IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received February 26, 2021, accepted March 13, 2021, date of publication March 18, 2021, date of current version August 18, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3067106

Present and Future of Network Security Monitoring

MARTA FUENTES-GARCÍA[1], JOSÉ CAMACHO[2], AND GABRIEL MACIÁ-FERNÁNDEZ[2]
[1]Fundación I+D del Software Libre (Fidesol), 18016 Granada, Spain
[2]Department of Signal Theory, Telematics and Communications, CITIC-UGR, University of Granada, 18071 Granada, Spain

Corresponding author: Marta Fuentes-García (mfuentes@fidesol.org)

This work was funded by the Ministry of Science and Innovation through CDTI through the Ayudas Cervera para Centros Tecnológicos grant of the Spanish Centre for the Development of Industrial Technology (CDTI) through the Project EGIDA under Grant CER-20191012, and in part by the Spanish Ministry of Economy and Competitiveness and European Regional Development Fund (ERDF) funds under Project TIN2017-83494-R.

ABSTRACT Network Security Monitoring (NSM) is a popular term to refer to the detection of security incidents by monitoring the network events. An NSM system is central for the security of current networks, given the escalation in sophistication of cyberwarfare. In this paper, we review the state-of-the-art in NSM, and derive a new taxonomy of the functionalities and modules in an NSM system. This taxonomy is useful to assess current NSM deployments and tools for both researchers and practitioners. We organize a list of popular tools according to this new taxonomy, and identify challenges in the application of NSM in modern network deployments, like Software Defined Network (SDN) and Internet of Things (IoT).

INDEX TERMS Network security, NSM, security monitoring, incident detection, incident response, SDN, IoT.

I. INTRODUCTION

Although most of the efforts in network security are still focused on preventing attacks, solutions and techniques based in detection and response are gaining more and more relevance [1], [2]. There is a general belief within the Information Technology (IT) Security community that, sooner or later, prevention measures are surpassed by attackers. At that point, detection and response mechanisms need to be applied [3]. Network Security Monitoring (NSM) is one of the most relevant approaches for network security [4]. The **NSM cycle** can be characterized by four phases [4], [5]: *1) Monitoring*, *2) Detection*, *3) Forensics/Diagnosis*, and *4) Response/Recovery*. Its goal is to monitor the state of a given network to detect abnormal events and, when detected, to manage them in a timely manner. This is a significant challenge, since communication networks produce a huge volume of data at a high pace, following the definition of a Big Data problem [6]. This is even a more difficult task if we consider the pervasive nature of present and upcoming scenarios, such as 5G and the IoT, or the adaptation to new network technologies (*e.g.*, SDN) [7], [8].

In this paper, we review the state-of-the-art in NSM, aiming to provide a taxonomy and a unified description of its components. We also look over some of the existing solutions according to this taxonomy. Finally, we analyze the most relevant trends in modern networks, the (new) challenges they pose, and how they are tackled from the NSM perspective. We evaluate the use of the aforementioned traditional tools for NSM to modern networks, as well as we review existing solutions and novel works for this new framework. Thus, the main contributions of this work are:

- A **modular taxonomy for detection and response** systems according to the NSM philosophy.
- A **classification of some for the trade solutions** following the proposed taxonomy.
- An evaluation on the application of **NSM for modern networks**.
- **New challenges in network security** for new communication paradigms, according to the proposed taxonomy.

This paper is addressed from a different and complementary standpoint to previous works [9]–[14], which only cover partially the NSM cycle and do not tackle it from a module taxonomy perspective, as it is proposed in this paper. This modular taxonomy aims helping researchers and practitioners to understand features, benefits and lacks in current detection and response for network security.

The rest of the paper is organized as follows: Section II introduces a taxonomy which describes the main components

The associate editor coordinating the review of this manuscript and approving it for publication was Moayad Aloqaily.

and architecture of an NSM system. Section III includes a review of some of the best known commercial and open source available tools, following the proposed taxonomy. Section IV evaluates the benefits and challenges of applying NSM to modern networks. Finally, Section V presents the main conclusions derived from this work.

II. MODULAR TAXONOMY OF A NETWORK SECURITY MONITORING SYSTEM

An NSM system should be able to provide traceability of the activities and processes that take place in the network and subsystems under monitoring. To achieve this goal, a typical NSM architecture is composed of different software and hardware elements that are distributed thorough the network. These elements send information about network events to a centralized point, where they are recorded and analyzed.

A comprehensive review on the most used NSM systems has leaded us to propose a taxonomy of the NSM functionalities. Most of these solutions implement at least one of these functionalities: *sensor*, *parser*, *integrator*, *detector*, *inspector*, and *actuator*.

- **Sensor** collects data from a network subsystem. Resulting data are in the form of records or logs.
- **Parser** transforms data format.
- **Integrator** combines multiple sources of data into a single data stream.
- **Detector** identifies anomalous events/records in a data stream.
- **Inspector** allows data exploration.
- **Actuator** performs automatic actions on the network/subsystem configuration.

These are inherently modular systems, which make it easier the scalability to build more complex systems. This is achieved by combining the outputs of different modules. For example, the output of an integrator (A) could be the input for a second integrator (B), which is also combined with a detector (C), thus creating a hierarchical detection structure. In addition, not all NSM systems implement all functionalities.

Sensor, parser and integrator are usually enclosed in the monitoring phase, while the rest of the modules have a one-to-one relation with the remaining steps in the NSM cycle (detection, forensics and response). The NSM modules are described in the following paragraphs.

A. SENSOR MODULE

A **sensor** is a software agent and/or hardware appliance that collects data from the network, generating logs or records to be analyzed by a security team. This module usually includes the functionality to send the collected data to a centralized location, where such information can be accessed and analyzed.

More simple sensors, like traffic sniffers, are composed of a collector module alone. Other more complex sensors often include some form of parser and/or detection module. When these complex sensors are complete security tools which output is captured and utilized as a part of another top system, we call them **security sensors**.

B. PARSER MODULE

NSM deployments with numerous and disparate sensors result in massive databases from which detecting when and where there is an attack is a challenging task. Besides, the data format varies widely among the set of sensors [15], [16]. For this reason, after data collection, data sources need to be processed to become fit for purpose.

In spite of the attempts to provide unification models for the exchange of alert information, such as *Intrusion Detection Message Exchange Format (IDMEF)* [15], [17], one of the main problems in data collection is that manufacturers, when designing the devices and software, do not usually follow a standardized format for information logging. This implies the need of a *parsing* process. **Parsing** is the process of identifying and extracting individual parts that compose a log to obtain a logical and organized data structure [15]. Thus, parsing allows to extract useful information from the data and homogenize different sources to a common format [15], [17]. For instance, IP addresses can be located in different parts of the log file depending on the sensor. In such case, the parsing process is useful to identify the IP addresses on each available log and match them in order to combine different sources in a meaningful way. This process is needed to feed detection and visualization tools that require *structured information*.[1]

The parsing process can be performed *ad-hoc* (by security operators), and it can be often implemented either as a separate module or as a part of the sensor or the integrator modules. On the other hand, parsing can be performed either *scripting-based* or *software-based*. The former refers to Linux commands and to scripting-based programming (*e.g.* python or perl), while the latter refers to programs that have been developed to optimize the extraction of information from complex data [20]–[22].

Finally, there are some challenges related to the parsing, namely: *i) sensitivity of the parsing code to format changes in the sensors*, usually caused by updates in their specifications or even their functionalities; *ii) scarcity of information* about the format used by each manufacturer; and *iii) lack of synchronization* in the timestamp of sensors, which can be especially challenging if they are distributed in different countries with distinct time zones and do not make use of synchronization services like *Network Time Protocol (NTP)* [15].

[1] **Structured data** refers to those data that can be well organized in fields and follow a specific structure (*e.g.* ZIP code). They are suitable for relational databases. **Unstructured data** refers to those data that do not follow a specific format and have not been processed yet. These come from variate sources and are heterogeneous data, which can be images, post from social networks, or sensor data, among others. Unstructured data are not suitable for relational databases. **Semi-structured data** refers to data that are typically unstructured but contain some metadata or tags that allow to describe them (*e.g.* XML). They are not suitable for relational databases [18], [19].

C. INTEGRATOR MODULE

Integrators combine the data collected by the sensors to extend their semantic information. Different approaches can be implemented in form of *integration engines*. The integration module can include one or more **integration engines** that work complementary together to make disparate data become useful information. The following paragraphs describe some of the most extended approaches to implement data integration.

Having redundant data is a frequent problem when data are collected from different data sources, which can be solved by *correlating* events. The term **correlation** in IT Security is applied to find connections among distinct data sources or IT Security events.[2] Correlating events may be particularly useful when *i)* they are duplicated due to different nodes are generating events and/or alerts related to the same incident, or *ii)* they are related to the same incident in the same sampling time period and can be unified into a single event. Like this, event correlation provides the following benefits: *i) extending the semantic information* by considering the context of the event, *ii) reducing the volume of data* to be analyzed, and *iii) escalating and prioritizing important events*, thus reducing the number of false positives. This yields useful information for the detection of attacks or abnormal activities, especially when they affect different assets [16], [17], [23].

Another mechanism that allows data integration is *pivoting*. **Pivoting** refers to the ability of going from one data source to another, which is usually performed by using links to navigate among windows that show related information. Thus, if there is an incident, the security operator will be able to investigate it and obtain contextual information. Let us imagine that there is a record that has been signaled as anomalous. By means of pivoting, it is possible to jump from the record to another window with detailed information of the related IPs, such as reputation information, whois, or domain names. Thus, pivoting reduces considerably the time needed to investigate a security incident (especially if the pivoting is graphically assisted) [24].

Finally, a further form of integration is the one used when Machine Learning (ML) techniques are applied over security data. In the context of ML, integration is often referred to as data *fusion*. **Fusion** allows to obtain a single stream of data from several disparate sources that can be dealt with properly by the rest of the modules. Data fusion is frequently classified in: *low*, *middle* and *high*, depending on how the sequence of data fusion and modeling is done through ML. If data fusion is performed from raw data, before modeling, then it is called **low-level**. If it is done after some form of data transformation or feature extraction, then it is called **middle-level**. If data fusion takes place after ML modeling and combines the output of several ML techniques, is called **high-level** [25]–[27].

D. DETECTOR MODULE

This is an essential part in an NSM system. **Detectors** are actually engines which goal is to detect suspicious behavior in the data. The volume of data to be analyzed can be reduced by filtering or grouping data, by feature extraction (considering only those features that are of interest) [28], [29], or by using a correlation engine [16], [17], [23].

Detection engines are usually classified in **signature-based**, if they use a library of patterns (*e.g.* rules or traces of code) to detect known attacks, and **data-driven**, if they use models of normal behavior to detect abnormal activities [5], [28]–[31]. The latter can also be *i) statistical-based*, *ii) knowledge-based*, and *iii) ML-based* [29], [30].

In general, the main drawbacks of signature-based detection are the need for frequent updates of the signature database, and the inability to detect *zero-day* attacks [31]. When data-driven detection is ML-based, supervised methods cannot detect zero-day attacks either, although they have a high performance detecting known attacks. Finally, unsupervised detection can in principle detect zero-day attacks, although it may generate many false alarms. Thus, a main challenge of unsupervised detection is to reduce the amount of false alarms, which can be performed by prioritizing and/or visualizing the events [15], [32]. This can also be achieved thanks to existing lists that contain events likely reported as false positives, which allow to avoid escalating those events as alarms [5], [33], [34].

In general terms, the number of security events, the velocity, and the pace in which they are generated is so high that security operators usually cannot handle all of them, and proper prioritization/triaging turns mandatory [15]. This can be achieved by defining metrics going beyond those traditionally used for the capability of detection (*e.g.* Receiver Operating Characteristics (ROC) or Area Under the Curve (AUC)). These metrics should provide information about the importance of an anomaly, rather than only detecting whether a given event is anomalous or net [35].

E. INSPECTOR MODULE

The NSM cycle includes the **diagnosis** of the detected IT Security incidents. This step helps the analysts to identify the root causes of the incident (forensics) so that problems within the network can be timely identified and corrected for [35], [36]. Besides, when an IT Security incident takes place, it is advisable recording the current state of the system and network. This may involve saving configurations, logs, users logged in the system or processes that where running when the incident occurred. The **inspector** module is responsible of performing these tasks. Additionally, it is desirable that this module includes a diagnosis engine, which can help, in combination with the detection component, to prioritize and triage the events [37].

Diagnosis is usually related to forensics tasks, where the origin of the alarm needs to be found [38]. To do this, we need to find the location of the incident, which is related to both

[2] Note that the term correlation in IT security has a different meaning to the traditional one in statistics.

the physical origin of the alarm (*e.g.* devices or sensors) and to the timing in which the incident took place (*e.g.* when it started and its extension in time). This is a difficult task that is usually performed manually by security operators [38], [39], although some works have proposed ML-based solutions to tackle this problem [40]–[44]. For example, authors in [40] propose two solutions: the first one is model-based and the second one is data-driven. Diagnosis is also dealt in the context of black box ML by using gradients in an unsupervised way [41]. These methods are frequently complex, since they require a big effort to implement and are hard to interpret for an analyst. Interpretation becomes easier if linear methods are applied, such as Principal Component Analysis (PCA) [42], [43]. In any case, using linear methods for diagnosis simplifies the definition of the inspector module, which allows to identify the variables related to a previously detected incident.

F. ACTUATOR MODULE

After an IT Security incident takes place and it is detected by the NSM system, the response and recovery of the system are of main importance. The aim of this step is recovering the affected systems to a secure state to minimize loses and damages suffered by the compromised organization. This stage can be carried out manually, by security operators; or automatically, by using an **actuator module** that implements response policies and actions against certain events [3], [45], [46]. Some authors [45] recommend following an OODA (Observe, Orient, Decide, Act) loop, which allows facing the attacks efficiently. This cycle is closely related to the NSM philosophy.

Typical response actions are discarding or modifying traffic that is related to the attack [34], as well as creating and restoring security backups [45]–[47]. In addition, reducing permissions and/or changing passwords for involved users in the affected network, as well as isolating and cleaning infected hardware and software can be other typical responses after an IT Security Incident is detected [47], [48]. Another advisable action (which is also related to the inspector module) is to register and analyze all events, records and acts related to the incident, so that similar problems can be detected and efficiently dealt with, or even prevented, in the future [48], [49].

Finally, one of the most important actions after detecting an IT Security Incident is to notify it to the stakeholders (*e.g.* workers, clients and/or corresponding authorities) so that they are aware of the issue and can take additional actions if needed [48], [50]. Yet, this action should not be considered as a single mechanism of response, but a complement to be applied in combination with any of the aforementioned response actions.

III. NSM SOLUTIONS IN THE MARKET

This section reviews some of the tools for the trade, following the modular taxonomy proposed in this paper. This classification starts with sensors and parsers, which are often found implemented in form of individual solutions, namely **single-module solutions**. Then, we present some examples of network security products that implement several NSM modules, namely **multi-module solutions**. Finally, as a part of the multi-module solutions, we include a collection of security tools that may be also considered as security sensors.

A. SINGLE-MODULE SOLUTIONS

In this part of the section, we enumerate different types of single sensors, which can be classified according to the type and origin of data that they collect in: *i) Network Traffic Sensors*, and *ii) Log and State Sensors*. Then, we present different types of single parsers, which can be classified according to their way of working in: *i) Command-based Parsers*, and *ii) Software-based Parsers*.

1) NETWORK TRAFFIC SENSORS

Traffic data can be collected directly from the network in different formats. Some of these formats are *packets*, *traffic flows*, and *traffic statistics*. All of them are described in the next paragraphs.

PACKETS

Each communication that uses the TCP/IP protocol stack is split into packets, which are individually routed to their destination [4], [5], [33]. Sensors usually capture packets using a programming library such as ***libpcap*** [51] and store them for later analysis. The most common format for the storage is `pcap`, a binary format that can be read by almost any sniffer and traffic analysis tool [4], [5], [15], [32]. There exist several tools for collecting network traffic. The most popular are ***Wireshark*** [32], [52] and ***tcpdump*** [51], which listen in a network interface and display or store the collected network traffic. They analyze the raw data from complete packets, displaying their information in an understandable format to users. `Wireshark` offers a Graphical User Interface (GUI) to explore packets, together with a command line tool, ***tshark***, while `tcpdump` only offers command line options [4], [5], [15], [24], [32], [33]. `Tshark` provides a more powerful and complex syntax to analyze traffic than `tcpdump`. However, in practice, `tcpdump` is the most used since it is more simple. `Wireshark` can also be employed to obtain flows, sessions and traffic statistics [52].

The main drawback of capturing packets is that it implies a huge volume of information, rendering it impractical for long captures. An alternative solution is to filter data to reduce the size of the capture [32].

TRAFFIC FLOWS

The information extracted from traffic flows provides a higher abstraction level, reducing the volume of data stored in comparison to packet captures, while still allowing a considerable amount of information. Traffic flows are also known as *traffic sessions*. One of the most extended protocols to capture flows is `NetFlow`, which was developed by Cisco Systems to extract and send information of traffic flows [53]. Although `NetFlow` was not originally developed for IT

Security, it is widely used in this context, since it provides a highly valuable summary of the flows. Two of the most relevant tools used for collecting and analyzing flows information are ***Argus*** and ***nfdump*** [32]. `Argus` collects and transforms session data [54], which are displayed and analyzed with the ***Ra*** client [32], [55]. `Nfdump` is a set of tools (including ***nfcapd*** and the homonym command ***nfdump***) for collecting and processing `NetFlow` data through the command line. `Nfcapd` *collects* `NetFlow` data while `nfdump` *reads* the files stored by `nfcapd` using an analysis syntax similar to that of `tcpdump` [32], [56].

TRAFFIC STATISTICS

This information is related to certain features of the network traffic, such as traffic volume or type of traffic, among others. Statistics do not allow to perform a forensic analysis *per se*, but help security operators in their investigation, complementing the data collected by other tools. One of the most extended tools to gather traffic statistics from network interfaces is the ***Simple Network Management Packet (SNMP)*** [57]. SNMP is an application layer protocol that allows to retrieve and interchange management information from network devices. This information can be collected using for example the ***Open SNMP***[3] distribution. `Wireshark` and `tshark` can also be used to obtain traffic statistics.

2) LOGS AND STATE SENSORS

Logs and state sensors gather information from applications or operating systems, among others. These sensors can be used either individually or to complement the information collected by other sensors that usually provide more detailed information. The sources include (but are not limited to): network management protocols, such as SNMP; system logs, such as `syslog`, which can be captured with tools like ***syslog*** [58]; or *Application Logs* obtained, for example, from ***Apache*** or ***sendmail***.

SYSLOG

This is a protocol implemented in the application layer to generate logs related to the activities in a system. This protocol records events, such as logins to a host or a server. This is also useful to launch alerts related to activities or errors in the operating system or the hardware, among others. Considering the type of resource that generates a record, in combination to the type of alert, it is possible to establish a scale of priorities, which is useful to help the security operators to manage such alerts.

APPLICATION LOGS

Each application service, such as web surfing or the e-mail, has its own format to record the logging information. ***Apache web server*** or ***Sendmail*** are only examples of applications that can generate logs. `Apache` is the most extended web server. It can provide data about the configuration of the websites as well as the databases, but also statistics about access to web pages. On the other hand, `Sendmail` is a Mail Transport Agent, which is in charge of routing the e-mails to their destination. Email logging data can be useful to investigate whether an affected host had exchanged any message with other machines before being compromised, and the nature of such messages.

Application Log sensors allow anomaly detection, registration of system accesses (both successful and failed), and prioritization in relation to the type of resource involved in an anomaly. This information can be useful for the investigation after an IT Security incident is detected [5], [15].

3) COMMAND-BASED PARSERS

Command-based parsers are Linux commands that can be used to find patterns matching with regular expressions. Depending on the selected command, they allow taking different actions on the filtered data. Thus, they can be used to create scripts for data parsing. Some of the best known Linux commands that allow parsing are ***awk***, ***grep***, or ***sed***. [59], [60].

4) SOFTWARE-BASED PARSERS

Software-based parsers are programs that allow extracting information from complex data. To do it, they look into the data to extract patterns automatically. This is performed by means of algorithms and configuration rules, rather than only using regular expressions. Some examples of tools that implement the parser module are ***Logstash*** [61] and the ***FCParser*** [22]. `Logstash` is part of the *Elastic Stack* [20], while the `FCParser` is a library for network data parsing. Both tools can parse data from several and disparate sources, including the transformation from unstructured data into structured data and the management of big data.

B. MULTI-MODULE SOLUTIONS

This section collects some network security tools that implement several NSM modules. Due to its growing importance in the last years, we pay special attention to *Intrusion Detection Systems (IDSs) / Intrusion Prevention Systems (IPSs)*, *Security Event Managements (SEMs) / Security Information and Event Managements (SIEMs)* systems, *Universal Threat Managements (UTMs)*, and tool collections; including examples of both open source and commercial solutions. We also consider other well-known security tools that are interesting from the NSM perspective, since they might be also considered *security sensors*.

Table 1 summarizes the studied solutions and the NSM modules that they include. This table aims to provide a quick insight into the main functionalities and features that the best known NSM solutions can provide. The '✓' is used to indicate that the solution implements the corresponding component, while the '-' symbol is used to indicate that the corresponding component is not implemented in the solution. The '◇' symbol is used to denote that the solution does not implement that component but there exist plugins to implement it. Finally,

[3] https://sourceforge.net/projects/opensnmp/

the '★' symbol is used to point out that the solution integrates another tool to implement the corresponding component.

1) IDSs AND IPSs

Intrusion Detection Systems (IDSs) are one of the most used security tools. They are mainly composed of a sensor, a parser, and a detection engine. When these systems also allow to deploy defensive responses to attacks, *i.e.* they include an actuator module, they are called **Intrusion Prevention Systems (IPSs)**. Some of the IDSs have evolved to **Security Event Management (SEM)** systems, which include an integrator module to improve the capability of detection by collecting data from different sources [32].

IDSs are systems that implement a set of techniques to detect suspicious activities (potential intrusions) by monitoring and analyzing the events in a network or a device [28], [32], [34]. They are classified as *Host IDS (HIDS)* and *Network IDS (NIDS)* according to the origin of the collected data [31], [34], [62]. **HIDSs** are deployed in end systems (hosts) and monitor user activity and the behavior of internal processes [5], [31], [33], [34]. **NIDSs** first collect data from the network using any of the aforementioned network traffic sensors; then, they analyze the data to find security violations. Regardless the type of IDS, once data are received and identified as (potentially) harmful, the system alerts security operators.

Since the best known IDSs are open source, we only include this category in our review.

SNORT

This is the most popular IDS, and it can be used also as a sniffer [34]. Snort is a signature-based NIDS, which allows port scanning, as well as registering and alerting for any defined anomaly. In the latest releases, this IDS also permits to define basic responses in form of rules that allow blocking network traffic related to a given alert [63]. `Unified2` is the output logging format generated by Snort. Logging can be generated in three modes: *packet logging*, *alert logging*, and *true unified logging* [64]. **Packet logging** is used for packet captures while **alert logging** only registers IT Security events. **True unified logging** allows recording both events and packets.

SURICATA

Suricata is both a real-time network IDS and a network IPS. It monitors the network traffic and performs offline processing of `pcap` files. Suricata is signature-based and provides the output in standard formats, such as `YAML` or `JSON`, but it can also be configured to generate logs in `Unified2` [65], [66].

OSSEC

This is an open source HIDS that performs log analysis, integrity checking, monitoring of Windows records, and rootkit detection. In addition, OSSEC provides alerts and maintains a copy of the modified files to perform forensics tasks. It also allows to configure firewall rules to block malicious network traffic, including specific IP addresses. OSSEC is multi-platform, since it can be used in most of the operating systems. Although this engine has some SIEM features, such as allowing the correlation of logs from several devices and formats, and mechanisms for compliance of security policies, it has been traditionally considered to be an IDS [67].

2) SEM AND SIEM SYSTEMS

A Security Event Management (SEM) system is in charge of "1*the collection, analysis and escalation of indications and warnings to detect and respond to intrusions*" [24]. Its aim is to visualize and understand network data by using a single and unified tool that combines different data sources (integrator). For that purpose, a SEM allows pivoting among different data sources to carry out data analysis and forensics, which reduces considerably the time needed to investigate a security incident (especially if the pivoting is graphically assisted) [24]. One of the features that makes a SEM system to be such a powerful tool is that it allows the visualization and prioritization of the events, thus helping security operators to interpret and understand the alarms [34], [68].

A Security Information and Event Management (SIEM) system can be described following the definition provided by Gartner [68], [69] as a system that "*analyzes event data in real time for early detection of targeted attacks and data breaches, and collects, stores, investigates and reports on log data for incident response, forensics and regulatory compliance*". SIEM systems are the combination of two different systems: SEM and Security Information Management (SIM) systems. The main difference in relation to the SEM is that a SIEM also performs reports and include features for regulatory compliance, while the SEM does not necessary do that (indeed, this is a functionality usually provided by the SIM module). SIEM are the most popular (and expensive) type of integrator systems in the industry. Like SEMs systems, SIEMs are usually composed of at least the following components: sensor, parser, integrator, detector and inspector. They can also include response modules.

We start this classification with a SEM and three SIEMs that are open source: ***Zeek***, ***Prelude***, ***Wazuh*** and ***OSSIM***.

ZEEK (Bro)

Zeek was originally developed by Vern Paxson and Robin Sommer [70] as a research work called Bro. Now, it has evolved and it is widely used by companies, as well as research and educative organizations [70]. This is a complete open source tool for NSM that permits both anomaly and signature based detection [32], [70]. Zeek collects network traffic using `libpcap`. Then, the engine of events processes the data, performing a passive analysis on such data. It also allows collection and analysis of sessions of particular services. In addition, Zeek can be programmed to take actions in the evaluation of events (*e.g.* to execute a program to provide active response for the detected event) and offers forensics capabilities thanks to its mechanism of event logging [70],

TABLE 1. NSM modules provided by the studied solutions. The '✓' is used to indicate that the solution implements the corresponding component. The '-' symbol is used to denote that the corresponding component is not implemented in the solution. The '◇' symbol is used to point out that the solution does not implement that component but there exist plugins to implement it. The '★' symbol is used to indicate that the solution integrates another tool to implement the corresponding component.

Type	Solution	Sensor	Parser	Integrator	Detector	Inspector	Actuator
IDS / IPS	*Snort*	✓	✓	-	✓	-	✓
	Suricata	✓	✓	-	✓	-	✓
	Open Source Host IDS (HIDS) SECurity (OSSEC)	★	✓	✓	✓	✓	✓
SEM	*Zeek*	✓	✓	✓	✓	✓	✓
SIEM	*Prelude*	★	✓	✓	✓	✓	-
	Wazuh	★	✓	✓	✓	✓	✓
	Open Source Security Information Management (OSSIM)	★	✓	✓	✓	-	-
	Splunk	★	✓	✓	✓	✓	✓
	USM	★	✓	✓	✓	◇	✓
UTM	*CloudGen Firewall*	✓	✓	-	✓	✓	✓
	WatchGuard	✓	✓	✓	✓	-	✓
	Sophos	✓	✓	-	✓	-	✓
Tool Collections	*Sguil*	★	★	-	★	★	★
	Security Onion	★	★	★	★	★	★
Other Security Tools (Security Sensors)	Firewalls	✓	✓	-	✓	-	✓
	Vulnerability Assessment	✓	-	-	✓	-	-
	File Integrity Monitoring (FIM)	✓	✓	-	✓	-	-
	Antivirus	✓	✓	-	✓	-	✓
	Threat Intelligence	-	-	-	-	-	-

[71]. Although it is usually included in the IDS classification, Zeek can be considered a SEM [4], [24], [70].

PRELUDE

This is a SIEM for Linux that collects, normalizes, combines and correlates security events. Prelude implements the IDMEF standard format (RFC 4765) as a part of the parsing component, so that it can read a wide range of log formats [72]. In addition, it generates reports about events. Its interface provides a forensic mode that allows to investigate data from large periods [73]. Therefore, Prelude implements all the NSM components excepting the response module. This SIEM can be used in a commercial version, which prices are customized for each organization and depend on the volume of events [74].

WAZUH

This is a SIEM for signature-based intrusion detection, which was developed by the homonym company [75]. Wazuh is based in OSSEC and it is used in combination with the *Elastic Stack* [21]. This allows the monitoring of the system for security analysis, intrusion and vulnerability detection. Furthermore, Wazuh provides response to security incidents, including integrity and compliance [75]. Thanks to the Elastic Stack features [20], the parsing component is implemented.

OSSIM

This SIEM was developed by Alien Vault (AT&T Cybersecurity since February 2019) [76], and it uses the Open Threat Exchange®(OTX®) [77] threat intelligence module, which allows the users to contribute and receive updated information in real-time about security information. OSSIM allows the collection, normalization and correlation of events. Thus, the capabilities of OSSIM include discovering *assets*,[4] assessing vulnerabilities, intrusion detection, monitoring of behavior, and correlation of events [78]. It integrates different software modules to provide a complete NSM solution. Among other tools, this solution includes both a host and a network IDS. The NIDS part provides intrusion detection and network traffic scanning. It also looks for signatures of the latest attacks, as well as for malware or other possible ways of attempting to compromise the system. The HIDS analyzes the behavior and state of the system, alerting when it suspects that there is something wrong. Similarly to other SIEMs, OSSIM allows to detect and prioritize the most important threats and anomalies [78].

Commercial Tools

This part of the section covers two examples of commercial SIEM systems, both included in the Gartner's "Magic Quadrant for Security Information and Event Management" for 2020 [79]. Magic quadrants assess the products in the market according to a set of criteria, which are mainly the *Ability to Execute* and the *Completeness of Vision*. **Ability to Execute** refers to the economic power of a vendor to implement relevant functionalities, and **Completeness of Vision** can be seen as the ability to understand present and future needs of the market. The Magic Quadrant of Gartner has four categories: *Leaders*, *Challengers*, *Visionaries* and *Niche Players*. **Leaders** have both high ability to execute and completeness of vision of the market, **Challengers** have high ability to execute but limited vision on the market, **Visionaries** have a good vision of the market but do not have competitive ability to execute, and **Niche Players** are focused in a small segment of the market (or do not have a complete vision of it) and have a limited ability to execute [80].

[4] In the case of OSSIM, asset is referred to machines.

Some of the most highlighted SIEM, according to the Magic Quadrant [79], are: ***Splunk*** and ***IBM*** (''Leaders''); ***AT&T Cybersecurity*** and ***FireEye*** (''Niche Players''); and ***LogPoint*** (the only one in the ''Visionaries'' category). Our classification covers Splunk and AT&T Cybersecurity.

SPLUNK

This is a commercial SIEM, which performs network monitoring and real-time data collection, parsing and correlation. Splunk also allows incident management (*e.g.* running a script or applying threat intelligence) and forensic analysis thanks to its mechanism of event correlation. It allows data and event analysis, providing visibility and context of the alerts. In addition, it uses Big Data techniques to integrate the data from the organization to be monitored (User Behavior Analytics), allowing to improve the intrusion detection by using machine learning algorithms [81], [82]. Splunk is considered as a *Leader* in the Gartner's Magic Quadrant because it provides SIEM solutions that *i)* are compatible with other different SIEM systems and scenarios and *ii)* are scalable and allow performing a wide range of actions related to both log management and response against IT security incidents (see Gartner's Magic Quadrant in [83]).

USM (AlienVault®UNIFIED SECURITY Management®)

This is a commercial SIEM based in OSSIM, and it was also developed by Alien Vault (AT&T Cybersecurity since February 2019) [76]. USM is a unified platform for threat detection and policy compliance (which is one of the main differences in relation to OSSIM, see [84] for more details), as well as incident response. ***AlienVault USM Anywhere*** provides USM as a cloud service [76]. Although it does not provide an inspector module, it is possible to complete this part of the NSM cycle by using the plug-in ***AlienApp*** [85]. USM is considered as a *Niche Players* in the Gartner's Magic Quadrant, since it is focused in specific sectors (such as financial services and healthcare) that are usually Small and Medium Businesses (see Gartner's Magic Quadrant in [83]).

3) UTMs

This is a type of ''*multi-function network security product used by small or midsize business*'' [86]. These devices have high level functionalities (multi-function gateway), which can be, for example, a firewall in the application layer of the TCP/IP and OSI models, Intrusion Prevention and Detection (IPS and IDS), antivirus, anti-spam and anti-phishing [87], [88]. The main advantages of the UTMs are their reduced cost and complexity, while the drawbacks are that UTMs usually have limited processing power, and they cannot correlate events.

Since these are hardware solutions, it is not possible to find open source implementations. Thus, we only include commercial tools in this part of the review.

This part of the section shows three examples of commercial UTM systems, all of them included in the Gartner's ''Magic Quadrant for Universal Threat Management'' for 2018 [89], [90]. Again, this quadrant assesses the UTMs in the market according to the same criteria as for SIEM systems and classifies them in: Leaders, Challengers, Visionaries and Niche Players (recall Section III-B2).

Some of the most highlighted UTM, according to the Magic Quadrant [89], [90], are: ***Huawei*** and ***SonicWall*** (''Challengers''); ***Fortinet*** and ***Sophos*** (''Leaders''); ***Juniper Networks*** and ***Barracuda Networks*** (''Niche Players''); and ***WatchGuard*** (the only one in the ''Visionaries'' category, and close to be a ''Leader''). Our classification covers Sophos, Barracuda Networks, and WatchGuard.

BARRACUDA CloudGen FIREWALL

This is a commercial UTM that provides intrusion detection and protection. CloudGen Firewall also protects against known attacks, such as Denial of Service (DoS) or botnet attacks. In addition, this solution enables authentication and VPN connection. Its firewall allows packet inspection and filtering [91]. CloudGen Firewall is classified as a *Niche Player* in the Gartner's Magic Quadrant in 2018 [89].

WatchGuard

This is a commercial UTM that provides intrusion detection and protection. WatchGuard correlates data from different sources, which enhances its capability of detection and response against threats, being also able of generating reports. In addition, it provides an antivirus functionality and application control, which is related to user's behavior. WatchGuard offers an Advanced Persistent Threat blocker that allows detecting and acting against complex attacks, such as ransomware; and it also has a spam prevention functionality [92]. WatchGuard is considered to be the only *Visionary* in the Gartner's Magic Quadrant in 2018 [89].

SOPHOS

This is a commercial UTM that provides intrusion detection and protection. Sophos allows discovering and acting against threats, which makes it possible mitigating the effect of such threats. After Sophos detects an infected system, it isolates that system. In addition, it provides mechanisms for remote access, such as VPNs. This solution also includes an advanced firewall to monitor traffic data and anti-spam functionalities [93]. Sophos is classified as a *Leader* in the Gartner's Magic Quadrant in 2018 [89].

4) TOOL COLLECTIONS

This type of network security tools are composed of a number of disparate software solutions. Furthermore, since they are open source they are continuously evolving.

SGUIL

This is a set of open source tools for network security monitoring, which allows to collect, analyze, alert and respond to intrusions [4], [94]. Sguil provides a real-time interface and includes two IDSs [34], [94]. Some of the tools that compose Sguil are [94]:

- ***MySQL***, as a database service.
- ***Snort*** and ***Suricata***, for network intrusion detection and scanning as well as packets logging and solving alerts. Squert[5] is an evolution of Sguil which also uses ***OSSEC*** and ***Zeek*** for intrusion detection [95].
- ***Tcpdump***, to collect network traffic from the logs of the packets.
- ***Wireshark***, to analyze the collected packets.

SECURITY ONION

This is a collection of open source tools, which is provided as a Linux distribution. Security Onion allows to monitor, record and manage logs, as well as to perform intrusion detection and response against IT Security Incidents [96]. It implements all the NSM modules. Some of the tools that compose Security Onion are [96]:

- ***Elastic Stack*** and ***Logstash***, as a search and analysis engine that also transform and centralize the data, providing visualization functionalities and implementing the parsing module [21], [61], [97].
- ***Snort***, ***Suricata*** and ***Zeek***, for network intrusion detection, scanning and issuing alerts, as well as packets logging.
- ***Wazuh***, for host intrusion detection.
- ***Sguil***, for network security monitoring and event drive analysis.
- ***Squert***, to consult and visualize Sguil data.
- ***Cyberchef***, to encrypt, compress and analyze data.
- ***NetworkMiner***, for forensic analysis.

5) OTHER WELL-KNOWN SECURITY TOOLS (Security Sensors)

In this section we have included some systems, resources, and tools that, from the NSM perspective, provide useful security information. Thus, although these are security tools by themselves, they also can be considered acting like security sensors as a part of more complex NSM systems (*e.g.* SIEM systems).

FIREWALLS

Firewall logs are one of the most useful security data sources, since they provide information about each access (failed or successful, authorized or not) to the network. One of the main advantages of firewalls is that they can be found in any network. We can find basic examples, such as the one provided as a part of ***Windows Defender*** in Windows 10 operating systems [98]; but also advanced firewalls, such as Sophos [93], which actually are enclosed in UTM solutions.

VULNERABILITY ASSESSMENT

Vulnerability assessment tools are run on the network and end systems. These tools unveil weaknesses and security holes that may enable an unauthorized access to the system. Two well-known tools for this purpose are ***Nmap*** [99] and ***Nessus*** [100]. `Nmap` (Network Mapper) is an open source program for port scanning to evaluate the security of the operating systems, allowing to discover vulnerabilities and providing useful information about open ports and services. Although `Nmap` was originally developed for Linux, it is now multi-platform [4], [32], [33], [99]. `Nessus` is also a multi-platform program for vulnerability scanning in operating systems. Originally, `Nessus` was open source, but now it is private software (although there are open-source alternatives, such as ***OpenVAS*** (Open Vulnerability Assessment Scanner) [101]). The vulnerability assessment analysis usually starts with a port scanning, which can be done, for example, using `Nmap`. Once the open ports are discovered, `Nessus` sends a number of probes against such ports to unveil existing vulnerabilities. The results can be exported to different formats, such as plain text or XML [100].

Other useful resources that allow to obtain vulnerability data are the ***National Vulnerability Database (NVD)*** and ***Common Vulnerabilities and Exposures (CVE)*** databases. NVD is a public service provided by the National Institute of Standards and Technology of the United States (NIST) to enumerate and classify existing vulnerabilities in current software and hardware [32], [102]. CVE is another similar service provided by the MITRE[6] that also includes the NVD [103]. These databases offer the most updated information about known vulnerabilities in operating systems and applications/services, and their solution (if known). Vulnerabilities are usually discovered either using any of the aforementioned or similar tools.

FIM

FIM systems allow to detect changes in the files stored at the devices in relation to a base copy of such files. Some of the parameters that are checked by a FIM are: *i)* the modification/creation date, *ii)* the permissions of access and modification, and *iii)* the checksum (hash) of the contents. One of the problems of this type of data source is the huge volume of data and the number of false positives that it tends to generate. One of the tools that implements FIM capabilities is OSSEC [67].

ANTIVIRUS

These programs are used to detect and remove malware from computers. Antivirus software are usually signature and/or rule based, and they are designed to analyze computer files. They are not typically designed to work as sensors. Yet, sometimes it is possible to configure them for log generation, which makes them useful as security sensors for NSM systems [104]–[108]. For example, ***Kaspersky*** has both free and commercial antivirus [109]. The first one provides basic protection while the commercial version provides additional tools such as VPN connection or password management. Another well-known example of antivirus is ***Windows Defender***, which is included in Windows 10 operating system [98].

[5] http://www.squertproject.org/

[6] https://www.mitre.org/

THREAT INTELLIGENCE

This is a mechanism, similar to a social network or RSS feeds, which allows users to contribute and receive updated information about security threats and/or issues. It allows sharing useful security information among organizations, which can also be useful to enhance detection engines. For example, if an organization detects a new attack, the rest of organizations using threat intelligence are informed, allowing them to prevent or deal with the attack in a more efficient way. Furthermore, threat intelligence uses knowledge related to the organization, including context or risk indicators, but also existing reports about previous attacks, among other data [110]. The goal of using information from the organization is to foresee threats based in the previous experience, taking into account threats both inner or external organization. Threat Intelligence tools are in charge of collecting this information and generating reports or alarms that can be integrated with other security mechanisms, such as SIEM systems. ***Threat connect*** [111] and ***Cyber Threat Alliance*** [112] are two commercial tools for threat intelligence, while ***Open Threat Intelligence*** [77] and ***Collective Intelligent Framework*** [113] are examples of open source solutions.

IV. NSM APPLICATION AND CHALLENGES FOR NEW PARADIGMS IN COMMUNICATIONS NETWORKS

5G networks and new communication paradigms, such as the Internet of Things (IoT) or cloud computing, make network management to be more complex [7], [114]–[118]. The wide adoption of the 5G leads to massive data generation, which is getting more and more increased at a high pace [7], [8], [114], [119]. Big Data processing, as well as feature extraction and data correlation are some of the main challenges affecting anomaly detection and, thus, intrusion detection, which are a main part of the NSM philosophy. Some works tackle intrusion detection in high-dimensional data from an anomaly detection perspective [8], [119].

In addition, distributed and decentralized networks are present and future of technology. This implies numerous benefits but also new challenges, specially for network security. In this section, we focus on some of the most relevant communication models in the present: *i)* SDN, and *ii)* IoT/ Industrial IoT (IIoT). In addition, we review those tools that were included in Section III and its potential use for each of the aforementioned modern networks. Finally, we identify current research needs for the proposed modules in Section II.

A. MULTI-MODULE NSM SOLUTIONS AND WORKS FOR MODERN NETWORKS

This section lists and classifies a collection of security solutions for modern network that cover one or more NSM modules, following the proposed taxonomy. Table 2 summarizes the reviewed solutions and the NSM modules that they include. This table aims providing a quick insight into the main functionalities and features that these works can cover from the NSM perspective. The '✓' is used to indicate that the solution implements the corresponding component, while the '-' symbol is used to indicate that the corresponding component is either not implemented or its covering is not clear in the solution.

SDN

The huge data volume derived from using mobile networks massively led to a new proposal for networks management optimization in 2016: the softwarization and virtualization of networks (SDN and Network Function Virtualization (NFV), respectively) [114]. Yet, these new paradigms are at the same time solution and problem from the security perspective. Like this, adopting SDN and NFVs introduce new vulnerabilities and security requirements, being the availability one of the most relevant [114], [116], [120], [126].

A number of works tackle these new security issues related to the SDN, some of them aiming to enhance the detection techniques or following a security monitoring approach [116], [120], [121], [123], [124], [126]–[128], [132]. In addition, Santos da Silva *et al* manifest the need of human intervention during the monitoring cycle [120]. On the contrary, other authors are more focused in a complete automation of the process, using deep learning to implement IDSs to increase data correlation and to be able to detect zero-day attacks [11], [121]. Finally, other authors follow approaches such as malware monitoring [131] or Threat Intelligence for SDN [132].

Additionally, it has been highlighted that it is needed to adapt traditional intrusion detection to virtualized networks, more precisely, to SDN [116], [120]. In this sense, some of the tools that where analyzed in Section III have been used in the SDN scope. For example, Snort is applied for intrusion and Distributed DoS (DDoS) detection by different authors [122], [124], [125]. On the other hand, Suricata is also used for intrusion detection in SDN [127], [128]. Finally, Barracuda, Sophos and WatchGuard provide SD-WAN (SDN-Wide Area Network) solutions [93], [129], [130], [144], [145].

IoT AND IIoT

IoT is characterized by designing a myriad of devices/gadgets that can be connected anywhere to a network. These devices range from smartphones to cars, but also include daily objects, such as fridges or televisions, and products in warehouses and stores. Nowadays, devices are hyper-connected both in local environments (*e.g.* personal wearables or smart homes) and in wide environments (*e.g.* smart cities) [146]. IoT networks are decentralized, which, in combination with its own nature, makes the traditional security requirements to be affected. There are a number of challenges and requirements in IoT security [147]–[152]. Similar to traditional networks, the most relevant requirements are related to privacy, confidentiality, integrity and availability. The latter is currently one of the most challenging issues in network security [147]–[152]. In general terms, the most important needs in IoT security are: providing scalability, interoperability, managing Big Data,

TABLE 2. NSM solutions and works in modern networks. The '✓' is used to indicate that the solution implements the corresponding component. The '-' symbol is used to point out that the corresponding component is not implemented in the solution.

Scope	Solution Type	Reference	Sensor	Parser	Integrator	Detector	Inspector	Actuator
Big Data	Monitoring Tool	[119]	✓	✓	-	✓	✓	-
SDN	IDS	[120]	✓	✓	-	✓	-	✓
	IDS	[11, 121]	✓	-	-	✓	-	-
	IDS	[122]	✓	✓	-	✓	-	✓
	IDS	[123]	✓	✓	-	✓	-	✓
	IDS	[124]	✓	✓	-	✓	-	-
	IDS	[125]	✓	-	-	✓	-	-
	IDS	[126]	✓	✓	-	✓	-	-
	IDS/IPS	[127]	✓	-	-	✓	-	✓
	IDS/IPS	[128]	✓	-	-	✓	-	✓
	UTM	[129]	✓	✓	-	✓	✓	✓
	UTM	[93]	✓	✓	-	✓	-	✓
	UTM	[130]	✓	✓	✓	✓	-	✓
	Malware Monitoring	[131]	✓	-	-	✓	-	-
	Threat Intelligence	[132]	✓	-	-	✓	-	✓
IoT / IIoT	IDS	[133]	✓	✓	-	✓	-	✓
	IDS	[12, 134]	✓	-	✓	✓	-	-
	IDS	[135]	✓	✓	-	✓	-	-
	IDS	[136]	✓	✓	-	✓	-	✓
	IDS	[137]	✓	-	✓	✓	-	✓
	IDS	[138]	-	-	-	✓	-	-
	IDS	[139]	✓	✓	-	✓	-	✓
	IDS	[140]	-	-	-	✓	-	-
	IDS	[141]	✓	✓	-	✓	-	-
	Security Platform	[142]	✓	-	-	✓	-	✓
	Monitoring Tool	[143]	✓	-	-	✓	-	✓

tackling with restricted resources, and providing resilience and robustness [147]–[150], [152].

All the aforementioned needs are extensible to the NSM philosophy. Furthermore, data integration and correlation are other important challenges from the NSM perspective [8], [153]. Recently, some authors have pointed the need of designing and implementing high-level SIEMs and effective IDSs that can be adapted to IoT protocols [137], [152], [154]–[156]. Most of research papers in recent years have been focused in the proposal of new IDSs and/or enhancing the detection methods [133], [135], [137]–[139], [157]. Additionally, some authors take explicitly into account the constraints in IoT resources in their IDS proposal [137]. Other authors highlight the necessity of anomaly detection and mitigation in IoT networks [156], [158], as well as the lack of IoT datasets for training and testing detection algorithms [13], [141].

In relation to commercial tools, Bitdefender proposes an IoT solution that provides different alternatives depending on the pricing [142]. These features range from 'Cloud Essentials' (it only includes basic protection) to IoT 'Full Stack' (including, IDS and IPS, anomaly detection, and DDoS detection and protection among others) [142], [159]. This tool is recommended by Kaspersky as an alternative option to their scan tool (in a Beta state since 2018) [106]. Finally, Avast provides a monitoring solution for smart homes, which aims to prevent, detect and contain security incidents related to all the connected devices [143], [160].

Furthermore, some authors highlight that there is a need to adapt traditional security mechanisms to IoT networks [147], [151]. In this sense, if we review the tools analyzed in Section III, Barracuda is the only one that has an IoT version of its traditional product, CloudGen Firewall [161].

On the other hand, according to Gartner, one of the most relevant global risks in the end of 2019 and the first quarter of 2020 was derived from the convergence between physical and cybernetic world. This connection is in part empowered by the massive IoT adoption. In March of 2020, this risk was relegated to a secondary place after the pandemic situation was declared [162], [163]. Yet, there is still a high risk that is greatly due to the wide adoption of IoT in different scopes such as smart homes, e-health or smart cities. Besides, IoT has been successfully adopted in industry, which application is called Industrial IoT (IIoT) [118], [146], [164]–[166]. This aims monitoring and controlling industrial processes to enhance their effectiveness and quality [164]. Thus, IIoT is of utmost importance in gas, petrol and energy industries (which are also considered critical infrastructures); and it is gaining relevance in other areas, such as agriculture and health [155], [165]–[170]. Thus, IIoT can be considered to be one of the pillars of Industry 4.0 [118], [165], [167], [168].

IIoT inherits complexity and risks from IoT. Additionally, it has particular requirements that, sometimes, are related to the deal with risks and lower them in critical infrastructures. Some of the highlighted requirements and challenges are scalability, authentication, integrity, availability and resilience [118], [154], [155], [164], [167], [169], [171]. Similar to what happens for IoT, most of research works are focused in IDS proposals [12], [134], [153] and attacks/anomaly detection (mainly ML-based) [136], [140], [172].

In relation to commercial tools, if we come back to the tools in Section III, Splunk is the only SIEM that is explicitly indicated for monitoring IIoT environments [173].

B. CURRENT RESEARCH CHALLENGES FOR NSM

We believe that NSM could benefit to each of the communication network areas under study, although there are still open issues to tackle. Below, we summarize the main challenges that, to the best of our knowledge, still need further research work for each of the NSM modules identified in the taxonomy proposed in Section II.

- **Sensor Module.** This is a well-established component, which is widely covered in the reviewed works. Most of the individual sensors enumerated in Section III can be used in modern networks together with new sensors that are implicit in the nature of some of them, such as IoT and IIoT.
- **Parser Module.** This component is considered in some of the studied works from the point of view of self-feature extraction. In some cases, a unification and redundancy reduction is also performed. However, there is still a research room, which should be focused towards establishing a unified format for event logging and feature extraction from Big Data.
- **Integrator Module.** This is one of the most important and useful NSM modules, since it allows aggregating data from different sources. Integrating is even more relevant for modern communication paradigms, where a number of heterogeneous devices are sending and receiving information that needs to be unified for its monitoring and incident detection. Yet, only four of the studied works take into account this module in an explicit manner. For this reason, finding a strategy to integrate, aggregate and correlate different data sources is still one of the main challenges for researchers.
- **Detection Module.** Most of current research works are mainly focused in this module, aiming to find new ways for applying ML algorithms and thus improving the capability of anomalies and/or attacks detection. One of the main challenges for this component is Big Data processing to create and apply detection models. Furthermore, prioritizing alarms and reducing the number of false positives are still open issues.
- **Inspector Module.** This component aims to locate an incident both physically and in time. This is even more important when we talk about decentralized networks (*e.g.* IoT), due to: *i)* the source of the event might not be placed in the same location as the event, and *ii)* a number of different devices are probably interchanging information thorough the network. Yet, only two of the reviewed works include an inspector module. This component needs further research, not only to provide logs and store the state after an incident takes place, but to make them interpretable. This will help security operators to understand the facts and make them more efficient in their forensic work.
- **Actuator Module.** This module is taken into account in many of the works under study, which define some actions such as blocking malicious connections. The main challenges for this component are defining and implementing self-recovery mechanisms to make the communications networks resilient. This is specially important in critical systems, typically related to IIoT environments.

Finally, scalability and compatibility with restricted resources (the latter specially for IoT and IIoT) are common issues that are open for each of these modules. In addition, solutions available in the market need to be updated in order to overcome these challenges and provide modern solutions covering most of the NSM modules. If these solutions are designed following this philosophy, they will be more scalable and it will be easier to complete and enhance them.

V. CONCLUSION

In this paper, we review the state-of-the-art for Network Security Monitoring (NSM), providing an overall insight and a unified classification of its main components. Our taxonomy classifies such components as sensors, parsers, integrators, detectors, inspectors and actuators. These modules can be combined in different ways, yielding a powerful and scalable architecture for incident detection. This work highlights the strengths and weaknesses of the identified modules.

We review existing solutions for NSM sensor and parser modules, which can be found individually in the market. Furthermore, we study some of the best known and widely used multi-module NSM solutions, according to the proposed taxonomy. The best known examples of these combinations are IDSs/IPSs, SEMs/SIEMs and UTMs.

Finally, we assess the applicability of the NSM philosophy in modern communications networks. We focus this evaluation in SDN and IoT/IIoT networks. Open issues and future research interests for each of the NSM modules in relation to new communications paradigms are summarized.

We believe this paper is of interest both for the research community and security practitioners, since it helps to focus the efforts of research and market solutions in a more effective manner. Furthermore, it allows the identification of tools and methods that are available to collect and process network security data for incident detection.

To conclude, we believe that the security landscape for both traditional and modern networks would be benefited from *i)* the investigation and development of inspector and actuator modules, which are the least developed solutions to date; and *ii)* the design of systems which include all the components identified. In addition, it is still needed to provide efficient solutions that take into account the restricted resources in

IoT and IIoT, as well as improving the resilience in critical infrastructures.

APPENDIX A
LIST OF ABBREVIATIONS

AUC	Area Under the Curve
CVE	Common Vulnerabilities and Exposures
DoS	Denial of Service
DDoS	Distributed DoS
FIM	File Integrity Monitoring
GUI	Graphical User Interface
HIDS	Host IDS
IDMEF	Intrusion Detection Message Exchange Format
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IoT	Internet of Things
IIoT	Industrial IoT
IT	Information Technology
ML	Machine Learning
NFV	Network Function Virtualization
NIDS	Network IDS
NIST	National Institute of Standards and Technology of the United States
NSM	Network Security Monitoring
NTP	Network Time Protocol
NVD	National Vulnerability Database
OSSEC	Open Source HIDS SECurity
OSSIM	Open Source Security Information Management
P2P	Peer to Peer
PCA	Principal Component Analysis
ROC	Receiver Operating Characteristics
SEM	Security Event Management
SDN	Software Defined Network
SIEM	Security Information and Event Management
SIM	Security Information Management
SNMP	Simple Network Management Packet
UTM	Universal Threat Management

REFERENCES

[1] Rapid7. (2015). *Prevention vs Detection, Rebalancing Your Security Program*. Accessed: Jul. 16, 2020. [Online]. Available: https://www.rapid7.com/resources/prevention-vs-detection/

[2] R. Samson. (2020). Prevention vs detection-based security approach. Clearnetwork. Accessed: Jul. 16, 2020. [Online]. Available: https://www.clearnetwork.com/prevention-vs-detection-cybersecurity-approach/

[3] Comodo. (2020). *Advanced Threat Protection: Security Incident Response Tools*. Accessed: Jun. 2, 2020. [Online]. Available: https://cutt.ly/TyXyxJz

[4] R. Bejtlich, *The TAO of the Network Security Monitoring: Beyond Intrusion Detection*. Reading, MA, USA: Addison-Wesley, 2005.

[5] R. G. Bace, *Intrusion Detection* (Technology Series). New York, NY, USA: Macmillan Technical Publishing, 2000.

[6] J. Camacho, G. Maciá-Fernández, J. E. D. Verdejo, and P. García-Teodoro, "Tackling the big data 4 vs for anomaly detection," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2014, pp. 500–505.

[7] X. Ji, K. Huang, L. Jin, H. Tang, C. Liu, Z. Zhong, W. You, X. Xu, H. Zhao, J. Wu, and M. Yi, "Overview of 5G security technology," *Sci. China Inf. Sci.*, vol. 61, no. 8, pp. 1869–1919, 2018.

[8] S. Thudumu, P. Branch, J. Jin, and J. J. Singh, "A comprehensive survey of anomaly detection techniques for high dimensional big data," *J. Big Data*, vol. 7, no. 1, 2020, Art. no. 42.

[9] H. Shiravi, A. Shiravi, and A. A. Ghorbani, "A survey of visualization systems for network security," *IEEE Trans. Vis. Comput. Graphics*, vol. 18, no. 8, pp. 1313–1329, Aug. 2012.

[10] I. Ghafir, V. Prenosil, J. Svoboda, and M. Hammoudeh, "A survey on network security monitoring systems," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW)*, Aug. 2016, pp. 77–82.

[11] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, Oct. 2016, pp. 258–263.

[12] S. Otoum, B. Kantarci, and H. T. Mouftah, "Detection of known and unknown intrusive sensor behavior in critical applications," *IEEE Sensors Lett.*, vol. 1, no. 5, pp. 1–4, Oct. 2017.

[13] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102419.

[14] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, "A survey of moving target defenses for network security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1909–1941, 3rd Quart., 2020.

[15] R. Marty, *Applied Security Visualization*. Reading, MA, USA: Addison-Wesley, 2010.

[16] S. Salah, G. Maciá-Fernández, and J. E. Díaz-Verdejo, "Fusing information from tickets and alerts to improve the incident resolution process," *Inf. Fusion*, vol. 45, pp. 38–52, Jan. 2019.

[17] S. Salah, G. Maciá-Fernández, and J. E. Díaz-Verdejo, "A model-based survey of alert correlation techniques," *Comput. Netw.*, vol. 57, no. 5, pp. 1289–1317, Apr. 2013.

[18] Talend. (2021). *Structured vs. Unstructured Data: A Complete Guide*. Accessed: Feb. 22, 2021. [Online]. Available: https://bit.ly/37C7DXg

[19] MongoDB. (2021). *Structured vs Unstructured Data*. Accessed: Feb. 22, 2021. [Online]. Available: https://bit.ly/3uhVJeR

[20] Elastic Stack. (2020). *Elastic Stack Features*. Accessed: Sep. 11, 2020. [Online]. Available: https://www.elastic.co/es/elastic-stack/features

[21] Elastic Search. (2019). *The Elastic Stack. Meet the Core Products*. Accessed: Sep. 1, 2019. [Online]. Available: https://www.elastic.co/es/products/elastic-stack

[22] J. Camacho and J. M. García-Jiménez. (2018). *FCParser*. [Online]. Available: https://github.com/josecamachop/FCParser

[23] A. AlEroud, Z. Yan, and J. M. Namayanja, *Information Fusion for Cyber-Security Analytics* (Studies in Computational Intelligence), I. Alsmadi and G. K. A. Aleroud, Eds. Cham, Switzerland: Springer, 2017.

[24] R. Bejtlich, *The Practice of Network Security Monitoring*. San Francisco, CA, USA: No Starch Press, 2013.

[25] T. G. Doeswijk, A. K. Smilde, J. A. Hageman, J. A. Westerhuis, and F. A. van Eeuwijk, "On the increase of predictive performance with high-level data fusion," *Anal. Chim. Acta*, vol. 705, nos. 1–2, pp. 41–47, Oct. 2011.

[26] M. Cocchi, "Introduction: Ways and means to deal with data from multiple sources," in *Data Fusion Methodology and Applications*, vol. 31. Amsterdam, The Netherlands: Elsevier, 2019, pp. 1–26.

[27] A. K. Smilde and I. V. Mechelen, "A framework for low-level data fusion," in *Data Fusion Methodology and Applications*, vol. 31. Amsterdam, The Netherlands: Elsevier, 2019, ch. 2, pp. 27–50.

[28] Z. Yu and J. J. P. Tsai, *Intrusion Detection: A Machine Learning Approach* (Electrical and Computer Engineering), vol. 3. London, U.K.: Imperial College Press, 2011.

[29] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, C. Wang, and Y. Liu, "A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 393–430, 1st Quart., 2019.

[30] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, nos. 1–2, pp. 18–28, Feb. 2009.

[31] M. Iturbe, "Data-driven anomaly detection in industrial networks," Ph.D. dissertation, Mondragon Unibertsitatea, Mondragón, Spain, 2017.

[32] M. Collins, *Network Security Through Data Analysis: Building Situational Awareness*, O. Media, Ed. Sebastopol, CA, USA: O'Reilly, 2014.

[33] D. J. Marchette, *Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint* (Statistics for Engineering and Information Science). New York, NY, USA: Springer, 2001.

[34] INCIBE. (2017). *Diseño y Configuración de IPS, IDS y SIEM en Sistemas de Control Industrial*. Accessed: Sep. 3, 2019. [Online]. Available: https://www.incibe-cert.es/blog/diseno-y-configuracion-ips-ids-y-siem-sistemas-control-industrial

[35] J. Camacho, J. M. García-Giménez, N. M. Fuentes-García, and G. Maciá-Fernández, "Multivariate big data analysis for intrusion detection: 5 steps from the haystack to the needle," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101603.

[36] T. Kourti and J. F. MacGregor, "Multivariate SPC methods for process and product monitoring," *J. Qual. Technol.*, vol. 28, no. 4, pp. 409–428, Oct. 1996.

[37] M. Fuentes-García, "Multivariate statistical network monitoring for network security based on principal component analysis," Ph.D. dissertation, Univ. Granada, Granada, Spain, 2020.

[38] D. P. Joseph and J. Norman, "An analysis of digital forensics in cyber security," in *Proc. 1st Int. Conf. Artif. Intell. Cogn. Comput.*, R. Bapi, K. Rao, and M. Prasad, Eds. Singapore: Springer, 2019, pp. 701–708.

[39] K. Okereafor and R. Djehaiche, "New approaches to the application of digital forensics in cybersecurity: A proposal," *Int. J. Simul. Syst. Sci. Technol.*, vol. 21, no. 2, pp. 1–36, Mar. 2020.

[40] E. Chanthery and A. Subias, "Diagnosis approaches for detection and isolation of cyber attacksand faults on a two-tank system," in *Proc. 30th Int. Workshop Princ. Diagnosis DX*, 2019, pp. 1–9.

[41] Q. P. Nguyen, K. W. Lim, D. M. Divakaran, K. H. Low, and M. C. Chan, "GEE: A gradient-based explainable variational autoencoder for network anomaly detection," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 91–99.

[42] A. Lakhina, M. Crovella, and C. Diot, "Diagnosing network-wide traffic anomalies," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 4, p. 219, Oct. 2004.

[43] J. Camacho, A. Pérez-Villegas, P. García-Teodoro, and G. Maciá-Fernández, "PCA-based multivariate statistical network monitoring for anomaly detection," *Comput. Secur.*, vol. 59, pp. 118–137, Jun. 2016.

[44] M. Fuentes-García, G. Maciá-Fernández, and J. Camacho, "Evaluation of diagnosis methods in PCA-based multivariate statistical process control," *Chemometric Intell. Lab. Syst.*, vol. 172, pp. 194–210, Jan. 2018.

[45] AT&T-Cybersecurity. (2020). *Incident Response Tools*. Accessed: Jun. 2, 2020. [Online]. Available: https://cutt.ly/2yXypMF

[46] Cynet. (2020). *The 7 Best Free and Open-Source Incident Response Tools*. Accessed: Jun. 2, 2020. [Online]. Available: https://cutt.ly/ayXykEL

[47] National Cyber Security Centre. (2019). *Small Business Guide: Response & Recovery*. Accessed: Jul. 17, 2020. [Online]. Available: https://cutt.ly/DapvwAL

[48] Deloitte. (2016). *Cyber Crisis Management: Readiness, Response, and Recovery*. Accessed: Sep. 8, 2020. [Online]. Available: https://cutt.ly/wfWnXWC

[49] J. Kisielius. (2020). Automated incident response explained. AlienVault. Accessed: Sep. 8, 2020. [Online]. Available: https://cutt.ly/3fWn72T

[50] Varonis. (2020). *How to Respond to a Cyber Security Incident*. Accessed: Sep. 8, 2020. [Online]. Available: https://www.varonis.com/blog/respond-cyber-security-incident/

[51] V. Jacobson, C. Leres, and S. McCanne. (1988). *Tcpdump and Libpcap*. Accessed: Sep. 3, 2019. [Online]. Available: https://www.tcpdump.org/

[52] G. Combs. (1998). *Wireshark*. Accessed: Sep. 1, 2019. [Online]. Available: https://www.wireshark.org/

[53] Cisco-Systems. (2004). *Cisco Systems NetFlow Services Export Version 9*. Accessed: Sep. 1, 2019. [Online]. Available: https://tools.ietf.org/html/rfc3954

[54] C. Bullard. (2014). Argus. QoSient. Accessed: Sep. 5, 2019. [Online]. Available: https://qosient.com/argus/man/man8/argus.8.pdf

[55] QoSient. (2007). *Ra Client*. Accessed: Aug. 15, 2019. [Online]. Available: https://manpages.debian.org/testing/argus-client/ra.1.en.html

[56] Open-Source. (2019). *NFDUMP*. Accessed: Aug. 17, 2019. [Online]. Available: http://nfdump.sourceforge.net/

[57] J. Schoenwaelder. (2008). Simple network management protocol (SNMP) context EngineID discovery. Jacobs University Bremen. Accessed: Nov. 27, 2019. [Online]. Available: https://tools.ietf.org/html/rfc5343

[58] C. Lonvick. (2001). The BSD syslog protocol. Cisco System. Accessed: Nov. 27, 2019. [Online]. Available: https://www.ietf.org/rfc/rfc3164.txt

[59] M. Probert. (2016). Grep, awk and sed—Three VERY useful command-line utilities. University of York. Accessed: Feb. 22, 2021. [Online]. Available: https://bit.ly/3pIqCph

[60] L. Carbonell. (2019). *Filtros: Awk, Grep, Sed y Cut*. Accessed: Feb. 22, 2021. [Online]. Available: https://bit.ly/3knlPbP

[61] Elastic Stack. (2021). *Logstash. Centraliza, Transforma y Almacena Tus Datos*. Accessed: Feb. 22, 2021. [Online]. Available: https://www.elastic.co/es/logstash

[62] T. Alpcan and T. Basar, *Network Security: A Decision and Game-Theoretic Approach*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[63] Cisco. (2014). *SNORT(R) Users Manual. Active Response*. Accessed: Oct. 2, 2020. [Online]. Available: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node26.html

[64] Cisco and Sourcefire. (1998). *Snort*. Accessed: Sep. 1, 2019. [Online]. Available: https://www.snort.org/

[65] (2020). *Suricata*. Accessed: Sep. 2, 2020. [Online]. Available: https://suricata-ids.org/

[66] ATT Cybersecurity. (2020). *Suricata IDS: An Overview of Threading Capabilities*. Accessed: Jun. 2, 2020. [Online]. Available: https://cutt.ly/jyZbAeI

[67] OSSEC Project Team. (2008). *Open Source HIDS SECurity*. Accessed: Aug. 17, 2019. [Online]. Available: https://www.ossec.net/

[68] Gartner. (2019). *What is Security Information and Event Management (SIEM)?* Accessed: Sep. 17, 2019. [Online]. Available: https://www.gartner.com/reviews/market/security-information-event-management

[69] K. Kavanagh, T. Bussa, and G. Sadowski. (Dec. 2018). Magic quadrant for security information and event management. Gartner. Accessed: Sep. 15, 2019. [Online]. Available: https://www.gartner.com/en/documents/3894573/magic-quadrant-for-security-information-and-event-manage, techreport

[70] V. Paxson and R. Sommer. (1994). *The Zeek Network Security Monitor (Bro)*. Accessed: Aug. 18, 2019. [Online]. Available: https://www.zeek.org/

[71] Bricata. (2020). *What is Bro IDS (Zeek)? And Why IDS Doesnt Effectively Describe it Overview and Resources*. Accessed: Jun. 2, 2020. [Online]. Available: https://bricata.com/blog/what-is-bro-ids/

[72] Prelude. (2020). *PRELUDE SIEM. Smart Security*. Accessed: Sep. 10, 2020. [Online]. Available: https://cutt.ly/bfTTiuN

[73] Y. Vandoorselaere. (2005). *Prelude*. Accessed: Aug. 18, 2019. [Online]. Available: https://www.prelude-siem.com/en/author/otran/page/2/

[74] Prelude. (2020). *Prelude OSS Project*. Accessed: Sep. 10, 2020. [Online]. Available: https://www.prelude-siem.org/

[75] Wazuh Inc. (2019). *The Open Source Security Platform*. Accessed: Oct. 18, 2019. [Online]. Available: https://wazuh.com/

[76] AT&T-Cybersecurity. (2019). *AlienVault(R) Unified Security Management(R) (USM)*. Accessed: Nov. 8, 2019. [Online]. Available: https://www.alienvault.com/products

[77] AT&T-Cybersecurity. (2012). *Open Threat Exchange (OTX)*. Accessed: Nov. 8, 2019. [Online]. Available: https://www.alienvault.com/open-threat-exchange

[78] AT&T-Cybersecurity. (2016). *AlienVault(R) OSSIM(TM), Open Source Security Information and Event Management (SIEM)*. Accessed: Nov. 8, 2019. [Online]. Available: https://www.alienvault.com/products/ossim

[79] K. Kavanagh, T. Bussa, and G. Sadowski. (Dec. 2020). Magic quadrant for security information and event management. Gartner. Accessed: Feb. 24, 2021. [Online]. Available: https://gtnr.it/37IM3Ak

[80] Gartner. (2019). *Gartner Magic Quadrant*. Accessed: Nov. 8, 2019. [Online]. Available: https://www.gartner.com/en/research/methodologies/magic-quadrants-research

[81] Splunk. (2005). *Use Splunk App for Infrastructure*. Accessed: Nov. 25, 2019. [Online]. Available: https://cutt.ly/itOzLSy

[82] Splunk. (2020). *One Platform for All Your Data Needs. Turn Data Into Outcomes*. Accessed: Sep. 9, 2020. [Online]. Available: https://cutt.ly/7fRQUMt

[83] Gartner Inc. (2018). *Gartner 2018 Magic Quadrant for SIEM*. Accessed: Oct. 18, 2019. [Online]. Available: https://cutt.ly/ztOzY3S

[84] AlienVault. (2019). *Compare AlienVault Products*. Accessed: Nov. 8, 2019. [Online]. Available: https://www.alienvault.com/products/ossim/compare

[85] AT&T-Cybersecurity. (2020). *Using the AlienApp for AT&T Cybersecurity Forensics and Response Actions*. Accessed: Jun. 2, 2020. [Online]. Available: https://cutt.ly/cyZBA1v

[86] Gartner. (2019). *Unified Threat Management (UTM)*. Accessed: Sep. 17, 2019. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/unified-threat-management-utm

[87] P. García-Teodoro, J. E. Díaz-Verdejo, and J. M. López-Soler, *Transmisión de Datos y Redes de Computadores*. London, U.K.: Pearson, 2014.

[88] W. Stallings, *Data and Computer Communications*, 8th ed. Boston, MA, USA: Pearson, 2014.

[89] BAKOTECH. (2018). *WatchGuard UTM is Recognized the Only Visionary in the Gartner Magic Quadrant for the 4th Time*. Accessed: Jun. 2, 2020. [Online]. Available: https://bit.ly/3aNkYO8

[90] R. Kaur and C. Neiva. (Dec. 2018). Gartner magic quadrant for unified threat management SMB multifunction firewalls. Gartner. Accessed: Feb. 24, 2021. [Online]. Available: https://gtnr.it/3sp51Up

[91] Barracuda. (2020). *Barracuda CloudGen Firewall*. Accessed: Jun. 2, 2020. [Online]. Available: https://cutt.ly/FgefB66

[92] WatchGuard. (2020). *WatchGuard Security Services*. Accessed: Jun. 2, 2020. [Online]. Available: https://www.watchguard.com/wgrd-products/security-services

[93] Sophos. (2020). *The World's Best Visibility, Protection, and Response*. Accessed: Jun. 2, 2020. [Online]. Available: https://www.sophos.com/en-us/products/next-gen-firewall.aspx

[94] B. Visscher. (2014). *Sguil*. Accessed: Aug. 18, 2019. [Online]. Available: https://sourceforge.net/projects/sguil/

[95] S. Brisa. (2015). *Squert Security Art Work*. Accessed: Feb. 22, 2021. [Online]. Available: https://bit.ly/3uljUce

[96] Security Onion Solutions. (2008). *Security Onion*. Accessed: Aug. 20, 2019. [Online]. Available: https://securityonion.net/

[97] Elastic. (2000). *X-Pack*. Accessed: Sep. 1, 2019. [Online]. Available: https://www.elastic.co/es/what-is/open-x-pack

[98] Microsoft. (2020). *La Versión de Windows Más Segura Creada Hasta la Fecha*. Accessed: Jul. 16, 2020. [Online]. Available: https://www.microsoft.com/es-es/windows/comprehensive-security

[99] G. Lyon. (1997). *Nmap Network Mapper*. Accessed: Aug. 17, 2019. [Online]. Available: https://nmap.org/

[100] Tenable. (1988). *Nessus*. Accessed: Aug. 20, 2019. [Online]. Available: https://cutt.ly/9tOlEnR

[101] Greenbone Networks. (2009). *Open Vulnerability Assessment Scanner (OpenVAS)*. Accessed: Sep. 18, 2019. [Online]. Available: http://openvas.org/

[102] National Institute of Standards and Technology. (2019). *National Vulnerability Database (NVD)*. Accessed: Aug. 14, 2019. [Online]. Available: https://nvd.nist.gov/

[103] MITRE. (1999). *Common Vulnerabilities and Exposures (CVE)*. Accessed: Sep. 3, 2019. [Online]. Available: https://cve.mitre.org/

[104] Microsoft. (2018). *Review Event Logs and Error Codes to Troubleshoot Issues With Microsoft Defender Antivirus*. Accessed: Feb. 22, 2021. [Online]. Available: https://bit.ly/3pCLgqE

[105] J. Jiménez. (2019). *Cómo Ver la Información Que Almacena Windows Defender de los Análisis Hechos Redes Zone*. Accessed: Feb. 22, 2021. [Online]. Available: https://bit.ly/2Nwym0r

[106] Kaspersky. (2018). *Protege Tu Hogar Con Kaspersky IoT Scanner*. Accessed: Jan. 26, 2021. [Online]. Available: https://tinyurl.com/y5koktek

[107] Kaspersky. (2018). *Kaspersky Security for Virtualization 4.0 Agentless. Kaspersky Security Logs*. Accessed: Feb. 22, 2021. [Online]. Available: https://bit.ly/3bu54HF

[108] Kaspersky. (2020). *Kaspersky Threat Intelligence*. Accessed: Jul. 16, 2020. [Online]. Available: https://www.kaspersky.es/enterprise-security/threat-intelligence

[109] Kaspersky. (2020). *Kaspersky Security Cloud Free*. Accessed: Jul. 16, 2020. [Online]. Available: https://www.kaspersky.es/free-antivirus

[110] J. Molina. (2016). *Threat Intelligence: El Porqué de las Cosas*. Accessed: Oct. 18, 2019. [Online]. Available: https://www.welivesecurity.com/la-es/2016/12/01/threat-intelligence/

[111] A. Vincent, R. Barger, A. Pendergast, and L. Reichel. (2011). *Threat Connect*. Accessed: Oct. 18, 2019. [Online]. Available: https://threatconnect.com/

[112] (2019). *Cyber Threat Alliance*. Accessed: Oct. 20, 2019. [Online]. Available: https://www.cyberthreatalliance.org/

[113] CSIRT-Gadgets. (2019). *The FASTEST Way to Consume Threat Intelligence*. Accessed: Nov. 8, 2019. [Online]. Available: https://csirtgadgets.com/commits/2018/1/6/the-fastest-way-to-consume-threat-intel

[114] SIGMONA. (2016). *Software-Defined and Virtualizaed Mobile Networks*. Accessed: Jan. 22, 2021. [Online]. Available: https://tinyurl.com/y5gatld6

[115] I. Al Ridhawi, M. Aloqaily, Y. Kotb, Y. Al Ridhawi, and Y. Jararweh, "A collaborative mobile edge computing and user solution for service composition in 5G systems," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 11, p. e3446, 2018. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3446

[116] M. Liyanage, I. Ahmad, J. Okwuibe, E. M. de Oca, H. L. Mai, O. López, and M. Uriarte, *Software Defined Security Monitoring in 5G Networks*. Hoboken, NJ, USA: Wiley, Jan. 2018, pp. 231–243.

[117] M. Aloqaily, O. Bouachir, A. Boukerche, and I. A. Ridhawi, "Design guidelines for blockchain-assisted 5G-UAV networks," *IEEE Netw.*, vol. 35, no. 1, pp. 64–71, Jan./Feb. 2021.

[118] S. Berger, O. Bürger, and M. Röglinger, "Attacks on the industrial Internet of Things—Development of a multi-layer taxonomy," *Comput. Secur.*, vol. 93, Jun. 2020, Art. no. 101790. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404820300754

[119] J. Camacho, R. Bro, and D. Kotz, "Networkmetrics unraveled: MBDA in action," 2019, *arXiv:1907.02677*. [Online]. Available: http://arxiv.org/abs/1907.02677 and https://dblp.uni-trier.de/rec/bibtex/journals/corr/abs-1907-02677

[120] A. S. Da Silva, J. A. Wickboldt, L. Z. Granville, and A. Schaeffer-Filho, "ATLANTIC: A framework for anomaly traffic detection, classification, and mitigation in SDN," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Apr. 2016, pp. 27–35.

[121] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep recurrent neural network for intrusion detection in SDN-based networks," in *Proc. 4th IEEE Conf. Netw. Softwarization Workshops (NetSoft)*, Jun. 2018, pp. 202–206.

[122] P. Wang, K.-M. Chao, H.-C. Lin, W.-H. Lin, and C.-C. Lo, "An efficient flow control approach for SDN-based network threat detection and migration using support vector machine," in *Proc. IEEE 13th Int. Conf. e-Bus. Eng. (ICEBE)*, Nov. 2016, pp. 56–63.

[123] C. Song, Y. Park, K. Golani, Y. Kim, K. Bhatt, and K. Goswami, "Machine-learning based threat-aware system in software defined networks," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2017, pp. 1–9.

[124] R. M. A. Ujjan, Z. Pervez, and K. Dahal, "Suspicious traffic detection in SDN with collaborative techniques of snort and deep neural networks," in *Proc. IEEE 20th Int. Conf. High Perform. Comput. Commun.; IEEE 16th Int. Conf. Smart City; IEEE 4th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Jun. 2018, pp. 915–920.

[125] S. Badotra and S. N. Panda, "SNORT based early DDoS detection system using opendaylight and open networking operating system in software defined networking," *Cluster Comput.*, vol. 24, no. 1, pp. 501–513, Mar. 2021.

[126] T. Jafarian, M. Masdari, A. Ghaffari, and K. Majidzadeh, "Security anomaly detection in software-defined networking based on a prediction technique," *Int. J. Commun. Syst.*, vol. 33, no. 14, p. e4524, 2020. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.4524

[127] T. Nagata-Bolivar, "Escalamiento de seguridad en redes SDN para generación de reglas en NIDS empleando J48 y TENSORFLOW para analizar ataques basados en tiempo," in *Proc. 15th LACCEI Int. Multi-Conf. Eng., Educ., Technol.*, 2017.

[128] K. Nam and K. Kim, "A study on SDN security enhancement using open source IDS/IPS suricata," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2018, pp. 1124–1126.

[129] Barracuda. (2021). *Secure SD-WAN. Boost Application Performance and Reduce Costs*. Accessed: Jan. 26, 2021. [Online]. Available: https://tinyurl.com/y5qhuj3x

[130] WatchGuard. *Don't Deploy Half an SD-WAN Solution*. Accessed: Jan. 26, 2021. [Online]. Available: https://tinyurl.com/y57sqde7

[131] M. J. Jo and J. S. Shin, "MWMon: A software defined network-based malware monitor," *J. Korea Ind. Inf. Syst. Res.*, vol. 20, no. 5, pp. 37–44, Oct. 2015.

[132] J. B. García, V. S. Vilchez, J. Z. Castro, and J. L. Q. Arroyo, "Using cyber threat intelligence to prevent malicious known traffic in a SDN physical testbed," in *Proc. IEEE 26th Int. Conf. Electron., Electr. Eng. Comput. (INTERCON)*, Aug. 2019, pp. 1–4.

[133] M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow," in *Proc. 11th Int. Conf. Availability, Rel. Secur. (ARES)*, Aug. 2016, pp. 147–156.

[134] S. Otoum, B. Kantarci, and H. Mouftah, "A comparative study of AI-based intrusion detection techniques in critical infrastructures," 2020, *arXiv:2008.00088*. [Online]. Available: https://arxiv.org/abs/2008.00088

[135] M. Aloqaily, S. Otoum, I. A. Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101842. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870519301131

[136] G. Efstathopoulos, P. R. Grammatikis, P. Sarigiannidis, V. Argyriou, A. Sarigiannidis, K. Stamatakis, M. K. Angelopoulos, and S. K. Athanasopoulos, "Operational data based intrusion detection system for smart grid," in *Proc. IEEE 24th Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Sep. 2019, pp. 1–6.

[137] J. Arshad, M. A. Azad, M. M. Abdeltaif, and K. Salah, "An intrusion detection framework for energy constrained iot devices," *Mech. Syst. Signal Process.*, vol. 136, Feb. 2020, Art. no. 106436. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0888327019306570

[138] I. Al Ridhawi, S. Otoum, M. Aloqaily, Y. Jararweh, and T. Baker, "Providing secure and reliable communication for next generation networks in smart cities," *Sustain. Cities Soc.*, vol. 56, May 2020, Art. no. 102080. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2210670720300676

[139] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6882–6897, Aug. 2020.

[140] S. Otoum, B. Kantarci, and H. T. Mouftah, "A novel ensemble method for advanced intrusion detection in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.

[141] A. Tabassum, A. Erbad, A. Mohamed, and M. Guizani, "Privacy-preserving distributed IDS using incremental learning for IoT health systems," *IEEE Access*, vol. 9, pp. 14271–14283, 2021.

[142] Bitdefender. *Bitdefender IoT Security Platform. Smart Home Cybersecurity for Your Business*. Accessed: Feb. 24, 2021. [Online]. Available: https://www.bitdefender.com/iot/

[143] Avast. *Avast Smart Home Security*. Accessed: Jan. 26, 2021. [Online]. Available: https://www.avast.com/smarthome

[144] Barracuda. (2021). *Software-Defined Wide Area Network (SD-WAN)*. Accessed: Jan. 26, 2021. [Online]. Available: https://tinyurl.com/yxhrb8lg

[145] WatchGuard. (2021). *About SD-WAN*. Accessed: Jan. 26, 2021. [Online]. Available: https://tinyurl.com/y4vnvnc8

[146] L. Patrono, L. Atzori, P. Šolić, M. Mongiello, and A. Almeida, "Challenges to be addressed to realize Internet of Things solutions for smart environments," *Future Gener. Comput. Syst.*, vol. 111, pp. 873–878, Oct. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X19324628

[147] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128614003971

[148] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Netw.*, vol. 32, pp. 17–31, Sep. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870515000141

[149] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, "On the security and privacy of Internet of Things architectures and systems," in *Proc. Int. Workshop Secure Internet Things (SIoT)*, Sep. 2015, pp. 49–57.

[150] D. Dragomir, L. Gheorghe, S. Costea, and A. Radovici, "A survey on secure communication protocols for IoT systems," in *Proc. Int. Workshop Secure Internet Things (SIoT)*, 2016, pp. 47–62.

[151] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128618307035

[152] P. I. R. Grammatikis, P. G. Sarigiannidis, and I. D. Moscholiosb, "Securing the Internet of Things: Challenges, threats and solutions," *Internet Things*, vol. 5, pp. 41–70, Mar. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2542660518301161

[153] M. A. Ferrag, M. Babaghayou, and M. A. Yazici, "Cyber security for fog-based smart grid SCADA systems: Solutions and challenges," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102500. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214212619311408

[154] A. Tzounis, N. Katsoulas, T. Bartzanas, and C. Kittas, "Internet of Things in agriculture, recent advances and future challenges," *Biosyst. Eng.*, vol. 164, pp. 31–48, Dec. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1537511017302544

[155] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges," *IEEE Access*, vol. 8, pp. 32031–32053, 2020.

[156] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, "Security analysis of network anomalies mitigation schemes in IoT networks," *IEEE Access*, vol. 8, pp. 43355–43374, 2020.

[157] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, Apr. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517300802

[158] F. Cauteruccio, L. Cinelli, E. Corradini, G. Terracina, D. Ursino, L. Virgili, C. Savaglio, A. Liotta, and G. Fortino, "A framework for anomaly detection and classification in multiple IoT scenarios," *Future Gener. Comput. Syst.*, vol. 114, pp. 322–335, Jan. 2021. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X19335253

[159] A. Sánchez. (2017). *Protege Tu Red Frente a Intrusos Con Bitdefender Home Scanner*. Accessed: Jan. 26, 2021. [Online]. Available: https://tinyurl.com/yyguxsyo

[160] Avast. (2020). *Seguridad del IoT*. Accessed: Jan. 26, 2021. [Online]. Available: https://tinyurl.com/yykeknqs

[161] Barracuda. (2021). *Barracuda CloudGen Firewall F-Series for Internet of Things*. Accessed: Jan. 26, 2021. [Online]. Available: https://tinyurl.com/y54kzxg5

[162] J. Bryan. (2020). An increased number of physical and cyber risks lurked as 2019 came to a close. Gartner. Accessed: Feb. 3, 2021. [Online]. Available: https://tinyurl.com/y5xvv7tt

[163] J. Lavelle. (2020). Gartner emerging risk survey shows renewed COVID-19 outbreak as top executive concern. Gartner. Accessed: Feb. 3, 2021. [Online]. Available: https://tinyurl.com/y5m47n52

[164] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[165] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial Internet of Things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, Oct. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0166361517307285

[166] R. Ande, B. Adebisi, M. Hammoudeh, and J. Saleem, "Internet of Things: Evolution and technologies from a security perspective," *Sustain. Cities Soc.*, vol. 54, Mar. 2020, Art. no. 101728. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2210670719303725

[167] J. Polge, J. Robert, and Y. L. Traon, "Assessing the impact of attacks on OPC-UA applications in the industry 4.0 era," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–6.

[168] C. Bai, P. Dallasega, G. Orzes, and J. Sarkis, "Industry 4.0 technologies assessment: A sustainability perspective," *Int. J. Prod. Econ.*, vol. 229, Nov. 2020, Art. no. 107776. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925527320301559

[169] M. Gidlund, G. P. Hancke, M. H. Eldefrawy, and J. Akerberg, "Guest editorial: Security, privacy, and trust for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 625–628, Jan. 2020.

[170] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in healthcare 4.0," *Comput. Commun.*, vol. 153, pp. 311–335, Mar. 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366419311880

[171] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd Annu. Design Automat. Conf.*, Jun. 2015, pp. 1–6.

[172] G. E. I. Selim *et al.*, "Anomaly events classification and detection system in critical industrial Internet of Things infrastructure using machine learning algorithms," *Multimedia Tools Appl.*, 2021, doi: 10.1007/s11042-020-10354-1.

[173] Splunk. (2017). *Splunk(R) for Industrial Data and the IoT*. Accessed: Jan. 26, 2021. [Online]. Available: https://tinyurl.com/y2xhmrxx

MARTA FUENTES-GARCÍA received the master's degree in software development and the Ph.D. degree in information and communication technologies from the University of Granada. Her Ph.D. was focused in anomaly detection using multivariate data analysis. Her research has been mainly related to anomaly detection and diagnosis both in industrial processes and network traffic. She also has work experience in different companies as a programmer. She is currently a part of the Research Team with Fidesol, which is a technological innovation support center. As a part of the EGIDA project, she is leading different initiatives and research related to security and privacy-based on ML and anomaly detection in IoT devices, which are focused on Industry 4.0. Her research interests include data science, statistics, exploratory data analysis, and anomaly detection, with especial emphasis in those data which are related to IT Security and industrial processes. She is particularly interested in knowledge transfer from science to industry and small medium enterprises.

JOSÉ CAMACHO received the degree in computer science from the University of Granada, Spain, in 2003, and the Ph.D. degree from the Technical University of Valencia, in 2007. He is currently an Associate Professor with the Department of Signal Theory, Telematics and Communication. He is also a Researcher with the Information and Communication Technologies Research Centre, University of Granada. His research interests include exploratory data analysis, anomaly detection and optimization with multivariate techniques applied to data of very different nature, including manufacturing processes, chemometrics, and communication networks. He is especially interested in the use of exploratory data analysis to Big Data. His Ph.D. was awarded with the second Rosina Ribalta Prize to the best Ph.D. projects in the field of information and communication technologies (ICT) from the EPSON Foundation, and with the D. L. Massart Award in Chemometrics from the Belgian Chemometrics Society.

GABRIEL MACIÁ-FERNÁNDEZ is currently an Associate Professor with the Department of Signal Theory, Telematics and Communications, University of Granada, Spain. He belongs to the Network Engineering and Security (NESG) Research Group, University of Granada. His research interests include systems and network security, with special emphasis on intrusion detection, reliable protocol design, penetration testing techniques, network information leakage, and denial of service.