Behavioral Anomaly Detection in Industrial Control Systems

An Evaluation of Flowmon ADS

Sawsan Youssef
Ondřej Ryšavý

Technical Report no. FIT-TR-2020-02
Faculty of Information Technology, Brno University of Technology

Abstract

This report provides results from the experiments aimed to evaluate the threat detection capabilities of the Flowmon Anomaly Detection System in the environment of Industrial Control Systems. The experiments follow a procedure described in the NISTIR 8219 report, which identifies a critical set of security threats to ICS and illustrates how behavior anomaly detection systems can be used as a key security component for industrial systems. We have shown that many of the identified security threats can be identified with the Flowmon ADS even without considering any specific ICS rules. The report systematically evaluates the scenarios considering network-based anomaly detection methods. We set up a virtual environment that contains ICS and Flowmon software. In this environment, we were able to demonstrate all scenarios and check Flowmon responses to the induced security threats.

Outline

1. Introduction

Cyber security is a prerequisite for the safe and reliable operation of modern industrial control systems (ICS). The threats to ICS can vary, including criminal groups, own employees, unexpected accidents and natural disasters. The Cybersecurity Framework [1] addresses potential threats and their prevention. Although it is not possible to prevent and identify all threats, detection of cyber incidents is an essential element of cyber security. By using the network monitoring and detection tools the organizations can detect cyber incidents in time to permit effective response and recovery. Moreover, network monitoring tools expand visibility and monitoring capabilities within manufacturing control systems, networks, and devices providing the oversight of resources and reducing disruptive cyber incidents by providing real-time information and anomaly-detection alerts.

Increased adoption of IT technologies enables access to previously isolated control systems via public networks. It brings many advantages and added business values but also represents a risk of unauthorized access leading to corrupting the system or data exfiltration. For this reason, properly applied security measures are necessary. Different techniques can be considered to protect ICS. Behavioral anomaly detection can be one of the key components of an ICS digital security solution. Systems for anomaly detection can not only help to increase the security and protection against attacks but can be a fruitful source for the identification of anomalous conditions being caused deliberately or inadvertently.

Increased visibility into ICS network operation and real-time alerting is the fundamental function of security devices. Security tools have to use non intrusive techniques to analyze industrial network communications. It is not acceptable for the monitoring tools to cause interruption or a performance impact as ICS systems rely on real-time data exchange. The tools should be able to identify new devices on the ICS network and of assets that have disappeared from the network. In the environment of ICS networks, the topology and the set of connected devices are fixed and thus any changes may be because of device failure or an indicator of unauthorized activities. Moreover, in the ICS environment, any unauthorized configuration changes and of the transfer of files in the network should be reported to the operator as a possible security incident.

The NISTIR 8219 report [2] provides a demonstration of different commercial available behavioral anomaly detection (BAD) tools for ICS in several scenarios considering typical security threats of ICS. The process control system (PCS) and the collaborative robotic system were used for the demonstration of BAD capabilities. The scope of this report is to demonstrate the cybersecurity capability of the Flowmon network monitoring and security tool for the ICS domain following the NISTIR approach. For this reason, we have created a virtual testbed similar to NISTIR's systems and carried experiments with selected scenarios. Although Flowmon is not a dedicated security tool for ICS, it was demonstrated that it can detect a large class of ICS anomalies according to the NISTIR 8219.

2. Environment

To evaluate the considered scenarios, we created a virtual environment for a typical ICS that consists of servers, hosts, and monitoring devices. The environment is created similarly to the system specified in the NISTIR document. The network topology is shown in Figure 1.

The environment is segmented to the following networks:

- System VLAN1 - contains HMI, the main interface for ICS operators and the controller station.
- System VLAN2 - contains Historian, OPC server and Open PLC host.
- LAN - contains Engineering workstation used to update, reconfigure and access the other hosts in the system. In the considered threat model, a possible attack can be executed from this internal network.
- WAN - represents the outside of the system. In the scenarios that include Internet hosts, these are located in WAN. Also the possible external attack can be executed from this segment.

All networks are interconnected using a single router device, which runs VyOS router operating system.

Flowmon Probe monitors communication in all networks. The networks connect devices using virtual switches. Virtual switches are configured to mirror all packets to Flowmon Probe, thus any communication within the system is visible to Flowmon Probe. In addition, the probe is also able to monitor the communication at the edge of the system.

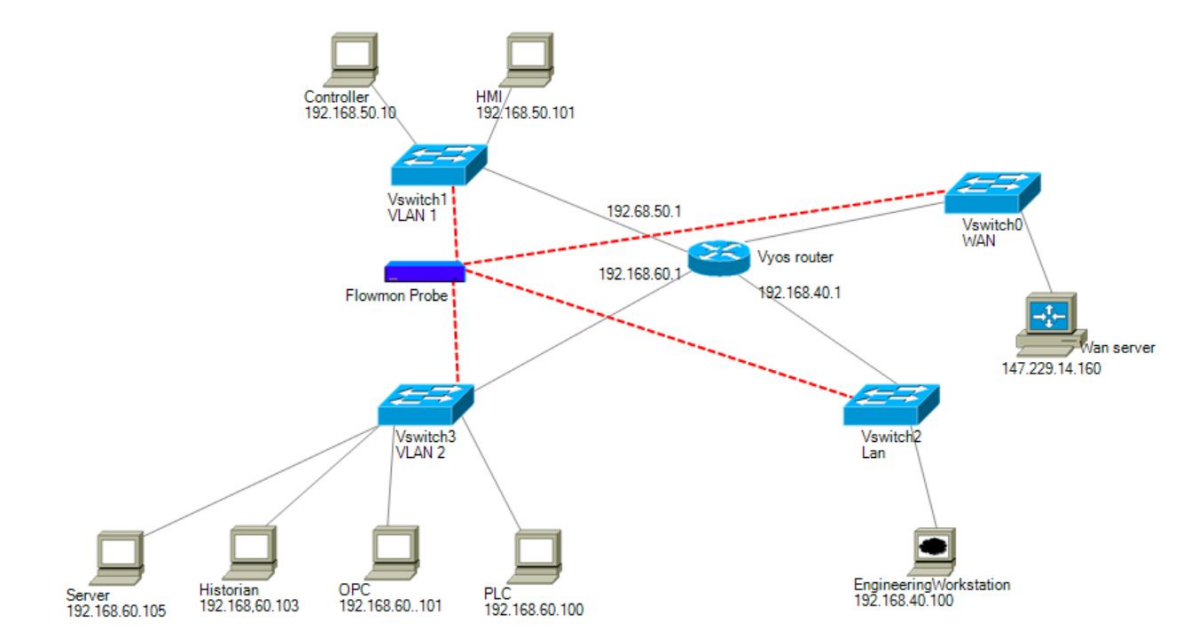


Figure 1: Network topology of ICS systems

3. Scenarios

We consider anomaly scenarios that include security threats detectable by network monitoring and security detection methods. The different classes of security threats are demonstrated, in particular:

- use of plaintext passwords
- user authentication failures
- new network devices
- abnormal network traffic between devices internet connectivity
- data exfiltration
- file transfers between devices
- denial of service (DoS)
- abnormal manufacturing system operations port scans/probes
- environmental changes

We have tested Flowmon tools in the selected scenarios from the NISTIR report. The NISTIR report contains four groups of scenarios. Each group demonstrates the capabilities of a selected commercially available tool. We give an overview of the three NISTIR groups as the last group is related to the PLC only. Each table consists of three columns from which the first two provide the reference number and the name of the scenario. The last column provides a section number for scenarios for which the Flowmon tool was tested.

The first group consists of scenarios that were tested and demonstrated using SilentDefense tools, which is a network monitoring tool for ICS. The list of all cases is as follows:

Ref	Name	Section
A.3.1	Unencrypted Passwords Are Used to Access a Networking Device	3.1
A.3.2	TCP Connection Requests Are Received from the Internet	-
A.3.3	Data Exfiltration Between ICS Devices via SMB	3.2
A.3.4	Data Exfiltration to the Internet via FTP	3.2
A.3.5	Unauthorized Device Is Connected to the Network	3.3
A.3.6	Loss of Communications with Modbus TCP Device	3.4
A.3.7	Brute-Force Password Attack Against an ICS Device	3.5
A.3.8	Invalid Credentials for Remote Access	3.6
A.3.9.	Unauthorized ICS Device Firmware Update	-

A.3.10	Unauthorized HMI Logic Modification	-
A.3.11	ICS Device Receives Diagnostic Modbus TCP Function Codes	-
A.3.12	ICS Device Receives Undefined Modbus TCP Function Codes	-
A.3.13	ICS Device Receives Malformed Modbus TCP Traffic	-
A.3.14	Illegal Memory Addresses of ICS Device Are Accessed	-
A.3.15	ICS Device Scanning Is Performed on the Network	3.8

We have tested the capability of Flowmon tools to detect the selected scenarios from this list. We have omitted cases that involves detection anomalies within Modbus protocol, because Flowmon currently does not offer deep analysis of Modbus traffic[1].

The second group of anomalies were specified to demonstrate Secure-NOK cybersecurity monitoring and detection system, which is tailored for industrial networks and control systems. The system involves agents installed on selected hosts of the system. Therefore it also offers functions that are outside of the capabilities of network monitoring tools. The set of scenarios is listed in the following table:

Ref	Name	Tested
B.3.1	Web Browser Is Used to Access the Internet	3.7
B.3.2	Data Exfiltration to the Internet via HTTP	3.2
B.3.3	Virus Test File Detected on Host	-
B.3.4	Host Scanning Is Performed on the Network	3.8
B.3.5	Port Scanning Is Performed on the Network	3.9
B.3.6	Unauthorized Installation of Software	-
B.3.7	Unauthorized Programmable Logic Controller Firmware Update	-
B.3.8	Unauthorized PLC Logic Download	-
B.3.9	Unauthorized PLC Logic Modification	-
B.3.10	Unauthorized Connection Is Established Between ICS Devices	-
B.3.11	Host-Based Firewall Is Disabled	-
B.3.12	Host-Based Anti-Virus Software Is Disabled	-

[1] The work on supporting MODBUS protocol analysis is currently in progress and will be provided in a future release of the tool.

B.3.13	Host Central Processing Unit Load Is Increased	-
B.3.14	Unauthorized Detachment of Keyboard to Host	-
B.3.15	Unauthorized Insertion of USB Storage Device	-

As it can be observed many of these cases are not detectable by network monitoring and relies on the installation of an agent to the monitored device. For this reason, we omit these cases in our experiments.

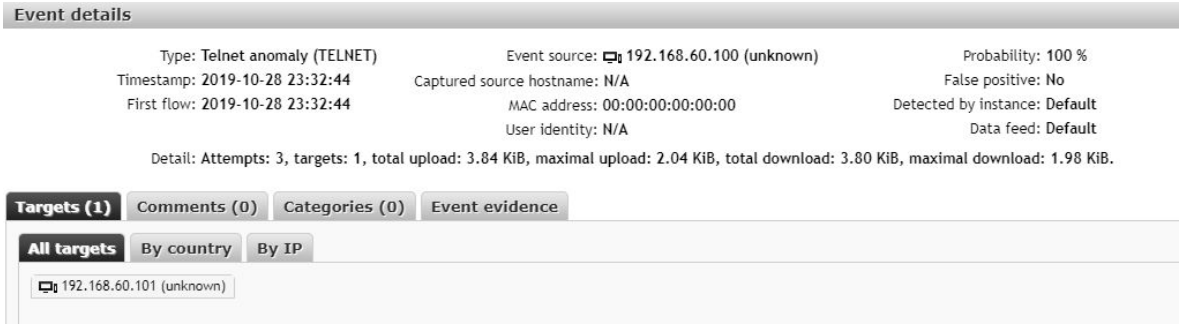
The last group of scenarios served to demonstrate the capabilities of the CyberX platform. The platform offers threat monitoring and asset discovery, combining a deep understanding of industrial protocols, devices, and applications with OT-specific behavioral analytics, threat intelligence, risk and vulnerability management, and automated threat modeling. The network-based anomaly detection method was demonstrated for the scenarios listed in the following table:

Ref	Name	Tested
C.3.1	Unencrypted Hypertext Transfer Protocol Credentials Are Detected	3.1
C.3.2	Unauthorized Secure Shell Session Is Established	3.11
C.3.3	Data Exfiltration to the Internet via DNS Tunneling	3.2
C.3.4	Data Exfiltration to the Internet via Secure Copy Protocol	3.2
C.3.5	Virus Test File Detected on Network	-
C.3.6	Unauthorized Device Is Connected to the Network	3.3
C.3.7	DoS Attack Is Executed Against the ICS Local Area Network	3.10
C.3.8	Data Exfiltration Between ICS Devices via User Datagram Protocol	3.2
C.3.9	Invalid Credentials Are Used to Access a Networking Device	3.6
C.3.10	Brute-Force Password Attack Against a Networking Device	3.5
C.3.11	Unauthorized PLC Logic Download	-
C.3.12	Unauthorized PLC Logic Update – CRS	-
C.3.13	Unauthorized PLC Logic Update – PCS	-
C.3.14	Undefined Modbus Function Codes Are Transmitted to the PLC	-
C.3.15	Unauthorized Ethernet/IP Scan of the Network	3.8

In the rest of this section, the detection scenarios are presented. Each scenario is introduced with its short description and the information on a Flowmon method used for detection. The screenshots from the Flowmon user interface provide some additional information on the way the Flowmon detects and reports the considered incident.

3.1. Unencrypted Passwords Are Used to Access a Networking Device

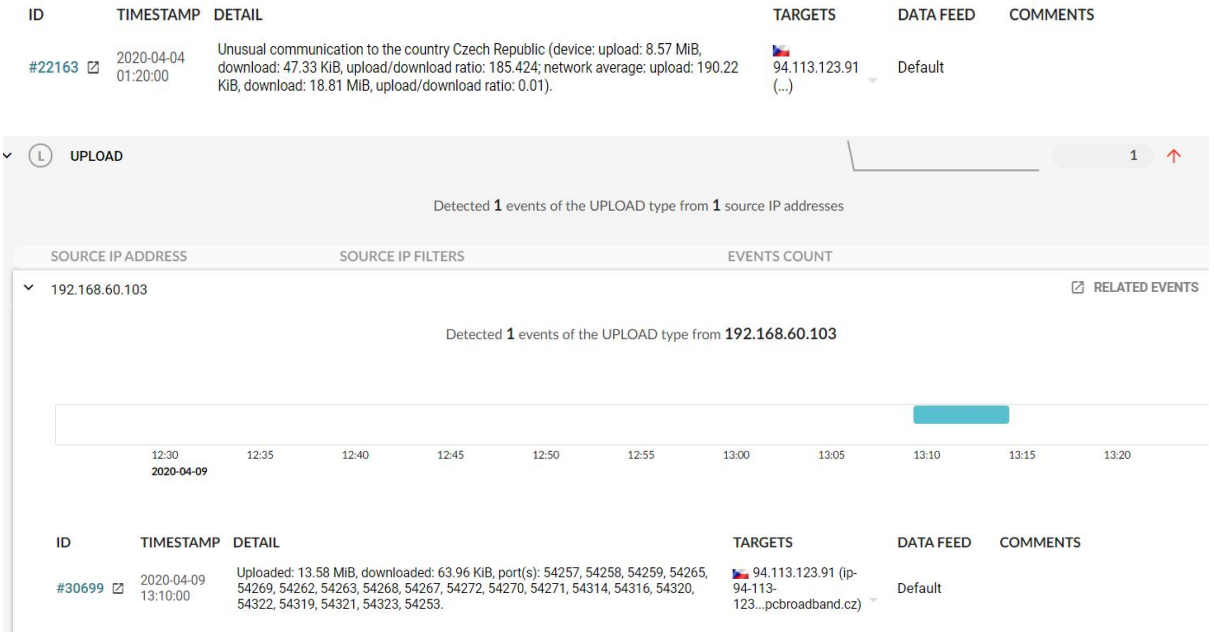
Sending plain passwords in the network is considered a security threat as it can be captured by the attacker and used for unauthorized access to protected systems. Among widely used communication protocols, the TELNET connections require authentication but do not provide protection for the transmitted passwords. This case is demonstrated by establishing a telnet connection between a device (TELNET client) in the VLAN2 and a device (TELNET server) in VLAN1.
The detection of this case corresponds to the detection of establishing TELNET connections. It can be done by defining a new alert in Flowmon Collector. If Flowmon ADS is deployed then the standard TELNET detection method informs about TELNET connections and thus the use of unencrypted passwords.



3.2. Data Exfiltration

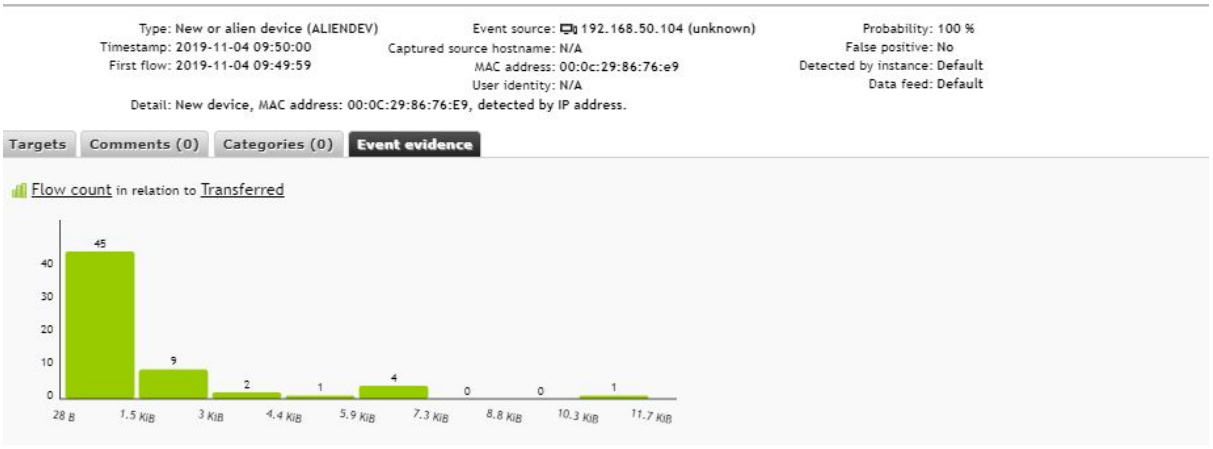
The goal of data exfiltration is to gather information about ICS systems possible as a part of a multistage attack. The FTP is a reliable protocol for file transfer that is commonly available on (ICS) hosts. The case considers the file transfer of different file types from the Historian machine (192.168.60.103) to a public IP address.
FTP application configuration: FTP server was set up with public internal routing 147.229.14.251, and created NAT rule on the virtual router for port forwarding to the FTP server in order to be reached from the public IP (ftp://147.229.14.251:21). several files were transferred to the external server.
Properly configured UPLOAD method can detect FTP transfer that may be related to data exfiltration. The configuration parameter determines the minimum amount of transferred data necessary for triggering the event. Moreover, this method can be also used to detect

transfer using any other protocol, not just FTP. Here the demonstration is provided for FTP transfer, but the similar approach can be used to detect transfers using other protocols too. FTP data upload was also recognized as unusual communication outside of the network by behavioral algorithm.



3.3. Unauthorized Device Is Connected to the Network

An environment of an industrial control system is rather fixed, with changes to the architecture only introduced during maintenance periods. Detection of a new device in an ICS network may indicate anomalous activity. As any unknown device represents a possible security risk, it is important to detect, locate and remove all unauthorized devices. Network-based anomaly detection can identify the unknown devices from the background traffic usually generated when the device is connected to the network.
Flowmon is able to detect unknown devices automatically by the ALIENDEV detection method.



It is also possible to inspect all flows of the unauthorized device as shown in the following figure.

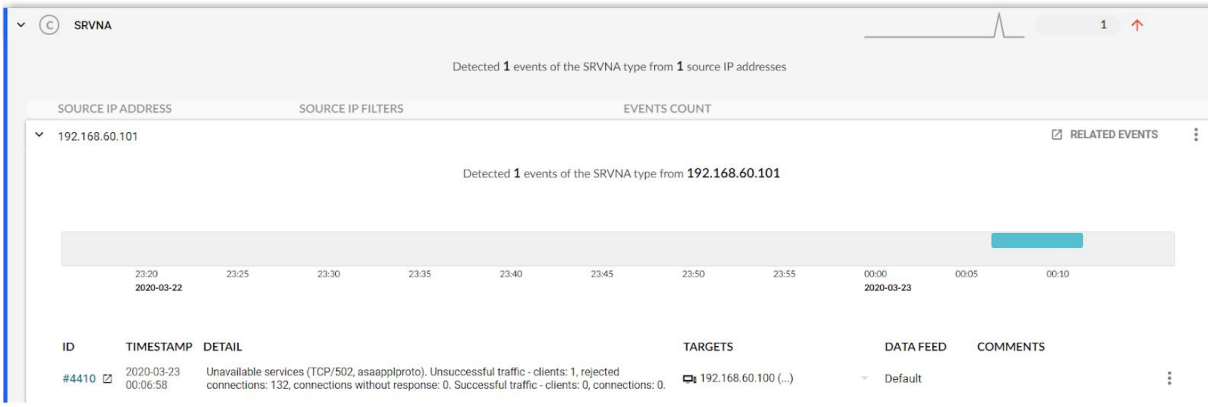
START TIME - FIRST SEEN	DURATION	PROTOCOL	SOURCE IP ADDRESS	SOURCE PORT	DESTINATION IP ADDRESS	DESTINATION PORT	TCP FLAGS	TOS	AVG RTT	AVG SRT	AVG JITTER	AVG DELAY
2019-11-04 09:49:59.851	0.104 s	UDP	192.168.50.104	55516	224.0.0.252	llmnr	.....	Best Effort & Default	N/A	N/A	N/A	N/A
2019-11-04 09:49:59.860	21.63 s	ARP	192.168.50.104	0	192.168.50.1	0	.....	Best Effort & Default	N/A	N/A	N/A	N/A
2019-11-04 09:49:59.874	12.626 s	UDP	192.168.50.104	62383	239.255.255.250	ws-discovery	.....	Best Effort & Default	N/A	N/A	N/A	N/A
2019-11-04 09:49:59.887	49.075 s	UDP	192.168.50.104	netbios-ns	192.168.50.255	netbios-ns	.....	Best Effort & Default	N/A	N/A	N/A	N/A
2019-11-04 09:50:00.086	21.933 s	UDP	192.168.50.104	54944	239.255.255.250	ssdp	.....	Best Effort & Default	N/A	N/A	N/A	N/A
2019-11-04 09:50:00.174	1.513 s	ARP	192.168.50.104	0	192.168.50.101	0	.....	Best Effort & Default	N/A	N/A	N/A	N/A

3.4. Loss of Communications with Modbus TCP Device

ICS during manufacturing operations requires high availability thus any connection failure of an ICS device that operates an important network service indicates anomalous activity and needs further investigation.

The anomaly is simulated by change of the filtering rules during the Modbus communication between the SCADA application and the OpenPlc program that causes to block all Modbus packets. Modbus uses TCP transfer with fixed server port 502. The firewall replies with a TCP reset for each incoming packet or connection request, which appears as if the Modbus server had terminated and the TCP socket was closed.

Flowmon provides the “service not available” detection method being able to detect the situation when it is not possible to establish communication with the required services.



3.5. Brute Force Password Attack

The ICS devices can be protected by login based authentication. The use of a weak password or leaving the default password makes the system vulnerable to a password guessing attack. The brute force password attack is possible against every system that does not limit the number of login attempts. It is usually based on the use of a list of leaked passwords that can be downloaded from the Internet[2].

The three different targets commonly occurring in the ICS environments have been tested:

- Telnet service
- FTP service
- HTTP service

The target of the attacks is the Historian machine that runs Windows Server 2008 with TELNET, FTP and HTTP services configured. All these services are password-protected, however, the server does not implement any other security measures, e.g., limiting the rate of authentication attempts, the scope of addresses of clients, etc.

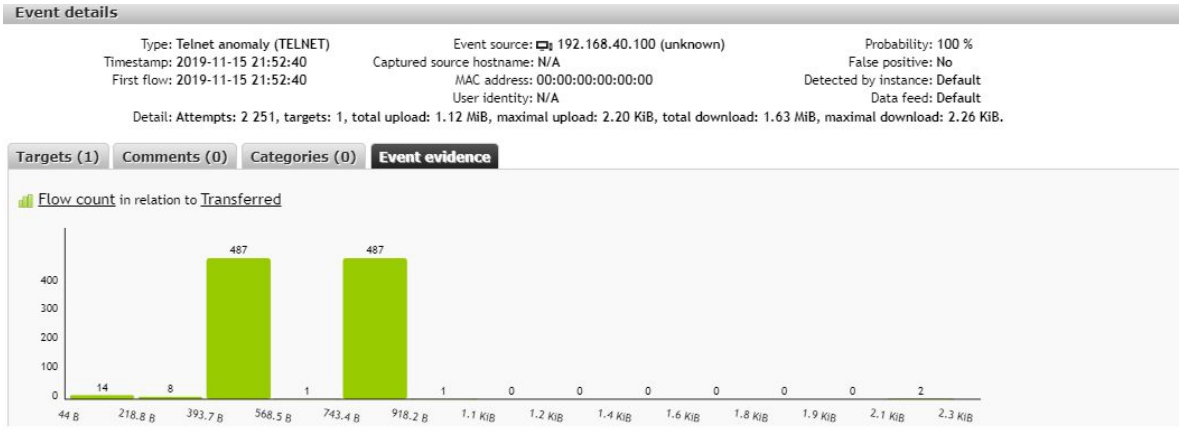
Telnet

This activity was demonstrated by executing NMAP telnet brute force password guessing from the engineering workstation (192.168.40.100) in the LAN segment targeting the Historian server (192.168.60.111) in VLAN1, which uses Telnet service for remote configurations. The service is password protected but does not limit the number of authentication attempts. NMAP tried 45000 attempts within 493 seconds.

```
nmap –p 23 –script telnet-brute 192.168.60.111
```

Flowmon ADS was able to detect telnet anomaly using the TELNET detection method. An event is reported to the users. In the Event evidence window, it can be seen that a large number of TELNET connections were created, which may indicate the password attack.

[2] Pwned Passwords is a web site that collects more than half of billion passwords exposed in various data breaches. https://haveibeenpwned.com/Passwords

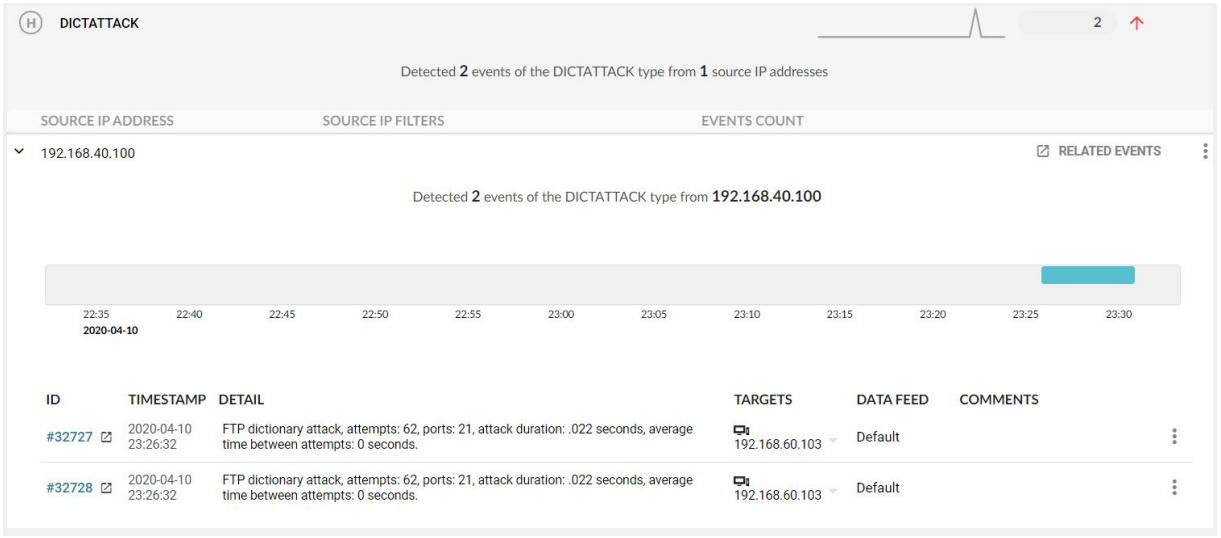


FTP

The approach of this attack is the same in the previous case. This time the target is an FTP server running on the Historian server (192.168.60.103). The attacker executes operation from the engineering workstation (192.168.40.100) using the following NMAP command:

```
nmap –p 23 –script ftp-brute 192.168.60.103
```

NMAP executes 50000 unsuccessful authentication attempts within 195 seconds. Flowmon is able to identify the activity as DICTATTACK anomaly:

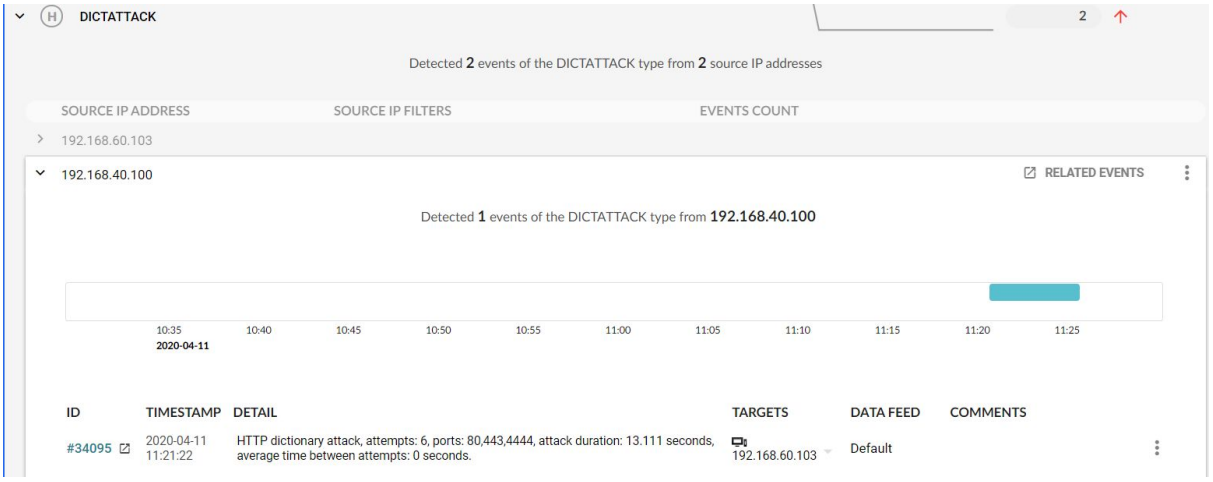


HTTP

The last tested attack is against the HTTP server that protects content using basic authentication. Again the service is located on the Historian host and NMAP tool is used to execute the attack:

```
nmap –p 80 –script http-brute 192.168.60.103
```

NMAP generates attempts to discover the credentials. Flowmon is able the accurately identify this activity as DICTATTACK event:

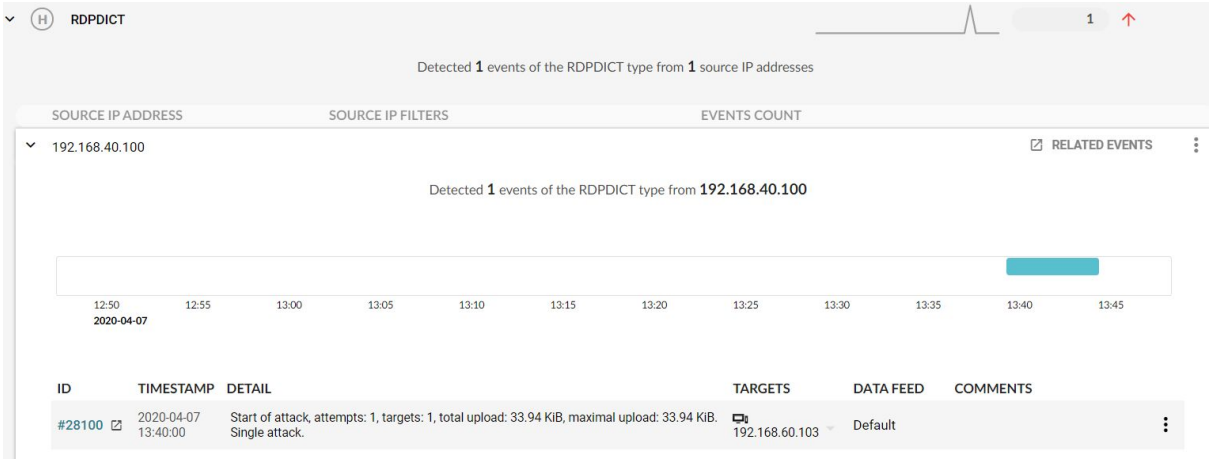


For all common ICS services that can be a victim of a brute force password cracking attack, Flowmon demonstrated the detection ability.

3.6. Invalid Credentials for Remote Access

Remote access to Microsoft Windows systems allows operators and administrators to remotely manage services of different ICS hosts. For an attacker, gaining remote access to ICS nodes is attractive. It is important to monitor authentication failures to detect possible occurrences of password attacks.

The HMI host is one of the possible computers with remote desktop service enabled. In this case, several attempts to connect to the remote service running on the HMI host are performed. To discover the attack, the FLOWMON offers standard method RDPDICT:

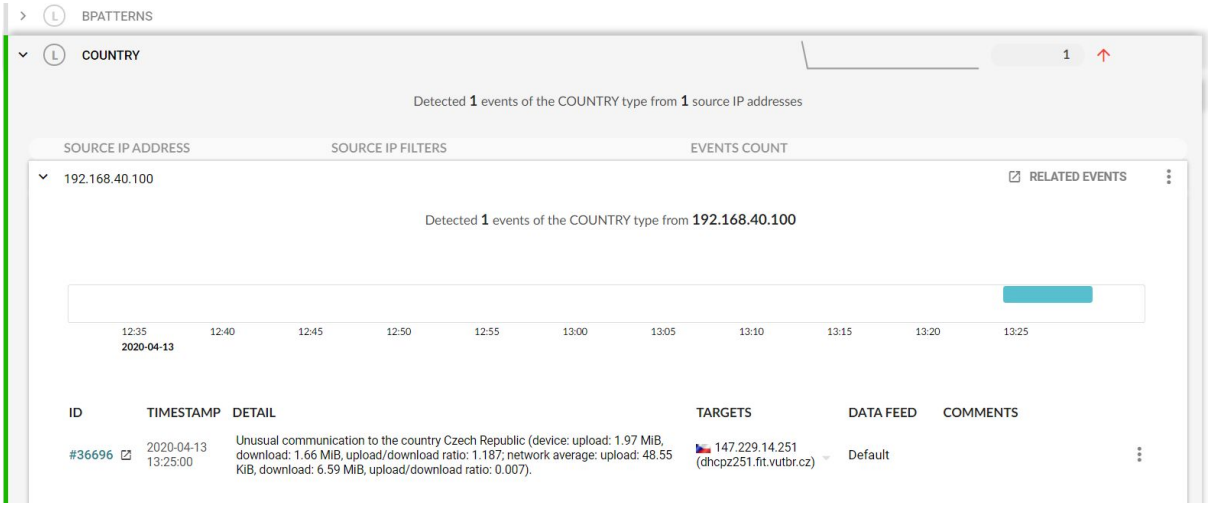


3.7. A Web Browser Is Used to Access the Internet

Internet-accessible devices are vulnerable as they represent a possible entry point for malware. Internet connections can also be used for data exfiltration. Detecting unauthorized connections to the Internet is important to mitigate security risks.

To demonstrate this case, an HTTP server was installed and configured on a host with internally routed public IP (147.229.14.251). The Internet Explorer web browser was used to connect to a web page, from the engineering workstation (192.168.40.100) to the configured HTTP server.

Flowmon detects the anomaly automatically by the COUNTRY method:



3.8. Host Scanning

Host scanning is a method for discovering active devices in the network. It can be used by the attacker in the reconnaissance stage of an attack.

Host scanning activity is executed from the engineering workstation, in order to discover hosts in VLAN2 , and VLAN1 segments. NMAP tool has a script to automatically perform host scanning:

- To detect all possible IP address within the given network segment using ICMP ping mechanism can be executed as follows:

```
nmap 192.168.60.0/24
```

- To detect host in the given network segment by using TCP protocol can be executed as follows:

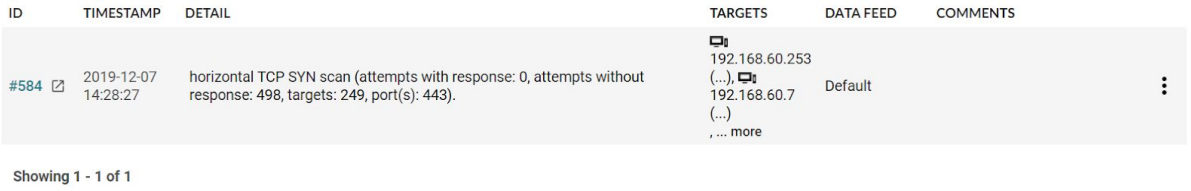
```
nmap -sP 192.168.60.*
```

Flowmon ADS is able to detect various types of Host Scanning activities as show in the following screenshots:

- The detection of ICMP-based scan:

ID	TIMESTAMP	DETAIL	TARGETS	DATA FEED	COMMENTS
#586	2019-12-07 14:25:00	ICMP scan was detected. Hosts scanned: 256.	192.168.60.0 (...), 192.168.60.1 (...) , ... more	Default	

- The detection of TCP-based host scan:



ID	TIMESTAMP	DETAIL	TARGETS	DATA FEED	COMMENTS
#584	2019-12-07 14:28:27	horizontal TCP SYN scan (attempts with response: 0, attempts without response: 498, targets: 249, port(s): 443).	192.168.60.253 (...), 192.168.60.7 (...) , ... more	Default	

Showing 1 - 1 of 1

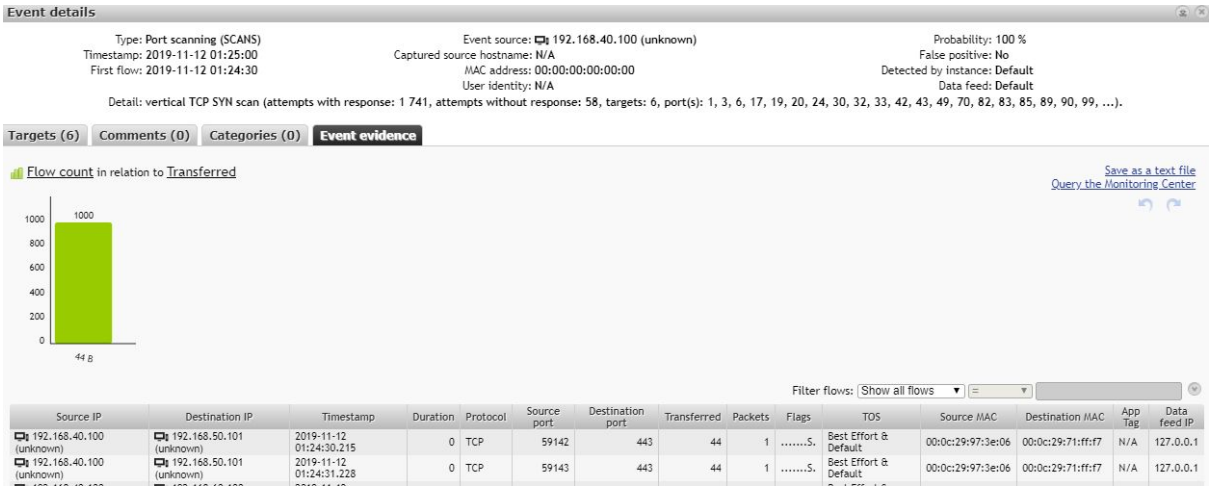
3.9. Port Scanning

The port scan is used for detecting active service on a target host. The performs this type of activity during the reconnaissance stage to list all services. The next step is usually to apply known exploits to identified services. If a service is vulnerable to the exploit the attacker can use it for unauthorized access to the system or attack the service. While port scanning can be a legitimate activity of monitoring and security tools, its occurrence should be detected and reported to the administrators.

This scenario is implemented using NMAP application which has a command to automatically scan all ports in the given network segment. The NMAP tool is used on Engineering Workstation to perform port scanning of host in VLAN2 segments:

```
nmap -p  1-65535 192.168.60.0/24
```

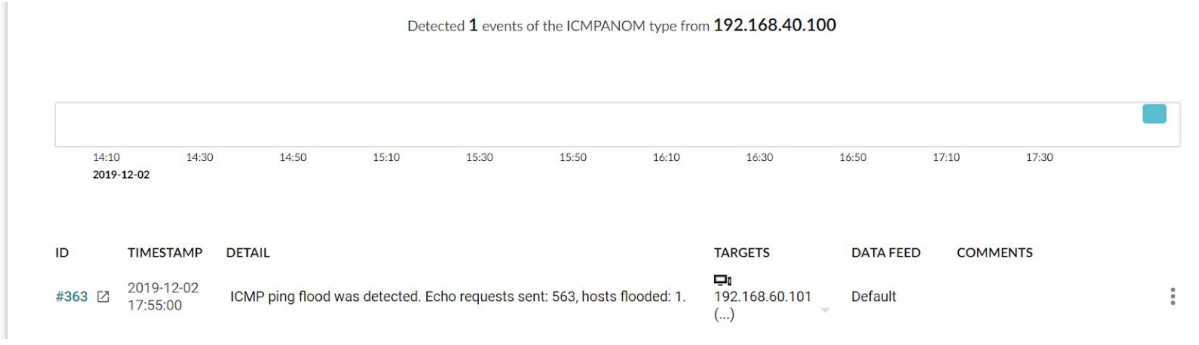
Flowmon ADS is able to automatically detect Port Scanning activities as show in the following output:



3.10. Denial of Service attack

The aim of the denial of service attack is to overwhelm the victim device. It then cannot serve legitimate requests which degrade the functionality of the system. In the ICS environment, this type of attack can have serious consequences. The ICS devices are vulnerable even to a simple form of DoS attacks as they usually do not have spare computation power necessary to withstand it.

To demonstrate this attack, the engineering station uses ICMP flooding against the OPC server. This activity was detected by Flowmon using the default configuration and detection modules.

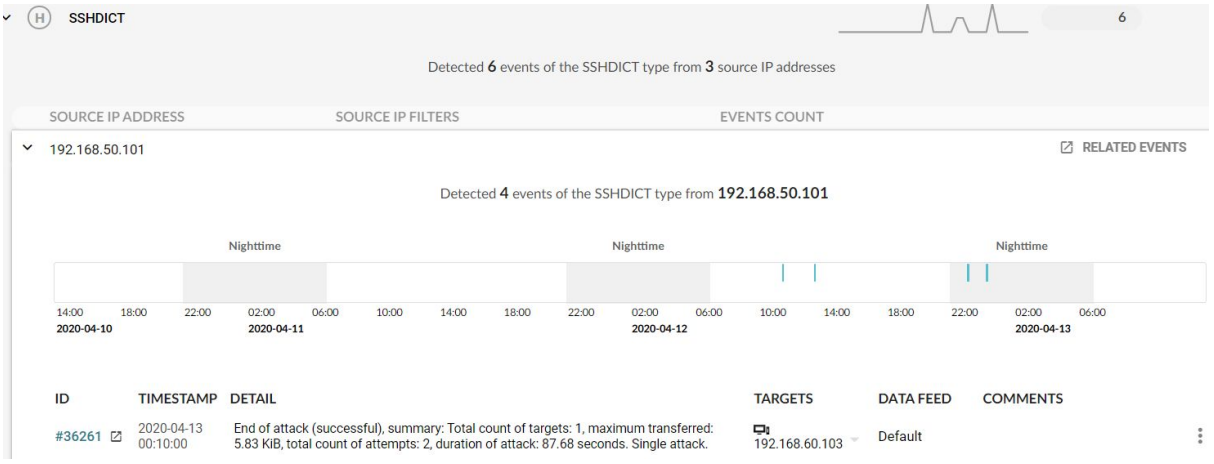


3.11. Unauthorized Secure Shell Session

A Secure Shell (SSH) session is a secure connection for remotely control of the target host. However, unauthorized SSH sessions with internet-based servers could indicate malicious activity. It is, therefore, necessary to identify all unauthorized SSH sessions to prevent malicious activities within the ICS environment.

The OpenSSH suite was installed and configured on an internet-based server. The open-source SSH client PuTTY was used to establish a connection with the SSH service from OPC workstation to the internet-based server emulated as host with internal routed public ip (147.229.14.251).

To detect unauthorized SSH connections, the standard SSHDICT detector is used.



4. Summary

The goal of this report was to demonstrate the capabilities of the Flowmon Anomaly Detection System (ADS) to strengthen the cybersecurity of the ICS. The Flowmon ADS is a security solution that uses anomaly detection techniques to detect threats hidden in the network traffic. It complements other security tools and creates a multi-layered protection system. We have shown that the Flowmon ADS techniques can be considered as a key security component for the protection of industrial networks. We have employed security scenarios from NISTIR 8219 to illustrate the detection methods and to provide a better understanding of the detection capabilities of the Flowmon ADS in ICS network environments.

References

1. “Framework for improving critical infrastructure cybersecurity,” NIST, Gaithersburg, MD, Apr. 16, 2018 [Online]. Available: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11
2. “Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection”, NIST, Gaithersburg, MD, Nov. 06, 2018 [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf