SCADAfence

How SCADAfence Detects Triton

Based on the MITRE ATT&CK Framework

What you can learn about the Triton Attack
and how SCADAfence helps prevent attacks
on industrial control systems (ICS)

SUMMARY OF THE TRITON ATTACK

The Triton malware attack was far from the first time that cyber attackers have attempted to target the networks of an industrial facility, but it was the first time that malware designed to attack safety systems was ever seen in the wild. Only a year after the attack, it was reported in 2018 that the malware most likely came from the Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM), a research entity in Russia.

The malware was designed to manipulate Schneider Electric's Triconex Safety Instrumented System (SIS) controllers – emergency shutdown systems – and was uncovered on the network at a critical infrastructure operator in the Middle East.

The malware campaign was extremely stealthy and was only uncovered because the attackers made a mistake and triggered the safety system, shutting down the plant. The outcome could've been much worse. Following the initial point of compromise, the malware was able to use techniques such as harvesting credentials and moved across the network to reach the SIS controllers.

However, Triton was only able to reach its goal because of some lax attitudes to security throughout the facility: the safety controllers were using improper network segmentation and the network was connected to internet-facing operational systems, allowing attackers to gain access using compromised valid credentials. Other failures -- like a key being left inside a machine -- provided attackers with access they should never have gained without physically being inside the facility.

While the malware has the potential to be highly damaging to valves, switches and sensors in an industrial environment, the threat can be countered by implementing some relatively simple cybersecurity techniques that make movement between systems almost impossible.

Triton targeted critical infrastructure in the Middle East, but there are lessons from the incident that can be applied to organizations in every sector, no matter where they are in the world.

THE MITRE ENGENUITY EVALUATION FOR ICS THREAT DETECTION

There is a lot of buzz recently on the topic of MITRE ATT&CK for ICS and rightfully so. The Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) project by MITRE is an initiative started in 2015 with the goal of providing a “globally-accessible knowledge base of adversary tactics and techniques based on real-world observations." The knowledge base helps security professionals make sense of the numerous varieties of tactics and techniques attackers use to infiltrate networks, steal data and other methods of exploiting organizations.

The MITRE ATT&CK framework enables security professionals to move beyond identifying the simplest and most common attack methods and instead allocate resources to get a better understanding of adversaries’ behaviors.

MITRE Engenuity ran its first evaluation of the ICS threat detection market. One of the challenges we face in ICS cybersecurity is the lack of detection and collection capability within most ICS environments. MITRE Engenuity ATT&CK Evaluations are intended to help vendors and end-users better understand a product’s capabilities in relation to MITRE’s publicly accessible ATT&CK for the ICS framework. As a true community-led effort, more than 100 participants from 39 organizations reviewed, provided comments, or contributed to the ATT&CK for ICS framework which was first launched in early 2020.

For the ATT&CK Evals, MITRE Engenuity used the MITRE ATT&CK for ICS knowledge base to emulate the tactics, techniques, and procedures (TTPs) associated with the TRISIS/TRITON malware.

HOW THE TRITON ATTACK OCCURRED

The attacker moved from the IT network to the OT network through systems that were accessible to both environments and gained remote access to an SIS engineering workstation and deployed the Triton attack framework to reprogram the SIS controllers.

Initial Compromise

- Utilized captured valid credentials to log into windows-based engineering workstation within the process environment - Remote Desktop (RDP) over port 3389 (T0885)

Persistence

- Outgoing SSH request was made over port 445 to the application to disguise as SMB traffic (T0885)
- Open SSH backdoor was masqueraded as a proprietary Rockwell protocol, listening on port 2223 and a service name of rockwell-csp3 (T0849).

Collection/Discovery

- Uses custom network and EtherNet/IP tools to conduct a stealth scan across the network on TCP port 44818 to identify any EtherNet/IP capable assets (T0846).
  - [to discover Rockwell devices]
- The script conducts a Rockwell broadcast discovery (T0888), gathers the device type (T0888), PLC operating mode (T0868), and a dump of all tag names (T0871).
- Triton is capable of auto detecting Triconex controllers by sending a specific UDP broadcast packet over port 1502 (T0888).
- The attacker leverages the Rockwell engineering tools to initiate a Program Upload (gets the PLC logic from Rockwel PLC) (T0871) and saves this file into their temp Rockwell directory.

Impair Process Control

- Sent ENIP command: to change the operating mode (T0858) of the safety PLC to Program Mode to allow for a full program download (T0843).
- Modifies the safety controller program (T0889) over EtherNet/IP using the custom python script through an online edit or program append action (T0843).
- Monitors their command-and-control tags before actuating the malicious logic (T0855):
  - TriStation ‘get main processor diagnostic data’ command.
  - Switch device operating mode [to “Running”]
- Stop the safety system: ‘enable all forces’ command (T0843) (forces values on the equipment)

Impact

- Safety system is disabled, resulting in Loss of safety (T0880)

How The SCADAfence Platform Prevents Attacks on ICS Networks Such As Triton

This analysis was based on the MITRE Engenuity scenario which used the MITRE ATT&CK for ICS knowledge base to emulate the tactics, techniques, and procedures (TTPs) associated with the TRISIS/TRITON malware.

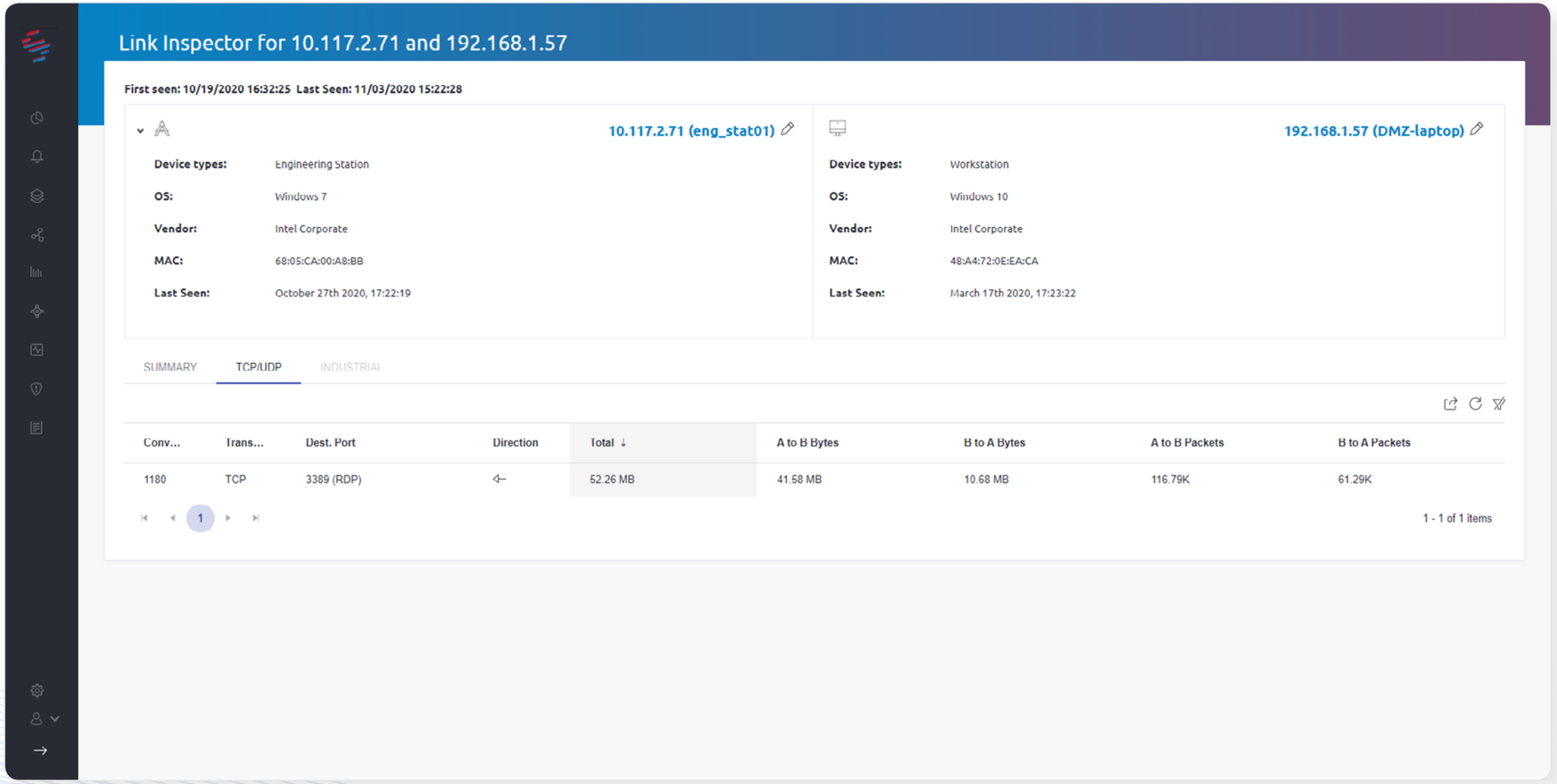
Attack method:
Adversaries communicated over a commonly used port to bypass firewalls or network detection systems and to blend in with normal network activity, to avoid more detailed inspection.

Tactic:
Command and Control (TA0101)

Technique:
Commonly Used Port (T0885)

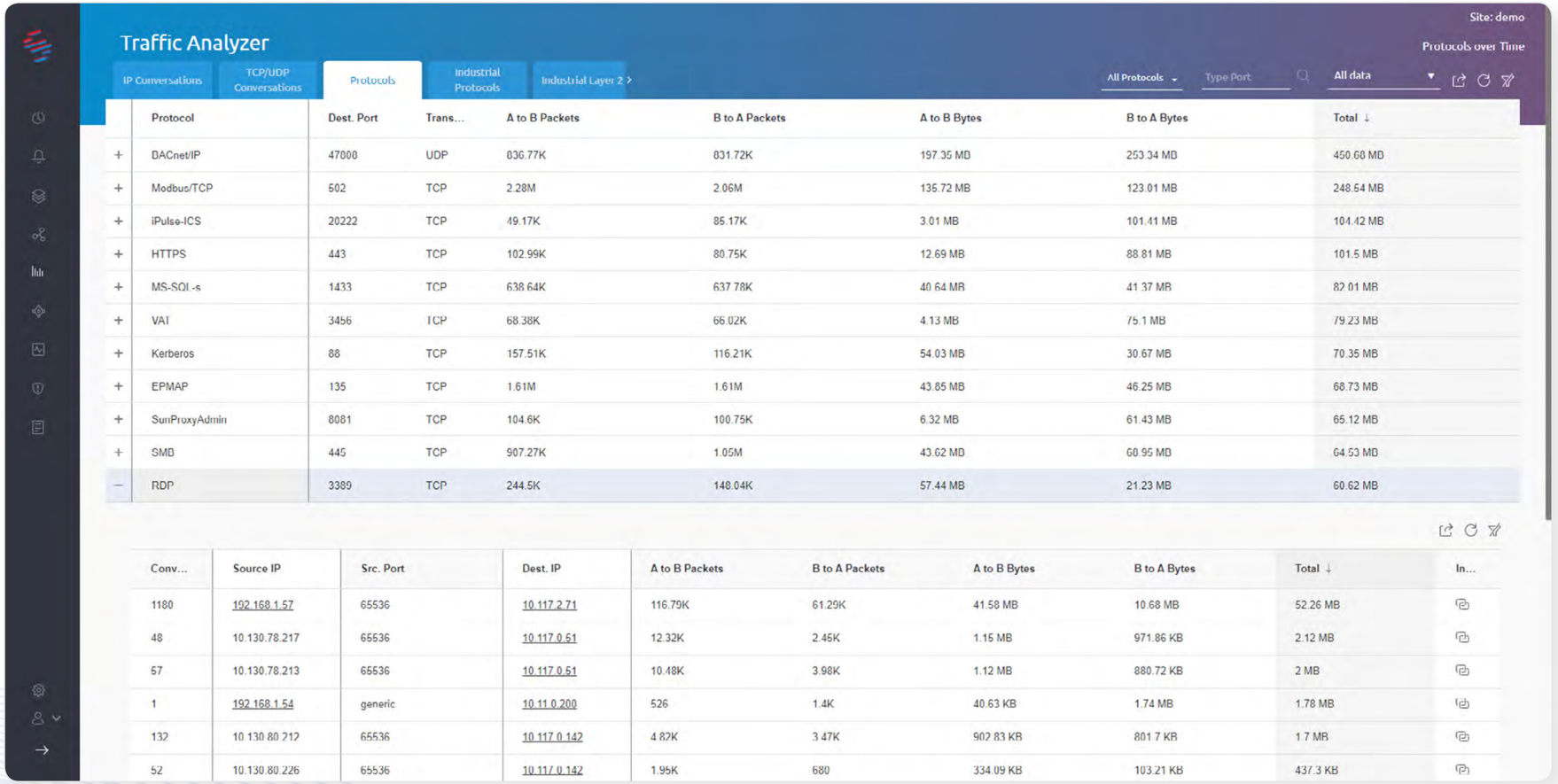
Criteria:
Evidence of an established network connection over TCP port 3389 as RDP.

1.A.1.1 - Link Inspector:
Port 3389 (RDP) connection between adversary and engineering-station

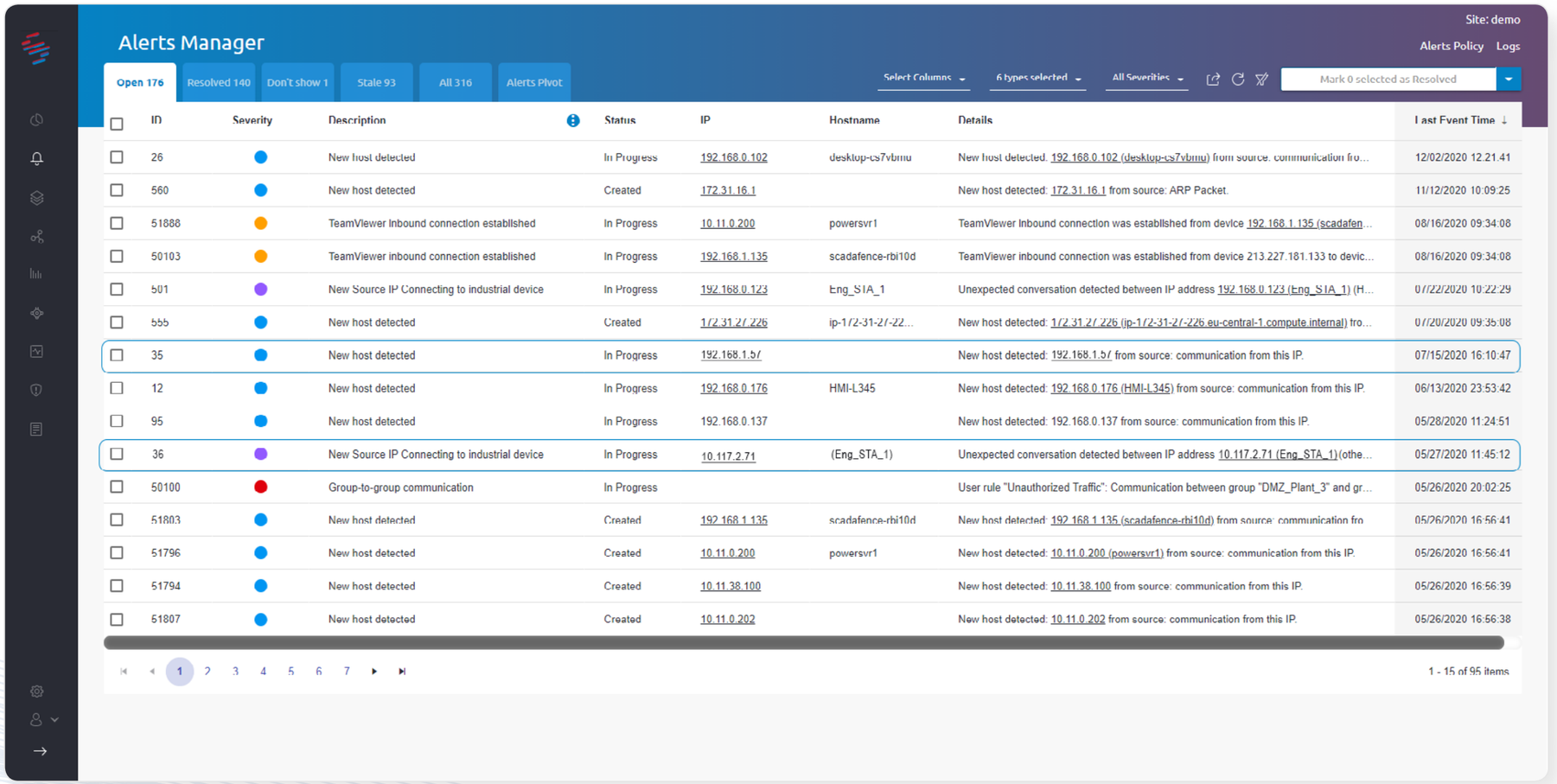


SCADAfence

1.A.1.2 - Traffic Analyzer - Protocols:
RDP connections



1.A.1.3 - Alerts Manager:
New host and new connection to industrial device alerts



SCADAfence

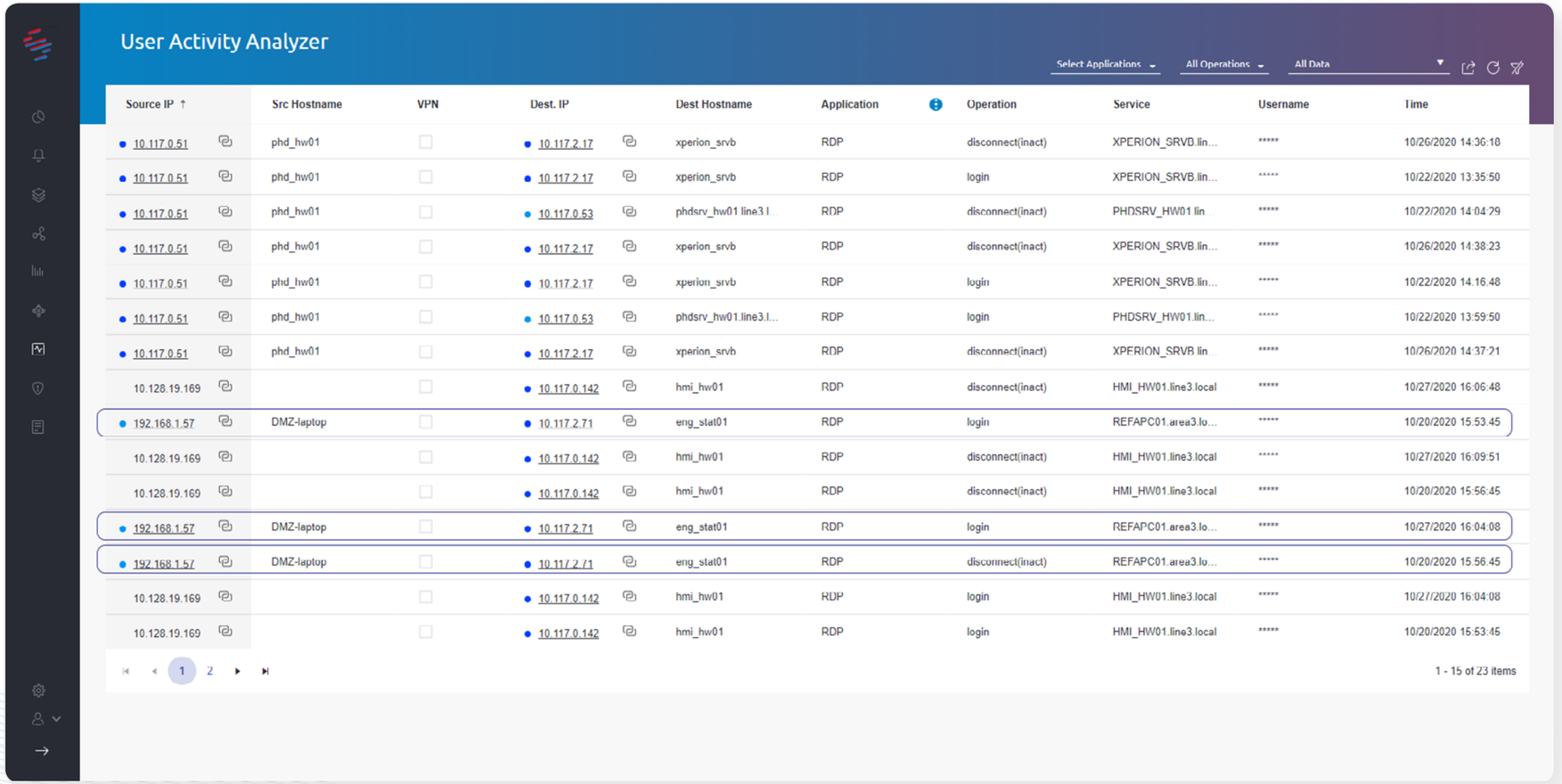
Attack method:
Adversaries may use the protocol associated with the port, or a completely different protocol to to bypass firewalls or network detection systems and to blend in with normal network activity

Tactic:
Command and Control (TA0101)

Technique:
Commonly Used Port (T0885)

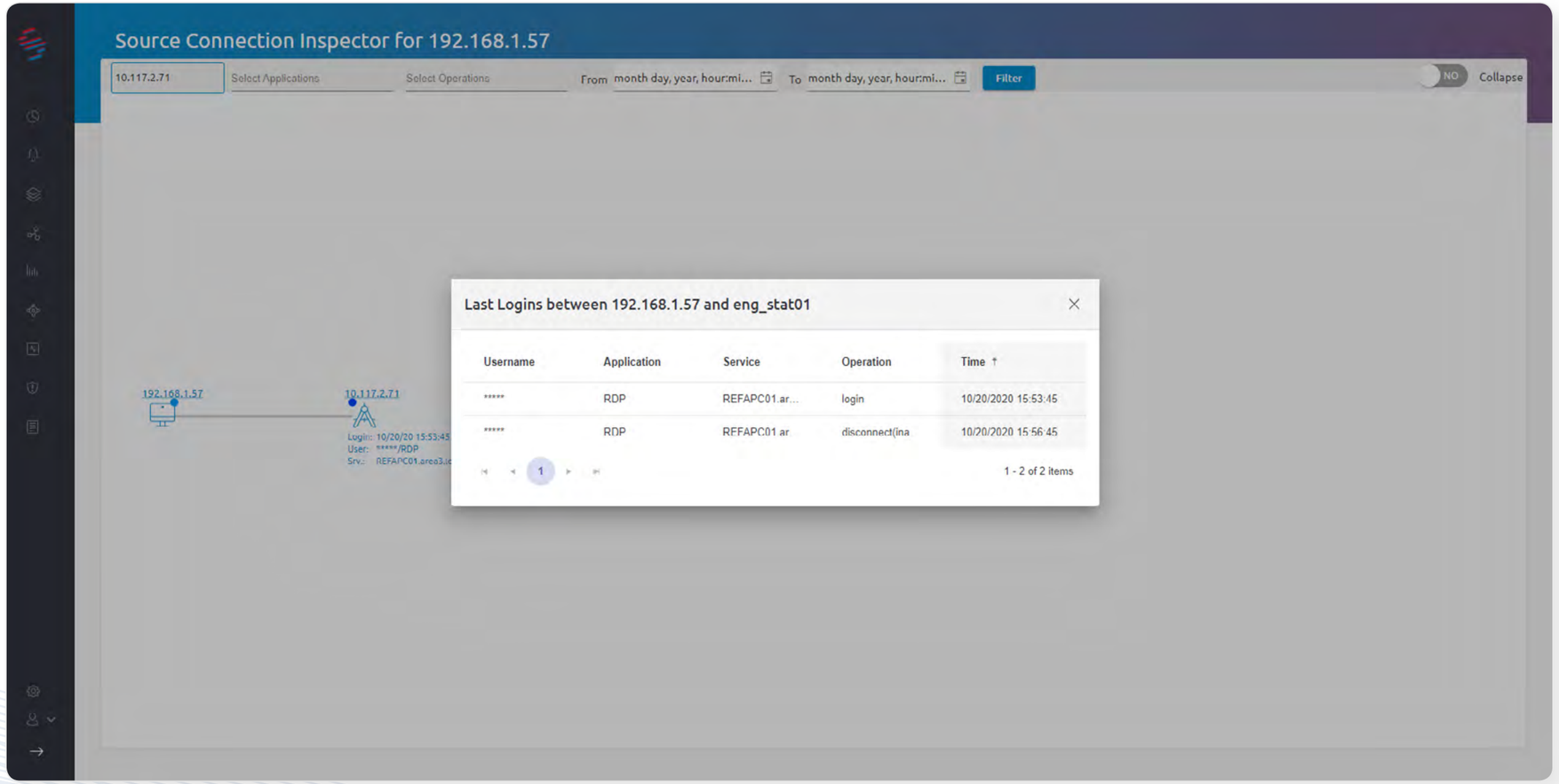
Criteria:
Successful logon as user “Engineer” on RDP (3389) may be present or as a part of the connection and process creation.

1.A.2.1 - User Activity Analyzer:
RDP connections and operations



1.A.2.2 - Connection Inspector:

Port 3389 (RDP) connection between adversary and engineering-station



Attack method:
Adversaries attempt to leverage Application Program Interfaces (APIs) used for communication between control software and the hardware.

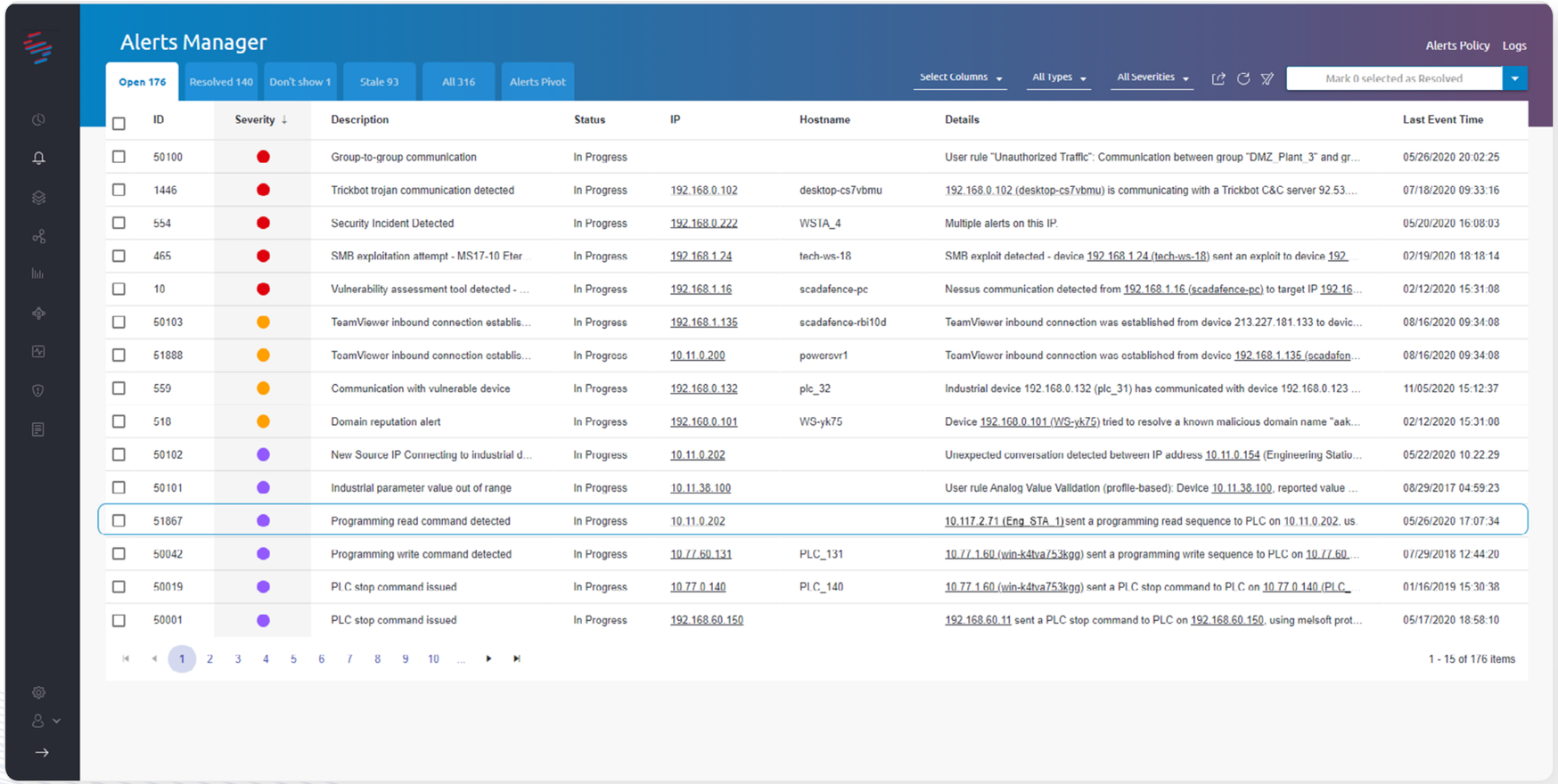
Tactic:
Execution (TA0104)

Technique:
Execution through API (T0871)

Criteria:
Evidence of an adversary initiated program upload action of the control PLC to collect the current running configuration.

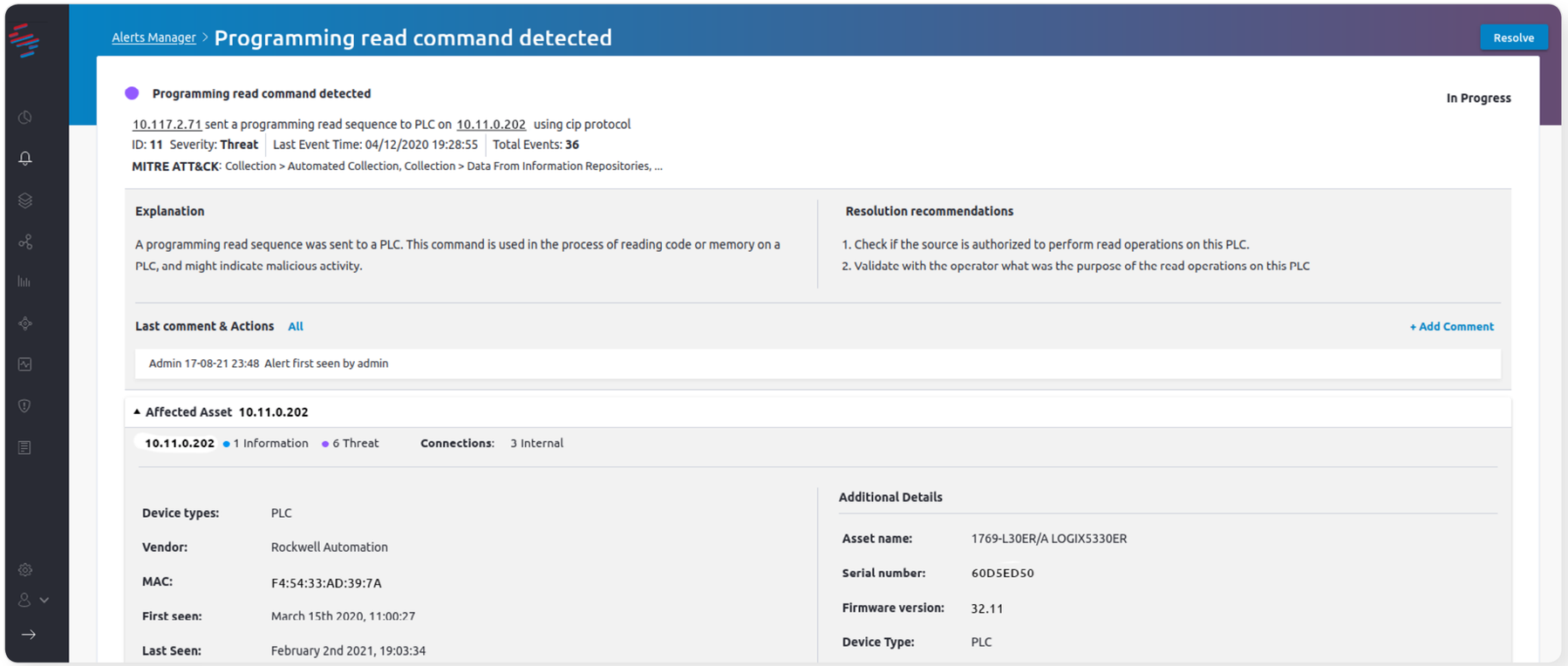
2.B.1.1 - Alerts Manager:

Program Upload (programming read) alert

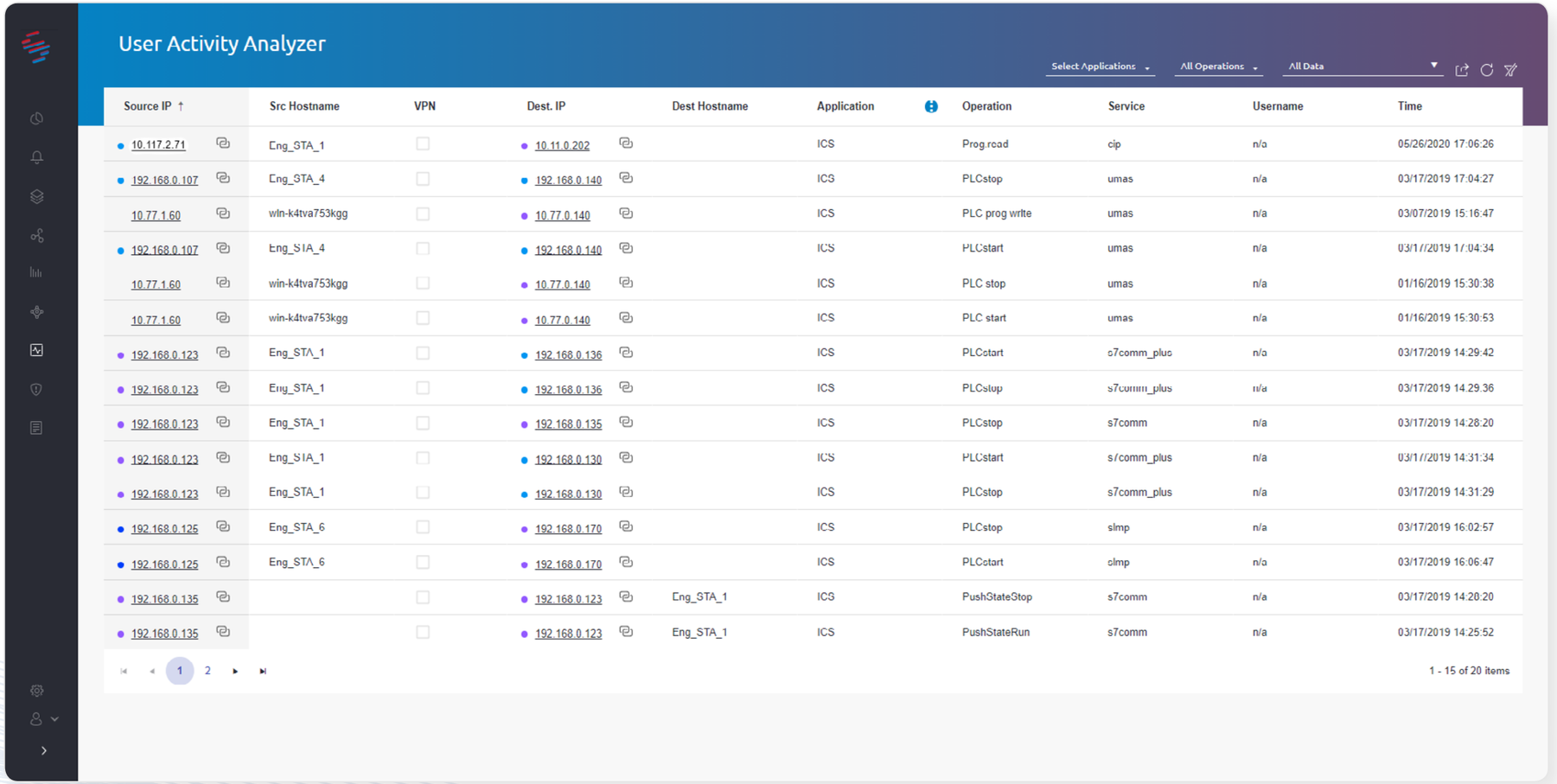


2.B.1.1.1 - Alerts Manager:

Program Upload (programming read) alert



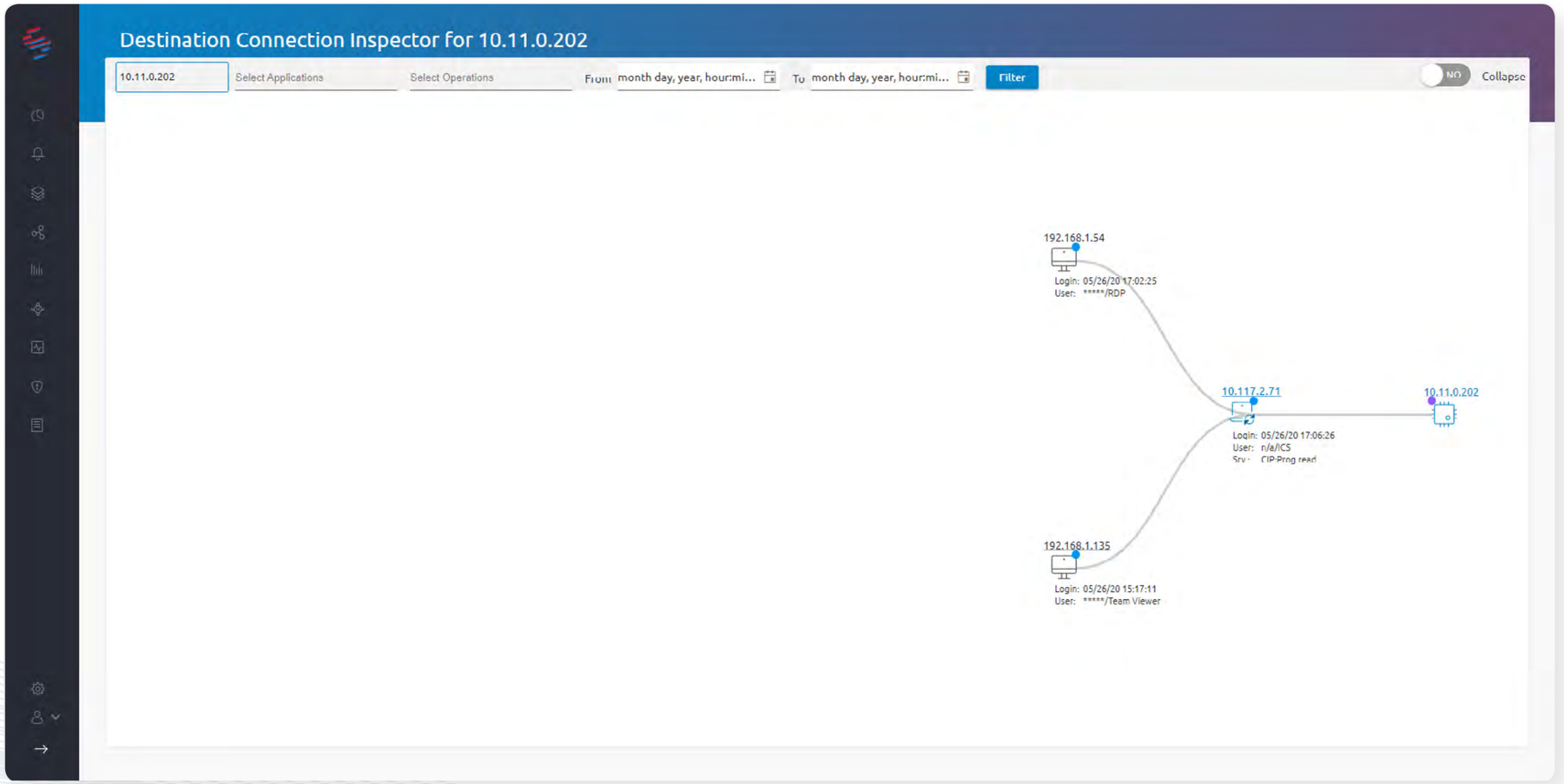
2.B.1.2 - User Activity Analyzer:
ICS connections and operations



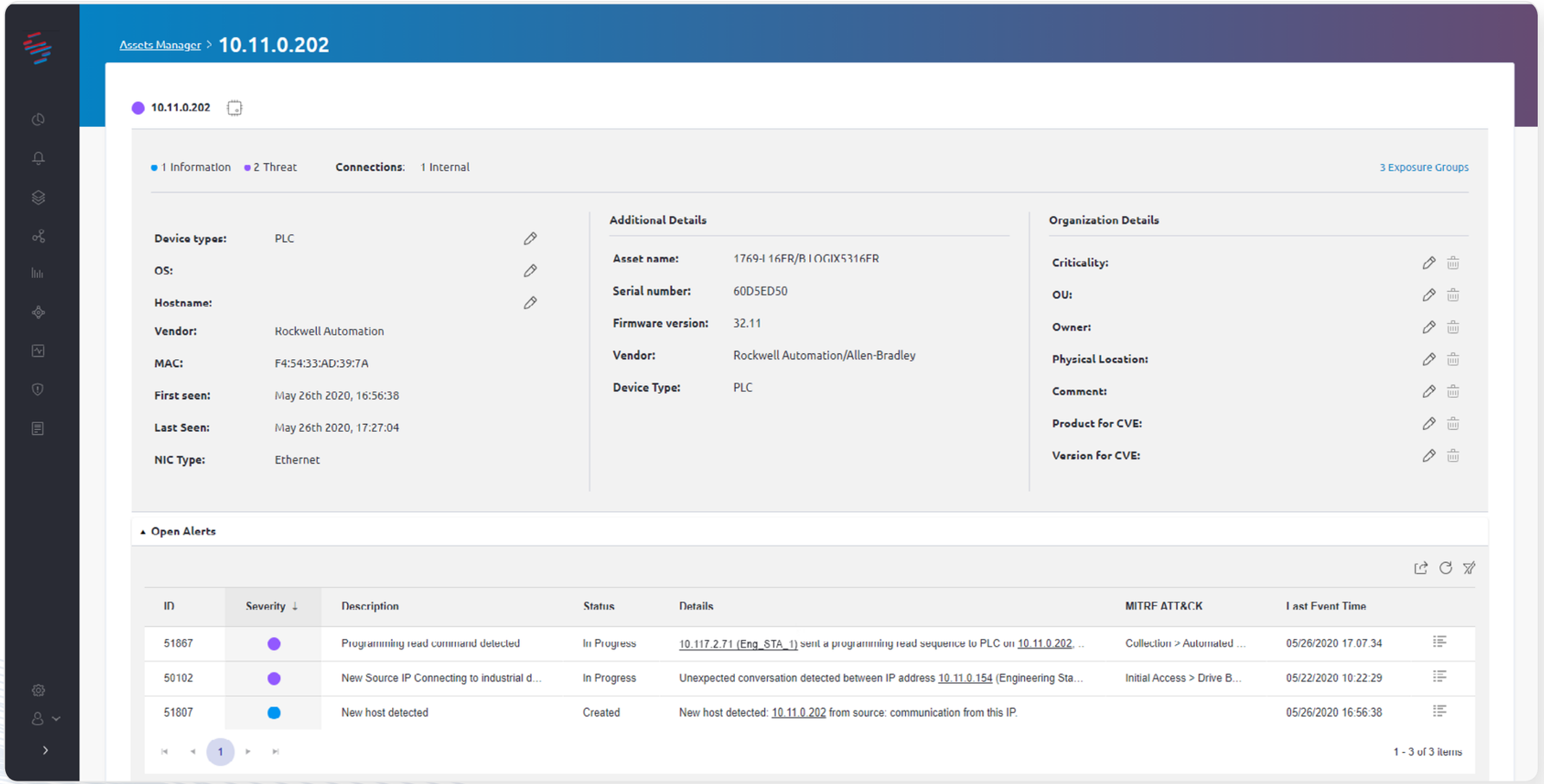
SCADAfence

2.B.1.3 - Connection Inspector:

Adversary to engineering-station to PLC



2.B.1.4 - Assets Manager:
PLC asset management page including device information and alerts

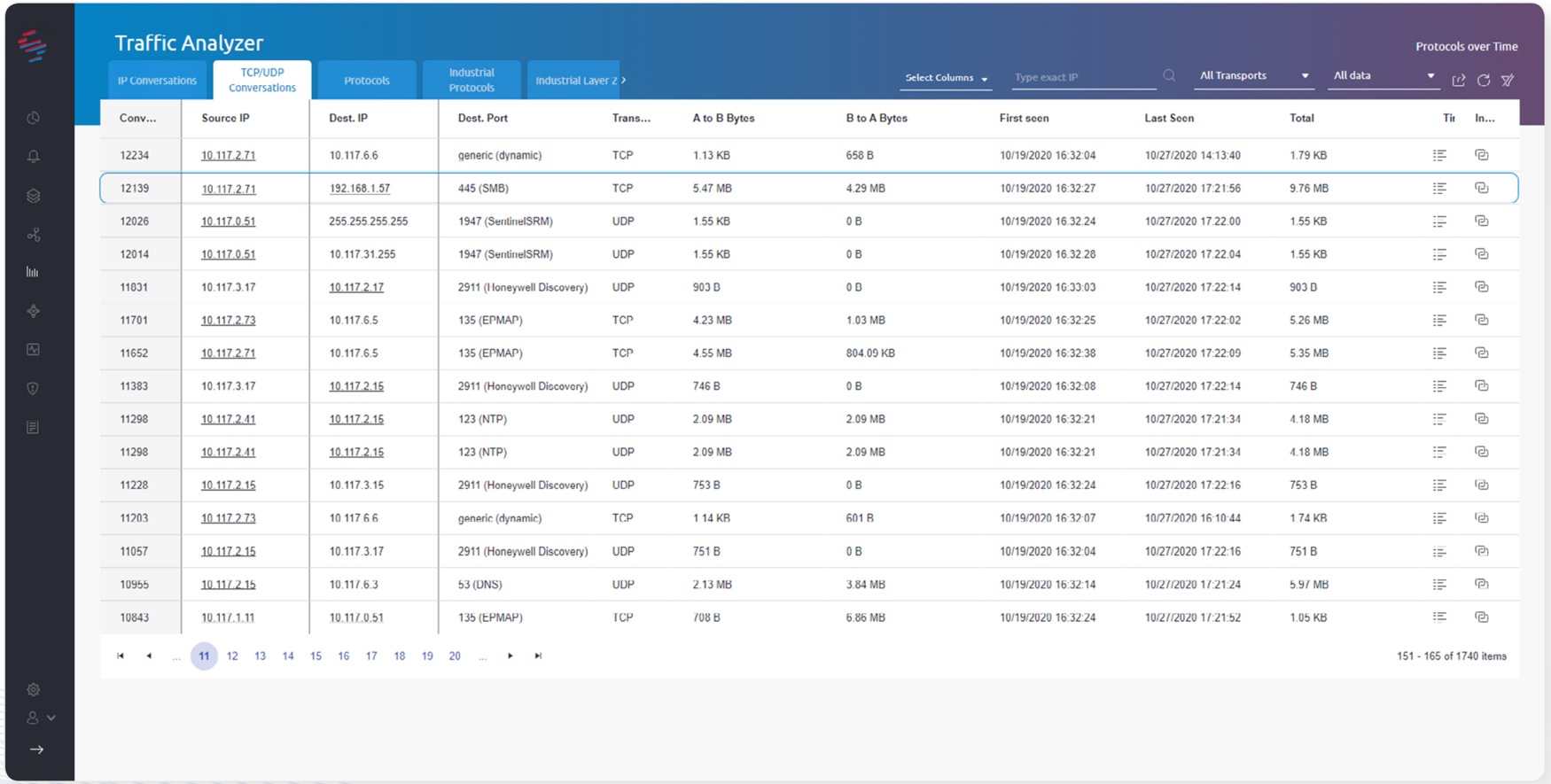


Attack method:
Adversaries may use the protocol associated with the port, or a completely different protocol to to bypass firewalls or network detection systems and to blend in with normal network activity.

Tactic:
Command and Control (TA0101)

Technique:
Commonly Used Port (T0885)

Criteria:
Evidence of an established network connection over TCP port 445 from the control machine to the adversary machine as an outbound SSH tunnel request.the current running configuration.

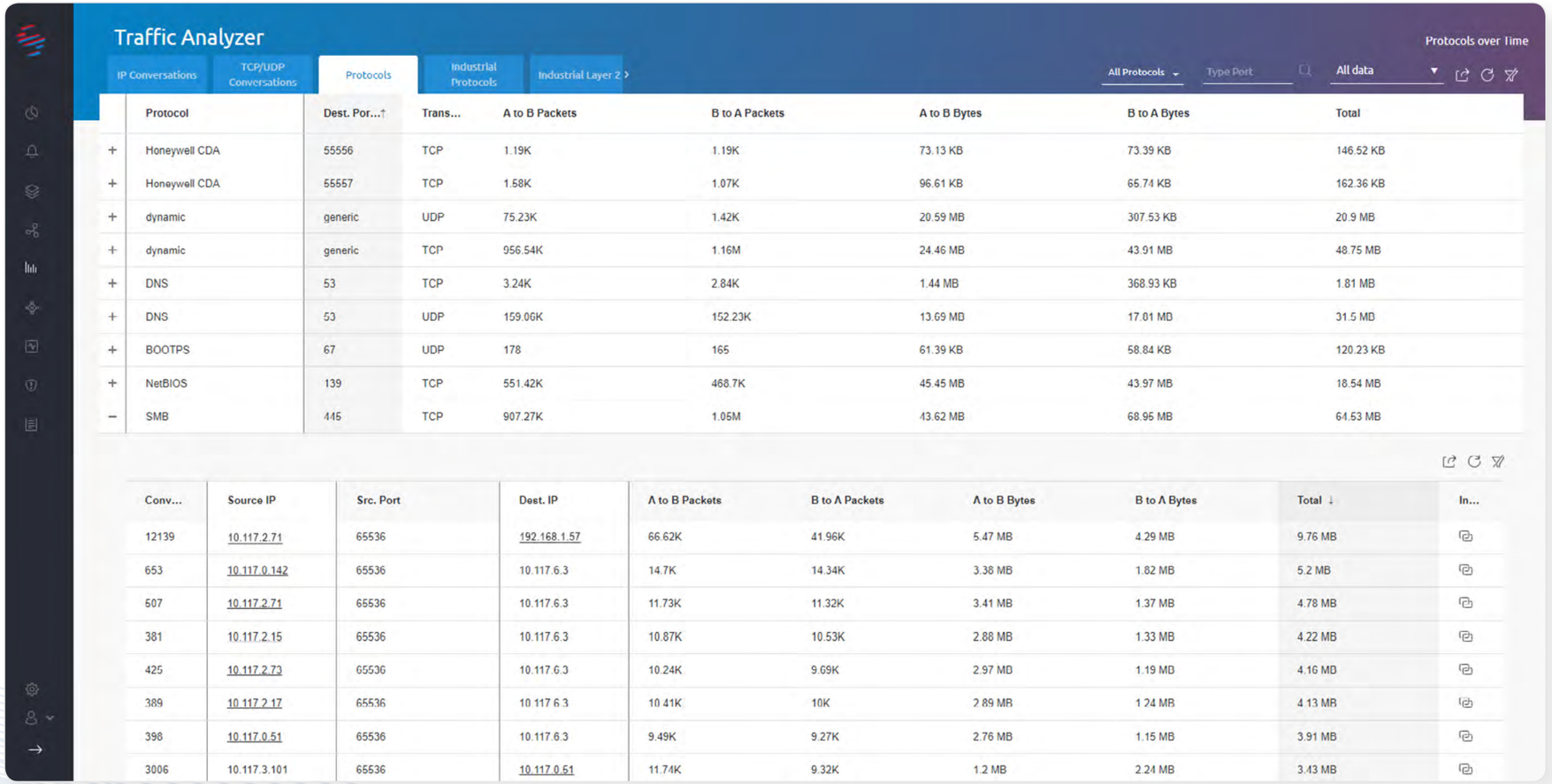


4.B.2.1 - Traffic Analyzer - TCP/UDP Conversations:
Port 445 connection between engineering-station and adversary

SCADAfence

4.B.2.2 - Traffic Analyzer - Protocols:

Port 445 connections



Protocol	Dest. Por...↑	Trans...	A to B Packets	B to A Packets	A to B Bytes	B to A Bytes	Total
+ Honeywell CDA	55556	TCP	1.19K	1.19K	73.13 KB	73.39 KB	146.52 KB
+ Honeywell CDA	55557	TCP	1.58K	1.07K	96.61 KB	65.74 KB	162.36 KB
+ dynamic	generic	UDP	75.23K	1.42K	20.59 MB	307.53 KB	20.9 MB
+ dynamic	generic	TCP	956.54K	1.16M	24.46 MB	43.91 MB	48.75 MB
+ DNS	53	TCP	3.24K	2.84K	1.44 MB	368.93 KB	1.81 MB
+ DNS	53	UDP	159.06K	152.23K	13.69 MB	17.01 MB	31.5 MB
+ BOOTPS	67	UDP	178	165	61.39 KB	58.84 KB	120.23 KB
+ NetBIOS	139	TCP	551.42K	468.7K	45.45 MB	43.97 MB	18.54 MB
− SMB	445	TCP	907.27K	1.05M	43.62 MB	68.95 MB	64.53 MB

Conv...	Source IP	Src. Port	Dest. IP	A to B Packets	B to A Packets	A to B Bytes	B to A Bytes	Total ↓	In...
12139	10.117.2.71	65536	192.168.1.57	66.62K	41.96K	5.47 MB	4.29 MB	9.76 MB	
653	10.117.0.142	65536	10.117.6.3	14.7K	14.34K	3.38 MB	1.82 MB	5.2 MB	
507	10.117.2.71	65536	10.117.6.3	11.73K	11.32K	3.41 MB	1.37 MB	4.78 MB	
381	10.117.2.15	65536	10.117.6.3	10.87K	10.53K	2.88 MB	1.33 MB	4.22 MB	
425	10.117.2.73	65536	10.117.6.3	10.24K	9.69K	2.97 MB	1.19 MB	4.16 MB	
389	10.117.2.17	65536	10.117.6.3	10.41K	10K	2.89 MB	1.24 MB	4.13 MB	
398	10.117.0.51	65536	10.117.6.3	9.49K	9.27K	2.76 MB	1.15 MB	3.91 MB	
3006	10.117.3.101	65536	10.117.0.51	11.74K	9.32K	1.2 MB	2.24 MB	3.43 MB	

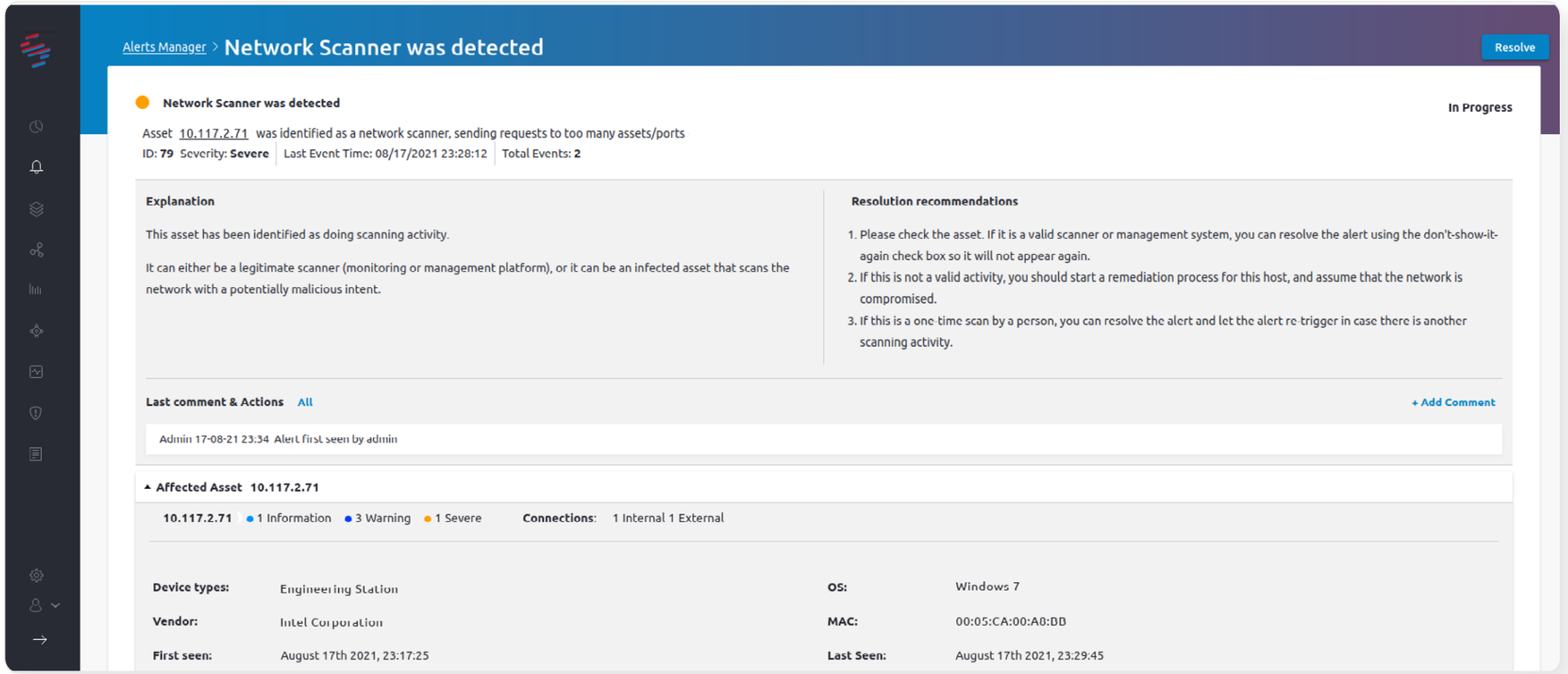
SCADAfence

Attack method:
Adversaries attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for subsequent Lateral Movement or Discovery techniques.

Tactic:
Discovery (TA0102)

Technique:
Remote System Discovery (T0846)

Criteria:
Evidence that a network discovery scan for TCP port 44818 was initiated from the control machine on hosts across the whole subnet.



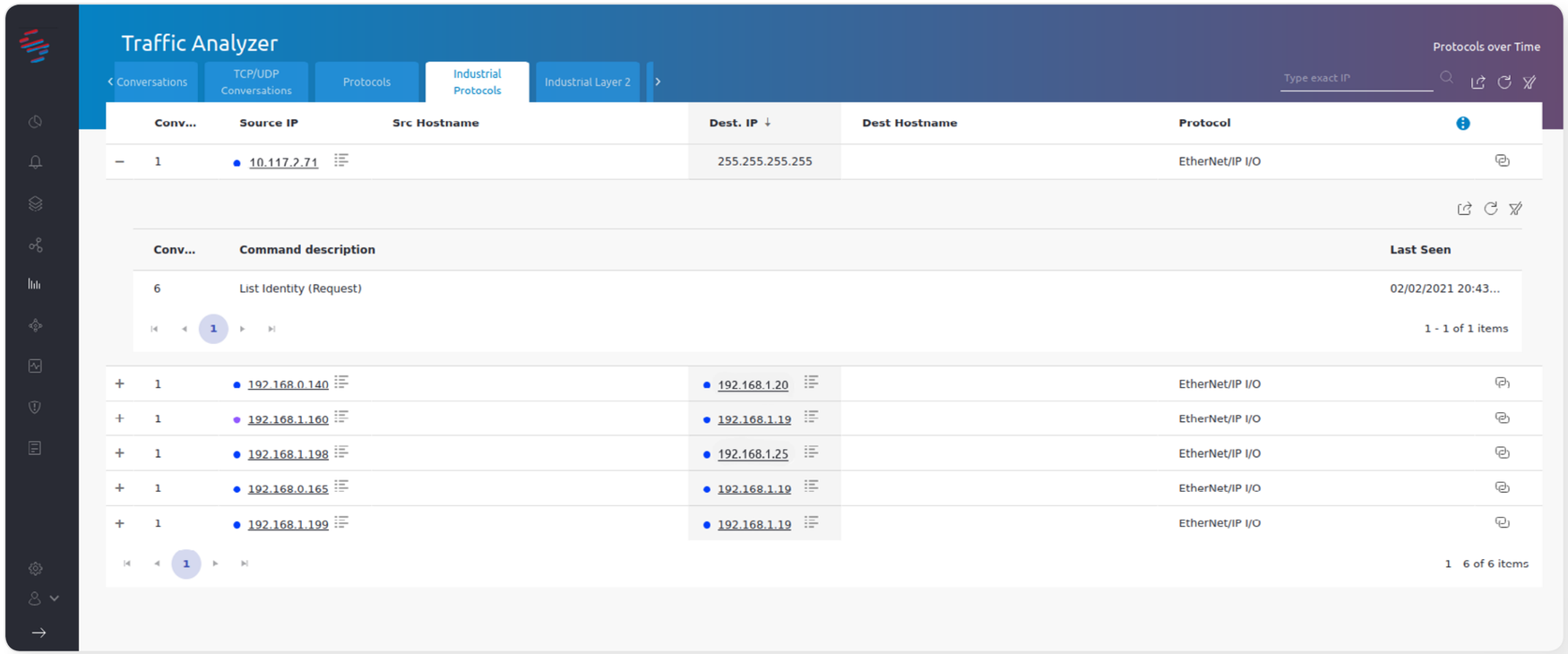
9.A.2 - Network Scanner detection alert

Attack method:
Adversaries attempt to get a listing of other systems by IP address on a network that may be used for subsequent Lateral Movement.

Tactic:
Discovery (TA0102)

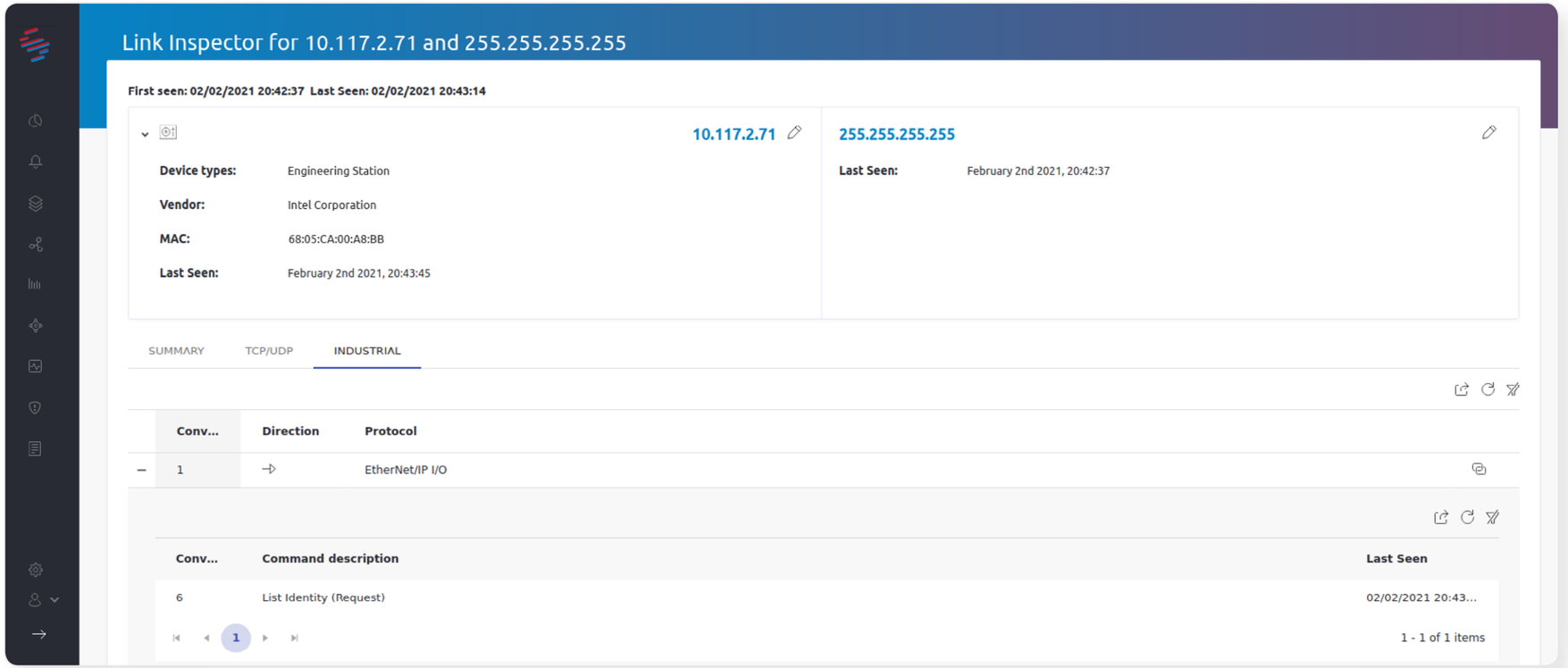
Technique:
Remote System Discovery (T0846) Link

Criteria:
Evidence of the network discovery broadcast request sent from the control EWS over TCP port 44818..



9.B.2.1 - Traffic Analyzer - Industrial Protocols:
EtherNet/IP broadcast scan (List Identity) commands visibility

9.B.2.2 - Link Inspector:
Control to broadcast

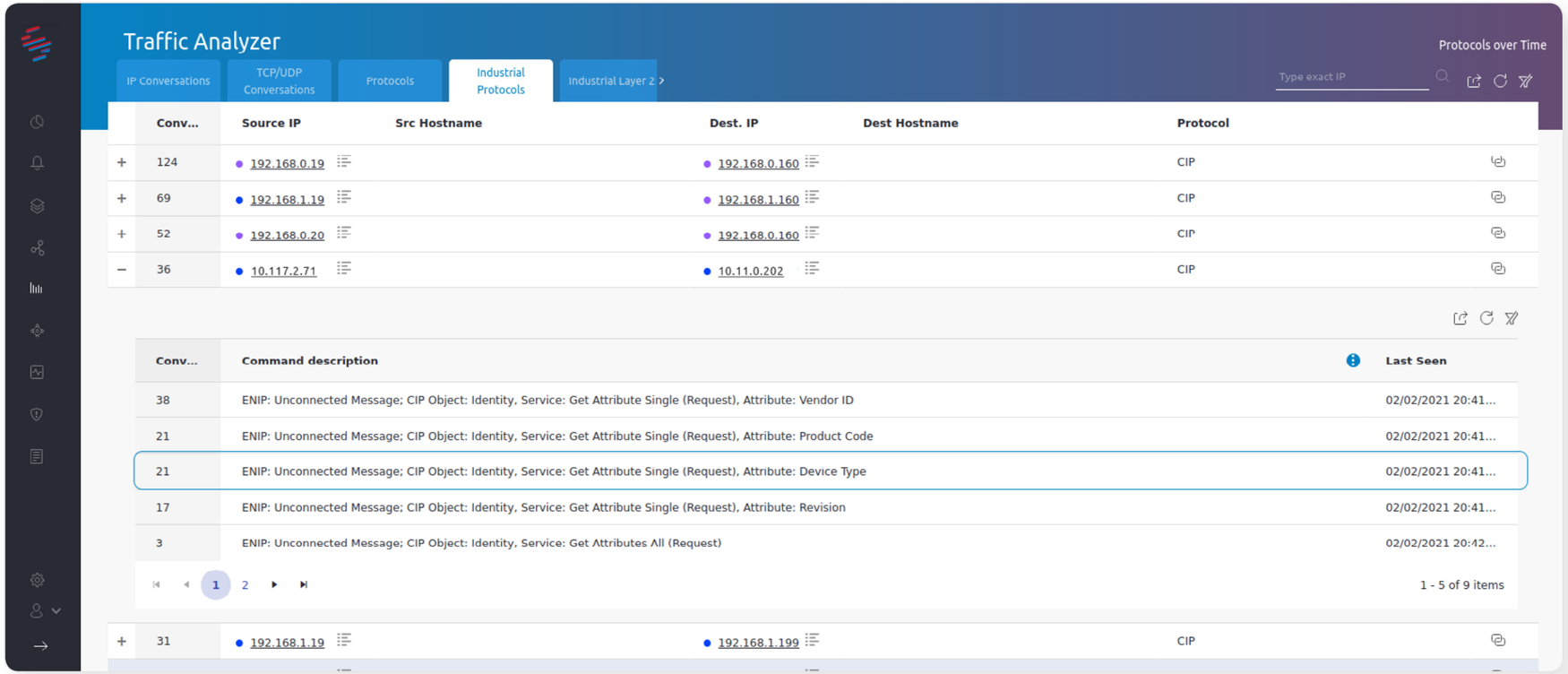


Attack method:
An adversary attempts to get detailed information about remote systems and their peripherals, such as make/model, role, and configuration.

Tactic:
Discovery (TA0102)

Technique:
Remote System Information Discovery (T0888)

Criteria:
Evidence of an adversary initiated Get Attribute Single CIP request for the “Device Type” attribute (instance 0x01, class 0x01) of the control PLC.



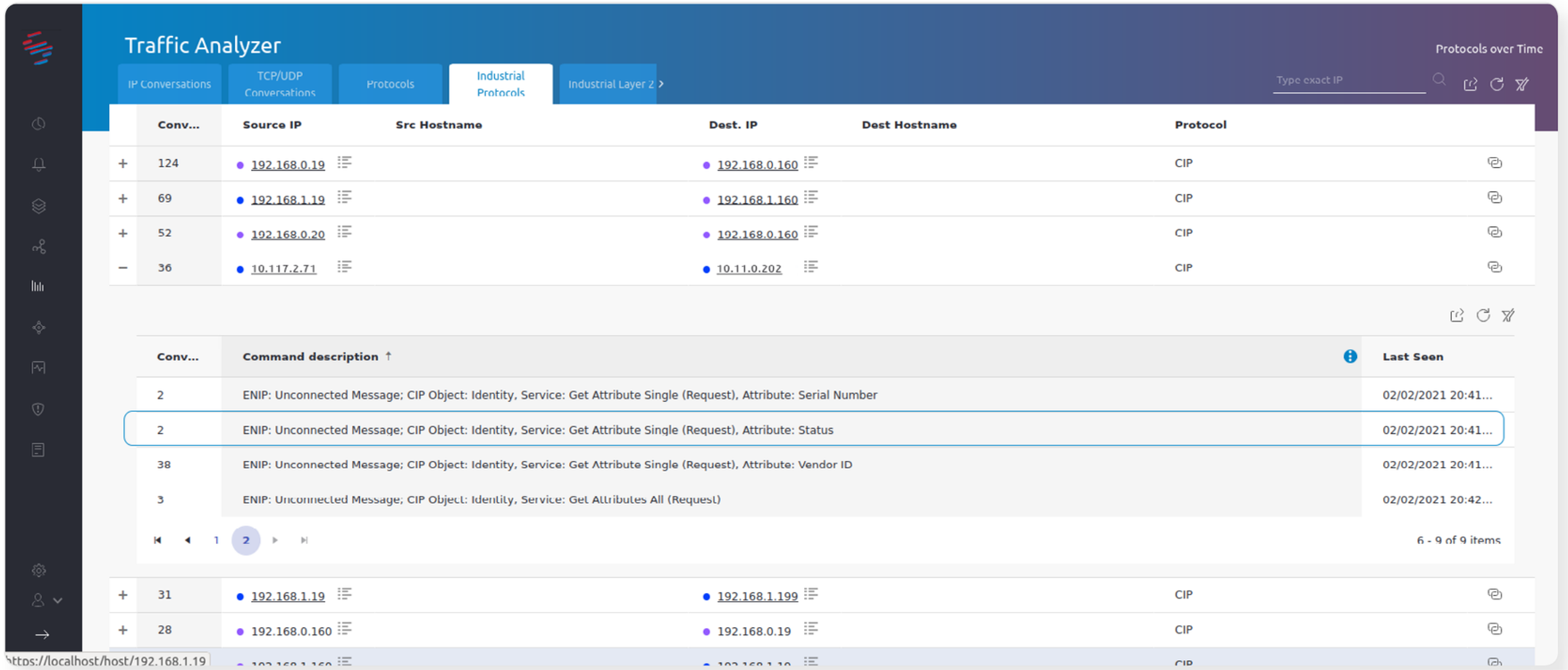
9.C.2 - Traffic Analyzer - Industrial Protocols:
CIP GetAttributeSingle ‘Device Type’ commands visibility

Attack method:
An adversary attempts to get detailed information about remote systems and their peripherals, such as make/model, role, and configuration.

Tactic:
Discovery (TA0102)

Technique:
Remote System Information Discovery (T0888)

Criteria:
Evidence of an adversary initiated Get Attribute Single CIP request for the “Status” attribute (instance 0x01, class 0x01) of the control PLC.



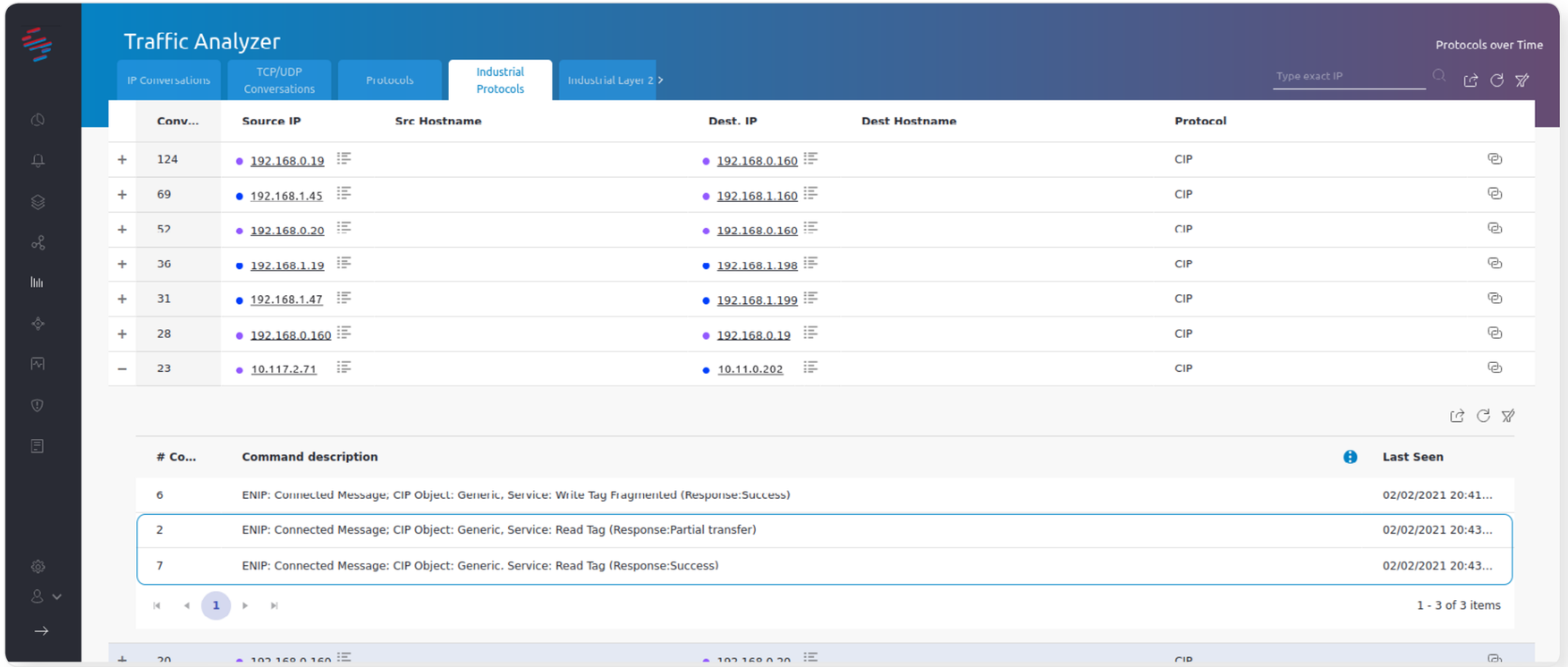
9.D.2 - Traffic Analyzer - Industrial Protocols:
CIP GetAttributeSingle ‘Status’ commands visibility

Attack method:
Adversaries attempt to leverage Application Program Interfaces (APIs) used for communication between control software and the hardware.

Tactic:
Execution (TA0104)

Technique:
Execution through API (T0871)

Criteria:
Evidence that all controller and program tag names were requested over CIP from the control PLC to the control machine.



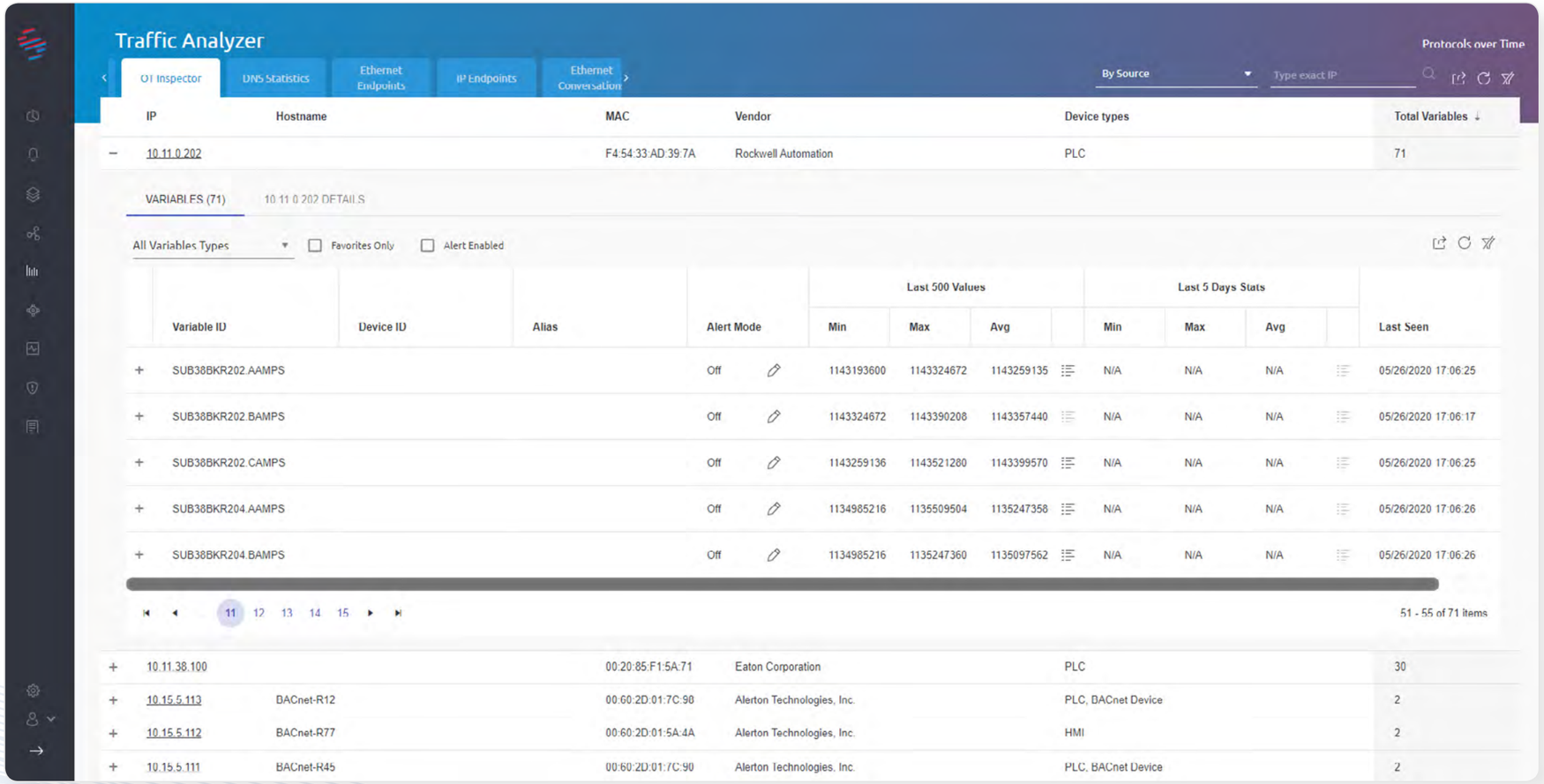
9.E.2.1 - Traffic Analyzer - Industrial Protocols:
CIP Read/Write Tags commands visibility

The SCADAfence OT Inspector helps maintain the integrity and availability of critical industrial processes by monitoring process values of PLCs, RTUs, and other field devices.

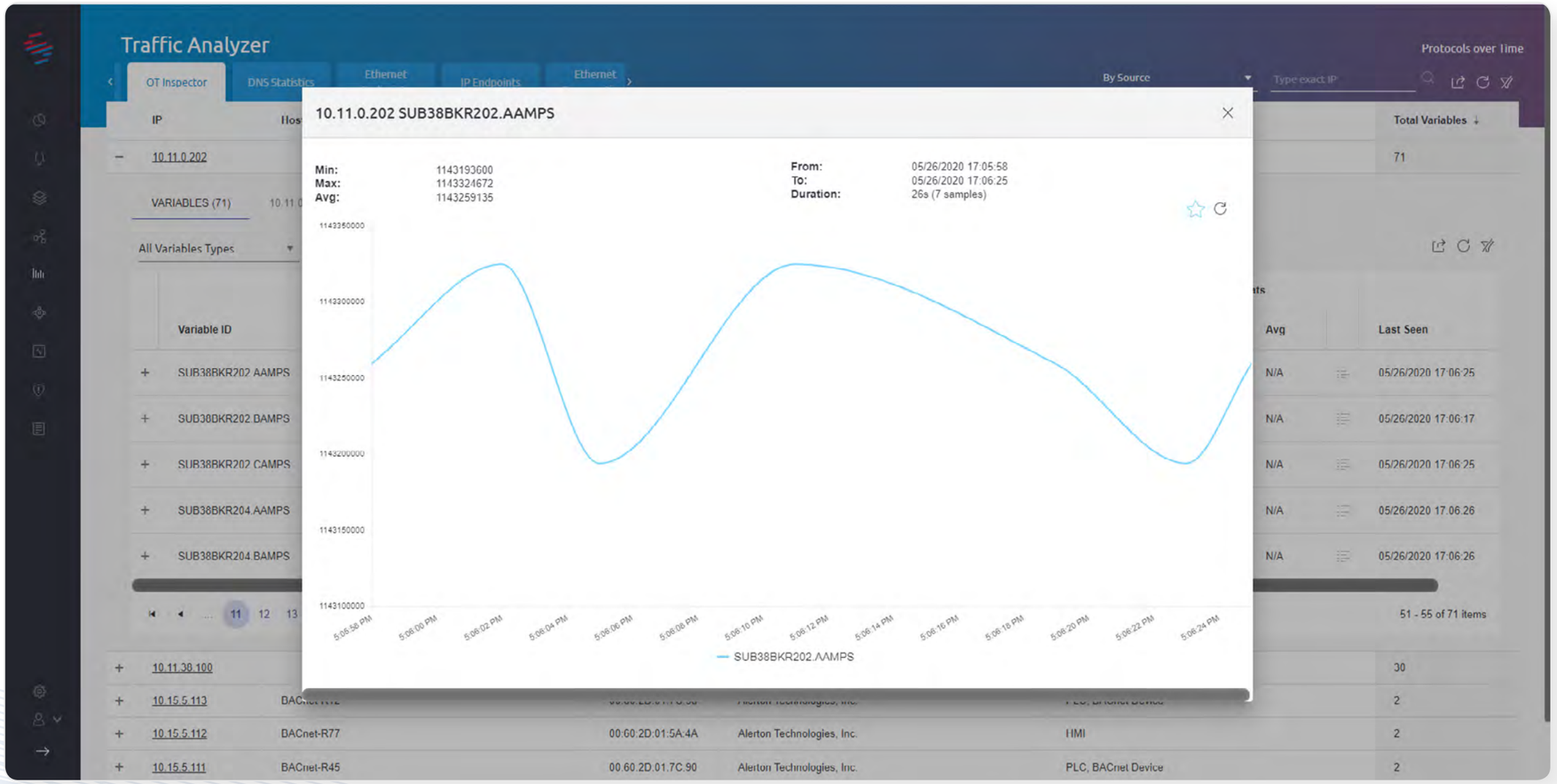
- Support in main industry protocols: Siemens-S7, EtherNet/IP-CIP, Modbus and Bacnet
- Enhanced visibility into the ENIP/CIP protocols where we determine and display the internal port structure and configuration of assets in the ENIP\CIP protocol.
- Supports the import of tag mapping files (from Engineering/HMI software) for variables of the Siemens S7 protocol.
- Detects and alerts upon packets that are not according to the BACnet protocol structure. Our system detects malformed packets based on non-standard opcodes, invalid values or packet length mismatch. Additionally, we can detect DoS trials, fuzzing, misconfigurations that endanger processes.
- Users can define thresholds and mark important data points and set up alerts on single data points

In the next 2 pages, you can see how the CIP Value Level Visibility and Value Level Data Point Views are displayed in the SCADAfence Platform

9.E.2.2 - Traffic Analyzer - OT Inspector:
CIP Value Level visibility



9.E.2.3 - Traffic Analyzer - OT Inspector:
CIP Value Level data point view



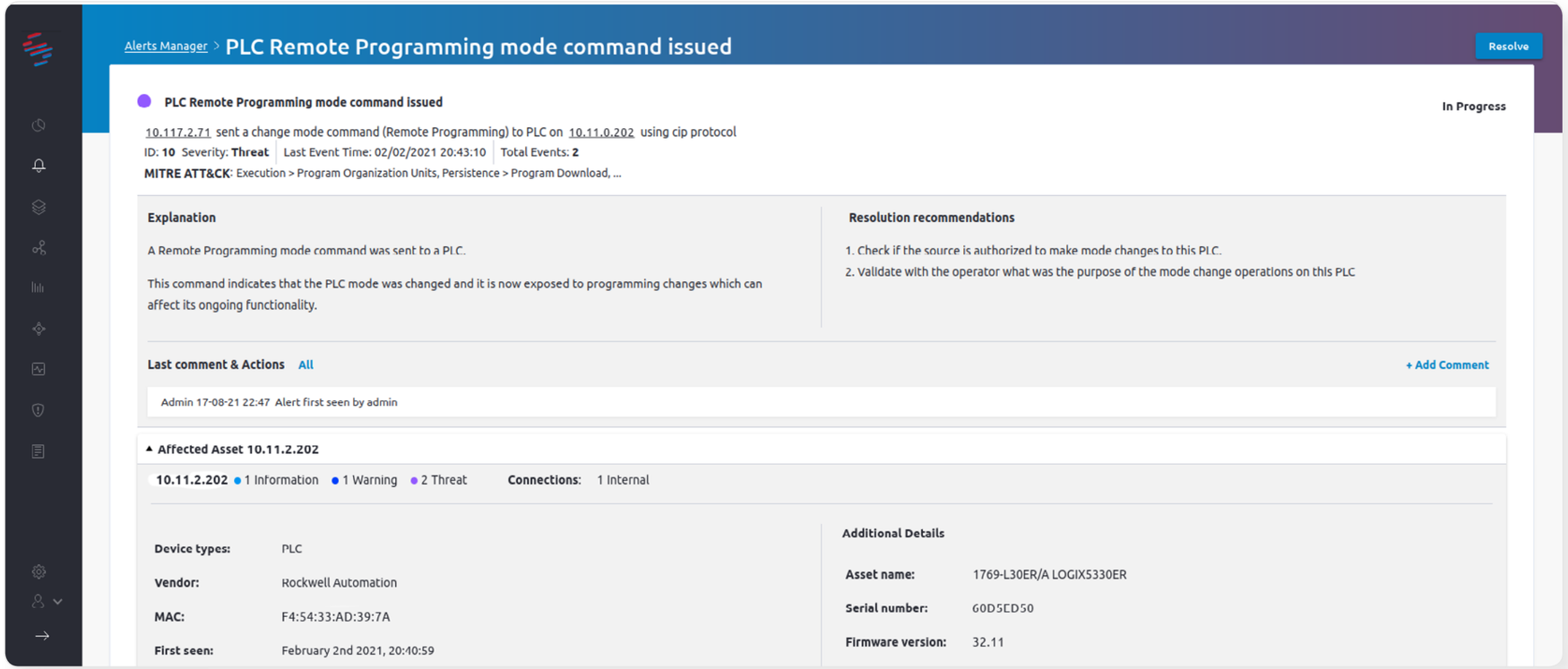
Attack method:
Adversaries change the operating mode of a controller to gain additional access to engineering functions such as Program Download.

Tactic:
Evasion (TA0103)

Technique:
Change Operating Mode (T0858)

Criteria:
Evidence of the safety PLC operating mode being switched to Program Mode following adversary CIP request to instance 0x01 of class 0x8E using service 0x07.

22.A.2 - Alerts Manager:
PLC Remote Programming Mode alert



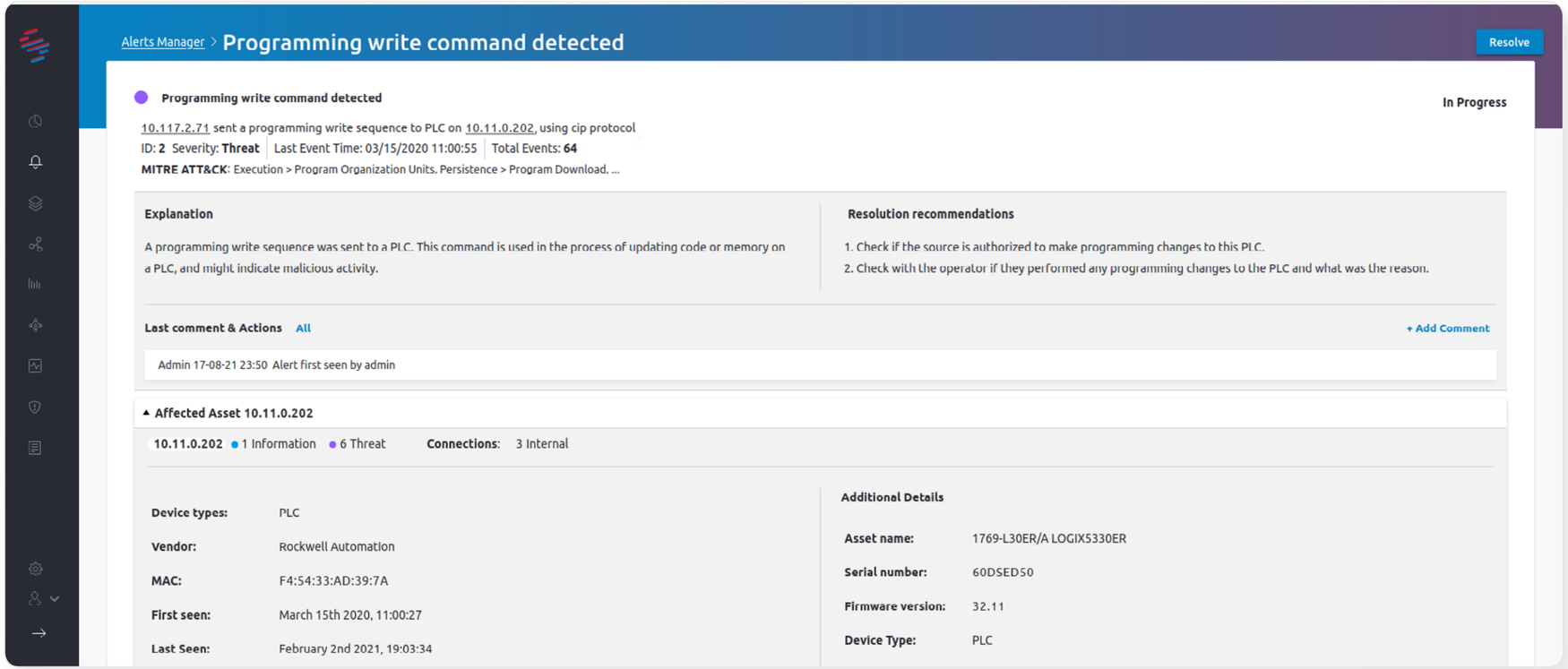
Attack method:
Adversaries perform a program download to transfer a user program to a controller.

Tactic:
Lateral Movement (TA0109)

Technique:
Program Download (T0843)

Criteria:
Evidence of an adversary initiated online edit action on the safety PLC, requested from the safety machine.

20.B.3 - Alerts Manager:
PLC Program Download alert



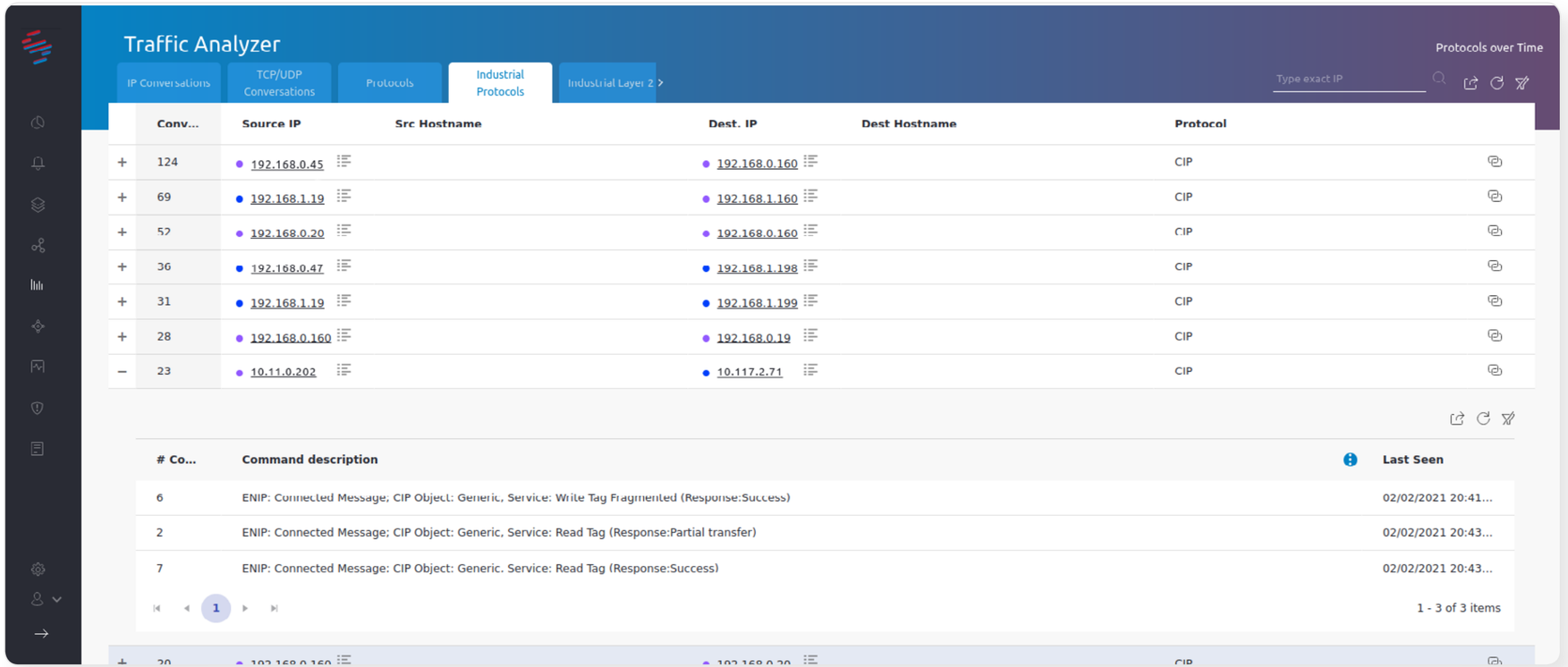
Attack method:
Adversaries attempt to leverage Application Program Interfaces (APIs) used for communication between control software and the hardware.

Tactic:
Execution (TA0104)

Technique:
Execution through API (T0871)

Criteria:
Evidence of an adversary initiated read/write action of the “CC” tag using the 0x4C/0x4D CIP service.

24.C.2 - Traffic Analyzer - Industrial Protocols:
CIP Read/Write Tags commands visibility

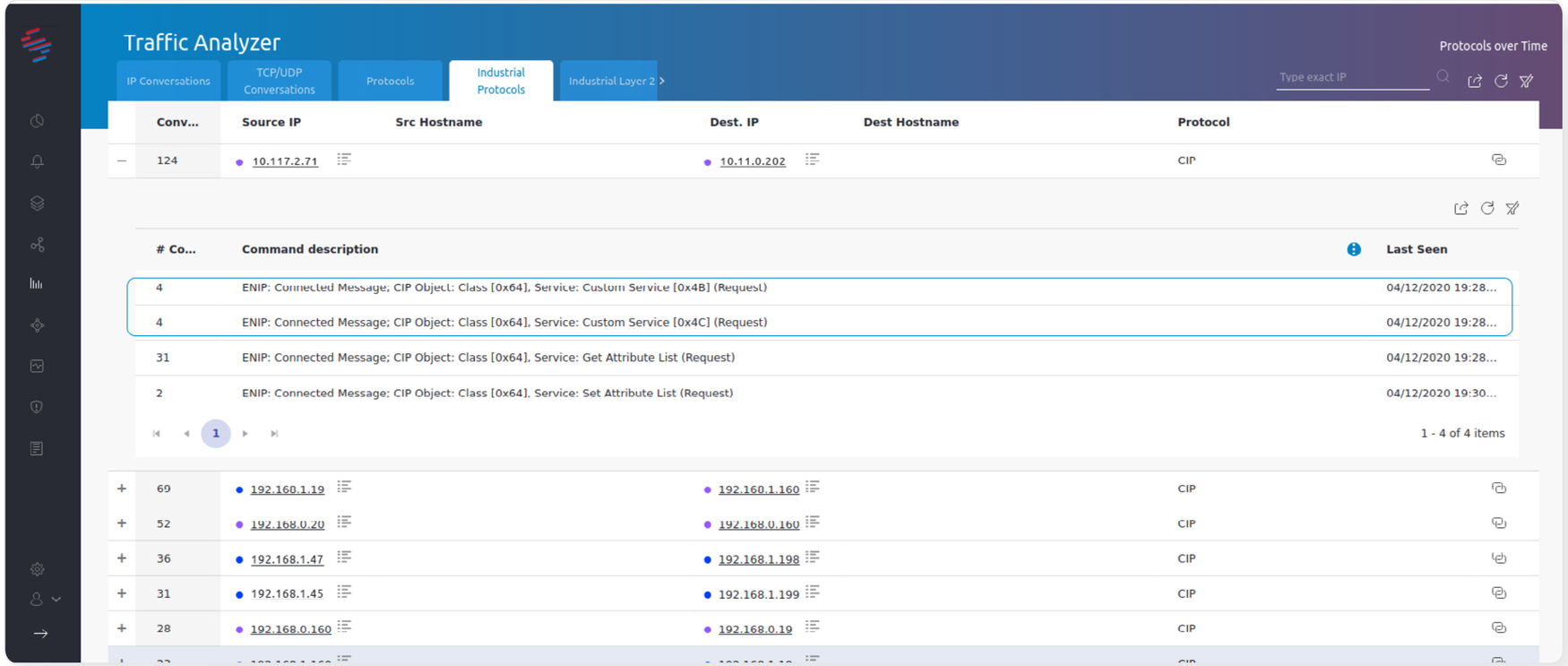


Attack method:
Adversaries attempt to leverage Application Program Interfaces (APIs) used for communication between control software and the hardware.

Tactic:
Execution (TA0104)

Technique:
Execution through API (T0871)

Criteria:
Evidence of abuse of a CIP handshake between the engineering-station and control PLC resulting in an adversary privilege escalation (handshake sequence consisted of a service 0x4B class 0x64 initiation request and 0x4C class 0x64 challenge response).



25.E.2 - Traffic Analyzer - Industrial Protocols:
CIP handshake commands visibility

Possible additional signatures and useful data:

1) https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/TRITON_Appendix_A.pdf
2) https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/TRITON_Appendix_B.pdf
3) https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN
4) https://www.fireeye.com/blog/threat-research/2018/06/totally-tubular-treatise-on-triton-and-tristation.html

About SCADAfence:

SCADAfence is the global technology leader in OT & IoT cybersecurity. SCADAfence offers a full suite of industrial cybersecurity products that provides full coverage of large-scale networks, offering best-in-class network monitoring, asset discovery, governance, remote access, and IoT device security. A Gartner “Cool Vendor” in 2020, SCADAfence delivers proactive security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in critical infrastructure, manufacturing, and building management industries to operate securely, reliably, and efficiently. To learn more, visit our website, check out our blog, or follow us on LinkedIn

SCADAfence