InprOTech

Smart security for your industry

The Current State of OT Cyber-Security, Moving Toward the Industry 4.0 with the Rise of AI Technologies and new Threats.

Saber Mhiri [1]

[1]InprOTech, saber.mhiri@inprosec.com

Abstract. Due to the increase in technology deployment in industrial platforms moving toward industry 4.0, the threat level of cyber-attacks raised due to the gravity of such attacks not only economically but possibly causing life casualties. This raise in technology deployment in the industrial field caused the cyber-criminals to focus their attacks on the used operation technologies OT as a new platform of attacks and gain.

Due to this attack direction, the number of ransomware attacks increased in the past years. as a result of the increasingly sophisticated cyber-attacks on operation technologies and its complicated nature, artificial intelligence AI have been considered a main tool for the protection against these attacks.

Although most of the giant industrial companies have greatly invested in their cyber-security, the obstacles facing the industrial small and medium companies SMEs have not been particularly addressed.

Keywords: industries 4.0, cyber security, Security information and event management SIEMs. Small and Medium Enterprises SME

1 INTRODUCTION

Security information and event management (SIEM) software gives enterprise security professionals both insight into and a track record of the activities within their IT environment. SIEM technology has been in existence for more than a decade, initially evolving from the log management discipline. It combined security event management (SEM) which analyzes log and event data in real time to provide threat monitoring, event correlation, and incident response with security information management (SIM) which collects, analyzes and reports on log data.

With the increase of connectivity inside the industrial networks, solutions such as SIEMs are needed. As the treats coming and targeting the industrial components and network, the industrial SMEs have suffered multiple costly attacks and are in dire need of security solutions that can face the rapidly increasing threats.

The leading companies in SIEM technologies are increasingly implementing AI technologies in order to improve the solutions in the market. Leading companies are also focusing as much on interface ergonomics and design as much as on the data collection and analyzing since the security responsibles needs to be well informed and organized when dealing with threats and using the different tools the SIEMs offers.

Security and Risk S&R professionals as well as security teams consider security analytic platforms such as Security Information and Event Management (SIEM) platforms as the best way to address their top cyber security challenges.

SIEM systems popularity among S&R professionals, the security analytic platform market is growing rapidly.

Currently, Security Information Management SIM systems have expanded from purely rules-based detection to include data science methods like machine learning and artificial intelligence. Vendors call this SIM 2.0, next-generation SIM, or evolved SIM.

In order to overcome the drawbacks of current SIEMs systems is by leveraging AI, profiling and classification technologies and providing affordable products that take into consideration the special needs of the industrial SMEs.

In this paper we start by analysing the challenges facing industrial SMEs in their changes toward the fourth industrial revolution in chapter2. In chapter 3 we represented the current existing solution targeting the security of industrial networks. In chapter 4 we described the general layout of an industrial network, showing it's complexity, and in chapter 5 we presented the general architecture of an industrial network. in chapter 6 we shown the variety of industrial protocols used mainly by the PLCs. In chapter 7 we presented the trend of security through monitoring implemented in the industrial network. Then, we presented in chapter 8 the technological trend of using AI as the future of cyber-security. Finally we conclude with the chapter 9.

2 CHALLENGES

Currently, the industry 4.0 is transforming the industrial environment into an IoT environment. This change dramatically increased the importance of cybersecurity in companies risk management strategies. Cybersecurity threats are becoming a more and more dangerous to companies since they can now affect their production lines through OT vulnerabilities, not only their IT hardware. Within the current industrial situation, traditional security mechanisms are not applicable, nor have they been adapted to react to the ever-evolving cyber-security threats. Thereby, businesses have been exposed to a series of cyber-security threats with logical and physical world consequences (environment, people, etc.). For these reasons, the threats industrial infrastructures are exposed to and the risks they entail are unimaginable. Keeping up with the updated security threats in order to maintain confidentiality, availability, integrity and data privacy became tougher to secure.

Cyber-security became a major concern to all types of businesses due to increasing number of Data breaches, targeted attacks, social media scams, banking Trojans and data theft while the most widespread attacks are: unauthorized access, electronic fraud and phishing. It became increasingly clear that information security systems should be able to take preventive measures to safeguard and protect information for organizations and technological systems by maintaining confidentiality, availability, integrity and privacy of the data.

Studies show that 25% of the SMEs have received some computer attack with an average cost between 20,000 and 50,000 and 70% of these attacks are SME-focused [1] since they are not prepared for such attacks. Several security incidents affected the OT systems in the past years that caused the different SMEs to search for a solution that protect them from this danger. This tendency of attacks and the need for protection prove the importance of our proposed solution. These attacks affect companies in different ways as, in 2015, the company Sabella [12] system of a tidal turbine was encrypted, preventing the generation of electricity for 15 days. In 2016, some hospitals from different countries (Germany, USA...)[14] had to reschedule surgical interventions due to lack of access to medical records. The San Francisco public transport company[13] had enormous economic losses because a ransomware affected all the terminals of ticket collection and it was not able to charge for the journeys. The most recent attack was in May 2017, when the ransomware WannaCry [15] affected all sort of companies and institutions including the British health system, the Russian Ministry of the Interior, the German train computer system and the Renault Company in France...among others. Some of the main reasons behind SME lack of SIEM implementation are the current SME limitations since they are traditionally closed-source solutions with a high cost of implementations, limited to integrate small IoT / IIoT (Industrial Internet of Things) solutions which limit SMEs access to them. This lack of small deployment puts the small and medium industrial businesses at risk. The European Agenda consider Security cyber-crime as one of its primary priorities for the next 5 years [16] due to the increase of cyber-attacks on different European SMEs, specially the vulnerable industrial facilities. Europe needs high-quality, affordable and inter-operable cyber-security solutions and products. Although there are different companies working on security solutions in the European zone, they can hardly compete on international level [24]. This limits the security system choices for industrial SMEs since most of the existing security solutions focus mainly on protecting the IT systems or provide big factories OT systems security solutions.

With the growing number of industrial companies converging into the industry 4.0, there is a growing need for specified OT network protection solutions to protect against the increasing amount of attacks targeting the industrial networks. This situation made cyber-security at the top of the European union concerns [17].

Lately, the ransomware attacks started targeting whole cities. Just in December 2019, 4 U.S cities where targeted by a ransomware [26] after the successful attack carried in May 2019 on the U.S city Baltimore [25] that crippled most of the city services affecting people lives. Baltemore attack came after the attack carried on Atlanta last year 2018 [27].

Due to the importance of these attacks both on economic and safety level, the European Agenda consider Security cyber-crime as one of its primary priorities for the next 5 years [17] due to the increase of cyber-attacks on different European SMEs, especially the vulnerable industrial facilities. Europe needs high-quality, affordable and inter-operable cyber-security solutions and products. According to the WEF global risks report published in 2019[6], cyber-attacks are ranked 5th in terms of likelihood and 7th in terms of impact. Also according to the DNV GL Global Opportunity report published in 2017 [19], cyber-crime is ranked 2nd in the terms among the most reported types of economic crime.

3 RELATED WORK

Although there are different companies working on security solutions in the European zone, they can hardly compete on an international level [24]. This limit the security system choices for industrial SME's since most of the existing security solutions focus mainly on protecting the IT systems or provide big factories OT systems security solutions.

Faced with a growing need for cybersecurity protection for SMEs and the lack of OT industrial security systems that cater to SMEs needs, we identified the need for a security event

management system for SMEs that want to converge into Industry 4.0 but need to protect themselves from the risks of cyber-attacks and threats associated with this convergence, addressing the shortages of traditional managers and covering their needs, Considering industrial cybersecurity from an integral point of view in the new framework of the connected Industry 4.0 [20].
Multiple providers are in the market working on new next-generation SIEMS, but sadly most of them are focused on big, internationals enterprises rather than SME's.
Among these SIEM solutions in the market we have:

- **logRhythm**: it applies different machine analytic targeted for treating advanced threats and offer appliance, software and virtual products, and it offers a wide range of modules such as security user behavior analytics SUBA, File Integrity Monitoring Tools FIM, Security orchestration, automation, and response SAOR, and endpoint monitoring.

- **IBM Security QRadar**: On one hand, they provide a SIEM capable of supporting OT protocols through their Device Support Module (SDM) [22] but the module needs excessive customization. On the other hand, they provide a wide range of modules such as user behavior analytics UBA, forensics, packet inspection and IBM big fix mostly useful for IT solutions. Although QRadar aims to integrate its AI system called Watson [23], the system is still in an early stage of learning.

- **Splunk**: It offers a 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.

- **AlienVault**: Although AlienVault USM offers a wide range of integrated security functionalities, including asset discovery, vulnerability management, and intrusion detection, customers say the security monitoring technologies included with USM offer more functionality for a lower cost than most competitors, and the pricing model is straightforward and easy to understand.

4 A typical OT network vs. the reality

When it comes to OT and IT networks, we usually expect the networks to be segregated and protected as Figure 1 shows. But in reality, the two networks are increasingly merging together and the boundaries between OT and IT are getting blurry.
IT technologies are being implemented in OT environment rapidly. These IT technologies bring with them threats that the OT environment pieces of equipment are simply not ready for.
Due to this situation, the OT environment is in increasing need of protection and monitoring [5].

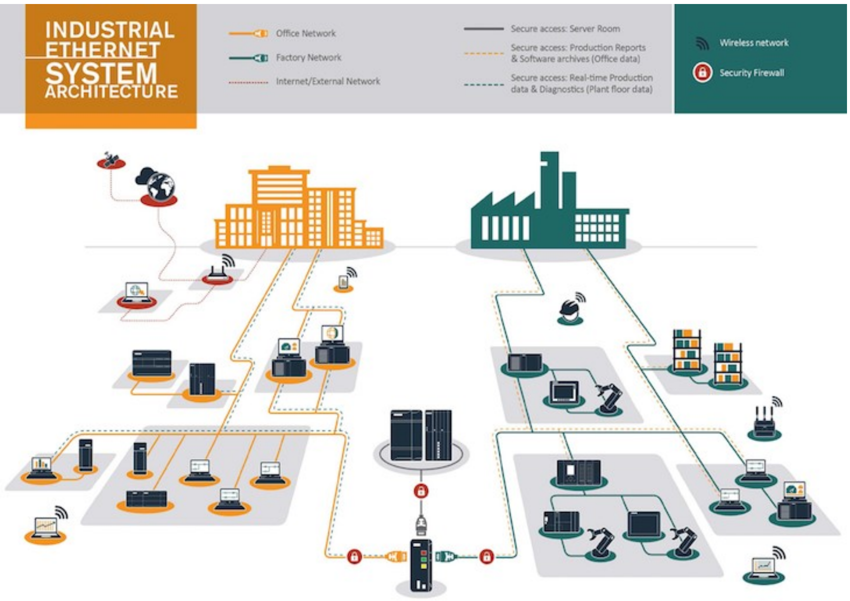

INDUSTRIAL ETHERNET SYSTEM ARCHITECTURE
Office Network
Factory Network
Internet/External Network
Secure access: Server Room
Secure access: Production Reports & Software archives (Office data)
Secure access: Real-time Production data & Diagnostics (Plant floor data)
Wireless network
Security Firewall

Figure 1: IT vs. OT environment expectation

5 Industrial Network architecture

Typically, the OT architecture starts from the PLC, since PLCs represent the brains of the OT network. The northbound of the PLC is usually connected to IT hardware and serve as a source of information to the SCADA systems. The southbound of the PLC is used for communicating with the different sensors and industrial equipment in the network as described in [6].

As Figure 2 shows, in a typical industrial network, it's possible to have multiple different networks, where each network use a completely different communication model and protocols.

It's also worth mentioning that machine to machine communications are common in OT network, meaning that a PLC, for example, can communicate directly with another PLC without the need to pass through a middle switch neither router.

Another example of these communications is the communications between PLCs and industrial material such as robotic arms.

Due to the use of different industrial communication protocols, these machine to machine communications is possible.

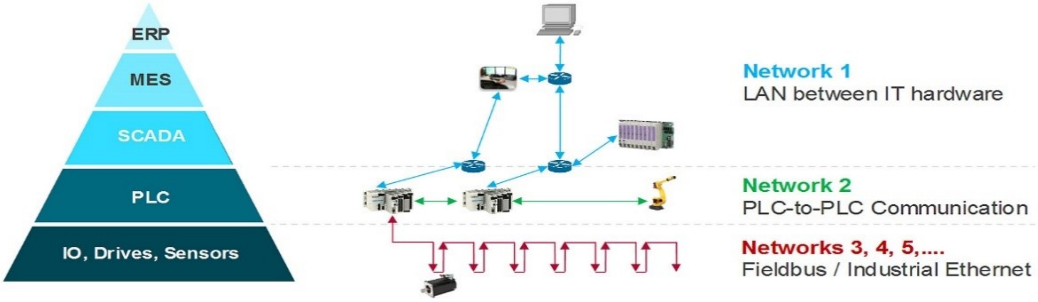
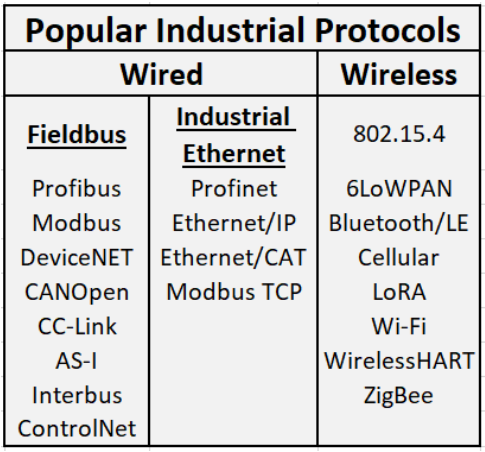


Figure 2: Industrial network hierarchy

6 PLC and protocols

Although there are multiple PLC providers in the market such as Siemens, Schneider, Allen Bradley, these PLC solutions offer similar functionalities with a difference in terms of supported protocols.
[7]discuss the PLC communication protocols and their different architectures.
The protocols supported by these PLCs can vary depending on the version of the PLC and provider, but in some cases, PLC providers may use a proprietary protocol such as the case of Siemens with their s7comm and s7comm plus protocols. Figure 3 shows the most commonly used protocols in the industry.



Popular Industrial Protocols		
Wired		Wireless
Fieldbus	**Industrial Ethernet**	802.15.4
Profibus	Profinet	6LoWPAN
Modbus	Ethernet/IP	Bluetooth/LE
DeviceNET	Ethernet/CAT	Cellular
CANOpen	Modbus TCP	LoRA
CC-Link		Wi-Fi
AS-I		WirelessHART
Interbus		ZigBee
ControlNet		

Figure 3: List of commonly used industrial protocols

7 Collecting Logs

In order to monitor the industrial network, we should start by collecting the logs of the machines in the network. To this end, several industrial networks may have historians implemented in their network. A Data Historian (also known as a Process Historian or Operational Historian) is a software program that records and retrieves production and process data by time; it stores the information in a time series database that can efficiently store data with minimal disk space and fast retrieval. But in reality, the use of historian isn't a common practice, especially that SME factories are still struggling with updates needed in order to get included in the industry 4.0 revolution.

On the other hand, the PLCs in the network do not save the logs unless programmed to do so, in the case of collecting the logs from the PLCs, we need to program each and every PLC in the network to save the logs and send it to our monitoring system. Most of the log collection solutions in the market, although presented as solutions that collect logs from the machines, they actually monitor the traffic in the network and generate their own logs.

The process of generating logs through traffic is implemented in the Check Point and Nozomi SCADAguardian solutions. The process is straight forward, the product gets connected to a mirroring port of a switch in the network and starts sniffing all the traffic passing through that network section.

As Figure 4 shows, all the blue boxes (log collectors) are directly connected to the switches in the network. These solutions monitor the traffic coming from the PLCs northbound and the rest of the IT network. Although these solutions are not placed in the lower level of the network, between the PLC and the different sensors of the factory, they do monitor and collect logs related to the PLC communication with the lower network level because most of the PLC communications go through the switches.

As for the communications between the PLC and the down layer of sensors, we can either deduce through analyzing the changes the PLC goes through while performing these communications, or, through programming the PLCs to save their logs and send them to a web-server on the network.

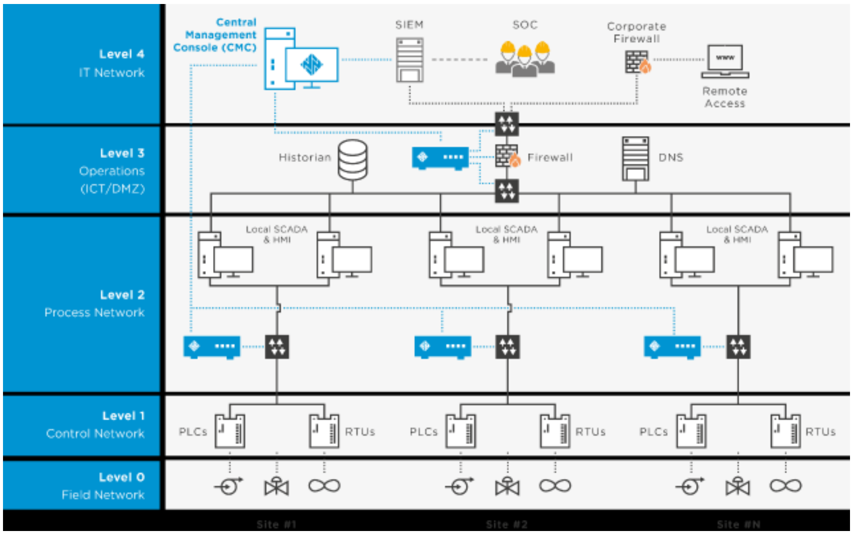


Figure 4: Log collection through sniffing network mirror switches [3]

8 Technological and Security Trends

Currently and according to [24], the main international SIEM companies are increasingly focusing on implementing new technologies such as AI in their products in order to face the new and evolving threats. But on the other hand, few companies are focused on producing a competitive SIEM product dedicated to industrial SME.

With the increasing development of attack tactics, the introduction of industry 4.0 and the IoT environment, the legacy SIEMs find themselves unable to protect the IT/OT environment due to its limits such as limited security types, inability to effectively ingest data, slow investigations, instability due to scalability, end-of-life or uncertain roadmap of the SIEM, closed ecosystem and being limited to on premises.

Due to the legacy SIEM limitations, modern SIEMs must provide most of the following functionalities: real-time monitoring, incident response, user monitoring, threat intelligence, advanced analytics and advanced threat detection.

Currently, the main trends and research objectives of the main SIEM providers are using AI techniques for detecting threats and getting involved in the industry 4.0 transition through providing SIEMs dedicated to OT and IoT.

Business leaders who took part in this survey [19] see the use of artificial intelligence to boost cybersecurity as a great business case.

Technologically, the main trends in SIEMs business are AI and block-chain technologies. Many companies incorporate partly or totally AI technologies in their SIEMs designs due to the tremendous success of the technology in detecting and responding to cybersecurity threats. According to [19] 85% of all cybersecurity attacks are predicted using AI. As for block-chain, the technology is still in its infant's state, still, the applications created with it showed that the block-chain power is game-changing. Currently, many companies are trying to implement this technology in their data collection and documentation steps due to the block-chain capability of permanently saving the data and verifying its authenticity.

9 CONCLUSIONS

We analyzed the challenges facing the industrial SMEs through their move toward the industrial Revolution 4.0, focusing on the cyber-security threats on their networks and showing the effect of such attack economically and on people life in the case of critical infrastructures, we have cited multiple examples that vary from industrial and critical infrastructures to whole cities.

We presented the different existing solutions addressing cyber-security in industrial networks while focusing on the SMEs needs. Then, we presented a description of the general layout of an industrial network focusing on it's complexity.

Likewise, we shown the architecture of the industrial network identifying the PLC as the main component in the network that the security system in the industry should protect. To that end, we presented the different protocols used by PLCs in the network.

We have shown and explained the main industrial networks monitoring techniques used by different solutions in the market as well as presenting the AI as the main technological trend in industrial cyber-security systems.

References

[1] https://empresas.blogthinkbig.com/problemas-ciberseguridad-y-solucion/

[2] https://www.matrikonopc.com/opc-drivers/opc-modbus/base-driver-details.aspx

[3] https://www.nozominetworks.com/

[4] https://www.rs-online.com/designspark/iot-industry-40-and-the-need-for-industrial-ethernet

[5] https://link.springer.com/chapter/10.1007/978-3-030-00024-0_11

[6] https://automationforum.co/basics-of-industrial-networking-architecture/

[7] https://library.automationdirect.com/plc-communications-coming-of-age/

[8] http://www.modbus.org/

[9] https://new.siemens.com/global/en.html

[10] http://snap7.sourceforge.net/siemens_comm.html

[11] https://os-s.de/thesis/MA_Maik_Brueggemann.pdf

[12] https://e-rse.net/hydrolienne-sabella-d10-energie-marine-22260/gs.kmhj6i

[13] https://globbsecurity.com/ataque-ransomware-metro-san-francisco-40189/

[14] https://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016?page=1

[15] https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/

[16] https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en

[17] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive?page=1

[18] http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

[19] http://www.safety4sea.com/wp-content/uploads/2017/01/DNV-GL-Global-Opportunity-Report-2017.pdf

[20] https://empresas.blogthinkbig.com/problemas-ciberseguridad-y-solucion/

[21] https://www.gartner.com/en/documents/3834683

[22] https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/com.ibm.dsm.doc/c_dsm_guide_install_manage_overview.html

[23] https://www.ibm.com/it-infrastructure/solutions/

[24] https://analyticpartners.com/resources/forrester-wave-marketing-measurement-optimization-2018/

[25] https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html

[26] https://www.cbsnews.com/news/ransomware-attack-pensacola-florida-4-u-s-cities-attacked-by-ransomware-this-month-2019-12-17/

[27] https://en.wikipedia.org/wiki/2019_Baltimore_ransomware_attack