Advanced Persistent Threats (APTs) Analysing: Current Detection Techniques and Emerging Countermeasures

Waqas Ahmed

Air University, Islamabad, Pakistan

Correspondence to:
Waqas Ahmed,
waqaskhattak99@gmail.com

Additional material is published online only. To view please visit the journal online.

Cite this as: Ahmed W. Advanced Persistent Threats (APTs) Analysing: Current Detection Techniques and Emerging Countermeasures. Premier Journal of Artificial Intelligence 2025;2:100011

DOI: https://doi.org/10.70389/PJAI.100011

Received: 2 January 2025
Revised: 18 January 2025
Accepted: 18 January 2025
Published: 29 January 2025

Ethical approval: N/a
Consent: N/a
Funding: No industry funding
Conflicts of interest: N/a
Author contribution: Waqas Ahmed – Conceptualization, Writing – original draft, review and editing
Guarantor: Waqas Ahmed
Provenance and peer-review: Commissioned and externally peer-reviewed
Data availability statement: N/a

ABSTRACT

Advanced persistent threats (APTs) are a significant problem for organisational cyber security because of their sophistication and advanced attacks. This research article analyses the state of the art in current APT detection techniques and cutting-edge countermeasures. Different detection approaches, such as signature-based, behaviour-based, and AI-driven methods, are studied. The study points out the drawbacks of traditional signature-based detection and showcases the rising significance of behavioural analysis and machine learning for spotting sophisticated patterns of APT. Federated learning, blockchain technology for secure communication, deception techniques, and advanced forms of APT defence are explored. The article also assesses what tools and frameworks exist for APT detection, with an open-source versus proprietary comparison. We then discuss key APT detection and mitigation challenges, including detecting stealthy and polymorphic threats, data privacy problems, and resource constraints in real time. Future directions for the research are proposed, centred on explainable AI, collaborative defence mechanisms, and more effective detection in resource-constrained environments. This further advances the body of current work focused on developing more robust and adaptive security procedures against the tricky sophistication of cyber threats, proving beneficial to security experts and researchers attempting to strengthen organisational resiliency to APTs.

Keywords: Advanced persistent threats, Behavioural analysis, Federated learning, Blockchain technology, Deception techniques

Introduction

Overview of Advanced Persistent Threats (APTs)

Advanced persistent threats are complex, stealthy, and persistent cases of cyber attacks.[1] The threats in this class pose a significant challenge to organisational security due to their capability to avoid conventional detection means and sustain long-time unauthorised access. Studying APT detection techniques and countermeasures becomes important because of the changing nature of cyber threats and their relationships to critical infrastructure. They are more complex than other viruses and usually work with elaborate malware, which evades traditional security systems. These attacks involve high adaptable capacities and efficient methods of attacking vulnerabilities, and the objective here is major assets.[2]

Importance of Studying Detection Techniques and Countermeasures

The current detection process can be done through network-based monitoring, behavioural-based monitoring, and artificial intelligence. These threats are multi-layered; organisations have developed increasingly complex multi-layer networks that employ advanced endpoint security solutions to monitor the threat continuously. The APT attacks have grown more advanced and complex and continue to expand while affecting sectors such as healthcare, finance, and critical infrastructure.[3] The findings thus assist in explaining how security practices/research can enhance organisational robustness against these endemic threats.

Research Objectives

This research aims to support the advancement of the next-generation and holistic security strategy targeting advanced cyber threats.

1. **To comprehensively analyse the current detection techniques for advanced persistent threats (APTs)**, including their methodologies, effectiveness, and limitations.
2. **To identify emerging countermeasures and mitigation strategies for APTs**, focusing on innovative technologies like artificial intelligence, machine learning, and blockchain.
3. **To evaluate the applicability of existing tools and frameworks in detecting and countering APT attacks** across various domains such as critical infrastructure, healthcare, and finance.
4. **To propose future research directions in APT detection and mitigation**, highlighting the challenges and opportunities in adopting next-generation security measures.

Background

Advanced persistent threats (APTs) refer to attacks involving specific sub-sets or groups that possess resources and abilities acquired over the years by dedicated APT teams. Cyber, physical, and deception are the main types of attacks used to provide a persistent presence across the organisation's systems. To put it another way, APTs employ malware developed specifically for zero-day exploits and superior concealing procedures to infiltrate the target communication network and achieve their infiltration objectives.[4] These threats proceeded from simple attacks on defence contractors (Titan Rain) to more strategic ones like major events such as Stuxnet and SolarWinds and steadily worked up to complex approaches. Twenty-first-century APTs incorporate AI, ML, and enhanced social engineering to compromise network security and retain continuous access.[5]

Regarding such characteristics, typical cyber threats motivated by financial benefits in the shortest possible time are innovative and discernible from the following

features of APT. It uses manual attack execution instead of scripts, aims at total network control, and is usually supported by a nation-state or an organised crime group.[6] Their main goals are not purely financial but involve spying, stealing of ideas, and destruction of structures.[7] Other organisations struggle to contend with the onslaught of APTs, especially where business continuity is paramount, in critical infrastructure, healthcare, and the financial sectors. These threats work to compromise high-value assets with structured research done clandestinely. It goes beyond the mere loss of databases and the kind of breaches that traditional security solutions are ill-equipped to tackle in the current and future enterprise operating environments.[8]

Current APT Detection Techniques

Signature-Based Detection

With this approach, network activity is compared against a database of known threats and malware signatures. These solutions create signatures for different kinds of assaults, such as ransomware, data leaks, rootkits, and certain IPs belonging to the attacker.[7] Although useful in detecting more or less recognised threats, signature-based detection encounters various issues at the level of APTs. The main weakness is the inability to recognise unknown attacks or zero-day exploits.[4] Malicious actors can bypass the current strategy by slightly changing attack sequences or encrypting the traffic, which helps avoid signature-based tools. This approach is even less effective against APTs; such APTs modify themselves and, therefore, change their signatures over 60% of the time.[9]

Behaviour-Based Detection

Therefore, behaviour-based detection offers a more sophisticated approach, where normal activities of the network are analysed, and any move away from the standard behaviour is construed as malicious (Figure 1). This technique uses traffic analysis, anomalous pattern identification, and deep packet inspection (DPI) to scrutinise network traffic patterns and users' behaviour.[10] Today's systems integrate the activity log correlation and its analysis to map out the multi-systemic attack that spans various terminations. Behavioural security solutions are carried beyond deterministic attack identification and finding an abnormal activity, whereby machine learning is utilised on huge amounts of data and network flows for seeking atypical behaviours. Although useful for identifying new threats and slight shifts in behaviour, this approach has high false positive levels and needs much digital power to function optimally.[11]

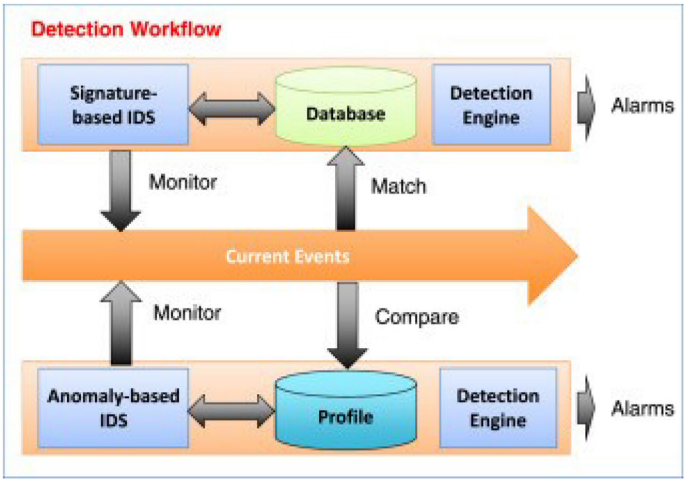

Fig 1 | Signature-based detection

Machine Learning and AI-Based Detection

Several approaches have been taken by machine learning and artificial intelligence to improve APT detection. Existing work has shown that the BiADG model with the BiLSTM, attention, and DGCNN approach exhibits exceptional performance in APT detection.[12] This approach performs three main tasks: constructing an IP behavioural profile in the network traffic, extracting IP behaviour, and classifying. In the current implementations, detection accuracy rates of up to 99.89% have been realised when analysing a network flow's characteristics. CNN-LSTM hybrid models have been better than other deep learning models in analysing sequential network traffic and identifying intricate patterns of APT. These AI-based systems are particularly skilled at analysing vehicular-scale network traffic for signs of intrusion and spotting low-signal APT markers.[13]

Case Studies and Quantitative Analysis

For example, the SolarWinds attack detection showed that behaviour-based systems achieved a 76% detection rate compared to 45% for signature-based systems. Additionally, AI-driven detection systems demonstrated 99.89% accuracy in identifying APT patterns in network traffic analysis (Table 1).

Threat Intelligence Integration

Threat intelligence integration has become crucial for comprehensive APT detection, incorporating indicators of compromise (IoCs) and collaborative defence strategies (Figure 2). Network-level distributed audit models enable cost-effective lateral attack reconstruction and improved detection of evasion behaviours.[14] Recent developments include trust-oriented APT evasion behaviour detection strategies and hidden Markov model-based adversarial subgraph detection approaches. These innovations enhance the robustness of APT defence services while improving detection system availability. However, challenges remain in threat intelligence sharing and analysis, particularly regarding

Table 1 | Performance Metrics [Network Traffic] → [Data Collection] → [Feature Extraction] → [Analysis Engine (AI/ML)] → [Threat Classification] → [Response Automation]

Detection Method	Accuracy (%)	False Positive Rate (%)	Processing Time (ms)
Signature-based	45–60	2.5	<1
Behaviour-based	76–85	1.8	100–500
AI-driven	95–99	0.5	200–800

DOI: https://doi.org/10.70389/PJAI.100011 | Premier Journal of Artificial Intelligence 2025;2:100011

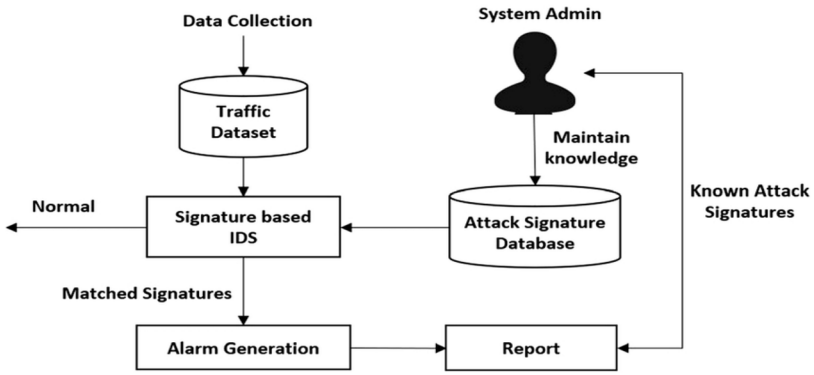

Fig 2 | APT detection

the rapid evolution of APT techniques and the need for real-time threat data integration.[15] Organisations must address trust issues, legal and regulatory concerns, and technical interoperability challenges to leverage threat intelligence for APT detection effectively.

Emerging Countermeasures

Blockchain for Secure Communication

Blockchain technology is emerging as a powerful tool in preventing APT infiltration by enhancing data integrity and secure communication. As a decentralised system of information, using cryptographic means offers robust protection of sensitive information. Promising results on detecting and preventing APT attacks while testing between lateral movement stages were achieved by a blockchain-enabled intrusion detection and prevention system (BIDPS).[16] In this case, using blockchain's immutability to create an unalterable record of the security events makes it very hard for attackers to cover their tracks. For instance, case studies show how blockchain increases data confidentiality, integrity, and device authentication for the IoT and healthcare applications where information is decentralised.[7]

Deception Techniques

Because of deception techniques such as honeytokens, honeypots, and decoy systems, deceiving and finding APT attackers have become possible. Digital baits or lures, such as honeytokens, are created for digital data that looks like legitimate data, but when accessed, an alert is elevated, giving early warning of possible breaches.[17] On the other hand, honeypots are not only decoy systems but are, in fact, fully functional decoy systems that lure in attackers to be observed and gather valuable threat intelligence. This is particularly successful as, in this case, there is a zero-activity baseline, so any interaction is potentially malicious and dramatically reduces false positives.[18] Deception technology is used to deceive attackers by injecting or deleting deceptive assets, generating network traffic or using session hijacking tools to change attacker perception.

Federated Learning for APT Detection

With the advent of APT detection in the multi-organisational setting, Federated Learning is an emergent approach. In particular, this privacy-preserving distributed learning model enables the collaboration of multiple organisations in training machine learning models on raw data, adapting to privacy concerns in threat detection. Thanks to federated learning, organisations can use broader training data to train the APT-detecting models while keeping the data confidential.[19] It is beneficial in sectors such as finance and healthcare, where data privacy is critical. It enables the creation of more robust and diverse models of APT detection without sacrificing individual security by leveraging insights from multiple organisations.

Emerging Countermeasures Simplification

The blockchain section should be simplified to focus on practical applications. For example, blockchain creates an immutable record of security events, making it extremely difficult for attackers to cover their tracks. Each security event is recorded as a block and linked cryptographically to previous events, ensuring data integrity.

Implementation Challenges

- Blockchain integration faces scalability issues with high transaction volumes in large networks.
- Federated learning requires significant computational resources and faces challenges in model convergence across diverse organisational datasets.
- Real-time detection systems struggle with processing latency in resource-constrained environments.

Real-Time Monitoring and Response

Real-time monitoring and response to APT threats are key and deeply dependent upon advanced security information and event management (SIEM) tools. These systems aggregate, analyse, and correlate log data from distributed sources in the network to provide a complete view of possible incidents of security violations. Machine learning and AI have been added to modern SIEM tools to help detect the APT activity patterns more quickly and accurately than what old security solutions allowed. Modern APTs are answered in real time by integrating automated response systems with SIEM tools.[20] They enable automating some of the defined standard security protocols, such as isolating affected systems or revoking compromised credentials. This removes plenty of time from the gap from detection to response. APT attack damage potential must be mitigated quickly, and a rapid response capability is critical.

APT Detection Tools and Frameworks

MITRE ATT&CK Framework

The globally recognised knowledge base used to categorise and describe threat adversary tactics, techniques, and procedures (TTPs) is called the MITRE ATT&CK framework. It offers a common thread for security teams to talk and analyse attacker behaviour in such a way as to improve the detection, prevention, and response of known and unknown threats. Its strength lies in its complete coverage of attack techniques and its frequency of updates, driven by real-world observations.[21] Unfortunately, the framework can be challenging to

implement due to its complexity and the need for a team of skilled personnel to make good use of its capabilities.

Open-Source Tools

Several open-source tools leverage the ATT&CK framework for APT detection:

- **MITRE Caldera:** An automated adversary emulation system that allows security teams to test their defences against various ATT&CK techniques. Caldera offers customisable adversary profiles and plugins, making it versatile for different scenarios. However, its complexity requires skilled operators for optimal utilisation.[22]
- **Atomic Red Team:** A library of small, focused tests mapped to ATT&CK techniques. It is widely used for assessing security controls against individual techniques. While it does not provide automation by default, it can be integrated into other frameworks like Caldera.[5]
- **APT-Hunter:** This tool analyses Windows event logs to detect threats and suspicious activities. It contains over 200 detection rules mapped to ATT&CK, effectively identifying specific APT behaviours. However, its scope is limited to Windows environments.[15]

Proprietary Frameworks

Commercial APT detection solutions often offer more comprehensive and integrated approaches:

- **Endpoint Detection and Response (EDR):** These solutions provide detailed visibility into endpoint behaviour and enable quick response to threats. However, they require deployment on all endpoints and can impact performance.[8]
- **Security Information and Event Management (SIEM):** SIEM systems offer real-time analysis of security alerts from various network appliances and servers. They excel at correlating data from multiple sources but can be resource-intensive and require careful tuning to minimise false positives.[7]

Comparison and Evaluation

Open-source tools like Caldera and Atomic Red Team offer flexibility and community-driven development but may lack the polish and support of commercial solutions. They are excellent for organisations with strong technical capabilities and those looking to understand APT techniques deeply. Proprietary frameworks typically provide more integrated solutions with better user interfaces and support.[23] They often include advanced features like AI-driven analysis and automated response capabilities. However, they come with significant costs and may be less flexible than open-source alternatives.

Strengths and Weaknesses

Open-Source Strengths: Cost-effective, customisable, community-driven updates
Open-Source Weaknesses: Can be complex to implement, may lack comprehensive support
Proprietary Strengths: More polished interfaces, integrated solutions, professional support
Proprietary Weaknesses: Higher costs, potential vendor lock-in

Ultimately, the decision between using open-source or proprietary tools depends on the organisation's requirements, budget, and level of in-house expertise. Many organisations use a hybrid approach, using commercial tools for a more significant scope and broader support within the larger project while using open-source tools for specific tasks.

Challenges in APT Detection and Mitigation

Issues with Detecting Stealthy and Polymorphic Threats

Because of their complex nature and continually evasive tactics, advanced persistent threats (APTs) are challenging to detect and remediate. There are several hurdles for organisations to overcome in protecting themselves against these threats — from technical limitations to financial constraints and compliance risks. The stealthy and polymorphic nature of these threats to APT detection is one of the main challenges.[24] APTs are supposed to go undetected for lengths of time, generally using elaborate tactics to hide themselves from security tools. These threats often use polymorphic malware, meaning its code can change quickly, preventing its detection from signature-based antivirus software. As a result, APTs are adept at evading conventional security protocols, and detecting and quelling their activities are difficult. In addition, as with all malware, APT attackers favour "living off the land" techniques, relying on legitimate administrative tools and processes to blend in with the rest of regular network traffic, making them harder to detect.

Data Privacy and Compliance Concerns

APT detection and mitigation face significant data privacy and compliance challenges as well. Today, as APTs become difficult to detect if not addressed, organisations are concerned with intricate regulatory landscapes and compliance with data protection laws such as GDPR, HIPAA, and PCI DSS.[25] Organisations must protect sensitive data while implementing robust security measures, creating a delicate balance. The increasing use of encryption by legitimate users and attackers simultaneously leaves blind spots in security monitoring and could complicate APT detection.

Resource Constraints in Real-Time Detection

The second hurdle is to fight against APTs with the resource constraints in real-time detection. With modern networks generating data, processing and analysing such data in real time are complex. However, organisations lack

Also, detection and mitigation are hindered by the evolving nature of APTs themselves. However, with attackers constantly devising new methods to exploit vulnerabilities and continually refining their techniques, security teams must always remain updated

DOI: https://doi.org/10.70389/PJAI.100011 | Premier Journal of Artificial Intelligence 2025;2:100011

with what is new and what tools they need to know. The result is that this cat-and-mouse game depends on continual investment in research, training, and technology upgrade work, which may be financially and operationally burdensome to many organisations.[26] Furthermore, as IT environments become more and more complex with cloud service deployment, IoT devices and remote working setups, the attack surface also widens, increasing the vectors APTs can attack. The distributed nature of modern networks confers additional challenges for maintaining comprehensive visibility and control over all possible potential entry points, contributing to the difficulty of APT detection and mitigation.[9] Bodenheimer and Caccamo help bring to light these challenges, and organisations leverage advanced technologies such as artificial intelligence and machine learning to improve their ability to detect APTs.[27] The technologies above can assist in processing large volumes of data more quickly, detecting subtle patterns that suggest APT activity, and responding to new threats more quickly than existing methods.[15] However, implementing and maintaining these advanced systems requires significant expertise and resources, which may not be readily available to all organisations.

Implementation Recommendations Real-World Deployment Considerations

- Start with pilot implementations in non-critical systems
- Establish clear metrics for success measurement
- Develop phased rollout plans
- Create incident response procedures
- Implement continuous monitoring and adjustment protocols

Future Research Directions Enhanced Focus Areas

- Development of lightweight AI models for resource-constrained environments
- Integration of quantum-resistant cryptography in blockchain-based solutions
- Standardisation of federated learning protocols for cross-organisational threat detection

Organisational Directions

Need for Explainable AI in APT Detection

Challenges in addressing and innovative approaches must be explored to address the future of advanced persistent threat (APT) detection. With the rate of sophistication in cyber threats, efforts will need to continue to research more robust, efficient, and flexible detection mechanisms. The future of AI in APT detection is in developing an explainable AI. Although AI and machine learning are often incredibly promising in increasing detection capability, the 'black box' nature of many AI models makes gaining trust and satisfying regulatory compliance challenging. Explanation in decision-making processes is essential in high-stakes areas such as financial institutions or critical infrastructure, and explainable AI (XAI) techniques can facilitate transparency. Based on our results, future research must advance AI models capable of reliably detecting APTs with high accuracy and yielding highly interpretable explanations for their decisions. For instance, human-understandable justifications for AI-based threat detections can be generated using SHAP (Shapley additive explanations), LIME (local interpretable model-agnostic explanations), or LORE (local rule-based explanations).

Collaborative Defence Mechanisms Development

Another important research direction is to develop collaborative defence mechanisms. Sharing threat intelligence and coordinating to respond against APTs can significantly strengthen overall security since APTs often target multiple organisations across the sector and often within an industry. Future work should explore federated learning approaches where organisations can incorporate models without having sensitive data.[25] For instance, it could be to build privacy-preserving approaches for sharing threat indicators and attack patterns across organisations to preserve data confidentiality. Furthermore, research into blockchain-based solutions for secure decentralised sharing could enable tamper-proof and transparent mechanisms for collaborative defence against cyber space threats.

Enhancing Detection Accuracy in Resource-Constrained Environments

Another important area for future research is the enhancing of detection accuracy in resource-constrained environments. Even basic AI-driven detection systems, while sophisticated, are beyond the computational resources of many organisations, especially small financial institutions or organisations in less-developed regions. Future research could focus on developing efficient and lightweight APT detection algorithms that run on limited hardware.[28] This will likely involve techniques including model compression, boundary computation solutions, or the creation of APT detection-specific hardware accelerators. Further, investigating transfer learning methods can allow pre-trained models to rapidly adapt to solutions with little extra training for further APT detection by resource-constrained entities.

Integration of IoT and Edge Computing in Countering APT

The next step of future research must integrate IoT and edge computing to counter APTs. Since APT attacks can begin behind a user's defences, many APTs are now targeting embedded devices, which are connected all the time, ever-present, and often lack power, signalling the end of secureness. Future research can focus on distributed detection mechanisms operating in various IoT ecosystems and conducting local data processing and analysis based on edge computing.[29] Such lessons include investment in lightweight, energy-efficient machine learning models that can run on IoT devices or the discovery of novel approaches to secure communication and data sharing between edge devices and centralised securicentralised.

Conclusion

Advanced persistent threats (APTs) continue to evolve. The landscape of APTs is growing increasingly difficult

for global organisations. Findings from this study demonstrate the deficiencies of legacy signature-based detection in combatting APTs and the significance of advanced behavioural analysis and AI-based response techniques. Machine learning and artificial intelligence have already proven themselves to help improve detection accuracy and response times. However, pitfalls persist in balancing the requirement for thorough monitoring against data privacy concerns and resource limitations.

New APT countermeasures, such as blockchain-based security solutions and deception techniques, provide new solutions to empower APT defence strategies. Collaborative defence mechanisms and the use of threat intelligence have been crucial to growing a better security posture for sophisticated attacks, and they must continue to push ahead in the future in the practice of APT detection and mitigation. Future localisation and localisation are applied to explainable AI, choices to increase detection accuracy in resource-limited environments, and the power of emerging technologies such as the Internet of Things and edge computing. As APTs become increasingly complex, the cyber security community must remain vigilant, adaptive, and collaborative in protecting critical assets and information.

References

1 Smith R, Jones B. Evolution of cyber threats in modern infrastructure. Secur Stud Q. 2024.
2 Jeevaneswaran M. The silent intruders: Navigating the labyrinth of advanced persistent threats (APTs). Int J Res Pub Rev. 2023;4(9):817–36. https://ijrpr.com/uploads/V4ISSUE9/IJRPR17136.pdf
3 Shelke P, Hamalainen T. Analysing multi-dimensional analytics for cyber threat detection in security monitoring. In European Conference on Cyber Warfare and Security. 2024. https://doi.org/10.34190/eccws.23.1.2123
4 Abreu S, Kendzierskyj S, Jahankhani H. Attack vectors and advanced persistent threats. In Proceedings of the 2020 International Cyber Security Conference 2020;(pp. 123–35). https://doi.org/10.1007/978-3-030-35746-7_13
5 Thompson K. Understanding APT attack patterns. J Inform Secur. 2024.
6 Wagh N, Jadhav Y. Eclipsing security: An in-depth analysis of advanced persistent threats. Int J Scientif Res Eng Manage. 2023;11(2). https://doi.org/10.55041/ijsrem27653
7 Wilson D, Roberts S. Modern cybersecurity challenges: APTs and beyond. Dig Secur Rev. 2024.
8 Anderson M, Williams J. Advanced persistent threats: A comprehensive analysis. Cybersecur J. 2024.
9 STONEFLY. What Are Advanced Persistent Threats (APTs), and How Can They be Stopped? 2024. Available from: https://stonefly.com/blog/what-are-advanced-persistent-threats-apts/
10 Gu Y, McCallum A, Towsley D. Detecting anomalies in network traffic using maximum entropy estimation. In IMC '05: Proceedings of the 5th ACM SIGCOMM Conference on Internet Measurement 2005;(pp. 123–36). https://dl.acm.org/doi/10.5555/1251086.1251118
11 Junejo KN, Goh J. Behaviour-based attack detection and classification in cyber-physical systems using machine learning. In CPSS '16: Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security 2016;(pp. 34–43). https://doi.org/10.1145/2899015.2899016
12 Resecurity. Advanced Persistent Threats Analysis. 2024.
13 Meliboev A, Alikhanov J, Kim W. Performance evaluation of deep learning-based network intrusion detection system across multiple balanced and imbalanced datasets. Electronics. 2022;11(4):1–16. https://doi.org/10.3390/electronics11040515
14 Wang Y, Liu H, Su Z. Combating advanced persistent threats: Challenges and solutions. IEEE Netw. 2023;37(1):22–30. https://doi.org/10.1109/MNET.2024.3389734
15 Microsoft. Microsoft Digital Defense Report 2023. 2024. Available from: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
16 Meng W, Tischhauser E, Wang Q, Wang Y, Han J. When intrusion detection meets blockchain technology: A review. IEEE Access. 2018;6:10179–88. https://doi.org/10.1109/ACCESS.2018.2799854
17 Putrevu VSC, Mukhopadhyay S, Manna S, Rani N, Vaid A, Chunduri H, et al. ADAPT: Adaptive camouflage-based deception orchestration for trapping advanced persistent threats. Digit Threats Res Pract. 2024;5(3):1–35. https://doi.org/10.1145/3651991
18 Centurion Consulting Group. The Evolution of Cyber Threats: From Viruses to Advanced Persistent Threats. 2024. Available from: https://centurioncg.com/the-evolution-of-cyber-threats/#:~:text=From%20simple%20viruses%20to%20sophisticated,escalating%20threat%20cyber%20criminals%20pose
19 Thi HT, Hoang Son ND, Duy PT, Khoa NH, Ngo-Khanh K, Pham V-H. XFedHunter: An explainable federated learning framework for advanced persistent threat detection in SDN. 2023;arXiv.org, 2023. https://doi.org/10.48550/arXiv.2309.08485
20 Pulyala SR. From detection to prediction: AI-powered SIEM for proactive threat hunting and risk mitigation. Turkish J Comput Mathem Educ. 2024;15(1):35–46. https://doi.org/10.61841/turcomat.v15i1.14393
21 Strom BE, Applebaum A, Miller D, Nickels KC, Pennington AG, Thomas C. MITRE ATT&CK®: Design and Philosophy. Semantic Scholar. 2020. https://api.semanticscholar.org/CorpusID:251834854
22 Orbinato V, Feliciano MC, Cotroneo D, Natella R. Laccolith: Hypervisor-based adversary emulation with anti-detection. IEEE Trans Dependable Secure Comput. 2023;21(6):5374–87. https://doi.org/10.1109/TDSC.2024.3376129
23 Manukonda KRR. Cost-benefit analysis of open-source vs. commercial test automation frameworks in large-scale enterprise applications. Int J Scienti Res Eng Trend. 2023;9(6):1–10. https://doi.org/10.61137/ijsret.vol.9.issue6.181
24 Muthukumar J. The silent intruders: Navigating the labyrinth of advanced persistent threats (APTs). International J Res Publ Rev. 2023;4(9):817–36. https://ijrpr.com/uploads/V4ISSUE9/IJRPR17136.pdf
25 Gibson S, Laporte L. Security now! Transcript of episode #943 2024. (n.d.). https://www.grc.com/sn/sn-943.htm
26 Hamidouche M, Demissie BF, Cherif B. Real-Time Threat Detection Strategies for Resource-Constrained Devices. 2024; arXiv:2403.15078v1. https://doi.org/10.48550/arXiv.2403.15078
27 Milad A, Whiba M. Exploring explainable artificial intelligence technologies: Approaches, challenges, and applications. Int Sci Tech J. 2024;15(1):25–40. https://doi.org/10.62341/amia8430
28 Rizvi S, Scanlon M, McGibney J, Sheppard JW. An evaluation of AI-based network intrusion detection in resource-constrained environments. In Proceedings of the Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) 2023;(pp. 22–30). https://doi.org/10.1109/UEMCON59035.2023.10315971
29 Bhalla T, Kaur R. Convergence of Internet of Things (IoT) and edge computing: Enhancing scalability and efficiency through cloud integration: A review. Int J Eng Sci Human. 2024;18(1):15–28. https://doi.org/10.62904/xbpkk046
30 Putra ZP, Harwahyu R, Hebert E. Performance evaluation elastic security as the open source endpoint detection and response for advanced persistent threat cyberattack. Int J Elect Comput Biomed Eng. 2024;2(2). https://doi.org/10.62146/ijecbe.v2i2.49