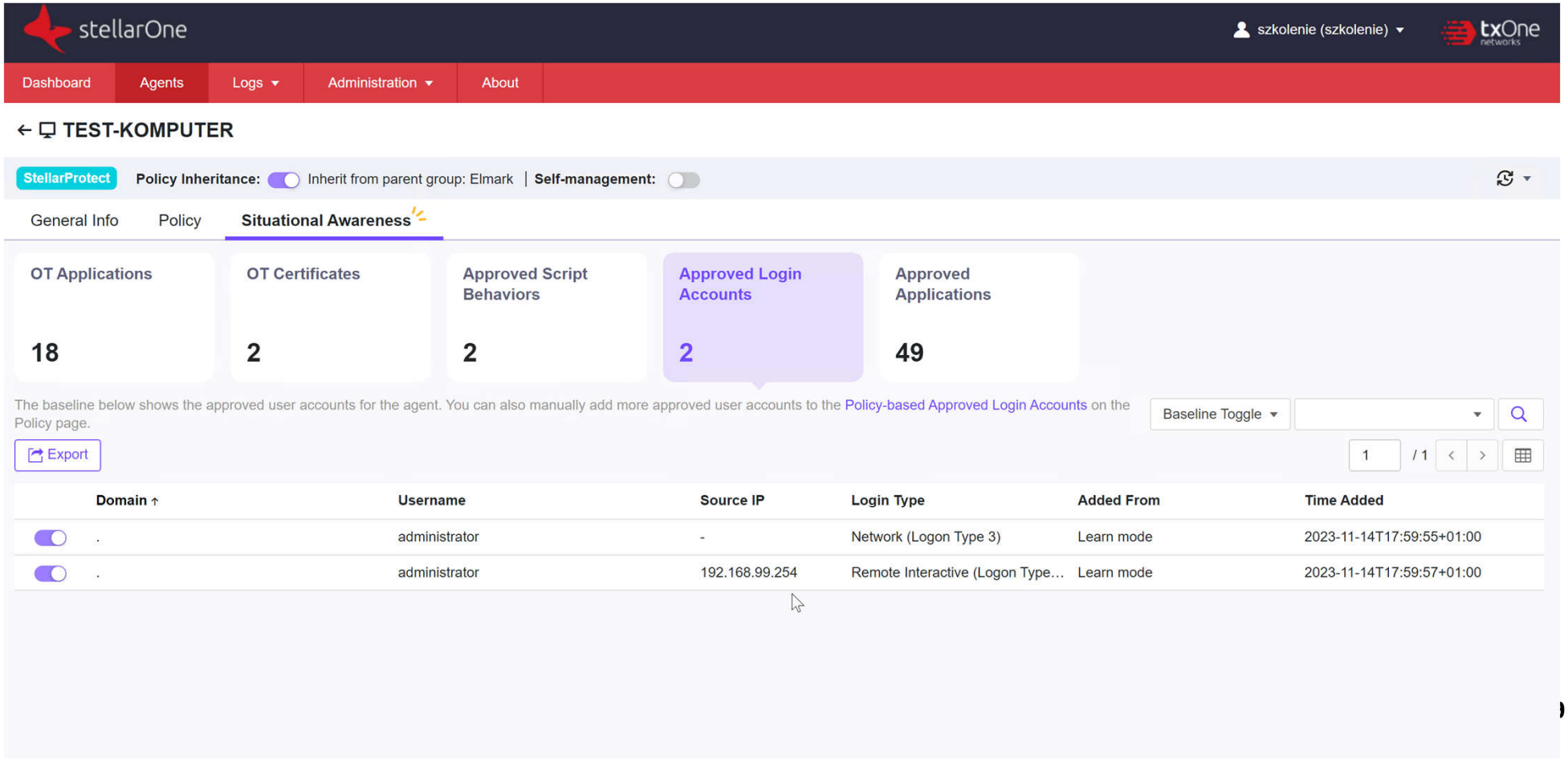
StellarOne – Wykrywanie anomalii

Nauka i akceptowanie prawidłowych aplikacji



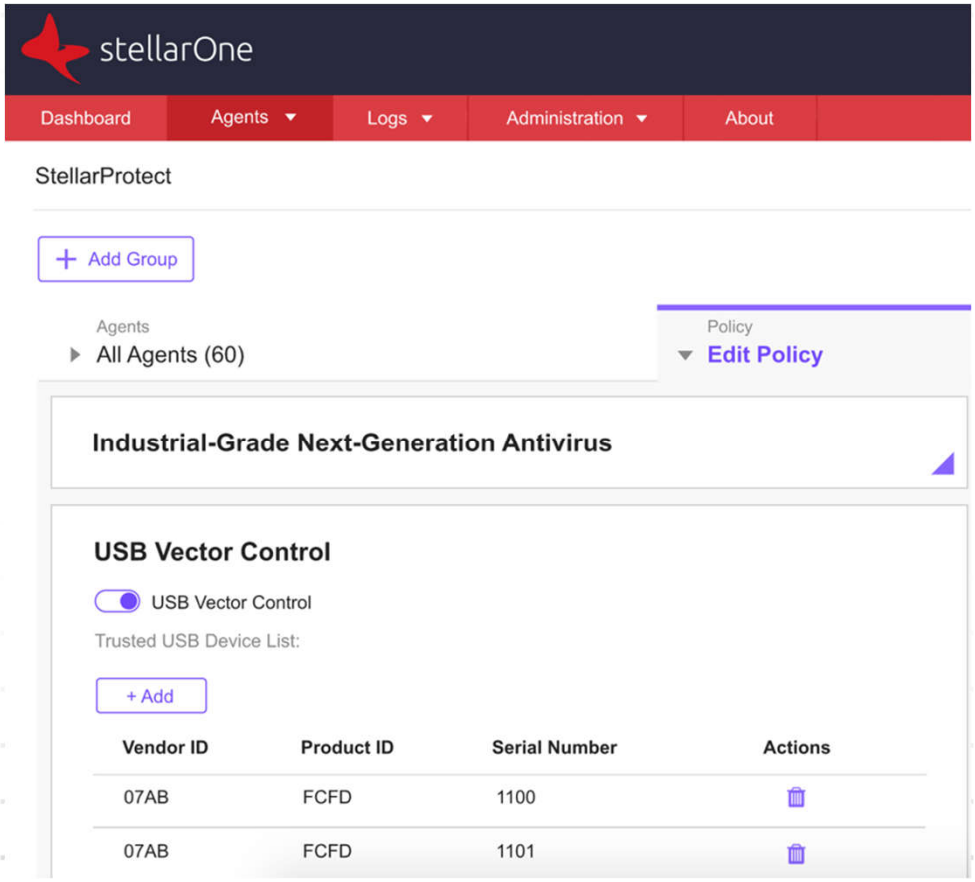
StellarOne – Wykrywanie anomalii

Nauka i akceptowanie logowania użytkowników

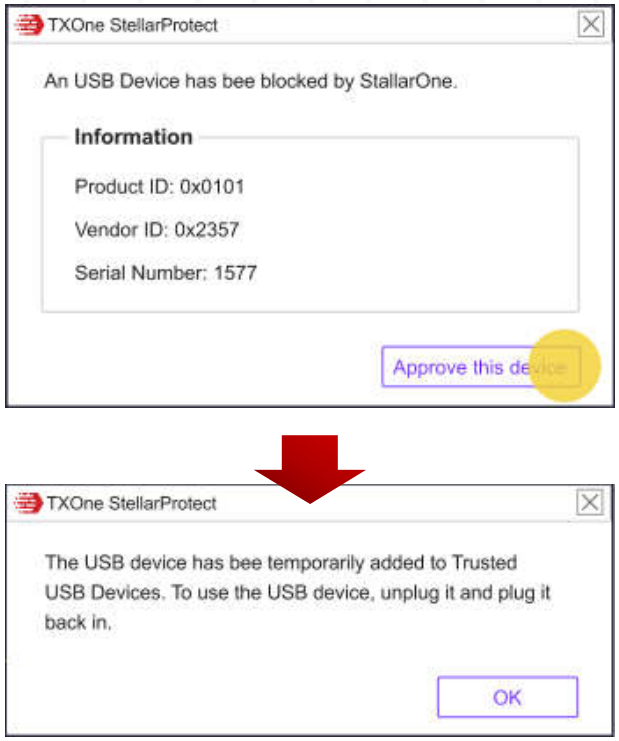


StellarOne – kontrola portów USB

Predefiniowane zaufane urządzenia USB

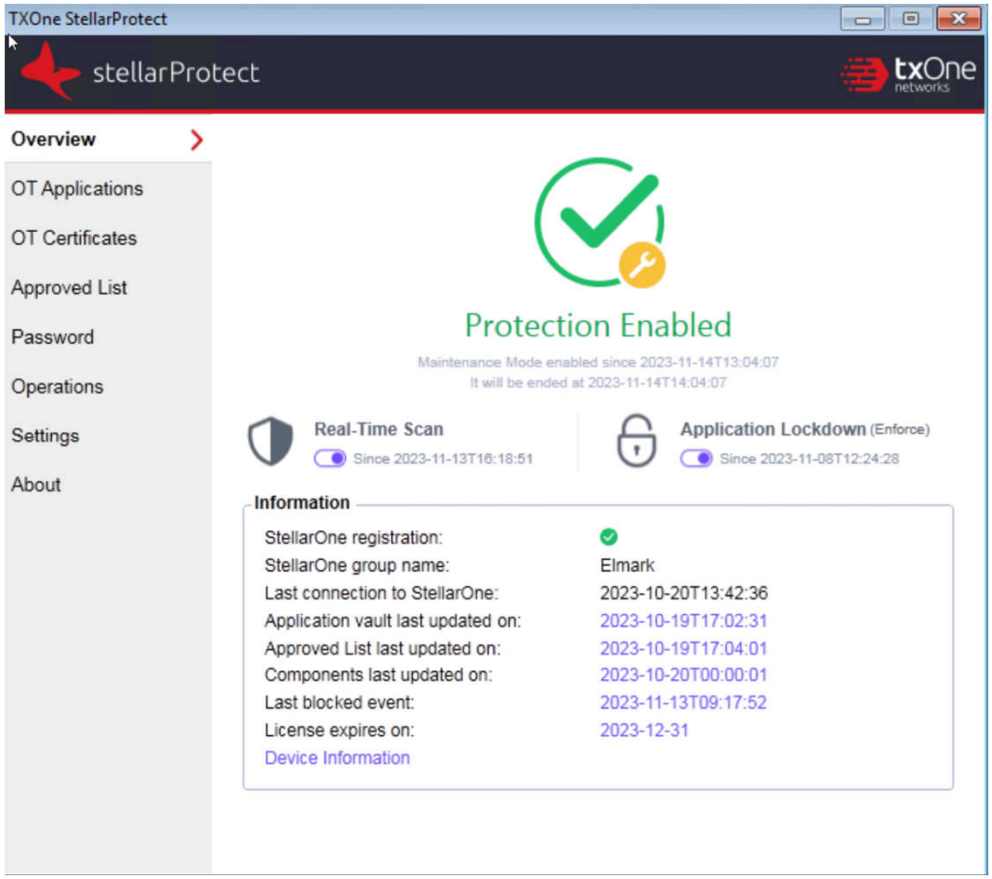


Pozwolenie na jednorazowe użycie



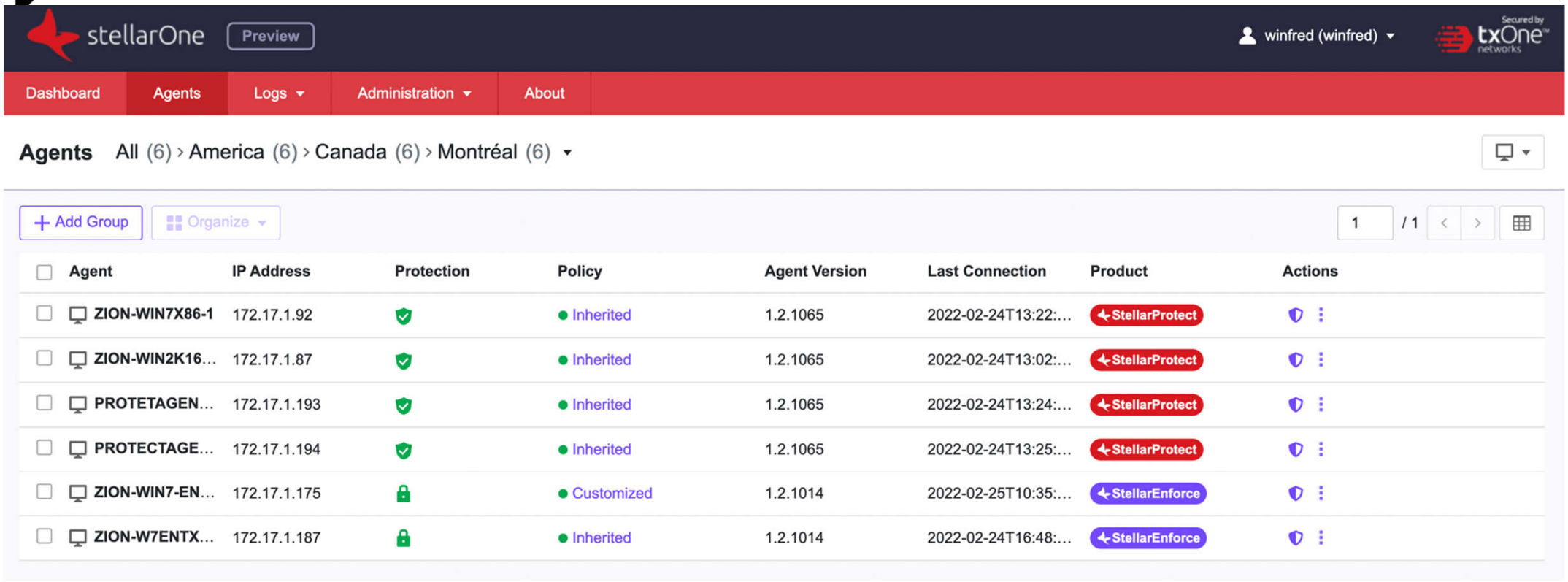
StellarOne – Tryb maintenance

Łatwe przejście w tryb serwisowy pozwalający na zmiany, dodanie aplikacji i procesów



StellarOne – centralne zarządzanie

ELMARK Automatyka

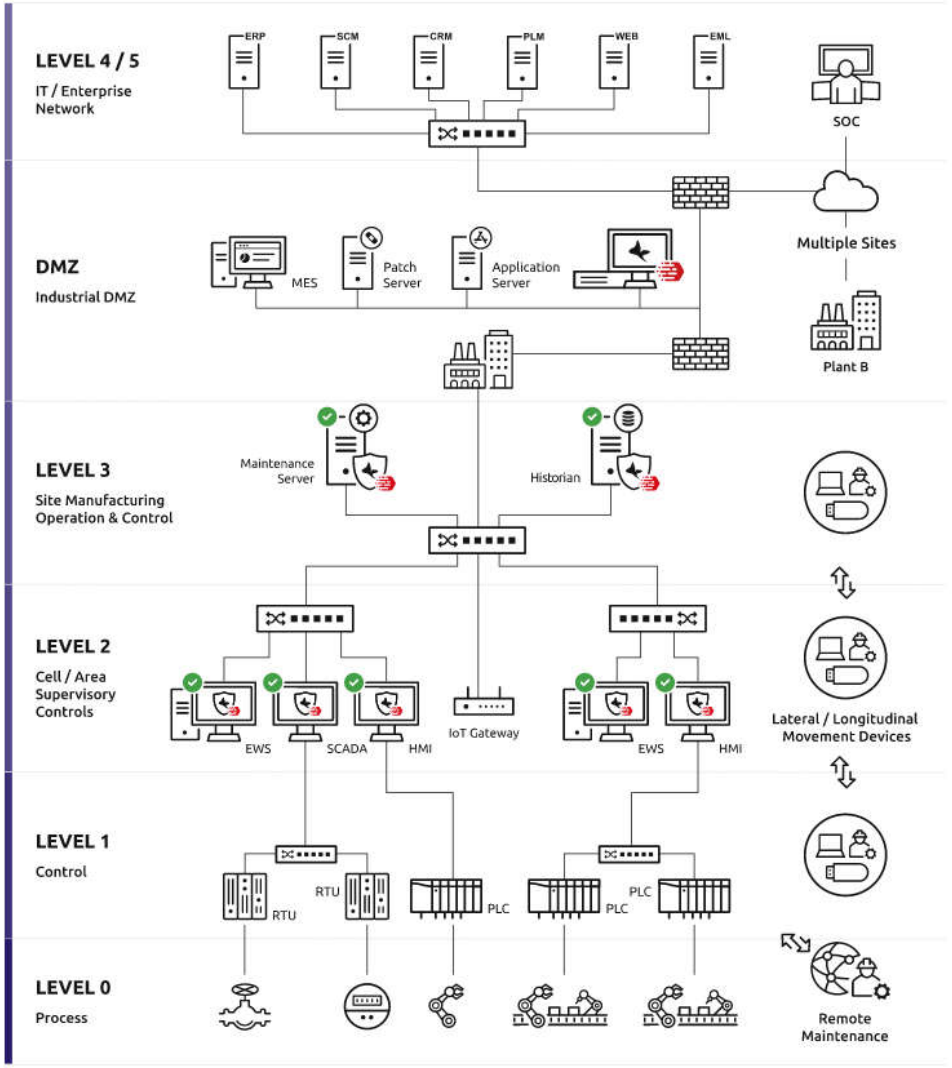


TXone Stellar vs standardowy antywirus

- Wsparcie dla starych systemów operacyjnych (Windows XP, Windows 7, Windows 2000)
- Bardzo lekki agent (niskie zapotrzebowanie na CPU i RAM)
- Długoletnie wsparcie
- Tryb serwisowy w którym działa ochrona antymalware
- Automatyczne rozpoznawanie aplikacji OT
- Możliwość nauczenia się zachowania użytkownika
- Wsparcie on-premise
- Łatwe masowe zarządzanie z podziałem na lokalizacje/grupy

Możliwości zastosowania

Ochrona wszelkiego typu maszyn i komputerów przemysłowych opartych o systemy Windows



TXOne Portable Inspector

txOne networks

Szybka weryfikacja assetów

PORTABLE SECURITY

Narzędzie do skanowania malware. Dla systemów odizolowanych.

- Nie trzeba niczego instalować
- Łatwa obsługa
- Widoczność zasobów (aplikacji OT) oraz centralne zarządzenie
- Możliwość kwarantanny lub usuwania zainfekowanego pliku
- Diody LED – wynik skanowania
- Windows oraz Linux
- Nie można go zainfekować – pliki są przechowywane na osobnych partycjach
- W wersji PRO bezpieczne przenoszenie plików (malware-free storage)

Portable Inspector – scenariusze wykorzystania

Inspekcja przyjęcia

- Skanowanie systemów odbieranych od dostawców pod kątem infekcji

Inspekcja wysyłki

- Skanowanie produktu przed wysyłką

Regularna kontrola

- Regularne skanowanie niezależnych systemów na obiektach
- Skanowanie maszyn gdzie instalowanie trzeciego oprogramowania nie jest możliwe (maszyny krytyczne, urządzenie objęte gwarancją)
- Skanowanie maszyn gdzie jedynie fizyczny i rejestrowany dostęp jest możliwy

Kontrola firm zewnętrznych

- Weryfikacja osób odwiedzających obiekt w celu prac serwisowych

Kompletne i unikatowe podejście do ochrony systemów OT

txOne networks

Deployment Model

Security Inspection

Installation-less malware scanning tool
Portable Inspector
Periodical health-check processes

Installation-less malware scanning tool with encryption
Portable Inspector Pro Edition
Periodical health-check processes with secure transporter

Management Console
ElementOne
Manage Portable Inspector and Portable Inspector Pro edition

Endpoint Protection

All-terrain digital safety for OT endpoints
Stellar
Recognize and preserve thousands of critical ICS and OT applications

Management Console
StellarOne
Manage Stellar

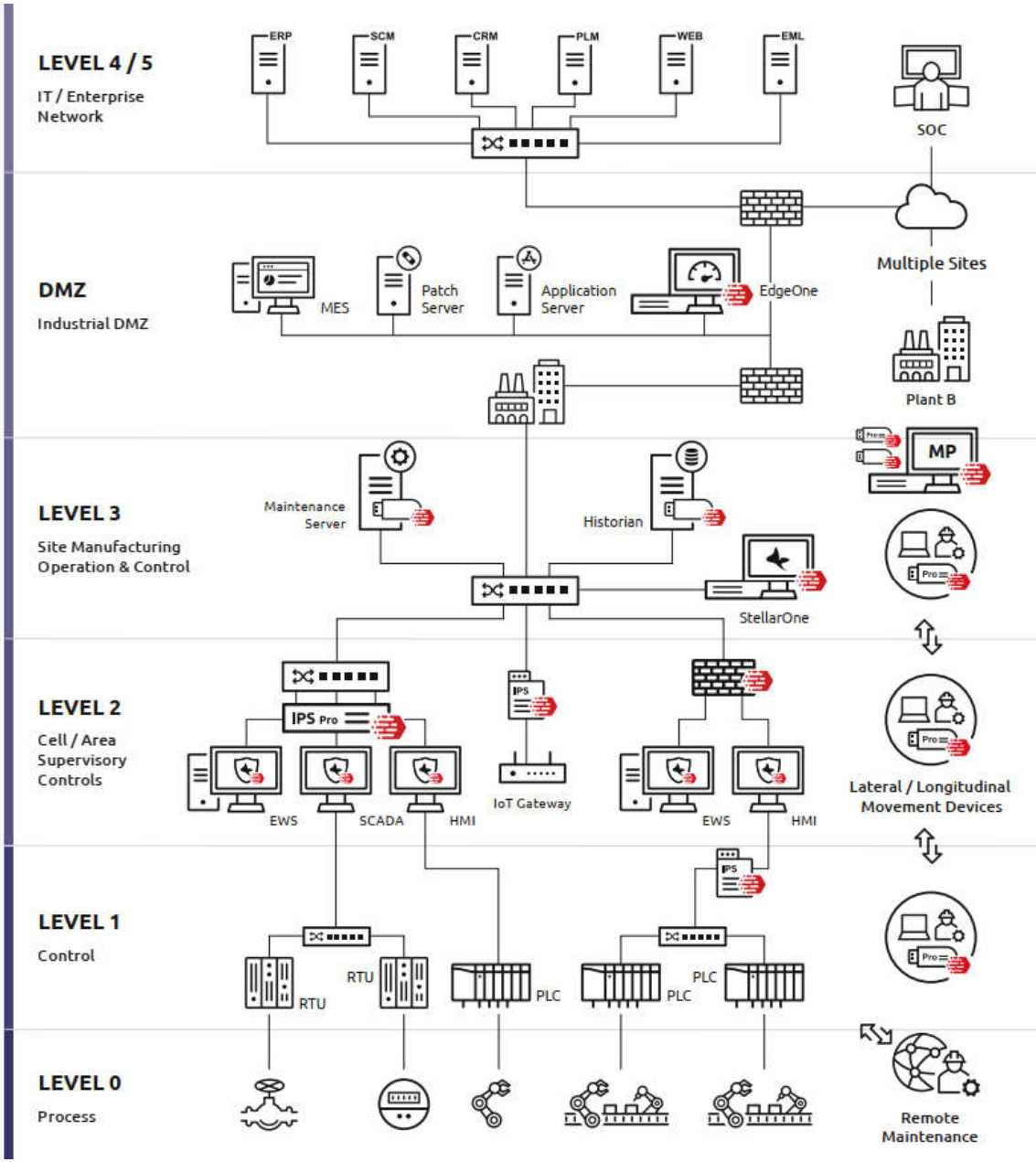
Network Defense

Industrial next-generation IPS
EdgeIPS
Micro segmentation for critical assets protection

Industrial next-generation firewall
EdgeFire
Enables secure network segmentation

Industrial next-generation IPS Array
EdgeIPS Pro (For large-scale networks)
Internal segmentation for critical assets protection

Industrial central management console
EdgeOne / OT Defense Console
Plant defense field management



Dziękujemy za uwagę

Sprawdź:

www.elmark.com.pl www.elmark-automation.com www.elmark.com.ro