The Future of Industrial Monitoring System, a Blueprint for an AI Empowered OT Threat Detection System

Saber Mhiri

***Abstract*—With the increasing threats facing the industrial networks and due to our direct contact with clients, we know from experience that the needs of these clients will eventually evolve and a new and better technologies will be required to face the evolving attack environment and techniques targeting the industrial platforms.**

Our company objective of protecting industrial compounds dictate the need for constant improve of the services and technologies used.

We're constantly keeping an eye on the market competitors and needs in order to have a competing product as well as identifying the technological innovations that can be utilized to help protecting our clients.

For these reasons, in Inprotech have created our own I+D division as well as creating a strong relationships with the regional and national I+D centers. These relationships are not limited to the current proposed solution but build over years of collaborations through multiple projects.

***Index Terms*—AI, OT network, PLC vulnerabilities, threat detection, Intrusion Detection Systems IDS.**

I. Introduction

With the introduction of the concept of Industry 4.0. the industrial companies started racing toward connecting their plants.

Being a cybersecurity auditing company, we have been working with multiple industrial clients helping them safely adapting their network while transitioning to the Industry 4.0 framework cybersecurity needs.

This connectivity increase has added more vulnerabilities to industrial networks. With this connectivity, the industrial networks are now facing an increasingly complicated attack strategy.

During our multiple visits to clients and directly communicating with plant managers and security responsibles, we noticed the limitations in their monitoring strategies as well as their limited capacity not only when it comes to their network activities, but also when it comes to using the different monitoring and analyzing tools they have in their disposal. These tools have limited capacity compared to the complicated nature of the attacks they face.

Certainly, with the increasing level and complicity of attacks targeting the industrial and critical infrastructure, most of the current technological cybersecurity solutions opted to use the power of AI to tackle the increasingly complicated natures of attacks. However, the current solutions used in industrial networks are either IT solutions that are customized for OT use or sometimes only marketed as OT/IT solutions.
In order to cover this gap of missing dedicated OT cybersecurity solutions that are equipped with modern sophisticated technologies capable of protecting the OT networks from the dangers it faces, we're developing a technology called SANTI. Through this technology, we will provide the industrial network security officers a complete, yet simplified view of their complicated network state. Using the AI modules will help identify threats in the network based on the network behavior, protect critical assets as well as helping with risk management by ranking the network threats.

The connectivity needs raised by applying the concept of Industry 4.0 have also encouraged the industrial equipment producer to produce new technological devices that support connectivity mechanisms including WiFi. This evolution made the connectivity and smart access to data of the network systems a main concern of the industrial users. Simply collecting the data of the network can't help securing it. We need a system capable of safely aggregating, listing, and filtering the complicated and huge amounts of data independently of the location.

To this end, we're developing a Big Data and cloud-capable of securely serving these needs.
In this work we presented this proposed solution using SANTI technology empowered by AI and cloud modules. In chapter 2 we present the current solutions existing in the market as the state of the art. Then in chapter 3 we describe the proposed solution. In chapter 4, we describe in details the modules related to the use of AI and cloud technologies. Finally, we conclude this paper with our intake of this work.

II. State of the art

When looking at the existing solutions in the market dedicated for industrial cybersecurity threat monitoring, we can detect these following products heavily marketed and implemented in industrial factories.

Products	Use Cases	Intelligence
Splunk enterprise security	Highly regulated industry	Integrates with Splunk UBA & machine learning toolkit
LogRhythm	Scales from midrange to enterprise	Machine analytics for advanced threats
IBM Security QRadar	enterprises and regulated industries	UBA, forensics, packet inspection, Watson integration
Checkpoint 1200R	Designed for OT environments, designed for small enterprises.	Firewall integrated threat detection
Guardian	Designed for medium and large enterprises	Asset Discovery and Network Visualization Vulnerability Assessment and Risk Monitoring Real-time Anomaly and Threat Detection Focused Risk Information and Time-Saving Response Tools Unified Security for Thousands of Distributed Sites

TABLE I
COMPETITORS USE CASE AND INTELLIGENCE.

Products	Use Cases	Intelligence
Splunk enterprise security	Use of machine learning for behavior analysis	Passive Only Vulnerability Scan
LogRhythm	Different types of analytics on industrial machines and Wide range of modules to expand functionalities	They do not support third party vulnerability databases and Low capacity to support large volume of events
IBM Security QRadar	Support of multiple industrial protocols with specialized module and IBM's own AI module: Watson	Automation only available in premium versions and High price
Checkpoint 1200R	Specialized hardware and modular solution and Support for any OT protocol	It is not specialized in OT but it is an adapted IT solution
Guardian	Support for a large number of OT protocols and Asset inventory and vulnerability analysis	Only passive vulnerability analysis

TABLE II
COMPETITORS ADVANTAGES AND INCONVENIENCE.

Products	Delivery	Pricing
Splunk enterprise security	Software or cloud	Based on max daily data volume; start at $1,800/GB/day
LogRhythm	Appliance, software or virtual instance	Subscription pricing tied to volume consumption
IBM Security QRadar	Cloud or hardware, software, software or virtual appliance	Cloud starts at $800/month; on premises at 10,4k
Checkpoint 1200R	hardware	$1854 /unit
Guardian	hardware	2058,26$ + IVA per unit

TABLE III
COMPETITORS DELIVERY AND PRICING.

- **Nozoomi**
  Although they offer a cutting-edge technological solution it only offers a passive vulnerability scanner compared.
- **Checkpoint**
  Although their solution is an IT solution with OT capability, it has decent functionalities although it only offers a passive vulnerability scanner compared to our SANTI passive and active vulnerability scanner.
- **logrhythm**
  different machine analytics targeted for treating advanced threats and offer Appliance, software and virtual products. Wide range of modules such as SUBA, FIM and SAO. According to [1], although the company offers a partner program to help facilitate custom integrations, it doesn't offer any app store like many competitors and their APIs are less open to third partners. Companies with third-party threat intelligence feeds should confirm the support with LogRhythm, as it supports a limited number of feeds. Customers have expressed concerns about their ability to support very high event volume environments.
- **IBM Security QRadar**
  SIEM capable of supporting OT protocols through their Device Support Module (SDM) but needs excessive customization. They provide a wide range of modules such as UBA, forensics, packet inspection and big fix mostly useful for IT solutions. Although Qradar aims to integrate their AI system called Watson, the system is still in an early stage. According to [1], while IBM offers the BigFix solution for endpoint monitoring, its clients have shown very little interest and have turned instead to third-party solutions. Workflow and incident response are better than average, but full orchestration and automation is only available through IBM's Resilient Incident Response Platform premium solution.
- **Splunk**
  full range of solutions with advanced analytics available throughout the platform. A wide range of partners offer integration services, and apps are available through the Splunkbase app store. Still, [1] reports that some of its clients have raised concerns about the licensing model and the overall cost of implementation. Additionally, since Splunk doesn't offer an appliance version of the solution, companies that want an on-premises appliance must turn to a third-party. According to [1], Splunk is mainly focused on core SIEM capabilities and lacks specific advanced threat detection solutions. Splunk Stream (included with Splunk Enterprise) can collect network traffic for analysis.

III. PROPOSED SOLUTION

The process starts with collecting the traffic data from the industrial network. These data would be generated by all the equipments present in the network, such as PLC, SCADA, robotic arms and more. In order to make our product impact on the network the least possible, we opted to use passive listening techniques in order to collect these datas. Through a span port connected to the main routers in the network, we can have all the traffic going through the network connected to that main router or switches in order to be processed by our modules. This data collection process would be performed by the SANTI hardware with a span port connected directly to the network.

After collecting the traffic in the network, the data will be processed in the big data cloud sub-module "processing engine". The collected data would be sent to the AI module for farther analyses. The processed data would be saved in a distributed database where we can perform further treatments such as searching through theses data or sending it to the AI module for further analysis.

The results of analysing and processing the collected data using the AI and the cloud modules would be presented to the end users through an intuitive interface.

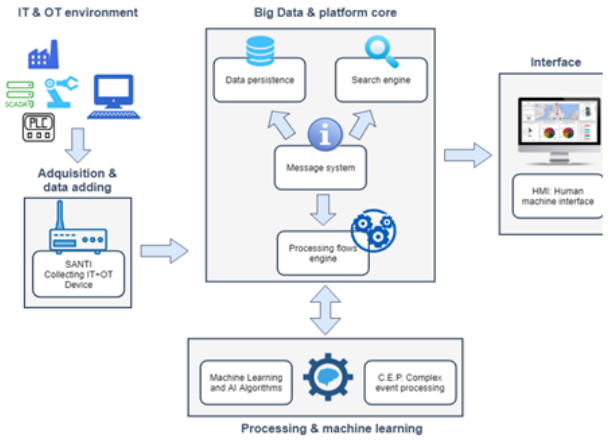

Fig. 1. Testing environment

A. Critical modules

1) AI module [2]:

- Development 1: Rules regarding traffic volume, type of traffic and schedule of communications
  - Why?
    When it comes to cybersecurity attacks on the industrial network, the slightest change in communication can indicate a serious change in the functionalities that can cause a serious economic and physical loss. Due to the nature of the industrial network (robust, robotic, and repetitive), if we manage to identify the slight changes in the network, we can theoretically identify attacks at their initial state. For example, if a machine usually communicates using a Profinet protocol, at certain hours of the day, with bandwidth use level that is under 50 bps and only using 5 specific memory addresses, any change in these informations can mean a possible attack.
  - Objective
    * To have a network traffic pattern capable of measuring and deducting the range of traffic in size and type for normal communications between different network elements.
    * To use this network traffic model to detect changes in traffic and launch alerts related to traffic size and type changes.
- Development 2: Detection of patterns of behavior between machines in order to group them into multiple classes
  - Why?
    Although each machine in the network has a specific functionality depending on its level of deployment, we think that certainly some attacks targeting PLC's do not distinguish between PLC's controlling a painting task in a car factory and another PLC controlling a freezing unit. An attack aiming to stop a PLC doesn't particularly care about the functionality of the PLC as much as it's model. Analyzing the behavior of machines in the network can help us identify a machine being attacked based on experience from other machines with the same behavior module.
  - Objective
    * Having a module capable of modeling the behavior of industrial machines based on their traffic and classify these machines into multiple classes.
- Development 3: Detection of critical actions that includes the user / device responsible for carrying out said action
  - Why?
    Focusing on the most PLC's activities especially the critical actions and relating them to the users help us identify the user/PC responsible for an attack that may affect the network. Monitoring and creating relationships between users and PLCs activities will help us stop attacks from happening at an early stage as well as protecting certain critical assets from being harmed by unauthorized users or actions.
  - Objective
    * Having a module that is capable of monitoring the changes in PLC behavior.
    * Having a module that is capable of monitoring the activities of the users in the network.
- Development 4: Intelligent and automatic scoring based on risk levels
  - Why?
    Due to the complexity of the industrial networks, most of the security officers monitoring it has problems identifying the most critical alerts and issues in their networks. Having a scoring system will eventually guide the users toward the most critical or tie sensitive threats in their networks to deal with.
  - Objective
    * Having a scoring module capable of assigning weight to network activities based on their threat level.
- Development 5: Inventory list with all the devices detected in the network communications.
  - why?
    The capacity to scan and enumerate the devices in the industrial network is a highly valued capacity when it comes to industrial networks monitoring. Due to the complexity of the industrial network communication, the need to display the network communications using different types of filtering will be a useful option when it comes to identifying the sources of attacks as well as the suspicious communications.
  - Objective
    * Listing all the devices identified during the network scans
    * Listing all the communications and informations related to the discovered devices.
- Development 6: Aggregation of customer data in a single console
  - why?
    When installing multiple units of our product, simultaneously supervising all these units well become an essential task in order to manage all the data and results generated by these units of our product. Having a centralized view of our clients datas will help us centralize the control of our clients security. This centralized view will help us intervene and assist the security monitor in charge of overseeing multiple factories at the same time.
  - Objective

    * Control multiple units of our products simultaneously through aggregating the network datas collected by these units.
- Development 7: Filtering of information based on the needs of the described functionalities
  - Why?
    Due to the huge amount of data that will be collected from the monitored industrial networks, the need of filtering these data in a way that help the identifying risks without having to go through multiple useless informations and irrelevant data.
  - Objective
    * Having a filtering module capable of thurrowly filter the collected data in order to have a focused view of the data that helps identifying threats in the network.
- Development 8: network pattern interface
  - Why?
    After the IA module manage to pattern the traffic, the interface should be able to show the normal network pattern through interactive network maps that are capable of showing the discovered pattern, for example having the most active assets in a specific color in the map, having the machines that communicate the most between each other shown in colored group, having the links width in map between machine reflecting the amount of bandwidth exchanged between the machine.
  - Objective
    * Having an interface module capable of reflecting the network patterns discovered by the IA module "traffic pattern"
- Development 9: machines relationship map
  - Why?
    After the IA module manage to identify the machines with similar configurations, the interface should be able to show these machines in the same color in the map as well as their history of attacks (how many time the machine had an alert associated to it, the risk score average of these attacks...)
  - Objective
    * Having an interface module capable of reflecting the network patterns discovered by the IA module (relations between machines "IA: Development 2").
- Development 10: user / machines lists
  - Why?
    The interface should be able to present the users responsible for changes in the network. We should be able to see all the machines that have been modifies and which user was responsible for these changes.
  - Objective
    * An interface capable of showing the machines with updated configurations, the users responsible for these configurations and for each user, the list of modified machine (filter by machine and by users).
- Development 11: Scoring interface
  - Why?
    In order to help the interface users to identify the most critical risks in their network, as well as the general state of the network, the interface should show the activity scores generated by the AI module in an intuitive way that guide the user through the complicated alerts in his system in order to assure a fast resolve of the risks
  - Objective
    * Intuitive scoring interface that help the users navigate through the alerts in the system based the threat level.
- Development 12: unique clients interface
  - Why?
    We need to have an interface capable of showing the alerts collected from the different instances of our products, filtered by these products locations and the network scoring. So in case I want to see all the alerts appearing in networks that have a general score of 8 or above in all my clients, the interface should present these alerts ordered by their threat levels and grouped by the client/locations it's implemented in.
  - Objective
    * An interface capable of grouping and ordering alerts from different product units.

IV. Conclusion

It's time for industrial network monitoring product to implement more advanced technologies in order to protect and minimize the risks in their networks. Using advanced modules such as Artificial technologies, Big data and cloud modules can highly improve the way we protect these critical infrastructure. In this work we presented the different development objectives that can help creating a next generation industrial cybersecurity monitoring solution.

References

[1] https://www.gartner.com/en/documents/3834683
[2] Nilsson, Nils J. Principles of artificial intelligence. Morgan Kaufmann, 2014.

[3] https://www.hindawi.com/journals/sp/2018/5418679/