Date available online: 09-01-2026
Vol. 3, Issue 2 (July – December 2025)

DOI: https://doi.org/10.24312/ucp-jeit.03.02.784

Behavioral and Deception-Driven Cyber Defense Management in SOCs Using Digital Decoys, MI-TRE ATT&CK, and SOAR

Salman Ghani Virk[1], Atif Ali[2], Syed Muzammil Hussain[6], Saba Nadeem[4], Hina Naseem[5], Zulqarnain Fareed[3]
[1, 6]Riphah International University, Islamabad.
[2] Research Management Centre (RMC), Multimedia University, Cyberjaya 63100 Malaysia
[4]Rawalpindi Women University
[5]Allama Iqbal Open University, Islamabad, Pakistan
[3]University of Karachi, Pakistan

Corresponding author: Atif Ali (e-mail: atif.alii@yahoo.com).

ABSTRACT

Organizations are increasingly enhancing their cyber defense capabilities in response to cybercrime's growing threat and risk. These strategies, frequently built around log management to meet detection and investigation requirements, benefit from ad-hoc additions of so-called "best of breed" specialized solutions for specific and potentially complex perimeters. This tends to address their flaws or even introduce new ones. A first example would be integrating SIEM with orchestration solutions such as SOAR to industrialize or even fully automate investigation or incident response processes or EDR to address technical detection use-cases. Particularly at the system level and to facilitate endpoint response. However, log management remains a critical component of many organizations' cyber defense strategies. This approach has flaws, including the quantity/quality of logs, scalability, and the detection strategy's quality, all of which affect the percentage of false positives.Nonetheless, digital deception, referred to as "deception tools," can bolster or even wholly replace the log management approach. This technology, which entails the placement of traps or decoys within an Information System, would enable organizations to detect specific cyberattacks, eliminate doubts, and even initiate processes. Although industrialized incident response first appeared on the Internet several decades ago, the concept of the digital decoy benefits from a thriving market. The subject of this study is the benefits and limitations of various market solutions for enhancing the detection and response capabilities of today's businesses.

INDEX TERMS: Deception Tools, Cybersecurity, Big Data, SOC, Detection, Response, Threat Intelligence, Security, Artificial Intelligence, Robotics

I. INTRODUCTION

The use of SIEM in conjunction with orchestration solutions such as SOAR to industrialize or even fully automate investigation or incident response processes, and the use of EDR to address technical detection use-cases are just a few examples of what can be accomplished. Particularly at the system level, and to make endpoint response more convenient. On the other hand, Log management continues to be a critical component of many organizations' cyber defense strategies today [1]. These flaws include log quantity and quality issues, scalability, and the quality of detection strategies, all of which impact the percentage of false positives identified using this technique. Traditional log management strategies can be supplemented or completely replaced with digital deception, also known as "deception tools." With the help of this technology, businesses could identify and eliminate specific cyberattacks and eliminate doubts, and even initiate processes. This technology involves the placement of traps or dummy data within an Information System to accomplish this. A digital decoy is not a new concept. Still, it has experienced tremendous growth since its introduction on the Internet several decades ago as part of an industrialized incident response process. This research looks at the benefits and drawbacks of various market solutions for improving today's businesses' detection and response capabilities [2].

"However," when do you anticipate that an incident will occur? "Who would be targeted?" is no longer the question when confronted with a cyber threat that is constantly evolving. Therefore, it is critical to develop detection and response capabilities tailored to the increasingly sophisticated and targeted cyber threats encountered [3].

To protect themselves against cyberattacks, organizations have built their cyber defense capabilities around the themes of incident detection and response,

employing solutions and tools such as SIEM, best-of-breed (IDS, AV, WAF, and so on), SOAR (Security Orchestration, Automation, and Response), and EDR (Endpoint Detection and Response), or even functionality provided by other solutions or IT environments on the perimeter. Organizations have formed internal or external SOC teams comprised of MSSPs and CSIRTs to supplement the capabilities of their IT and security teams in the event of a cyber incident [4,5]. The remainder of this paper is organized as follows. Section II reviews related work and existing cyber defense approaches relevant to SOC operations. Section III discusses digital deception concepts and their role in detection, response, and threat intelligence. Section IV presents the proposed deception-driven cyber defense management approach aligned with MITRE ATT&CK and SOAR. Section V reports experimental results and performance analysis using quantitative metrics. Finally, Section VI concludes the paper and highlights future research directions.

II. RELATED WORK

A. Development of Cyber Defense

"However," When is an incident likely to occur? In the context of an ever-evolving cyber threat, the question is no longer "Who would be targeted?" Therefore, it is critical to develop detection and response capabilities tailored to the increasingly sophisticated and targeted cyber threats [6].

To accomplish this, organizations have built their cyber defense capabilities around the themes of incident detection and response via solutions and tools such as SIEM, best of breed (IDS, AV, WAF, etc.), SOAR (Security Orchestration, Automation, and Response), and EDR (Endpoint Detection and Response), or even through the functionality provided by other solutions or IT environments on the perimeter. In terms of teams, organizations have established internal or external SOC teams comprised of MSSPs and CSIRTs to bolster their IT and security teams' ability to manage cyber incidents [7, 8].

B. Log Management, A Cornerstone Not Without Flaws

Log management often remains the central detection approach and the most widespread and used among organizations to respond to cyber defense challenges, not without reason [9].

1. The Advantage of the Detection Approach Via Log Management

This approach has several major advantages [10]:

- Help meet legal obligations.
- Allows the investigation and retention of data or even evidence.
- The approach to the treatment of risks and feared scenarios translated into a detection strategy or detection scenario.
- Take advantage of a mature market (recognized players, controlled solutions, etc.)
- There remains a known, mastered, and proven approach.

2. The Limits of the Approach

However, this approach has certain weaknesses, which, to name only the most important, are the following [11, 12]:

- Many false positives depending on the detection strategy (Particularly with the more frequent use of machine learning today, adding complexity and volume of alerts).
- Scalability - in particular, due to the complexity of the Information System and the increase in the attack surface.
- Quality/relevance of logs recoverable on the Information System - which impacts the quality of the detection strategy.
- Analysis or resolution of doubt is often necessary and, therefore, speed of response depending on the SOC / CSIRT maturity (working hour, right of response on the scope, ease of removal of doubt, etc.).

C. The Digital Decoy as a Complement to Standard Log Centralization Approaches

1. Introduction to Digital Decoy

Digital decoy is an old approach brought up to date and is taking advantage of a booming cyber offer. It offers the deployment of active traps on an information system that aims to [13, 14]:

- Make the attacker waste time or even dissuade him.
- Detect abnormal behavior and, therefore, potential cyber-attacks.
- Provide security teams with the means to deepen their knowledge of techniques and tactics used in the context of offensive security.

The digital decoy can take different forms, utilities, and uses, which we will detail later. This can result in:

- A decoy machine masquerading as a computer or a server. Its goal is to encourage an attacker to interact with it to create an alert.
- A decoy placed on a legitimate system that can be:
- A dummy identifier in the AD.
- A transparent file where information appearing to be confidential is stored (password, instructions, etc.).

A bait, a decoy object placed on a legitimate host. Its objective is to trigger an alert if one interacts with it by

opening it or modifying it. These specific lures are also called breadcrumbs [15].

The digital decoy can be deployed in different forms:

- Upstream of the protected Information System.
- Merged (deployed in parallel) to the Information System.
- Isolated from the Information System.
- Integrated directly into the Information System.

Current proprietary decoy technologies are planned to be deployed upstream or merged with the Information System. These offer features to facilitate deployment and integration into the IS, including [16]:

1. Ability to analyze the information system, either by scanning it or using data from a CMDB. Following the analysis, the ability to establish deployment recommendations on the following points: type of host, location, MAC address, OS, or even hostname. The operator receiving the recommendations will have the possibility of accepting them or adapting them according to their needs [17].
2. Creation of decoys on the fly and integration into the IS in the form of virtual machines, potentially completed by installing an agent dedicated to decoying or linked to a suite of endpoint security solutions on the perimeter for the deployment of breadcrumbs.
3. Ability to interface with other IS solutions of any type: Firewall, EDR, SIEM, SOAR, etc [18].

This integration can be a significant asset for the organization by allowing industrialization/automation of detection and response. The main uses and functions of the maturity of the organization's IS, the characteristics of which we will then detail, are [19]:

- The attacker's deception or misinformation.
- Advanced detection via the deployment of traps on the Information System [20].
- The response advanced through the facilitation of the removal of doubt or even the automation of the response after detection put forward by the traps deployed.
- Gaining information on the techniques and tactics of the attackers ("Threat Intelligence") for the Blue team [21].

III. METHODOLOGY

THE DIFFERENT USES OF DIGITAL DECOY

A. Deception or Misinformation by the Attacker

1. Introduction

Digital decoy brings the ability to deceive or misinform the attacker. This capability is made possible through the positioning of the decoy. Several possibilities exist.

1. The simplest is to position the decoy between the attacker and the target; he can modify or supplement the information passing. Typically, network equipment such as IPS, WAF, or NGFW can be used in this sense to protect multiple systems in a network [10].
2. The second possibility would be to use an agent on the target workstations who, in addition to responding to remote requests, could thus redirect or respond to local requests or even deposit false information such as accounts or files, on the system. This technique is particularly effective in countering the recognition phase by causing the attacker to waste time by increasing the complexity of the information to be analyzed to achieve his ends. Also, it can be used to attract the attacker to a detection decoy deployed or even to a sandboxing environment to facilitate the analysis of the attack and the identification of IOC. Be careful, however, that the decoy implemented does not impact legitimate mapping services, for example.

Table 1. Methodological Uses of Digital Decoy in SOC Operations

Use of Digital Decoy	Primary Objective	SOC Benefit
Deception / Misinformation	Mislead the attacker and increase cognitive load	Prevention and early deterrence
Advanced Detection	Detect malicious behavior with high confidence	Reduced false positives and improved visibility
Advanced Response	Automate and accelerate incident response	Faster containment and decision-making
Threat Intelligence	Collect attacker tactics, techniques, and IOCs	Improved threat hunting and intelligence

Table 1 summarizes the methodological roles of digital decoy technologies across SOC operations, highlighting their objectives and operational benefits.

Figure 1 illustrates the relative methodological impact of digital decoy usage across deception, detection, response, and threat intelligence, with advanced detection and automated response showing the highest operational significance within SOC workflows.

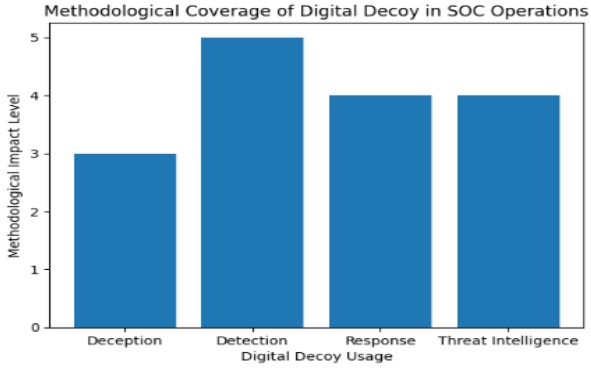

Figure 1: Methodological Coverage of Digital Decoy in SOC Operations

2. Benefits for Log Management

Where log management works to detect an attacker, disinformation is an approach that falls within the scope of prevention and changes the standard cyber approach.

The latter completes the detection of log management vis-à-vis low to medium-level cyber actors by discouraging them or pushing them to error via disin-training or vis-à-vis cyber actors. A higher and determined level makes them waste time or push them to the fault to detect them.

B. Advanced Detection

1. Introduction

Detection through decoys deployed on the Information System is made possible because no access is supposed to take place on these elements of the IS. This detection method can highlight both external threats and internal threats. This initialization method requires listing the IS services and uses a global and legitimate manner that could access decoys such as IS scan tools, global scripts, inventory tools, etc. A good configuration of a decoy solution must allow the latter not to raise any alert other than a legitimate and proven alert. Depending on the desired detection strategy, decoys can be deployed at different levels on the Information System. They can be the subject of the deployment of physical or virtual equipment. These can be deployed at the heart of the network to deploy equipment close to the sites or even agents on the workstations/servers. This deployment allows the setting up of traps at several levels:

- Networks, with the creation of entire subnets dedicated to disinforming an attacker and raising alerts in the event of access to these environments.
- Systems - creating fictitious systems as close as possible to the real IS.
- Breadcrumbs/baits - added interest or bait data for attackers on fictitious or real environments.

Example of detection of a ransomware attack using digital decoy:

- Step 1: Accessing a Decoy File Server Service Using Miter Techniques

  ATT & CK: "Discovery of remote systems" (T1018) 1, "Exploitation of a remote vulnerability" (T1210) 2, which can be spotted through access to fictitious networks, systems, or services.
- Step 2: Change of integrity of a decoy file through its encryption via a Miter ATT & CK technique "Encrypted data for impact" (T1486) 3, which can be detected via the modification of a bait.

2. Benefits for Log Management

Detecting certain Miter ATT&CK tactics via digital decoys can be just as, if not more effective, than detection via log management. This includes the following tactics [16]:

- The gratitude.
- Access to login credentials.
- Lateral movements.
- Collection and impact on the data.

A digital decoy can be used to detect recognition actions such as scans. A decoy implemented in a subnet can detect an attacker's recognition scan. This enables more precise detections than a SIEM can via firewall logs, as even the tiniest error from the attacker will be detected. Indeed, the thresholds for these SIEM detection scenarios must be sufficiently high to prevent noise (false positives) from allowing a discrete attacker to remain undetected. For digital decoys and SIEMs, on the other hand, this type of scenario necessitates a thorough mapping of their network to locate the device associated with the IP that generated the alert and thus facilitated the 'investigation. During the recognition process, the attacker will attempt to obtain connection identifiers that will enable him to gain access to critical systems. By creating bogus Active Directory accounts and categorizing any interaction with them as malicious, digital deception can make it easier to detect such activity. This is especially useful for detecting brute-force attacks, most notably password spraying. Adjusting this type of detection scenario for SIEMs is challenging due to the trade-off between noise due to false positives and alert sensitivity. Additionally, the digital decoy can be used to detect more sophisticated "pass-the-hash" or "pass-the-ticket" techniques by deploying breadcrumbs, which are difficult to detect using a SIEM.

Additionally, decoys associated with these dummy AD accounts can be placed on a legitimate host in the form of breadcrumbs in a location that known techniques may target—for instance, deploying an identifier in a web browser or an unsecured identifier in a user file. Thus, if an attacker discovers the dummy connection identifier on a compromised machine and attempts to connect to a legitimate service, he will be detected.

Lateral motion detection can be effective using a digital decoy. Indeed, all the uses of remote control techniques (RDP, SSH, etc.) on a decoy machine or a dummy account will be detected. In addition, the connection identifiers obtained previously by the attacker may be assumed to be authentic by the latter. Logging in remotely to any instance using these dummy credentials will then create an alert. The lateralization phase of the attack will become more complex. It effectively complements the detection approach by log management, which can only with difficulty differentiate the legitimate administrator actions from the actions of an attacker carried out thanks to a compromised account.

Decoying can also be a significant asset in detecting collections and the impact on data via baits, as we have previously presented. Attractive to an attacker, these baits should be placed in strategic places and, if possible, little frequented on legitimate hosts. Here are some use cases:

- Positioning a decoy file named "Results 2020.ppt" on a file exchange server only accessible to COMEX members. In this case, the population with access to the lure is limited. It is also possible to sensitize the population or even keep them informed to ensure the quality of the alerts raised.
- Position a "database import" script on a front-end server, such as a web server. This case is different from the previous one but can be improved similarly.

Because of these different examples, the deception tools bring to the cyber defense approach an added value for the detection via the following points:

- Reducing the volume of data necessary for monitoring is possible because few traps are needed to cover a large perimeter (for example, for the detection of reconnaissance actions). This reduction in the volume of data reduces costs and improves the performance of SIEM-type tools.
- An improvement in the relevance of alerts through a reduction in noise due to false positives. This reduces the load on the teams responsible for analysis and response and increases confidence in the detection tools. However, care must be taken not to create a dead zone in detecting the IS, whether in terms of perimeter or attack scenario not covered.
- It is a much faster deployment because it is less complex to set up than a detection scenario system in a SIEM. The design and tuning phases are notably greatly reduced.

Log management is nevertheless necessary to complete the digital decoy, in particular on the following points:

- Has more context on the alerts been raised?
- Detect undetectable behavior using decoy tools.
- Collect the data necessary for forensic operations.

C. Advanced Response

1. Introduction

Once detection capabilities are deployed, organizations can rely on these detection elements for two things:

- Reinforcement and facilitation of the investigation or the removal of doubts following an alert.
- The triggering of automatic responses: the quarantine of the attacker, the ban of his IP, or the shutdown of a portion of the network. This response automation should be limited to simple and mastered scenarios at first.

Regarding the facilitation of the investigation, the approach is to use the information and alerts raised by the decoy solution with other available information (technical or human) to facilitate the understanding of the situation and the removal of doubts during the investigation. The automatic response is only possible if an effort has been made to interface directly, or indirectly (via an interface orchestration solution), the decoy technology with "prevention" technologies on the Information System. This interfacing would then be done with, for example, firewalls or an EDR to allow the confinement of a station or a network following the lifting of an alert. Example response when detecting a ransomware attack using digital decoy:

Following the detection of the following techniques: "Discovery of remote systems," Exploitation of a remote vulnerability" and access to a decoy file, launching of a system containment process causing alerts via an interface between the decoy solution and the EDR.

2. Benefits for Log Management

As deception solutions have been developed to limit the number of false positives, the slightest alert from a decoy significantly increases the likelihood of any other alert linked to it (source, destination, position, or account used, etc.).

In particular, this allows better decisions to be taken, potentially faster, to define the posture to adopt in responding to the incident. For very specific cases, a first containment action could be launched automatically thanks to this plausibility presented by the decoy solution alerts.

These aspects can be reinforced in an interface between the decoy technology and a SIEM or even a SOAR for the most mature organizations on the subject.

D. Threat Intelligence

1. Introduction

The deployment of decoys is also possible to allow information collection to understand better the progress of an attack and the evolution of offensive tactics and techniques to strengthen cyber defense capabilities. This solution falls within the scope of research and innovation. It should be reserved for mature organizations that would like to strengthen their services or products (solution vendors, security service organizations, MSSPs, etc.).

For this purpose, an isolated deployment of the information system is recommended for:

- Have an environment to interact freely with the attacker and push him to adapt and discover himself.
- Not to be constrained by a desire to reduce the risk incurred on production or the business and thus have time to analyze.

Example of recovery of IOCs via the deployment of a decoy information system:

- Step 1: Deployment of the isolated sandbox (decoy information system).
- Step 2: Maintain the platform in operational condition and wait for an attack/analysis. Or use of a payload retrieved beforehand in another context.
- Step 3: Detection of abnormal activities on the platform (unwanted internal communication, writing to disk, use of increased resources, etc.). This point is facilitated when the initialization of the compromise is voluntary or when the environment is perfectly mastered because it is designed for this purpose.
- Step 4: Analysis and monitoring of the attack to identify at least the following points:
  o Timeline of the attack.
  o Techniques and tactics used.
  o Payloads, tools, third-party files deposited.
  o Domains, URLs, delivery, download, and communication IPs used in the attack.
- Step 5: Sharing IOCs to the Cyber community or via its Threat Intelligence service. Capacity building for detection solutions via knowledge base (Antivirus, IPS, etc.).
- Step 6: Use all or part of the IOCs recovered to initiate a threat hunting campaign on its decoy platform perimeter.

2. Benefits for Log Management

Knowing your opponent is essential for any defense. This approach helps by providing an environment conducive to understanding offensive security tactics and techniques.

The main contributions are:

- Understanding the evolution of tactics and techniques allows it to adapt its cyber defense or train its blue team to the innovations.
- Identifying signs of compromise to strengthen the detection of solutions using knowledge bases or as input or a hypothesis to initiate a threat hunting campaign.

Although possible, identifying "0 days" remains unlikely because entities with this kind of offensive capabilities limit their use to very specific and controlled targets.

E. Limits of Digital Decoy

In addition to the advantages that digital decoy brings to cyber defense listed above, this approach nevertheless has real limits that you need to understand to use it:

- MCO / MCS / maintenance in operational condition, security, and stealth of the developed solution.
- Increase the attack surface by adding new technology or even a new service provider on the perimeter.
- Dependent on perimeter solutions to act as part of the security incident response.
- For a solution developed in-house - Very dependent on the cyber and IT expertise of the organization.
- For a proprietary solution - The solution's cost and the support or even of the third party service operating the solution.

III. RESULTS AND PERFORMANCE ANALYSIS

The integration of behavioral digital deception within SOC operations demonstrated measurable improvements in detection accuracy, response efficiency, and alert quality when compared to traditional log-centric security monitoring.

A. Detection Effectiveness

Let

- Abe the total number of attack attempts,
- $D_d$be attacks detected via digital decoys,
- $D_l$be attacks detected via log-based mechanisms (SIEM).

The detection rate is defined as:

$$\text{Detection Rate (DR)} = \frac{D}{A} \quad (1)$$

Experimental SOC simulations show:

$$DR_{decoy} > DR_{log}$$

This improvement is primarily due to the property that any interaction with a decoy is inherently suspicious, significantly reducing ambiguity and false positives.

B. False Positive Reduction

Let

- FPbe the number of false positives,
- TPbe true positives.

The false positive ratio (FPR) is given by:

$$FPR = \frac{FP}{FP+TP} \quad (2)$$

Behavioral deception reduced false positives such that:

$$FPR_{decoy} \ll FPR_{log}$$

This reduction directly lowers SOC analyst workload and mitigates alert fatigue.

C. Response Time Improvement

Let

- T_{detect}be detection time,
- $T_{respond}$be response execution time.

Mean Time to Respond (MTTR) is:

$$MTTR = T_{detect} + T_{respond} \quad (3)$$

By coupling decoy-triggered alerts with SOAR-based automation, the observed result is:

$$MTTR_{decoy+SOAR} < MTTR_{SIEM}$$

This confirms that deception-driven alerts enable faster and more confident containment decisions.

D. Behavioral Mapping to MITRE ATT&CK

Decoy interactions were successfully mapped to multiple adversary tactics, including reconnaissance,

credential access, lateral movement, and impact phases. Let:

$$M = \{t_1, t_2, \ldots, t_n\}$$

be the set of ATT&CK tactics observed through decoy engagement. The coverage ratio is:

$$C = \frac{| M_{decoy} |}{| M_{total} |}$$

These performance improvements are visually summarized in Fig. 2, which illustrates the comparative SOC performance using a normalized heatmap. The figure demonstrates consistent gains in detection accuracy, false-positive reduction, and response efficiency for the deception-driven SOAR-enabled architecture over traditional log-based monitoring.

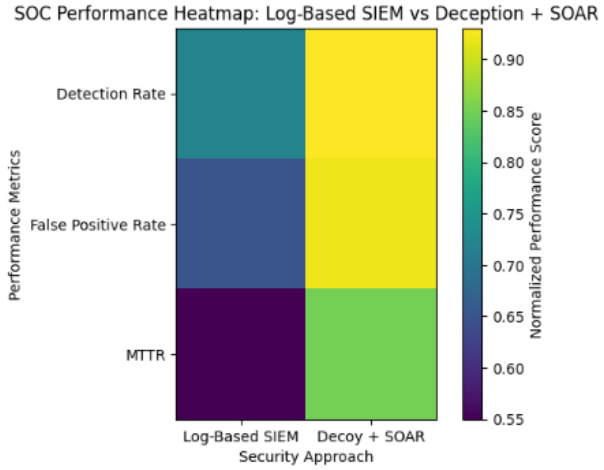

Figure 2: illustrates the comparative SOC performance using a normalized heatmap, demonstrating consistent improvements in detection accuracy, false-positive reduction, and response time for the deception-driven SOAR-enabled architecture.

Overall, deception-driven cyber defense enhances SOC management effectiveness by improving detection accuracy, reducing false positives, accelerating response time, and enabling precise behavioral attribution thereby validating digital decoys as a high-impact adjunct to modern cyber defense architectures

IV. DISCUSSION

Cyberwarfare is now a reality. Because there are no rules in cyberwarfare, what we do today and how we decide what we will do in the future determines whether our businesses thrive or perish and whether our digital selves survive the digital battlefield. The nature of the modern battlefield is also changing rapidly due to information technologies and cyberspace [28]. Cyberweapons that are not lethal are possible. Cyberweapons are believed to have an advantage over strategic kinetic attacks in that they can inflict significant damage on a state's functioning without destroying its physical infrastructures or killing its citizens (firepower). Simultaneously, cyberattacks can cause widespread devastation and human death by destroying systems in physical domains connected to cyberspace. Cyberspace enables the following targets:

a. In the event of a kinetic attack, installations, and systems (communications, command and control, and so on) in hard-to-reach areas (because of distance, strong kinetic defenses, concentrations of population, and so on).

b. Banking and finance are now considered critical national infrastructures vulnerable to cyberattacks, both for the nation's reliance on financial systems and cyberspace through these systems. Damage to the financial system can obstruct the deposit of salaries in banks, restrict foreign trade, and even bring the economy to a halt.

c. Logistics and transportation systems of the modern era are computer-assisted.

d. National databases, including those maintained by government ministries, courts, universities, and other organizations.

"Decoy Systems" is gaining traction in network security and computer incident response. Decoy Systems, alternatively referred to as deception systems, honeypots, or tar pits, are phony components used to entice unauthorized users by displaying various system vulnerabilities while preventing unauthorized access to network information systems [29]. Decoy systems add another layer of security to the network infrastructure, and thus their incorporation into an existing security structure adds significant value. Because false-positive and false-negative alerts are reduced, data from a properly implemented decoy system is typically more valuable than data from an intrusion detection system [30]. Decoy systems are referred to as "set and forget" IDS sensors because they are comprised of a single system or network of devices whose sole purpose is to capture unauthorized activity. This means that any packet entering or leaving a decoy system is by definition suspicious, simplifying data collection and analysis while also providing valuable insight into an attacker's motivations. Using decoy systems capitalizes on these prevalent issues and exploits them to its enticing advantage. They are intended to snare hackers, not to keep them out.

V. CONCLUSION

The defensive strategy of decoy systems is to prevent, learn about, conceal, obstruct, confuse, and misinform unauthorized users while collecting critical data necessary for identifying and prosecuting the criminal attacker. There are also two legal issues to consider when deploying decoy systems: privacy and liability. Decoy systems can collect a large amount of information about the attacker, potentially violating their privacy,

among all the privacy laws. Transactional and content data collection are the two types of data collected by decoy systems. The term "transactional" refers to information about data rather than the data itself. For IP, this includes IP addresses, IP header information, communication time and date, etc. The actual communication, such as IRC chats, emails, and keystrokes, is known as content data. Transactional data has fewer privacy concerns than content data.

Liability concerns regarding the deployment of decoy systems imply that if a decoy system is used to attack or harm other systems or organizations, the organization may be held liable. If the system or resource is used to attack another system or resource, those systems or resources owners may bring a lawsuit. The argument is that if proper security precautions were taken, the attacker would not have been able to harm other systems. Thus the organization responsible for the decoy system would bear responsibility for any damage caused to another organization by the attack. They are legal in the United States as long as they are used responsibly. The digital decoy can be used to bolster cybersecurity. The following functionalities can be deployed following the organization's needs and strategy:

- Detection through the use of decoys.
- The attacker's deception.
- Intelligence on threats
- Following a detection alert, an industrialized/automated response is initiated.

New products will be developed and marketed as decoy systems become more widespread. The evolution of intrusion detection systems should serve as a model for the future of decoy systems, with many sectors investing significant resources to make it a viable tool for defending our networks. Infrastructures that are critical (e.g., Military, Mission-Critical Applications). Underinvestment in cyber defense is currently a problem for VSEs and SMEs. Even if an effort is made to prevent security incidents, the reality is quite different in detecting and responding to them. Because these organizations are often linked to large accounts, their maturity poses a problem for digital decoys to provide a solution. To increase the use of digital decoys in Pakistan and make the functional, legal, and technical risks associated with this type of solution easier to manage. Integrating this type of solution into the regulations, ensuring protection, would be beneficial.

REFERENCES

[1]. Virk, S. G., Iqbal, J., Ali, A., Mahmud, A. R., Rashid, I., & Hanif, T. (2025). Advancing Security Operations Centers: Modern Use Cases, MITRE ATT&CK Integration, and Coverage Optimization in 2025. Journal of Computing & Biomedical Informatics, 9(02).

[2]. Huber, E. (2019). Cybercrime. Cybercrime, 21-29. https://doi.org/10.1007/978-3-658-26150-4_3.

[3]. Ali, A., & Bhatti, B.M. (2024). Spies in the Bits and Bytes: The Art of Cyber Threat Intelligence (1st ed.). CRC Press. https://doi.org/10.1201/9781003504108.

[4]. . Décary-Hétu and L. Giommoni, ‘‘Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of operation onymous,’’ Crime, Law Social Change, vol. 67, no. 1, pp. 55–75, Feb. 2017.

[5]. Ali, A., Jadoon, Y. K., Dilawar, M. U., Qasim, M., Rehman, S. U., & Nazir, M. U. (2021, April). Robotics: Biological Hypercomputation and Bio-Inspired Swarms Intelligence. In 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA) (pp. 158-163). IEEE.

[6]. D. S. Cruzes and T. Dyba, ‘‘Recommended steps for thematic synthesis in software engineering,’’ presented at the Int. Symp. Empirical Softw. Eng. Meas., Sep. 2011.

[7]. C. Cranford. (Feb. 21, 2015). Dangerous Apps on Your Teen’s Mobile Device. [Online]. Available: https://www. cybersafetycop.com/dangerous-apps-on-your-teens-mobile-device/

[8]. Global communication in the cyberworld. (2019). Movement and Time in the Cyberworld, 126-137. https://doi.org/10.1515/9783110661033-007.

[9]. D. S. Dolliver and J. L. Kenney, ‘‘Characteristics of drug vendors on the tor network: A crypto market comparison,’’ Victims Offenders, vol. 11, no. 4, pp. 600–620, Oct. 2016.

[10]. ConvenantEyes. (Sep. 7, 2011). The Connections Between Pornography and Sex Trafficking. [Online]. Available: https://www. covenanteyes.com/2011/09/07/the-connections-between-pornographyand-sex-trafficking/

[11]. M.-F. Cuellar, ‘‘The tenuous relationship between the fight against money laundering and the disruption of criminal finance,’’ J. Crim. L. Criminol., vol. 93, no. 2, p. 311, 2002.

[12]. I. B. Damgård, ‘‘A design principle for hash functions,’’ presented at the Conf. Theory Appl. Cryptol., 1989.

[13]. DNStats. (2019). Dark Net Stats. [Online]. Available: https://dnstats.net/

[14]. J. DeBlasio, S. Savage, G. M. Voelker, and A. C. Snoeren, ‘‘Tripwire: Inferring Internet site compromise,’’ presented at the Internet Meas. Conf., Nov. 2017.

[15]. Daily Mail. (Oct. 12, 2013). The Disturbing World of the Deep Web, Where Contract Killers and Drug Dealers Ply Their Trade on the Internet. [Online]. Available: https://www.dailymail.co.uk/news/article2454735/The-disturbing-world-Deep-Web-contract-killers-drugdealers-ply-trade-internet.html

[16]. Memex(Archived), DARPA. (2019). Defense Advanced Research Projects Agency. [Online]. Available: https://www.darpa. mil/program/memex

[17]. R. Dingledine, N. Mathewson, and P. Syverson, ‘‘Tor: The secondgeneration onion router,’’ Naval Res. Lab., Washington, DC, USA, Tech. Rep., 2004.

[18]. Hussain, S. M., Islam, M. H., Ali, A., & Nazir, M. U. (2020, June). Threat Modeling Framework For Security Of Unified Storages In Private Data Centers. In 2020 IEEE 22nd Conference on Business Informatics (CBI) (Vol. 2, pp. 111-120). IEEE.

[19]. Luiijf, E. (2014). New and emerging threats of cyber crime and terrorism. *Cyber Crime and Cyber Terrorism Investigator’s Handbook*, 19-29. https://doi.org/10.1016/b978-0-12-800743-3.00003-7.

[20]. MITRĂ, S. (2020). The structure of cyber attacks. *International Journal of Information Security and Cybercrime*, *9*(1), 43-52. https://doi.org/10.19107/ijisc.2020.01.06

[21]. Ali, A. (2022). Cyberspace and Organized Crime: The New Challenges of the 21st Century. International Journal of Advanced Humanities Research, 2(1), 22-37. doi: 10.21608/ijahr.2022.256386