Cyber Threat Intelligence Methodologies: Hunting Cyber Threats with Threat Intelligence Platforms and Deception Techniques

Arturo E. Torres, Francisco Torres, and Arturo Torres Budgud

Abstract Faced with the great wave of cyber threats, as well as the considerable increase in cybercrime in recent years, organizations have been forced to redefine their digital defense strategies to protect their information assets, infrastructure, and reputation from different people—malicious adversaries. Given this, the IT cybersecurity community has chosen to use intelligence techniques to prepare for emerging cyber threats. Therefore, the field of Cyber Threat Intelligence (CTI) has had significant growth in recent years, given the growth and evolution of cyber threats, as well as the complexity of the techniques used by adversaries. However, the CTI field has different challenges for companies that don't have a big budget or lack the experience to implement a CTI plan. The main contribution of this research is based on the compilation and investigation of the schemes, tools, challenges, and sets of methodologies most used for the execution of a CTI program, as well as the deployment of a CTI platform based on deception techniques (honeypots) for data collection and cyber threat events. This enables organizations with smaller budgets to use the CTI platform and the methodologies described in this document to stay secure.

Keywords Cyber Threat Intelligence (CTI) · Information technology · Cyber security events · Cyber threats · Intelligence sources · Cyber security · Deception techniques · Honeypots · Etc

A. E. Torres (✉) · F. Torres · A. T. Budgud
Universidad Autonoma de Nuevo Leon, San Nicolás de los Garza, N.L., Mexico
e-mail: arturo.torrescv@uanl.edu.mx; francisco.torresgrr@uanl.edu.mx;
arturo.torresbg@uanl.edu.mx

F. Torres-Guerrero et al. (eds.), *2nd EAI International Conference on Smart Technology*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-031-07670-1_2

1 Introduction

In recent years, organizations have made significant progress in many aspects at a global level, thanks to the accelerated growth and constant use of technology in their day-to-day life, that is, digital tools have become critical for organizations and your daily operation. For example, in 2019, more than 3.9 billion email accounts were registered, with an approximate of 559,000 emails sent and received every second during that year, and it is expected that by 2024 the figure will reach 4.3 billion email accounts [1]. However, dependence on digital information and tools brings with it a large number of challenges that organizations must face, since, in recent years, trends in digital crimes and cyber threats have increased considerably. Following the example mentioned above of the use of email, according to Internet Live Stats [2], approximately 2,962,154 emails were sent per second in 2020, with 67% of these being classified as spam. This tells us that digital systems are being pressured by adversaries and not only in quantity, but also in the complexity of the techniques used, such as phishing or Business Email Compromise (BEC), to be able to compromise the systems or steal corporate information [3], this being the main vector of digital fraud and malware distribution in recent years with a recorded loss of $ 1.25 trillion in 2018 alone.

Unfortunately, dependence on technology, as well as the large amount of critical and confidential information handled by organizations today, has become the target of cybercriminals, who have developed new ways to affect integrity, availability, and confidentiality of the organizations' systems and data, using advanced techniques such as digital hijacking, better known as ransomware, which recorded an approximate loss of 10.1 billion euros in 2019 [4]. The main problem that organizations face is that advanced cyber threats bypass the protection controls implemented in organizations, such as firewalls and antivirus, which are commonly based on detection engines for static signatures or known threats. Therefore, cybersecurity specialists have chosen to develop new ways to prepare for and generate new strategies in the face of these advanced threats, using collaborative intelligence platforms to prevent and/or minimize the risk of a cyberattack before it happens. This practice is known as Cyber Threat Intelligence (CTI), which is defined as knowledge based on evidence, which includes context, mechanisms, indicators, implications, and practical advice, about an existing or emerging threat to information assets of organizations that can be used to inform decisions regarding the subject's response to that threat [5].

1.1 Contributions

The main contribution of this research is based on the compilation and investigation of the schemes, tools, challenges, and sets of methodologies most used for the execution of a CTI program. This will allow organizations with smaller budgets to use the CTI platform and the methodologies described in this document to generate a defense strategy and stay secure. This chapter is organized as follows:

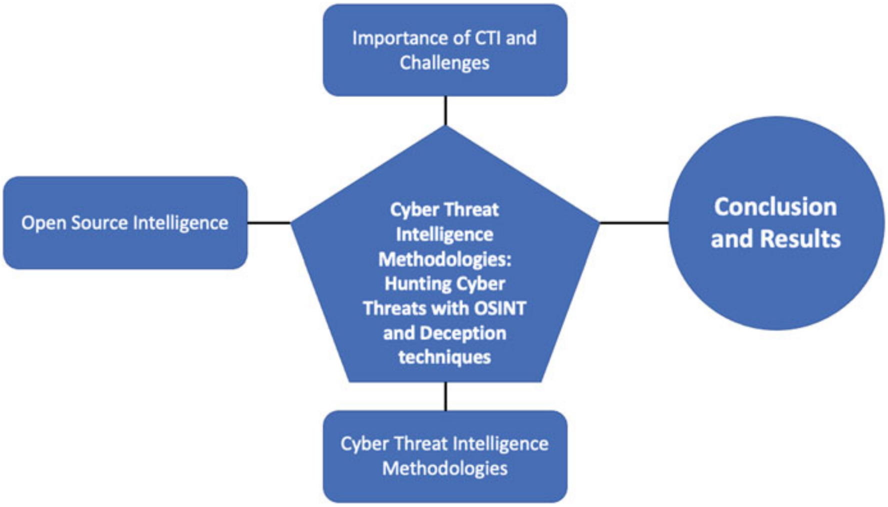

Importance of CTI and Challenges
Open Source Intelligence
Cyber Threat Intelligence Methodologies: Hunting Cyber Threats with OSINT and Deception techniques
Conclusion and Results
Cyber Threat Intelligence Methodologies

Fig. 1 Contributions and research structure

- Section II raises the importance of the CTI field, as well as the challenges that generating intelligence represents for organizations.
- Section III aims to present the research of the most relevant methodologies in the field of CTI during the last years.
- Section IV's contribution is the deployment of a TIP exposed to the internet based on deception techniques for the collection of cyber threat events for the generation of CTI.
- Section V presents the results obtained from the investigation.
- Section VI presents the conclusions of the research article (Fig. 1).

2 Importance and Challenges of CTI

The CTI field has been widely accepted by different cybersecurity specialists from different industry sectors, such as the energy sector, which has been subject to different types of advanced cyberattacks, for which reason research has been carried out to develop CTI platforms that integrate the strategic, tactical, and operational levels of IT, aiming to provide a comprehensive response to the evolving threat landscape of energy systems [6]. On the other hand, Verizon confirmed 927 incidents of cyberattacks and about 207 cases of disclosure of confirmed unauthenticated data in the financial sector, for which various cyber defense strategies and techniques for the financial sector have been explored [7], as well as the integration of digital systems, Internet of Things (IoT), cloud computing paradigms to develop smart systems, smart homes and smart cities [8]. However, one of the main points that needs to be

Table 1 Differences between data, information, and intelligence [9]

Differences between data, information, and intelligence
Data consists of discrete facts and statistics collected as a basis for further analysis.
Information is multiple data points combined to answer specific questions.
Intelligence analyzes data and information to discover patterns and stories that inform decision-making.

Table 2 Cybersecurity: Data, information and intelligence [9]

Cybersecurity: Data, information and intelligence
Data is usually just indicators like IP addresses, URLs, or hashes. It doesn't tell us much without analysis.
Information answers questions like, "How many times has my organization been mentioned on social media this month?" Although this is a much more useful result than raw data, it still does not directly report a specific action.
Intelligence is the product of a cycle of identifying questions and objectives, gathering relevant data, processing and analyzing that data, producing actionable intelligence, and distributing that intelligence.

understood in this area is the difference between data, information, and intelligence to understand CTI. Therefore, we can define data as an individual element that contains information on either a system, an action or an executed process, that is, individual elements with a specific meaning. On the other hand, we can define the term threat as the possible danger that can be used to exploit an existing vulnerability with the intention of causing damage to systems, networks, or entire organizations (Table 1).

These three terms are sometimes used without much attention according to Dr. Christopher Ahl-berg [9], which explains that some threat feeds are advertised as intelligence when in reality they are just data packets. Organizations often embed threat data sources into their network only to find that they cannot process all the additional data, which only adds to the burden on analysts trying to classify threats. Rather, threat intelligence lightens that burden by helping analysts decide what to prioritize and what to ignore. Therefore, a different context can be given to the terms data, information, and intelligence when talking about cybersecurity (Table 2).

Therefore, we can say that CTI is the ability to acquire knowledge about a company, as well as its existing conditions and capabilities, in order to determine the possible actions of a malicious actor or threat when exploiting existing critical vulnerabilities. In addition, it uses multiple information security disciplines (threat intelligence, vulnerability management, security configuration management, incident response, etc.) and sets of tools to collect information about the network through monitoring and reporting to provide decision makers at all levels to prioritize resource allocation to perform risk mitigation.

2.1 CTI Challenges

The main challenge in executing a CTI strategy focuses on the quality of intelligence obtained through data analysis and lies mainly in being able to transform this large amount of information into something actionable that can be used to make decisions for top management [10], for example, being able to prioritize activities and assign budget or personnel based on the impacts that may be had based on the data collected. This requires not only time and/or effort from the IT or cybersecurity team, but also organization, collaboration between the different areas, and experience and resources assigned by senior management to carry out these investigations successfully. Although, the commercialization of products and services related to CTI from different developers and manufacturers has helped automate many of the tasks related to the extraction, detection, and update of threats, and especially the automation of responses to incidents [11].

In order to significantly interrupt or prevent the attack or intrusion of the adversary, it is necessary to have a defensive strategy and prepare the infrastructure to take into account the security needs, controls, processes, and resources that must be available. With knowledge of the adversary's tactics and objectives, defenders must prepare their infrastructure to counter attacks in the widest range possible to cover all possible adversaries' attack vectors. However, there is some research that mentions this as a great challenge, since it is mentioned that the CTI field lacks a mature methodology, which can affect the analysis of threats and adversaries by defenders [12]. Despite its challenges, CTI should not be ruled out yet, since it is an emerging field that has great potential and constant development by the cybersecurity analyst community, with the objective of applying defense strategies and controls against adversaries. seeking to engage an organization

3 CTI Methodologies

There are different methodologies in the field of CTI, which could be defined as a structure to think about how attackers operate, discover their methods and in which part of the general life cycle of the attack that event is occurring. More specifically, CTI methodologies allow us to be very prescriptive in how we attack a specific situation, that is, they allow us to focus attention on the appropriate areas to ensure monitoring and mitigation of existing or emerging threats. They also provide a common language to communicate internally and also externally regarding threat details, interrelationships between events, and correlations with external data sources. So, we can say that they allow us to connect and understand where something is happening and focus our resources within that small area rather than trying to take a reactive approach. In addition, it allows us to be much more focused on the specific area that needs our attention to assign specific resources to a threat or technique used by an adversary that could harm our organization. That way, defenders don't waste time, effort, and resources working in areas that are not necessarily affected or perhaps not necessarily relevant to the incident they are facing or are about to face.

3.1 Cyber Kill Chain Model

The methodology developed by Lockheed Martin [13] is based on the military concept of "Kill Chain," which consists of seven different areas that allow us to understand in which part of the process or attack chain a specific threat occurs, whether in reconnaissance, weaponry, delivery, etc. Therefore, if we understand where that threat is in the process, we can focus our resources and our efforts on mitigating it. And if we have a proper framework, we can understand what actions need to be taken in that area so that we can respond quickly to the opponent's techniques [14]. For example, first comes recognition, where the adversary is looking for a weakness, that is, obtaining registration credentials or information that can be used for a phishing attack, where in this case, the weakness is the user who you receive the phishing added to the vulnerabilities of your device. The next thing is weaponization, which consists of creating the delivery of the threat, using an exploitation technique (exploit), such as a Backdoor typically. Delivery is the process of sending that payload to the victim, which could be a malicious email, it could be a USB memory left on a desk on the floor of a parking lot near the organization or even in the parking of this. Then we have vulnerabilities, in which the attacker performs the act of executing the code on the remote system and then proceeds to the phase of the actual installation of malware in that target. And that brings us to C&C, which will create a channel or persistence where the attacker can control the system remotely by sending instructions with some specific objective or purpose. At that point, the attacker already has control of perhaps more than one system; therefore, it is very important to monitor the different C&C channels detected in our network. And at the end of this, the desired actions are performed. So that's the intended goal, whether it's encrypting data, destroying it, exfiltering it, etc (Fig. 2).

This methodology describes an intelligence-based, threat-focused approach to studying intrusions from the perspective of adversaries. Each phase of the intrusion is assigned to courses of action for detection, mitigation, and response and shows that there are certain phases that the adversary has to fulfill in order to complete its objective, and that in addition, they have been used in different fields of the industry to generate strategies based on taxonomies of specific threats such as Trojans that affect the financial sector [16] and various investigations are explored on how to be able to predict certain threats or adversaries' behavior [17], which leads us to think that this model is based on the reconstruction of an attack in order to better understand it and mitigate it. Therefore, if we can understand where a specific action is in the process, we will know how to focus our efforts and resources to mitigate

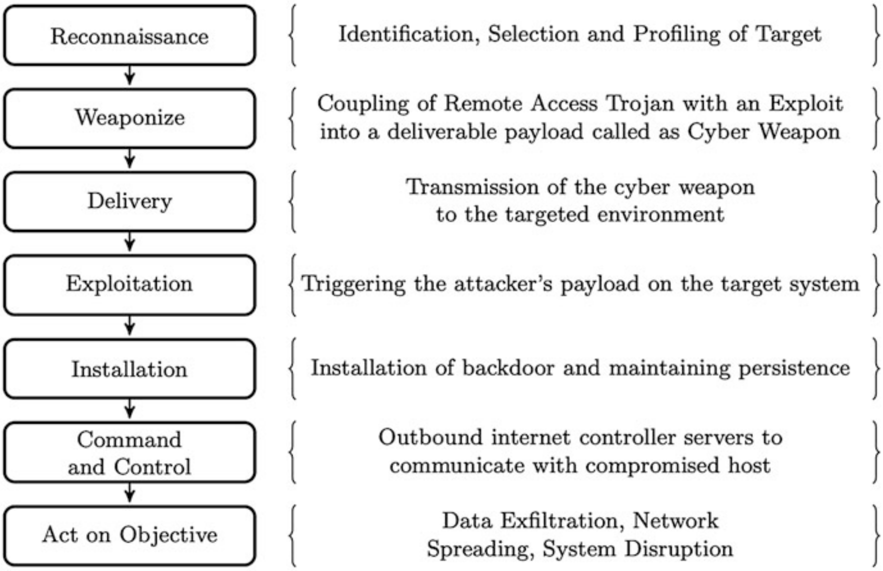

Reconnaissance
Identification, Selection and Profiling of Target
Weaponize
Coupling of Remote Access Trojan with an Exploit into a deliverable payload called as Cyber Weapon
Delivery
Transmission of the cyber weapon to the targeted environment
Exploitation
Triggering the attacker's payload on the target system
Installation
Installation of backdoor and maintaining persistence
Command and Control
Outbound internet controller servers to communicate with compromised host
Act on Objective
Data Exfiltration, Network Spreading, System Disruption

Fig. 2 Cyber Kill Chain Model phases [14, 15]

the threat before it reaches a final phase, such as a link in a chain is broken. the objective is to break the progress of the cyberattack in any of its phases [18].

3.2 The Diamond Model of Intrusion Analysis

Intrusion analysis has long been considered an art to be learned and practiced, rather than a science to be studied and refined. However, approaching it only as an art has long-delayed improvements and understanding, further slowing down the evolution of threat mitigation that relies on efficient, effective, and accurate analysis. Unknowingly, analysts have used the Diamante model for decades, but have lacked the full framework to understand, improve, and focus their efforts. This model describes the main capacities and characteristics of an intrusion event: adversary, capacity (techniques and tools used by an adversary), infrastructure, and victim, which are linked in a diamond-shaped diagram, in which the edges are used to represent relationships between features that can be exploited analytically to discover and further develop awareness of malicious activity [19], that is, the model describes that an adversary deploys a capacity on some infrastructure against a victim (Fig. 3).

These activities, in turn, are known as events, which define a series of steps that the adversary must execute to achieve their objective. Likewise, the authors of the model describe 7 fundamental bases to understand the intrusion model process in

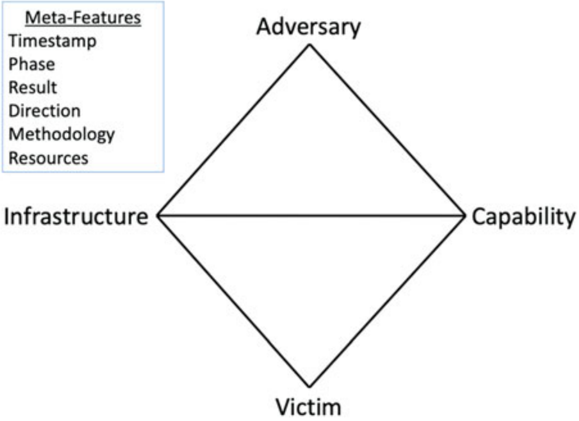


Fig. 3 The Diamond Model of intrusion analysis [19]

Table 3 Axioms of the Diamond Model [19]

Diamond Model Axioms	
Axiom 1	For every intrusion event, there exists an adversary taking a step towards an intended goal by using a capability over infrastructure against a victim to produce a result.
Axiom 2	There exists a set of adversaries (insiders, outsiders, individuals, groups, and organizations) that seek to compromise computer systems or networks to further their intent and satisfy their needs.
Axiom 3	Every system, and by extension every victim asset, has vulnerabilities and exposures.
Axiom 4	Every malicious activity contains two or more phases that must be successfully executed in succession to achieve the desired result.
Axiom 5	Every intrusion event requires one or more external resources to be satisfied prior to success.
Axiom 6	A relationship always exists between the adversary and their victim(s), even if distant, fleeting, or indirect.
Axiom 7	There exists a subset of the set of adversaries that have the motivation, resources, and capabilities to sustain malicious effects for a significant length of time against one or more victims while resisting mitigation efforts. Adversary-victim relationships in this subset are called persistent adversary relationships.

the form of Axioms, where the objectives and/or needs of the adversaries are defined in order to meet their objectives (Table 3).

The model establishes a formal method that applies scientific principles to the analysis of threats, in particular, those of measurement, testability, and repeatability, providing a comprehensive method of documentation, synthesis, and correlation of the activity [20]. For this reason, we can say that both the events and the processes or threads of each activity carried out by the attacker are necessary elements for a complete understanding of the malicious activity itself, since a more effective and strategic mitigation requires an understanding and context of the intrusions themselves, with the main objective of being able to expand the panorama of the threat and understand the phases and processes of this. This scientific approach and simplicity produce improvements in analytical effectiveness, efficiency, and precision. Ultimately, the model provides opportunities to integrate and generate real-time intelligence for network defense, automating correlation between events, confidently classifying events in adverse campaigns, and forecasting adverse operations while planning and playing mitigation strategies.

While the Kill Chain model provides information on the attackers' operations, the Diamante model broadens the perspective and context of the attackers between each of the intrusion phases, that is, it together allows to have a broader view of the attacker and not just the technical indicators. In addition, the Diamante model provides a formal mathematical method for the analysis and grouping of effective graphs (e.g., grouping/ranking) to solve many kinds of analytical problems. [19]. The Diamond Model identifies how and why an attack occurs, since we can see that an attacker attacks a victim based on two main attributes, called infrastructure and capacity, precisely capturing and organizing the fundamental concepts that underpin everything that does intrusion analysis, as well as how intrusion analysis is synthesized and used for network defense and mitigation [21]. However, its greatest contribution is that it ultimately applies scientific rigor and principles of measurement, testability, and respectability to the domain, allowing intrusion analysis to be more effective, efficient, and accurate, leading to faster, more effective, and efficient mitigation to defeat adversaries.

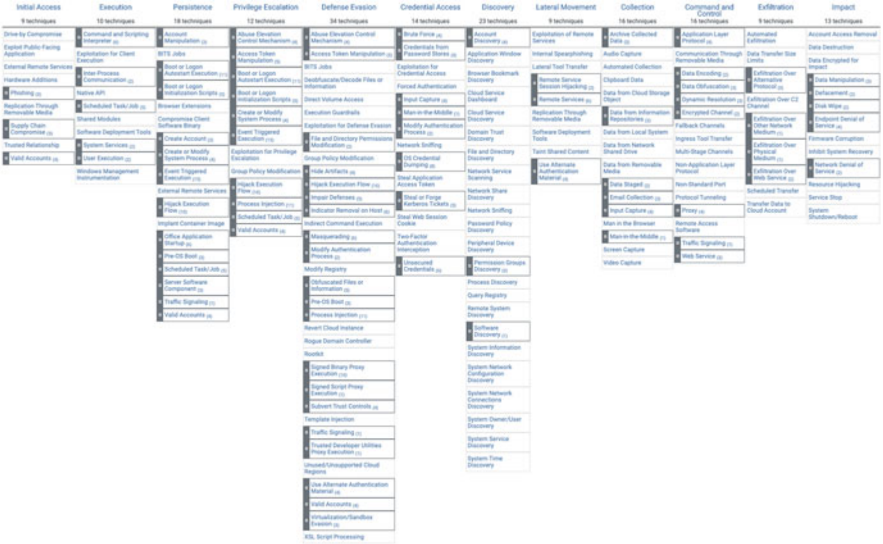
3.3 MITRE ATT&CK

MITRE is a nonprofit organization that works in the public interest in federal, state, and local governments, as well as in industry and academia. Likewise, it contributes to different areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, space security, political and economic experience, reliable autonomy, threat exchange, and cyber resilience [22]. Likewise, this organization developed a methodology called ATT&CK, which is used as a basis for the development of specific threat models in the private sector, in the government, and in the community of cybersecurity products and services that contain known behaviors of attackers or adversaries, better known as advanced persistent threats (APT), which are organized attack groups with a large amount of resources and advanced techniques that allow them to carry out complex attacks [23], and in turn, research related to this methodology in critical infrastructures has been presented [24]. For example, they often stay on an organization's network and obtain information before proceeding to the next phases of their attack. ATT&CK focuses on how external adversaries engage and operate within computer information networks (Table 4).

This model originated from a project that aimed to document and categorize postengagement adversary tactics, techniques, and procedures (TTP) against Microsoft Windows systems to improve the detection of malicious behavior. [25].

Table 4 MITRE ATT&CK core components [25]

MITRE ATT&CK core components	
Tactics	Describe the tactical objectives during an attack
Techniques	Describe the means by which adversaries achieve tactical objectives
Sub-techniques	Describe more specific means by which adversaries achieve tactical objectives at a lower level than techniques
Procedures	They are the specific implementations that the adversaries have used for techniques or sub-techniques



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	12 techniques	34 techniques	14 techniques	23 techniques	9 techniques	16 techniques	16 techniques	9 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (15)	Execution Guardrails	Man-in-the-Middle (2)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (3)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (2)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Group Policy Modification	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Removable Media	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection (11)	Hide Artifacts (9)	Steal Application Access Token	Network Sniffing		Data Staged (2)	Non-Application Layer Protocol		Network Denial of Service (2)
		Hijack Execution Flow (11)	Scheduled Task/Job (5)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)	Password Policy Discovery		Email Collection (3)	Non-Standard Port		Resource Hijacking
		Implant Container Image	Valid Accounts (4)	Impair Defenses (9)	Steal Web Session Cookie	Peripheral Device Discovery		Input Capture (4)	Protocol Tunneling		Service Stop
		Office Application Startup (6)		Indicator Removal on Host (6)	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Man in the Browser	Proxy (4)		System Shutdown/Reboot
		Pre-OS Boot (5)		Indirect Command Execution	Unsecured Credentials (7)	Process Discovery		Man-in-the-Middle (2)	Remote Access Software		
		Scheduled Task/Job (5)		Masquerading (7)		Query Registry		Screen Capture	Traffic Signaling (1)		
		Server Software Component (3)		Modify Authentication Process (2)		Remote System Discovery		Video Capture	Web Service (3)		
		Traffic Signaling (1)		Modify Registry		Software Discovery (1)					
		Valid Accounts (4)		Obfuscated Files or Information (6)		System Information Discovery					
				Pre-OS Boot (5)		System Network Configuration Discovery					
				Process Injection (11)		System Network Connections Discovery					
				Revert Cloud Instance		System Owner/User Discovery					
				Rogue Domain Controller		System Service Discovery					
				Rootkit		System Time Discovery					
				Signed Binary Proxy Execution (10)							
				Signed Script Proxy Execution (1)							
				Subvert Trust Controls (6)							
				Template Injection							
				Traffic Signaling (1)							
				Trusted Developer Utilities Proxy Execution (1)							
				Unused/Unsupported Cloud Regions							
				Use Alternate Authentication Material (4)							
				Valid Accounts (4)							
				Virtualization/Sandbox Evasion (3)							
				XSL Script Processing							

Fig. 4 MITRE ATT&CK Enterprise Matrix [26]

Since then, it has grown to include other operating systems, as well as other areas such as mobile devices, cloud-based systems, and industrial control systems. The basis of ATT&CK is the set of techniques and sub-techniques that represent actions that opponents can perform to achieve objectives. These objectives are represented by the categories of tactics to which the techniques and sub-techniques belong. The relationship between tactics, techniques, and sub-techniques can be visualized in the ATT&CK Matrix (Fig. 4).

MITRE ATT&CK offers cybersecurity analysts a common language to structure, compare, and analyze CTI for any organization that wants to move toward an informed defense on existing or emerging threats, as it includes information on malware, tools, TTP, business techniques, behavior, and other indicators associated with threats.

3.4 MITRE Shield

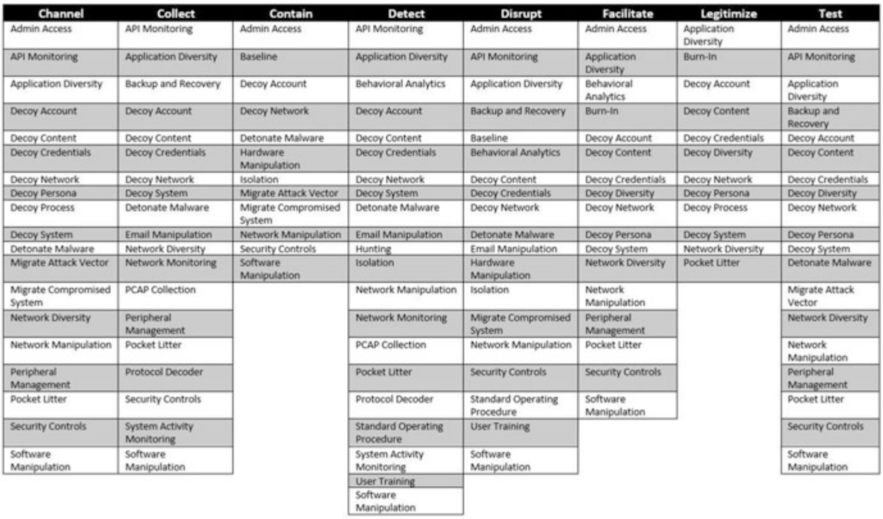
Based on the ATT&CK methodology, a new methodology called MITRE Shield was developed, which is based on the implementation of the concept of active cybernetic defense, which aims to carry out cyberdefensive actions until being able to deceive the adversary, having an active participation with him to study and learn more about the tactics and techniques used to generate a CTI and prepare for future threats. The Shield matrix consists of the following components (Table 5).

Within Shield, there is also a matrix of tactics that denotes what the defender is trying to achieve through columns and techniques, which describe how the defense achieves the tactics. However, those terms have been made to fit the domain of Active Cyber Defense. These tactics within MITRE Shield must be taken into account as a strategy of each planned active defense operation in order to respond to any intrusion from an adversary or threat. Given this, it is necessary to develop the techniques described within Shield to implement security controls in an operational environment. MITRE found that a single technique can be compatible with several different tactics, and for any tactic, there are multiple techniques that can be used. In addition, it has a section where ATT&CK tactics and techniques are mapped so that defenders can have the applicable active defense information, including the presented opportunity space, the active defense technique that will be implemented, and the use case for that implementation (Fig. 5).

The combination of ATT&CK and Shield methodologies can help defenders deepen their understanding of the opponent's behavior and engagements and suggest ways the defender can implement an active defense strategy. [28]. Therefore, the goal of Shield is that defenders can take advantage of the tactics and techniques of this methodology to better create, implement and operate their active defense solutions, showing how the defensive side of Shield to align with ATT&CK, with the main objective that organizations and their defenders can take advantage of both strategies to maximize their defensive efforts and be able to generate a more solid strategy that allows them to learn from adversaries while defending against them.

Table 5 MITRE Shield core components [27]

MITRE Shield core components	
Tactics	They are abstract goals of the defenders.
Techniques	They are general actions that a defender can take that can have several different tactical effects depending on how they are implemented.
Procedures	They are implementations of a technique.
Opportunity	They describe high-level active defense possibilities that are introduced when attackers employ their techniques.
Use Cases	High-level descriptions of how a defender might do something to take advantage of the opportunity presented by the attacker's action



Channel	Collect	Contain	Detect	Disrupt	Facilitate	Legitimize	Test
Admin Access	API Monitoring	Admin Access	API Monitoring	Admin Access	Admin Access	Application Diversity	Admin Access
API Monitoring	Application Diversity	Baseline	Application Diversity	API Monitoring	Application Diversity	Burn-In	API Monitoring
Application Diversity	Backup and Recovery	Decoy Account	Behavioral Analytics	Application Diversity	Behavioral Analytics	Decoy Account	Application Diversity
Decoy Account	Decoy Account	Decoy Network	Decoy Account	Backup and Recovery	Burn-In	Decoy Content	Backup and Recovery
Decoy Content	Decoy Content	Detonate Malware	Decoy Content	Baseline	Decoy Account	Decoy Credentials	Decoy Account
Decoy Credentials	Decoy Credentials	Hardware Manipulation	Decoy Credentials	Behavioral Analytics	Decoy Content	Decoy Diversity	Decoy Content
Decoy Network	Decoy Network	Isolation	Decoy Network	Decoy Content	Decoy Credentials	Decoy Network	Decoy Credentials
Decoy Persona	Decoy System	Migrate Attack Vector	Decoy System	Decoy Credentials	Decoy Diversity	Decoy Persona	Decoy Diversity
Decoy Process	Detonate Malware	Migrate Compromised System	Detonate Malware	Decoy Network	Decoy Network	Decoy Process	Decoy Network
Decoy System	Email Manipulation	Network Manipulation	Email Manipulation	Detonate Malware	Decoy Persona	Decoy System	Decoy Persona
Detonate Malware	Network Diversity	Security Controls	Hunting	Email Manipulation	Decoy System	Network Diversity	Decoy System
Migrate Attack Vector	Network Monitoring	Software Manipulation	Isolation	Hardware Manipulation	Network Diversity	Pocket Litter	Detonate Malware
Migrate Compromised System	PCAP Collection		Network Manipulation	Isolation	Network Manipulation		Migrate Attack Vector
Network Diversity	Peripheral Management		Network Monitoring	Migrate Compromised System	Peripheral Management		Network Diversity
Network Manipulation	Pocket Litter		PCAP Collection	Network Manipulation	Pocket Litter		Network Manipulation
Peripheral Management	Protocol Decoder		Pocket Litter	Security Controls	Security Controls		Peripheral Management
Pocket Litter	Security Controls		Protocol Decoder	Standard Operating Procedure	Software Manipulation		Pocket Litter
Security Controls	System Activity Monitoring		Standard Operating Procedure	User Training			Security Controls
Software Manipulation	Software Manipulation		System Activity Monitoring	Software Manipulation			Software Manipulation
			User Training				
			Software Manipulation				

Fig. 5 The Shield Matrix [28]

4 Threat Intelligence Platform (TIP)

The techniques and results that CTI has provided in recent years have gained a great deal of attention in cybersecurity communities as a way to forecast potential threats and reduce attack detection time in terms of supply chain processes. death, as well as the use of open-source intelligence information (OSINT) is becoming a fundamental approach to gain awareness about cybersecurity threats; however, to process the large amount of information is usually one of the most important challenges in this area for defenders. Therefore, cybersecurity researchers and analysts have opted for the use of intelligence tools and platforms to be able to manage all threat analysis tasks in an orderly manner. A threat intelligence platform (TIP) helps organizations aggregate, correlate, and analyze threat data from multiple sources in real time and is comprised of several core features that enable organizations to implement an intelligence-driven approach to security to support defensive actions. The main purpose is to help organizations understand risks and protect against a variety of threat types that are likely to affect their environments collected from different intelligence sources (Table 6).

A TIP automatically analyzes the content of the threat indicators and the relationships between them to enable the production of useful, relevant, and timely threat intelligence from the data collector. This analysis allows the identification of tactics, techniques, and procedures of the threat actors or TTPs. These platforms can be a cloud or on-premises system to facilitate threat data management from a variety

Table 6 Threat Intelligence Platforms stages

Threat intelligence platforms stages	
Collect	A threat intelligence platform collects and aggregates multiple data formats for multiple sources, including formats such as STIX, CSV, XML, email, and various intelligence sources.
Correlate	The threat intelligence platform enables organizations to automatically begin to analyze correlation and pivot on data so that actionable intelligence on who, why, and how again of an attack can be obtained on the blocking measures introduced.
Enrichment and contextualization	A threat intelligence platform must be able to automatically enhance or allow threat intelligence analysts to use third-party threat analysis applications to enrich the data collected in an investigation.
Analyze	Automatically analyzes the content of threat indicators and the relationships between them to enable the production of useful, relevant, and timely threat intelligence from the data collector.
Integrate	Platform data must find a way back to the security tools and products an organization uses to enable process automation and communication.
Act	Integrated processes and workflows accelerate collaboration within the broader communications and security team, such as intelligence sharing and analytics organizations.

of existing security tools, such as SIEM, Firewall, API, Terminal Management Software, or Intrusion Prevention System (IPS). Investigations and papers have been presented where some threat intelligence exchange platforms are evaluated [29] [30], where users from the IT community and other communities in general can share their incident information in a trusted environment, such as Malware Information Sharing Platform (MISP) [31], which allows us to share, store, and correlate indicators of compromise of targeted attacks, threat intelligence, financial fraud information, and vulnerability information [32]. The malware information exchange platform can be accessed from different interfaces, such as a web interface (for analysts or incident handlers) or via a ReST API (for systems that push and pull IOCs). The inherent goal of MISP is to be a robust platform that ensures smooth operation when revealing, maturing, and exploiting threat information.

4.1 T-Pot: Platform Based on Deception Techniques

Currently, there are tools and/or platforms whose main objective is to be able to simulate a productive environment or service to maintain active communication with the adversary, commonly known as honeypots, which allows defenders to collect more information about the TTPs to be able to generate CTI. There are different honeypot platforms on the market, especially by some cybersecurity manufacturers, such as TrapX Security [33], Attivo Networks [34] and Fortinet [35], that help to

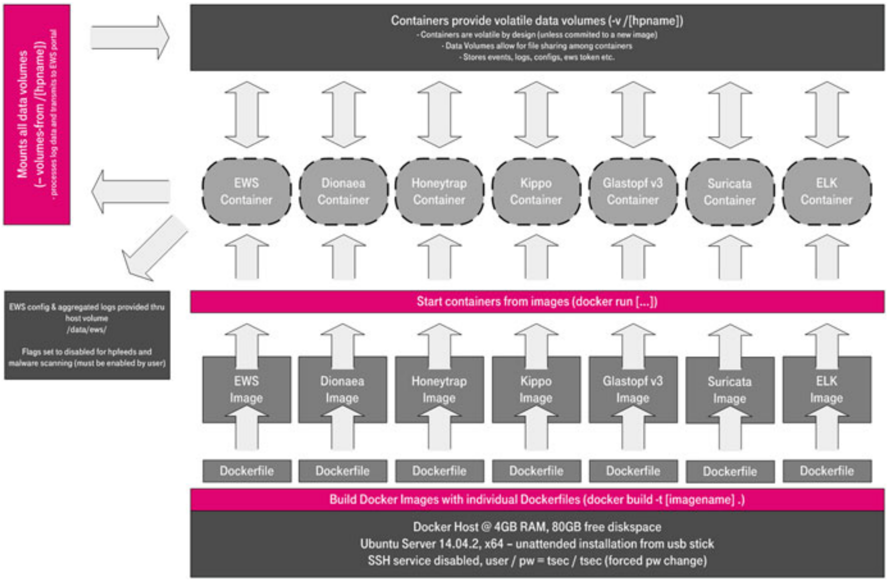

Mounts all data volumes
(--volumes-from /[hpname])
- processes log data and transmits to EWS portal
Containers provide volatile data volumes (-v /[hpname])
- Containers are volatile by design (unless commited to a new image)
- Data Volumes allow for file sharing among containers
- Stores events, logs, configs, ews token etc.
EWS Container
Dionaea Container
Honeytrap Container
Kippo Container
Glastopf v3 Container
Suricata Container
ELK Container
EWS config & aggregated logs provided thru host volume
/data/ews/
Flags set to disabled for hpfeeds and malware scanning (must be enabled by user)
Start containers from images (docker run [...])
EWS Image
Dionaea Image
Honeytrap Image
Kippo Image
Glastopf v3 Image
Suricata Image
ELK Image
Dockerfile
Dockerfile
Dockerfile
Dockerfile
Dockerfile
Dockerfile
Dockerfile
Build Docker Images with individual Dockerfiles (docker build -t [imagename] .)
Docker Host @ 4GB RAM, 80GB free diskspace
Ubuntu Server 14.04.2, x64 – unattended installation from usb stick
SSH service disabled, user / pw = tsec / tsec (forced pw change)

Fig. 6 T-Pot arquitecture [38]

detect external and internal threats, and studies reveal that two-thirds of the incidents found were from external actors, while the remaining third involved internal actors [36]. There are some investigations related to platforms that have multi-honeypot systems, which have focused on the investigation and relevance of the data collected through attacks. [37]. T-Pot is based on a vanilla ISO image of Ubuntu 14.04.02, which is heavily dependent on docker and docker-compose. The goal proposed by T-Pot is to create a system whose full TCP network range, as well as some important UDP services, acts as decoys for adversaries, in order to forward all incoming attack traffic to the honeypot sensors. more suitable for interacting and processing said information [38] (Fig. 6).

The project provides multiple coupled honeypots and a large number of preinstalled research tools, such as ELK, which provides a search engine and analytics, as well as an interface for data visualization. [39], Spiderfoot, which allows to perform Footprinting tasks, by acting as an aggregator of a multitude of sources, on which it allows a simple and fast search by having its own web interface [40], Cyberchef—a web application for data encryption, encoding, compression, and analysis [41]; Suricata—capable of real-time intrusion detection (IDS); online intrusion prevention (IPS); network security monitoring (NSM); and offline pcap processing [42], among others (Table 7).

Table 7 T-Pot honeypots [38]

T-Pot honeypots	
adbhoney	Low interaction honeypot designed for Android Debug Bridge over TCP/IP
ciscoasa	A low interaction honeypot for the Cisco ASA component capable of detecting CVE-2018-0101, a DoS, and remote code execution vulnerability.
citrixhoneypot	Detect and log CVE-2019-19781 scan and exploitation attempts.
conpot	Conpot is a low interactive server-side Industrial Control Systems honeypot designed to be easy to deploy, modify, and extend.
cowrie	Cowrie is a medium to high interaction SSH and Telnet honeypot designed to log brute force attacks and the shell interaction performed by the attacker.
dicompot	A Digital Imaging and Communications in Medicine (DICOM) honeypot.
dionaea	Dionaea is meant to be a nepenthes successor, embedding python as scripting language, using libemu to detect shellcodes, supporting ipv6 and tls.
elasticpot	This is a honeypot simulating a vulnerable Elasticsearch server opened to the internet.
glutton	Glutton provide SSH and a TCP proxy. SSH proxy works as a MITM between attacker and server to log everything in plain text.
heralding	Simple honeypot that collects credentials of the following protocols: ftp, telnet, ssh, rdp, http, https, pop3, pop3s, imap, imaps, smtp, vnc, postgresql, and socks5.
honeypy	A low interaction honeypot with the capability to be more of a medium interaction honeypot.
honeysap	A low-interaction research-focused honeypot specific for SAP services.
honeytrap	A network security tool written to observe attacks against TCP or UDP services.
ipphoney	This is a honeypot simulating a printer that supports the Internet Printing Protocol and is exposed to the internet.
mailoney	SMTP honeypot.
medpot	HL7/FHIR honeypot.
rdpy	Remote Desktop Protocol in twisted python.
snare	A web application honeypot sensor.
tanner	Decides how SNARE should respond to the client.

5 Experimentation and Results

In this investigation, we deployed T-Pot in the public cloud of Amazon Web Services (AWS), with the main objective of exposing the available honeypots of the T-Pot platform to the internet, in order to be able to collect real threats that are mostly automated in cyberspace, which will allow us to collect some of the adversaries' TTPs and analyze the information to model it with the methodologies described in the document through case studies, with the purpose of being able to identify how each of the models facing a real cyberattack and how they complement each other. The following is the data collected by the platform for 20 days and the characteristics and resources used to deploy the T-Pot platform on AWS (Fig. 7 and Table 8).

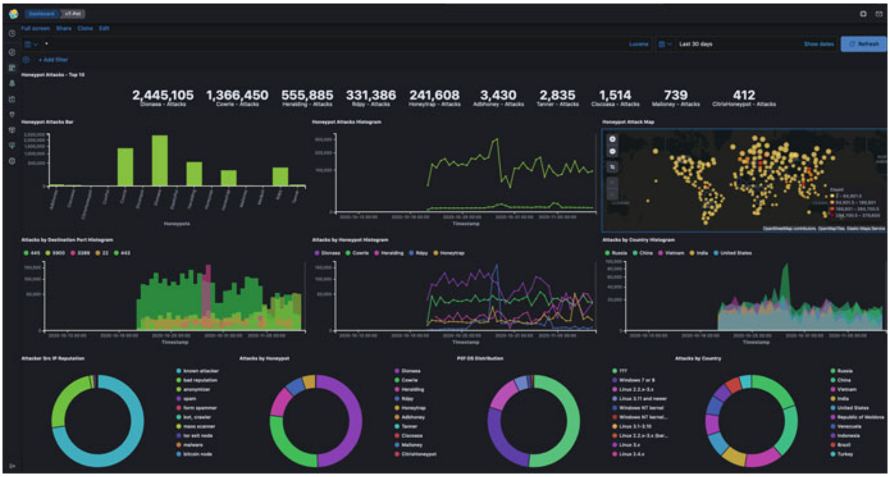


Fig. 7 Detected attacks on T-Pot honeypots at AWS after 20 days

Table 8 AWS-arranged resources to deploy T-Pot

T-Pot resources	
RAM	t2.xlarge (16Gbps)
vCPUs	4
OS	Linux/Debian 10
Days Active	20
Public Ip	Yes

5.1 *Case Study*

In this section, we analyze the data collected by the honeypots exposed to the internet to analyze the Cyber Kill Chain, ATT&CK, and Shield and Diamond Models, in order to understand some of the phases and TTP's carried out by the adversaries to achieve their objectives within the infrastructure deployed.

The case study that arises involves a victim who deploys a service with SSH, or Secure Shell, makes it very easy to access remote servers while keeping them safe from hackers. The adversaries used mass scanning techniques to detect known vulnerabilities in the exposed systems. Additionally, adversaries performed email creation using techniques such as social engineering and phishing based on previous GeoIP scans to decide the language to use. Additionally, adversaries generated an exploit to run a webshell as malware from a previously infected website. Different attempts to access the platforms by protocols such as SSH and RDP from IPs classified as malicious were detected. Some of these IPs managed to access the systems through the use of techniques such as Brute Force and dictionary attacks.

Once the adversary entered the system, command executions were detected for downloading files through a shellcode to a URL classified as malicious by malware content. After downloading, command executions were detected for downloading malware files from an IP classified as malicious. Once the malicious domains/IPs and the malware downloaded by the adversary were detected, we proceeded to review open intelligence sources such as Virus Total to search for the IPs or domains related to the installed malware. The results of the investigations carried out with the methodologies described in the document are presented below. The Cyber Kill Chain Model helps us understand each of the phases of the attack chain carried out by the adversaries and guides us to be able to start searching for the relevant events in each of the phases (Table 9).

With the information collected by the honeypot platform and the Cyber Kill Chain Model, it is possible to delve much more into the tactics and techniques used by the adversaries to understand their objectives and operations through the use of MITRE ATT&CK (Table 10).

Once the TTPs of the adversaries are modeled in ATT&CK, we can use MITRE Shield to make a map of the TTPs found in ATT&CK used by the adversaries to carry out an active defense strategy. For example, initial access to the exposed systems was done through a remote exposed system through a valid account. Given this, Shield gives us the possibility of generating an active defense strategy with the opportunity to validate if the adversary already has credentials from one or more accounts valid for any network system by using a decoy or honeypot to collect more information on the TTPs used by the adversary as we have been doing during this investigation (Table 11).

With Diamond Model, we use a victim-centered approach (honeypot) in order to reveal the connection between the adversary's related elements, such as infrastructure and capabilities organized in events (Table 12 and Fig. 8).

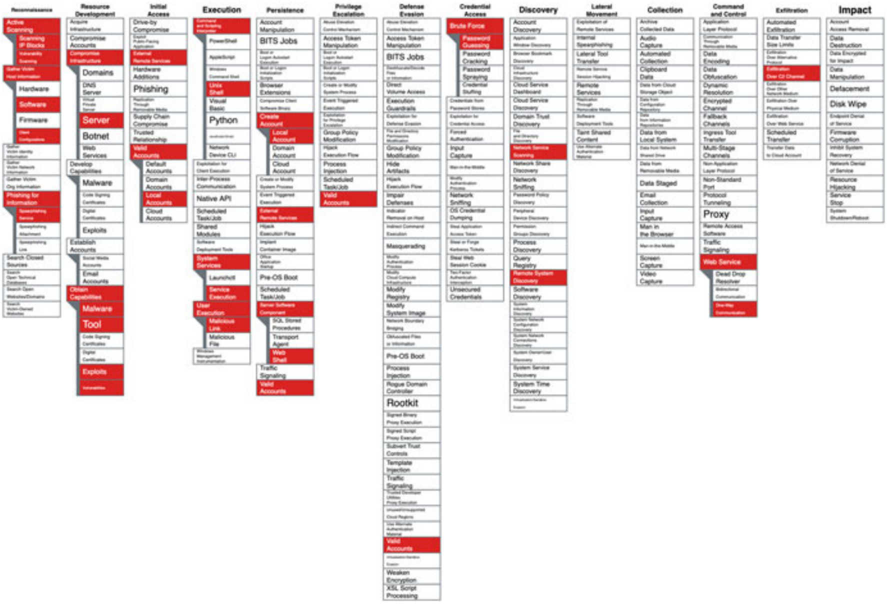
6 Conclusions

The conventional incident response process is generally initiated after a successful exploitation phase is executed, causing defenders to be inherently disadvantaged and their response too late. In this research, we have demonstrated the effective use of the most used methodologies in the CTI field for the detection, mitigation, and generation of CTI during the analysis and investigation process of real TTPs collected using a platform with deception techniques; it was found that these methodologies complement each other. In which, the Cyber Kill Chain Model helps us understand the phases of an adversary's attack; therefore, we obtain an initial guide for defenders on where to focus their resources, and in turn, it helps to feed the MITRE ATT&CK model, which gives us the opportunity to list and understand what TTPs are used by adversaries in each of their attack phases and provide the necessary information for the generation of an active defense strategy with MITRE Shield. Therefore, Shield is responsible for guiding us on how to take advantage of

Table 9 Case study results with Cyber Kill Chain Model

Phase	Procedure	Indicators
Reconnaissance	ip_rep.keyword: mass scanner	*Suricata Signature:* ET SCAN NMAP -sS window 1024 ET POLICY RDP connection request ET DOS Microsoft RDP Syn then Reset 30 Second DoS Attempt ET SCAN Potential SSH Scan
Weaponization	Webshell creation Previous Infected URL data: password data: covid	SSH Dictionary Attack detected Phishing emails detected
Delivery	message: login message: success eventid: cowrie.login.success src_port: 22	*Attacker IP:* 206[.]189[.]50[.]126, 46[.]101[.]156[.]22, 185[.]153[.]199[.]182 *Message Log:* login attempt / succeeded
Exploitation	message: download input: wget	*Downstream URL:* http://104[.]168[.]195[.]213/Thorbins.sh http://212[.]73[.]150[.]134/NoHomobins.sh *Exploited vulnerabilities:* CVE-2001-0540, CVE-2012-0152, CVE-2019-0708
Installation	eventid: cowrie.command.input input: wget input: run input: 104[.]168[.]195[.]213	*Malware/Trojan:* 48251b805670802373821564eb9c7056703a6822d4e025c790d3acce0776c7fa *Malware/Downloader:* a2ef7e6b666d570dd6e26cddf4d4fd7f *Executed commands:* cd /tmp || cd /run || cd /; wget http:// 104[.]168[.]195[.]213/Thorbins.sh; chmod 777 Thorbins.sh; sh Thorbins.sh; tftp 104[.]168[.]195[.]213-c get Thortftp1.sh; chmod 777 Thortftp1.sh; sh Thortftp1.sh; tftp -r Thortftp2.sh -g 104[.]168[.]195[.]213; chmod 777 Thortftp2.sh; sh Thortftp2.sh; rm -rf Thorbins.sh Thortftp1.sh Thortftp2.sh; rm -rf *
C2	Se realizaron busquedas en Virus Total y Spiderfoot con los hashes del malware y las IP’s encontradas	23[.]47[.]207[.]24:80 (TCP) 184[.]28[.]221[.]115:80 (TCP) 23[.]47[.]206[.]49:443 (TCP) 17[.]249[.]25[.]246:443 (TCP) 17[.]142[.]169[.]200:443 (TCP) 17[.]253[.]21[.]208:443 (TCP)
Actions on objectives	N/A	N/A

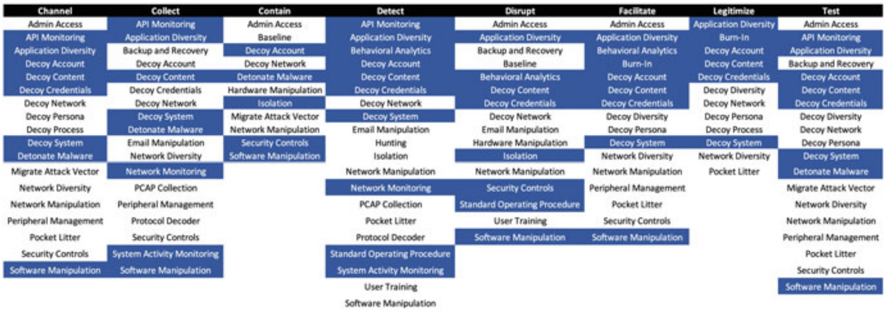
Table 10 Case study results with MITRE ATT&CK



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Active Scanning	Acquire Infrastructure	Drive-by Compromise	**Command and Scripting Interpreter**	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism
Scanning IP Blocks	Compromise Accounts	Exploit Public-Facing Application	PowerShell	BITS Jobs	Access Token Manipulation	Access Token Manipulation
Vulnerability Scanning	**Compromise Infrastructure**	**External Remote Services**	AppleScript	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs
Gather Victim Host Information	Domains	Hardware Additions	Windows Command Shell	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information
Hardware	DNS Server	Phishing	**Unix Shell**	Browser Extensions	Create or Modify System Process	Direct Volume Access
Software	Virtual Private Server	Replication Through Removable Media	Visual Basic	Compromise Client Software Binary	Event Triggered Execution	Execution Guardrails
Firmware	**Server**	Supply Chain Compromise	Python	**Create Account**	Exploitation for Privilege Escalation	Exploitation for Defense Evasion
Client Configurations	Botnet	Trusted Relationship	JavaScript	**Local Account**	Group Policy Modification	File and Directory Permissions Modification
Gather Victim Identity Information	Web Services	**Valid Accounts**	Network Device CLI	Domain Account	Hijack Execution Flow	Group Policy Modification
Gather Victim Network Information	Develop Capabilities	Default Accounts	Exploitation for Client Execution	Cloud Account	Process Injection	Hide Artifacts
Gather Victim Org Information	Malware	Domain Accounts	Inter-Process Communication	Create or Modify System Process	Scheduled Task/Job	Hijack Execution Flow
Phishing for Information	Code Signing Certificates	**Local Accounts**	Native API	Event Triggered Execution	**Valid Accounts**	Impair Defenses
Spearphishing Service	Digital Certificates	Cloud Accounts	Scheduled Task/Job	**External Remote Services**		Indicator Removal on Host
Spearphishing Attachment	Exploits		Shared Modules	Hijack Execution Flow		Indirect Command Execution
Spearphishing Link	Establish Accounts		Software Deployment Tools	Implant Container Image		Masquerading
Search Closed Sources	Social Media Accounts		**System Services**	Office Application Startup		Modify Authentication Process
Search Open Technical Databases	Email Accounts		Launchctl	Pre-OS Boot		Modify Cloud Compute Infrastructure
Search Open Websites/Domains	**Obtain Capabilities**		**Service Execution**	Scheduled Task/Job		Modify Registry
Search Victim-Owned Websites	**Malware**		**User Execution**	**Server Software Component**		Modify System Image
	Tool		**Malicious Link**	SQL Stored Procedures		Network Boundary Bridging
	Code Signing Certificates		Malicious File	Transport Agent		Obfuscated Files or Information
	Digital Certificates		Windows Management Instrumentation	**Web Shell**		Pre-OS Boot
	Exploits			Traffic Signaling		Process Injection
	Vulnerabilities			**Valid Accounts**		Rogue Domain Controller
						Rootkit
						Signed Binary Proxy Execution
						Signed Script Proxy Execution
						Subvert Trust Controls
						Template Injection
						Traffic Signaling
						Trusted Developer Utilities Proxy Execution
						Unused/Unsupported Cloud Regions
						Use Alternate Authentication Material
						Valid Accounts
						Virtualization/Sandbox Evasion
						Weaken Encryption
						XSL Script Processing

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Password Guessing	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Password Cracking	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Password Spraying	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	**Exfiltration Over C2 Channel**	Data Manipulation
Credential Stuffing	Cloud Service Dashboard	Remote Services	Data from Cloud Storage Object	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Credentials from Password Stores	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Exploitation for Credential Access	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Forced Authentication	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Input Capture	**Network Service Scanning**	Use Alternate Authentication Material	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Man-in-the-Middle	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service
Modify Authentication Process	Network Sniffing		Data Staged	Non-Standard Port		Resource Hijacking
Network Sniffing	Password Policy Discovery		Email Collection	Protocol Tunneling		Service Stop
OS Credential Dumping	Peripheral Device Discovery		Input Capture	Proxy		System Shutdown/Reboot
Steal Application Access Token	Permission Groups Discovery		Man in the Browser	Remote Access Software		
Steal or Forge Kerberos Tickets	Process Discovery		Man in the Middle	Traffic Signaling		
Steal Web Session Cookie	Query Registry		Screen Capture	**Web Service**		
Two-Factor Authentication Interception	**Remote System Discovery**		Video Capture	Dead Drop Resolver		
Unsecured Credentials	Software Discovery			Bidirectional Communication		
	System Information Discovery			**One-Way Communication**		
	System Network Configuration Discovery					
	System Network Connections Discovery					
	System Owner/User Discovery					
	System Service Discovery					
	System Time Discovery					
	Virtualization/Sandbox Evasion					

Table 11 Case study results with MITRE Shield



Channel	Collect	Contain	Detect	Disrupt	Facilitate	Legitimize	Test
Admin Access	**API Monitoring**	Admin Access	**API Monitoring**	Admin Access	Admin Access	**Application Diversity**	Admin Access
API Monitoring	**Application Diversity**	Baseline	**Application Diversity**	**Application Diversity**	**Application Diversity**	**Burn-In**	**API Monitoring**
Application Diversity	Backup and Recovery	**Decoy Account**	**Behavioral Analytics**	Backup and Recovery	**Behavioral Analytics**	**Decoy Account**	**Application Diversity**
Decoy Account	Decoy Account	Decoy Network	**Decoy Account**	Baseline	**Burn-In**	**Decoy Content**	Backup and Recovery
Decoy Content	**Decoy Content**	**Detonate Malware**	**Decoy Content**	**Behavioral Analytics**	**Decoy Account**	**Decoy Credentials**	**Decoy Account**
Decoy Credentials	Decoy Credentials	Hardware Manipulation	**Decoy Credentials**	**Decoy Content**	**Decoy Content**	Decoy Diversity	**Decoy Content**
Decoy Network	Decoy Network	**Isolation**	Decoy Network	**Decoy Credentials**	**Decoy Credentials**	Decoy Network	**Decoy Credentials**
Decoy Persona	**Decoy System**	Migrate Attack Vector	**Decoy System**	Decoy Network	Decoy Diversity	Decoy Persona	Decoy Diversity
Decoy Process	**Detonate Malware**	Network Manipulation	Email Manipulation	Email Manipulation	Decoy Persona	Decoy Process	Decoy Network
Decoy System	Email Manipulation	**Security Controls**	Hunting	Hardware Manipulation	**Decoy System**	**Decoy System**	Decoy Persona
Detonate Malware	Network Diversity	**Software Manipulation**	Isolation	**Isolation**	Network Diversity	Network Diversity	**Decoy System**
Migrate Attack Vector	**Network Monitoring**		Network Manipulation	Network Manipulation	Network Manipulation	Pocket Litter	**Detonate Malware**
Network Diversity	PCAP Collection		**Network Monitoring**	**Security Controls**	Peripheral Management		Migrate Attack Vector
Network Manipulation	Peripheral Management		PCAP Collection	**Standard Operating Procedure**	Pocket Litter		Network Diversity
Peripheral Management	Protocol Decoder		Pocket Litter	User Training	Security Controls		Network Manipulation
Pocket Litter	Security Controls		Protocol Decoder	**Software Manipulation**	**Software Manipulation**		Peripheral Management
Security Controls	**System Activity Monitoring**		**Standard Operating Procedure**				Pocket Litter
Software Manipulation	**Software Manipulation**		**System Activity Monitoring**				Security Controls
			User Training				**Software Manipulation**
			Software Manipulation				

the adversaries' TTPs to actively defend ourselves and collect more information in order to actively generate CTI to complement ATT&CK and the Diamond Model. Finally, the Diamond Model powered by Kill Chain, ATT&CK, and Shield, is very useful to list the capabilities and infrastructure of the adversaries, with the main objective of understanding and documenting their attack methodology to generate CTI, which can be alienated by Shield constantly.

Understanding how a cyberattack can benefit a security team in our organization can benefit the cybersecurity community by encouraging defenders to collect data on adversaries to increase the knowledge base of TTPs, facilitating the selection

Table 12 Case study results with Diamond Model

Event	Description	Phase	Methodology	Infrastructure	Capability
1	The adversaries used mass scanning techniques to detect known vulnerabilities of the exposed systems.	Reconnaissance	Active scanning	Bad IPs reputations	Massive scanners tools
2	Creation of Phishing Emails based on the previous GeoIP scans to decide the language to use.	Resource development	Spear phishing service	N/A	Email
3	The adversaries could create or obtain a malicious payload or exploit to execute a webshell as a downloader/trojan malware.	Resource development	Compromise Infrastructure Obtain Capabilities	N/A	Malicious payload/malware
4	Different attempts to access the platforms by protocols such as RDP from IPs classified as malicious were detected.	Initial access	External Remote Access	206[.]189[.]50[.]126 46[.]101[.]156[.]22	Automated scripts/tools
5	Different attempts to access the platforms by protocols such as SSH from IPs cataloged as malicious were detected.	Initial access	External Remote Access Valid Accounts	206[.]189[.]50[.]126 46[.]101[.]156[.]22 185[.]153[.]199[.]182	Automated scripts/tools and dictionaries
6	Some of these IPs managed to access the systems through the use of techniques such as Brute Force and dictionary attacks.	Credential access	External Remote Access Valid Accounts	46[.]101[.]156[.]22	Brute force attack
7	Once the adversary entered the system, command executions were detected for downloading files through a shellcode to a URL classified as malicious by malware content.	Execution	Malicious link	http://104[.]168[.]195[.]213/Thorbins.sh http://212[.]73[.]150[.]134/NoHomobins.sh	Service execution Vulnerable exposed server
8	Command to add, modify, and give execution permissions and deletion of events were detected for the downloading of malicious files.	Persistence	Web shell	http://104[.]168[.]195[.]213/Thorbins.sh	Web shell Malicious payload/malware
9	Once the malicious domains/IPs were detected and the malware downloaded by the adversary, open intelligence sources such as Virus Total were reviewed to search for the IPs or domains related to the installed malware.	Command and control	Web service	23[.]47[.]207[.]24:80 184[.]28[.]221[.]115:80 23[.]47[.]206[.]49:443 17[.]249[.]25[.]246:443 17[.]142[.]169[.]200:443 17[.]253[.]21[.]208:443	Vulnerable exposed server

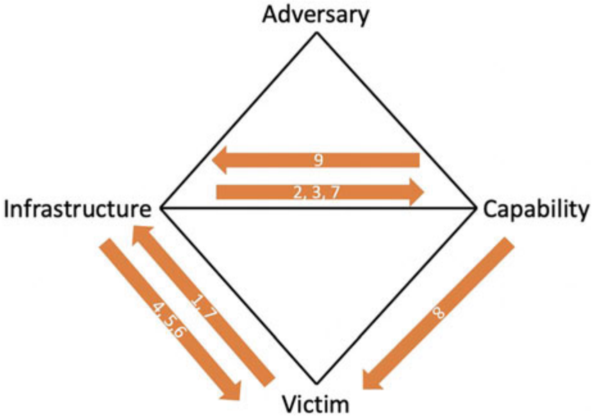


Fig. 8 Case study results with Diamond Model

of defense measures. If defenders implement countermeasures faster than their opponents evolve, they maintain a tactical advantage.

References

1. N. Gilbert, «Number of Email Users Worldwide 2020: Demographics & Predictions,» Finances Online, [En línea]. Available: https://financesonline.com/number-of-email-users/. [Último acceso: 27 10 2020]
2. I.L. Stats, «Internet Live Stats,» [En línea]. Available: https://www.internetlivestats.com/one-second/#email-band. [Último acceso: 27 10 2020]
3. Interpol, «Business Email Compromise Fraud,» [En línea]. Available: https://www.interpol.int/en/Crimes/Financial-crime/Business-Email-Compromise-Fraud. [Último acceso: 27 10 2020]
4. R.E.T. Landscape, «ENISA Threat Landscape 2020 – Ransomware,» April 2020. [En línea]. Available: https://www.enisa.europa.eu/publications/ransomware. [Último acceso: 27 10 2020]
5. Gartner, «How Gartner Defines Threat Intelligence,» Gartner, 23 02 2016. [En línea]. Available: https://www.gartner.com/en/documents/3222217/how-gartner-defines-threat-intelligence. [Último acceso: 27 10 2020]
6. R. Leszczyna, M.R. Wróbel, Threat intelligence platform for the energy sector. Softw. Pract. Exp. **49**(8), 1225–1254 (2019)
7. Y.A.R.V. Creado, Active cyber defence strategies and techniques for banks and financial institutions. J. Financ. Crime **27**(3), 771 (2020)
8. E. A. B. T. a. J. H. N. Moustafa, «A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems,» *IEEE Access,* vol 6, 2018
9. D.C. Ahlberg, *The Threat Intelligence Handbook* (CyberEdge Group, 2019)
10. M. &. R. S. &. A. (. D. A. &. R. Y. Abu, «Cyber threat intelligence – Issue and challenges,» Indonesian J. Electr. Eng. Comput. Sci. 2018
11. Fortinet, «Threat Intelligence at Machine Speed,» [En línea]. Available: https://www.fortinet.com/fortiguard/labs. [Último acceso: 06 11 2020]
12. K. O. &. C. Doerr, «Cyber Threat Intelligence: A Product Without a Process?,» Int. J. Intell.Count. Intell., 2020

13. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Lockheed Martin Corporation, «LM-White-Paper-Intel-Driven-Defense,» [En línea]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf. [Último acceso: 28 08 2020]
14. SANS, «Leveraging the Human to Break the Cyber Kill Chain,» SANS, 2016. [En línea]. Available: https://www.sans.org/security-awareness-training/blog/leveraging-human-break-cyber-kill-chain. [Último acceso: 02 09 2020]
15. T. &. R. A. Yadav, «Technical Aspects of Cyber Kill Chain,» *Third International Symposium on Security in Computing and Communications,* 2015
16. T.D.A.B. Dargahi, A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. J. Comput. Virol. Hack. Tech., 277–309 (2019)
17. B.I.A.A.M.S.T.S.B. Junaidu, Proposed framework for effective detection and prediction of advanced persistent threats based on the cyber kill chain. Sci. Pract. Cyber Secur. J. **3**(3) (2019)
18. lockheedmartin, «Applying Cyber Kill Chain® Methodology to Network Defense,» lockheedmartin, 2015. [En línea]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf. [Último acceso: 02 09 2020]
19. A.P.C.B. Sergio Caltagirone, «The Diamond Model of Intrusion Analysis,» 2013. [En línea]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf. [Último acceso: 03 09 2020]
20. Q. M. A. N. I. A. A. C. a. J. D. Hamad AL-Mohannadi, «Cyber-Attack Modeling Analysis Techniques: An Overview,» de *4th International Conference on Future Internet of Things and Cloud Workshops*, United Kingdom, Warwickshire, 2016
21. Q. M. A. N. I. A. A. C. a. J. D. H. Al-Mohannadi, «Cyber-Attack Modeling Analysis Techniques: An Overview,» *IEEE 4th International Conference on Future Internet of Things and Cloud Workshops,* 2016
22. MITRE, «Corporate Overview,» [En línea]. Available: https://www.mitre.org/about/corporate-overview. [Último acceso: 04 11 2020]
23. MITRE, «Groups,» MITRE, [En línea]. Available: https://attack.mitre.org/groups/. [Último acceso: 04 11 2020]
24. T. A. J. C. P. M. a. S. N. G. G. R. Kwon, «Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping,» de *Resilience Week (RWS)*, Salt Lake City, 2020
25. MITRE ATT&CKÒ: Design and Philosophy, «MITRE,» [En línea]. Available: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf. [Último acceso: 04 11 2020]
26. MITRE, «Enterprise Matrix,» [En línea]. Available: https://attack.mitre.org/matrices/enterprise/. [Último acceso: 04 11 2020]
27. MITRE, «About Shield's structure and terminology,» [En línea]. Available: https://shield.mitre.org/resources/getting-started. [Último acceso: 04 11 2020]
28. MITRE, «Active Defense Matrix,» [En línea]. Available: https://shield.mitre.org/matrix/. [Último acceso: 04 11 2020]
29. A. de Melo e Silva, J. J. Costa Gondim, R. de Oliveira Albuquerque y L. J. GarcÃa Villalba, «A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence,» *Future Internet,* 2020
30. C. S.,. A. M.,. a. R. B. Clemens Sauerwein, «Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives,» de *Internationalen Tagung Wirtschaftsinformatik*, St. Gallen, Switzerland, 2017
31. 10.1145/2994539.2994542, «MISP – The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform,» *Workshop on Information Sharing and Collaborative Security,* 2016.
32. MISP, «MISP – Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing,» [En línea]. Available: https://www.misp-project.org/features.html. [Último acceso: 08 11 2020]

33. TrapX, «TrapX,» [En línea]. Available: https://trapx.com. [Último acceso: 07 11 2020]
34. Attivo Networks, «ThreatDefend® Detection & Response Platform,» [En línea]. Available: https://attivonetworks.com/product/deception-technology/. [Último acceso: 07 11 2020]
35. Fortinet, «FortiDeceptor,» [En línea]. Available: https://www.fortinet.com/products/fortideceptor. [Último acceso: 07 11 2020]
36. 2. D. B. I. Report, «Enterprise Verizon,» [En línea]. Available: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf. [Último acceso: 07 11 2020]
37. B.J.R.E. Sanjeev Kumar, «Multi Platform Honeypot for Generation of Cyber Threat Intelligence,» de *9th International Conference on Advanced Computing (IACC)*, 2017
38. Telekom Security, «Introduction into T-Pot: A Multi-Honeypot Platform,» 2015. [En línea]. Available: http://github.security.telekom.com/2015/03/honeypot-tpot-concept.html. [Último acceso: 07 11 2020]
39. elastic, «¿Qué es el ELK Stack?,» [En línea]. Available: https://www.elastic.co/es/what-is/elk-stack. [Último acceso: 07 11 2020]
40. spiderfoot, «Spiderfoot,» [En línea]. Available: https://www.spiderfoot.net. [Último acceso: 07 11 2020]
41. Crown Copyright 2016, «Cyberchef,» [En línea]. Available: https://gchq.github.io/CyberChef/. [Último acceso: 07 11 2020]
42. Suricata, «Suricata,» [En línea]. Available: https://suricata-ids.org. [Último acceso: 07 11 2020]