IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 30, 2021, accepted January 17, 2022, date of publication January 21, 2022, date of current version February 7, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3145029

SOC Critical Path: A Defensive Kill Chain Model

ANTONIO VILLALÓN-HUERTA[1], HECTOR MARCO GISBERT[2], (Senior Member, IEEE), AND ISMAEL RIPOLL-RIPOLL[2]

[1]S2 Grupo, 46022 Valencia, Spain
[2]Department of Computing Engineering, Universitat Politècnica de València, 46022 Valencia, Spain

Corresponding author: Hector Marco Gisbert (hecmargi@disca.upv.es)

ABSTRACT Different kill chain models have been defined and analyzed to provide a common sequence of actions followed in offensive cyber operations. These models allow analysts to identify these operations and to understand how they are executed. However, there is a lack of an equivalent model from a defensive point of view: this is, there is no common sequence of actions for the detection of threats and their accurate response. This lack causes not only problems such as unstructured approaches and conceptual errors but, what is most important, inefficiency in the detection and response to threats, as defensive tactics are not well identified. For this reason, in this work we present a defensive kill chain approach where tactics for teams in charge of cyber defense activities are structured and arranged. We introduce the concept of SOC Critical Path (SCP), a novel kill chain model to detect and neutralize threats. SCP is a technology–independent model that provides an arrangement of mandatory steps, in the form of tactics, to be executed by Computer Network Defense teams to detect hostile cyber operations. By adopting this novel model, these teams increase the performance and the effectiveness of their capabilities through a common framework that formalizes the steps to follow for the detection and neutralization of threats. In this way, our work can be used not only to identify detection and response gaps, but also to implement a continuous improvement cycle over time.

INDEX TERMS SOC critical path, security operations center, computer network defense, cyber kill chain.

I. INTRODUCTION

The high benefits technology has contributed to are questionless, but so are the risks it introduces on a daily basis for individuals, organizations and countries. Hostile actors such as foreign countries, terrorist groups and organized crime are well aware of these risks and they take advantage of them, from cyber crime to cyber war. In this context, Computer Network Operations (CNO), defined [1] as those capabilities used to attack adversary computer networks, defend our own and exploit enemy computers to enable intelligence gathering play a prominent role, both in offensive operations, such as attack or exploitation, and in defensive operations.

The defensive CNO discipline is called Computer Network Defense (CND) and it is defined as [1] those actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity in own information systems and computer networks. CND activities are provided by a Security Operations Center (SOC), a center focused on the prevention, detection and response to security incidents [2]. Defensive centers for cyber security adopt different names [3], [4] [5], such as SOC, CSIRT, CERT, CSOC, ISIRT, etc., according to its specific functions, capabilities or even licenses. In this paper, we will refer to all of them as SOC.

In this context, a SOC has a clear goal of preventing, detecting and neutralizing cyber threats. Of course, the achievement of this high–level simple goal, is a complex task. Leaving aside the prevention activities, such as those related to systems hardening or user awareness, and focusing on the detection and neutralization activities, a SOC detects and responds to incidents. However, no single common definition of the mandatory tactics and their arrangement to perform this task have been identified among literature. While offensive kill–chain models are well defined and discussed, no defensive equivalent has been ever proposed. This situation leads SOCs to work by following non–structured approaches, a fact that impacts not only in their detection and response capabilities, but also in their effectiveness and improvement over time.

We define the SOC Critical Path (SCP) as the sequence of mandatory activities to detect and to neutralize a threat. SCP is a kill chain model, which is a specific arrangement of actions, identified as tactics, mandatory to achieve a goal.

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

In this case this goal is the SOC goal, as stated before. Such a kill chain model formalizes SOC activities and provides defensive centers with the mandatory tactics they have to sequentially implement so as to be successful; as in offensive kill chain approaches, it not only helps to structure activities, but also to identify gaps and improvements in this implementation. In most cases SOC activities are done in an unstructured, not fail–safe way, thus giving hostile actors the opportunity to succeed in their activities.

In this work, we propose SCP as a model to detect and enable the neutralization, of threats. We consider this model to provide a platform–agnostic SOC kill chain, identifying the mandatory, sequential actions a SOC must perform. Each of the presented tactics can be deployed by different techniques, out of the scope of this paper, and some of them can also can be divided into sub–tactics, not mandatory but relevant to the detection and neutralization.

The contributions of this paper are as follows:

- To identify the mandatory tactics to detect security incidents, thus enabling its appropriate handling by defensive teams.
- To provide the basis for a global SOC detection and response process, not only linked to pure incident response, establishing a whole continuous improvement cycle.
- To establish the proper arrangement of the identified tactics in the form of a kill chain model. As this arrangement is mandatory for a SOC, it defines the correct sequence of tasks to be performed to detect and respond to incidents, i.e., the defensive kill chain.
- To identify the most relevant sub–tactics for each of the main established first–level tactics in order to help SOC analysts to develop particular techniques to achieve them.

The rest of this paper is organized as follows. The background in Section II provides concepts regarding the identified problem in SOC processes and emphasizes kill chain approaches, which are always defined from an offensive perspective. In Section III we assess the problem of the lack of a unified structure for CND operations and its importance in the identification of situations on the infrastructure that can lead to a security incident. Section IV analyzes prior work on this issue. In Section V we propose the SCP model as a global sequence of tactics to be performed by blue teams to identify incidents, as well as an example regarding the practical application of our model. Section VI discusses the results and compares them with those of other approaches. Finally, Section VII concludes the paper and identifies future research directions.

II. BACKGROUND

In this section we provide the necessary background related to SOC processes and kill chain model approaches that will be the pillars not only to understand the identified issue in Section III but also to properly follow the proposed SCP model in Section V.

A. SOC CONCEPTS

As in any cyber operation, to be able to achieve its defensive goals, a SOC has to develop tactics, techniques and procedures. Tactics specify what to do, at the highest level of description, to accomplish a certain mission, while techniques specify how tactics are implemented; procedures, outside of the scope of this work, describe a particular implementation.

These tactics and techniques enable an effective threat detection and neutralization in a SOC. A threat is defined [6] as any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service; in this reference the authors identify four types of threat sources:

- Adversarial. Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources.
- Accidental. Erroneous actions taken by individuals during the course of executing their everyday responsibilities.
- Structural. Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed the expected operating parameters.
- Environmental. Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.

To detect and neutralize a threat, from the adversarial to the environmental ones, any SOC has to manage a high volume of initially unstructured information: to acquire and analyze data from multiple sources, and to turn this high volume of information into an actionable, reduced, set of data. This is done through a set of technologies and processes represented in the so–called SOC funnel: the conversion of millions of inputs in a few actionable outputs suitable for management by a human team (the blue team).

The definitions for these sets of data, from millions of inputs to the reduced set of actionable outputs, are not clear among professionals [7]. In this work, we use the key definitions presented in this section.

A log message, or simply a log, is the minimum information unit generated by an information system [7], such as an application, operating system or database.

Log data are linked to and stored in the information systems that generate it. Some or all of the generated logs are sent to a SIEM and also called events. SIEM systems were designed [8] to collect events from different sources, normalize them to a common following a common syntax and structure, and store them once normalized.

An **event** is defined as a relevant, from a security point of view, contextualized information that reflects an observed change in the normal behavior of an object, such as an

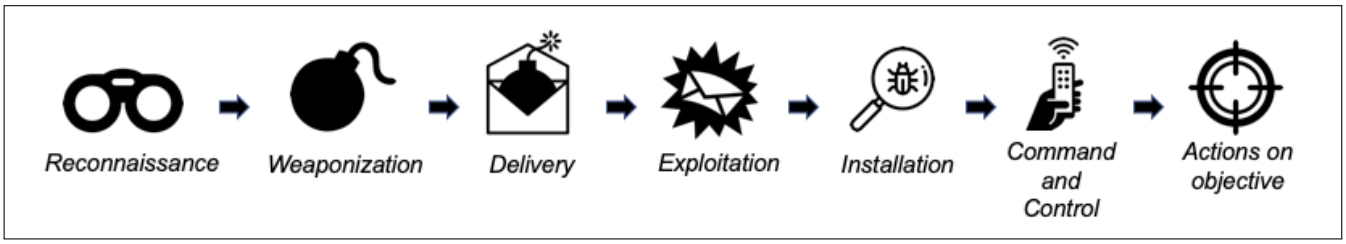

FIGURE 1. Cyber kill chain.

information system or a person. All events are stored in a SIEM, and three types are identified:

1) Raw events, those that automatically arrive to the SIEM from different data sources.
2) Aggregated events are those generated by the aggregation of raw events for a more efficient processing or analysis.
3) Correlated events, those generated by the correlation of raw or aggregated events.

An **alert** is an interesting event that requires spawning actions; alerts are usually managed on a ticketing system, where they are sent from the SIEM (if they are not part of the same product). Please note that on this ticketing platform not all alerts will have the SIEM as a source, as they can also arrive from other sources: from a user phone call to a manually introduced ticket on the platform. These alerts are also called actionable events, as they require specific actions to be executed in response to the alert.

Alerts are processed automatically and manually; when analyzed, this analysis can raise an **incident**. The incident concept is not well defined among cyber security researchers [9], although we accept the definition stated in [10], which refers to incidents, or cyber incidents, as any occurrence that has an impact on any of the components of the cyber space or on the functioning of the cyber space, regardless of whether it is natural or human–made, malicious or non–malicious intent, deliberate, accidental or due to incompetence, due to development or due to operational interactions. In this context, an incident can be seen as an alert or set of alerts that can impact in cyber operations. A key objective for a SOC would be a 1:1 ratio between alerts and incidents: as all alerts require an action that can be either manual or automated, those alerts that are not real incidents involve many negative factors, such as economic loss, productivity decrease or analyst burn out.

B. KILL CHAIN MODELS

A kill chain can be defined as a sequence of actions that a hostile actor has to perform in a particular arrangement to achieve their goals. Kill chain models have been developed to describe threat actors' campaign phases [11], as they describe the structure of the intrusion. Kill chain models help analysts to describe phases of intrusions, map adversary kill chain indicators to defender courses of action or identify patterns that link individual intrusions into broader campaigns, among others [12]. Kill chain models have been applied to the detection and understanding of potentially unwanted codes such as remote access tools [13], ransomware features [14] or banking Trojans [15], as well as to protect industrial control systems from advanced threat actors [16], [17] or to model the operations of these actors [18].

The most used kill chain model is the Cyber Kill Chain® framework [12], developed by Lockheed Martin, as a part of the Intelligence Driven Defense® model for identification and prevention of cyber intrusion activity, identifying what a threat actor must complete in order to achieve its objective. It was first described in [12] as a seven–step process suitable for CNA or CNE operations, as shown in figure 1.

These seven steps are defined as follows [12], [19]:

1) **Reconnaissance.** Research, identification and selection of targets.
2) **Weaponization.** Before attacking a target, the threat actor has to couple a remote access Trojan with an exploit into a deliverable payload.
3) **Delivery.** Transmission of weapons to the targeted environment to launch a particular operation.
4) **Exploitation.** After the weapon is delivered, exploitation triggers intruders' code.
5) **Installation.** Installation of an implant, just as a remote access Trojan, a backdoor or any kind of malicious software, on the victim system allows the adversary to maintain persistence inside the environment.
6) **Command and Control.** Compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel, thus allowing the threat actor to control its target remotely.
7) **Actions on Objectives.** After progressing through the first six phases, intruders can take actions to achieve their original objectives, such as information theft, denial or hop to a third–party infrastructure.

The Cyber Kill Chain represents an industry-accepted methodology for understanding how an attacker will conduct the activities necessary to cause harm to an organization and has been largely discussed [20] (in [21] the authors identify some of the discussions regarding the application of the Cyber Kill Chain). Some authors [22], [23] have proposed the addition and removal of different stages in order to improve or adjust the original model, and the topic has also been discussed in technical conferences. Also, some efforts to unify models and variants, such as [24], have been made.

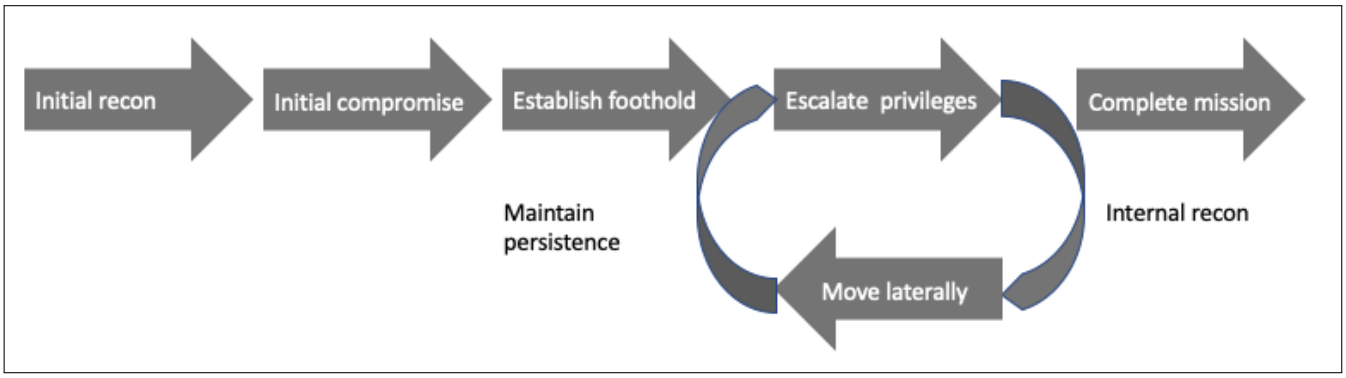

FIGURE 2. Mandiant's attack life cycle model.

Despite this, the original proposal has been widely used and applied to specific problems regarding advanced threat actors, such as those related to the modeling of the attack stages against critical structures [25]–[27].

Some critics of the CKC are related to its approach as a linear progression that does not accurately represent the actions of an actor; Mandiant (FireEye) presented in [28] the Mandiant Attack Life Cycle, a kill chain model in which the Weaponization stage is removed and introduces a loop to represent the continuous activities of internal recon, lateral movement and persistence performed by a hostile actor, as shown in figure 2. A summary of critics and improvements to CKC can be found in [29], and the proposed variants of the cyber kill chain model can be found on [30] or [31].

III. THE ISSUE: A LACK OF DEFENSIVE KILL CHAIN

The main issue we have identified is the lack of a suitable, arranged set of tactics, in the form of a kill chain (this is, in the form of mandatory steps to accomplish a goal). There is not a single high–level, platform–agnostic kill chain, or even identification of tactics to achieve the SOC goals: this is, in order to establish the mandatory steps to detect and neutralize threats. This lack of such a model may be due to the fact that defensive centers focus on the alleged attacker activities as the first and main input, so they start their work always trying to detect, in order to respond, to such activities. With this focus on the incident response against hostile operations, subjects such as the correct data acquisition or processing are not properly covered, thus leaving windows of opportunity for an attacker to succeed.

Many approaches to model a SOC, including its processes perspective, have been proposed and developed in the academic and industrial literature. Nevertheless, as stated before, we have not identified a single high–level, platform–agnostic kill chain or even identification of tactics to achieve the SOC goals, in order to establish the mandatory steps to detect and neutralize threats. Of course, this is considered a relevant problem. The same way hostile operations are modeled in order to improve our knowledge about them and about the threat groups that perform these operations, we consider it mandatory to establish an equivalent model, in the form of a kill chain, for the defensive operations that enable the detection and neutralization of hostile activities. Such a model can improve aspects such as SOC classification, services, capabilities and technologies; however, most importantly, it can help defenders to analyze and to establish the requirements for an effective detection and neutralization of threats, to implement suitable techniques for each tactic and to arrange its activities.

The identification of hostile activities has been largely analyzed; both the particular tactics, techniques and procedures that a hostile actor has to perform in order to achieve its goals, as well as the particular arrangement of these tactics, are now well structured and accepted through the community. Focusing on tactics, techniques and procedures, from an offensive point of view, different approaches have been identified and analyzed, without establishing a particular arrangement, identifying commonly accepted models such as MITRE ATT&CK tactics and techniques matrix. In addition, focusing on the arrangement of these elements, an offensive point of view has been largely developed, such as Cyber Kill Chain. Different kill–chain approaches have been defined and used for the modeling of hostile activities [32].

Surprisingly, this state of the art, while dealing with the execution of offensive operations has no equivalent, commonly accepted approach for defensive operations. We find an important lack of the identification and definition of tactics and techniques for a SOC to run, as well as on its correct arrangement. In other words, there is no model for the mandatory activities a SOC has to perform. A model is defined [33] as an abstract representation of some domain of human experience, used to structure knowledge, to provide a common language for discussing that knowledge, and to perform analyses in that domain. Models are necessary in order to better understand and discuss abstract entities representing and structuring common knowledge and experiences, and allowing analysts to profile attackers from their goals to their TTP.

To successfully perform CND operations we consider that it is necessary to define a global SOC kill chain model regarding both the mandatory tactics to be executed and their arrangement. Therefore, we propose a kill chain model to

allow a SOC to detect and neutralize threats. Of course, this model would have to be independent from aspects such as the budget or the technology; this is, no matter which technologies or how much money a defensive center has, the model has to be similar. However, most importantly, it has to be independent from the hostile activities they face, and regardless of the type of threat a SOC is handling, the model must always be the same. Please note that most of the threats a SOC has to deal with will be adversarial, but accidental, structural or even environmental threats must also be detected and neutralized.

In this work we address an issue that has not been largely addressed and that is a must for any defensive center. The lack of a suitable model for CND operations implies not only the absence of a homogeneous work flow across different SOCs, but also heterogeneous approaches to incident detection that cause security flaws and security monitoring deficiencies among SOC customers, resulting in unprotected infrastructure assets and undetected security breaches. This problem is especially important as the first mandatory actions, those related to planning and acquisition of data, are in many cases not specially considered. This situation, with many processes focused on pure incident response, leads SOCs to perform a right processing and even a right analysis among incomplete data, thus resulting on an incorrect monitoring that leads to a late incident detection and response. In addition, they do not face the fact that not all SOC responses have to follow a well–defined incident response process, but in many cases these responses have to be simpler, and so they are in practice.

IV. TECHNIQUES AND LIMITATIONS

Defensive centers have been largely analyzed from different high–level perspectives, but none of them establishes a set of common tactics and their particular arrangement to provide a suitable SOC model. Many approaches are focused on the incident response process, which in our opinion is not correct, as this response is the last step of a set of activities a SOC has to successfully perform to achieve its goals. In addition, in some cases models are presented from a generic perspective, without identifying the activities a SOC has to develop in order to successfully detect and neutralize threats.

In [34] the authors propose the people, processes and technologies (PPT) model, later used specifically for a SOC in works such as [35], [36], [37] or [5]; in this triad, the processes branch is not uniform among the literature [5], providing an incomplete picture of the actions performed on the SOC daily basis.

Regarding this process definition for a SOC, many approaches are linked to incident handling processes [38], [39], leaving aspects as the acquisition or processing of data, although referred, in a secondary role. With this focus, critical aspects for incident detection are not considered, thus providing valid models once an incident is identified (from the response point of view) but lacking a unified approach to

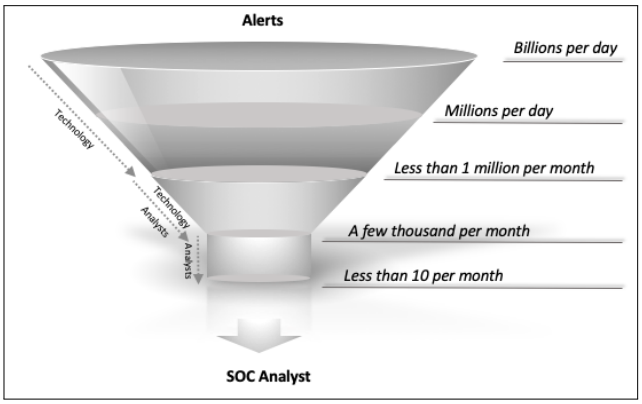

FIGURE 3. SOC funnel.

the previous mandatory tasks. In addition, a key concept is not considered in the approaches focused on incident response: the fact that in a SOC not all response activities are linked to this process. Response actions can vary depending on many factors, both technical (for example, those related to the priority or potential impact of an incident) and non–technical (for example, those related to signed contracts for a particular customer).

In 2013 Forrester introduced [40] the concept of the SOC funnel as a graphical simplification for SOC work. The SOC funnel represents the reduction process that must be performed by a SOC in order to obtain actionable alerts from billions or millions of raw events, as shown in figure 3. Although this model is conceptually correct, the authors did not specify the different tactics or the mandatory steps to accomplish this goal. More specific academic works, such as [41], have used this conceptual model, but also without deepening its tactics. Although this is a valid high–level approach, it does not specify what a SOC has to execute to achieve it.

In [42] the authors proposed a SOC architecture based on four layers: data acquisition, data processing (which includes filtering, merging and formatting), correlation analysis and visualization. As the work is focused on correlation, this model does not approach the tasks after analysis, simplifying them as a global visualization step. We consider visualization as not a key tactic for a SOC, but a technique for human analysis. Especially when dealing with big data environments, situational awareness in any of its forms is an important decision–support mechanism [43] [44] for Computer Network Defense. From an architectural point of view, the layers of a SOC have also been analyzed in works such as [35] or [5].

These approaches identify the mandatory layers for a SOC to run: generation, acquisition, data manipulation and output or presentation layers. Although these layered–approaches can be linked to the tactics the SOC has to execute, they do not consider a real kill chain model but layers inside the SOC architecture, including people, processes and technologies. In addition, they do not represent the mandatory feedback

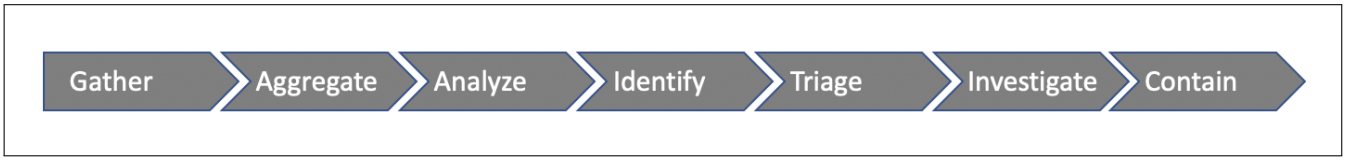

FIGURE 4. Blue team cyber kill chain.

that this chain must have, as the output of the process has to provide enhancements to the initial point.

In 2014 Ryan Stillions wrote a blog post [45] in which he presented the Detection Maturity Level (DML), a model to assess the maturity of an organization to detect cyber attacks in terms of its capabilities to consume and act upon given threat information. The DML model is composed of nine levels of maturity, from the most technical ones –really, level 0 represents no information about the threat– to the highest level ones –goals and strategy of the attacker–. The DML model has been improved [46], [47] by adding a tenth level of abstraction, DML-9, regarding identity of the threat actor, a useful information to connect multiple attacks to the same actor in order to predict strategy, tactics, techniques and procedures expected to be used in an operation. This hierarchical model can provide an approach not only to evaluate the detection capabilities of an organization, but also to the semantic modeling of an advanced threat actor, from a group to specific indicators left after an operation, thus helping the analysts to model the interests and behavior of the actor and its modus operandi in specific operations. However, neither the DML model nor its improvements detail the activities a SOC has to execute in order to provide these detection capabilities.

In [48] the authors presented a process for incident detection in a SOC inside a global incident response timeline. This process is based on four steps to identify the sources responsible for detecting and reporting incidents, the available channels to do so, the steps to accept inputs and, finally, the requirements on people and technology for this process to work. This is a valid approach, although it lacks an established arrangement and we identify a gap between the source identification and how this source could use the defined channels for notification.

In 2017 Matt Swann introduces, at Microsoft BlueHat Israel conference, the concept of a blue team cyber kill chain as a defender–centric version of the standard, offensive, cyber kill chain, as shown in figure 4; this approach defines the chain of actions a defender needs to go through to find and evict attackers. The author discusses the proposed stages and its window of opportunity in relation to the offensive kill chain, and it also presents a ''response pyramid'' which goes from the protected assets inventory to the ability to collaborate with third parties to disrupt campaigns. Although this approach relies mainly on incident response capabilities, it is an interesting starting point for the identification of SOC tactics. However, it has not been improved in other works, so it has not evolved since 2017; for example, the last step, contain, would have to be adapted to a more generic response approach.

MITRE Shield is an active defense knowledge base that captures and organizes what they are learning about active defense and adversary engagement. While MITRE ATT&CK provides the attacker's tactics and techniques, MITRE Shield provides tactics and techniques available to defenders. These TTP are linked to the active defense concept, understood as [49] the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy. MITRE Shield focuses on the tactics to respond to a hostile operation once it has been detected, not on the previous, mandatory steps to detect this operation. In this sense, we miss in the framework the identification of tactics for a SOC to monitor infrastructure and raise alerts.

Finally, as we have stated before, Mandiant Attack Life cycle is a relevant approach and reference for our work. It focuses on the detection of the activities of a hostile actor against an infrastructure. This approach, although useful for defensive teams (it focuses on what can be detected) is not accurate for the global modeling of threat actors; it is again focused on activities performed by the attacker, and so has been used in many works in both IT [50], [51] and OT environments [52], [53]. Nevertheless, it does not focus on what the defensive team must do to detect an operation.

None of the identified approaches among literature defines a formal arrangement of tactics, in the form of a kill chain model, to be performed by a SOC. This is, as we have stated before, no defensive kill chain model has been ever proposed. Most of the analyzed proposals focus on pure incident handling methodologies, which should be considered particular response techniques not suitable for all alerts a SOC handles daily. Some of them do not even propose tactics to be executed, but only an abstract model without delving into what activities a SOC has to perform. The closest approach we have found is Matt Swann's blue team cyber kill chain, which has not evolved in last few years and, as we will defend in section VI lacks mandatory tactics and also focuses on incident handling, not on the whole cycle a SOC must follow to achieve its goals.

V. OUR PROPOSAL

We define the SOC Critical Path (SCP) as the sequence of mandatory actions to detect and enable the neutralization, of a threat, as shown in figure 5. We can see SCP as a defensive version of a cyber kill chain. The SCP starts with the generation of a log record in a particular system and ends

FIGURE 5. SOC critical path.

with the appropriate response to a detected incident. This incident can be raised by any threat, not only by adversarial ones.

As stated before, in our approach we propose the SCP steps as shown in figure 5. These steps are partially equivalent to those defined in the Intelligence Cycle [54] and we have adopted a similar nomenclature for them where applicable. Each of these steps represents a tactic that specifies what the SOC must perform to achieve its goals, and each of them comprises different techniques to achieve the particular tactic. Please note that the proposed arrangement is mandatory: it is not possible to raise an alert if there is no data analysis, there is no data analysis without basic or complex processing, and there is no processing if we are not able to acquire relevant data. In addition, for some of the identified tactics, we have proposed specific sub–tactics; these sub–tactics are not mandatory in all cases, but they are recommended and, in today's SOCs, their execution is a common approach. We have not gone into them in depth, as their details are outside of the scope of this work.

The SCP starts with the planning tactic, which will identify what needs to be monitored for alert raising and how these data must be processed and analyzed in order to detect and respond to security incidents. In this step, it is mandatory to analyze potential hostile operations and techniques against our protected assets, to understand how threat actors will try to damage us, to identify attack surfaces in our infrastructures, and to establish guidelines on what and how monitoring will be performed. The planning tactic, as the first step of our approach, will guide all the activities executed by a SOC to detect and neutralize threats, and it will receive feedback from the rest of the tactics of our model, especially from the Response one.

Once the global monitoring and response strategies are defined, data Acquisition is the next SCP step, where relevant data is acquired from the monitored infrastructure and sent to a central repository, typically the SIEM platform. Monitored infrastructure generates logs, and some or all of them are selected for detection purposes. In order to detect malicious activities, it is mandatory not only to send those logs regarding special actions, but also those related to usual activities on the monitored infrastructure. In this tactic we identify two particular sub–tactics: Extraction, regarding what information is mandatory to acquire, and Transportation, regarding what mechanisms must be used to send the acquired data from its data source to the central repository.

When received by the SIEM, logs are processed and converted into events. This processing includes, at least, some kind of standardization and the storage and retention of the normalized data in the SIEM. Depending on the SIEM technology, it can range from simple to complex processing mechanisms, but in any case it is a must, as without proper processing, the events cannot be analyzed, which is the next step of the SCP. Most technologies include a normalized format for information (logs) received from multiple, hybrid sources, such as firewalls, endpoints or proxies, as well as predefined retention capabilities that can range from a few hours to months or years, with deletion and the cold storage being the last step of the data processing. Please note that, in this context, the deletion of data does not necessarily mean its real removal, but its elimination from a warm site and its storage in a cold site that cannot be exploited for detection but for forensic purposes. In this tactic we identify three sub–tactics: Reception, regarding the mechanisms that enable the correct receiving of the data, Normalization, regarding what approach is followed to convert hybrid data to a common format, and Storage, regarding what strategies the SOC must follow to store the received and normalized data in a way that allows the next step of the SCP, the Analysis.

Once processed, SIEM technologies also provide the capability to analyze events, which is the next step in SCP. This analysis can be performed both automatically and manually. SIEM can usually perform automatic reduction, aggregation and correlation. They also provide specific capabilities for manual analyses, ranging from simple queries to the stored data to particular, platform–dependent languages. As in classical intrusion detection schemes, the goal of this analysis is to identify misuses and anomalies that can lead to an incident, so in the Analysis tactic we identify two mandatory sub–tactics: misuse analysis and anomaly analysis. Please note that the particular techniques that compose these sub–tactics are those regarding intrusion detection approaches, such as expert systems, neural networks or statistical anomaly detection.

When a misuse or an anomaly is detected, an alert is raised, usually on a ticketing platform. The alert generation can be automatic, from pre–defined use cases in the SIEM platform, but also manually, when an analyst defines a new hypothesis, customizes it and identifies a misuse or an anomaly not

known before. Although alerting could be included in a global analysis tactic, we consider it apart, as for us it is not pure analysis but its result; it is equivalent to the dissemination step of the intelligence cycle stated before. In addition, please note that on the ticketing platform, related to these manual alerts, we can manage both alerts from SIEM data but also alerts from particular situations outside the SIEM scope, such as user calls. In this platform, the SOC must centralize all incident–related actionable events. We do not identify any sub–tactics for the Alert tactic, as it is a simple one, but only particular techniques to achieve it in an effective way, such as alert numbering schemes or alert data enrichment.

Through the ticketing platform, analysts respond to the alert that has been raised. All alerts require an appropriate response that can be automatic or manual, and given that all alerts on the ticketing platform require a response, a SOC objective is that all of them are real incidents. This response starts with the identification of the incident and, in case it is a real one (true positive), it continues with specific actions that are performed in order to neutralize the threat. Inside the incident response process these actions can range from deception to containment, and from simple actions to complex methodologies. The incident response process is well defined among many methodologies [55], [56]; a summary can be found in [57]. Many works define the particular sub–tactics, after the incident identification, such as containment, eradication, recovery and lessons learned [58], with little variation from this approach [59]. In any case, as we have stated before, SOC particular response activities depend on multiple factors, so these sub–tactics do not always apply; for example, a particular agreement with a customer may define the response to a specific incident type just as the notification of the action, or by automatic network block without further investigation or activities. For this reason, these sub–tactics are outside of the scope of this work, and cannot be considered mandatory in all cases.

To perform the response tactic, analysts may have to acquire and contextualize data from different sources, including their own ticketing platform, the SIEM, particular relevant systems of the organization or third–party repositories. If the incident is not a real one (false positive), the response tactic will not consider all the steps related to pure incident response, but the SOC will close the related ticket; in these cases, that a SOC has to minimize, it will also be an improvement to the process by refining correlation rules, use cases or acquisition exceptions.

Finally, please note that as in many processes SCP will improve global detection and response capabilities by giving appropriate feedback to the planning stage from all of the steps of the SCP, which will be produced by the analysis of all of the tactics role in detecting and neutralizing a threat, from the acquisition to the response one; in the same way, the improvements achieved will be applicable to all the tactics of the SCP.

A. A PRACTICAL EXAMPLE

To provide a practical result for our proposal, we have analyzed a particular technique performed by threat actors in their operations and how our model helps a SOC to detect and neutralize it. We have chosen the Command and Control (C2) tactic stated by MITRE ATT&CK, in particular the T1071.001 technique, related to command and control through web traffic protocols. While using this technique, adversaries may communicate using application layer protocols associated with web traffic to avoid detection and network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server, as MITRE ATT&CK framework states. Please note that choosing any other tactic or particular technique for our example would follow the same structure and provide the same results.

In order to be able to detect this C2 technique, first of all the SOC team must analyze how threat actors perform it. As stated before, they communicate with the command and control system through web traffic, this is, through the legitimate navigation of the users inside the compromised infrastructure. In this way, a malicious HTTP/S hit is hidden inside the whole, legitimate web traffic. As the amount of data to be analyzed in order to detect this malicious hit is very large, this technique allow the threat actor to go easily unnoticed. In addition, this technique evades network traffic filtering mechanisms, as outgoing web navigation protocols are usually allowed in all organizations.

Once the technique is analyzed, following our proposed kill chain, the SOC team must approach the first step: Planning. This is when the SOC plans the rest of the relevant tactics and techniques that will be later executed, so defining all the mandatory tasks for all of the SCP steps. First of all, the SOC must plan how to acquire relevant information for the detection and neutralization of the threat actor. In this case, as we are dealing with HTTP/S command and control, the main data source will be this kind of traffic, which can be acquired by different techniques, such as passive acquisition (for example, sniffing network traffic and dissecting the particular protocols) or through the parsing of proxy logs. The SOC team must analyze the pros and cons of the different techniques that can be applied to the acquisition, in order to identify and put into practice the most suitable approximation. This planning not only has to consider technical aspects, but also economic, legal or human ones.

In relation to the processing, the SOC team must consider elements such as the storage of the acquired data, its retention period and, most importantly, the usability and agility of the SIEM platform where this data is processed. As it is mandatory to process all navigation traffic, not just specific alerts such as blacklist navigation attempts, the parameters to estimate the processing capabilities, such as the amount of needed storage, the computing power or the events per second rate, must be adjusted in order to provide

SOC analysts a suitable environment for their work. The processing requirements will depend on the acquired data, so the proper arrangement of the proposed tactics we are defending is mandatory.

The next step in our model is related to the analysis of the data in the SIEM platform. This analysis can be performed through different techniques, both automated and manual, and its goal is to identify misuses and anomalies that can lead to an incident. Following our model, the SOC team will identify and put into practice analysis techniques suitable for the detection of web command and control channels, such as the use of black lists (misuse) or statistical or knowledge based anomalies, the so called "hunts" in threat hunting terminology. Please note that without a suitable processing, analysis can not be accomplished, confirming once again the mandatory arrangement for the tactics of the SCP.

Once data has been analyzed and particular conditions are met, the SOC will raise an alert if a suspicious activity has been detected. This alert will be sent to a ticketing platform, global for the SOC incident management processes, and it is mandatory to define how the alert will be generated in this platform, taking into account parameters such as classification, criticality or service level agreements for each type of alert.

Finally, when an alert is generated, some action from the SOC is required, reaching the last tactic of the SCP: the Response. The SOC team will respond, in one way or another, to the potential incident. In this last step, the SOC will follow the established operating procedures for each particular case. These procedures can range from a simple notification to the affected organization to a whole incident response deployment, following in this last case the usual sub–techniques: identification, containment, eradication and recovery. Again, the alerting, and thus the response tactics, must be executed after the analysis of the acquired and processed data, so we must stress one more time the relevance of the arrangement of the proposed tactics.

As we have stated, each of the tactics of the SOC Critical Path will provide feedback to the planning step, starting again the SCP in order to improve over time the SOC detection and response capabilities. In our example, this feedback is especially based on the analysis of the incidents that have not been properly detected, identifying which tactic or tactics have not been fully accomplished and improving them. This continuous improvement is mandatory for a SOC, as hostile actors modify their techniques over time and their detection and neutralization will always be the SOC's goal.

In this practical example, we have followed our proposed model to provide a suitable detection and response to a particular technique inside a hostile operation. We have identified particular tasks inside each step and justified the arrangement of our proposed tactics, thus providing SOC teams an example on how to apply the SCP to a real detection case. In order to present the improvements of our approach over previous techniques, we can compare the SCP to an equivalent kill chain model. But as we have stated in this work, it is hard to provide this comparison, as no direct, equivalent model has been identified during our research. SOC Critical Path is a novel proposal, being Matt Swann's blue team cyber kill chain the closer approach, but not having a direct equivalence.

Comparing our model to the blue team cyber kill chain, in Swann's work we find in first place the Gather step, which is equivalent to our acquisition, but without a proper, previous planning. This absence of a Planning tactic as a primary mandatory task can lead the SOC to execute subsequent steps lacking a clear, defined goal. Without identifying the relevant data sources that enable the identification of a particular offensive technique, without planning which processing requirements are mandatory and without a proper identification of analysis techniques, it is not possible for a SOC to provide an accurate detection capability.

The Blue Team Cyber Kill Chain's next step is the Aggregation one, a phase in which the defensive team joins the gathered data from multiple sources. In our model, we consider it a specific step for processing in which aggregation is set. But in opposition to the blue team cyber kill chain, inside the SCP Processing tactic, aggregation is just one of the particular techniques that a SOC can consider, together with other approaches just as reduction or, simply, storage of the acquired data. A processing tactic is much more suitable for a kill chain model, and inside this tactic, aggregation is a specific technique, but not the only one.

Next, the blue team cyber kill chain defines analysis and identification, which are equivalent to the analysis and alert steps in our model. The rest of the blue team cyber kill chain defined steps are triage, investigation and containment. We consider these tactics incorrect for a general model, as they focus on particular tasks not performed by a SOC in all cases. Triage and investigation can be considered particular techniques for our response tactic. If this response is a global incident response, these steps should be included in a general identification step, as they define tasks to perform this identification. In addition, containment is a tactic suitable for this global incident response, but in this case it should be considered together not only with identification, but also with eradication and recovery, as most incident response strategies define [60], [61].

Being hard to compare the SOC Critical Path to an equivalent model, as we have presented a novel approach, differences and benefits over the blue team cyber kill chain are clear. Our proposal provides a technology–agnostic arrangement of tactics for a defensive team to detect and respond to threats. Comparing this arrangement to the blue team cyber kill chain, we advocate that our model not only covers the whole cycle for a SOC to perform its task, but provides a homogeneous point of view of the mandatory tactics without considering particular techniques for any of them. This abstraction allows analysts to follow our model and, when needed, to go down into the techniques to perform their task. We consider this fact increases global detection and response performance, as the difference between what the

SOC has to execute (the tactic) and how it has to be executed (the technique) is clear at all times. Also, giving feedback to the Planning tactic, which in the SCP is mandatory to enhance all the SOC work, closes the cycle and provides a continuous improvement element to our model.

VI. DISCUSSION

We have proposed a model for the SOC Critical Path, the sequence of mandatory actions to detect and enable the neutralization, of a threat. This model provides the arrangement of tactics that a SOC must perform to achieve its goals. In this sense, our approach gives analysts not only a kill chain equivalent for defensive cyber operations, but also a set of mandatory tactics to be considered in a center that provides cyber defense capabilities. Each of the defined tactics can be more or less complex, depending on the SOC maturity, but we defend all of them to be mandatory for a SOC to accomplish its goals. In addition, please note that this model is suitable not only for the detection and neutralization of adversarial threats, but is a common approach for all types of threats.

For the proposed tactics of the SCP we have chosen terms close to those used in the Intelligence Cycle, as we have stated before. We defend that SOC activities are in fact related to counter intelligence activities, as the SOC goal is the prevention, detection and neutralization of threats. Of course, these terms could be largely discussed (for example, the Planning tactic could be called the Preparation tactic), but we consider this is pure nomenclature. We have actively avoided terms used by the Cyber Kill Chain® as we consider it especially relevant to distinguish both approaches, one with an offensive perspective and the SCP with a defensive one.

As we have stated, all reviewed approaches for kill chain models are focused on the offensive point of view; these models provide the mandatory, arranged tactics for an attacker to achieve their goals. However, unlike in the offensive perspective, previous defensive proposals do not focus on tactics and techniques, neither on a critical path (kill chain in offensive jargon) to achieve a defensive actor's goals. Different studies analyze SOC processes with special emphasis on the incident response capabilities, thus not giving the mandatory importance to tactics to provide analysis or acquisition capabilities, and also considering a homogeneous, not real, work for a SOC day to day. As we defend, a global incident response is only a particular kind of response of all of the possibilities a SOC can provide to its customers.

The absence of a defensive kill chain model makes it hard to compare our approach with equivalent proposals. In fact, this absence is a real problem, as SOC activities are in many cases unstructured, not correctly formalized nor arranged, making it difficult to improve capabilities over time and thus giving adversaries relevant advantages to succeed. Different proposals have been analyzed in this work, none being suitable for the definition of mandatory tactics and their arrangement in the form of a defensive kill chain. The closest approach we have found, the blue team cyber kill chain, lacks important tactics and, as most of the frameworks, focuses on global incident response without taking into account relevant aspects such as the planning or proper acquisition of data, as we have stated in the practical example shown in section V-A. For this reason we have proposed a novel kill chain model which sets all the relevant steps and their correct arrangement for a successful detection capability.

Future research lines would include to deepening into each of the presented tactics, in order to define sub–tactics inside the defined tactics. Those sub–tactics would not be mandatory to accomplish the global SOC goal, but recommended. In the cases where these sub–tactics can be identified in a specific order, they could be considered a more specific approach to the SCP. In our approach, we have provided sub–tactics for the main identified tactics, but we consider this to be an ongoing work. It is also important to note that in some cases the internals of some of the proposed tactics are well structured in the literature and have been discussed in our work, for example regarding the response tactic, while in other cases the potential sub–tactics are not so well structured, such as in the acquisition one.

In addition, an interesting future research line would be the specification of techniques for each tactic we have presented in this work. Although we provide a high–level description for SCP, we consider our research as the first proposal that has to be improved. These techniques would define how a specific tactic can be executed, and its structure could be similar to the MITRE ATT&CK approach, but considering the defensive point of view.

VII. CONCLUSION

In this work we have presented the SOC Critical Path (SCP), a sequence of mandatory actions to appropriately detect and respond to security incidents, which is the main goal of Computer Network Defense, executed by centers such as a SOC. The SCP is equivalent, from a defensive point of view, to models such as the Cyber Kill Chain, which are focused on the attacker's perspective. Although this offensive point of view has been discussed in many works, the defensive one presents an important lack of research, so we have addressed an issue not largely analyzed in spite of being a must for a SOC to accomplish its goals: to prevent but, especially, to detect and to neutralize security threats. In this sense, our approach provides a kill chain equivalent to a SOC team.

We have proposed an approach based on the definition and arrangement of the tactics that must be implemented in any defensive center. Our goal was to identify these tactics from a global perspective, from the generation and registration of interesting activities in a protected IT asset to the analysis of data, alerting and final incident response. Although many studies focus on this later step, the one related to the incident response, we have tried to consider all mandatory tactics to achieve the SOC goals at the same importance level. For each identified tactic we have discussed and proposed sub–tactics that, in a particular arrangement, conform to the global tactic to achieve.

Finally, we identified some future research lines mainly related to the specification of sub–tactics and particular techniques in each of the identified tactics in our research. We consider this future work as a mandatory enhancement of this first approach to the process of detecting and neutralizing security threats.

REFERENCES

[1] "Information operations primer. fundamentals of information operations," Dept. Mil. Strategy, U.S. Army War College, Planning, Oper., Carlisle, PA, USA, Tech. Rep., Nov. 2011.
[2] F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, and G.-J. Ahn, "Matched and mismatched SOCs: A qualitative study on security operations center issues," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2019, pp. 1955–1970.
[3] C. Zimmerman, *Cybersecurity Operations Center*. McLean, VA, USA: The MITRE Corporation, 2014.
[4] J. M. Brown, S. Greenspan, and R. Biddle, "Incident response teams in IT operations centers: The T-TOCs model of team functionality," *Cognition, Technol. Work*, vol. 18, no. 4, pp. 695–716, Nov. 2016.
[5] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges," *IEEE Access*, vol. 8, pp. 227756–227779, 2020.
[6] "Guide for conducting risk assessments," Joint Task Force Transformation Initiative, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., 2012.
[7] D. Nathans, *Designing and Building Security Operations Center*. Rockland, MA, USA: Syngress, 2014.
[8] S. Bhatt, P. K. Manadhata, and L. Zomlot, "The operational role of security information and event management systems," *IEEE Security Privacy*, vol. 12, no. 5, pp. 35–41, Sep. 2014.
[9] V. Gnatyuk, "Analysis of ≪incident≫ definitions and its interpretation in cyberspace," *Ukrainian Sci. J. Inf. Secur.*, vol. 19, no. 3, pp. 175–180, Dec. 2013.
[10] "Enisa overview of cybersecurity and related terminology," ENISA, Eur. Union Agency Netw. Inf. Secur., Tech. Rep., Sep. 2017.
[11] I.-C. Mihai, S. Pruna, and I.-D. Barbu, "Cyber kill chain analysis," *Int. J. Info. Sec. Cybercrime*, vol. 3, p. 37, Aug. 2014.
[12] E. Hutchins, M. Cloppert, and R. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues Inf. Warfare Secur. Res.*, vol. 1, no. 1, p. 80, 2011.
[13] R. HosseiniNejad, H. HaddadPajouh, A. Dehghantanha, and R. M. Parizi, "A cyber kill chain based analysis of remote access trojans," in *Handbook of Big Data and IoT Security*. Springer, 2019, pp. 273–299.
[14] T. Dargahi, A. Dehghantanha, P. N. Bahrami, M. Conti, G. Bianchi, and L. Benedetto, "A cyber-kill-chain based taxonomy of crypto-ransomware features," *J. Comput. Virol. Hacking Techn.*, vol. 15, no. 4, pp. 277–305, Dec. 2019.
[15] D. Kiwia, A. Dehghantanha, K.-K.-R. Choo, and J. Slaughter, "A cyber kill chain based taxonomy of banking trojans for evolutionary computational intelligence," *J. Comput. Sci.*, vol. 27, pp. 394–409, Jul. 2018.
[16] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," *SANS Inst. InfoSec Reading Room*, to be published.
[17] X. Zhou, Z. Xu, L. Wang, K. Chen, C. Chen, and W. Zhang, "Kill chain for industrial control system," in *Proc. MATEC Web Conf.*, vol. 173, 2018, Art. no. 01013.
[18] P. N. Bahrami, A. Dehghantanha, T. Dargahi, R. M. Parizi, K.-K. R. Choo, and H. H. Javadi, "Cyber kill chain-based taxonomy of advanced persistent threat actors: analogy of tactics, techniques, and procedures," *J. Inf. Process. Syst.*, vol. 15, no. 4, pp. 865–889, 2019.
[19] F. A. Garba, S. B. Junaidu, I. Ahmad, and M. Tekanyi, "Proposed framework for effective detection and prediction of advanced persistent threats based on the cyber kill chain," *Sci. Practical Cyber Secur. J.*, vol. 3, no. 3, pp. 1–11, Sep. 2018.
[20] L. Myers, "The practicality of the cyber kill chain approach to security," *CSO Online*, to be published.
[21] W. Zeng and V. Germanos, "Modelling hybrid cyber kill chain," in *Proc. Int. Workshop Petri Nets Softw. Eng.*, 2019, pp. 1–18.
[22] M. Laliberte, *A Twist on the Cyber Kill Chain: Defending Against a Javascript Malware Attack*. New York, NY, USA: Dark Reading, Sep. 2017.
[23] B. D. Bryant and H. Saiedian, "A novel kill-chain framework for remote security log analysis with SIEM software," *Comput. Secur.*, vol. 67, pp. 198–210, Jun. 2017.
[24] P. Pols, "The unified kill chain: Designing a unified kill chain for analyzing, comparing and defending against cyber attacks," Cyber Secur. Academy, Tech. Rep., 2017.
[25] A. Hahn, R. K. Thomas, I. Lozano, and A. Cardenas, "A multi-layered and kill-chain based security analysis framework for cyber-physical systems," *Int. J. Crit. Infrastruct. Protection*, vol. 11, pp. 39–50, Dec. 2015.
[26] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electr. Inf. Sharing Anal. Center (E-ISAC)*, to be published.
[27] X. Zhou, Z. Xu, L. Wang, K. Chen, C. Chen, and W. Zhang, "Kill chain for industrial control system," in *Proc. MATEC Web Conf.*, vol. 173, 2018, Art. no. 01013.
[28] D. McWhorter, "Apt1: Exposing one of China's cyber espionage units," Mandiant, Reston, VA, USA, Tech. Rep., 2013.
[29] M. S. Khan, S. Siddiqui, and K. Ferens, "A cognitive and concurrent cyber kill chain model," in *Computer and Network Security Essentials*. Springer, 2018, pp. 585–602.
[30] H. Kim, H. Kwon, and K. K. Kim, "Modified cyber kill chain model for multimedia service environments," *Multimedia Tools Appl.*, vol. 78, no. 3, pp. 3153–3170, Feb. 2019.
[31] W. Zeng and V. Germanos, "Modelling hybrid cyber kill chain," in *Proc. PNSE@ Petri Nets/ACSD*, 2019, pp. 143–160.
[32] B. D. Bryant and H. Saiedian, "A novel kill-chain framework for remote security log analysis with SIEM software," *Comput. Secur.*, vol. 67, pp. 198–210, Jun. 2017.
[33] D. Bodeau, C. McCollum, and D. Fox, *Cyber Threat Modeling: Survey, Assessment, and Representative Framework*. McLean, VA, USA: HSSEDI, The Mitre Corporation, 2018.
[34] G. D. Bhatt, "Knowledge management in organizations: Examining the interaction between technologies, techniques, and people," *J. Knowl. Manage.*, vol. 5, no. 1, pp. 68–75, Mar. 2001.
[35] S. G. Radu, "Comparative analysis of security operations centre architectures; proposals and architectural considerations for frameworks and operating models," in *Proc. Int. Conf. Inf. Technol. Commun.*, Springer, 2016, pp. 248–260.
[36] R. Van Os, "SOC-CMM: Designing and evaluating a tool for measurement of capability maturity in security operations centers," Tech. Rep., Sep. 2016.
[37] O. Lindström, "Next generation security operations center," Tech. Rep., Nov. 2018.
[38] C. Onwubiko, "Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy," in *Proc. Int. Conf. Cyber Situational Awareness, Data Analytics Assessment (CyberSA)*, Jun. 2015, pp. 1–10.
[39] M. Mutemwa, J. Mtsweni, and L. Zimba, "Integrating a security operations centre with an Organization's existing procedures, policies and information technology systems," in *Proc. Int. Conf. Intell. Innov. Comput. Appl. (ICONIC)*, Dec. 2018, pp. 1–6.
[40] E. Ferrara, C. McCClean, R. Holland, and T. Frechette, "Security operations center (SOC) staffing," Tech. Rep., Aug. 2013.
[41] D. Blum, "Institute resilience through detection, response, and recovery," in *Rational Cybersecurity for Business*. Springer, 2020, pp. 259–295.
[42] S. Yuan and C. Zou, "The security operations center based on correlation analysis," in *Proc. IEEE 3rd Int. Conf. Commun. Softw. Netw.*, May 2011, pp. 334–337.
[43] K. Demertzis, N. Tziritas, P. Kikiras, S. L. Sanchez, and L. Iliadis, "The next generation cognitive security operations center: Adaptive analytic lambda architecture for efficient defense against adversarial attacks," *Big Data Cognit. Comput.*, vol. 3, no. 1, p. 6, Jan. 2019.
[44] A. D'Amico and K. Whitley, "The real work of computer network defense analysts," in *VizSEC 2007*. Springer, 2008, pp. 19–37.
[45] R. Stillions. (Apr. 2014). *The DML Model*. [Online]. Available: http://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html
[46] S. Bromander, A. Jøsang, and M. Eian, "Semantic cyberthreat modelling," in *Proc. STIDS*, 2016, pp. 74–78.
[47] V. Mavroeidis and S. Bromander, "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence," in *Proc. Eur. Intell. Secur. Informat. Conf. (EISIC)*, Sep. 2017, pp. 91–98.

[48] J. Muniz, G. McIntyre, and N. AlFardan, *Security Operations Center: Building, Operating, and Maintaining your SOC*. Indianapolis, IN, USA: Cisco Press, 2015.
[49] *O. of the Chairman of the Joint Chiefs of Staff, DOD Dictionary of Military and Associated Terms*, Dept. Defense, Richmond, VA, USA, Jan. 2021.
[50] I. Ghafir and V. Prenosil, "Proposed approach for targeted attacks detection," in *Advanced Computer and Communication Engineering Technology*. Springer, 2016, pp. 73–80.
[51] J. D. Mireles, J.-H. Cho, and S. Xu, "Extracting attack narratives from traffic datasets," in *Proc. Int. Conf. Cyber Conflict (CyCon U.S.)*, Oct. 2016, pp. 1–6.
[52] A. Cook, H. Janicke, R. Smith, and L. Maglaras, "The industrial control system cyber defence triage process," *Comput. Secur.*, vol. 70, pp. 467–481, Sep. 2017.
[53] A. Hassanzadeh and R. Burkett, "SAMIIT: Spiral attack model in IIoT mapping security alerts to attack life cycle phases," in *Proc. Electron. Workshops Comput.*, Aug. 2018, pp. 11–20.
[54] N. S. Office, *NATO Glossary Terms Definitions (English French)*. New Delhi, India: NSO, 2018.
[55] *Information Technology–Security Techniques—Information Security Incident Management—Part 1: Principles of Incident Management*, Standard ISO/IEC 27035-1:2016, International Organization for Standardization, Tech. Rep., Nov. 2016.
[56] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," Nat. Inst. Standards Technol., Gaithersburg, MA, USA, Tech. Rep., Aug. 2012.
[57] I. A. Tøndel, M. B. Line, and M. G. Jaatun, "Information security incident management: Current practice as reported in the literature," *Comput. Secur.*, vol. 45, pp. 42–57, Sep. 2014.
[58] R. Andrade, J. Torres, and S. Cadena, "Cognitive security for incident management process," in *Proc. Int. Conf. Inf. Technol. Syst.*, Springer, 2019, pp. 612–621.
[59] N. H. A. Rahman and K.-K. R. Choo, "A survey of information security incident handling in the cloud," *Comput. Secur.*, vol. 49, pp. 45–69, Mar. 2015.
[60] L. R. Johnson, *Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response*. Rockland, MA, USA: Syngress, 2013.
[61] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer security incident handling guide," *NIST Special Publication*, vol. 800, no. 61, pp. 1–147, 2012.

ANTONIO VILLALÓN-HUERTA received the M.Sc. degree in computer engineering from the Universidad Politecnica de Valencia, Spain. He is currently the Chief Security Officer at S2 Grupo. With 25 years of experience in the cyber security field, in his career, he has executed and managed analysis, defense, attack and exploitation projects, and designed and managed security operations and incident response centers. He is the author of different books, articles and chapters on the subjects of cyber security and cyber intelligence, and a regular speaker in many congresses and courses. His research interests include the Russian cyber intelligence community and the modeling and detection of advanced threat actors.

HECTOR MARCO GISBERT (Senior Member, IEEE) received the Ph.D. degree in computer science and cybersecurity from the Universitat Politecnica de Valencia, Spain. He is currently an Associate Professor and a Cybersecurity Researcher with the Universitat Politecnica de Valencia. He is a member of the Engineering and Physical Sciences Research Council (EPSRC), U.K. Previously, he was an Associate Professor with the University of the West of Scotland, U.K., and a Cybersecurity Researcher with the Universitat Politecnica de Valencia, where he co-founded the "Cybersecurity Research Group." He was part of the team developing the multi-processor version of the XtratuM hypervisor to be used by the European Space Agency in its space crafts. He participated in multiple research projects as the Principal Investigator and a Co-Investigator. He is the author of many papers of computer security and cloud computing. He has been invited multiple times to reputed cybersecurity conferences, such as Black Hat and DeepSec. He has published more than ten Common Vulnerabilities and Exposures (CVE) affecting important software, such as the Linux kernel. He has received honors and awards from Google, Packet Storm Security and IBM for his security contributions to the design and implementation of the Linux ASLR. His research interests include low level cybersecurity, secure and non-secure world kernel and userland security, virtualization security, and applied cryptography.

ISMAEL RIPOLL-RIPOLL received the Ph.D. degree in computer science from the Universitat Politècnica de València (UPV), in 1996. He is currently a Professor of several cybersecurity subjects with the Department of Computing Engineering, UPV. In reverse chronological order: before working on security, he participated in multiple research projects related to hypervisor solutions for European spacecrafts, dynamic memory allocation algorithms, real-time linux, and hard real-time scheduling theory. He is also applying all this background to the security field. His current research interests include memory error defense/attacks techniques (SSP and ASLR) and software diversification. He is the Leader of the Cybersecurity Researcher Group, UPV.