ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

ARLITECH

BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

OT védelem. Az élet alapjainak biztonsága: ivóvíz, energia, gyógyszer, közlekedés, egészségügy, gyártás…

akos.jenei@arlitech.hu

WWW.ARLITECH.HU

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

JENEI ÁKOS

Ügyvezető
informatikus mérnök

Több, mint 25 éve az IT biztonságban.

akos.jenei@arlitech.hu

WWW.ARLITECH.HU

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

ARLITECH
CLICO txOne

akos.jenei@arlitech.hu

WWW.ARLITECH.HU

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

Referenciák

2007-2010

ÁNTSZ

Euroleasing

FÖMI

MÜPA

HMEI

OEP

Szegedi Vízmű

Észak-Budai Tervező,...

Kuka-Robotics

Zalakerámia

Future Films

2010-2020

ÁNTSZ

FÖMI

MTE

Univer

Credigen Bank

MÜPA

HMEI

MKEH

OBH

TriGránit

NIF

Korda Filmstúdió

Magyar Államkincstár

Szellemi Tulajdon NH

Gödöllői önkormányzat

2020-

MTE

MÜPA

Korda Filmstúdió

KnausTabbert

KÖBE

MBVK

Westend

MNV

MFB

ARKANCE

Asura Technologies

Ionart Studios

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

Gondolatébresztés

01

Okoépületek

Zárak, liftek, hűtés, fűtés, árnyékolás.

02

Energia, megújuló energia

Gázmotor-, naperőmű-, szélerőmű vezérlés, energiaelosztás.

02

Egészségügy

Műtők, laborszellőzés, diagnosztikai eszközök, laboratóriumi Információs rendszerek,röntgen, gyógyszeradagoló rendszerek,...

03

Gyógyszergyártás

Gyógyszercsomagoló, fertőtlenítő, gyártó gépek.

04

Vasút

Váltók, energia, sorompók,...

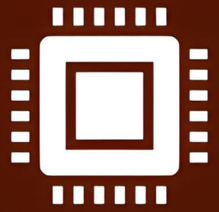
04

Vízmű

Szivattyúk, kutak, átemelők, szennyvíztisztítók.

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

IT (Information Technology) és az OT (Operational Technology) közötti különbségek

IT		*“Adatot mozgat”*
OT		*“Fizikai rendszereket mozgat”*

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

IT és az OT közötti különbségek

	Üzemidő	Frissítések	Biztonság	Tudatosság
IT	3-5 Év	Beütemezett és automatizált	Anti-malware, Tűzfalak, Backup-szerver	Rendben
OT	20-30 Év	Soha vagy ritkán	Ritkán	Kellően Rossz

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

OT biztonsági útmutató: NIST SP 800-82r3

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

- → FENYEGETÉSEK ÉS SÉRÜLÉKENYSÉGEK
- → RENDSZERTOPOLÓGIÁK
- → BIZTONSÁGI INTÉZKEDÉSEK

Kiberbiztonsági programfejlesztés
Kockázatkezelés
Kiberbiztonsági architektúra

Vezérlő
Épületautomatizálási
Közlekedési

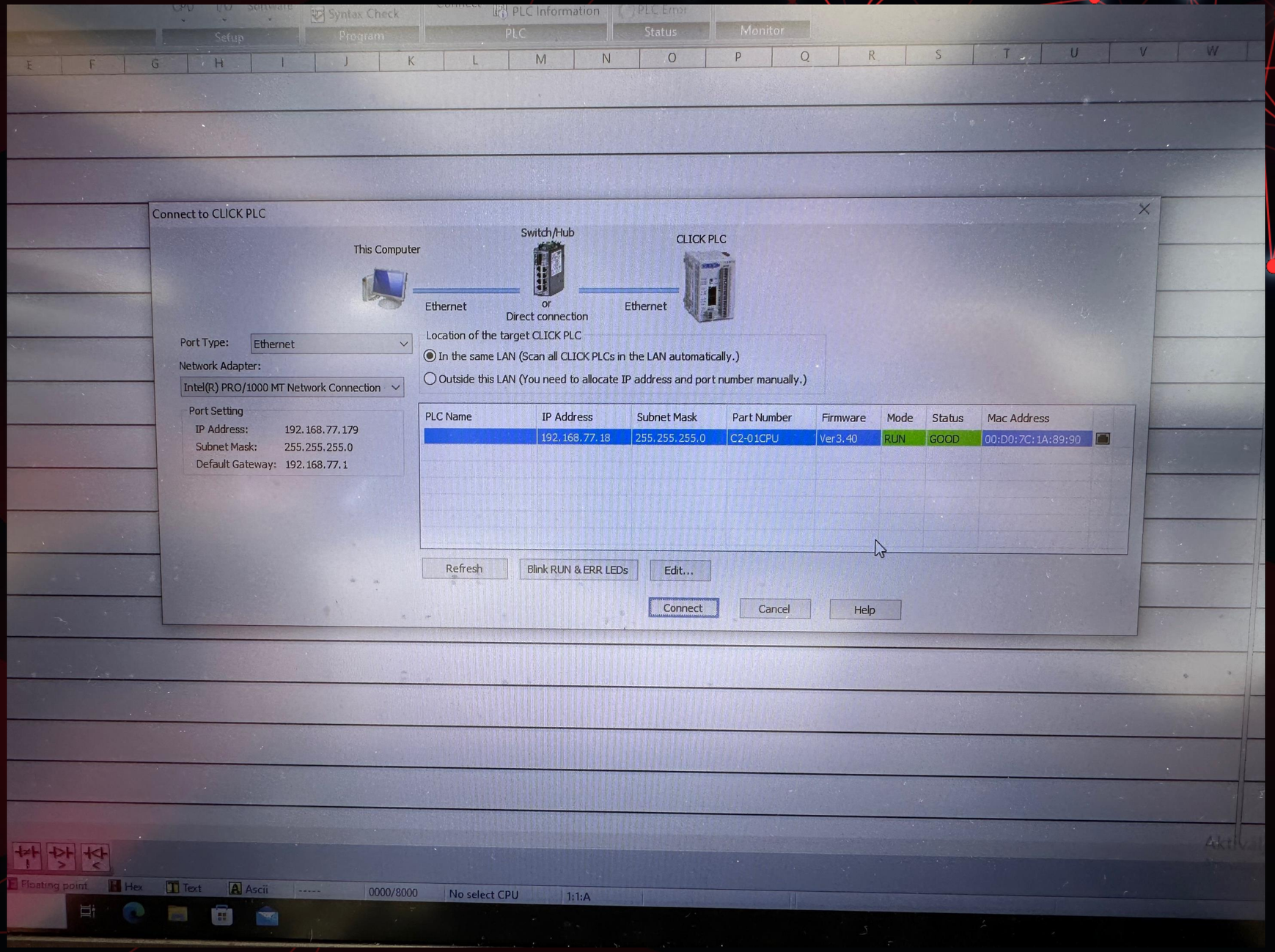
ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

MITRE ATT&CK® Matrix for ICS

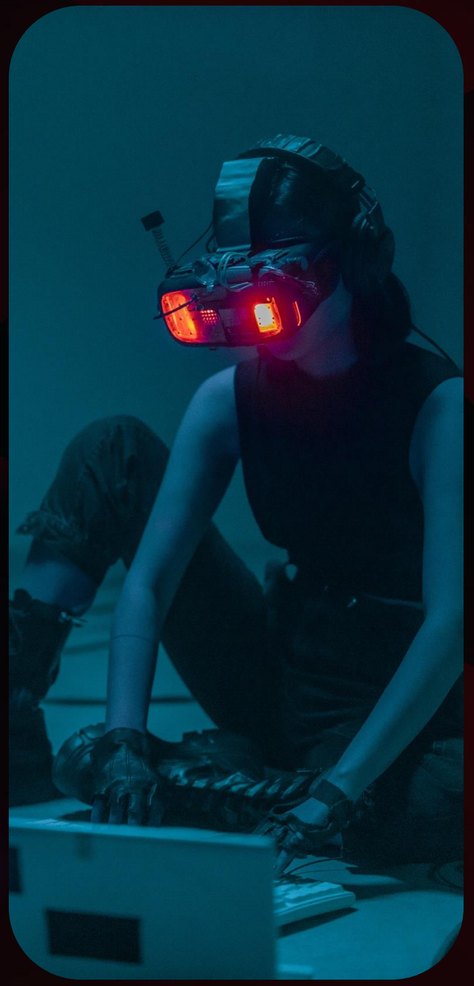
Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

MS

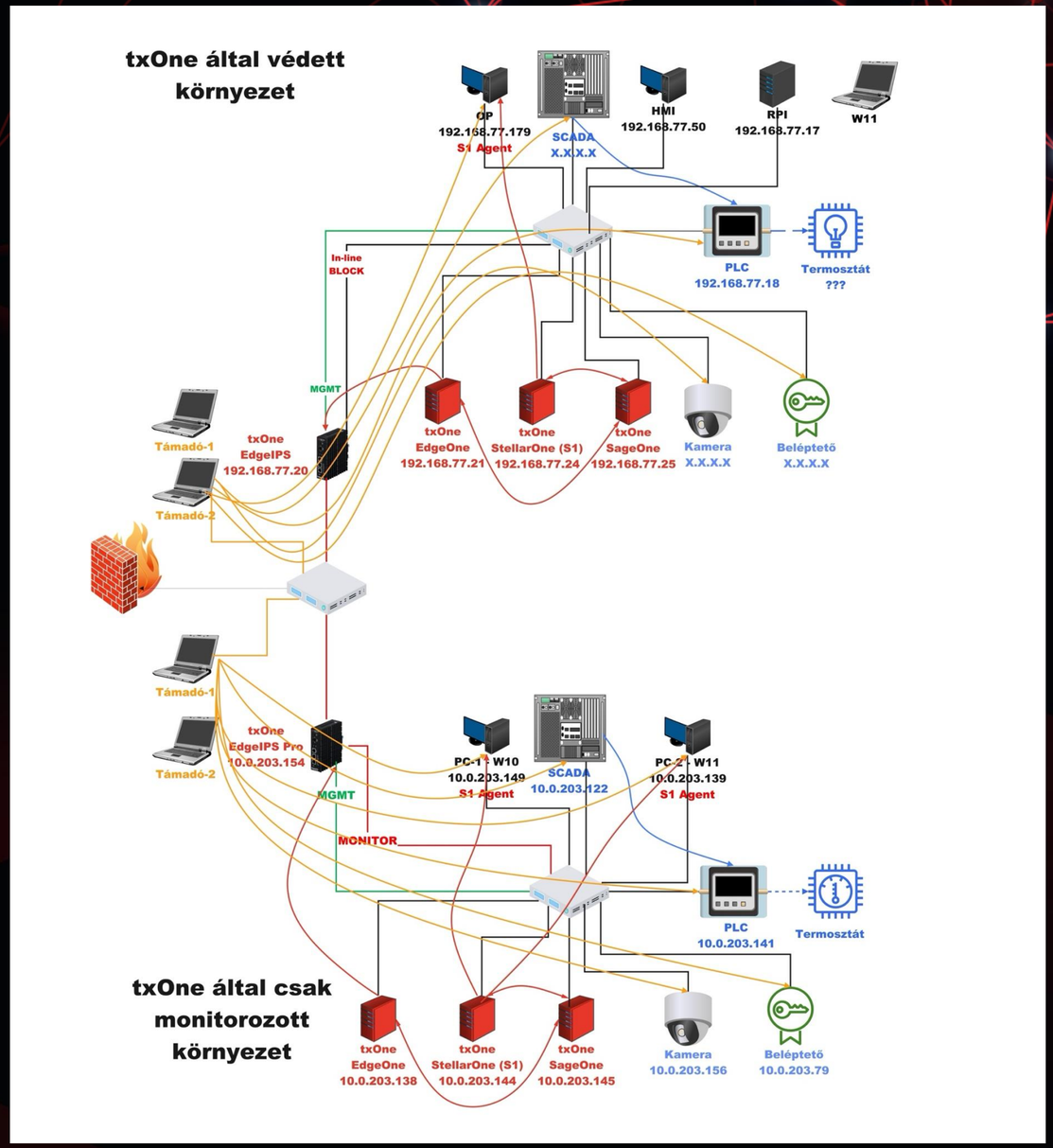


ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK



Workshop Topológia

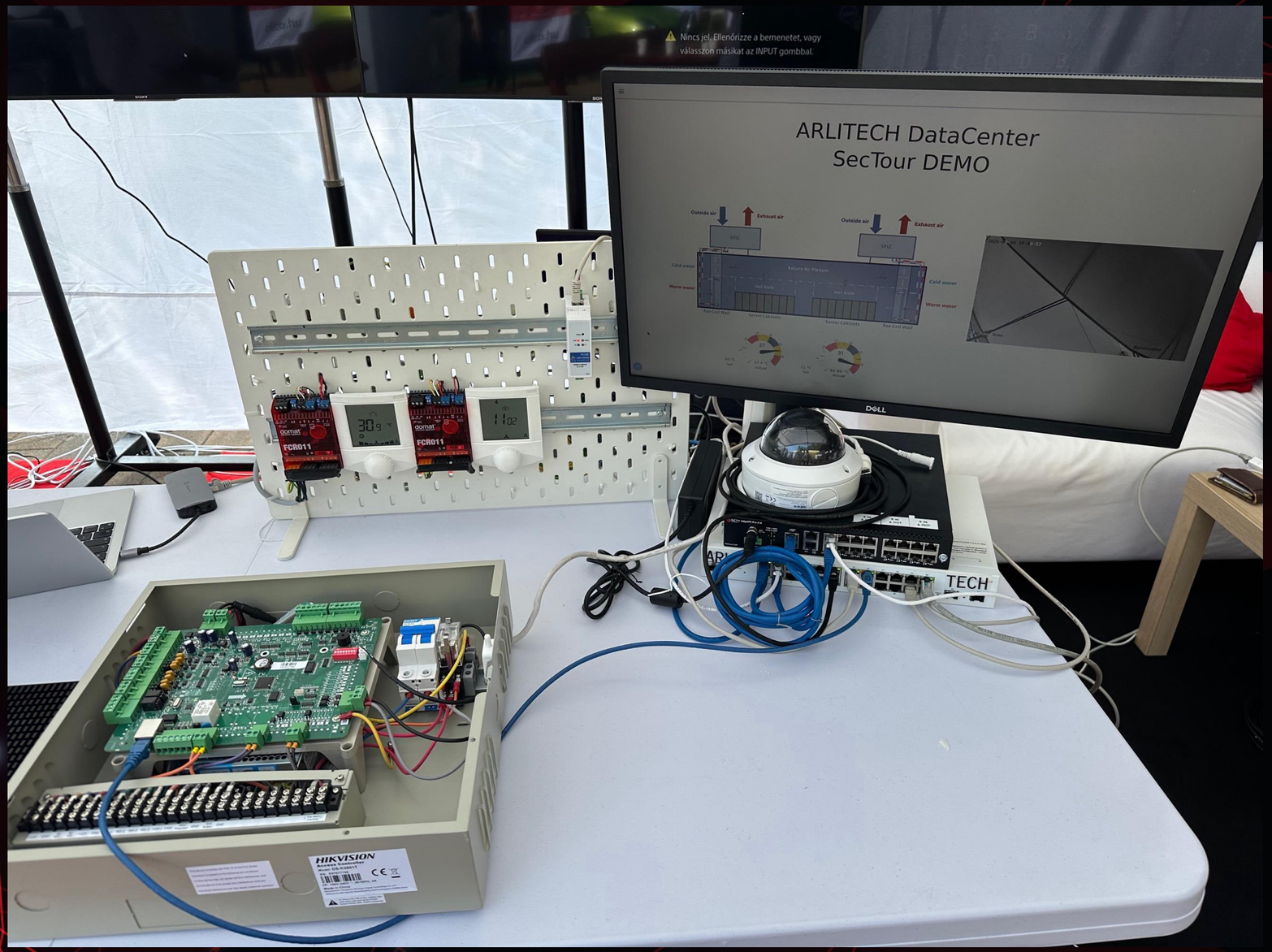
Minden kép valós adatokat tartalmaz a kiállított tesztrendszerből.



ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

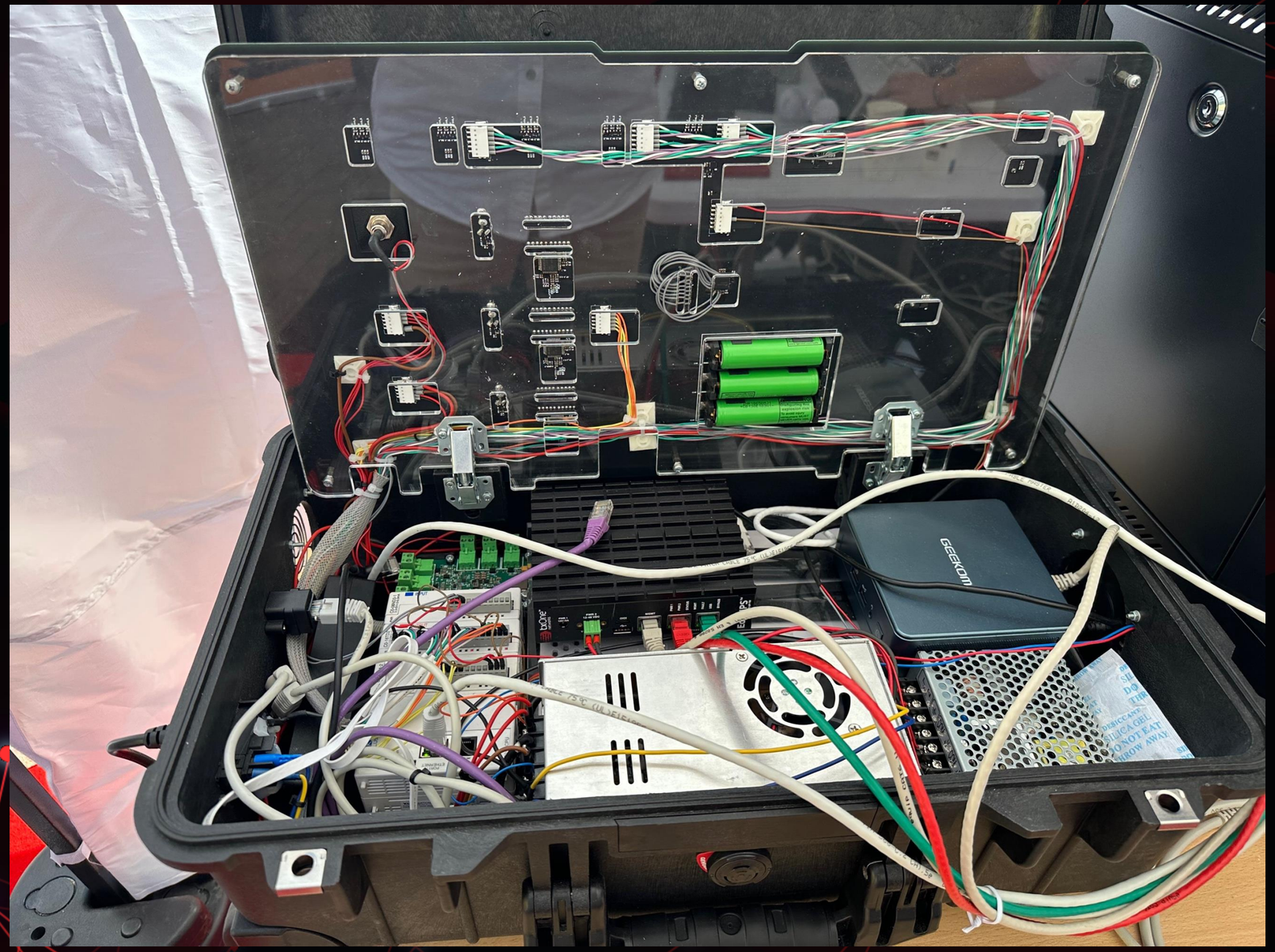
Workshop demo

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK



Védtelen hálózat

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK



Védett hálózat

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

Az OT kiberbiztonsági program 6 alapelve

1. Eszközcentrikus biztonság
2. Hálózati szegmentáció
3. Eszközleltár és passzív eszközfelderítés
4. Biztonságos távoli hozzáférés és MFA
5. Javítócsomagok és kompenzáló védelem nem frissíthető rendszerekhez
6. Folyamatos monitorozás és anomáliaészlelés

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

Az OT kiberbiztonsági program 6 alapelve

1. Eszközcentrikus biztonság

Az eszközök hatékony védelme azok teljes életciklusán keresztül.

Rendszerbe való:
- **beléptetés (malware ellenőrzés, hitelesítés)**
- **beállítás**
- **karbantartás.**

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

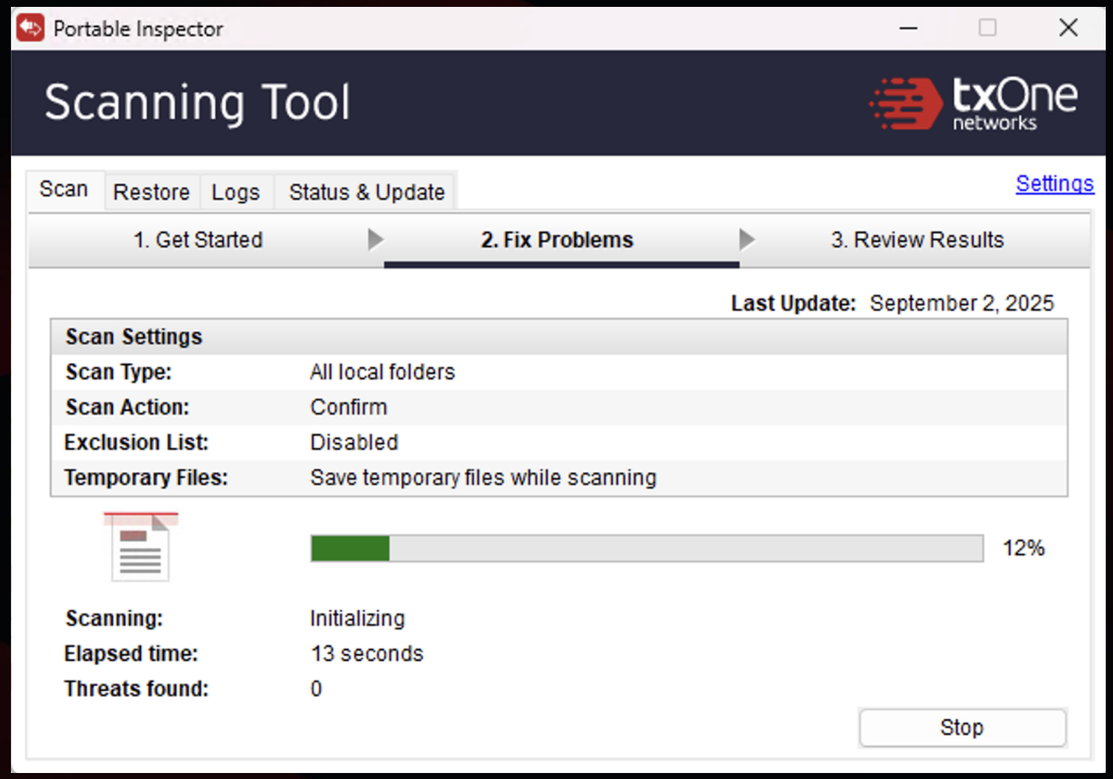
txOne Portable Inspector

Portable Inspector

- A rendszer védelme a beérkező és kimenő eszközök ellenőrzésével
- Belső fenyegetések kiküszöbölése
- Nem igényel telepítést
- Szabályozási megfelelés egyszerűsítése
- USB-kialakítás
- Malware fertőzés visszajelzése háromszínű LED segítségével
- Eszközadatok gyűjtése az OT-rendszerek átláthatóságának növeléséhez

Portable Inspector Pro

- Minden ami az alapverzióban van + fájlok biztonságos átvitele



ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

Az OT kiberbiztonsági program 6 alapelve

2. Hálózati szegmentáció

Az OT hálózatokat zónákra és biztonságos kommunikációs csatornákra kell bontani:

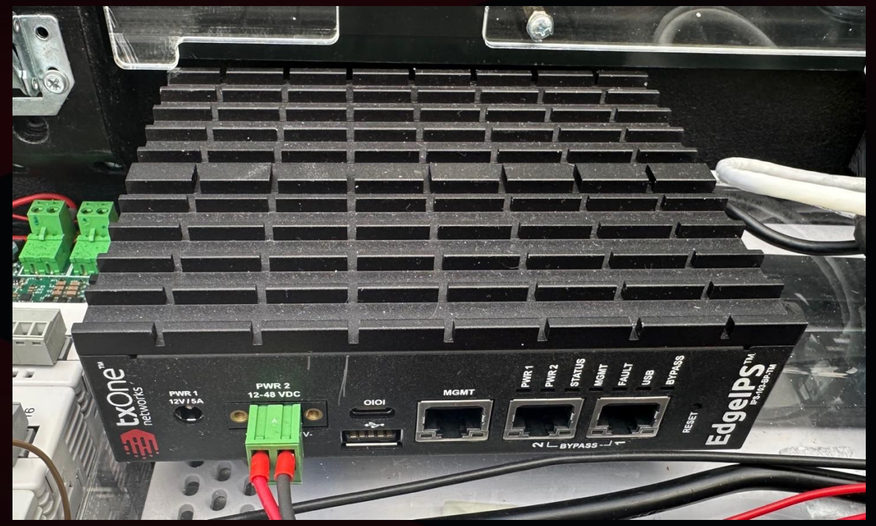
- IT
- termelés
- vezérlés
- ...

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

EdgeIPS

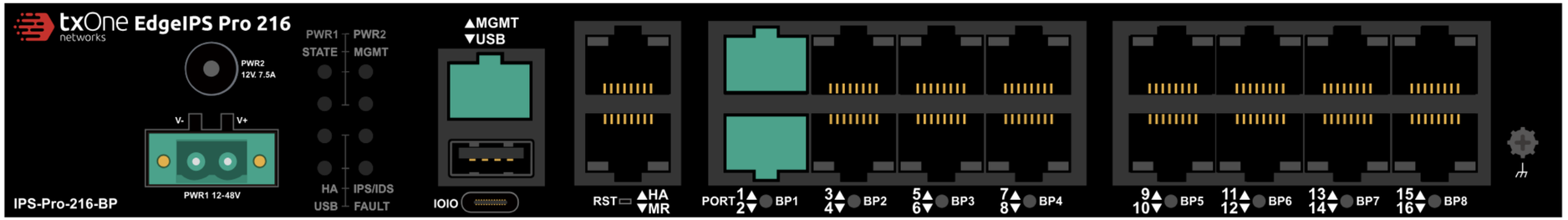
EdgeFire

Célhardverek, nem aktíveszközökön, tűzfalakon bekapcsolható funkció.



ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

EdgeIPS szegmentáció



Total Number of Items: 16 | Search | 1 / 1

All Pairs | All Pair Modes

Port	Pair	Pair Mode	Security Operation Mode	Hardware Bypass Mode	Policy Enforcement	Policy Enforcement Operation Mode
PORT1	PAIR1	Default	Inline Mode	Fail Open	Device: all_monitor	Monitor Mode
PORT2	PAIR1	Default	Inline Mode	Fail Open	Device: all_monitor	Monitor Mode

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

Az OT kiberbiztonsági program 6 alapelve

3. **Eszközleltár és passzív eszközfelderítés**

PLC-k, HMI-k, eszközök,.. azonosítása.

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

txOne Portable Inspector

Portable Inspector

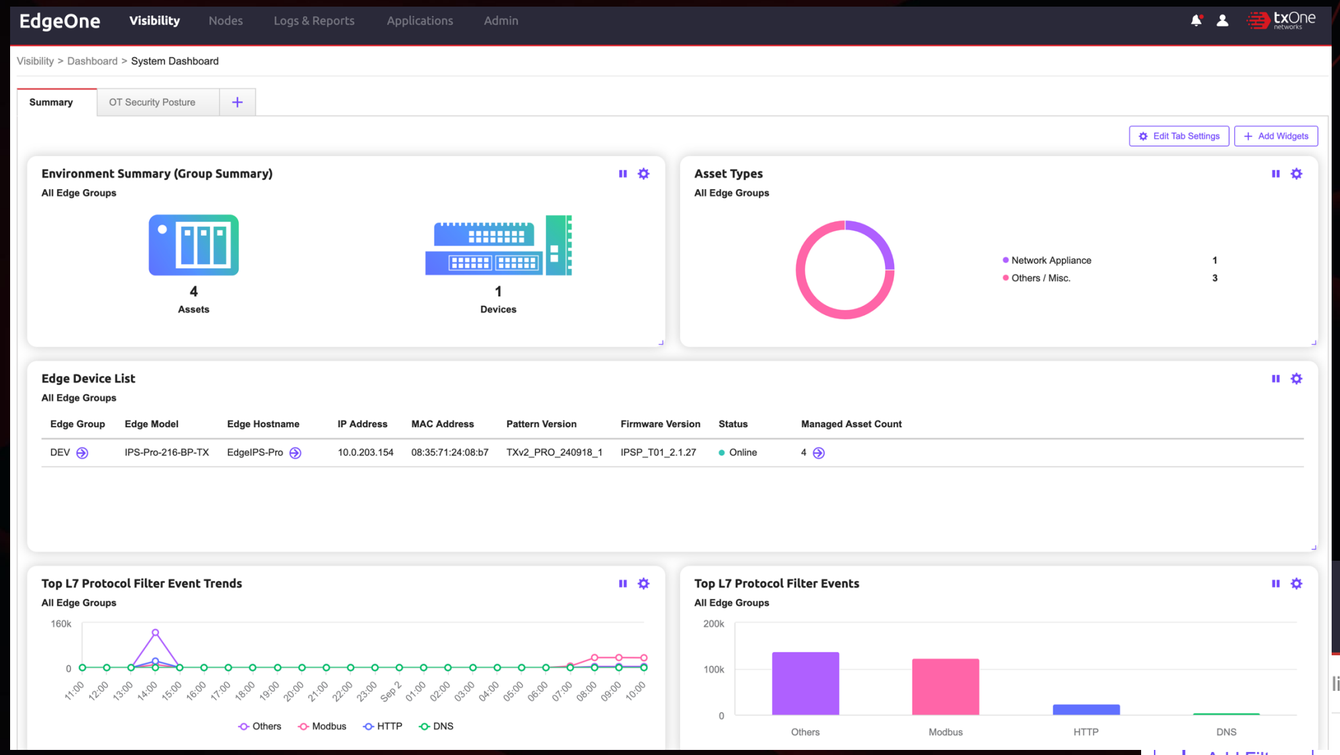
- A rendszer védelme a beérkező és kimenő eszközök ellenőrzésével
- Belső fenyegetések kiküszöbölése
- Nem igényel telepítést
- Szabályozási megfelelés egyszerűsítése
- USB-kialakítás
- Malware fertőzés visszajelzése háromszínű LED segítségével
- Eszközadatok gyűjtése az OT-rendszerek átláthatóságának növeléséhez

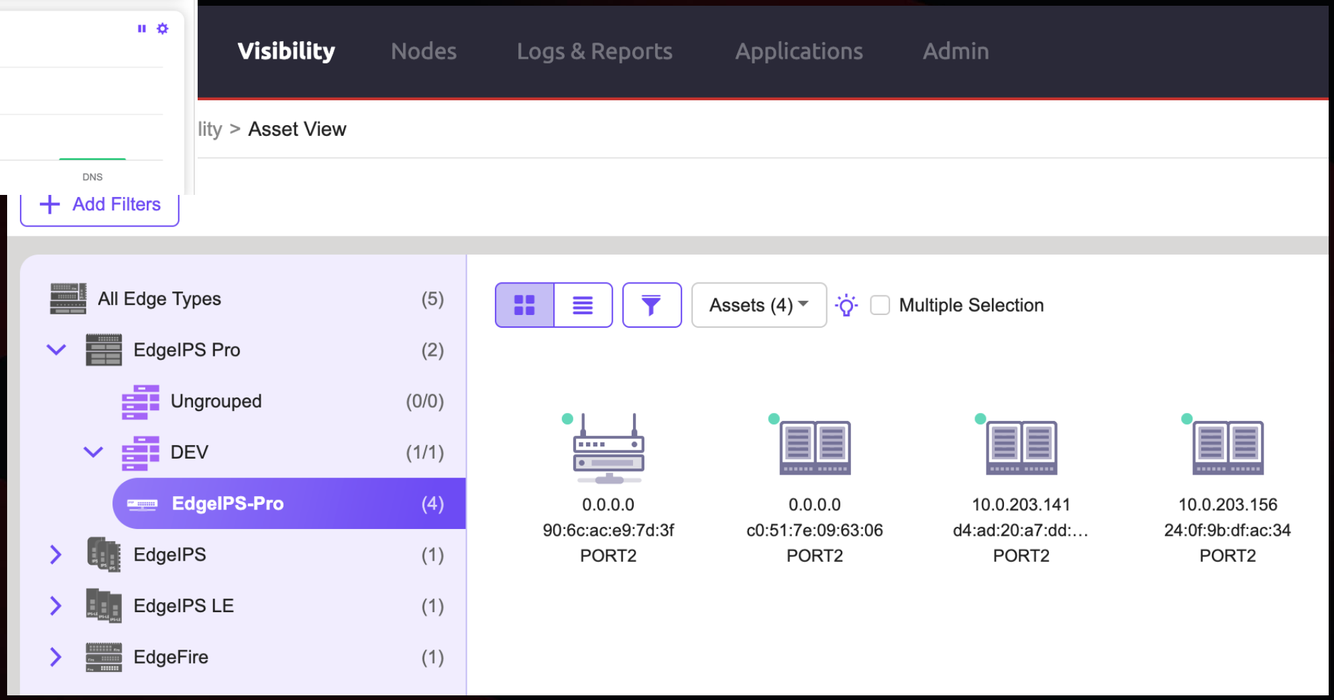
Portable Inspector Pro

- Minden ami az alapverzióban van + fájlok biztonságos átvitele

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

txOne EdgeOne





ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

Az OT kiberbiztonsági program 6 alapelve

4. **Biztonságos távoli hozzáférés: VPN és MFA**

Biztonságos távoli hozzáférés.

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

EdgeFire

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

Az OT kiberbiztonsági program 6 alapelve

5. Javítócsomagok és kompenzáló védelem nem frissíthető rendszerekhez

IPS, virtual patching:

frissítés, leállás elkerülése.

ARLITECH

BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

✓	1048640	Buffer Overflow	High	Deny and Log	WEB Microsoft PCT Buffer Overflow -1 (CVE-2003-0719)
✓	1049406	Exploits	High	Deny and Log	WEB /etc/motd File Download
✓	1049407	Reconnaissance	High	Deny and Log	WEB Linux /etc/shadow File Download
✓	1049409	Exploits	High	Deny and Log	WEB .htgroup access
✓	1049556	Exploits	Medium	Allow and Log	WEB Microsoft IIS 5.1 Frontpage fpsrvadm.exe File Download
✓	1049576	Exploits	High	Deny and Log	WEB Microsoft IIS 5.1 Frontpage Extensions Path Disclosure Information Vulnerability -2 (CVE-2002-1717)
✓	1049578	Exploits	High	Deny and Log	WEB Microsoft IIS 5.1 Frontpage Extensions Path Disclosure Information Vulnerability -3 (CVE-2002-1717)
✓	1049579	Reconnaissance	High	Deny and Log	FRONTPAGE fourdots request (CVE-2000-0153)
✓	1049659	Exploits	Critical	Deny and Log	WEB Cisco IOS HTTP Configuration Arbitrary Administrative Access (CVE-2001-0537)
✓	1049682	Exploits	High	Deny and Log	WEB .htpasswd file download (CVE-2001-0892)
✓	1049736	Exploits	High	Deny and Log	WEB .htaccess file download (CVE-2000-0234)
✓	1049802	Web threats	Critical	Deny and Log	WEB Directory Traversal -2.u
✓	1049842	Web threats	High	Deny and Log	WEB OVActionD SNMPNotify Command Execution (CVE-2001-0552)
✓	1049859	Buffer Overflow	High	Deny and Log	WEB Oracle 9I Application Server PL/SQL Apache Module Buffer Overflow Vulnerability (CVE-2001-1216)
✓	1049945	Buffer Overflow	Critical	Deny and Log	WEB Microsoft IIS Chunked Encoding Transfer Heap Overflow Vulnerability
✓	1050002	Exploits	Critical	Deny and Log	WEB /etc/inetd.conf Access
✓	1050080	Buffer Overflow	High	Deny and Log	DNS ISC Bind 8 Transaction Signatures Buffer Overflow -1 (CVE-2001-0010)
✓	1050081	Buffer Overflow	High	Deny and Log	DNS ISC Bind 8 Transaction Signatures Buffer Overflow -2 (CVE-2001-0010)
✓	1050082	Buffer Overflow	High	Deny and Log	DNS ISC Bind 8 Transaction Signatures Buffer Overflow -3 (CVE-2001-0010)
✓	1050132	Reconnaissance	High	Deny and Log	EXPLOIT Multiple Vendor XDMCP Default Access Control Vulnerability (CVE-2000-0374)
✓	1050153	Buffer Overflow	Critical	Deny and Log	WEB Microsoft IIS 5.0 .printer ISAPI Extension Buffer Overflow -2 (CVE-2001-0241)
✓	1050340	Reconnaissance	High	Deny and Log	WEB Whisker/Nikto web scanner attempt
✓	1050358	Buffer Overflow	High	Deny and Log	RPC Microsoft Windows DCOM RPC Interface Buffer Overflow (CVE-2003-0352)
✓	1050420	Buffer Overflow	High	Deny and Log	RPC Microsoft Windows DCOM RPC Interface Buffer Overflow -1 (CVE-2003-0352)

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

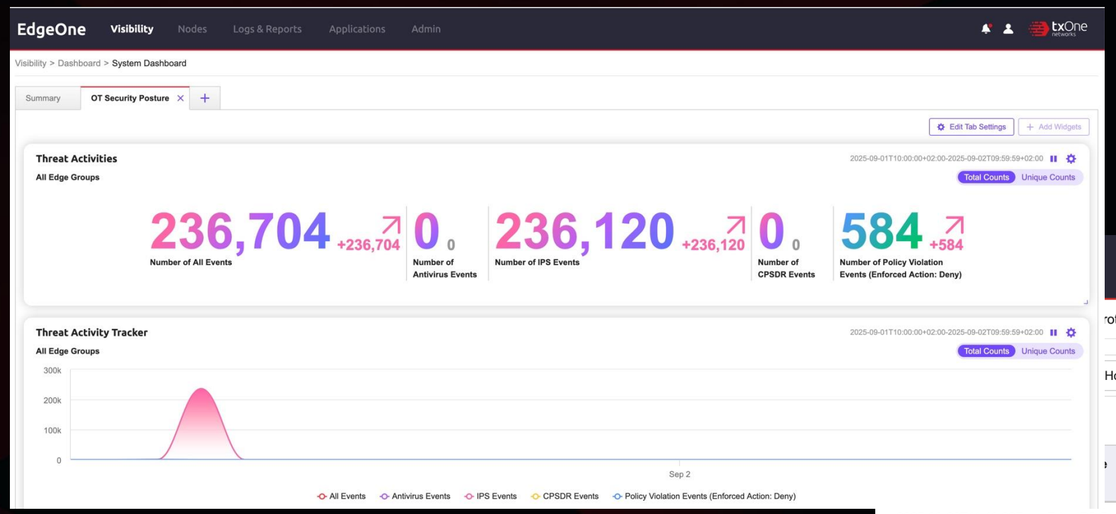
Az OT kiberbiztonsági program 6 alapelve

6. **Folyamatos monitorozás és anomáliaészlelés**

Az OT rendszerek valós idejű megfigyelése.

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

txOne EdgeOne



Nodes | **Logs & Reports** | Applications | Admin

rotocol Filter Logs

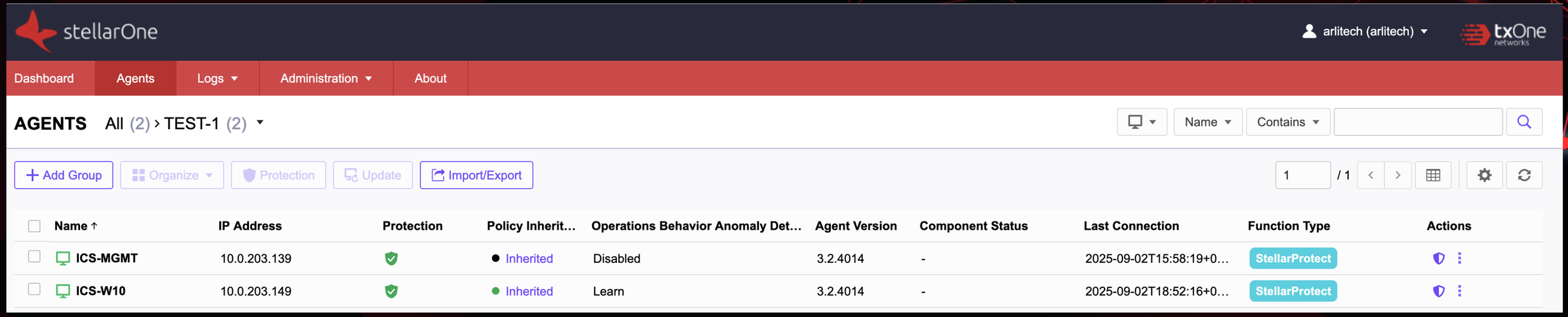
Hour | + Add Filters | Search

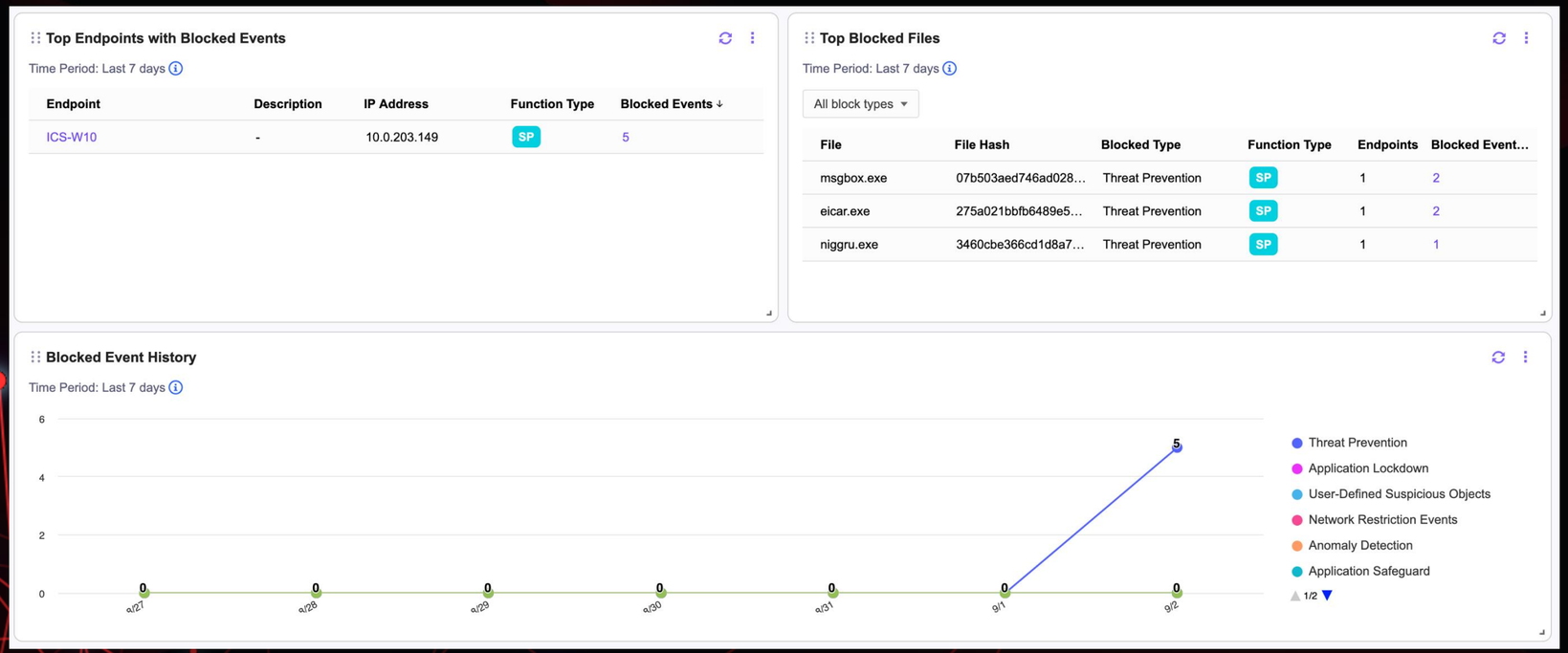
Total Number of Items: 5000 | 1 / 50

	Serial Number	Protocol Layer	Policy Rule Name	Profile Name	Interface	Source MAC Address	Source IP Address	L7 Protocol Name	Extra Information
2025-09-02T11:43:36Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 2, FunctionCode: 0x03, Address: 20~20
2025-09-02T11:43:35Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 2, FunctionCode: 0x03, Address: 20~20
2025-09-02T11:43:35Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 1, FunctionCode: 0x03, Address: 9~27
2025-09-02T11:43:35Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 2, FunctionCode: 0x03, Address: 20~20
2025-09-02T11:43:35Z	EdgeIPS-Pro	TXP06230000012	Layer2	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	90:6c:ac:da:db:85	-	Others	-
2025-09-02T11:43:35Z	EdgeIPS-Pro	TXP06230000012	Layer2	Device:all_monitor:all_monitor	Device:all_monitor	PORT2	90:6c:ac:e9:7d:3f	-	Others	-
2025-09-02T11:43:34Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 2, FunctionCode: 0x03, Address: 20~20
2025-09-02T11:43:34Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 1, FunctionCode: 0x03, Address: 9~27
2025-09-02T11:43:34Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 2, FunctionCode: 0x03, Address: 20~20
2025-09-02T11:43:33Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 1, FunctionCode: 0x03, Address: 9~27
2025-09-02T11:43:33Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 2, FunctionCode: 0x03, Address: 20~20
2025-09-02T11:43:32Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 1, FunctionCode: 0x03, Address: 9~27
2025-09-02T11:43:32Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 2, FunctionCode: 0x03, Address: 20~20
2025-09-02T11:43:32Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 1, FunctionCode: 0x03, Address: 9~27
2025-09-02T11:43:32Z	EdgeIPS-Pro	TXP06230000012	Layer2	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	90:6c:ac:da:db:85	-	Others	-
2025-09-02T11:43:32Z	EdgeIPS-Pro	TXP06230000012	Layer2	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	90:6c:ac:da:db:85	-	Others	-
2025-09-02T11:43:31Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 1, FunctionCode: 0x03, Address: 9~27
2025-09-02T11:43:31Z	EdgeIPS-Pro	TXP06230000012	Layer3	Device:all_monitor:all_monitor	Device:all_monitor	PORT1	00:0c:29:1d:cc:96	10.0.203.122	Modbus	UnitID: 2, FunctionCode: 0x03, Address: 20~20

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

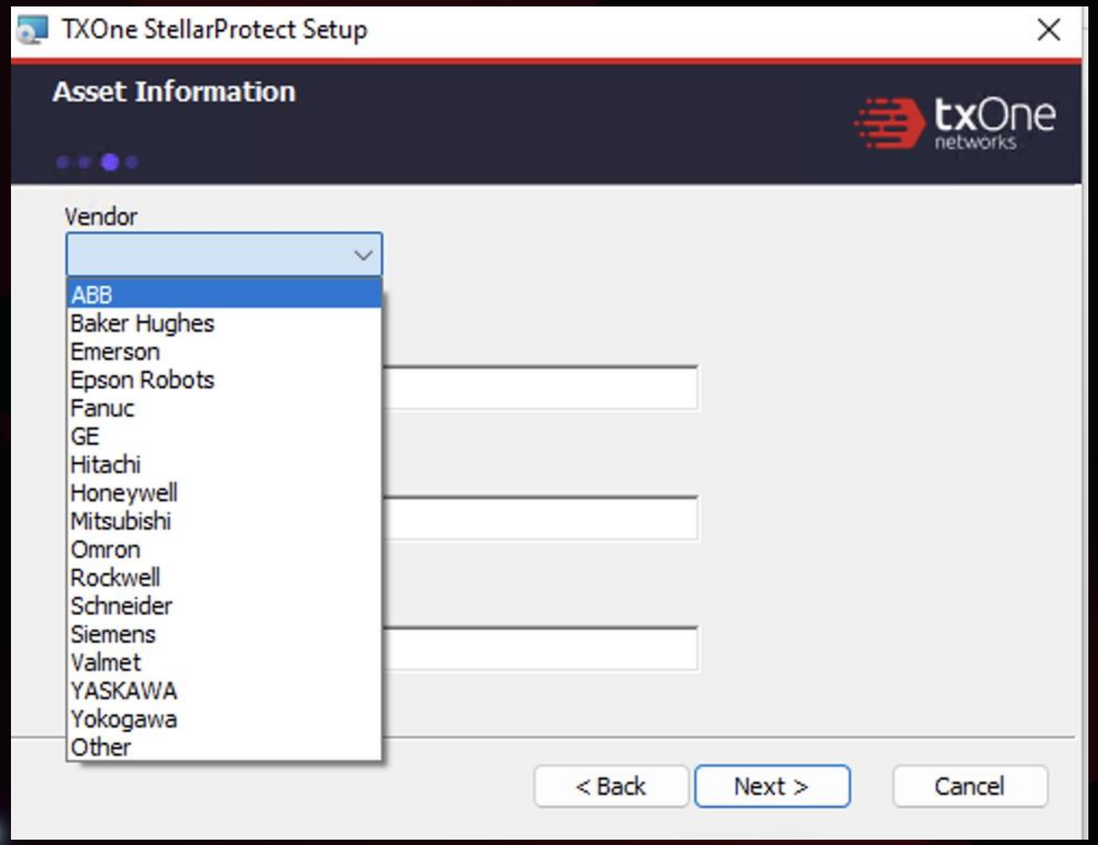
txOne stellarOne





ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

txOne stellarOne



Top Blocked Files

Time Period: Last 7 days

All block types

File	File Hash	Blocked Type	Function Type	Endpoints	Blocked Event…
msgbox.exe	07b503aed746ad028…	Threat Prevention	SP	1	3
eicar.exe	275a021bbfb6489e5…	Threat Prevention	SP	1	2
svájgerárpi.exe	07b503aed746ad028…	Threat Prevention	SP	1	1
sectour.exe	07b503aed746ad028…	Threat Prevention	SP	1	1

ARLITECH
BIZTONSÁGOSABB VILÁGOT ÉPÍTÜNK

Köszönöm a figyelmet, várunk mindenkit a workshopon.

Web: www.arlitech.hu
Email: info@arlitech.hu
Facebook: https://www.facebook.com/arlitech.official
X: https://x.com/arlitech
Linkedin: https://hu.linkedin.com/company/arlitech
WhatsApp: https://whatsapp.com/channel/0029VaQKLxI0AgW9CfNXof2c
Instagram: arlitech.official

akos.jenei@arlitech.hu
www.arlitech.hu
+36 30 3119042