Parisa Premchand Goud, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Intelligent Honey Pot-Based Framework For Modern Cyber Security Defense

[1]Parisa Premchand Goud, [2] Gadde Anusha

[1]Assistant Professor, [2]M.Tech Student, Department of CSE,
Megha Institute Of Engineering And Technology For Women,
Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana

Abstract—A comprehensive analysis of honey pot integration with various cyber security frameworks is presented in this paper. These frameworks include firewalls, Intrusion Detection and Prevention Systems (IDPS), Security Information and Event Management (SIEM) systems, and Security Orchestration, Automation, and Response (SOAR) platforms. The paper builds a framework for improving honey pot functions using AI and ML using a systematic research process that includes literature review and case-based analysis. Adaptive responses to sophisticated cyber attacks, predictive analytics, and dynamic threat information may all be generated using this novel technique. The results highlight the importance of honey pots in improving the accuracy of threat detection, decreasing resource overhead, and giving useful information on the strategies, methods, and procedures (TTPs) used by attackers.

Keywords—honey pots, cyber security, IDPS, SIEM, SOAR, firewalls, artificial intelligence, machine learning, cyber deception technologies, dynamic threat intelligence, threat detection, attacker TTPs

I. INTRODUCTION

As cyber attacks have grown in both frequency and complexity, cyber security has become a more complicated issue. Successful defence against these threats requires adaptive security solutions that can identify and lessen the impact of assaults while also shedding light on the tactics used by adversaries. With their unmatched powers in detecting, analysing, and reacting to hostile behaviour, honey pots—specialized decoy systems—have become crucial components of current cyber security frameworks [10]. The strategic technique for honey pot placement is introduced in this research, with an emphasis on deploying honey pots in areas that maximise their usefulness.

The suggested method positions honey pots to intercept a variety of attack vectors, from external reconnaissance to internal threats, by examining network architecture and detecting high-risk regions. [2] In This approach is ideal for complicated situations because, unlike traditional arrangements, it adjusts to changes in the network in real time. The paper introduces a system for automatic honey pot setup to tackle the difficulties of multi-cloud and hybrid infrastructures. [8] In response to real-time threat information and network behaviour, this system uses machine learning algorithms to dynamically modify honey pot characteristics, including resource allocation and emulation profiles. Because of their flexibility, honey pots may be easily integrated into fluid situations without affecting their performance or detecting capabilities. [8] This study brings together the fields of cyber security and artificial intelligence by demonstrating how ML and AI are improving honey pot systems.

Artificial intelligence (AI) honey pots transform from passive decoys into proactive instruments that can foresee and counteract complex threats by integrating real-time anomaly detection and predictive analytics. (1), (2) By bringing together experts from different fields, we can make sure that honey pots are able to detect harmful activity and also help the cyber security ecosystem as a whole by learning and adapting. Honey pot integration with critical cyber security systems, such as firewalls, Intrusion Detection and Prevention Systems (IDPS), Security Information and Event Management (SIEM) systems, and Security Orchestration, Automation, and Response (SOAR) platforms, is the focus of this paper. The purpose of the research is to examine the methods and

advantages of this integration. Our main emphasis is on how these integrations work together to improve threat detection, allocate resources more efficiently, and fortify organisational defenses against sophisticated threats like zero-day vulnerabilities and targeted assaults.

The study goes on to say that honey pots combined with AI and ML may provide predictive threat analysis and dynamic response capabilities, which is a huge deal. Contributing to the expanding corpus of information on advanced cyber security methods, this paper offers a thorough examination of honey pot integration across multiple domains. These results highlight the crucial importance of honey pots in battling the ever-changing threat environment and should help academics and practitioners comprehend the strategic benefits of including them into comprehensive defence designs.

Integration of Honeypots with Intrusion Detection and Prevention Systems (Idps)

A comprehensive and multi-layered strategy for cyber security may be achieved by the combination of honey pots and Intrusion Detection and Prevention Systems (IDPS). Offering strong defence against both existing and new threats, this synergy combines the proactive detection capabilities of IDPS with the investigative and deceitful skills of honey pots. Organisations may improve their defenses against advanced attacks and keep their operating systems safe by using honey pots.

As part of the intrusion detection and prevention system (IDPS), honey pots serve as controlled environments that can detect and isolate malicious traffic [1, 3]. The IDPS forwards suspicious traffic to honey pots for further investigation when it detects it. Forensic examination of the assault may be conducted in detail thanks to this redirection, which also protects the main network by confining the danger. For instance, the IDPS may use the honey pot as a decoy system to catch attackers off guard when it detects suspicious or abnormal traffic based on signatures, such Distributed Denial of Service (DDoS) attempts or malware dissemination. The third Honey pots' containment qualities are vital. Security teams may study the attackers' techniques, tools, and goals in a controlled environment, away from vital systems, by separating harmful actions. By revealing attack patterns and vulnerabilities in real-time, this data is crucial for improving IDPS's detection criteria. Furthermore, IDPS signatures may be updated using insights obtained from honey pot logs, enhancing its ability to detect and prevent similar attacks going forward.

Enhanced Detection And Analysis

The capacity to identify and analyse unknown threats is a notable advantage of combining honey pots with IDPS. Honey pots are great at finding zero-day vulnerabilities and new methods of attack, in contrast to conventional detection systems that depend significantly on previously established signatures or criteria. Honey pots' dynamic environment reveals attackers' purpose and capabilities, providing crucial information that enhances the ecosystem for threat detection as a whole. Another important benefit is real-time monitoring. Honey pots help organisations to quickly react to emerging dangers by continuously observing attacker behaviour. References [1], [9] Additionally, the integration establishes a feedback loop whereby the data gathered by honey pots contributes to the improvement of IDPS rules, guaranteeing that the system can dynamically respond to emerging threats.

Reducing false positives and increasing detection accuracy are the goals of this iterative approach. Optimizing Resources and Intelligence on Threats within the IDPS system, honey pots can help optimise resource utilisation. Honey pots are used to redirect harmful traffic, which helps primary detection and prevention systems work much more efficiently. By doing so, operational systems are able to concentrate on their core operations and prioritise valid traffic, free from the distraction of potentially detrimental interactions. Honey pots are also great for gathering forensic and threat information. There is a plethora of information available in the logs and payloads recovered after encounters with attackers. This

includes indications of compromise (IOCs) and TTPs, or tactics, methods, and procedures. Not only does this information help build more robust security systems, but it is also essential for incident response.

Use Cases And Applications

Honey pots with IDPS integration have real-world uses in many different fields. For example, honey pots may detect and report intrusion attempts (both external and internal) in cloud systems by analysing suspicious traffic patterns. Similarly, honey pots are used in industrial control systems to examine focused assaults in a controlled environment, away from real infrastructure. Honey pots provide a controlled environment for researchers and developers to test and improve IDPS algorithms. Researchers may enhance cyber security systems by validating and improving detection algorithms via interactions with real-world threat data.

II. INTEGRATION OF HONEYPOTS WITH FIREWALLS AND ROUTING CONTROL

A significant step forward in developing strong, multi-layered network security systems is the incorporation of honey pots with routing control techniques and firewalls. One of the main functions of firewalls is to monitor and filter all network traffic, both incoming and outgoing, in order to prevent unauthorized access. As decoys, honey pots interacted with malicious traffic that evaded traditional detection procedures when placed strategically behind these firewalls. This method improves the security architecture as a whole by increasing threat detection capabilities and shedding light on the methods and tools used by attackers.

Mechanism Of Integration

The purpose of a honey pot is to deceive would-be hackers by seeming to be a real system or service on the network. They are additional lines of defence that catch traffic that may have passed through firewalls before. [4] This location is carefully planned to keep operating systems safe from any potential damage, allowing for the controlled analysis of suspicious behaviours. Understanding the tactics and intentions of malicious actors requires the acquired data, which includes payloads, attacker instructions, and interaction logs. Honey pots are much more effective when integrated with routing control. When firewalls detect suspicious traffic, routing protocols may be set up to redirect it to honey pot servers. This focused rerouting not only stops attackers from overwhelming the functioning network, but it also isolates malicious traffic. Honey pots are made to accept interactions from possible attackers via routing controls that use real-time traffic evaluations. This makes them very useful as investigative tools. (1), (2)

Implementation And Dynamic Rule Updates

To maximise their efficacy, honey pots deployed with firewalls need meticulous preparation. Honey pots are usually set up in parts of networks that might be a target for attackers, such as parts that imitate valuable assets like application servers or databases. Because of its advantageous location, both the possibility of engagement by hostile forces and the capacity to gather more detailed data are enhanced. One major benefit of this connection is that firewall rules may be dynamically updated using insights obtained from honey pot interactions. For example, firewall settings may be fine-tuned using honey pot data on newly discovered attack signatures, exploited vulnerabilities, or hostile IP addresses. The network's ability to withstand cyber attacks is strengthened by this feedback loop, which makes sure that the main defence systems are always adapting to new threats. C. Improved Intelligence Gathering and Threat Detection Honey pots and firewalls work together to greatly enhance the capacity to identify sophisticated attacks. Firewalls filter traffic first according to predetermined criteria, but honey pots are great at detecting hidden or unusual attack patterns. Honey pots provide useful intelligence, such attacker tactics, methods, and procedures (TTPs) and Indicators of Compromise (IOCs), by recording extensive interactions with attackers. Defence plans, both short- and long-term, rely heavily on this information. Honey pots also let

businesses analyse recorded assaults for forensic evidence, which sheds light on how attackers operate. To build focused mitigation plans and be ready for future dangers of a similar kind, this level of analysis is crucial. D. Real-World Uses and Advantages There are real-world consequences in many different areas for integrating honey pots with firewalls and routing management.

This integration is useful in corporate networks because it allows for the isolation and analysis of targeted assaults on systems that are valuable to the company. Honey pots are a great way to explore potential attack vectors for industrial control systems without endangering real infrastructure. They replicate operational technological settings and allow for targeted research. Improved firewall rules are one advantage of this integration; they help find vulnerabilities that weren't there before, which means fewer false negatives. Additionally, operational networks are shielded from potential harm during attack investigations thanks to honey pots' controlled environment, which lessens the effect of attacks on genuine systems. In addition to speeding up incident response, this method equips security teams with comprehensive records and useful knowledge to better mitigate risks.

III. INTEGRATION OF HONEYPOTS WITH SOC AND SOAR SYSTEMS

One strong and unified approach to current cyber security is the integration of honey pots with Security Orchestration, Automation, and Response (SOAR) technologies and Security Operations Centres (SOC). Security operations centres (SOCs) are the nerve centres of an organization's security operations, where security incidents are monitored, analysed, and responded to. By coordinating responses across various security technologies and automating procedures, SOAR systems improve these operations. When honey pots are integrated into this ecosystem, they enhance the data gathered and processed by SOCs, while also giving SOAR systems the insight they need to automate responses more efficiently. A. Honey pots as Sources of Secure Online Data the purpose of honey pots, which are specialised sensors, is to fool attackers into thinking they are engaging with legitimate network systems. Integrating honey pots into a SOC allows for the generation of comprehensive logs of attacker behaviour, including their TTPs. [5] The security operations centre (SOC) receives these logs and compares them with other security telemetry, including information gathered from firewalls, intrusion detection systems, and endpoint protection software.

Security operations centres (SOCs) are able to detect trends that could point to sophisticated or persistent assaults by combining data from many sources to get a fuller view of current risks. Honey pots help SOC analysts by providing richer data that helps them rank events according to their severity and possible effect. For instance, if honey pots discover a pattern of repeated attempts to exploit vulnerabilities, it might indicate a campaign of targeted attacks and warrants rapid examination. When it comes to finding zero-day vulnerabilities and other threats that evade standard detection methods, this capacity is invaluable. B. SOAR-Powered Automated Responses SOAR systems use honey pot data to automate many parts of threat detection, investigation, and response. [9] Predefined procedures, such as system isolation, IP address blocking, or file quarantining, may be initiated by SOAR systems when honey pots identify suspicious behaviour.

The time it takes to react to threats is reduced and problems are dealt consistently and methodically thanks to this automation. Integrating with SOAR also makes it easier to create and use specialised playbooks for honey pot interactions. To limit harmful activity without interfering with normal activities, a playbook may, for example, send all communication from a certain source that the honey pot has detected to extra security checks. The efficacy of defenses against changing threats is guaranteed by the dynamic nature of SOAR procedures. Chapter Four: Intelligence

on Potential Dangers Collaboration and sharing when it comes to sharing useful threat information across SOC and SOAR systems, honey pots are essential. Insights into the tactics, tools, and strategies used by attackers may be found in the logs gathered by honey pots. With this information, the organisation may strengthen its security posture, update its detection procedures, and improve its incident response tactics. [6] By sharing the data collected by honey pots with global threat intelligence platforms, SOCs may encourage cooperation between other businesses and security providers.

By sharing intelligence, we can better prepare for new threats and lessen the chances of coordinated assaults on several locations. D. Advantages of merging several important advantages may be gained by integrating honey pots with SOC and SOAR systems. To start with, it helps security teams spot and counteracts advanced persistent threats (APTs) and other covert dangers by increasing threat visibility and shedding light on attacker behaviour. Secondly, it automates operations and reduces the human effort needed to resolve security incidents, which speeds incident response. By streamlining their processes, SOC analysts may devote their attention to the most pressing issues, which boosts productivity and decreases reaction times.

By letting businesses practice attack scenarios and reaction tactics in safe settings, honey pot data also helps with proactive defenses. To make sure that security personnel are ready to deal with any attacks, SOAR systems can automate these simulations. E. Obstacles and Things to Think about Honey pot integration with SOC and SOAR systems have many benefits, but it also has certain drawbacks. Concerns about data overload are among the top ones. If not filtered and prioritised correctly, the massive amounts of logs generated by honey pots may overload security operations centres. Organisations may improve their threat detection and response capabilities by implementing good data management and analysis processes, which will allow them to make better use of honey pot data. The compatibility of honey pot installations with the company's overarching security plan is an additional factor to think about. Honey pots need to be strategically located and their outputs need to be in sync with the goals of SOC and SOAR systems for integration to work. 2 and 6 Maximising ROI and achieving meaningful outcomes from the integration depend on this alignment.

IV. INTEGRATION OF HONEYPOTS WITH SIEM SYSTEMS

One of the most significant advancements in cyber security is the incorporation of honey pots into SIEM systems. An organization's security posture may be better understood with the use of SIEM systems, which aggregate and analyse alarms and logs from various security solutions. By including honey pots, which function as decoy systems, SIEM systems are able to get enhanced data streams that provide valuable insights into the behaviour of attackers. Anomaly detection, incident response, and the overall security architecture are all improved by this mutually beneficial interaction. A. Use of Honey pots to Collect Data for SIEM Systems Honey pots are ideal for recording extensive information on harmful actions, such as the methods used by attackers, vulnerabilities that were exploited, and the payloads that were sent.

[6] Integration with other security solutions, including firewalls, intrusion detection systems (IDS), and endpoint protection platforms, allows these logs to be aggregated in a SIEM system. By collecting all of this data, SIEM systems can correlate network events and look for trends that might indicate an attack is happening or is about to happen. [6] Honey pot data provides a significant edge in identifying sophisticated attacks. For example, if a honey pot is being used often, it might indicate that someone is trying to find weaknesses or conduct reconnaissance. When the SIEM system detects such actions, it might mark them as high-priority events, requiring swift attention. Also, honey pots are decoys, so attackers can only show their strategies in a controlled setting, reducing the

danger to live systems. B. Real-Time Alerts and Event Correlation the improved capacity for event correlation is one of the main advantages of combining honey pots with SIEM systems. Honey pot data is processed by SIEM systems with other security events in order to reveal correlations between occurrences that at first glance seem to be unrelated. A concerted assault might be shown, for instance, by a correlation between an increase in honey pot login attempts and suspicious traffic reported by a firewall. By using a comprehensive approach, security professionals are better able to tackle intricate threats.

One of the most important features of SIEM systems that are enhanced by honey pot integration is real-time alerting. Notifications are generated by the SIEM platform and given a priority according to the seriousness and effect of the threats detected by the honey pots. By minimising the possibility of false positives and guaranteeing prompt response, these notifications allow security personnel to concentrate on the most essential situations. Honey pots increase the granularity of these alerts by providing extensive logs, which improve event investigation and action by giving contextual information. Section C. Strategies for Execution It takes meticulous preparation and execution to integrate honey pots with SIEM systems effectively. It is recommended to strategically place honey pots in areas of the network that are prone to malicious activity, such as inactive IP ranges or close to valuable assets like databases.

Their outputs need to be set up such that the SIEM platform can receive them directly via APIs or standardised log formats. This makes sure that other security products can easily integrate and process the ingested data. To make the most of the valuable insights offered by honey pots, it is recommended to establish custom alarm rules inside the SIEM system. As an example, the honey pot environment may be configured to produce warnings in response to certain actions, including multiple login attempts, unexpected command executions, or file uploads. With these individualised criteria, threat identification is more accurate and less background noise is introduced. D. Advantages of Merging There are a lot of benefits to integrating honey pots with SIEM systems. One way it does this is by shedding light on malicious actor actions that more conventional detection methods would miss. This, in turn, increases threat visibility. Honey pots record interactions that show the techniques and resources utilised by attackers, providing useful insight into new security risks. Second, by letting SIEM systems prioritise events using honey pot data, this connection enhances incident response. By providing contextual information, honey pots enable security teams to respond quickly and efficiently, reducing the likelihood of harm. The addition of threat intelligence and forensic analysis is another major perk. Organisations may learn what went wrong and how to stop attacks in the future with the aid of honey pots and the extensive logs they provide after an incident. Sharing the collected information with threat intelligence systems furthers the fight against cybercrime as a whole.

Integration Of Machine Learning And Artificial Intelligence With Honeypots

Incorporating honey pot systems with Machine Learning (ML) and Artificial Intelligence (AI) is a huge step forward in cyber security. Together, AI's predictive power and honey pots' interactive capabilities provide a powerful tool for better cyber threat identification, analysis, and mitigation. Honey pots are decoy devices that gather extensive information about how attackers behave. With the use of AI, this data can be analysed to spot trends, abnormalities, and potential entry points for future attacks, creating a defence system that is both proactive and adaptable. Analysis of Data and Pattern Recognition (A) Due to their design, honey pots capture the actions of malevolent actors, which naturally results in big databases. Payloads, logs of attacker interactions, and other forensic artefacts are all part of these databases. By analysing this data, AI models may detect trends that can reveal the methods, resources, and goals of an attack. To better understand and prevent certain kinds of attacks, machine learning algorithms may be taught to use

honey pot data from the past. Organisations may use this research to spot APTs and zero-day vulnerabilities, which are difficult for conventional rule-based detection systems to spot. Artificial intelligence systems are able to spot small data anomalies that differ from established patterns of valid behaviour by using unsupervised learning models. [7] Insights into these outliers allow security teams to react swiftly to new risks as they emerge. Situations like cloud infrastructures and IoT networks, where the attack surface is dynamic, greatly benefit from this feature.

B. Ongoing Security and Foreseeing Potential Dangers AI-powered honey pots go above and beyond traditional security measures by actively detecting and preventing potential dangers. By analysing data collected from honey pot interactions, predictive models may foresee possible attack situations and devise defence methods accordingly. Preventing attacks by securing susceptible systems is possible with the use of AI systems that analyse attacker tactics, methods, and procedures (TTPs). On top of that, honey pots with AI may analyse risks in real-time and adjust their setups accordingly. As a result, they will remain effective even when attackers change their tactics to avoid detection. A major benefit over static defence methods, this agility reduces downtime and lessens the effect of cyber attacks. C. Cyber security Use Cases There are a lot of real-world uses for honey pots that combine ML and AI. A significant one is the creation of all-encompassing threat intelligence.

Honey pots enabled by AI sift through attack vectors to provide useful information that may guide cyber security strategy as a whole. Improving the network's overall resilience, changing security rules, and honing intrusion detection and prevention technologies are all made possible by this knowledge. Anomaly detection is another important use. False positives or overlooked dangers are common outcomes of traditional systems' reliance on predetermined rules to detect hostile actions. This shortcoming is overcome by anomaly detection models powered by AI, which learn from both historical and real-time data to identify suspicious actions with more precision. One example is how AI-powered honey pots, when connected with SIEM systems, may assist prioritise incidents by recognizing high-risk occurrences and giving context. D. Results and Advantages Honey pots may reap several rewards when used with AI and ML. Shorter reaction times are among the most notable.

Faster threat mitigation is made possible by AI systems that automate honey pot data processing and initiate instantaneous responses based on specified criteria. If we want to keep cyber events to a minimum, we need to respond quickly. The accuracy of identifying and reacting to APTs is further improved by honey pots that are supplemented with AI. Because of their stealthy and targeted nature, these threats need sophisticated analytical tools to detect. The sophisticated patterns linked to these dangers are easily detected by machine learning models built on honey pot data. The defence systems get stronger as time goes on because these models keep getting better via iterative learning.

V. COMPREHENSIVE BENEFITS OF HONEYPOTS IN CYBERSECURITY FRAMEWORKS

Honey pots have several uses in cyber security frameworks, and when integrated they improve the efficiency and efficacy of threat analysis, response, and detection. Organisations may get a better understanding of the strategic significance of these advantages in different areas by combining them into a unified framework. Powerful New Tools for Identifying Potential Dangers Honey pots are great at spotting new attack patterns, zero-day vulnerabilities, and advanced persistent threats (APTs) those more conventional systems could overlook. [1, 6] A honey pot is a dynamic environment that may reveal an attacker's tactics, methods, and procedures (TTPs), in contrast to a signature-based detection tool. Honey pots allow for the analysis of botnet operations without endangering operational assets, and they are particularly useful for identifying Distributed Denial of

Service (DDoS) assaults. (A) Thorough Forensic Examination Honey pots collect useful forensic information by recording malicious interactions, attacker instructions, and payloads. Systems like Intrusion Detection and Prevention Systems (IDPS) may benefit from these data points by improving their detection algorithms, which in turn provide insights into the methodology of threat actors. For example, hackers might learn about potential security holes in an organization's infrastructure by analysing malware that has been caught in a honey pot.

Section B. Real-Time Threat Analysis Honey pots collect information that goes beyond only detecting threats at the moment. Detailed assessments of attacker behaviours and Indicators of Compromise (IOCs) may be transmitted across SIEM systems and external threat intelligence platforms. (2), (3) this makes it easier for organisations to work together on cyber security and helps them stay ahead of new threats. C. Efficient Distribution of Resources Honey pots alleviate the strain on major security measures by redirecting hostile traffic away from operating systems, allowing them to prioritise legal traffic. (1), (2) As a result, the system as a whole runs more smoothly and false alarms are less likely to create problems. To lessen the load on live systems, a honey pot set up in the cloud, for instance, may block brute-force attacks.

Taking Precautions and Being Flexible Intelligent honey pots that include AI and ML allow for adaptive reactions and predictive analytics. (1), (2) Honey pots may adapt their setups on the fly to counter advanced attacks because to these features, which enable them to mimic changing attack situations. For example, honey pots driven by AI may detect and block ransom ware efforts by identifying patterns used in the early stages of encryption. E. Use in a Variety of Settings Honey pots have a wide range of potential uses due to their adaptability. Honey pots are used in industrial control systems to analyse targeted assaults in a safe setting by replicating operational situations. They keep an eye out for suspicious activity in cloud infrastructure communications, such attempts at unauthorized access or threats from within the system. These diverse use cases showcase their versatility, allowing them to be used in both traditional IT networks and specialised settings.

Limitations And Challenges Of Integrating Honeypots With Cybersecurity Tools

Even though there are many benefits to integrating honey pots with SIEM, Intrusion Detection and Prevention Systems (IDPS), and SOAR platforms, there are also some limitations and challenges that need to be considered for the integration to work. Data Deluge and the Difficulty of Management Existing data processing capacities inside IDPS, SIEM, and SOAR systems might be overwhelmed by the massive amounts of logs and interaction data generated by honey pots. [2, 6] Security teams could have trouble detecting and responding to threats quickly enough if they don't have effective methods for filtering and prioritising data.

Section A. Maintenance Expenses and Resource Distribution Honey pots are expensive to set up and keep running since they need certain hardware, software setups, and constant attention. [4], [8] Organisations with limited cyber security funds or manpower may find that integrating honey pots with existing systems, such as IDPS or SOAR, worsens resource pressure. B. the Danger of Honey pot Exposure and Avoidance If an attacker is skilled enough, they may learn to spot honey pots and use that information to launch assaults that target particular decoys. Such cases may weaken the overall resilience of the cyber security system and make honey pots less effective [5, 9].

Section C. Harmony with Company Goals For honey pot integration to be successful, the organization's operational objectives and security requirements must be well aligned. Ineffective threat detection and mitigation may result from honey pots that are not strategically placed or whose outputs are not configured to assist IDPS, SIEM, and SOAR processes. Concerns about scalability and adaptability (D) Making

sure honey pots can scale and adapt to different situations is becoming harder as networks become more sophisticated. Incorporating honey pots into cloud infrastructures, IoT networks, or industrial control systems necessitates customised settings that may not perfectly mesh with preexisting technologies such as SIEM or SOAR. E. Possibility of Moral and Lawful Concerns There may be ethical and legal issues with honey pots if they unintentionally collect data from good users or don't follow data privacy rules.

(2) And (7) their implementation and integration are already complicated enough without having to worry about complying with legal norms in different countries. To overcome these obstacles, you need to strike a balance between reactive and proactive measures, such as thorough planning, sophisticated analytics, and frequent adjustments to honey pot settings and integration tactics. Organisations may fully use the power of honey pots to bolster their cyber security posture by addressing these constraints.

VI. CONCLUSION

A significant step forward in current threat detection, analysis, and response tactics is the incorporation of honey pots into cyber security frameworks. [6] Honey pots provide a controlled environment for isolating and analysing harmful actions. They operate as decoy systems, which helps organisations, enhance their defenses and get insights into attacker techniques. (2), (6) Security infrastructures are made much more resilient and adaptable when honey pots are integrated with other tools like firewalls, Intrusion Detection and Prevention Systems (IDPS), Security Information and Event Management (SIEM) systems, and Security Orchestration, Automation, and Response (SOAR) platforms).

Honey pots are already successful against sophisticated and ever-changing cyber attacks, but when combined with AI and ML, they acquire proactive capabilities like threat prediction and dynamic defence adaption. Not only does this integration lighten the load on main security systems, but it also gives organisations actionable threat information, so they can react quickly and effectively to new threats. Industrial control systems, cloud computing, and workplace networks are just a few of the many real-world uses for honey pots, proving their usefulness and adaptability. Honey pot installations provide organisations with valuable data that may be used to improve detection rules, allocate resources more effectively, and foster a more collaborative and informed global cyber security ecosystem. Honey pots, when strategically placed, will continue to be an essential part of effective and flexible security measures, even as cyber threats develop and change. 2 and 9

REFERENCES

1. A. Abdou, R. Sheatsley, Y. Beugin, T. Shipp, and P. McDaniel, “HoneyModels: Machine Learning Honey pots,” MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM). IEEE, pp. 886–891, Nov. 29, 2021. doi: 10.1109/milcom52596.2021.9652947. Available:
2. M. Valicek, G. Schramm, M. Pirker, and S. Schrittwieser, “Creation and Integration of Remote High Interaction Honey pots,” 2017 International Conference on Software Security and Assurance (ICSSA). IEEE, pp. 50–55, Jul. 2017. doi: 10.1109/icssa.2017.21. Available:
3. M. S. Rana and M. A. Shah, “HONEYPOTS IN DIGITAL ECONOMY: AN ANALYSIS OF INTRUSION DETECTION AND PREVENTION,” IET Conference Proceedings, vol. 2021, no. 4. Institution of Engineering and Technology (IET), pp. 91–98, Oct. 12, 2021. doi: 10.1049/icp.2021.2415. Available:
4. K. D. Yesugade, M. S. Avinash, N. S. Satish, S. C. Sandeep, S. Malav. “Infrastructure Security Using IDS, IPS and Honey pot.” International Engineering Research Journal (IERJ) Volume 2 Issue 3 Page 851-855, 2016, ISSN 2395-1621, Available:
5. Feng Zhang, Shijie Zhou, Zhiguang Qin, and Jinde Liu, “Honey pot: a supplemented active defense system for network security,” Proceedings of the

8th International Scientific and Practical Conference of Students, Post-graduates and Young Scientists. Modern Technique and Technologies. MTT'2002 (Cat. No.02EX550). IEEE, pp. 231–235. doi: 10.1109/pdcat.2003.1236295. Available:

6. V. Mahajan and S. K. Peddoju, "Integration of network intrusion detection systems and honey pot networks for cloud security" 2017 International Conference on Computing, Communication and Automation (ICCCA). IEEE, pp. 829–834, May 2017. doi: 10.1109/ccaa.2017.8229911. Available:
7. K. E. Silaen, M. Meyliana, H. L. H. S. Warnars, H. Prabowo, A. N. Hidayanto, and M. S. Anggreainy, "Usefulness of Honey pots Towards Data Security: A Systematic Literature Review," 2023 International Workshop on Artificial Intelligence and Image Processing (IWAIIP). IEEE, pp. 422–427, Dec. 01, 2023. doi: 10.1109/iwaiip58158.2023.10462777. Available:
8. T. Alyas et al., "Multi-Cloud Integration Security Framework Using Honey pots," Mobile Information Systems, vol. 2022. Hindawi Limited, pp. 1–13, Aug. 17, 2022. doi: 10.1155/2022/2600712. Available:
9. H. Lajwanti, F. Urooj, W. Muhammad, S. Mehwish. (2024). "Enhancing Cyber security Through Honey pot-Based Intrusion Detection and Prevention Systems." 2nd International Multidisciplinary Conference on Emerging Trends in Engineering Technology2024 (2nd IMCEET-2024), pp 149-154, Oct 2024, Available:
10. Maroš Cerge ˇ ˇt, Jan Hudec "Cyber-Security Threats Origins and their ´ Analysis" Acta Polytechnica Hungarica, vol.10, nr.9. 2023