Journal Homepage: www.ijarpr.com ISSN: 3049-0103 (Online)

International Journal of Advance Research Publication and Reviews

Vol 03, Issue 11, pp 111-118, November, 2026

Development and Simulation of a Deception-Based Honeynet Framework for Cyber Threat Hunting

Abdulkadir. Akinsola[1], Francisca N. Ogwueleka[2], and Uche M. Mbanaso[3]

[1, 3] Centre for Cyberspace Studies, Nasarawa State University, Keffi, NIGERIA

[2] Department of Computer Science, University of Abuja, Abuja-FCT, NIGERIA

ABSTRACT

Cyber threat hunting is a proactive approach to identifying suspicious activity that may evade conventional security controls. However, defenders may have limited visibility into how external sources interact with exposed services, and the volume of security events can make activity analysis challenging. This study develops and simulates a deception-based honeynet framework that integrates the T-Pot honeynet with Wazuh and the Elastic Stack. The framework deploys decoy services to record external interactions, forwards relevant honeypot logs for monitoring and analysis, and presents the collected events through dashboards. The study examines the resulting telemetry using descriptive analysis of event volumes, honeypot distribution, destination ports, observed source IP addresses, and Suricata alerts, alongside qualitative review of selected log records. The results demonstrate the framework's ability to collect and visualise activity directed at the deployed decoy services and to provide data for examining activity patterns. The study does not establish comparative detection accuracy or response-time improvements; these require further controlled evaluation.

Keywords: *Threat hunting, decoys, honeypots, vulnerabilities*

1. Introduction

Cyber threat hunting involves actively seeking out and identifying malicious activity within a computer network. Deception systems are a promising new approach to cyber threat hunting that can complement traditional security controls. Deception systems work by luring attackers into interacting with fake assets that are designed to look like real assets. When an attacker interacts with a fake asset, the deception system can detect the attack and alert the security team.

Deception systems for cyber threat hunting have emerged as a proactive approach to strengthen cybersecurity defences (Smith, 2022). Deception systems deceive and mislead attackers, divert their attention, and gather valuable information about their tactics, techniques, and procedures (TTPs). This strategic approach allows organisations to detect, analyse, and respond to cyber threats more effectively. Cyber threat hunting is the process of actively searching for and identifying cyber threats within an organisation's network or systems. Traditionally, this involved using various security tools and techniques to detect and respond to known threats. However, as cyberattacks evolve, organisations have recognised the need to adopt a more proactive, intelligence-driven approach (Zhou, 2020).

The development of deception systems adds a new layer of defence, aiming to lure potential attackers into engaging with decoy assets and environments designed to mimic legitimate systems and data. These decoys are designed to look enticing to attackers and often contain fabricated vulnerabilities, enticing files, or simulated network segments (Waisman, 2023). By interacting with these deceptive elements, attackers unknowingly leave behind valuable breadcrumbs that defenders can use to identify their presence, map their behaviour, and gather intelligence on their intentions (Zhou, 2020).

2. The Simulation of Deception Techniques

The simulation framework integrates key components from existing literature and practical cybersecurity operations to model how organisations can proactively detect, engage, and disrupt sophisticated cyber threats. It establishes the relationships between threat actor behaviours, deception deployment, simulated environments, threat hunting operations, detection and response metrics, and iterative feedback mechanisms, thereby providing a structured, adaptive, and intelligence-driven approach to cyber threat intelligence, including:

a. **Threat Actor Behaviours (TTPs):** Threat actor behaviours are simulated by replicating attacker tactics, techniques, and procedures (TTPs) across different stages of the attack lifecycle. Frameworks such as MITRE ATT&CK are used to model realistic adversary actions and predict attack paths. Simulation enables proactive detection, identification of security gaps, and improvement of cyber threat hunting capabilities (Zhu, 2019)

b. **Deception Techniques:** Deception techniques use decoy systems such as honeypots, honeytokens, and fake services to mislead attackers. These techniques increase attacker uncertainty, delay intrusion progress, and generate high-quality threat intelligence. Layered deception strategies improve detection accuracy and enhance cyber threat hunting operations (Zhang et al., 2021)

c. **Simulation Environment:** A simulation environment provides a controlled and isolated platform for testing cyber-attacks and defensive strategies. It enables safe deployment of deception techniques and observation of attacker behaviour without risking real systems. Adaptive mechanisms allow continuous refinement of security strategies based on attacker interactions. (Dowling et al., 2020).

d. **Cyber Threat-hunting operations:** Cyber threat hunting involves proactive investigation of network activities to detect hidden threats before alerts are triggered. Deception technologies provide high-fidelity data that supports hypothesis-driven threat hunting. Continuous, iterative hunting improves detection, reduces dwell time, and strengthens the organisation's security posture. (Kahlhofer, 2024).

e. **Detection and Response Metrics:** Detection and response metrics measure the effectiveness of cybersecurity defences using indicators such as detection latency and dwell time. These metrics provide a quantitative evaluation of threat detection and incident-response performance. Continuous metric monitoring helps optimise security strategies and improve cyber resilience (Chakraborty, 2023).

f. **Analysis and Feedback Loop:** The analysis and feedback loop continuously evaluates security data to refine detection and deception strategies. Insights from attacker interactions are used to improve threat hunting hypotheses and defensive measures. This iterative process ensures adaptive and intelligence-driven cybersecurity operations (Zhu, 2019).

3. Deception Theory

Deception theory forms a critical foundation for implementing cyber deception strategies in threat hunting. Originating in psychology, military science, and information warfare, deception theory involves deliberately manipulating an adversary’s perception to mislead, delay, or disrupt their actions. In cybersecurity, deception is employed to create controlled environments (e.g., honeypots, honey tokens, decoy files, or deceptive services) that mimic legitimate assets, enticing adversaries to interact with them. These interactions expose the presence, intent, and tactics of malicious actors.

Cyber deception does not rely solely on static decoys; instead, it strategically alters the attack surface, creating uncertainty and doubt for attackers. By engineering plausible but fake assets within the network, defenders increase cognitive and operational load on attackers, forcing them to expend more effort, time, and resources. In threat hunting, deception provides a high-fidelity data source by identifying threat actors who bypass conventional defences and interact with the deceptive artefacts.

Deception's success depends heavily on believability, consistency, and placement. Therefore, deception theory underpins the design of deceptive environments and ensures their integration into proactive threat hunting frameworks. This supports the rationale for increasing the likelihood that suspicious sources interact with decoy assets. The present study does not measure changes in attacker dwell time.

4. Game Theory in Cybersecurity

Game theory, a branch of mathematics focused on strategic interaction among rational agents, offers a powerful lens through which to model attacker-defender dynamics in cybersecurity. In the context of cyber threat hunting, game theory is used to simulate adversarial decision-making and to design optimal defence strategies based on expected attacker responses.

In particular, Stackelberg games are commonly applied, where the defender (leader) commits to a strategy (such as deploying deception assets), and the attacker (follower) reacts based on perceived utility. These models help defenders determine the best placement of honeypots or which systems to harden/deceive to maximise attacker confusion or misdirection.

Bayesian games also feature prominently, where the defender operates under incomplete information about the attacker’s capabilities or intent. In such scenarios, defenders assign probabilities to different attacker types and update their beliefs based on observed actions — mirroring real-world threat hunting activities where intelligence is incomplete.

By incorporating game theory, cyber defenders can anticipate attacker behaviour, balance risk and cost, and proactively adapt their threat hunting operations. This theoretical basis improves decision-making under uncertainty and supports deception as a means of influencing adversarial choices.

5. Related Work

Casanova & Sánchez-Macián (2023) developed a framework called "Threat Trekker," a machine learning-based framework designed to enhance proactive cyber threat hunting. Unlike traditional detection systems that react to known threats, Threat Trekker assumes adversaries may have already infiltrated the system. It proactively searches for unusual patterns or activities indicative of intrusion attempts. The framework utilises connectors to feed data directly into an event streaming channel, allowing real-time processing and feedback into the host network. The authors highlight the efficacy of employing machine learning to classify subtle attacks, emphasising the importance of proactive strategies in complex environments.

Turner et al. (2025) developed a framework called the "Technique Inference Engine" (TIE), a machine learning-powered tool designed to help analysts identify tactics, techniques, and procedures (TTPs) that may co-occur in cyber threat campaigns. Recognising the challenges posed by the vast volume of network traffic and evolving adversary techniques, TIE compiles a large dataset of cyber threat intelligence reports labelled with relevant TTPs. It applies implicit feedback recommender models to predict additional techniques that may be part of a given campaign. The tool provides a web interface where analysts can input observed TTPs and receive a ranked list of likely associated techniques, enhancing the efficiency and effectiveness of threat hunting efforts.

Puzis et al. (2020) developed ATHAFI, a comprehensive framework designed to automate threat hunting across multiple levels. It addresses the rapid evolution of cyberattacks that often outpace traditional intrusion detection systems. The framework incorporates adaptive targeted data collection, attack hypothesis generation, hypothesis testing, and continuous threat intelligence feeds. A key component is the Workflow Generation module, which adapts threat hunting procedures based on the latest threat intelligence or the most probable attack hypotheses. By integrating various commercial off-the-shelf products, ATHAFI aims to boost analysts' productivity, enabling them to perform investigations more efficiently and respond effectively to emerging threats.

Karuna et al. (2021) developed the WILEE system, which automates cyber threat hunting by translating high-level threat descriptions into concrete implementations using a custom domain-specific language (DSL). WILEE employs natural language processing to parse threat descriptions and generate corresponding DSL representations. It then uses genetic algorithms to generate queries that confirm or refute hypotheses about potential adversarial workflows. By automating query generation and using a structured approach to threat description, WILEE aims to scale cyber hunting and address the challenges posed by the vast quantity and complexity of data in large enterprise networks.

6. The Framework

Cyber threat hunting is a proactive, continuous process aimed at identifying and mitigating sophisticated cyber threats that evade traditional security controls. The cyber threat hunting lifecycle provides a structured, repeatable framework that guides security teams through the stages of threat hunting — from preparing for an investigation to validating findings and refining detection strategies. This lifecycle ensures hunting activities are systematic, hypothesis-driven, and adaptable to evolving adversary tactics, techniques, and procedures (TTPs).

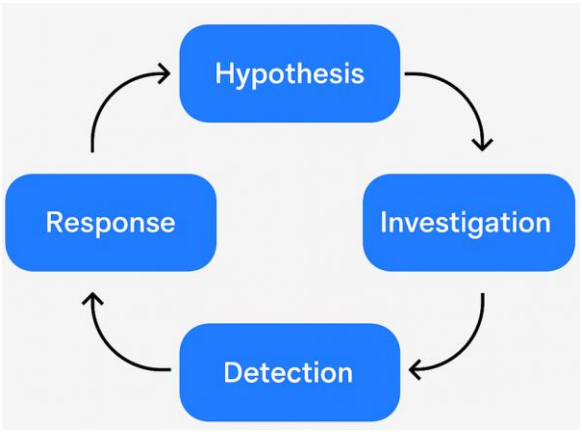


Figure 2: High-Level Structure of the Cyber Threat Hunting Framework (Source: Authors)

The broader cyber threat-hunting lifecycle can be organised into preparation and hypothesis generation, investigation, and detection and response. The implemented honeynet in this study focuses on deploying decoy services, collecting and monitoring their logs, and analysing the resulting telemetry. The following sections describe the lifecycle concepts relevant to the framework.

6.1 Preparation and Hypothesis Generation phase

Hypothesis development is the foundational phase of the cyber threat hunting lifecycle, where security analysts define assumptions about potential threats

within the network. This phase is typically driven by threat intelligence, known attacker behaviours, anomaly detection, or insights from previous incidents. Analysts form hypotheses about unauthorised access, lateral movement, or attempts at data exfiltration. These hypotheses guide the investigation and keep threat hunting structured rather than randomly. In deception-based environments, data from honeypots and decoy systems provide high-quality indicators to refine hypotheses. This phase requires a deep understanding of adversarial tactics and system behaviour to ensure realistic and actionable assumptions. Additionally, hypothesis development aligns closely with frameworks such as MITRE ATT&CK, enabling analysts to map potential attack vectors. A well-defined hypothesis improves efficiency, reduces unnecessary analysis, and increases the likelihood of uncovering hidden threats. Ultimately, this phase ensures that threat hunting is proactive, intelligence-driven, and focused on high-risk areas within the system.

6.2 Data Collection and Analysis Phase

Data collection involves gathering relevant security data from multiple sources to validate the formulated hypothesis. This includes logs from endpoints, network traffic, authentication systems, and security monitoring tools such as SIEM platforms. In deception-based cyber threat hunting, analysts also collect data from honeypots, honeytokens, and decoy services, which provide direct insight into attacker behaviour. The quality and completeness of collected data significantly affect threat-hunting effectiveness. Data must be timely, accurate, and comprehensive to ensure meaningful analysis. This phase also involves normalising and aggregating data from different sources to create a unified dataset for investigation. Efficient data collection lets analysts track attacker activity across systems and correlate events effectively. In simulation environments, data collection is controlled and structured, allowing repeatable, consistent analysis. Ultimately, this phase ensures sufficient evidence to validate or refute the threat-hunting hypothesis.

6.3 Threat Detection and Investigation Phase

The data analysis phase involves examining collected data to identify patterns, anomalies, and indicators of malicious activity. Analysts use both automated tools and manual techniques to correlate events and uncover hidden threats. This includes analysing login attempts, network traffic patterns, command-execution logs, and system behaviour. In deception-based environments, interactions with honeypots provide high-fidelity data that is easier to analyse compared to traditional logs. Analysts may apply behavioural analysis, anomaly detection, and correlation techniques to detect suspicious activities. This phase also involves mapping observed behaviours to known attacker tactics, techniques, and procedures (TTPs). The goal is to validate the hypothesis and determine the threat's scope. Data visualisation tools and dashboards often help identify trends and patterns. Effective analysis requires both technical expertise and contextual understanding of the system. Ultimately, this phase transforms raw data into actionable insights that inform detection and response decisions.

6.4 Response and Mitigation

The response and mitigation phase involves taking appropriate actions to contain, eliminate, and recover from identified threats. Once a threat is confirmed, security teams implement response strategies such as isolating affected systems, blocking malicious IP addresses, and removing compromised accounts. In some cases, deception techniques may continue to monitor attacker behaviour before full containment. This phase also includes documenting the incident and restoring all affected systems to a secure state. An effective response minimises the attack's impact and prevents further damage. Coordination between security teams and system administrators is essential during this phase. Automated response mechanisms may be used to accelerate containment and remediation. The team also records lessons learned from the incident to improve future responses. Ultimately, this phase ensures that threats are effectively neutralised and system integrity is restored.

6.5 Feedback and Continuous Improvement

The feedback and continuous improvement phase ensures that insights gained from threat hunting activities are used to enhance future security operations. This phase involves analysing the effectiveness of detection and response actions and identifying areas for improvement. Security teams refine detection rules, update threat intelligence, and adjust deception strategies based on observed attacker behaviour. In simulation environments, this phase is particularly important as it enables iterative testing and optimisation of defensive mechanisms. Continuous improvement ensures that the system remains adaptive to evolving threats and attacker techniques. Feedback from each hunting cycle improves hypothesis development and makes future investigations more efficient. This phase also supports knowledge sharing across security teams, improving overall organisational readiness. By incorporating lessons learned, organisations can reduce vulnerabilities and strengthen their security posture. Ultimately, this phase transforms cyber threat hunting into an ongoing, intelligence-driven process rather than a one-time activity.

7. Design of Framework for Cyber Threat Hunting

The framework developed in this study uses the T-Pot honeynet as the deception environment and Wazuh as the platform for collecting and monitoring relevant honeypot logs. The Elastic Stack supports storage, searching, and visualisation of the collected events. The implementation is intended to provide additional telemetry for cyber threat-hunting analysis.

The implemented framework operates in three main stages:

a. Deception-based data generation – T-Pot deploys selected honeypot services that simulate network services and record interactions directed at them.

b. Data collection and monitoring – relevant honeypot logs are collected and monitored through Wazuh, with events made available for analysis and visualisation in the Elastic Stack.

c. Analysis and visualisation – collected events are examined to describe event volumes, honeypot distribution, destination ports, observed source IP addresses, and security alerts.

d. This workflow provides a structured way to collect and examine activity directed at decoy services. The implementation supports analysis of recorded activity; it does not by itself establish that every event represents a confirmed attack or that automated intelligence sharing or response was performed.

7.1 Requirement Engineering for Cyber Threat Hunting

Requirements engineering is the systematic process of defining and documenting the capabilities a system is expected to provide. For a honeynet-based threat-hunting framework, requirements may include safe deployment of decoy services, reliable log collection, monitoring, analysis, and visualisation. The requirements below describe desired capabilities for a broader operational framework; they should not be interpreted as features all implemented or tested in this study.

i. The framework should support different honeypot types (low-interaction, medium-interaction, and high-interaction) to capture diverse attack vectors (Fraunholz et al., 2017).

ii. The honeynet must capture inbound and outbound malicious traffic and forward logs to Wazuh for centralised analysis.

iii. Data collected should be enriched with external intelligence sources (e.g., MISP or AbuseIPDB) for actionable threat hunting.

iv. Suspicious behaviour should trigger alerts and dashboards for SOC analysts.

v. The honeynet must be scalable to accommodate multiple network segments within the enterprise.

vi. Real-time log forwarding and correlation should not degrade network performance.

vii. The honeypot must be isolated to prevent compromise of the production network (Pouget & Dacier, 2004).

viii. Regular updates and patches should be supported to maintain system effectiveness.

ix. Dashboards and visualisation must be intuitive for SOC analysts.

x. Ability to monitor attacker behaviours in real time.

xi. Smooth data ingestion into Wazuh SIEM for correlation with existing enterprise logs.

xii. Automated reports on TTPs, IoCs, and vulnerabilities to aid decision-making.

xiii. Deployment of honeypots must comply with organisational and legal policies, especially regarding data privacy (Almeshekah & Spafford, 2016).

xiv. Honeynet servers must balance system resource usage against production workloads.

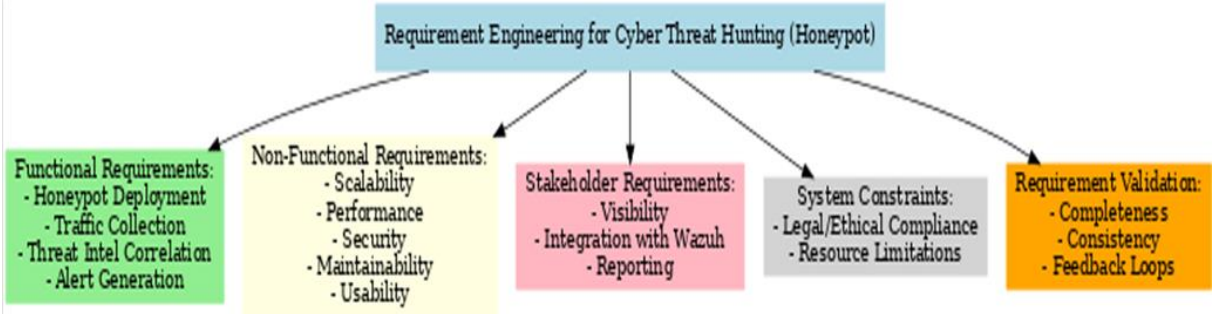


Figure 4 Components of Cyber Threat Hunting

7.2 System Architecture for Cyber Threat Hunting

The system architecture for cyber threat hunting is layered and modular, integrating data collection, analysis, intelligence enrichment, and response mechanisms. Its primary goal is to enable proactive detection of advanced threats and provide defenders with actionable insights before adversaries can cause significant damage.

i. Data Acquisition Components: Sources include network traffic logs, system and application logs, endpoint telemetry, firewall records, intrusion detection systems (IDS), and security appliances.

ii. Data Processing and Storage Layer: Data enrichment techniques, such as geolocation, reputation scoring, and threat intelligence correlation, are applied here to add context to raw events.

iii. Analytics and Detection Layer: Threat hunting teams use this layer to pivot on indicators, run queries, and test hypotheses about potential adversary presence.

iv. Response and Intelligence Layer: This layer supports incident response, case management, and automated defence actions, such as blocking malicious IPs, deactivating compromised accounts, or isolating suspicious endpoints.

8. Conclusion

This study developed and simulated a deception-based honeynet framework by integrating T-Pot with Wazuh and the Elastic Stack. The deployed environment recorded external activity directed at its decoy services. Analysis of the collected telemetry showed differences in event volumes across honeypots and identified commonly observed destination ports, source IP addresses, and Suricata alerts. These findings demonstrate that the integrated framework can collect, centralise, and visualise honeynet activity, providing security analysts with additional telemetry for examining suspicious interactions and activity patterns. The findings should be interpreted within the scope of the deployment and observation period. They do not, on their own, demonstrate improved detection accuracy, reduced alert noise, increased attacker dwell time, or faster incident response.

The study suggests that deception systems can complement conventional security monitoring by generating telemetry from interactions with decoy services. The practical value of this information depends on the quality of deployment, log coverage, analysis methods, and integration with existing security operations. The research also draws on deception theory and game theory to explain the strategic rationale for using deceptive assets; however, it does not experimentally validate attacker decision-making or game-theoretic outcomes. Future work should include longer observation periods, controlled comparisons with conventional monitoring, and evaluation using defined detection and response metrics.

References:

Abu Sayed, M., Anwar, A. H., Kiekintveld, C., Bosansky, B., & Kamhoua, C. (2023). Cyber Deception against Zero-day Attacks: A Game Theoretic Approach. arXiv e-prints, arXiv-2307.

Almeshekah, M., & Spafford, E. H. (2025). Design principles for cyber deception systems. Computers & Security, 138, 103012. https://doi.org/10.1016/j.cose.2024.103012

Al-Shaer, E., Duan, Q., & Liu, J. (2019). Automated Deception for Cyber Defence. Springer.

Bienzobas, Á. C., & Sánchez-Macián, A. (2023). Threat Trekker: An approach to cyber threat hunting. arXiv preprint arXiv:2310.04197.

Behl, A., & Behl, K. (2025). Proactive cyber threat hunting: Techniques, tools, and future directions. Journal of Information Security and Applications, 78, 103645. https://doi.org/10.1016/j.jisa.2024.103645

Chakraborty, T., Jajodia, S., Park, N., Pugliese, A., Serra, E., & Subrahmanian, V. S. (2018). Hybrid adversarial defense: Merging honeypots and traditional security methods. Journal of Computer Security, 26(5), 615-645.

Cranford, T. W., Gonzalez, C., & Lebiere, C. (2021). Towards a cognitive theory of cyber deception. Cognitive Science, 45(2), e13013. https://doi.org/10.1111/cogs.13013

Creswell, J. W., & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.). SAGE Publications.

Deep Threat Analytics. "Deception Technology in Cyber Defense: Enhancing Network Security." Deep Threat Analytics, 2023, https://www.deepthreatanalytics.com/network-security/deception-technology-cyber-defense-enhancing/.

Dowling, S., Schukat, M., & Barrett, E. (2020). New framework for adaptive and agile honeypots. Etri Journal, 42(6), 965-975.

Ferguson-Walter, Kimberly J., Maxine M. Major, Chelsea K. Johnson, and Daniel H. Muhleman. "Examining the Efficacy of Decoy-based and Psychological Cyber Deception." 30th USENIX Security Symposium (USENIX Security 21), USENIX Association, Aug. 2021, pp. 1127–1144.

Fang, F., Xu, H., & Hayel, Y. (2023). Decision and Game Theory for Security.

Fugate, M., Ferguson-Walter, K., & Lamont, G.s (2019). Artificial intelligence and game theory models for defending critical networks with cyber deception. AI Magazine, 40(1), 31–43. https://doi.org/10.1609/aimag.v40i1.2849

Fidelis Security. "Applications of Deception Technology in Cybersecurity." Fidelis Security, 2023, https://fidelissecurity.com/cybersecurity-101/deception/deception-technology-applications/.

https://www.researchgate.net/publication/353779928_Incorporating_Deception_into_CyberBattleSim_for_Autonomous_Defense

Jajodia, S., Ghosh, A., Subrahmanian, V. S., Swarup, V., Wang, C., & Wang, X. S. (2016). Cyber deception: Building the scientific foundation. Springer.

Kahlhofer, M., Achleitner, S., Rass, S., & Mayrhofer, R. (2024, September). Honeyquest: Rapidly measuring the enticingness of cyber deception techniques with code-based questionnaires. In Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses (pp. 317-336).

Karuna, P., Hemberg, E., O'Reilly, U. M., & Rutar, N. (2021). Automating cyber threat hunting using NLP, automated query generation, and genetic perturbation. arXiv preprintarXiv:2104.11576.

Li, Y., Chen, X., & Luo, X. (2025). Honeynet-based cyber threat intelligence generation. Future Generation Computer Systems, 150, 12–27. https://doi.org/10.1016/j.future.2024.12.018

Mbanaso, U. M., Abrahams, L., & Okafor, K. C. (2023). Research techniques for computer science, information systems and cybersecurity. Springer.

Mohammed, M. A., and A. M. Abdulazeez. "Cyber Threat Hunting: Proactive Techniques for Identifying Hidden Threats." Journal of Network and Computer Applications, 2024, https://www.sciencedirect.com/science/article/pii/S1084804524001814.

Puzis, R., Zilberman, P., & Elovici, Y. (2020). ATHAFI: Agile threat hunting and forensic investigation. arXiv preprint arXiv:2003.03663.

POMDPs to recognize cyber attacker's intent. arXiv preprint arXiv:2007.09512. https://arxiv.org/abs/2007.09512

Sayed, Md Abu, Ahmed H. Anwar, Christopher Kiekintveld, Branislav Bosansky, and Charles Kamhoua. "Cyber Deception Against Zero-Day Attacks: A Game Theoretic Approach."

Smith, J. D., & Johnson, A. B. (2022). "Advancing Cyber Threat Hunting through Deception Technologies." Journal of Cybersecurity, 5(1), tyaa005.

Shokri, R., & Kantarcioglu, M. (2025).

Adversarial behavior modeling in cyber defense systems. ACM Computing Surveys, 57(2), 1–36. https://doi.org/10.1145/3664567

Scarfone, K., & Mell, P. (2025). Guidelines for threat hunting and advanced detection (NIST Special Publication 800-92 Rev. 2, Draft). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92r2-draft

Shinde, A., Doshi, P., & Setayeshfar, O. (2020). Active deception using factored interactive Turner, M. J., Carenzo, M., Lasky, J., Morris-King, J., & Ross, J. (2025). Technique Inference Engine: A Recommender Model to Support Cyber Threat Hunting. arXiv preprint arXiv:2503.04819.

Walter, E. C., Ferguson-Walter, K. J., & Ridley, A. D. (2021). Incorporating deception into CyberBattleSim for autonomous defense. In IJCAI-21 1st International Workshop on Adaptive Cyber Defense.

Wan, Z., Cho, J.-H., Zhu, M., Anwar, A. H., Kamhoua, C., & Singh, M. P. (2021). Foureye: Defensive deception based on hypergame theory against advanced persistent threats. arXiv preprint arXiv:2101.02863. https://arxiv.org/abs/2101.02863

Zhou, R., Shi, H., & Zhou, W. (2020). "Deception for Cybersecurity Defence: A Survey." IEEETransactions on Dependable and Secure Computing, 18(1), 250-266.

Zhu, Q. (2019). Game theory for cyber deception: A tutorial. arXiv preprint arXiv:1903.01442. https://arxiv.org/abs/1903.01442

Zhang, L., & Thing, V. L. (2021). Three decades of deception techniques in active cyber defense-retrospect and outlook. Computers & Security, 106, 102288.

Fraunholz, D., Krohmer, D., Anton, S. D., & Schotten, H. D. (2017). A survey of honeypots and honeynets: Issues of deployment, challenges, and research directions. 2017 12th International Conference on Availability, Reliability and Security (ARES), 1-10.

Pouget, F., & Dacier, M. (2004). Honeypot-based forensics. AusCERT Asia Pacific Information Technology Security Conference.

Almeshekah, M. H., & Spafford, E. H. (2016). Planning and integrating deception into computer security defenses. Proceedings of the 2016 New Security Paradigms Workshop, 127-138.

Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2008). A survey on automated dynamic malware-analysis techniques and tools. ACM Computing Surveys, 44(2), 1–42.

MITRE ATT&CK Framework (2023). Adversarial Tactics, Techniques, and Common Knowledge. Retrieved from https://attack.mitre.org

Sittig, D. F., & Singh, H. (2020). A socio-technical perspective on cyber threat detection and response architectures. Journal of Biomedical **Informatics, 108, 103500.**