SIEM For industrial SME: needs and the obstacles

Saber Mhiri

***Abstract*—Currently, industry 4.0 is transforming the traditional industrial environment into an IoT environment. This change dramatically increased the importance of cybersecurity in industrial SME (Small and Medium Enterprises) risk management strategies.**

Cybersecurity threats are becoming more and more dangerous to Industrial SME's since they can now affect their production lines by taking advantage of their numerous OT vulnerabilities. Within the current industrial situation, traditional security mechanisms are not applicable, they have not been adapted to react to the ever-evolving cybersecurity threats. Due to this situation, industrial SMEs has been exposed to a series of cybersecurity threats with logical and physical world consequences (environment, people, etc.).

For these reasons, the need for SIEMs (Security Information and Event Management) dedicated to industrial SMEs is today's top priorities for security analysts both at industrial and governmental levels.

***Index Terms*—5G mobile communications, admission control, optimization, software defined networking**

I. Introduction

SEcurity information and event management (SIEM) software give 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.

The leading companies in SIEM technologies are increasingly implementing AI technologies in order to improve the rising rule dependent 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 S&R professionals need to be well informed and organized when dealing with threats and using the different tools the SIEM's 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.

Due to Security Information and Event Management (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.

This paper is composed of four sections, in section 2 we represent the challenges facing SME and the involved cybersecurity risks. In section 3 we cite some examples showing the impact of the topic in terms of risk, opportunities and governmental legislation. In section 4, we study the state of the art, where we focused on the main companies in the SIEM market. In section 5, we presented the latest technology and security trends that drive the security industry such as AI and block-chain. In section 6 we represent the main characteristics that every SIEM producer should consider while designing and developing their products if they hope to target the industrial SME market.

II. Challenges and risks

The inability of current SIEM's to protect institutions (IT and industrial OT0 alike) from an increasing number of data breaches and targeted attacks represent the main challenge industrial SME's face.

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 since they are not prepared for such attacks.

Several security incidents affected the OT systems in the past years that caused the different SME's to search for a solution that protects 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 [1] system of a tidal turbine was encrypted, preventing the generation of electricity for 15 days. In 2016, some hospitals from different countries (Germany, USA...) had to reschedule surgical interventions due to lack of access to medical records [3]. The San Francisco public transport company had enormous economic losses because ransomware affected all the terminals of ticket collection and it was not able to charge for the journeys [2]. The most recent was in May 2017, when the ransomware WannaCry [4] 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 solutions IoT /

IIoT which limit SME's access to them. This lack of small deployment puts the small and medium industrial businesses at risk.

III. Importance

Due to the importance of these attacks both on economic and safety level, the European Agenda consider Security cybercrime as one of its primary priorities for the next 5 years [5] due to the increase of cyber-attacks on different European SME's, especially the vulnerable industrial facilities. Europe needs high-quality, affordable and interoperable cybersecurity 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 [7], cyber-crime is ranked 2nd in the terms among the most reported types of economic crime.

IV. Related Work

Although there are different companies working on security solutions in the European zone, they can hardly compete on an international level [12]. 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 SME's and the lack of OT industrial security systems that cater to SME's 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 [8].

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 SUBA, FIM, SAO, and endpoint monitoring.

According to Gartner [9], although the company offers a partner program to help facilitate custom integration, it doesn't offer any app store as many competitors do and their APIs are less open to third partners. Similarly, companies with third-party threat intelligence feeds should be sure to confirm support with LogRhythm, as it supports a limited number of feeds out of the box.

Although they provide a highly scalable decentralized architecture, it is reported that some customers have expressed concerns about LogRhythm's ability to scale to support very high event volume environments and advises that potential buyers should evaluate LogRhythm's ability to support their event and data volumes.

IBM Security QRadar: On one hand, they provide a SIEM capable of supporting OT protocols through their Device Support Module (SDM) [10] but the module needs excessive customization. On the other hand, 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 its AI system called Watson [11], the system is still in an early stage of learning.

Still, according to Gartner [9], while IBM offers the BigFix solution for endpoint monitoring, its clients have shown very little interest in it and have turned instead to third-party solutions. It's also reported that QRadar's UBA functionality lag behind other vendors, and the IBM Resilient incident response tool doesn't offer native integration with the QRadar platform. Also, workflow and incident response and management capabilities are better than average, but full orchestration and automation is only available through IBM's Resilient Incident Response Platform premium solution. Threat-hunting capabilities also come at a premium, through IBM's i2 Analyst's Notebook.

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. Still, Gartner [9] 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 provider.

According to Gartner [9], 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, and the Splunk Universal Forwarder can be used as a lightweight agent for endpoint analysis, the firm said.

AlienVault: Although AlienVault USM offers a wide range of integrated security functionality, 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.

AlienVault's target market is mid-sized enterprises and smaller organizations. As a result, enterprise-oriented features, such as role-based workflow, ticketing integrations, support for multiple threat intelligence feeds and advanced analytics capabilities, struggle to compete with those of competitors that focus on enterprise customers.

Also, according to Gartner [9], there can be some frustrating trade-offs inherent in choosing between USM Appliance and USM Anywhere – for example, capturing NetFlow data is supported by USM Appliance, but not by USM Anywhere, though USM Anywhere can capture VPC flow logs from AWS.

V. Technological and Security Trends

Currently and according to [12], 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 SIEM's 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 [7] 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 [7] 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 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.

VI. The needed SIEM for industrial SME

The needed SIEM for SME's should fulfill the following requirements:

- First, it should be able to protect the industrial SME's during their transition into the industry 4.0. The current situation of industrial SME's is that most of the machines are still running on old software versions or in some cases not even connected to the network. Also, most of the machines are controlled by industrial computers running old OS (such as WinXP and Win7) in order to keep the old control software running. These SME's are in need of a protection system that doesn't disturb their production lines and does not require them to update all their machines in an unexpected past.
- Second, it should be able to incorporate state of the art technologies s such as AI technologies and strategies. Most of the high-end SIMS in the market are moving toward implementing AI in their products at different levels. According to [7], 85% of all cyber-attacks are predicted using AI technologies, which means that the future of Cybersecurity is Artificial Intelligence.
- Third, the SIEM solution should be scalable in order to support the growing SME's with adequate IoT/IIoT solutions.
- Finally, it should have a low cost in order for it to be available and affordable to the majority of SME's. Currently, the SIEM's services are usually paid by consumption, which will cost all the way between $1,800/GB/$day and $10,4k$ for premiums.

VII. Conclusions

The cybersecurity threats to critical and economic infrastructure is a reality. And the need for a protection system such as a SIEM is a necessity for SME's. Although most of the big security companies developed SIEMS, their services are neither adequate nor dedicated to industrial SME's.

In this paper, we discussed the problems and dangers facing industrial SME's, presented the current state of the art and finally stated the needed characteristics of a SIEM that can serve industrial SME's.

References

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

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

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

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

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

[6] http://www3.weforum.org/docs/WEF$_Global_Risks_Report_2019.pdf$

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

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

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

[10] https://www.ibm.com/support/knowledgecenter/SS42VS$DSM/$

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

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