informatics

MDPI

Article

Advancing Cybersecurity with Honeypots and Deception Strategies

Zlatan Morić *, Vedran Dakić * and Damir Regvart

Department of System Engineering and Cybersecurity, Algebra University, 10000 Zagreb, Croatia; damir.regvart@algebra.hr

* Correspondence: zlatan.moric@algebra.hr (Z.M.); vedran.dakic@algebra.hr (V.D.)

Abstract: Cybersecurity threats are becoming more intricate, requiring preemptive actions to safeguard digital assets. This paper examines the function of honeypots as critical instruments for threat detection, analysis, and mitigation. A novel methodology for comparative analysis of honeypots is presented, offering a systematic framework to assess their efficacy. Seven honeypot solutions, namely Dionaea, Cowrie, Honeyd, Kippo, Amun, Glastopf, and Thug, are analyzed, encompassing various categories, including SSH and HTTP honeypots. The solutions are assessed via simulated network attacks and comparative analyses based on established criteria, including detection range, reliability, scalability, and data integrity. Dionaea and Cowrie exhibited remarkable versatility and precision, whereas Honeyd revealed scalability benefits despite encountering data quality issues. The research emphasizes the smooth incorporation of honeypots with current security protocols, including firewalls and incident response strategies, while offering comprehensive insights into attackers' tactics, techniques, and procedures (TTPs). Emerging trends are examined, such as incorporating machine learning for adaptive detection and creating cloud-based honeypots. Recommendations for optimizing honeypot deployment include strategic placement, comprehensive monitoring, and ongoing updates. This research provides a detailed framework for selecting and implementing honeypots customized to organizational requirements.

Keywords: honeypots; deception technology; cybersecurity; threat detection; deception

Academic Editor: Olga Kurasova

Received: 22 November 2024
Revised: 27 January 2025
Accepted: 29 January 2025
Published: 31 January 2025

Citation: Morić, Z.; Dakić, V.; Regvart, D. Advancing Cybersecurity with Honeypots and Deception Strategies. *Informatics* **2025**, *12*, 14. https://doi.org/10.3390/informatics12010014

1. Introduction

In an age of escalating cyber threats, safeguarding networks and systems has emerged as a global challenge for organizations. As cybersecurity teams pursue novel techniques to identify and mitigate unauthorized access, honeypots have surfaced as a formidable asset in the repertoire of defensive strategies. A honeypot is a decoy system or application intended to lure and examine malicious activities, functioning as a trap for attackers while providing valuable intelligence on emerging threats. Honeypots simulate vulnerable targets, allowing IT teams to identify system vulnerabilities, analyze attacker behavior, and strengthen network defenses against threats such as phishing, Distributed Denial of Service (DDoS) attacks, and other cyber intrusions. This paper investigates the essential function of honeypots in cybersecurity, analyzing their capabilities, constraints, and practical uses. This study thoroughly analyzes diverse honeypot solutions, evaluating their detection efficacy, scalability, and reliability to offer in-depth insights into their significance in contemporary cybersecurity strategies. The study is based on a

comprehensive examination of current literature and a comparative analysis of widely used honeypot tools, resulting in recommendations for optimal practices and implementation strategies.

Honeypots significantly reduce the risk to critical systems by diverting attackers and capturing valuable intelligence. However, careful consideration is required for their design and operation to ensure effectiveness. Misleading signals can be inadvertently generated by poorly configured or inadequately monitored honeypots, as real systems may not be accurately emulated or complete, and correct data about attacker behavior may not be provided. Incorrect threat assessments can be led to by such issues, or, in some cases, the honeypot can be detected by attackers, allowing their strategies to be altered to evade detection. To mitigate these risks, the design of honeypots must incorporate realism, with legitimate systems being closely mimicked while isolation from production environments is maintained. Continuous monitoring and analysis of honeypot activity are essential to ensure the data collected is actionable and accurate. The integrity and utility of honeypots as part of an organization's cybersecurity strategy are maintained through these critical considerations.

This paper has two scientific contributions:

- It introduces a new methodology for honeypot comparative analysis;
- It systematically assesses honeypots as a defensive measure and analyzes their effectiveness, scalability, and operational demands.

This paper is organized as follows: In the next three sections, we cover the related research, research goals, and types of honeypots. Then, we introduce our methodology for honeypot comparison and comparison criteria before comparing the solutions used. The last three sections are dedicated to best practices/recommendations, discussing future research directions and conclusions.

2. Related Works

Given the evolving threat landscape, innovative methods are needed to prepare students for cybersecurity education. Honeypots are an effective educational tool, enabling engagement with simulated cyberattacks to understand attacker tactics, tools, and techniques. Students can develop a robust understanding of honeypot technologies and their applications in cybersecurity through practical exercises. It has been proven that incorporating honeypots into the curriculum significantly enhances students' knowledge and technical skills, improving their ability to address real-world security challenges [1]. This information is the foundation for strengthening robust cybersecurity measures and improving organizations' security posture.

The primary advantage of honeypots is that they provide immediate and correct insights into attackers' activities. For instance, it has been proven that Digital Twin honeypots enhance threat intelligence by adapting to diverse network scenarios and detecting sophisticated, persistent threats [2]. Furthermore, honeypots provide capabilities for identifying and mitigating real-time fingerprinting attacks, which are essential for preventing attackers from recognizing and bypassing these deceptive systems [3]. Such capabilities maintain honeypots' effectiveness and integrity as defensive instruments.

Honeypots are considered pivotal in educational contexts, significantly enhancing students' understanding and knowledge of cybersecurity. Research has proven that comprehension of cybersecurity principles and technical ability improve with participation in honeypot activities. Students engage with honeypots to gain practical experience in finding and analyzing cyber threats, a competency considered valuable for future roles as cybersecurity professionals [4].

Additionally, recent studies have highlighted the integration of honeypots with other security technologies. Incorporating honeypots with machine learning algorithms and blockchain frameworks has been associated with developing sophisticated systems capable of predicting and mitigating cyber threats more efficiently [5]. The ongoing evolution of honeypot technology and its potential to revolutionize cybersecurity methodologies is reflected in these advancements. Furthermore, the ability of honeypots to generate valuable insights into the TTPs utilized by attackers has been acknowledged. Honeypots are strategically deployed in various environments, including those vulnerable to phishing, scamming, and account hijacking, allowing for the collection of extensive cyberattack data [6]. Accurate defense strategies and the effectiveness of threat detection mechanisms are formulated and improved using such data.

Advancements have been made in centralized honeypot management systems, in addition to attacker profiling through geographically distributed honeypots. For instance, the SoftSwitch framework uses software-defined switching to enhance honeypot deployment in VLAN networks. This approach enables secure, centralized control over honeypots while ensuring improved scalability and reduced overhead. Centralized frameworks are particularly effective in managing large-scale networks and maintaining consistency in honeypot configurations across diverse environments [7].

Adaptive honeypots, designed to alter their behavior based on attackers' actions, have exhibited notable effectiveness. These systems employ reinforcement learning to adjust responses dynamically, allowing for more effective attacker engagement while minimizing the likelihood of detection. For instance, honeypots have been enhanced through reinforcement learning to adapt to detection tries by malware, thereby improving their ability to sustain engagement and collect valuable intelligence [8]. Moreover, it has been proven that systems based on reinforcement learning are effective in addressing sophisticated attacks, such as runtime Denial Of Service (DoS), through the dynamic optimization of defense strategies [9]. The concept is further illustrated by adaptive systems such as ASGuard, which engage attackers through reinforcement learning while being protected from deep compromises. ASGuard optimizes honeypot functionality by defining reward functions that balance attack data collection with system safety, showing the effectiveness of reinforcement learning in mitigating cyber threats [10].

Researching honeypots within the environments of the Internet of Things (IoT) has yielded encouraging results. Sophisticated and diverse honeypot systems have been developed by researchers, with complexity being evolved in response to the observed behavior of attackers. The unique challenges and risks associated with IoT devices are understood to be invaluable through these systems [11]. Moreover, the enhancement of deployment and management in software-defined networks (SDNs) is achieved effectively by integrating honeypots. This approach helps centralized control while the incidence of false positives is reduced, improving the overall operational efficiency and effectiveness of honeypot systems [12].

In industrial cybersecurity, honeypots have been used to emulate industrial control systems (ICSs) and detect cyberattacks. These systems can replicate various protocols and devices, enabling a deeper understanding of attacker strategies and enhancing critical infrastructure security [13]. Additionally, honeypots play a vital role in detecting and analyzing malware. Malicious activities are captured and scrutinized, helping researchers understand and mitigate emerging threats, including zero-day vulnerabilities and advanced cyber threats [14]. Insights into honeypot deployment have been gathered from real-world implementations. For example, a deployment at IIT Kanpur [15] provided valuable lessons on the configuration, management, and effectiveness of honeypot systems in detecting and analyzing cyber threats. This experience proved the importance of adaptive

deployment strategies, highlighting the potential of honeypots in academic and enterprise environments.

Advancements in honeypot technology are propelling progress in cybersecurity. Researchers using large language models (LLMs) have designed more realistic and dynamic honeypots. These systems engage human attackers more effectively, providing comprehensive insights into their tactics and methodologies. Moreover, the deployment of honeypots in wireless networks has been examined, resulting in notable benefits. Wi-Fi honeypots detect and respond to unauthorized access rapidly, enhancing security for residential and corporate networks [16].

Honeypot placement and deployment strategies have also been improved using game-theoretic approaches. Interactions between defenders and attackers have been simulated, enhancing honeypot systems' efficiency and reducing associated risks [17].

The integration of blockchain technology with honeypots has shown significant potential. Blockchain-based frameworks have enhanced the security and reliability of honeypot systems by generating immutable records of identified threats and developing more robust defense mechanisms [18].

Virtual honeypots have been used to design and simulate intrusion detection systems. These systems analyze extensive datasets and find cybersecurity vulnerabilities, establishing them as critical assets for network security [19]. Researchers have also assessed the influence of various honeypot configurations on attacker behavior using cognitive models. Studying decisions made by adversaries in different scenarios can improve the effectiveness of honeypot systems [20].

Academic and research institutions have increasingly adopted honeypots for collecting cyberattack data and enhancing security education. These deployments offer critical insights into attack patterns, and significant contributions are made to prepare future cybersecurity professionals. Honeypots are regarded as indispensable tools in cybersecurity. The ability to replicate real-world systems, collect detailed attack data, and integrate advanced technologies is a cornerstone of modern cybersecurity strategies. The effectiveness of honeypot technology is expected to be enhanced through continued research and development, ensuring enduring relevance as a critical component in addressing cyber threats [21]. Advancements in honeypot technology are being made to address emerging cyber threats through innovative approaches. Recent large-scale analyses of honeypot data have highlighted persistent exploitation of legacy vulnerabilities and a growing focus on IoT-specific threats. For instance, billions of global connections captured by honeypots were examined in a study, revealing that modern attack landscapes are dominated by IoT-based malware and keylogging campaigns, which underscores the need for adaptive defense mechanisms [22].

Honeypot classifications were thoroughly analyzed, highlighting their benefits and drawbacks, including ethical issues and evasion tactics employed by advanced attackers [23]. The efficacy of honeypots in intercepting hacker communications and collecting intelligence was also emphasized, underscoring their significance in proactive security strategies [24].

Cyber deception encompasses strategies such as obscuring genuine network assets and disseminating misleading information to bewilder opponents. In 2018, the progression of cyber deception was researched, highlighting its transition from static systems such as conventional honeypots to dynamic, adaptive techniques that use computational game theory and machine learning [25]. Another team of researchers has shown that dynamic honeypots employing machine learning may adjust to adversary behavior in real time, enhancing detection rates [26].

Enhancing deception using game theory game-theoretic methodologies has proved crucial in perfecting deception tactics. A group of researchers proposed a honeypot

allocation model that optimizes placement through partially observable Markov decision processes, facilitating enhanced deception in uncertain environments [27]. Researchers enhanced this approach by integrating network mobility into tactical network defenses, highlighting adaptive techniques to mitigate adversary actions [28].

The configuration and placement of honeypots profoundly influence their efficacy. A paper from 2021 evaluated the effectiveness of bidirectional deception, wherein authentic systems are camouflaged as honeypots in conjunction with conventional honeypots to generate ambiguity for adversaries [28]. The results demonstrate that these techniques enhance attackers' uncertainty and bolster defensive results. Researchers also noted that deception networks, such as honeynets, enhance these advantages by incorporating many honeypots, confusing adversaries' capacity to distinguish between decoys and genuine systems [29].

In summary, honeypots are recognized as indispensable tools in modern cybersecurity, providing a multifaceted approach to understanding and combating cyber threats. Decoy systems functioned to attract and engage malicious actors, allowing for the collection of critical intelligence on attack patterns, techniques, and tools. Diverse domains are spanned by their applications, including education, industrial cybersecurity, the environments of the Internet of Things, and wireless networks. The instrumental role of honeypots in improving threat detection, analysis of malware, and enhancement of cybersecurity training has been established. The capabilities of advanced technologies, such as machine learning, blockchain, and game-theoretic methods, have been further enhanced through integration. At the same time, continued effectiveness in an evolving threat landscape is ensured by strategic deployment and adaptability. As advancements in honeypot technology are made, a vital role in cybersecurity strategies is expected to be supported to mitigate emerging threats and reinforce organizational security postures.

3. Research Goal and Methods

This research comprehensively examines the significance of honeypots in cybersecurity, with theoretical and practical contributions to the field. The advantages and limitations of various honeypot categories are named through analysis, and a detailed comparative analysis of prominent solutions is presented. Multiple dimensions are investigated in the research, including interaction levels (low and high), supported operating systems, services provided, and capabilities for attack detection and analysis. The implementation and comparative evaluation of specific honeypot solutions are directed as the primary focus, alongside the refinement of best practices and the formulation of strategic recommendations. The insights derived from this analysis are intended to enhance existing methodologies and practices in cybersecurity and address emerging challenges and threats.

The study makes a scientific contribution by systematically assessing honeypots as a defensive measure and analyzing their effectiveness, scalability, and operational demands. The evaluation is grounded in empirical data and rigorous methodological frameworks, ensuring that the reliability and applicability of the findings are supported. The gap between theory and practice is aimed to be bridged by equipping cybersecurity experts with actionable insights that enhance comprehension and application of honeypot technology. A robust framework for selecting and implementing honeypot solutions is provided, aiding organizations in finding optimal solutions tailored to unique security requirements.

Furthermore, this research offers a practical contribution through detailed comparative analysis, which serves as a decision-making tool for organizations looking to deploy honeypot systems. A comprehensive summary of the evaluated solutions is provided, allowing stakeholders to discern the strengths and limitations of each approach.

Additionally, this study proposes practical recommendations for effective honeypot deployment, encompassing aspects such as configuration, maintenance, and integration into broader security infrastructures. These contributions to formulating innovative defense strategies will strengthen organizations' cybersecurity posture.

A comprehensive and systematic approach was employed to fully understand the significance of honeypots in cybersecurity and evaluate the currently available solutions. This research included a thorough literature review, including scholarly books, peer-reviewed articles, and other relevant sources. A combination of research methods was employed to ensure the robustness and validity of the findings.

A systematic collection of the pertinent literature and credible web sources was undertaken to establish a foundational understanding of the subject and to provide context for the analysis presented in this paper. The Inductive Approach was employed to analyze specific case studies, allowing for the extraction of novel insights concerning the role and practical significance of honeypots in contemporary cybersecurity frameworks. Deductive techniques were employed in the study to examine the broader aspects of honeypot technology, with conclusions derived from established theoretical frameworks and validated assumptions. Fundamental components were deconstructed from intricate concepts, evaluations, and findings. The approach was used to analyze individual honeypot solutions based on predefined criteria, including scalability, detection capabilities, and ease of deployment. The similarities and differences among various honeypot solutions were systematically assessed. This method helped the identification of shared characteristics and distinguishing features, resulting in a nuanced understanding of each solution's relative strengths and weaknesses.

The critical role of deception strategies in real-time cybersecurity response is recognized, as attackers are misled, and actionable threat intelligence is gathered. These strategies create realistic decoy systems, data, or environments that mimic legitimate assets. When attackers engage with deceptive elements, monitoring, analysis, and enhancement of an organization's threat detection and response capabilities are conducted. The functioning in real-time response is described.

- Early Detection: Deception systems identify malicious activity during the reconnaissance or initial attack phases by attracting attackers to decoy systems;
- Attack Containment: Once interaction with the honeypot or decoy system occurs, activities are confined to a controlled environment, preventing access to production systems;
- Dynamic Engagement: Advanced deception techniques, including adaptive honeypots, are designed to modify their behavior in response to the attacker's actions, thereby prolonging engagement and facilitating the gathering of more detailed intelligence;
- Automated alerts are enabled through real-time logging and integration with Security Information and Event Management (SIEM) systems. That allows security teams to receive immediate notifications and facilitates a faster incident response.

The advantages of actionable threat intelligence are as follows:

- Improved Defense Posture: Data collected from deception systems provides insights into attacker TTPs, allowing organizations to update their defenses proactively;
- Real-Time Insights: Actionable threat intelligence is derived from honeypots, allowing for the identification of active threats, including zero-day vulnerabilities and emerging attack trends, which provides immediate context for security teams;
- Threat Actor Profiling: Profiles of attackers are built based on their interactions through deception strategies, which can be shared with broader threat intelligence networks to enhance collective cybersecurity;

- Resource Optimization: Identifying false positives and focusing on real threats reduces incident response teams' workloads, enabling effective resource allocation through actionable intelligence.

The research's focus on proactive cybersecurity measures strengthens the integration of deception strategies into the proposed work. The research goals are aligned with these strategies, which enhance threat detection, enable faster responses, and contribute to long-term improvements in organizational security.

This structured methodology ensured a balanced evaluation, and the critical factors influencing the selection and implementation of honeypot systems were also highlighted. The following section provides an overview of honeypot types, setting the stage for an in-depth evaluation and comparison of specific solutions. This multifaceted approach contributes theoretical and practical insights, reinforcing scientific value and relevance to cybersecurity.

4. Honeypot Types

Honeypots are critical tools for acquiring reliable insights into the evolving landscape of cyber threats. They provide detailed intelligence on attack vectors, exploits, and malware, aiding in identifying and mitigating emerging risks. Attackers continually refine unauthorized access methods, while honeypots detect and document these developments, which play a pivotal role in a cybersecurity strategy. Additionally, honeypots identify and capture insider threats, allowing for a broader spectrum of potential vulnerabilities to be addressed.

Various honeypot categories are present, each designed to address specific threat types. The classification and interpretation of honeypots are determined by the nature of the threat being mitigated, with each category contributing uniquely to an effective and comprehensive cybersecurity strategy. For example, fictitious email addresses are deployed in concealed locations accessible only through automated email address collectors, referred to as email traps or spam traps. Since these addresses serve no other purpose, any messages received are unequivocally classified as spam. Email traps automatically block messages with similar content, blocking the originating IP address.

Malware honeypots are focused on analyzing malicious software that targets organizational systems, while similarities to spam honeypots are noted. The behavior of bots and other automated threats is effectively studied using honeypots, environments specifically designed to attract such entities. Such systems significantly contribute to detecting and preventing unwanted automated traffic and bot-based intrusions.

Honeypots are recognized for their exceptional efficiency in identifying known and novel threats and improving threat detection capabilities. They establish an environment that lures attackers, allowing honeypots to observe and analyze adversarial behavior. This approach provides valuable insights into attackers' tactics and techniques to penetrate systems. Examining attacks within a controlled environment allows a deeper understanding of adversary strategies, enhancing the organization's ability to prepare for and respond to potential cyber threats.

A typical honeypot deployment strategy involves strategically placing these systems within a network. That is intended to maximize attacker visibility while minimizing risks to actual systems. As illustrated in Figure 1, the positioning and configuration significantly optimize honeypot effectiveness [30].

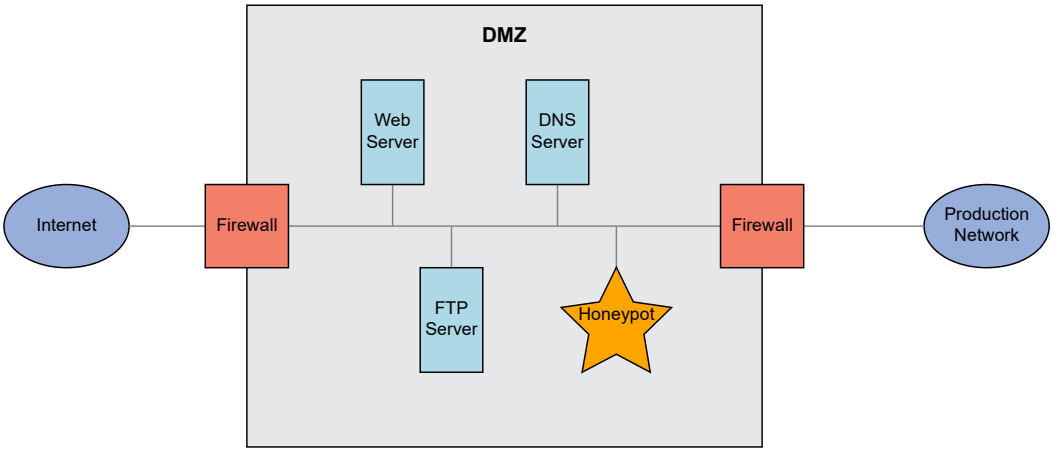

Figure 1. Deployment of a honeypot in a DMZ network configuration.

Honeypots deployed for research purposes are regarded as invaluable tools in cybersecurity due to the data on malicious activities that are collected and analyzed. These systems facilitate an in-depth examination of attacker methodologies, with critical insights being provided for the enhancement of forensic analysis capabilities. Research honeypots were deployed within the university infrastructure to monitor and analyze attack patterns targeting educational networks. Additionally, honeypots were deployed by a government agency as part of a pilot project to study advanced persistent threats (APTs) targeting critical infrastructure. Similarly, honeypots were integrated into the network of a private company as a pilot initiative to assess their effectiveness in detecting unauthorized access attempts and phishing activities. Despite the complexities involved in their setup, maintenance, and data collection processes, research honeypots significantly contribute to understanding and mitigating sophisticated threats. Attacker behaviors in these controlled environments were observed, leading to the identification of emerging vulnerabilities and the provision of actionable insights to improve security measures.

Additionally, preventing future attacks is supported by identifying vulnerabilities and strengthening security protocols. In contrast, production honeypots are designed to be integrated seamlessly into existing security systems, thereby enhancing the ability of an organization to detect and respond to attacks in real time. Honeypots are employed to strengthen system protection and effectively reduce risk levels. Compared to research honeypots, a more limited functionality is presented while an easier development and implementation process is offered. It has been noted that production honeypots particularly effectively detect various attack techniques. However, less detailed insights into the perpetrators are offered compared to research honeypots.

Honeypots are typically categorized based on their level of interaction, which determines the extent of engagement with attackers. This classification provides a practical framework for understanding functionality and deployment. There are three primary types of honeypots: high-interaction honeypots, low-interaction honeypots, and hybrid honeypots, focusing on their unique characteristics and applications in cybersecurity.

4.1. High-Interaction Honeypots

High-interaction honeypots are characterized as advanced honeypots designed to engage intruders by replicating fully operational services and systems. In contrast to low-interaction counterparts, actual environments are simulated by these honeypots, which include complete operating systems, network services, and applications. A realistic and enticing target for attackers is provided, enabling detailed observation and analysis of

behaviors, tools, and tactics. High-interaction honeypots are considered particularly valuable for in-depth research and forensic investigations.

High-interaction honeypots offer unique advantages in cybersecurity, as they provide detailed intelligence on attackers' methodologies and behaviors. These systems simulate fully operational environments, allowing attackers to interact extensively with the honeypot. As a result, valuable data are captured across several dimensions of intelligence by high-interaction honeypots.

- Tactics, Techniques, and Procedures (TTPs): Attackers engage with realistic systems, allowing granular data to be collected on their methods, including reconnaissance techniques, malware deployment strategies, lateral movement attempts, and command-and-control (C2) operations. This intelligence is utilized to develop targeted detection and response measures;
- Zero-Day Vulnerabilities and Exploits: High-interaction honeypots detect and study zero-day exploits in a controlled environment, as attackers may use unpatched or unknown vulnerabilities during interactions. Security teams prepare patches or mitigation strategies before widespread exploitation occurs;
- Behavioral Profiling: Attacker profiles are created based on interactions facilitated by high-interaction honeypots. Behavioral data, including the sequence of commands, preferred tools, and decision-making patterns, are utilized to identify specific threat actor groups or to predict future attacks;
- Malware samples are often captured directly from attackers by high-interaction honeypots. The functionality of these samples can be understood, payloads can be uncovered, and Indicators of Compromise (IOCs) can be identified, which can subsequently be shared across threat intelligence platforms;
- These honeypots effectively detect, and study advanced persistent threats (APTs) characterized by prolonged and sophisticated attack campaigns. The multi-stage processes these actors employ are observed through the in-depth interaction capabilities allowed for security analysts;
- Data from high-interaction honeypots inform incident response insights, providing real-time information regarding attack timelines, potential entry points, and attackers' objectives. Response efforts are accelerated, and this intelligence enhances organizational resilience.

The capabilities of high-interaction honeypots are leveraged to play a pivotal role in cybersecurity, with unparalleled insights that extend beyond immediate threat detection to long-term strategic defense enhancements.

4.1.1. Benefits of High-Interaction Honeypots

The ability to capture comprehensive data on attacker methodologies is considered one of the primary benefits of high-interaction honeypots. Since these honeypots mimic natural systems, detailed information can be gathered about advanced and sophisticated attack strategies that low-interaction honeypots might miss. Insights into zero-day exploits, custom malware, and multi-stage attacks are included. The richness of the data collected makes these honeypots invaluable for threat intelligence, enabling a better understanding of the capabilities and intent of attackers by organizations. Furthermore, the entire lifecycle of an attack, from survey to exploitation and post-compromise activities, can be revealed by high-interaction honeypots. Comprehensive visibility enables cybersecurity professionals to identify vulnerabilities and develop more effective countermeasures.

4.1.2. Challenges and Considerations

Despite their advantages, high-interaction honeypots present significant challenges. Due to their complexity and realism, higher costs and substantial resources are necessitated for deployment and maintenance. Configuring these systems to resemble actual production environments requires careful planning and technical expertise, including maintaining up-to-date software, patching vulnerabilities, and monitoring activity without disrupting the honeypot's functionality.

Moreover, the realistic nature of high-interaction honeypots introduces potential security risks. If an attacker successfully compromises the honeypot, an attempt may be made to use it as a pivot point for infiltrating other parts of the network. The isolation of high-interaction honeypots from production systems is a critical requirement. Network segmentation, strict access controls, and comprehensive logging mechanisms must be implemented to prevent the use of the honeypot as a stepping stone for further attacks.

4.1.3. Optimal Strategies for the Deployment of High-Interaction Honeypots

Organizations must adopt several best practices to mitigate the risks associated with high-interaction honeypots:

- High-interaction honeypots will be deployed in a segregated network environment to prevent unauthorized access to critical systems. Virtualized environments or sandboxing technologies may also be utilized to contain potential breaches;
- Continuous monitoring of honeypot activity is considered essential. Advanced logging mechanisms should capture every interaction, including network traffic, system commands, and file modifications. These data must be securely stored and analyzed in real-time to detect and respond to suspicious activity;
- Although high-interaction honeypots are designed to mimic natural systems, it is recommended that specific controls be implemented to limit the attacker's ability to utilize the honeypot for malicious purposes. Outbound network connections may be restricted or heavily monitored to prevent data exfiltration;
- Regular updates and maintenance are required for high-interaction honeypots to ensure relevance and effectiveness. Security patches are applied, simulated services are updated, and configurations are refined to reflect the latest attack trends;
- High-interaction honeypots should be integrated into the organization's incident response framework. Any activity within the honeypot can trigger further investigation or proactive measures to address potential threats.

Implementing these best practices ensures the effectiveness of high-interaction honeypots as tools for threat detection and analysis while minimizing the risks posed to an organization's broader network.

4.1.4. Applications in Cybersecurity

High-interaction honeypots are utilized in research environments, where detailed attack data are captured to aid in developing new detection and prevention technologies. Critical infrastructure sectors are also employed, where understanding targeted attack methodologies is crucial for protecting sensitive assets. Furthermore, high-interaction honeypots are vital in identifying APTs and other sophisticated adversaries.

High-interaction honeypots are especially effective in deception and traceability tactics. By incorporating Runtime Application Self-Protection (RASP) technology, these systems identify sophisticated threats like SQL injection and DDoS attacks with a high detection rate while concurrently tracking attackers with notable precision. In healthcare cybersecurity, hybrid models that integrate high- and low-reactivity honeypots improve the safeguarding of sensitive data against man-in-the-middle attacks and other sophisticated

threats [31–33]. They are also essential in training and simulation environments. They can be used in advanced metering infrastructure security in IoT networks via federated learning and incentivized data sharing, safeguarding against intrusions and improving data quality [34,35].

High-interaction honeypots are recognized as powerful tools for understanding and mitigating cyber threats. However, their deployment requires careful consideration of cost, complexity, and security risks. Organizations can gain unparalleled insights into attacker behavior through adherence to best practices and effectively leveraging their capabilities, while potential vulnerabilities can be minimized.

4.2. Low-Interaction Honeypots

Low-interaction honeypots are regarded as more uncomplicated and resource-efficient than high-interaction honeypots, offering a limited level of engagement with attackers. Honeypots are designed to emulate specific services, applications, or protocols, providing a controlled environment that mimics natural systems without replicating their full functionality. Low-interaction honeypots effectively utilize basic behaviors and interactions to lure attackers, enabling valuable data to be collected by security teams while minimizing the risks associated with full system simulation.

Low-interaction honeypots are designed to simulate specific services or ports, attracting attackers while minimizing the complexity and risk of replicating a real system. The basic functionality of services such as HTTP, FTP, SSH, or SMTP is emulated by these honeypots, with an environment that appears vulnerable but lacks the operational depth of a complete system. By focusing on these limited interactions, essential attack data, such as scanning attempts, brute-force attacks, and basic exploitation methods, is captured by low-interaction honeypots. The following are some examples:

- **Service Emulation**: A low-interaction honeypot is configured to simulate an SSH service, where login attempts are responded to, and attacker credentials and command inputs are logged without actual system access being granted;
- **Port Simulation**: These honeypots often open specific ports, such as 22 (SSH) or 80 (HTTP), to attract attackers scanning for vulnerable systems. When attackers attempt to connect, the honeypot records their activities, including payload delivery attempts and scanning tools used;
- **Basic Interaction Recording**: Although these systems do not provide a complete environment for attackers to explore, critical data such as attackers' IP addresses, timestamps, and attempted attack vectors are logged.

The limited functionality of low-interaction honeypots is associated with significantly reducing the required resources for deployment and maintenance. However, it has been noted that this simplicity also reduces effectiveness in capturing detailed attacker behaviors or advanced threat methodologies. Despite these limitations, early detection of threats is facilitated, patterns in automated attacks are identified, and a first line of defense in a layered security strategy is provided.

4.2.1. Characteristics and Advantages

The ability to emulate services and protocols, such as those defined by the TCP/IP model, is recognized as one of the critical features of low-interaction honeypots. These systems simulate the behavior of vulnerable applications or network components without implementing the underlying operational complexities. The likelihood of attackers exploiting vulnerabilities in the honeypot itself is reduced by this approach, resulting in a level of safety that is inherently greater than that of high-interaction honeypots.

Low-interaction honeypots are recognized for their advantages in detecting and logging specific types of attacks, including network scans, brute-force attempts, or automated exploitations. Their simplicity is associated with quick deployment and minimal maintenance, which is ideal for organizations with limited resources or technical expertise. Furthermore, these honeypots ensure that genuine or sensitive information is not stored, mitigating the risk of critical data being compromised during an attack. The highly scalable nature of low-interaction honeypots is attributed to their minimal system requirements. Multiple instances may be deployed across a network to monitor diverse attack vectors without incurring significant hardware or software costs. The scalability is especially beneficial for organizations that build extensive early-warning systems or conduct broad threat intelligence collection.

Early-warning systems leverage low-interaction honeypots to provide proactive alerts about potential cyber threats, allowing organizations to take preventive measures before attacks escalate. These systems detect early-stage activities such as reconnaissance, scanning, and initial exploitation attempts. Multiple honeypot instances are deployed across various network segments, allowing for the monitoring of diverse attack vectors and the acquisition of a comprehensive understanding of potential threats. The primary advantage of early-warning systems is detecting malicious intent before its impact on critical systems. For example, information about attackers' tools, techniques, and tactics can be captured by honeypots deployed in external-facing environments during port scanning or brute-force attempts. Unauthorized lateral movement or insider threats may be detected by internally deployed honeypots, thereby providing additional layers of security. These systems typically achieve integration with SIEM platforms to facilitate the automation of data analysis and correlation collected by honeypots. Real-time alerts are enabled for security teams based on suspicious activities, including repeated login attempts, payload delivery, or anomalous traffic patterns. Organizations utilize insights from early-warning systems to strengthen defenses, adjust access controls, and address vulnerabilities preemptively. Proactive sensors are acted upon by early-warning systems built around honeypots, enhancing an organization's situational awareness and resilience against evolving cyber threats. An invaluable component of modern cybersecurity strategies is their scalable and cost-effective nature.

4.2.2. Limitations and Challenges

Although low-interaction honeypots are considered cost-effective and easy to manage, inevitable drawbacks are associated with their limited functionality. It is noted that only superficial aspects of actual services can be emulated by these systems, indicating that the full depth of attacker behavior cannot be captured. For instance, it is unlikely that complex attacks requiring sustained interaction or deep system exploration will be fully observed in a low-interaction honeypot environment. As a result, these honeypots exhibit less effectiveness in understanding sophisticated or targeted attack methodologies than high-interaction systems. The risk of detection by attackers is presented as another challenge. The limited capabilities of a low-interaction honeypot may be quickly identified by experienced adversaries, who may recognize it as a decoy and alter their tactics accordingly. The effectiveness of the honeypot can be reduced, and its presence within the network may be exposed.

4.2.3. Considerations for Low-Interaction Honeypot Deployment

Despite their limitations, low-interaction honeypots can achieve high effectiveness when employing strategic deployment. The best practices for implementation are included as follows:

- The low cost and minimal resource requirements of low-interaction honeypots allow for their deployment in large numbers across multiple network segments. The likelihood of capturing diverse attack attempts increases, and broader visibility into threat activity is provided;
- Focused use cases are identified for these honeypots, including detecting automated attacks, gathering essential threat intelligence, and providing an early-warning system. The deployment of low-interaction honeypots should be aligned with organizations' primary security objectives;
- It is recommended that logs generated by low-interaction honeypots be integrated with SIEM tools or other monitoring solutions. It ensures that the collected data are effectively analyzed and utilized to improve security measures;
- Although low-interaction honeypots are easily deployed, gaps in understanding advanced threats may be caused by overreliance on them. Complementation of their deployment by other security measures, such as intrusion detection systems and high-interaction honeypots, is recommended to provide a balanced defense strategy.

The strategic deployment of low-interaction honeypots is ensured to effectively contribute to threat detection and intelligence through advanced monitoring and integration with other security tools while addressing their inherent limitations.

4.2.4. Applications and Low-Interaction Honeypot Use Cases

Low-interaction honeypots are particularly effective in environments where cost-efficiency and ease of management are prioritized. In small to medium-sized businesses, the use of such measures is often observed, particularly where resources for complex cybersecurity solutions may be limited. These honeypots are commonly deployed in educational settings to provide hands-on experience in essential threat detection and response. Additionally, organizations, such as Internet service providers or enterprises managing extensive IT infrastructures, offer valuable tools for monitoring large-scale network activity. These organizations deploy multiple low-interaction honeypots to identify trends in attack behavior and allow for adjustments in defenses accordingly.

4.2.5. Comparative Insights

Compared to high-interaction honeypots, low-interaction honeypots offer a less detailed but more manageable solution for threat detection. High-interaction systems lack depth and realism; however, their simplicity reduces risks and operational overhead. High-interaction honeypots are considered more suitable for research and forensic analysis, while low-interaction honeypots are recognized for their excellence in scalable deployment and early-stage threat detection.

Low-interaction honeypots provide a practical and efficient approach to cybersecurity, allowing organizations to monitor and respond to a wide range of attacks. Although the comprehensive insights of high-interaction systems cannot be replicated, their ease of use and low cost are recognized as essential components of layered security strategies. When integrated with other tools and techniques, low-interaction honeypots significantly contribute to an organization's threat intelligence and defensive capabilities.

4.3. Hybrid Honeypots

Hybrid honeypots combine the strengths of low-interaction and high-interaction honeypots, resulting in a versatile and robust solution for cybersecurity challenges. Integrating these two approaches addresses the limitations inherent in each type, achieving a more comprehensive threat detection and analysis system. This dual-layered strategy maximizes scalability while achieving detailed insights into attacker behavior.

4.3.1. Characteristics and Benefits Are Identified and Discussed

The defining feature of hybrid honeypots is the ability to operate on multiple levels of interaction. Low-interaction honeypots are deployed as the initial layer, utilized as scalable and efficient gateways designed to attract a wide range of attacks, including automated exploits and reconnaissance scans. Upon detection of an attack, suspicious activity is redirected to a high-interaction honeypot for deeper engagement and analysis. Organizations use this layered architecture to balance resource efficiency with detailed threat intelligence. The scalability of hybrid honeypots is recognized as one of the primary advantages. Extensive networks can be covered by the low-interaction layer with minimal overhead, making it suitable for monitoring diverse attack vectors across large infrastructures. Simultaneously, the high-interaction layer provides the depth necessary for analyzing complex and targeted attacks, capturing valuable information about advanced TTPs. Additionally, it has been noted that hybrid honeypots are highly adaptable and can integrate various components and methods to address specific organizational needs. The effectiveness of hybrid systems in dynamic threat environments is ensured by this flexibility, where the strategies of attackers have continually evolved.

4.3.2. Considerations for Hybrid Honeypot Deployment

The implementation of hybrid honeypots must be carefully planned to optimize functionality and ensure seamless interaction between the two layers. Hybrid honeypots rely upon effective communication between the low- and high-interaction components. Robust configurations and protocols are required to ensure that alerts from the low-interaction layer are efficiently escalated to the high-interaction layer for further analysis. The placement of hybrid honeypots within a network is considered critical. The low-interaction layer is to be positioned to detect a wide array of external and internal threats, while the high-interaction layer is to be isolated in a secure environment to prevent the pivoting of attackers into production systems. The low-interaction layer exhibits resource efficiency, while the high-interaction layer requires significant computational power and monitoring capabilities. Organizations must allocate resources effectively to ensure the performance and reliability of the hybrid honeypot system. Automated mechanisms for transferring suspicious activity from the low-interaction layer to the high-interaction layer should be incorporated into hybrid honeypots to minimize response time and enhance efficiency. Manual intervention is reduced, and timely analysis of potential threats is ensured.

4.3.3. Applications and Hybrid Honeypot Use Cases

In enterprise environments, hybrid honeypots are regarded as particularly valuable due to the requirements for both broad coverage and detailed threat analysis. Extensive corporate networks, critical infrastructure, and cloud-based environments are well suited for monitoring. The scalability of low-interaction honeypots and the analytical depth of high-interaction systems are leveraged, allowing for effective detection and response to both generic and advanced threats by hybrid honeypots. In research and development, hybrid honeypots are employed to investigate evolving attack methodologies and assess new security measures' effectiveness. They collect detailed data on sophisticated attacks, making a valuable tool available for refining cybersecurity strategies and developing innovative defense mechanisms.

4.3.4. Insights of Comparison

The gap between low- and high-interaction systems is bridged by hybrid honeypots, with the best attributes of both being combined. Hybrids offer more detailed insights compared to low-interaction honeypots without scalability being sacrificed. In contrast to high-interaction honeypots, it has been observed that hybrids are more resource-efficient and can handle a broader range of attacks. It is suggested that hybrid honeypots are considered an optimal choice for organizations seeking comprehensive and cost-effective cybersecurity solutions.

4.3.5. Challenges and Limitations

Despite their advantages, hybrid honeypots face challenges in deployment and maintenance. Integrating low- and high-interaction components must be performed with technical expertise and careful configuration to ensure seamless operation. Additionally, the complexity of these systems can increase the likelihood of misconfigurations or false positives if not correctly managed. The effectiveness of hybrid honeypots is maintained through regular updates and monitoring. As detection mechanisms are adapted to attackers, the evolution of hybrid systems is required to ensure relevance and capability in addressing new threats.

Hybrid honeypots are recognized as powerful and versatile tools in modern cybersecurity. They combine low-interaction systems' scalability with high-interaction systems' analytical capabilities, resulting in a balanced threat detection and analysis approach. When deployed strategically, hybrid honeypots enhance an organization's ability to identify, understand, and respond to a wide range of cyber threats, thereby being regarded as an essential component of a comprehensive security strategy.

4.3.6. Full Fake Network

Entire fake networks within an organization's infrastructure, commonly referred to as decoy or deception networks, are created as a highly effective strategy for diverting attackers away from critical systems. These networks simulate a legitimate environment's architecture, services, and applications with fake data and endpoints. When attackers infiltrate the network, interaction with these decoy systems is lured, wasting time and resources while TTPs are revealed. The primary advantage of deploying fake networks is reducing risk to critical systems through the misdirection of attackers. Attractive targets that mimic sensitive systems, such as databases or internal servers, are presented by fake networks, which are acted upon as traps that delay the progression of attacks. Security teams utilize the delay to detect, monitor, and analyze the attackers' activities in real-time, allowing for rapid incident response and mitigation.

Furthermore, the cost and complexity of an attack can be increased by fake networks. Attackers must expend additional effort to determine whether real systems or decoys are being engaged. This uncertainty reduces the likelihood of successful exploitation, while the chances of attackers exposing themselves through errors or premature actions are increased. In addition to defense, these decoy networks provide valuable insights into attack trends and emerging threats. Detailed logs and interaction data are captured, allowing security teams to improve their understanding of threat actors and refine broader cybersecurity strategies. When deception technologies such as honeypots and honeytokens are combined with fake networks, a critical component of a layered defense strategy is established, ensuring that attackers are continuously misled and vital systems are safeguarded.

4.4. Summary of Honeypot Types

The categorization and analysis of honeypots into low-interaction, high-interaction, and hybrid types possess distinct advantages and limitations, reflected in their unique roles in cybersecurity. Low-interaction honeypots are characterized by simplicity, scalability, and low maintenance requirements. These systems excel at early-stage detection of threats, such as automated attacks, brute-force attempts, and basic reconnaissance activities. However, the effectiveness of understanding sophisticated attacker methodologies is restricted by their limited emulation capabilities and data quality, as deep insights into tactics, techniques, and procedures (TTPs) cannot be provided.

High-interaction honeypots are recognized for their detailed emulation of real-world systems and extensive engagement with attackers. These systems capture rich data, such as attacker behavior, malware samples, and the exploitation of zero-day vulnerabilities, and are deemed invaluable. Their use is considered particularly beneficial in research and forensic investigations, where the entire lifecycle of an attack is understood to be crucial. Despite these advantages, significant resources are required to deploy and maintain high-interaction honeypots, and scalability for large-scale threat monitoring is limited.

Hybrid honeypots bridge the gap between the two extremes. These systems combine the scalability and efficiency of low-interaction systems with the analytical depth of high-interaction honeypots. These systems utilize a layered approach, in which suspicious activities are filtered and redirected by low-interaction components to high-interaction environments for deeper analysis. This balance enables comprehensive threat detection and analysis while the resource demands and operational complexity associated with high-interaction honeypots alone are mitigated.

The strengths and weaknesses of each type are emphasized in Figure 2, focusing on detection range, emulation accuracy, data quality, scalability, extensibility, embeddability, setup complexity, and maintenance requirements. Low-interaction honeypots demonstrate high scalability and minimal resource demands, while high-interaction honeypots exhibit superior data quality and emulation realism. A balance is achieved through hybrid honeypots, which are versatile for various cybersecurity objectives.

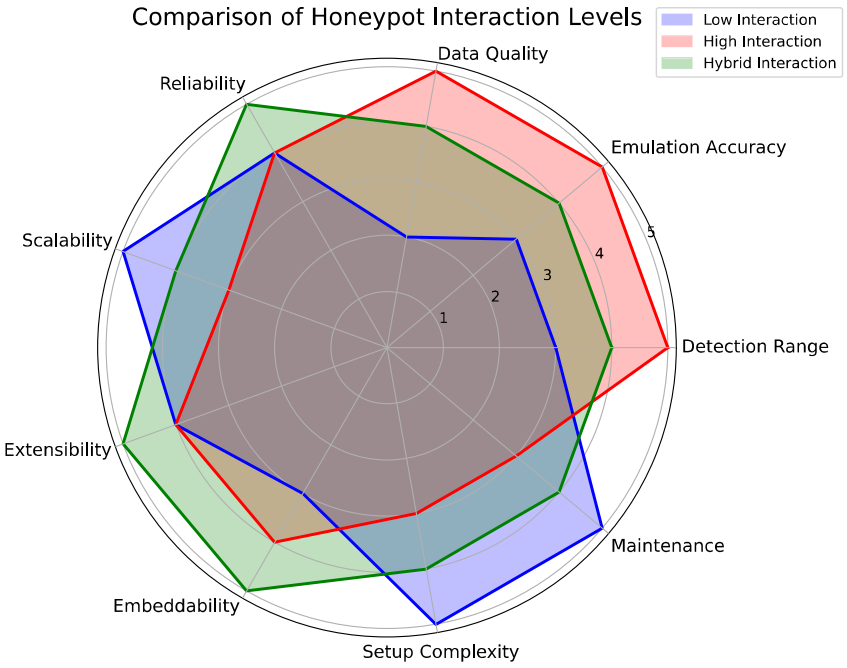

Figure 2. Honeypot-type comparative analysis.

Specific organizational needs, available resources, and targeted threat vectors should inform the choice of honeypot type. Low-interaction honeypots are suitable for organizations prioritizing large-scale deployment and early detection, whereas high-interaction honeypots are optimal for detailed forensic investigations. Hybrid honeypots are balanced and represent an effective solution for organizations requiring scalability and detailed threat intelligence. Integrating these systems within a layered cybersecurity strategy ensures a comprehensive threat detection, analysis, and mitigation approach.

5. Honeypot Solutions and Comparison Criteria

The pivotal role of honeypots in cybersecurity is recognized. This section outlines the selected honeypots and the criteria used for their evaluation, providing insights into attacker methodologies and offering assistance in threat detection and mitigation.

5.1. Honeypot Categories and Their Implementations

A selection of widely used honeypot solutions was evaluated across various categories to provide a comprehensive analysis of their capabilities and applications. The selected honeypots were categorized according to their primary use cases, which included protocols, platforms, and attack vectors. The categories and corresponding solutions are included as follows:

- SSH honeypots, Kippo, and Cowrie are designed to mimic Secure Shell (SSH) services, with attacks targeting remote access protocols being captured;
- HTTP honeypots, including Glastopf, Nodepot, and Google Hack Honeypot, emulate web services to detect attacks such as SQL injection, XSS, and other web vulnerabilities;
- WordPress honeypots, including Formidable Honeypot, Blackhole for Bad Bots, and Wordpot, monitor threats specific to WordPress installations and plugins;
- Database honeypots such as ElasticHoney, HoneyMySQL, and MongoDB are utilized. HoneyProxy replicates database services to analyze SQL injection and data exfiltration attempts;
- Email honeypots, including Honeymail, Mailoney, and SpamHAT, are designed to collect information about spam and phishing campaigns;
- IoT Honeypots: HoneyThing simulates IoT devices, enabling the detection and analysis of IoT-specific threats;
- Other honeypots, including Dionaea, Honeypot-FTP, HoneyNTP, Thug, and Canarytokens, are encompassed by a broader spectrum of use cases such as malware collection, FTP-based attacks, and phishing.

5.2. Selected Honeypots for Evaluation

A comprehensive set of honeypots was selected for this study, which addresses diverse attack vectors and represents different categories of interaction levels and functionalities. The honeypots that have been chosen include Honeyd, Dionaea, Cowrie, Amun, Glastopf, Kippo, and Thug. The need to evaluate a diverse range of tools that align with research goals of assessing honeypot effectiveness, scalability, and operational requirements is reflected in this selection.

The justification for the selection of these honeypots is presented as follows:

- Honeyd is recognized as a versatile tool capable of simulating a wide range of services using TCP or UDP protocols, thereby being deemed ideal for understanding broad-spectrum attacks;

- Dionaea is recognized for its capability to capture and analyze malware, with malicious payloads being preserved for in-depth study, thereby addressing malware-specific threats;
- Cowrie and Kippo: These SSH honeypots were selected to emphasize logging detailed attacker interactions, including commands and keystrokes, which provide insights into exploitation tactics directed at remote access systems;
- Amun is a lightweight honeypot designed to emulate multiple services, balancing versatility with ease of deployment and making it suitable for studying general attack behaviors;
- Glastopf specializes in simulating vulnerable web applications, effectively capturing web-based attacks, such as SQL injection and XSS;
- Thug is designed as a client-side honeypot that emulates web browsers and plugins and is considered critical for analyzing malicious websites and payloads that target end users.

A comprehensive evaluation of the capabilities of these honeypots in handling different types of cyber threats, ranging from brute-force attacks on SSH services to web-based vulnerabilities and malware delivery, was provided through their selection. The selection process ensured a balance between diversity in attack coverage and practical considerations, such as deployment complexity and the relevance of the attack scenarios to real-world cybersecurity challenges.

The evaluation of widely used honeypot solutions is highlighted, revealing their diverse capabilities and applications. Organizations can now select tools tailored to specific protocols, platforms, and attack vectors, enhancing their overall security posture.

5.3. Framework for Comparison

An objective and detailed evaluation was ensured by assessing the selected honeypot solutions using a set of predefined criteria. These criteria were developed based on the authors' expertise and existing literature [36]. The following aspects were considered in the evaluation framework:

- Detection Scope: This criterion evaluates the range of attack vectors and threats a honeypot can detect. A broader detection scope indicates the honeypot's versatility in identifying various attack methods, including malware propagation, exploitation attempts, and unauthorized access;
- Emulation Accuracy: This parameter measures the fidelity of the honeypot in replicating real-world systems and services. High emulation accuracy is critical for deceiving attackers and capturing realistic attack scenarios. However, this metric is less relevant for high-interaction honeypots, as genuine applications or services are often involved;
- Data Quality: The value of a honeypot is primarily influenced by the quality of the data collected. This includes the granularity of logs, contextual details about attacks, and the ability to capture unique insights into attacker behavior;
- Reliability: This criterion assesses the honeypot's ability to function consistently under varying workloads. Honeypot's reliability is ensured by its ability to withstand high volumes of attacks without failure, thereby maintaining effectiveness in dynamic environments;
- Scalability and performance must be efficiently managed by honeypots to accommodate increasing workloads and to scale across distributed networks. The capacity of a honeypot to support multiple instances and distribute processing demands across parallel computing nodes is evaluated by this metric;

- Extensibility is critical for extending and customizing a honeypot to meet specific organizational needs. This metric quantifies the ease with which new features or functionalities can be added;
- Embeddability: This criterion evaluates how much a honeypot seamlessly integrates with other cybersecurity tools or systems. Effective embeddability ensures compatibility with SIEM platforms, threat intelligence systems, and other security infrastructure;
- Setup and Usage Complexity: This section examines the technical effort required to configure and operate the honeypot. Solutions characterized by simpler setups and intuitive management interfaces are considered more accessible to organizations with limited resources;
- Requirements for Maintenance: This criterion evaluates the ongoing effort required to maintain the honeypot, including software updates, log management, and troubleshooting.

Evaluating honeypot solutions based on predefined criteria ensures a comprehensive analysis of their capabilities. The detection scope, emulation accuracy, data quality, reliability, scalability, extensibility, embeddability, setup complexity, and maintenance requirements are highlighted to guide organizations in selecting solutions aligned with their security needs and operational capacities.

5.4. Process of Analysis

A systematic analytical approach was followed in the evaluation of honeypot solutions. The performance of each solution was assessed under simulated attack scenarios against the defined criteria. Common cyberattacks, such as brute force, phishing, and malware delivery, were included in these scenarios, along with advanced techniques that targeted specific protocols or platforms. The results of this analysis provided a nuanced understanding of the strengths and limitations of each honeypot solution. For example, database honeypots such as HoneyMySQL effectively captured detailed SQL injection attempts, whereas HTTP honeypots like Glastopf demonstrated superior capabilities in simulating vulnerable web applications. SSH honeypots like Cowrie offered extensive logging capabilities, with attacker commands and interaction patterns being captured in detail.

The following sections build upon this evaluation, with detailed case studies and practical recommendations for optimizing honeypot performance and integrating it into broader cybersecurity strategies. This work aims to support organizations leveraging honeypot technology to strengthen their defenses and gain a deeper understanding of emerging cyber threats.

5.5. Practical Evaluation Methodology

A practical evaluation of the selected honeypots was conducted by simulating network attacks in a controlled testbed environment to complement the feature-based comparison. The performance in real-world scenarios was aimed to be assessed, and the capabilities were validated against predefined criteria, including detection scope, reliability, and scalability. A segmented network environment was designed for the testbed, with internal- and external-facing systems incorporated to mimic realistic organizational infrastructure, as shown in Figure 3. Isolated virtual machines were utilized to deploy honeypots, ensuring that interactions with attackers were contained within the testbed, preventing unintended impacts on production systems. Both benign user behavior and malicious activities were included in the simulated traffic to replicate diverse network conditions. Standard penetration testing tools such as Metasploit and Nmap were used to simulate these attacks for scanning, brute-forcing, and exploitation attempts. At the same time,

custom scripts were employed to simulate malware delivery and credential harvesting attacks.

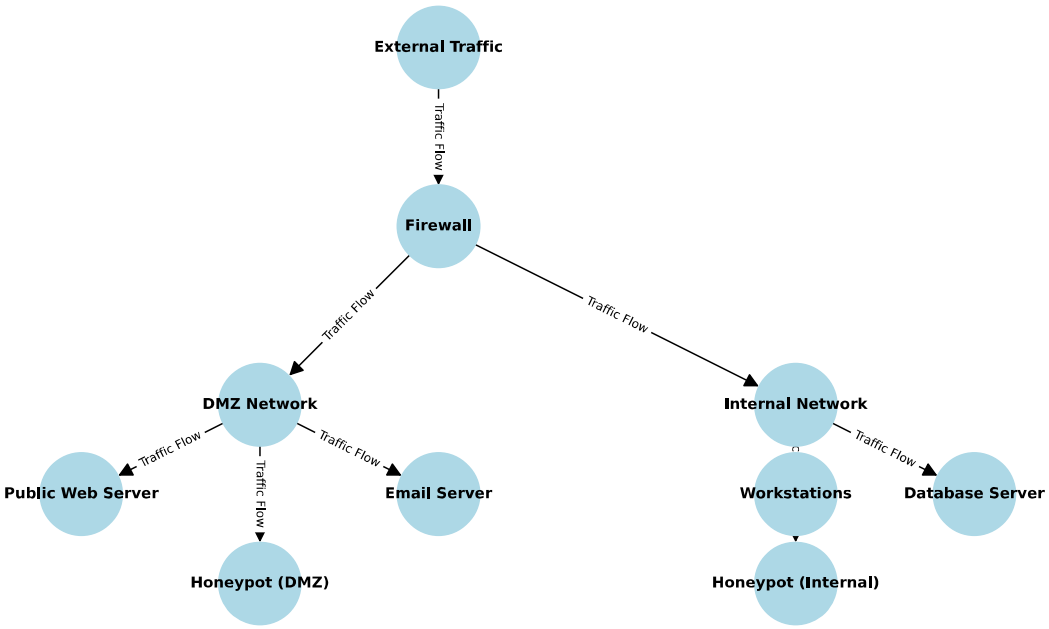

Figure 3. Testbed setup: segmented network environment.

A segmented network environment was designed for the testbed, with internal- and external-facing systems integrated to simulate realistic conditions. Honeypots were deployed on virtual machines within a controlled infrastructure, with VMware ESXi 8.0 being utilized as the virtualization platform. Ubuntu 20.04 and Windows 11 were the operating systems for the honeypots, while Kali Linux was used to simulate attacks. Network traffic was routed through a firewall to replicate real-world segmentation and security measures. Additionally, logging tools were configured on the honeypots to capture interaction logs, system events, and network traffic, ensuring comprehensive data collection was achieved during the experiments.

Three primary scenarios were evaluated: reconnaissance attacks, credential-based attacks, and payload delivery. Specific capabilities of the honeypots were tested through the design of each scenario, and intermediate results were produced that validated their performance. The ability of the honeypots to detect and log scanning activity was evaluated for reconnaissance attacks. Network scans targeting open ports and service banners were performed using tools such as Nmap and Nessus. Techniques such as TCP SYN, ACK scans, and service enumeration were employed in these scans. It was shown that basic details, such as IP addresses and scanning intervals, were logged by low-interaction honeypots, but insights into the scan techniques were lacking. In contrast, high-interaction honeypots captured detailed logs, including identifying scanning methods (e.g., Nmap SYN scan) and potential attacker intent. The capability of the honeypots to withstand and log brute-force login attempts was assessed in credential-based attacks. Iterative username and password combination testing on SSH and HTTP services was conducted using automated tools such as Hydra and custom Python scripts. Attack input, including keystrokes and authentication attempts, was captured by high-interaction honeypots, such as Cowrie, which provided valuable insights into attack strategies. Meanwhile, failed low-interaction honeypots recorded login attempts and source IP addresses, but interaction-level details were not captured. In the payload delivery scenario, the ability of the honeypots to capture and analyze malicious payloads was tested. Malware samples, including reverse shells and ransomware, were delivered through HTTP POST requests and FTP

uploads. High-interaction honeypots, such as Dionaea, were utilized to capture and preserve the delivered files, allowing for further analysis of their behavior and associated Indicators of Compromise (IOCs). Low-interaction honeypots logged file upload attempts, but the files were not retained for subsequent examination.

During the reconnaissance phase, the superiority of high-interaction honeypots was demonstrated by providing granular details regarding scanning methods and attacker behavior. In contrast, low-interaction honeypots were restricted to basic logging, including IP addresses and scanning intervals. The importance of interaction-level logging was highlighted by the results from credential-based attacks, with detailed attacker inputs, including keystrokes and authentication attempts, being significantly captured by high-interaction honeypots compared to low-interaction systems. Finally, it was underscored by the payload delivery tests that the critical role of file-capture capabilities was highlighted, with Dionaea being recognized as an effective tool for the preservation and analysis of malicious payloads, thereby enabling more profound insights into malware behavior and associated Indicators of Compromise (IOCs).

Each honeypot was configured according to standard deployment guidelines to ensure consistency and comparability across the solutions. The logs and alerts generated by the honeypots were captured and analyzed through a centralized logging system, which ensured comprehensive data collection. A variety of attack scenarios were included in the evaluation, such as port scanning, SSH brute-forcing, SQL injection, and malware delivery. Automated and manual attacks replicated a broad spectrum of threat actor behaviors. Key metrics were recorded during the evaluation, including detection time, accuracy, resource utilization, and scalability under varying attack loads. The effectiveness of honeypots in providing actionable intelligence was evaluated by analyzing logs and alerts generated during these interactions. The strengths and weaknesses of each honeypot in handling specific attack types were identified through a comparative analysis. The predefined comparison criteria aggregated and evaluated the results to draw meaningful conclusions.

The following section details the findings from this practical evaluation, and conclusions are presented based on the honeypots' performance during the simulated attack scenarios. The integration ensures alignment of the narrative with both the feature-based comparison and the practical observations, providing a holistic view of the honeypots' capabilities.

6. Comparative Evaluation and Results Analysis

This section presents an in-depth comparative evaluation and analysis of the selected honeypot solutions using the previously defined criteria. Each solution's performance, capabilities, and limitations are systematically assessed in this evaluation, aiming to highlight the strengths and weaknesses of various honeypot tools. The findings across criteria such as detection scope, emulation accuracy, data quality, reliability, and operational complexity are summarized in Table 1.

Table 1. Results of evaluation based on defined criteria.

	Honeyd	**Dionaea**	**Cowrie**	**Amun**	**Glasstopf**	**Kippo**	**Thug**
Detection range	Multifunctional	Multifunctional	Specialized	Multifunctional	Specialized	Specialized	Multifunctional
Emulation accuracy	Acceptable	All right	All right	Acceptable	Excellent	All right	All right
Quality of collected data	Weak	Excellent	All right	All right	All right	All right	All right
Readability	Excellent	Excellent	All right	Excellent	All right	Acceptable	Acceptable
Scalability	Excellent	All right	Acceptable	All right	Acceptable	Acceptable	Acceptable

Expandability	Excellent	Excellent	All right	Excellent	Excellent	Acceptable	All right
Embeddable	Acceptable	Excellent	Acceptable	All right	All right	Acceptable	All right
Setup/Use complexity	Acceptable	All right	All right	All right	All right	All right	All right
Maintenance	All right	All right	Acceptable	All right	All right	All right	All right
Detection range	Multifunctional	Multifunctional	Specialized	Multifunctional	Specialized	Specialized	Multifunctional

The evaluation criteria presented in Table 1 are used to classify the performance levels of honeypot solutions across various metrics through qualitative descriptors. The descriptors—"Weak", "Acceptable", "All right", and "Excellent"—are arranged hierarchically to indicate the relative effectiveness and reliability of each honeypot solution.

- Poor performance or significant deficiencies in a given attribute characterize a weak category. Solutions categorized as "Weak" fail to meet minimum standards, demonstrating limited utility or reliability in practical cybersecurity scenarios. For example, honeypots rated "Weak" in data quality may have incomplete or unstructured logs collected, resulting in a diminished threat analysis value;
- Honeypots categorized as "Acceptable" are observed to meet fundamental functional requirements; however, noticeable limitations are exhibited. Although deemed sufficient for minimal or constrained applications, the reliability of these solutions under complex or high-intensity use cases may be compromised. A baseline standard is reflected by this level, which is deemed suitable for less critical environments;
- The category labeled "All right" indicates moderate performance. Honeypots in this tier generally perform well in standard scenarios, with reliable functionality and the expectations of routine cybersecurity tasks being met. However, advanced capabilities or scalability required for dynamic or specialized applications may be lacking;
- The "Excellent" classification is reserved for solutions that demonstrate superior capability and performance. These honeypots excel at scalability, emulation accuracy, and data quality, resulting in consistent outcomes within complex and diverse operational environments. Solutions in this category are frequently regarded as benchmarks for the industry.

In addition to performance levels, honeypots are categorized by their functional scope as "Multifunctional" or "Specialized".

- Honeypots classified as "Multifunctional" are designed to address various attack vectors and cybersecurity needs. These versatile solutions often demonstrate the capability to simulate multiple services, protocols, or operating environments. Particular value is attributed to them in environments where diverse threats must be monitored simultaneously. A multifunctional honeypot that emulates network protocols and application layers provides comprehensive coverage, rendering it suitable for large-scale deployments or research scenarios;
- Honeypots are designated "Specialized" and focus on particular attack types, protocols, or environments. The design has been optimized for in-depth analysis of specific threats, including SSH brute-forcing and web application vulnerabilities. While multifunctional solutions may lack versatility, their narrow focus allows greater accuracy and detail in targeted scenarios, rendering them invaluable for forensic investigations or particular use cases.

Combined with performance levels, the classifications provide a nuanced framework for selecting honeypot solutions tailored to an organization's operational priorities and cybersecurity challenges. For example, a specialized honeypot exhibiting "Excellent" data quality performance is ideal for environments requiring granular threat intelligence. At

the same time, a multifunctional solution rated "All right" may be utilized for broader monitoring needs in less critical contexts.

The comparative analysis of various honeypot solutions across multiple evaluation criteria, including detection scope, emulation accuracy, data quality, reliability, scalability, extensibility, integration, and maintenance, is illustrated in Figure 4. The performance of each honeypot is represented as a distinct polygon on the radar chart, enabling a visual comparison of strengths and weaknesses. The capabilities of the honeypot are enhanced as the area covered by the polygon increases. For example, consistently high scores are demonstrated by Dionaea across all criteria, reflecting versatility and reliability, while Honeyd excels in scalability, although data quality and integration are lagged. The varying applications and trade-offs of each honeypot solution are underscored by this figure, which aids in organizations' selection of the most suitable tool for specific cybersecurity requirements. The radar chart visually captures the nuances, with a concise yet detailed representation of the evaluation results being provided.

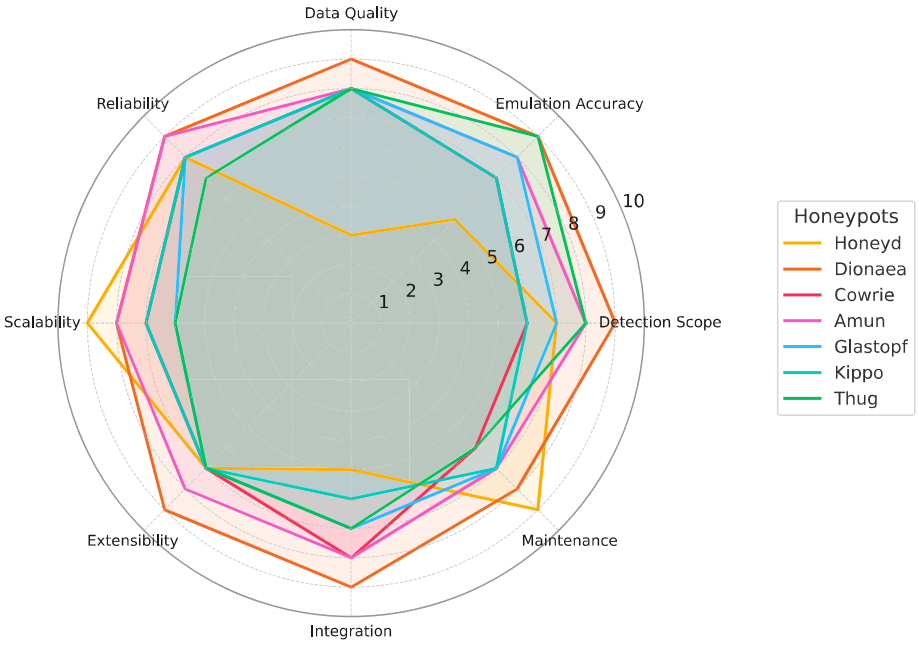

Figure 4. Combined honeypot comparative analysis.

Among the solutions evaluated, Honeyd demonstrated notable versatility through its ability to simulate any service using TCP or UDP protocols. This capability grants a broad detection range, although the quality of data collection is limited to fundamental information such as timestamps and IP addresses, which diminishes the utility for detailed analysis. Conversely, Dionaea employs modular protocols to cover a similarly extensive detection range. At the same time, exceptional data collection capabilities are distinguished, particularly in preserving malware for in-depth analysis.

The honeypot Cowrie focused on SSH services with a narrower detection range. At the same time, detailed logging of attacker actions, including commands and keystrokes, is excelled. The value of Cowrie for targeted forensic investigations is attributed to this specificity. Modular components are utilized by Amun to emulate multiple services, resulting in a balance between versatility and high emulation accuracy. Vulnerable web applications are simulated by Glasstopf, with exceptional accuracy demonstrated by executing realistic exploits by attackers. Kippo, like Cowrie, is targeted at SSH services but is limited in scope. At the same time, Thug is designed to emulate web browsers and plugins to analyze threats posed by malicious websites with high fidelity.

Honeypot solutions evaluate the critical parameter of reliability. Honeyd exhibits consistent performance under various workloads, while Dionaea stands out with stability during extended periods of high traffic. Cowrie ensures seamless integration with widely used threat intelligence platforms, providing reliability and compatibility. Similarly, robust reliability is maintained by Amun, Glasstopf, and Kippo during testing, though performance is constrained by design limitations in Glasstopf.

The ease of installation and use is found to vary significantly across the evaluated honeypots. Honeyd's straightforward setup is accessible to users with basic technical knowledge, whereas Dionaea's installation process, despite being slightly more complex, is well documented, facilitating implementation. Cowrie strikes a balance, offering intuitive configuration while requiring expertise to maximize its advanced features. Glasstopf and Kippo are considered easy to deploy, while Thug demands significant technical proficiency due to the complexities involved in its browser-based emulation setup.

Regarding scalability and performance, Honeyd exhibits high efficiency, with the capability of managing up to 100 IP addresses provided by its default configuration. Dionaea supports multiple network interfaces and IPs, enhancing its utility in large-scale deployments. Cowrie and Amun exhibit scalable designs, with configuration changes being allowed by Cowrie without system restarts. It has been determined that Glasstopf and Kippo are suitable for moderate-scale applications; however, the robustness of Honeyd and Dionaea's performance is not matched. Thug supports concurrent sessions, while moderate bandwidth usage is reflected by its resource-intensive operations.

The differentiation of these honeypot solutions is attributed to their extensibility and integration capabilities. Honeyd features a modular architecture, allowing for moderate customization, while Dionaea offers exceptional extensibility through modular components. Cowrie and Amun similarly support modular expansion, exhibiting notable integration capabilities. Glasstopf and Kippo provide satisfactory modularity, while advanced expertise is required to realize Thug's full potential, which is extensible.

The embeddability of these honeypots, or their ability to be integrated with other tools, is further influenced by their utility in comprehensive cybersecurity strategies. Honeyd lacks robust integration interfaces, while Dionaea demonstrates excellence through its SQLite database and compatibility with external systems. Cowrie's seamless integration with threat intelligence platforms is underscored by its operational utility. Amun and Glasstopf achieve moderate integration capabilities while lacking an API interface limits Kippo's applicability in integrated setups. Thug provides satisfactory embeddability, though its complexity can hinder streamlined integration.

Maintenance requirements present varying challenges. The minimal maintenance needs of Honeyd are recognized as enhancing its operational efficiency, while Dionaea maintains stability over time despite minor issues. Although reliability is associated with Cowrie, significant management effort is required due to the intricate configuration options. Amun, Glasstopf, and Thug, being categorized as low-interaction honeypots, are associated with reduced maintenance requirements; however, periodic attention is necessitated by the complexity of Thug.

A notable distinction is found between these honeypots regarding their buildability and emulation services. Multiple versions of Honeyd are accessible, but basic Python scripts are relied upon for emulation, limiting the interaction depth. In contrast, Dionaea demonstrates high proficiency in emulating services, with protocols such as SMB, HTTP, FTP, and MySQL covered with impressive realism. This capability enhances Dionaea's effectiveness in analyzing complex attack scenarios.

The specific objectives of the deployment determine the choice of a honeypot system. Low-interaction honeypots, such as BOF and specter, are characterized by simplicity in configuration and minimal risk, making them suitable for detection. High-interaction

systems, such as Mantrap and Honeynets, are designed to facilitate deeper engagement with attackers, allowing for comprehensive data collection while introducing additional risks. Hybrid approaches offer a balanced solution by combining low-interaction systems' scalability and high-interaction honeypots' analytical depth.

A honeypot strategy is required to be developed with careful consideration of several factors. The type of honeypot, network placement, operating system selection, and service configuration are considered critical decisions. Regular updates to honeypot systems are required to maintain their appeal to attackers, while robust monitoring and logging mechanisms are incorporated to capture detailed activity data. Deception techniques, such as honeytokens and lure services, further enhance the ability of the honeypot to engage attackers and gather intelligence. The selection and deployment of honeypots are affected by the availability of resources. Organizations with limited resources may prioritize low-interaction honeypots due to minimal hardware and maintenance requirements. In contrast, hybrid or high-interaction honeypots can be considered by those with moderate to high resource availability for more comprehensive threat analysis and engagement. It is ensured that the chosen honeypot strategy is aligned with the organization's budget, infrastructure, and personnel capabilities, optimizing its effectiveness without overburdening resources.

A decision tree is presented in Figure 5, designed to assist in selecting the most suitable honeypot solution based on organizational needs, resource availability, and specific cybersecurity objectives. A primary decision regarding deploying a honeypot is initiated, followed by evaluating factors such as the focus on breadth or depth of coverage, resource constraints, and the specific type of analysis required (e.g., web application, database, or general malware analysis). Honeypot solutions are recommended, including Dionaea for malware analysis and scalability, Glasstopf for web-focused threats, and Cowrie for in-depth SSH interaction at the terminal nodes. This structured approach allows organizations to make informed, data-driven decisions tailored to operational requirements and technical capacities, ensuring optimal honeypot deployment.

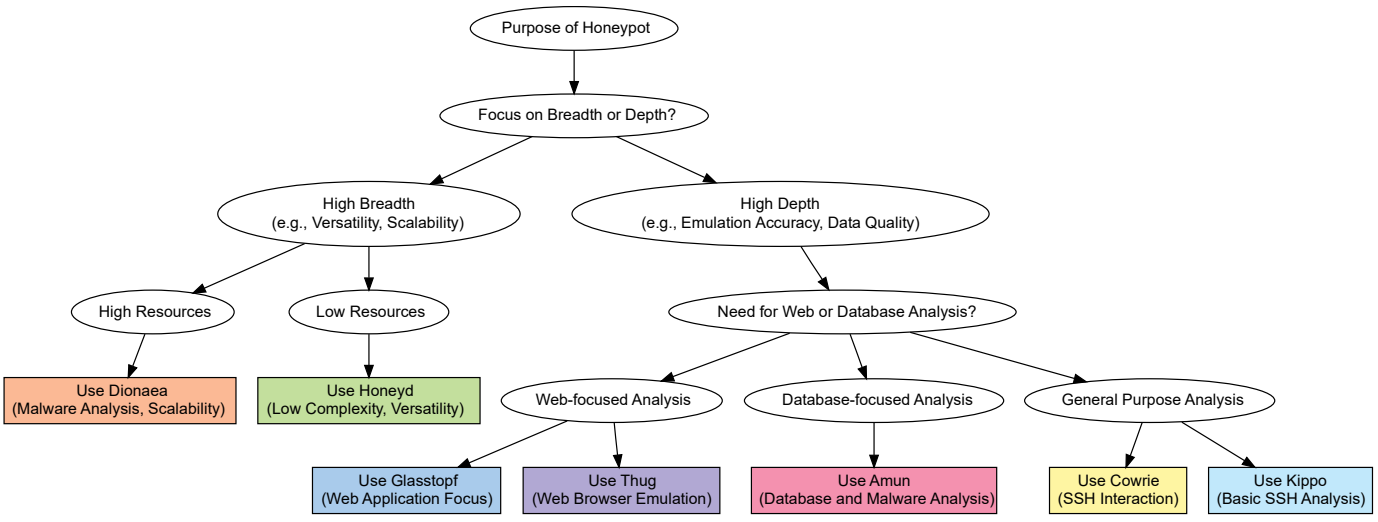

Figure 5. Honeypot selection decision tree.

The comparative evaluation of honeypot solutions reveals a diverse landscape of tools, each characterized by unique strengths and limitations. Honeypot selection is aligned with organizational objectives and integrated into broader security frameworks, allowing for effective leveraging of these systems to enhance cybersecurity posture. The importance of a strategic approach to honeypot deployment is underscored, with a balance being achieved between technical capabilities and operational goals.

7. Best Practices and Recommendations

The insights derived from this research are categorized into three key areas: implementation strategies, foundational safety assumptions coupled with mitigation techniques, and seamless integration of honeypots into existing security infrastructures. These categories provide a comprehensive framework for maximizing the efficacy of honeypot deployments while mitigating potential risks. In the following sections, a systematic evaluation of these topics will be conducted, with their significance highlighted and practical recommendations offered to enhance the utility of honeypots in diverse cybersecurity contexts.

7.1. Honeypot Implementation Strategies

An appropriate honeypot implementation strategy must be selected by carefully considering an organization's vulnerabilities, its most susceptible attack vectors, and its capacity for managing system maintenance. For example, it may be found that low-interaction honeypots are suitable for organizations primarily exposed to basic bot attacks due to their simplicity and ease of deployment. In contrast, environments that are faced with more sophisticated threats may require the utilization of high-interaction honeypots, which are characterized by the demand for advanced technical expertise and resource allocation.

Multiple methodologies are used to implement honeypot systems, which must be aligned with the organization's objectives and security posture. A clear understanding of the desired outcomes should guide the type and number of honeypots deployed. Arbitrarily deploying honeypots within a network without a thorough knowledge of the system's purpose and configuration is ineffective and does not yield actionable intelligence. Therefore, it is essential that a foundational understanding of the chosen honeypot type be acquired before installation.

Technical expertise and human resources significantly influence the successful implementation of honeypots. Robust knowledge of computer science and advanced security concepts is required for high-interaction honeypot systems, in particular. These systems aim to deceive attackers and collect detailed information about their activities while ensuring the honeypot remains unknown. The effectiveness of a poorly concealed honeypot is at risk of being lost, and reputational damage may even be incurred.

Deployment strategies for honeypots are broadly categorized into external and internal implementations. In an external deployment, a honeypot is configured within a publicly accessible environment, such as a demilitarized zone (DMZ). A DMZ is defined as a subnet utilized to isolate specific services, enabling the observation of attacker behavior and data collection on malicious activities, such as worms and network surveillance. This configuration provides insights into external threats targeting the organization, as shown in Figure 6.

Internal implementations are designed to detect and analyze threats within an organization's network. These honeypots focus on insider threats, malware propagation, or unauthorized access from within the organization. For instance, if an employee tries to compromise a system on the local network, an internal honeypot can be utilized to deceive the attacker, allowing for capturing critical data regarding their identity, tactics, and intent. This approach is considered particularly valuable for identifying and mitigating insider threats.

The honeypot implementation strategy aligns with the organization's specific needs, resources, and threat landscape, enhancing the ability to detect, analyze, and respond effectively to diverse cyber threats.

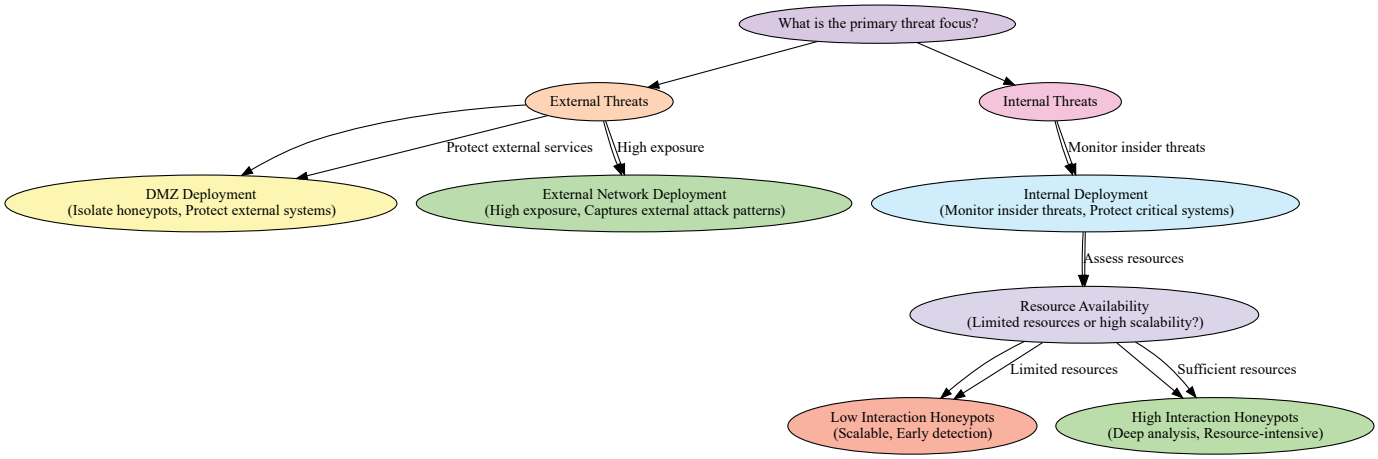

Figure 6. Decision flow for honeypot deployment strategies.

7.2. Security Assumptions and Mitigation Techniques

When honeypots are deployed as part of a multi-layered security defense strategy, organizations must carefully address several critical factors to ensure their effectiveness and safety. The considerations encompass honeypot placement, isolation, tracking, maintenance, integration with other security measures, and adherence to legal frameworks. Each aspect plays a vital role in enhancing the utility of honeypots and mitigating associated risks.

The effectiveness of a honeypot is significantly impacted by its location within the network. Honeypots that are strategically positioned are provided to potential attackers, with legitimate targets being presented, thereby increasing the likelihood of engagement. The environment where a presence is likely to be established by attackers should be considered for placement within the network. For example, the deployment of outward-facing honeypots in external infrastructures is associated with exposure to regular scans, botnet exploits, and diverse attack methods, which often increase signal noise and complicate the identification of genuine threats. Conversely, the identification of insider threats or localized infections is focused on by internal honeypots, with more targeted insights into potential vulnerabilities being offered.

Isolation is to be maintained to minimize risks, with honeypots being kept separate from critical systems within the network. Sensitive information should never be stored, as access to a honeypot could be exploited by attackers to launch lateral attacks. Configurations are designed to entrap attackers within a controlled environment, enabling the collection of valuable intelligence while access to other network resources is prevented.

Comprehensive monitoring and data collection are essential for the effectiveness of honeypots, and they must be meticulously monitored. The primary purpose is to gather intelligence on attackers' TTPs. Regularly analyzing honeypot logs is crucial for identifying malicious activity and generating actionable alerts. This analysis enhances an organization's ability to promptly respond to potential attacks and refine its overall security posture.

Regular updates and proper management ensure a honeypot's authenticity. Security personnel must ensure that honeypots are convincingly replicated as natural systems. Failure to maintain an updated and realistic honeypot diminishes its attractiveness, resulting in reduced utility. Proficient management ensures the honeypot's continued functionality in detecting and analyzing cyber threats.

7.2.1. Integration with Broader Security Measures

Honeypots should seamlessly integrate into an organization's security infrastructure, including firewalls, intrusion detection systems, incident response frameworks, and SIEM platforms. This integration amplifies the honeypot's value, as dynamic contributions to threat detection and alert generation can be made. Furthermore, honeypots offer unique opportunities to refine and enhance detection systems by leveraging real-time intelligence from attacker interactions.

The assumptions underlying honeypot deployment and associated risks are recognized as necessitating a strategic approach to ensure effectiveness. A comprehensive overview of these security assumptions, potential risks, and recommended mitigation strategies is provided in Table 2. Key considerations are highlighted, such as the necessity of ensuring realistic decoys to prevent the identification of honeypots by attackers, the implementation of strict network segmentation to isolate honeypots from production systems, and the utilization of multiple data sources to enhance the accuracy of threat intelligence. This table is a practical guide for addressing common challenges in honeypot deployment, emphasizing the importance of proactive measures to minimize risks and maximize utility in detecting and analyzing malicious activity.

Table 2. Assumptions, risks and mitigation strategies for honeypot deployment.

Security Assumption	Potential Risk	Mitigation Strategy
Honeypot isolation prevents lateral movement.	The attacker identifies the honeypot and avoids it.	Ensure realistic decoys with controlled data flow.
Deployed honeypots collect attacker TTPs.	Incomplete or misleading data may lead to poor threat modeling.	Use multiple honeypots and correlate data with external sources.
Honeypots attract only malicious traffic.	False positives from benign users accessing the honeypot.	Filter traffic through access controls or pre-screening mechanisms.
Honeypots are isolated from production systems.	Improper configuration allows attackers to pivot into production environments.	Implement strict segmentation, network controls, and logging.
Honeypots are hidden and undetectable.	Advanced attackers use fingerprinting to identify honeypots.	Regularly update honeypot signatures to match real systems.
Honeypots enable early detection of threats.	Insufficient response to collected data may lead to missed threats.	Automate alerts and responses through SIEM systems.
Baits in honeypots are secure from misuse.	Attackers use baits to access other systems.	Ensure baits are isolated and carefully monitored.
Data collected from honeypots is helpful for analysis.	Misinterpretation of data may result in incorrect decisions.	Combine honeypot data with other threat sources for better analysis.
Honeypots protect against advanced threats.	Some attackers may bypass honeypots without interaction.	Deploy honeypots in key network locations to maximize detection chances.
Resources needed for honeypots are adequate.	Resource limitations reduce the effectiveness of honeypots.	Adjust the number and type of honeypots according to available resources.
Collaborative honeypot data enhances threat intelligence.	Privacy or legal violations may arise from shared data.	Use anonymized data and adhere to legal and regulatory standards.
Honeypots integrate seamlessly with security systems.	Poor integration reduces the value of honeypot data.	Ensure compatibility with SIEM, IDS, and other monitoring tools.
Honeypots detect insider threats effectively.	Insider threats avoid interacting with honeypots.	Use internal honeypots strategically placed in sensitive areas.
Regular updates keep honeypots relevant.	Outdated honeypots fail to attract modern attackers.	Schedule regular updates and align with evolving threat landscapes.
Honeypot isolation prevents lateral movement.	The attacker identifies the honeypot and avoids it.	Ensure realistic decoys with controlled data flow.

Deployed honeypots collect attacker TTPs.	Incomplete or misleading data may lead to poor threat modeling.	Use multiple honeypots and correlate data with external sources.

Honeypots and deception systems are valuable for individual organizations and foster collaborative intelligence. The collective understanding of emerging threats is significantly enhanced by sharing data from honeypots across organizations or sectors. For example, data on attack patterns, IOCs, and adversary TTPs observed in honeypot environments are pooled by organizations through threat intelligence platforms. Defenses are strengthened through this collaborative approach, which allows for the learning of participants from each other's experiences and the proactive application of countermeasures. Actionable intelligence is shared in a manner that is particularly impactful in sectors such as finance, healthcare, and critical infrastructure, where cascading effects across organizations are often caused by cyber threats. For instance, data shared from honeypots deployed in multiple sectors are analyzed, common vulnerabilities are identified, and coordinated responses are developed to mitigate risks. Faster detection and response to APTs and zero-day exploits are enabled by collaborative intelligence, as collective data provide a broader view of the attack landscape.

Furthermore, partnerships between the public and private sectors can amplify the benefits of deception systems. Governments can leverage insights from private-sector honeypots to enhance national cybersecurity strategies, while private organizations can benefit from aggregated threat intelligence to strengthen their security postures. Collaborative frameworks such as Information Sharing and Analysis Centers (ISACs) and sector-specific working groups provide structured mechanisms for secure and effective data exchange.

The raising of ethical and legal concerns is often associated with luring attackers through deception technologies, such as honeypots or fake networks, mainly when interactions with data involving privacy considerations occur. The primary goal of deception systems is to enhance security; however, alignment with applicable laws and ethical standards must be ensured during deployment to avoid unintended consequences. A primary ethical concern is raised when the deception system utilizes realistic data that mimics sensitive information, such as personally identifiable information (PII) or proprietary business data. Even if these data are entirely synthetic, inadvertent interactions by attackers may occur, leading to its storage or sharing outside the organization, which raises potential privacy concerns. Legal liabilities may be incurred if regulators view such actions indirectly as exposing sensitive data to unauthorized parties.

Another challenge is presented by jurisdictions where the monitoring or recording of attacker activities in honeypots is governed by strict privacy laws, such as the General Data Protection Regulation (GDPR) in Europe. Organizations may require the disclosure of monitoring tools, even when targeting malicious actors, which could conflict with the covert nature of deception technologies.

Organizations must adopt a transparent and compliant approach to deploying honeypots and decoy networks to address these concerns. The following points are required:

1. It has been established that all data utilized in deception systems is entirely synthetic and does not replicate any actual sensitive information;
2. A thorough review of privacy and surveillance laws in applicable jurisdictions is conducted to ensure compliance;
3. Disclosure policies are maintained by organizations where required, ensuring clarity about the use of deception technologies and their intended purpose;

4. Risks should be minimized by designing deception systems that contain attackers within controlled environments, thereby preventing lateral movement into actual production systems or unintentional exposure of accurate data.

Adherence to these practices can help organizations leverage the benefits of deception technologies while minimizing potential ethical or legal risks, ensuring a responsible approach to enhancing security.

7.2.2. False Credentials Challenges

The management of false credentials is recognized as a notable challenge in deploying honeypots and deception systems. Although these credentials are often intentionally designed to attract attackers, complications can inadvertently arise from their improper management. For example, attackers may detect and identify that these credentials are part of a deception strategy, making the honeypot ineffective. Poorly constructed false credentials could be exploited by sophisticated adversaries to pivot toward legitimate systems, thereby increasing the organization's risk. Additionally, ethical and legal concerns could be raised if false credentials are inadvertently mimicked by legitimate user accounts or sensitive information is referenced. Attackers can exfiltrate and disseminate these credentials, resulting in reputational damage or potential regulatory scrutiny. The importance of ensuring that false credentials are carefully crafted, monitored, and isolated from real production systems is underscored by this challenge. To mitigate these risks, it is recommended that credentials distinct from actual user accounts be utilized to avoid confusion or exploitation. Robust logging and monitoring systems should be implemented to detect and analyze any interactions with false credentials. The false credentials should be regularly updated and validated to ensure their effectiveness and prevent compromise of security or ethical standards.

Mitigation Techniques: To safeguard against DoS attacks, it is recommended that rate-limiting mechanisms be included in honeypot configurations to prevent excessive simultaneous requests from overwhelming the system. Such configurations enable administrators to effectively control data flows while system integrity is preserved, and robust data collection is ensured. Additionally, exploit-based and anomaly-based methods must be incorporated into intrusion detection mechanisms to identify deviations from standard traffic patterns promptly. Reference data, including intrusion signatures and baseline behavioral profiles, should be dynamically updated to reflect current threat landscapes. Configuration data are stored for intermediate results, which aid in refining detection mechanisms and maintaining system adaptability.

7.2.3. Content Filtering and Traffic Control:

ontent Filtering Systems (CFSs) can augment honeypots by restricting access to harmful content, ensuring that attackers are directed toward the honeypot. In contrast, risks to legitimate systems are mitigated. These filters enhance the honeypot's ability to isolate malicious activity and protect the broader network.

Combined with deception techniques, honeypots create a multi-faceted defense mechanism that enhances cybersecurity effectiveness. Deception techniques create realistic but fake assets, such as files, credentials, or entire network environments, to mislead attackers and study their behavior. Honeypots achieve several objectives through this integration alongside the proposed methodologies.

1. Enhanced Luring: Luring capabilities are achieved through deception techniques that increase the attractiveness of honeypots by mimicking high-value assets or vulnerabilities likely to attract attackers. For instance, decoy databases or credentials

placed within the honeypot environment guide attackers deeper into the trap, enabling detailed monitoring and engagement;

2. Behavioral Analysis in Depth: Attackers' methods, tools, and intentions are revealed in greater detail as interactions with the deception-enhanced honeypot occur. This insight contributes to understanding emerging threat patterns, and actionable intelligence is provided to secure actual systems;
3. Delay and Diversion: Deception techniques combined with honeypots are a delay mechanism, with attackers diverting from critical systems. Organizations present convincing but controlled environments to allow time for detection, analysis, and response while ensuring the security of production systems;
4. Real-Time Threat Detection: Specific attacker actions, such as attempts to exfiltrate sensitive data or exploit particular vulnerabilities, can be identified and flagged through deception in honeypots. These actions trigger alerts, allowing incident response teams to respond swiftly;
5. Integration with Threat Intelligence Platforms: The data collected from honeypots utilizing deception techniques can be directly shared with threat intelligence platforms, enhancing the broader security ecosystem by contributing new IOCs and attacker profiles.

The proposed approach maximizes threat detection, analysis, and mitigation efficiency by aligning honeypots with deception techniques. This combination ensures a proactive and robust defense strategy that adapts to dynamic threat landscapes. Addressing these security assumptions and implementing robust mitigation techniques can maximize the effectiveness of honeypots and minimize risks, ensuring they remain a valuable component of a comprehensive cybersecurity defense strategy.

7.3. Integration with Existing Security Infrastructure

Depending on the desired objectives and the targeted network segment, three primary approaches can be followed for integrating honeypot technology into an organization's security infrastructure. These approaches deploy honeypots within the Local Area Network (LAN), the perimeter network, or directly on the Internet. Each method offers distinct advantages and challenges, and its effectiveness is determined by the degree to which the design aligns with organizational requirements.

The comprehensive workflow for honeypot integration into security infrastructures is illustrated in Figure 7, with the interactions between honeypots, SIEM systems, intrusion detection systems (IDSs), firewalls, and incident response frameworks being highlighted. The diagram shows how data collected from honeypots is fed into SIEM for correlation and analysis, is utilized by IDSs for real-time monitoring, and is filtered through firewalls for preventive measures. Incident response systems then leverage insights from SIEM and IDSs to take actionable steps, creating a feedback loop that enhances honeypot configurations and overall security posture. The dynamic interplay of these components in strengthening an organization's defenses against cyber threats is underscored by this workflow.

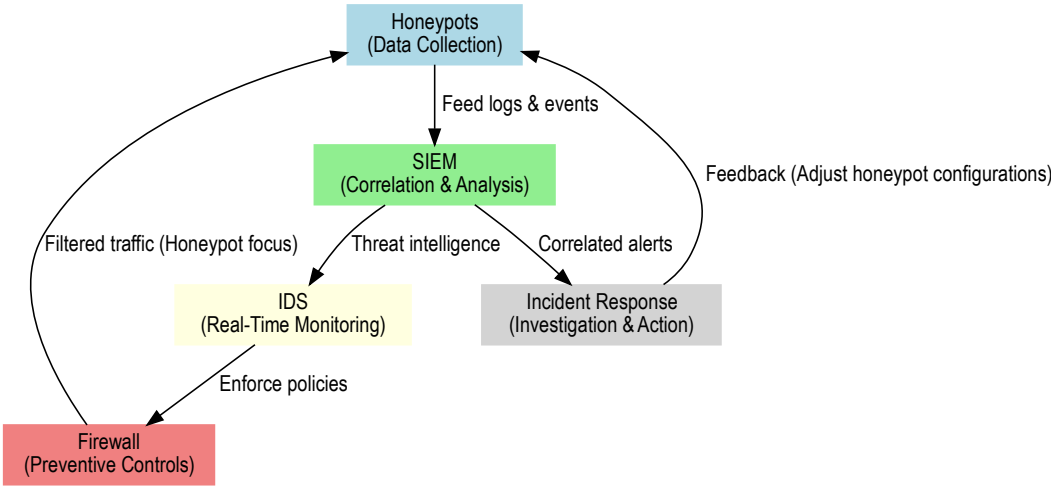

Figure 7. Strategic placement of honeypot in a multi-layered network security architecture.

7.3.1. Honeypots in the LAN Segment

Honeypots are deployed within the LAN segment, integrated into the internal network, and placed in the same environment as production servers. This honeypot configuration detects malicious activities from external sources and internal actors, such as compromised devices or insider threats [37]. Figure 8 illustrates the placement of a honeypot within the LAN segment. This approach enables comprehensive monitoring of internal and external threats, resulting in a dual-layer advantage.

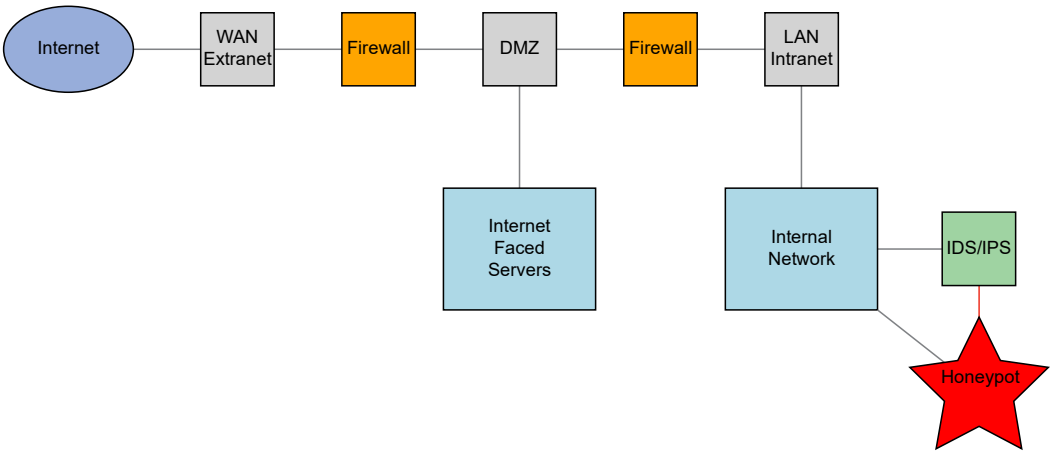

Figure 8. Strategic placement of honeypot in a LAN segment.

However, this configuration introduces notable security risks. If attackers detect and exploit the honeypot, it could be leveraged to infiltrate the internal network. To mitigate these risks, low-interaction honeypots in the LAN environment are recommended. Limited capabilities for interaction with such systems are offered, minimizing the chances of being used as a launch point for further attacks. Despite the challenges encountered, a LAN-deployed honeypot is particularly effective for uncovering insider threats and mapping internal vulnerabilities.

7.3.2. Honeypots for the DMZ Segment

Honeypots deployed in the DMZ segment monitor and interact with external threats while maintaining isolation from the internal network. Critical services like web and email servers are typically hosted in the DMZ, a segregated network zone. Honeypots are placed in this zone to allow for the observation and analysis of malicious activities targeting these

outward-facing services. This placement's primary advantage is its isolation, which is believed to limit the potential for attackers to pivot into the internal network.

However, it has been determined that the DMZ's honeypots are insufficient when considered a standalone security solution. Threats within the LAN cannot be detected or mitigated, leaving internal systems unprotected. For comprehensive coverage, it is suggested that DMZ honeypots be complemented with additional deployments within the internal network. The ability to detect unauthorized access in both the DMZ and within the LAN is enhanced by this dual-layered approach.

7.3.3. Honeypots for the Internet Traffic

Honeypots are placed directly on the Internet to enable organizations to monitor and analyze attacks that originate entirely from external sources. Honeypot is exposed to various external threats, including scanning, botnet activities, and direct exploitation attempts. Figure 9 depicts the placement of a honeypot outside the corporate network on the Internet. This method is particularly effective for gathering intelligence on external threat actors and their tactics.

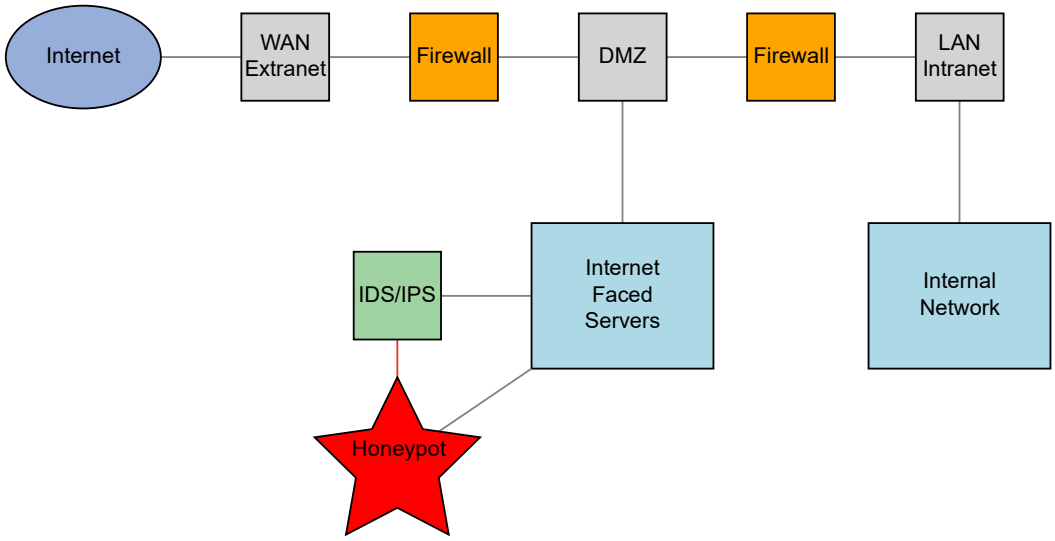

Figure 9. Honeypot deployment in an extranet configuration for enhanced threat monitoring.

Due to its exposure, traditional protections such as firewalls are lacking in an Internet-deployed honeypot, intentionally left vulnerable to entice attackers. However, the honeypot is to be isolated from the LAN and DMZ to prevent attackers from using it as a pivot point. Integrating the honeypot with an intrusion detection system (IDS) or Intrusion Prevention System (IPS) is essential for continuous monitoring and capturing actionable threat intelligence. This approach primarily focuses on the detection of attacks targeting public-facing infrastructure.

7.3.4. Considerations for Integration

The strengths and limitations of each deployment strategy are recognized, and the choice of placement is to be guided by organizational needs, the threat landscape, and available resources. Internal threat detection is prioritized in LAN deployments, isolation, and external threat analysis are offered by DMZ deployments, and Internet-facing honeypots ideally collect intelligence on broader attack trends.

The deployment strategy for honeypots is guided by robust IT design principles and meticulously aligned with defined security objectives to optimize their utility while preserving the network's integrity. A comprehensive and effective integration of honeypot

technology into the existing security infrastructure is achieved by employing a combination of deployment approaches tailored to the organization's specific requirements.

8. Future Works

As cybersecurity threats grow in sophistication and evolve rapidly, significant innovation in developing and applying honeypots is anticipated. Several emerging trends are expected to shape the future trajectory of honeypot technology, with enhanced capabilities being offered and an expansion of their role in organizational cybersecurity frameworks.

The detection and analysis capabilities of honeypots are anticipated to be enhanced by advancements in machine learning (ML) and artificial intelligence (AI). By leveraging these technologies, future honeypots will be able to achieve more precise and automated detection of cyberattacks. The integration of ML algorithms is expected to allow honeypots to be adapted dynamically to evolving attack patterns, thereby enhancing the ability to recognize previously unseen threats. Proactive defense is to be supported by actionable insights.

The increasing focus on automation is expected to revolutionize the deployment and operation of honeypots. Automation will streamline the implementation process, enabling honeypots to be deployed more efficiently and reduce manual intervention. Moreover, systematic automation in data analysis will enable faster and more accurate interpretation of the data gathered by honeypots, enhancing their utility in real-time threat intelligence and incident response.

Integrating honeypots with other security tools, such as IDSs and IPSs, is a critical future direction. Enhanced interoperability and coordination between these systems will strengthen the collective ability to detect, prevent, and analyze cyberattacks. This integration will facilitate a more cohesive security ecosystem, allowing the strengths of multiple security tools to be leveraged for comprehensive threat defense.

The evolution of cloud-based honeypots is aligned with the growing trend of infrastructure migration to cloud environments by organizations. Cloud-based honeypots are positioned uniquely to differentiate between attacks targeted at cloud-native applications and those aimed at traditional assets. The increasing importance of this capability is anticipated as cloud adoption is expanded and attackers develop more sophisticated methods for exploiting cloud-based vulnerabilities.

Honeypots will also contribute to advancements in deception-based security technologies. As a component of broader fraud and diversion strategies, honeypots will enhance the ability to misdirect attackers, creating additional layers of complexity within organizational defenses. These deceptive methods will be critical in delaying attackers and increasing the cost of executing successful intrusions.

The ongoing development of these trends is underscored by the enduring relevance of honeypot technology in combating cybercrime. Advancements in AI and ML are being incorporated, automation is being enhanced, integration with security tools is being fostered, and adaptation to cloud-based infrastructure is being undertaken, ensuring that honeypots will be maintained as a vital component of cybersecurity strategies. As increasingly sophisticated attackers confront organizations, the effectiveness of honeypot technology is ensured in addressing current and emerging challenges through innovation. The role of honeypots is expected to be solidified as indispensable tools in safeguarding digital assets and maintaining robust security postures.

9. Conclusions

The increasing complexity and specificity of cyber threats necessitate proactive and sophisticated countermeasures. This study underscores the pivotal role of honeypots as a multifaceted defense mechanism within contemporary cybersecurity frameworks. Their integration with broader security infrastructures, including firewalls, intrusion detection systems, and incident response protocols, highlights their potential to strengthen organizational resilience against evolving cyber threats.

Honeypots generate actionable intelligence by capturing and analyzing attacker TTPs. This paper distinguishes between research honeypots, recognized for their excellence in data collection aimed at forensic and threat intelligence purposes, and production honeypots, integrated into security operations for real-time threat mitigation. The strengths and limitations of honeypot solutions were revealed through evaluation, allowing for tailored deployments based on organizational needs. For instance, Dionaea and Cowrie showcased exceptional versatility and data accuracy, while Honeyd and Thug provided insights into scalability and specific attack vectors. This work's methodological contribution is provided by employing simulated network attacks to assess honeypot efficiency, which offers an empirical basis for comparing solutions. Detection and logging capabilities across selected honeypots were evaluated using tools like Nmap and Metasploit, and critical insights into their operational effectiveness were revealed. It was noted that Amun, Dionaea, Cowrie, and Thug exhibited robust performances in capturing and analyzing a wide range of threats. At the same time, Glasstopf and Honeyd faced configuration and activity-tracking challenges.

Furthermore, emerging trends in honeypot technology are identified, including the integration of machine learning for automated threat detection, the adoption of cloud-based honeypots for addressing cloud-native threats, and advancements in deception strategies to enhance adversary engagement. These innovations position honeypots as dynamic and adaptable tools capable of addressing current and future cybersecurity challenges.

The study's contributions are extended to practical applications, with a decision-making framework for selecting and deploying honeypots. This framework aids in aligning honeypot implementation with specific security objectives and resource constraints within organizations. Best practices, such as strategic placement, continuous monitoring, and integration with existing security tools, are emphasized, and this research provides actionable recommendations for maximizing the effectiveness of honeypots.

Honeypots are recognized as indispensable components of a layered security strategy, with unique threat detection, analysis, and mitigation advantages. The advancements in honeypot technology, along with a robust methodological approach to their evaluation, are ensured to maintain relevance and efficacy in the combat against sophisticated cyber threats of today and tomorrow. The insights derived from this research contributed significantly to the understanding and operationalization of honeypots, with their role in safeguarding digital assets and enhancing organizational security postures being reinforced.

Author Contributions: Conceptualization, Z.M. and V.D.; methodology, Z.M.; software, Z.M.; validation, V.D. and D.R.; formal analysis, D.R.; investigation, D.R.; resources, Z.M.; data curation, V.D.; writing—original draft preparation, V.D.; writing—review and editing, V.D. and Z.M.; visualization, Z.M.; supervision, V.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Šimon, M.; Huraj, L.; Hrinkino, D. Using a Honeypot to Improve Student Cybersecurity Awareness. In Proceedings of the 2023 21st International Conference on Emerging eLearning Technologies and Applications (ICETA), Stary Smokovec, Slovakia, 26–27 October 2023; pp. 440–445. https://doi.org/10.1109/iceta61311.2023.10343633.
2. Nintsiou, M.; Grigoriou, E.; Karypidis, P.A.; Saoulidis, T.; Fountoukidis, E.; Sarigiannidis, P. Threat Intelligence Using Digital Twin Honeypots in Cybersecurity. In Proceedings of the 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 31 July–2 August 2023; pp. 530–537. https://doi.org/10.1109/csr57506.2023.10224997.
3. Touch, S.; Colin, J.-N. Asguard: Adaptive Self-Guarded Honeypot. In Proceedings of the 17th International Conference on Web Information Systems and Technologies, Online, 26–28 October 2021; pp. 565–574. https://doi.org/10.5220/0010719100003058.
4. Subhan, D.; Lim, C. Analyzing Adversary's Attack on Ethereum Collected from Honeypots. In Proceedings of the 2023 11th International Conference on Information and Communication Technology (ICoICT), Melaka, Malaysia, 23–24 August 2023; pp. 313–318. https://doi.org/10.1109/ICoICT58202.2023.10262563.
5. Benedict, S. EA-POT: An Explainable AI-Assisted Blockchain Framework for HoneyPot IP Predictions. *Acta Cybern.* **2022**, *26*, 149–173. https://doi.org/10.14232/actacyb.293319.
6. Valeros, V.; Rigaki, M.; Garcia, S. Attacker Profiling Through Analysis of Attack Patterns in Geographically Distributed Honeypots. *arXiv* **2023**, arXiv:2305.01346. https://doi.org/10.48550/arXiv.2305.01346.
7. Baykara, M.; Daş, R. SoftSwitch: A Centralized Honeypot-Based Security Approach Usingsoftware-Defined Switching for Secure Management of VLAN Networks. *Turk. J. Elec. Eng. Comp. Sci.* **2019**, *27*, 3309–3325. https://doi.org/10.3906/elk-1812-86.
8. Dowling, S.; Schukat, M.; Barrett, E. Using Reinforcement Learning to Conceal Honeypot Functionality. In Proceedings of the Machine Learning and Knowledge Discovery in Databases: European Conference, ECML PKDD 2018, Dublin, Ireland, 10–14 September 2018; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2019; pp. 341–355. https://doi.org/10.1007/978-3-030-10997-4_21.
9. Veluchamy, S.; Kathavarayan, R.S. Deep Reinforcement Learning for Building Honeypots against Runtime DoS Attack. *Int. J. Intell. Syst.* **2021**, *37*, 3981–4007. https://doi.org/10.1002/int.22708.
10. Naik, N.; Shang, C.; Jenkins, P.; Shen, Q. D-FRI-Honeypot: A Secure Sting Operation for Hacking the Hackers Using Dynamic Fuzzy Rule Interpolation. *IEEE Trans. Emerg. Top. Comput. Intell.* **2020**, *5*, 893–907. https://doi.org/10.1109/TETCI.2020.3023447.
11. Schuba, M.; Hofken, H.; Linzbach, S. An ICS Honeynet for Detecting and Analyzing Cyberattacks in Industrial Plants. In Proceedings of the 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 9–10 December 2021; pp. 1–6. https://doi.org/10.1109/ICECET52533.2021.9698746.
12. Nila, C.; Preda, M.; Apostol, I.; Patriciu, V.-V. Reactive WiFi Honeypot. In Proceedings of the 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, Romania, 1–3 July 2021; pp. 1–6. http://doi.org/10.1109/ECAI52376.2021.9515048.
13. Drăghicescu, D.; Caranica, A.; Fratu, O. Honeypot Technologies for Malware Detection and Analysis. *StratXXI_CSC* **2021**, *17*, 265–271. https://doi.org/10.53477/2668-2028-21-34.
14. Sehgal, R.; Majithia, N.; Singh, S.; Sharma, S.; Mukhopadhyay, S.; Handa, A.; Shukla, S.K. Honeypot Deployment Experience at IIT Kanpur. *IITK Dir.* **2020**, 49–63. https://doi.org/10.1007/978-981-15-1675-7_6.
15. Sladić, M.; Valeros, V.; Catania, C.; Garcia, S. LLM in the Shell: Generative Honeypots. *arXiv* **2023**, arXiv:2309.00155. https://doi.org/10.48550/arXiv.2309.00155.
16. Subhan, D.; Lim, C. Unveiling Attack Patterns: A Study of Adversary Behavior from Honeypot Data. In Proceedings of the 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), Bogor, Indonesia, 22–24 August 2023; pp. 178–183. https://doi.org/10.1109/ICoCICs58778.2023.10276516.
17. Florea, R.; Craus, M. A Game-Theoretic Approach for Network Security Using Honeypots. *Future Internet* **2022**, *14*, 362. https://doi.org/10.3390/fi14120362.
18. Mocanu, F.; Scripcariu, L. Intrusion Detection Platform with Virtual Honeypots. In Proceedings of the 2023 International Symposium on Signals, Circuits and Systems (ISSCS), Iasi, Romania, 13–14 July 2023; pp. 1–4. https://doi.org/10.1109/ISSCS58449.2023.10190854.

19. Katakwar, H.; Aggarwal, P.; Dutt, V. Modeling the Effects of Different Honeypot Proportions in a Deception-Based Security Game. *AHFE Int.* **2023,** *91*, 132-145. https://doi.org/10.54941/ahfe1003727.
20. Ziaie Tabari, A.; Ou, X. A Multi-Phased Multifaceted IoT Honeypot Ecosystem. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 9-13 Nov 2020. https://doi.org/10.1145/3372297.3420023.
21. Osman, M.; Nadeem, T.; Hemida, A.; Kamhoua, C. Optimizing Honeypot Placement Strategies with Graph Neural Networks for Enhanced Resilience via Cyber Deception. In Proceedings of the 2nd on Graph Neural Networking Workshop 2023, Paris, France, 8 December 2023; pp. 37–43. https://doi.org/10.1145/3630049.3630169.
22. Anwar, A.; Chen, Y.H.; Hodgman, R.; Sellers, T.; Kirda, E.; Oprea, A. A Recent Year on the Internet: Measuring and Understanding the Threats to Everyday Internet Devices. In Proceedings of the 38th Annual Computer Security Applications Conference, Austin, TX, USA, 5–9 December 2022; pp. 251–266. https://doi.org/10.1145/3564625.3564649.
23. Zobal, L.; Kolar, D.; Fujdiak, R. Current State of Honeypots and Deception Strategies in Cybersecurity. In Proceedings of the 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Dublin, Ireland, 28–30 October 2019; pp. 1–9. https://doi.org/10.1109/ICUMT48472.2019.8970921.
24. Zhou, Z.; Shen, W. HoneyPot: Enhancing Cybersecurity through a Computer Simulation Technology. *HSET* **2024**, *105*, 97–101. https://doi.org/10.54097/0q8h9k30.
25. Wang, C.; Lu, Z. Cyber Deception: Overview and the Road Ahead. *IEEE Secur. Priv.* **2018**, *16*, 80–85. https://doi.org/10.1109/MSP.2018.1870866.
26. Acosta, J.C.; Basak, A.; Kiekintveld, C.; Leslie, N.; Kamhoua, C. Cybersecurity Deception Experimentation System. In Proceedings of the 2020 IEEE Secure Development (SecDev), Virtual Conference, 28–30 September 2020; pp. 34–40. https://doi.org/10.1109/SecDev45635.2020.00022.
27. Anwar, A.H.; Kamhoua, C.A.; Leslie, N.O.; Kiekintveld, C. Honeypot Allocation for Cyber Deception Under Uncertainty. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 3438–3452. https://doi.org/10.1109/TNSM.2022.3179965.
28. Sayed, M.A.; Anwar, A.H.; Kiekintveld, C.; Kamhoua, C. Honeypot Allocation for Cyber Deception in Dynamic Tactical Networks: A Game Theoretic Approach. In Proceedings of the International Conference on Decision and Game Theory for Security, Avignon, France, 18–20 October 2023. https://doi.org/10.48550/arXiv.2308.11817.
29. Aggarwal, P.; Du, Y.; Singh, K.; Gonzalez, C. Decoys in Cybersecurity: An Exploratory Study to Test the Effectiveness of 2-Sided Deception. *arXiv* **2021**, arXiv:2108.11037. https://doi.org/10.48550/arXiv.2108.11037.
30. Javadpour, A.; Ja'Fari, F.; Taleb, T.; Benzaïd, C. A Mathematical Model for Analyzing Honeynets and Their Cyber Deception Techniques. In Proceedings of the 2023 27th International Conference on Engineering of Complex Computer Systems (ICECCS), Toulouse, France, 14–16 June 2023; pp. 81–88. https://doi.org/10.1109/ICECCS59891.2023.00019.
31. European Network and Information Security Agency (ENISA). Proactive Detection of Security Incidents. 2012. Available online: https://www.enisa.europa.eu/sites/default/files/publications/ENISA_Honeypots_study.pdf (accessed on 22 November 2024).
32. Sun, Q.; Fan, C.; Zhang, W.; Chen, J.; Wang, H.; Zhang, R. Research and Application of High Interaction Deception Defense and Traceability Based on RASP Technology. In Proceedings of the 2024 2nd International Conference On Mobile Internet, Cloud Computing and Information Security (MICCIS), Changsha, China, 19–21 April 2024; pp. 48–52. https://doi.org/10.1109/MICCIS63508.2024.00016.
33. Melhem, H.; Salloum, E.; Oudeh, A.Y.; Anbar, M.; Molhem, M.; Golubtsov, I. Strengthening Health Care Networks: A Security Model for Enhanced Cyber Resilience Using Hybrid Honeypots. In Proceedings of the 2024 6th International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), Moscow, Russia, 29 February–2 March 2024; pp. 1–6. https://doi.org/10.1109/REEPE60449.2024.10479780.
34. Hegedüs, D.L.; Balogh, Á.; Érsok, M.; Erdődi, L.; Olcsák, L.; Bánáti, A. Beyond Static Defense: Dynamic Honeypots for Proactive Threat Engagement. In Proceedings of the 2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania. 23–25 May 2024; pp. 000547–000552. https://doi.org/10.1109/SACI60582.2024.10619764.
35. Albaseer, A.; Abdi, N.; Abdallah, M.; Qaraqe, M.; Al-Kuwari, S. FedPot: A Quality-Aware Collaborative and Incentivized Honeypot-Based Detector for Smart Grid Networks. *IEEE Trans. Netw. Serv. Manag.* **2024**, *21*, 4844–4860. https://doi.org/10.1109/TNSM.2024.3387710.
36. Wang, Z.; You, J.; Wang, H.; Yuan, T.; Lv, S.; Wang, Y.; Sun, L. HoneyGPT: Breaking the Trilemma in Terminal Honeypots with Large Language Model. *arXiv* **2024**, arXiv:2406.01882. https://doi.org/10.48550/arXiv.2406.01882.
37. Yang, X.; Yuan, J.; Yang, H.; Kong, Y.; Zhang, H.; Zhao, J. A Highly Interactive Honeypot-Based Approach to Network Threat Management. *Future Internet* **2023**, *15*, 127. https://doi.org/10.3390/fi15040127.

1.