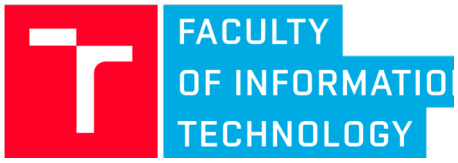
Study on visual representation of IoT diagnostic information

Technical Report, version 1.0

Matěj Grégr



Technical Report no. FIT-TR-2019-02

Faculty of Information Technology
Brno University of Technology
Brno, Czech Republic

October, 2019

Abstract

Monitoring of Internet of Things (IoT) networks can be a challenging task as traditional monitoring approaches often lack sufficient visibility of IoT communication. The study examines the visualization of diagnostic IoT information in current monitoring systems and evaluated user experience by trying to find out cybersecurity incidents detected by behavior anomaly detection systems.

Table of Contents

1 Introduction

Monitoring of Internet of Things (IoT) networks can be a challenging task as traditional monitoring approaches often lack of sufficient visibility of IoT communication. Furthermore, current monitoring systems are usually optimized to gather, collect, and visualize traditional networking properties, such as the amount of transferred data, available free disk space, system uptime, CPU usage, etc. However, this kind of information can be either meaningless to gather from IoT nodes or not possible to obtain at all. IoT network monitoring should provide different views on data than traditional network monitoring and offers more benefits to the operator of the IoT network. For example, it is maybe not necessary to gather CPU usage of every sensor in a large sensor network as there is probably no value for the operator to see this information. However, it can be a benefit for the operator to see e.g., battery duration of sensors aggregated in a map.

This study focuses on current monitoring systems and analyses their dashboards and visualizations. The aim of this study is to try to provide some guidance on how we should visually represent IoT diagnostic data.

Several different definitions of the IoT network exists. Some view IoT devices as every device with an IP address connected to the Internet or a private network. For some, the IoT is a network with different kinds of sensors, detectors, etc. There are also Industrial Control System (ICS), supervisory control and data acquisition (SCADA) systems often consider as an IoT network as well. Unfortunately, these networks require different approaches for monitoring. ICS and SCADA networks are usually stable with some large, fixed grid units that communicate with a controller on a regular basis. Sensors networks are, on the other hand, very dynamic, full-meshed networks without a central controller or regular communication. All these pieces of information should be taken into consideration for data visualization.

2 IoT monitoring systems

There are several companies, such as Flowmon, Claroty, Spiceworks, Dynatrace, relayr., Pandorafms, Sentryo, and others, offering either open source or commercial products for IoT monitoring and traffic analysis. Every company typically provides its platform, which is a web page application in most cases. The web application provides a user with several dashboards that present and visualize available data. It depends on every platform and product which protocols can analyze and visualize, but the focus is mainly aimed at Industrial IoT networks and protocols.
Only scarce information about these platforms and monitoring software exists as they are usually not publicly available. Thus, it is challenging to provide a comprehensive study of available visualizations and dashboards — this section summaries our findings from available whitepapers and public information.
Claroty[1] is a security research company founded by researches with knowledge gained from both industry careers and work within a special cyber unit of the Israeli Defense Force. The company offers The Claroty platform and claims that the platform should address specific challenges associated with cybersecurity in the industrial environment. Furthermore, the

company claims that the platform provides (i) more accurate records of installed systems, (ii) improves collaboration between internal and external operations and support groups, and (iii) provides more rigorous management of change and configuration control discipline. The platform should support a variety of protocols used for communications between system elements such as MODBUS or other more obscure or proprietary, such as protocols used by leading control systems suppliers (e.g., Siemens, Rockwell, Honeywell, Emerson, ABB, Yokogawa, Schneider Electric, GE, and Mitsubishi). The platform offers several views presented in the following pictures [1], larger pictures are shown in Appendix A.

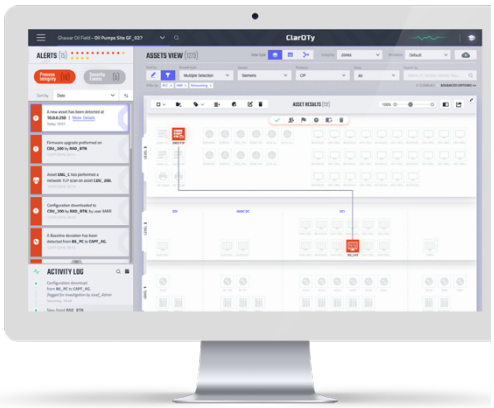


Figure 1: Platform dashboard

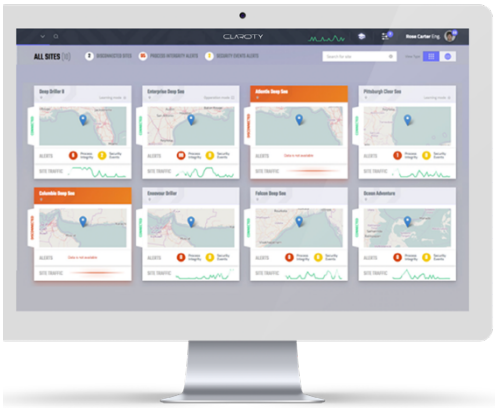


Figure 2: Multi System Display

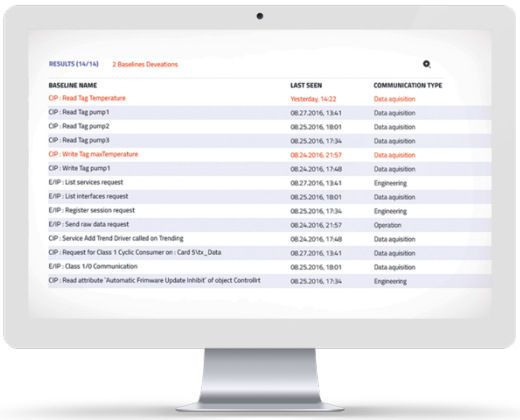


Figure 2: Alert grouping

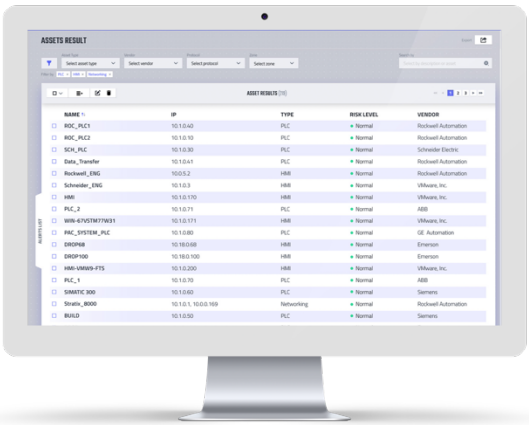


Figure 4: Asset Discovery

According to analyzed resources, the Claroty platform offers several visualization views and dashboards to present *Assets* (Fig. 4) available in the IoT network and *Alerts* (Fig. 3) detected from various Claroty sensors. Together with Cisco ISE, it should be possible to use information about asset data to create new policies that are fine-tuned for industrial networks [2]. Claroty uses SPAN monitor port for traffic analysis, meaning that sensors are able to analyze the whole packet.

To summarize, the Claroty platform seems to offer several dashboards similar to other IDS/IPS systems, but sensors are more focused on IoT industrial protocols.

PandoraFMS (Flexible Monitoring System) is offered as All-in-One monitoring software by Spanish company Ártica ST. The product claims support for several protocols, such as ZigBee, MQTT, CoAP, DDS, NFC, AMQP, RFID, Z Wave, and others. Traditional industrial protocols such as Modbus and SNMP are supported as well. Pandora FMS uses either agents installed on a system to extract information and report back to Pandora FMS' server, or polling monitoring, e.g., using SNMP, ICMP or TCP/UDP probes. The web application offers several dashboards with charts of long term gathered data (see Figure 5) or a map of monitored devices (see Figure 6), larger figures can be found in Appendix C.
To summarize, the system offers similar monitoring options as e.g., to Zabbix, Nagios, or Icinga. Several IoT protocols should be supported. The system uses mainly agents for monitoring. If an operating system offers a possibility to install an agent, it can provide valuable information that cannot be obtained via passive monitoring. However, running an agent on an IoT sensor is often not possible or feasible and can be a limitation of the system.

Figure 5: PandoraFMS dashboard

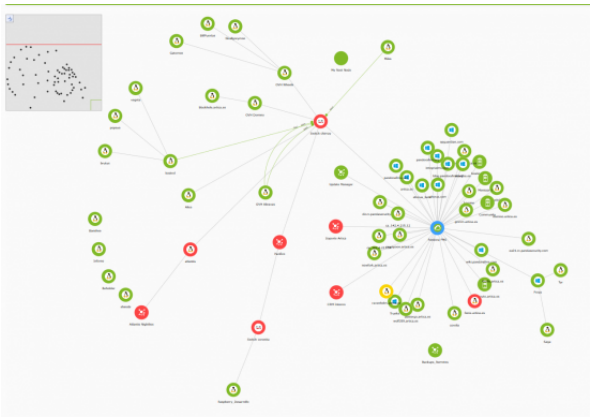
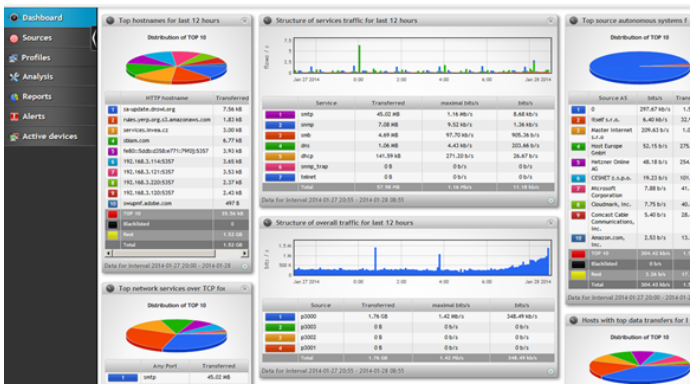
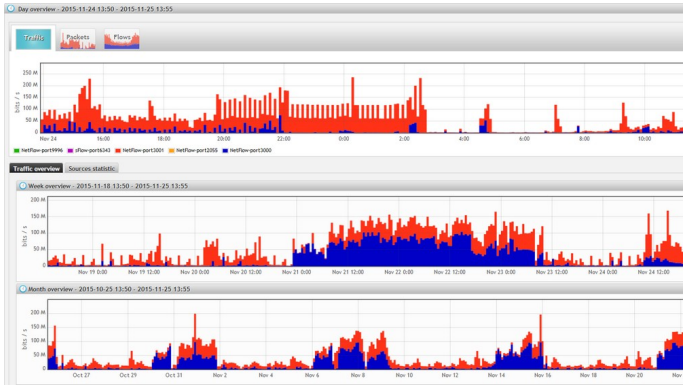


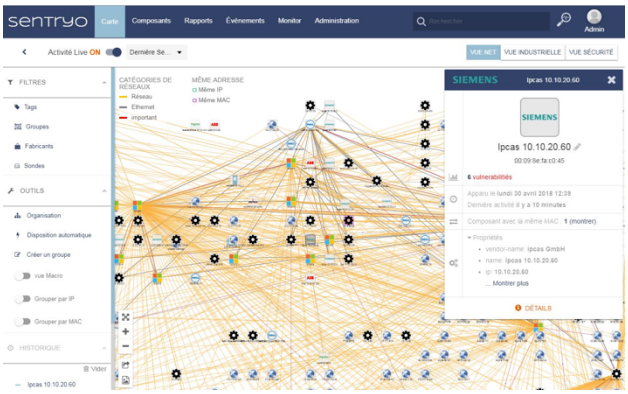
Figure 6: Map of monitored devices

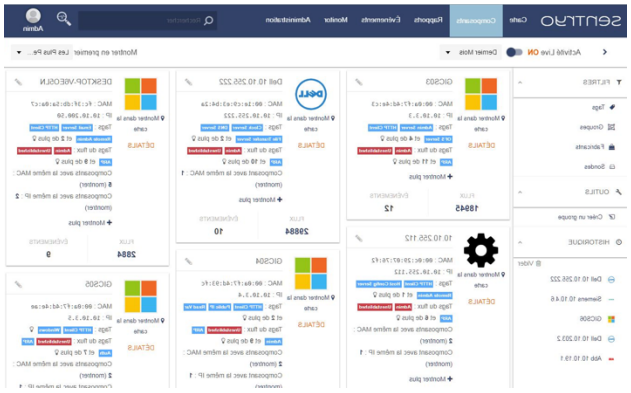
Flowmon offers high-performance network monitoring technology based on NetFlow/IPFIX. The monitoring uses standalone probes exporting IPFIX data to a collector. The collector can provide a broad range of additional detection applications, such as DDoS mitigation, anomaly behavior detection, Network Performance Monitoring, or IoT monitoring. Several IoT protocols are supported, such as CoAP, DLMS, IEC61850, IEC-104, or MMS. Traditional NetFLow/IPFIX monitoring supports only accounting on IP and transport layers. To avoid the limitation, Flowmon extended IPFIX protocol with IoT metadata to provide a global view on the whole IoT network and its communication. Collector presents gathered data using several dashboards, as seen in the following figures. An operator can create some of the dashboards according to his/her needs.





Sentryo offers CyberVision solution platform that gives control engineers visibility over equipment connected to their industrial networks. The system can identify vulnerabilities, analyze alarms, and control the security of the ICS infrastructure. The company claims that the system provides threat detection and uses artificial intelligence and machine learning algorithms. Information is gathered from edge sensors that listen to the industrial network. Deep Packet Inspection (DPI) is used for parsing the standard IP protocols as well as the proprietary industrial protocols. The supported protocols are not listed in Sentryo documentation, but the system claims that it is possible to integrate the system with major industrial companies, such as Siemens, ABB, Honeywell, etc. The system offers several dashboards showing discovered assets, communication maps between IoT devices or alerts. Examples of these dashboards are displayed in the following figures, larger figures can be found in Appendix B.





3 Evaluation of IoT diagnostic information

The previous section described several monitoring platforms offering systems or applications able to monitor IoT data. As discussed in the Introduction, several definitions of IoT networks exist. For the rest of this study, we focus on Industry IoT networks (IIoT) and communication in Industrial Control Systems (ICS) and supervisory control and data acquisition systems (SCADA) to increase the visibility of ICS communication and prevent cyber-attacks on smart grids. A monitoring system should offer enough visibility for an ICS/SCADA network operator to easy a troubleshooting process or detection of a security incident.

To evaluate a monitoring system properly, we should understand which data is gathered by the system and which information is available. A benefit of a monitoring system that uses DPI is that the system can extract more pieces of information that are missing in a system collection only flow metadata. A drawback of such a system is that it is much more CPU intensive, and a large data storage is needed. The compromise can be a system that uses enriched metadata. That is, flow data with additional information. The study will evaluate the Flowmon system, that uses enriched IPFIX flow records.

As described in the NIST report Securing Manufacturing Industrial Control Systems [3], ICS systems are used in many industries to monitor and control physical processes. As ICS systems continue to adopt connectivity and remote access capabilities, ICS becomes more vulnerable to cybersecurity threats. Monitoring systems should offer a set of detection mechanisms and capabilities either in the form of behavioral anomaly detection or other mechanisms to easy the process for an operator and to increase cybersecurity in ICS environments.

The NIST study demonstrates behavior anomaly detection techniques that businesses can implement and use to strengthen the ICS cybersecurity. Three different detection methods were used: network-based, agent-based, and operational historian/sensor-based. For this study, network-based and operational historian based methods are relevant. These methods can work with flow metadata, and their findings can be visualized in a dashboard or a graph. We selected several anomaly detection examples from the study [3] and showed how they could be visualized using the Flowmon Monitoring Center.

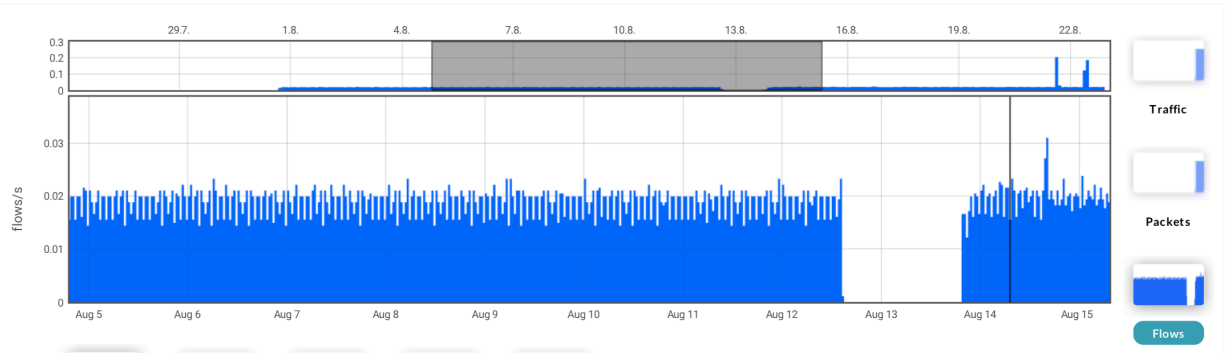
Example 1: Loss of Communications with ICS Device

ICS devices should exhibit high availability. If an ICS device hosting a network service becomes unavailable, it may be a sign of anomalous activity and should be investigated.

The NIST study presents this anomaly as an event listed in a dashboard - see the following Figure.

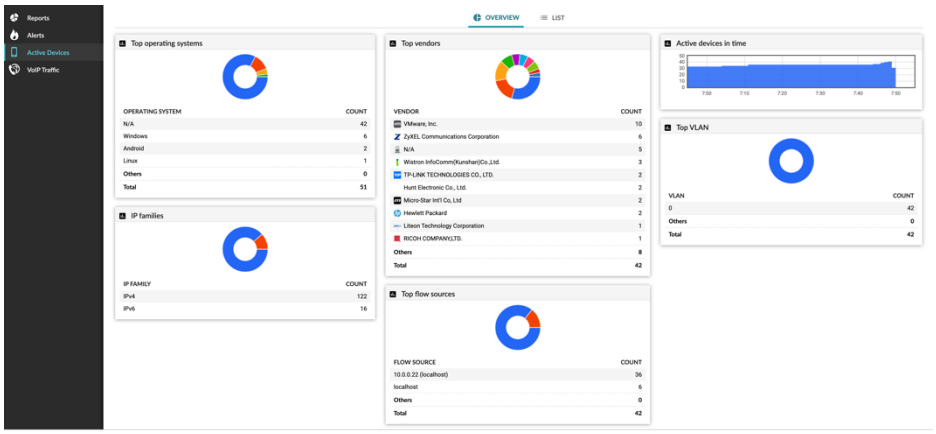
	Timestamp	Event name(s)	Sensor	Engine	Profile	Status	Severity	Source IP	Destination IP	Dest. Port	L7 Proto
			(No	(N	(Not s	Not ana	(No				(Not set)
☐	Dec 11, 2017 11:26:01	MODBUS/TCP device ...	Local	Indus...	-	Not analyzed	H	-	192.168.1.101 (...	-	MODBUSTCP
☐	Dec 11, 2017 11:26:00	Device with many faile...	Local	Indus...	-	Not analyzed	L	192.168.0.98 (h...	192.168.1.101 (...	502 (TCP)	-

The lost of communication can also be presented as a graph. For example, the following figure shows how lost in communication can be obtained and interpreted via Flowmon GUI. The figure shows IEC104 traffic seen by a probe during a time interval. The IEC104 traffic exhibit similar and stable flow pattern, as IEC104 device scan and gather information every few milliseconds. Thus, if there is communication loss, it's immediately visible to an ICS operator, and he/she can investigate further why there is such a loss. It's possible to display the communication pattern for every device. However, the process cannot be easily automatized in Flowmon GUI, and operator work is needed. We suggest that a possibility to display such a communication pattern for each device in a selected network should be addressed in a future release.

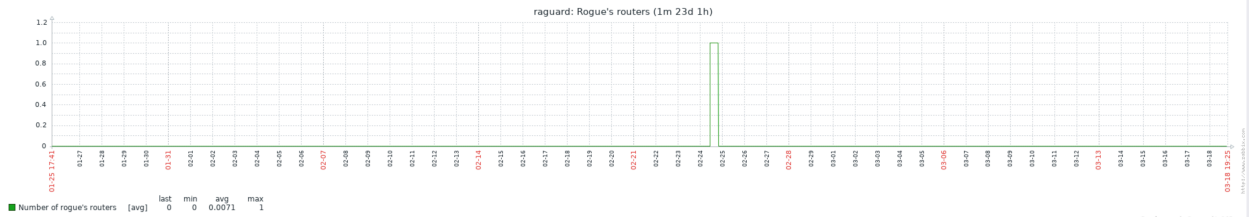


Example 2: ICS Device Scanning Is Performed on the Network

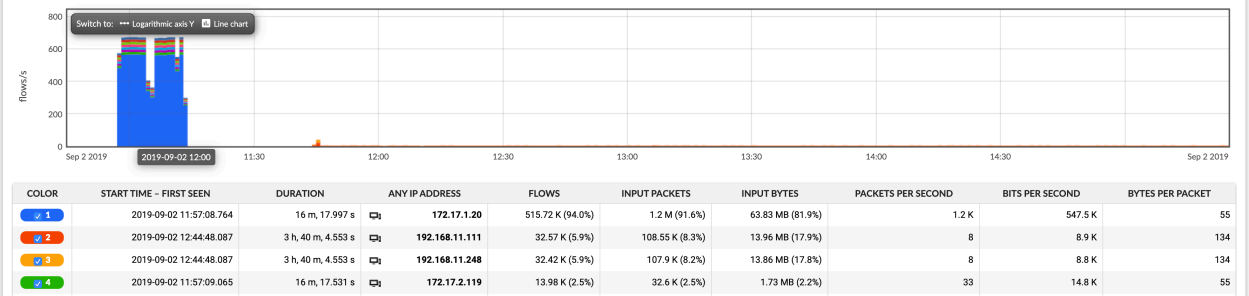
During the reconnaissance phase, an attacker may attempt to locate vulnerable devices in an ICS network and will likely probe for ICS-specific services. Once a vulnerable service is discovered, an attacker may attempt to exploit that service.
This cyberattack can be visualized in several different ways. One approach is to use some form of asset detection. If the scan is run from a device not previously connected in the ICS network, the monitoring system should visualize such a node and inform an operator. Flowmon GUI supports Active device detection that offers a dashboard that can be used for finding such anomaly. An example of such a dashboard is in the following figure.



The active device dashboard offers several top statistics, e.g., top vendors, operating systems, and VLAN. It is possible to see a number of active devices on a long term chart. Advanced filtration can be used as well. Unfortunately, the dashboard lacks a view offering the last devices detected during the selected time period. The system can be queried for such information, but a view is missing. For example, the system could show a chart with new devices for a selected time period. A similar graph is shown in the following figure. The presented data are from an internal monitoring system that watches rogue routers connected in a network. It's visible from the graph that there was a new device connected for a short period of time. As ICS networks are rather stable with the same amount of nodes and controllers, such information presented by the ICS monitoring system could be convenient.



Another approach is to watch the number of flows per device. To be able to find all active devices in a network, the attacker must create a large number of flows during the attack. As ICS devices use a rather stable amount of flows per device, it should be possible for an operator to see a higher amount of flows from an attacker's machine. The Flowmon GUI can be queried for such information, as shown in the following figure.



COLOR	START TIME – FIRST SEEN	DURATION	ANY IP ADDRESS	FLOWS	INPUT PACKETS	INPUT BYTES	PACKETS PER SECOND	BITS PER SECOND	BYTES PER PACKET
1	2019-09-02 11:57:08.764	16 m, 17.997 s	**172.17.1.20**	515.72 K (94.0%)	1.2 M (91.6%)	63.83 MB (81.9%)	1.2 K	547.5 K	55
2	2019-09-02 12:44:48.087	3 h, 40 m, 4.553 s	**192.168.11.111**	32.57 K (5.9%)	108.55 K (8.3%)	13.96 MB (17.9%)	8	8.9 K	134
3	2019-09-02 12:44:48.087	3 h, 40 m, 4.553 s	**192.168.11.248**	32.42 K (5.9%)	107.9 K (8.2%)	13.86 MB (17.8%)	8	8.8 K	134
4	2019-09-02 11:57:09.065	16 m, 17.531 s	**172.17.2.119**	13.98 K (2.5%)	32.6 K (2.5%)	1.73 MB (2.2%)	33	14.8 K	55

The figure shows that there is a higher number of flows from a specific machine - 172.17.1.20 during a time period. It is possible to either use advanced analysis to get the result or set up a profile that watches selected nodes. A dashboard showing the flow/s statistic per device without a need to create a specific configuration per device would help tremendously.

Summary

This study examines several monitoring platforms supporting IoT monitoring such as Flowmon, Claroty, Pandorafms, and Sentryo. Each of these platforms supports several different IoT protocols with a focus mainly on industrial protocols. We used the NIST report as an example of several cybersecurity attacks that can happen in the ICS network. We evaluate the monitoring systems, to find out if the monitoring platforms can be used to visualize cybersecurity threats in ICS networks. Originally these platforms were usually designed for standard IP network monitoring. That means dashboards, charts, and other data visualizations don't necessarily support IIoT specific use cases. However, with small modifications, these systems can be used to query IIoT specific information and visualize them.

References

1. Eric C. Cosman, Claroty - A New Platform For OT Cybersecurity, whitepaper, [October 2019]
2. Claroty Ltd., Claroty Continuous Thread Detection, [online], available at: https://developer.cisco.com/ecosystem/spp/solutions/171260/ [October 2019]
3. McCarthy, James, et al. Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection. No. NIST Internal or Interagency Report (NISTIR) 8219. National Institute of Standards and Technology, 2018.

Appendix A: Claroty dashboards

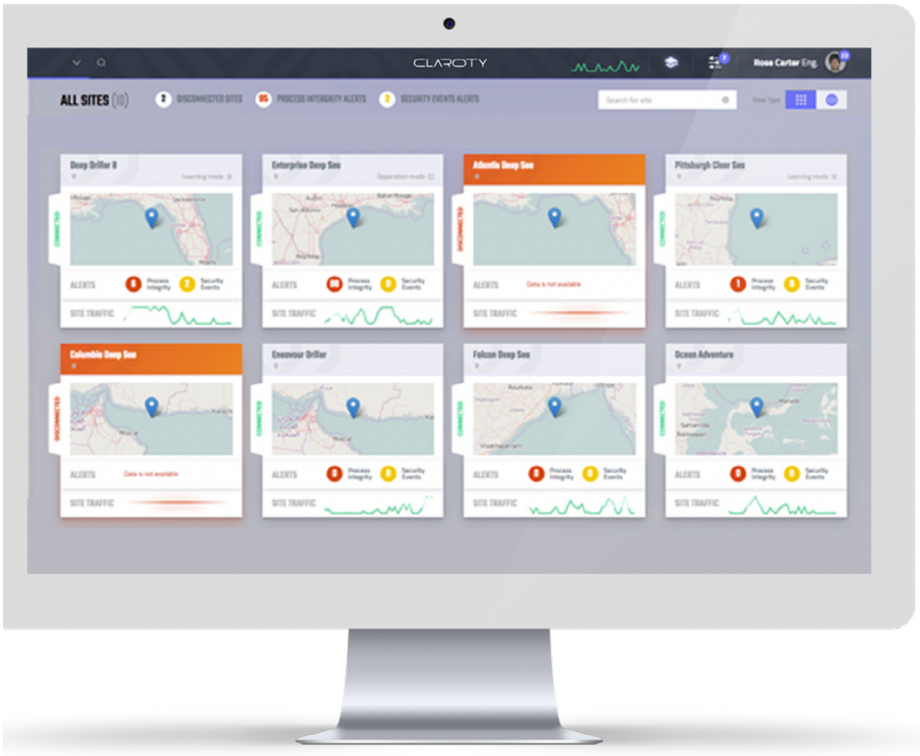


Figure 3: Central management

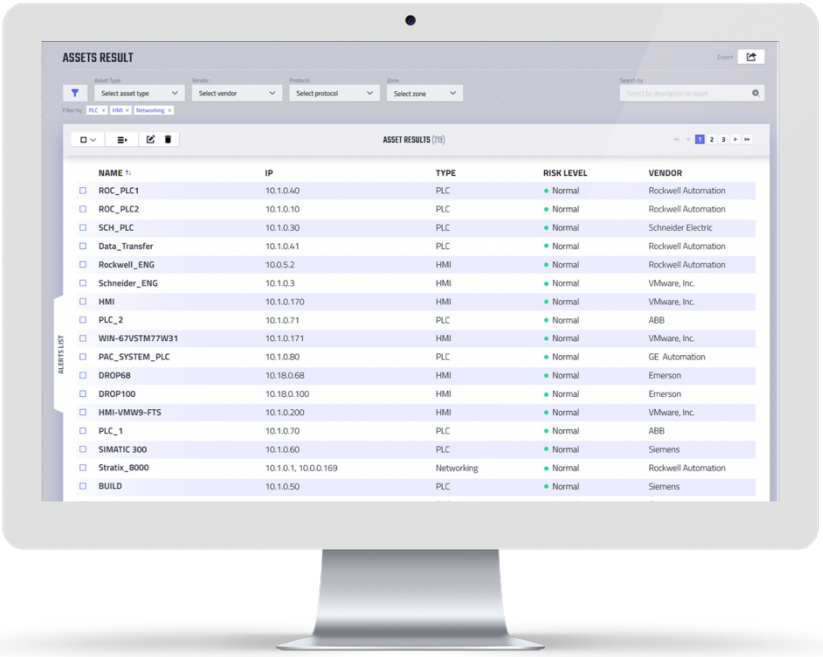
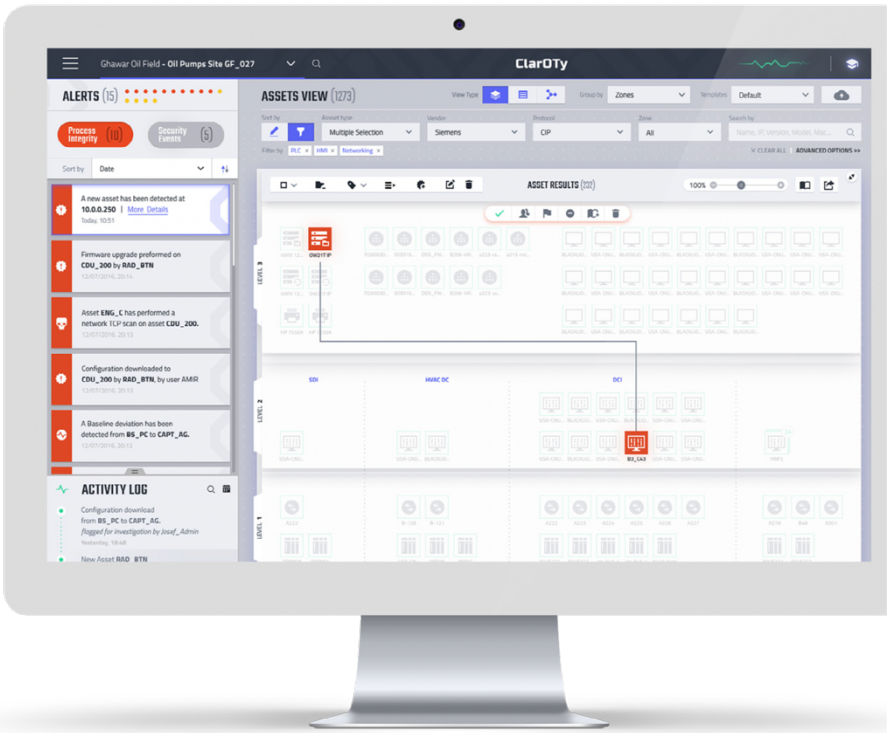
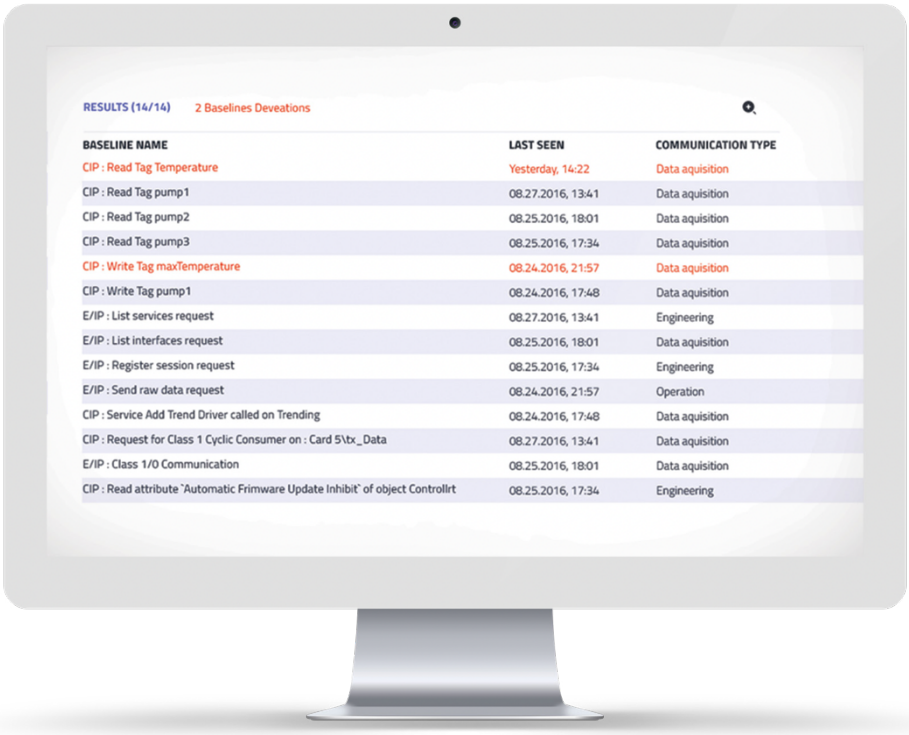


Figure 4: Asset discovery

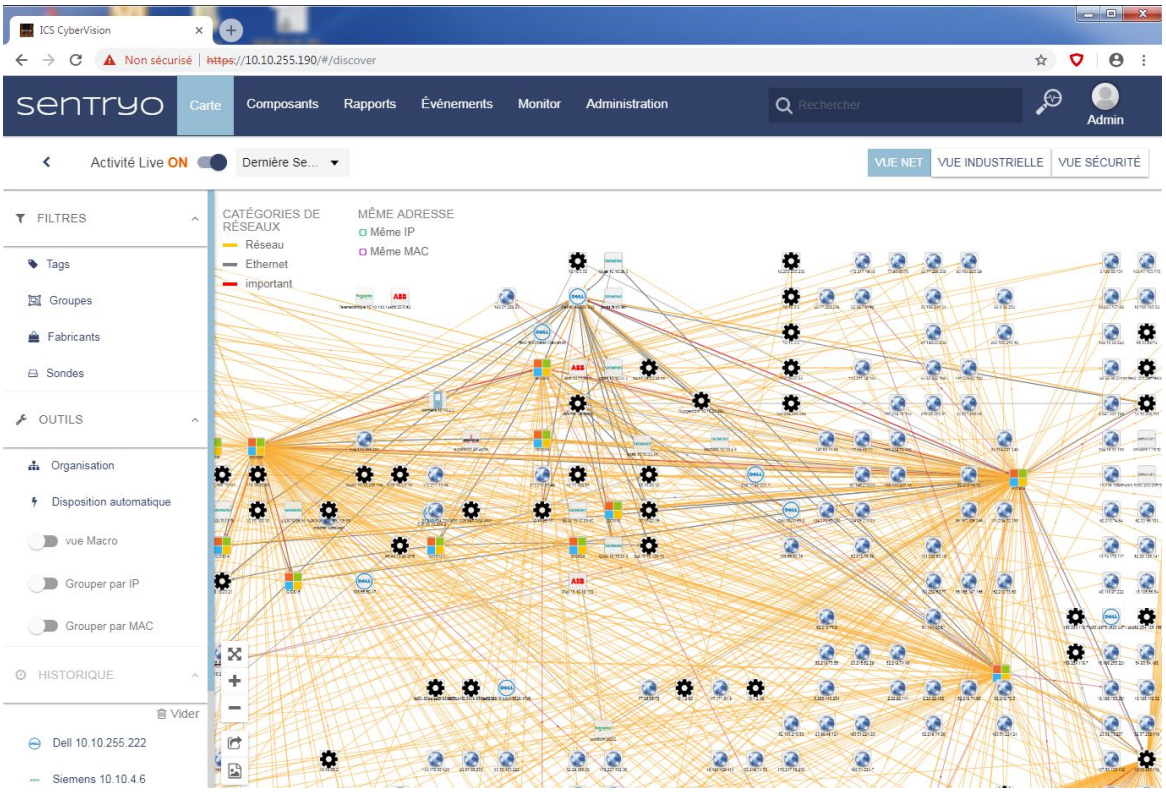


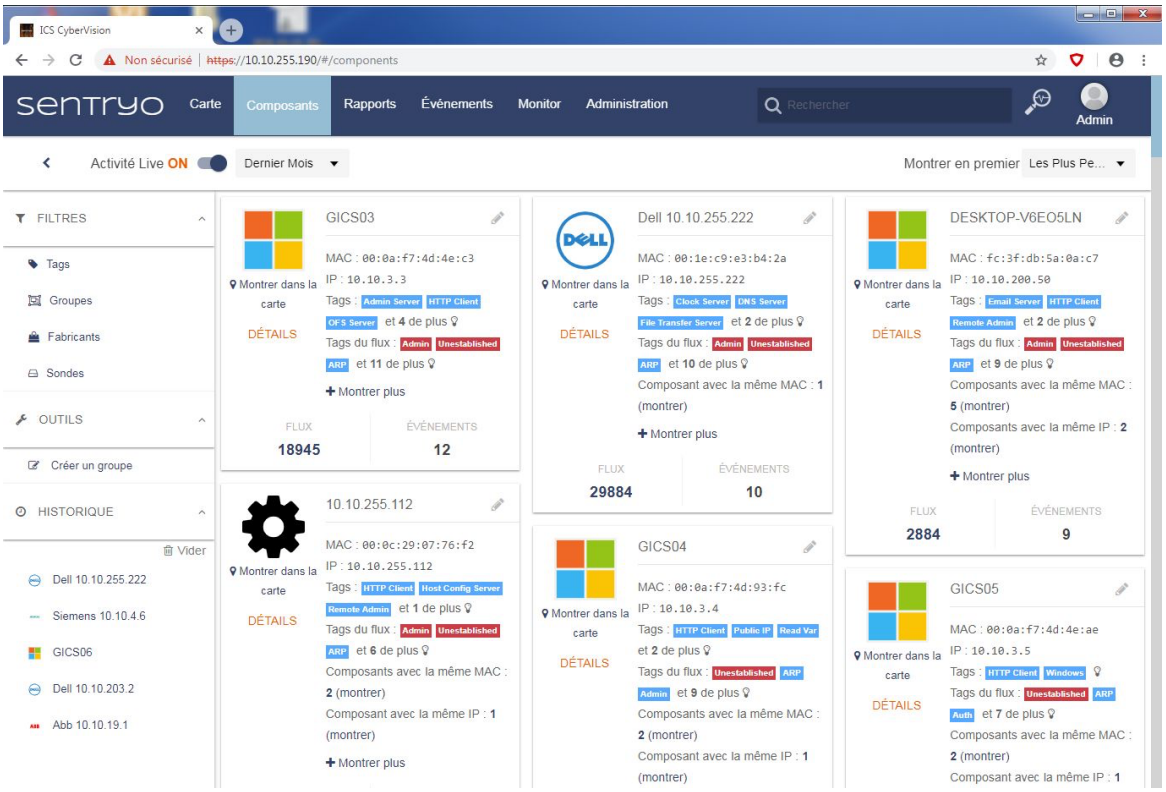


RESULTS (14/14) 2 Baselines Deveations

BASELINE NAME	LAST SEEN	COMMUNICATION TYPE
CIP : Read Tag Temperature	Yesterday, 14:22	Data aquisition
CIP : Read Tag pump1	08.27.2016, 13:41	Data aquisition
CIP : Read Tag pump2	08.25.2016, 18:01	Data aquisition
CIP : Read Tag pump3	08.25.2016, 17:34	Data aquisition
CIP : Write Tag maxTemperature	08.24.2016, 21:57	Data aquisition
CIP : Write Tag pump1	08.24.2016, 17:48	Data aquisition
E/IP : List services request	08.27.2016, 13:41	Engineering
E/IP : List interfaces request	08.25.2016, 18:01	Data aquisition
E/IP : Register session request	08.25.2016, 17:34	Engineering
E/IP : Send raw data request	08.24.2016, 21:57	Operation
CIP : Service Add Trend Driver called on Trending	08.24.2016, 17:48	Data aquisition
CIP : Request for Class 1 Cyclic Consumer on : Card 5\tx_Data	08.27.2016, 13:41	Data aquisition
E/IP : Class 1/0 Communication	08.25.2016, 18:01	Data aquisition
CIP : Read attribute `Automatic Frimware Update Inhibit` of object ControlIrt	08.25.2016, 17:34	Engineering

Appendix B: Sentryo dashboards





Appendix C: PandoraFMS dashboards