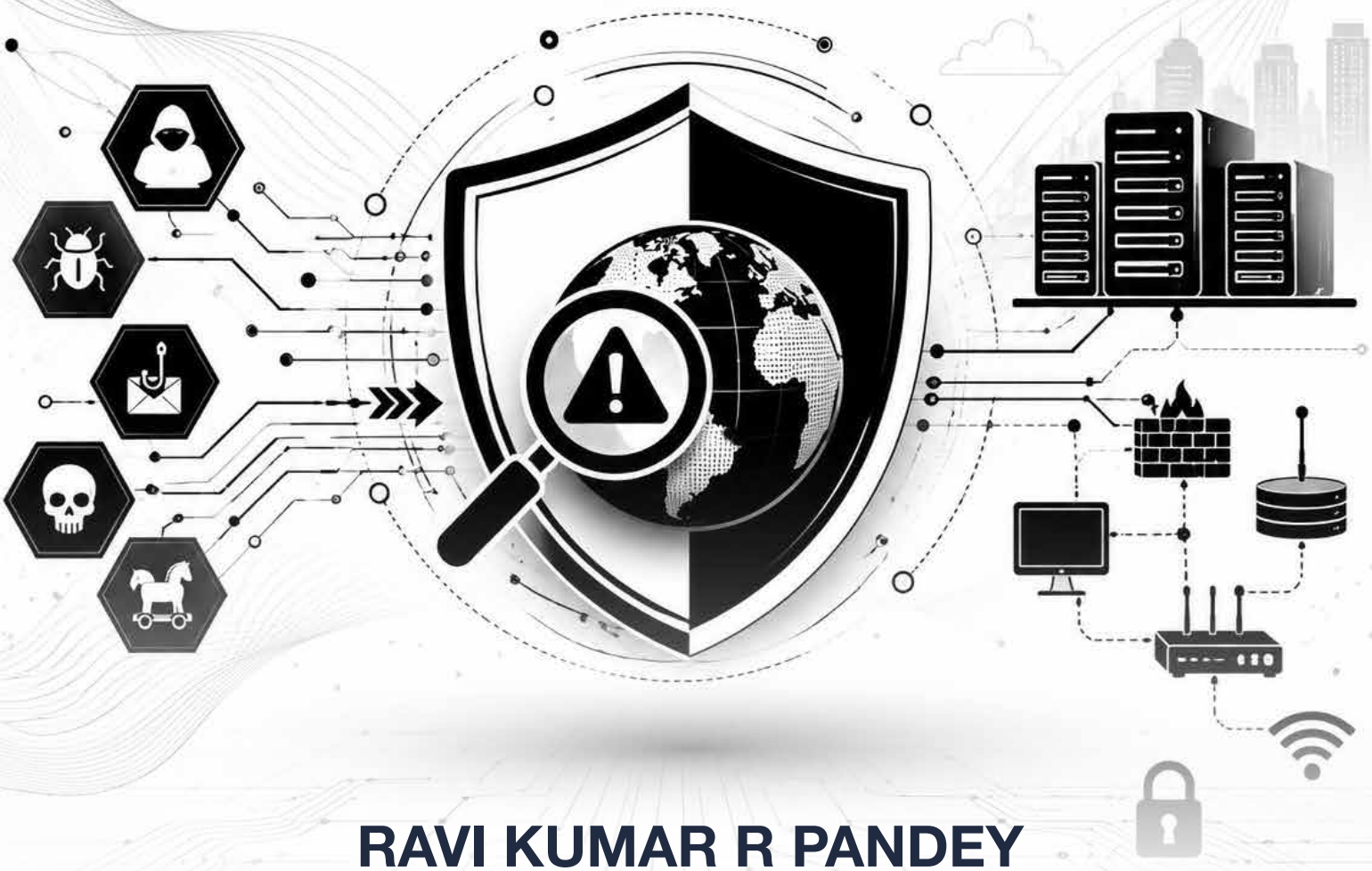
EC-COUNCIL
UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

THREAT INTELLIGENCE

AND ITS RELATIONSHIP WITH

IT INFRASTRUCTURE



RAVI KUMAR R PANDEY
EC-COUNCIL UNIVERSITY

CIS304: Auditing IT Infrastructures for Compliance
Professor Julie Beck
2024, December 01

TABLE OF CONTENTS

TABLE OF CONTENTS

Abstract

The research paper reaches out to our formal understanding of intelligence per se, it begins with the psychological approach and the tenets that have been refined in the postwar era through nurturing and physiological development. Subsequently, we proceed to distinguish between preconceived notions and recent discoveries that eroded our largely inaccurate beliefs about intelligence. Further, we draw parallels with cybersecurity and threat intelligence, which are the crux of our paper, and the humble beginning of computation and networking, this extends to the pioneering technological corporations that are renowned for their contributions to information systems. The foundations of networking and internet access are mentioned briefly. Proceeding further, we dissect the resources inspected to create a platform for intelligence to operate. The complications that are encountered by cybersecurity personnel, organizations, and key stakeholders in assembling the information in a structured form, we also compare and contrast contingency models such as business continuity, incident response, and disaster recovery plans invoked during times of crises. What all these plans and threat intelligence models could impart to us is considered in detail. In the end, our conclusion will be the culmination of all information researched to provide recommendations to enhance the cybersecurity posture and create pathways for further speculation.

Introduction and Background

From the days of yore, intelligence has been sought after and perceived as a mysterious cognitive gift bestowed upon living beings. When we relate it to homo sapiens, it spawns into a fundamental human trait that is imbued with our ability to communicate with our environment and execute actionable tasks, be it for our benefit or detriment (Wechsler, 1944). Intelligence, in its dynamism, enables us to understand and solve problems with our knowledge. However, the ingestion of knowledge and the intellectual capacity derived from it are dependent on the physical formation of our brain during its fetal stage and the manner in which we are nurtured. This would eventually be the epitome of our intelligence quotient (IQ). For centuries, intelligence hardening has been part and parcel of statecraft and a key ingredient to all human activities. We will explore these archaic principles and tenets in relation to cybersecurity and its derivatives.

Humanistic Intelligence

In 1985, a renowned psychologist introduced the Triarchic Theory of Intelligence, which posits interconnectivity that goes beyond the accepted notion based on academic excellence and intelligence capability (Sternberg, 1985). Rather, the (3) subsets derived are analytical, creative, and practical intelligence that are inherently interconnected. Analytical espouses logical reasoning, critical thinking, and cognitive skills, which are prudent to embark on our mission to examine ideas, formulate plans for problem-solving, and discernment to discriminate objects of contention. Creativity motivates us to think divergently to prepare us for novel situations through mustering the courage for imaginative thinking and the amalgamation of abstract ideas. This acts as a foundation for us when we delve into practicality and pragmatism when attending to real-life situations. It teaches us to apply our knowledge and thought to our daily tasks while adapting to differing paradigms in our environment that may not always be conducive, and the ability to relate to people for amicable outcomes. [1]

Formative Years

Information technology (IT) is a realm of its own and has evolved since the 1940s. The humble beginnings of basic computational processes have evolved into a super phenomenon that dictates a large process in our lives. Technology began as an electronic numerical integrator and computer (ENIAC). They were large and expensive to build. It was primarily used for military and large-scale scientific calculations (Ceruzzi, 2012). As with all information systems, they require a language to underpin their processes, even though it is completely alien to the human mind and is perceived as gibberish. However, these languages hid very powerful abilities to quantify electronic transmission. They subsequently developed languages such as FORTRAN and COBOL to translate input and output information.

Progressing further into the ('70s – '80s) corporations such as Intel, IBM, and Macintosh birthed microprocessors whose innovations created a new era of information systems, which significantly reduced the size and cost, allowing for a more personal and mobile ownership of the systems. With that, companies such as Exrox added a new feature known as a graphic user interface (GUI) that was bolstered by Apple Corporation. The computer systems were set for a new phase and complemented the demands of customers, which sparked the need for interconnectivity and information sharing globally (Castells, 1996). This led to the formation of ARPANET, which was the pioneer that embarked on the mission to formalize the foundations for network connectivity.

As time progressed from the 1990s to the present age, we saw the rise of the World Wide Web (www), which provided a platform from which we could gain access to the cyber world for interaction. Having established such a platform, e-commerce and

software companies such as Amazon, Google, and Yahoo seized the opportunity to establish their dominance (Dong & McIntyre, 2014). They provided accessibility for commercial transactions, electronic mail, social, and professional uses, which coincided with technologically advanced mobile phones. Furthermore, in the present times, we are shifting from physical server operations to cloud computing. [2]

Problem Statement

An elusive concept, cyber threat intelligence (CTI) is the synthesis of data that explains trends in risk that are prevalent in the cyber industry, the complexity arising from the tactics deployed, potential for breach, methodology of hackers, objectivity, and vulnerabilities in software and applications (Cert - UK, 2015). The definition of threat intelligence can be summed up as collection, analysis, and application. This is, however, inexhaustive in definition, as several vendors, which include governments and professional organizations, have espoused differing views and procedures to deduce intelligence, this is largely motivated by economic competitiveness. United Kingdom (UK) cyber security strategy surmised a comprehensive yet structured definition that is "evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard" (Cert - UK, 2015, para. 2). The summary provided by Cert – UK is the most holistic, succinct, and accurate description of threat intelligence, therefore it is incumbent upon the decision makers to leverage on this definition to formulate their policies and most importantly their (TTPs). On the other hand, as threats are becoming increasingly sophisticated in their approach, we are facing a barrier of inefficiencies and inadequate knowledge of threats and methodology. It seems that perpetrators are way ahead in their motives and actions, while we are at their mercy, our ability to recover and restore accelerates post-incident.

In the application of (CTI), some different steps and phases need to be observed. This serves a dual role in organizing procedures and processes while maintaining vigilance on legalities. The main proponents of intelligence began with the military and delivered substantial results for their operations. The practice revolutionized warfare and gave an edge to all stakeholders, which eventually unfurled to all levels of society (Ferris, 2004). Driving motivation aims to forecast any detrimental effects in our daily lives. However, their success failed to lure the wider industries to adopt a similar establishment despite rising cyber threats (Ainslie, 2023). The main reason for resistance is due to complexity and financial burdens. [3]

Cyber Threats

The level of sophistication and frequency of cyber-attacks has quadrupled over the last decade. The level of methodology and accuracy employed by hackers has fascinated professionals and cybersecurity enthusiasts. The actors perpetuating disruptive actions are agile and can be classified as individuals and autonomous groups working as proxies for larger criminal enterprises or a country (Johnson et al., 2016). Despite attempts to embed effective measures for collaboration of different phenomena encountered in intelligence gathering, there is still much to be invested in research & development. It is also imperative for organizations to share information based on their discovery, this is not limited to information technology companies (IT) but rather all organizations that utilize electronic means of operations. The collated information emboldens the pursuit to identify, examine, surveil, and formulate appropriate responses promptly, furthermore, when there are collective exchanges between communities and other stakeholders, our intellectual posture is acuminated.

Objectives Of the Project

The purpose of this project is to delve into threat intelligence and its impact on existing and future cybersecurity infrastructure. We would seek to identify the present and future obstacles in collating intelligence and deciphering the information contained. Additionally, we also discuss the steps and processes involved in preparing and collating the information alongside the approach taken by different models and plans formulated and adopted as part of the security posture (Alazab et al., 2024). This is done by following the threat landscape, examining vulnerabilities, and making recommendations that may be applicable in the present or future. We also address the role of threat intelligence in different areas of cybersecurity, such as network administration, system configurations, and device management. The project also serves to absolve and critique present cybersecurity frameworks by comparing and contrasting doctrines from different governments and professional organizations. Apart from that, we also devise ways to harden security and enhance the interfaces used by the analyst to ensure that their vision and actions remain unperturbed and unhindered. Furthermore, statistical and mathematical equations are discussed (Mouiche & Saad, 2025). This is done to highlight the factors that are oblivious to most cybersecurity experts due to limitations in their knowledge of coding, mathematical equations, and algorithms. [4]

Literature review

In the initial discussion, we explore the definition of intelligence and its pivotal role embedded in human psychology and traits. We move on to dissect a modern worldview in the post-war era that deduced key components that are not only congruent but also augmented in our societal norms that inadvertently shaped our perspectives on applied intelligence (Wechsler,1944). We expand and explain the core considerations that are the cornerstone of modern intellectual pursuits, and at the same time, help us understand our evolving needs (Sternberg, 1985). Moving on, we seek to draw parallels with information technology and security, from the humble beginnings of electronic nuances and the uncertainties that precede it. On the other hand, we deter negligence and draw inferences that necessitate intellectual capabilities when dealing with information systems and algorithms. Networking technology laid the foundations for interconnectivity, notwithstanding the impulsion from the general masses of users who yearned for accessibility to information.

In formulating our research, we consult government organizations such as the FBI, Cert – UK, Science Direct, SANS, and, other renowned private commercial technological firms that are at the forefront of providing cyber security mechanisms (Ainslie, 2023) There can be no foundation of theory without valuable inputs from prestigious institutional resources written by experts in their respective fields with scholarly reviews to enable a fruitful discourse on threat intelligence and derive clarity from it (Johnson, 2016) We also source peer-reviewed articles from technology companies that have expertise in several matters and who are at the helm of cybersecurity platforms and threat sharing. Their input is invaluable as they possess the most pertinent information that is relatively new. Apart from theoretical approaches, we dive into statistical and graphical distillation of raw data (Jia et al, 2025).

Threat Intelligence (TI)

As technology advances by leaps and bounds, it has created many opportunities to facilitate social connectivity and financial and professional pursuits. With the development of ARPANET decades ago, there was an incident that pressured the need to broaden the scope of cybersecurity, the Morris worm infection (1988) which had multiple vectors of attack did not destroy systems or data rather it significantly reduced computer performance to almost a halt (FBI, n.d.) Such incidence ignited a discourse on the viability of enhancing cyber security in the electronic realm due to volatility of viruses, worms, and trojans, this could be configured and programmed to subvert systems, networks, and devices.

As part of organizational strategies, it is prudent to prepare a model that can coalesce with multiple intelligence platforms without hindrance, which can delay our reaction (Arvatz, 2021). Generally, the steps taken to implement begin with equitability, which, in simple terms, is a plan that outlines the scope that needs to be achieved based on the organization's operations. This is a direction that would automatically chart the discourse for the preparation of the prioritized intelligence requirements (PIR). The (PIR) does not just contain rudimentary policies. It is specific and technical information, likened to an instruction manual. We proceed to map the types of data needed to support objectives. This data explains where the intelligence is sourced from, such as forums, intelligence databases, and user input. This may also involve vendors and contractors who, on their part, manage certain segments of our systems, networks, and devices.

Types of Threat Intelligence

Several forms of threat intelligence include strategic, tactical, and technical (Palo Alto, n.d.). Strategic provides an in-depth and holistic overview of the threat landscape. The audience of such reports is reserved for senior management and those in the organizational hierarchy with vested powers for decision-making. The report would address the evolving threat landscapes, the profile of the actors, the methodology, doctrine deficiencies, and global political volatility that can have a repelling effect that limits the defensive posture. Similarly, organizations can articulate premeditated proactive policies for future challenges.

Tactical segments the data and expands in areas such as the tactics, techniques, and procedures (TTPs) posed by the hackers. The inheritor of such technical information would accelerate the analyst examination of the threat as it would factor in the details of vectors, tools utilized, target profile, and the steps required to harden security. Additionally, they may also highlight the motives and nature of their transgression (Palo Alto, n.d.). Lastly, technical threat intelligence is the most concise and sophisticated as it pinpoints the source of attack and the methods deployed, including the exact IP address, technicalities of the malware transmitted, and the components in the electronic system that were exploited and weaponized to facilitate the breach. In real-time defensive operations, critical information validates swift defensive actions to mitigate losses.

Upon receiving intelligence reports and advisories, the most crucial component involves not just the tools but also the human element that is tasked with analyzing and reporting to decision-makers. The analytical approach can be done in (2) ways: automated, which leverages cyber tools and technologies to deduce actionable information. Whereas in the manual examination, the task is left to the security operations (SecOps) team (Threat Intelligence, 2021). At this juncture, we will explain in detail the concepts implemented for both approaches. [5]

Automation

In automation, data that is retrieved from alerts is stored in the form of strings and binary data, such as hashes and registries. The most pertinent files and system components that are core to the operations of the infrastructure and system make up a large section of the events triggered. To enable successful triggers, tickets must be configured based on the criteria and sensitivity (Torq, 2021). The indicators of compromise (IoC) should be able to extract data from messaging and logging systems for it to match the criteria. Doing so keeps us ahead of our adversaries, and any gaps in the transmission of threat information to relevant parties for actions must be addressed without delay.

First, the information collected must be matched with resourceful databases such as NIST, SANS, CVE, and others, enabling confidence, integrity, and accuracy in the data collated. When we assess the alerts, we need to refine the information to accept data that is useful, similar to the alerts, avoiding unwanted triggers for non-threatening situations. The critical data that must be collected and accurately matched with the (IoC) should include Internet Protocol (IP), domains, and emails. Having mapped this pivotal information will assist in forensics and investigations.

Manual

The manual examination is a tedious and time-consuming affair that is part of the (2nd) phase of the detection cycle. The data extracted must be relevant to the threat to avoid confusion and delay in the preparation of the response. Furthermore, not all data can be obtained based on the system owner's whims and fancies. They are legal obligations to observe (Hodigital, 2019). The mandatory key information to be collected is chronologically listed events, type, and purpose of data, which includes technical information. While it may take some time for the personnel to peruse through, the information collected must be entered into the automated system for a proper amalgamation and generation of reports.

Phases and Lifecycle

Within the lifecycle of implementing threat intelligence, there are (6) essential stages to be fulfilled. Planning, collection, processing, analysis, dissemination, and feedback. These phases must be adhered to ensure relevance and actionable intelligence policies (Warier, 2024). In the planning stages, doctrine formulation and a role-based dedicated team with a prim and proper analytical skill would seek to collate as much information as possible from network logs and threat feeds. The culling of information must be prioritized based on criticality and actionable insights to bolster response effectively.

For collection, security logs from the network, system, and devices alongside interviews with those affected will be embarked on. It is done with the assistance of various cyber tools to refine data according to pre-defined policies, including the sampling of data for validation (Sigma Cyber Security, 2024). At the processing stage, the examination of data collected is done to ensure that redundant and duplicated information is removed to add context to metadata. Doing so will exacerbate the posture of the incident response team. When converting raw data into actionable context, we utilize the framework from platforms such as MITRE. They can draft patterns of attack and map potential vulnerabilities with immediate security controls. These steps would also be disseminated to relevant stakeholders for the execution of decisions.[6]

In any given scenario, communication is pivotal to ensure that teams and management have an awareness of the crisis (Baker, 2023). The data obtained must be presented in an ingestible format with confidence and accuracy, due to the nature of the report and the audience, who are executives that will make decisions pertaining to the security posture. Furthermore, the iteration is essential to highlight gaps in the report. Any feedback, including clarifications, will pave the way for further enhancements.

Key Challenges and Enhancement

While threat intelligence has proven to be indispensable for the defensive posture, there are, without criticism, several misgivings and integration issues that have arisen, which will be discussed. Many of the threat software and applications have done reasonably well in serving the community. However, a few have excelled. We will not mention their names. We will examine their approach to technology. Threat intelligence must coincide with an organization's safety protocols to enable valid interpretation of actionable decisions (Bromiley, 2023). Operationalizing threat intelligence can be a conundrum due to the evolving needs of an organization, while many of the alerts and reports are to be taken in confidence to avoid being caught off guard, the organizations may have issues with entertaining redundant warnings that have no consequences for them. Attributes to be examined are the types of industries that would be impacted and the nature of the threats, including the tactics, techniques, and procedures (TTP).

Granular knowledge narrows the scope of concern to a more personalized application and integration. Furthermore, constant development and examination of security policies are required as adversaries are constantly changing their modus operandi; additionally, configuration of logs and alerts may derail due to ignorance of the latest developments and discrepancies in integration. The incorporation of sharing standards must be reformed to enable a cohesive and conducive methodology of access to information. In the present times, due to the volatility of information sharing based on

geographical realities, it can be misconstrued with many uncertainties (Ainslie et al., 2023). This would inadvertently deter a geographical split, such as standards prioritized by the EU in contrast with those of the USA and others.

Methodology Adopted

The methodology that we procure is succinctly geared toward the purpose and mission of threat intelligence. It promotes technology and is compared against the delivery capabilities, in addition to the various models, and their approach is considered. We examine the challenges in a rapidly evolving landscape with lesser-than-stellar capabilities and the aggression of cybercrimes. We also draw inferences from peer-reviewed journals that shed light on the different facets of cyber intelligence, ranging from policy formation, applications, discernment of different security logs, and the ingestion of raw data.

Detection and Mitigation

In this area, we have to source guidance from the multi-layered threat intelligence framework (MLTIF), which deploys a range of threat detection and mitigation steps in (4) primary layers. Network, host, application, and users. Focusing on these areas will make it easier to segment our resources and build our focus on sensitive components in our IT infrastructure (Alazab et al., 2024). Analysis of network traffic obtains inputs from intrusion detection prevention systems (IDPS) and firewall logs. The IDPS) maintains vigilance and observes anomalies and suspicious activities. In doing so, it can prevent attacks such as denial-of-service (DOS) attacks and port scanning. To harden security, we have to set a comprehensive policy and configure our firewalls to regulate traffic entering and leaving our networks. Proceeding further, host layers can be secured through the implementation of host-based intrusion detection and prevention systems (HIDPS), making it difficult for hackers to launch buffer overflow attacks or to surveil the host layer for vulnerabilities (Heimdal, 2022). The tactic used is to examine a single specific host for dubious activities and monitor the pattern of malware code. In the application layer, also known as the (7th) layer in the (OSI) model, we have the web application firewall (WAF) embedded with robust coding practices protecting the [7] website traffic that filters HTTP/S requests and responses. Through it, code developers can detect security gaps in their coding structures for improvement. The user layer is the most crucial aspect due to the human element, and improper and unhygienic practices that can fortuitously facilitate a breach. Therefore, constant training and dissemination of information are critical. However, having understood human nature to commit errors and to be negligent, it is advisable to conduct an audit and compliance checks.

Machine Learning

Several platforms have been recognized for their contribution to cybersecurity measures. Firms can leverage the structure and simplify their defensive posture efficiently (Alazab, 2024). Gradient boosting (GBM) is an iterative ensemble technique that deploys decision trees to nullify past errors in endpoints, thus enabling better predictions. The other counterpart, known as (Light GBM), uses a leaf approach rather than a level-wise growth for voluminous datasets, allowing for (GPU) learning without a one-hot encoding. Extremely randomized trees maintain classification and regression while focusing on balancing accuracy and interpretability in their feature.

The instance-based learning methodology is deployed by K – Nearest Neighbour (KNN). The algorithm searches for commonalities in the training set for the prediction of common values. To complement this technology, the Gaussian Naïve Bayes approach is one of probability classification for profoundly high-dimensional datasets due to its refinement and efficiency. Another group of machine learning involves hyperplanes, which is derived from supervised learning algorithms. This methodology separates data into classes for high-dimensional spaces and non-linear boundaries. To achieve this, linear discrimination analysis (LDA) is used and can refine boundaries for dimensionality reduction. Quadratic Discrimination Analysis (QDA) is similar to (LDA) and is a covariance-based non-linear decision boundary for accuracy in estimates.

System of Measurements and Filtration

In many dialogues for threat intelligence integration and the technology itself, few have discussed the reasons for anomalies on a coding and algorithm level. We are quick to succumb to arguments at a superficial level and churn out rhetorical arguments. This would not lead to any developments other than perpetuating the vicious cycle of inadequacies. Information gain and correlation coefficient are metric approaches for decision tree algorithms. They do so by segmenting class data with a specific function (Alazab et al., 2024). Entropy calculation of the parent node disseminates and reveals deficiencies and inconsistencies in the parent node before splitting via probability. For each elemental value resulting from the split, we compare the entropy of child nodes with the parent node. The information gained for feature classification is reduced from the entropy partitioning of data.

Coefficient Correlation

Measurement of strength and direction of the relationship of (2) variables, this selection seeks to identify features with strong connections to target variables (Alazab et al., 2024). The calculation contains values, means, and standard deviations for the amount of observables. The calculation is achieved through Pearson's technique of

correlation, which espouses the feature and target. Variables and methods like point biserial correlation for categorical variables, the coefficient that ranges between -1 and 1. Positive results will run concurrently, while negative results will have a negative correlation. When a strong linear relationship is achieved with the numerical provided, it indicates a strong relationship and confident predictability.

Integrating (CTI) with Networks

Developing and implementing functional network administration in light of cyber threats is becoming increasingly tedious due to the vast number of potential risks and the inconsistencies in reporting. Also, the sheer volume of transmitted data creates another level of a conundrum for administrators and security mechanisms to detect malicious traffic (Barford et al., 2009). With the largely unavoidable challenges, the practice of honeynets is explored to extract detailed and accurate information from data, which reduces the overwhelming and time-consuming efforts required to inspect reports. This creates a situational awareness of the real threats. An example would be scanning activities employed by hackers to exfiltrate network information. On the other hand, honeynets would declassify legitimate and non-harmful events, such as those involving pen-testers who extract information for comparison with cybersecurity databases and check the security of the infrastructure. [8]

Graphs

In threats, we will understand advanced persistent threats (APTs) that are sophisticated and designed to prolong a hacker/s presence for strategic pursuits such as espionage and data exfiltration. The attacks have caused substantial financial losses to governments and corporations (Jia et al., 2025). In the present system, raw data is converted to graphs for analysts to accurately match the vectors of attack and highlight full information, such as location and target details. It also provides details such as the IP addresses of all parties. There are several deficiencies with the nodes' matching attack vectors. The attributes do not provide tactics and clarity. In an experiment conducted by the aforementioned author, they found the graphs displayed nodes that had multiple connections, which made it confusing for analysts to derive tactical semantics to build their responses.

In response, a proposal was put forth to develop a hyperattack graph (HAG). The framework derives its tactical advantage from the MITRE attack model and can include other systems, too. When contrasting traditional graphs, (HAG) utilizes hyperedges to link systems, networks, and devices in their ultimatum of deducing tactics pursued by the actors. The analyst can therefore tap into their experiences to have a comprehensive understanding of the attack.

The main challenge is the accurate matching of relationships between entities in (CTI) reports. This can cause analysts to overlook overlapping relationships in connections that can be vital for data extraction and identification. To solve this conundrum and aid natural language processing (NLP), (3) techniques are used to bolster named entity recognition (NER). Bidirectional encoder representations from transformers (BERT), Bidirectional gated recurrent unit (BIGRU), and conditional random field (CRF) (Jiang et al., 2020). The functions of these systems are to exfiltrate embedded and contextualized words from opposing sides. Subsequently, they process data in sequence from different directions, allowing for the recollection of pre and post-contextual information. These extractions are labeled for predictions. When we leverage them against the strength of each component, it enhances our task for entity recognition and extraction of text data.[9]

Threat Intelligence and Legal Framework

While we face an urgency to quantify our approach to cybersecurity, we must not run afoul of domestic and international regulatory frameworks. This would lead to a self-defeating approach. In an organization that adopts or provides IT services, there must be the inclusion of corporate governance (CSA, 2018). The said act in the Republic of Singapore stipulates a certain core regulation on governance. Governance in cybersecurity is defined as the creation and maintenance of frameworks to ensure the CIIOs) strategies are aligned with the business goals. The goals are made up of defining and managing risks. Strategy and resources must be allocated to the implementation of the strategy and must include the board of directors and senior management, who mold the culture and mindset, and foster resilience in the industry. A key prospect that is part of the hierarchy must include knowledgeable key personnel who are tasked with advisory roles to the upper echelons of decision-makers. Additionally, vested powers of authority and approvals must be delegated to ensure no conflict of interest arises.

Furthermore, a culture of resilience and economic pursuits must be imbued to ensure that we can foster the right change. This can be done in (2) ways: open communication and learning to supplement our defined appetites. A risk management methodology must also be addressed to ensure accurate and timely reporting to all stakeholders. We should also have a tolerance for residual risk, and process hazard analysis should be explored to mitigate safety impacts from hazardous events.

Results

After having examined the various facets of threat intelligence that range from applications and software, we opine that the threat landscape and our ability to combat it have certain level of impediments. This is due to commercial competition amongst different intelligence platforms, software, and application companies. They are hesitant to overtly share information and may even obscure critical data for their benefit. Furthermore, they would prefer organizations to contract with them for a better and more conclusive service.

Intellectual property issues create setbacks as some companies can develop algorithms that far exceed what is available in the commercial sphere. When we tabulate this consideration, cost factors as a result, consumers are unable to fully implement cybersecurity measures, and they may also choose a reduced protection option to meet their needs. Graphical weakness and interactivity are also concerning, as the quantity of data generated requires a cautious approach to avoid overlooking critical information and anomalies.

The most profound discovery is the issues surrounding coding and the algorithms that reduce and expand vulnerabilities, as we have discussed earlier, gaps in the coding structure and linear equations that pose obstacles for full integration or incapacitate certain segments of the threat detection, which may also extend to the end user's systems, networks, and devices.

Recommendations

The adoption of evaluation metrics advances the quality of data collected to effectively handle larger volumes of data. On the same note, we should also consider multi-layered integration of threat intelligence data. To avoid excessive false positives and negatives, we should configure the machine learning equations to disregard false alerts and give prominence to real-time threats. The scalability framework should also include cloud computing and the distribution of services. Effective distribution can bolster security posture through the cohesive sharing of information. Adapting the MLTIF approach for testing in all situations.

The introduction of (HAG) is an innovative model emphasizing the extraction of entities and their relation to (CTI) reports, harnessing joint extraction tactics for enhanced efficiency and performance. The approach leverages hypergraph-based methodologies for implementing strategic-level attack graphs and is refined with the inclusion of a semi-hypergraph algorithm for an adroit identification of attack techniques within given templates. The HAG will be a very critical addition for combating cyber threats.

Conclusion

In conclusion, we seek to discern competitive postures and vested responsibilities that can impede effective information sharing. This can have a repelling effect as insufficient information creates trouble for the wider community. Exploring multiple-layered models for a robust interface, such as the HAG, should be refined further and researched to harden security posture and response. We should also widen our perspectives on cybersecurity and not simply disparage administrators and executives during breaches. We should look at the mathematical and technical implications in code development. These are the areas that have much potential.

Bibliography

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023, September). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. Computers & Security, 132.

https://www.sciencedirect.com/science/article/pii/S0167404823002626#bib0077

Alazab, M., Khurma, A R., Arenas, G M., Jatana, V., Baydoun, A., & Damasevicius, R. (2024, September).
Enhanced threat intelligence framework for advanced cybersecurity resilience. Egyptian Informatics Journal.

https://www.sciencedirect.com/science/article/pii/S1110866524000847#sec4

Arvatz, A. (2021, October 15). 4 Simple steps for an effective threat intelligence program. Threat intelligence, detection, and response.

https://www.rapid7.com/blog/post/2021/10/15/4-simple-steps-for-an-effective-threat-intelligence-program/

Barford, P., Chen, Y., Goyal, A., Li, Z., Paxon, V., & Yegneswaran, V. (2009, January 01). Employing honeynets for network situational awareness. Cyber situational awareness.

https://link.springer.com/chapter/10.1007/978-1-4419-0140-8_5

Bromiley, M. (2023, November). Operationalized threat intelligence. Analyst program.

https://sansorg.egnyte.com/dl/bdcZZrB53k

Castells, M. (1996). The rise of the network society. Information Technology.

https://archive.org/details/riseofnetworksoc0000cast/page/n5/mode/2up

Ceruzzi, E., P. (2012). Computing: A concise history. Computer science – history.

https://archive.org/details/computingconcise0000ceru/page/n5/mode/2up

Cert-UK. (2015). An introduction to threat intelligence. A catalyst for collaboration.

https://www.ncsc.gov.uk/files/An-introduction-to-threat-intelligence.pdf

CSA. (2018). Cybersecurity Code of Practice for Critical Information Infrastructure – second edition revision one.

Cybersecurity Act 2018.

https://www.csa.gov.sg/docs/default-source/legislation/ccop---second-edition_revision-one.pdf?sfvrsn=421a71ab_1

Dong, X., & McIntyre, S. (2014, November). The second Machine Age: Work, progress, and prosperity in a time of brilliant technologies. Quantitative Finance.

https://www.researchgate.net/publication/266742603_The_Second_Machine_Age_Work_Progress_and_Prosperity_in_a_Time_of_Brilliant_Technologies

FBI. (n.d.). Morris worm. History.

https://www.fbi.gov/history/famous-cases/morris-worm

Ferris, J. (2010, September 08). Netcentric warfare, C4ISR and information operations: Towards a revolution in military intelligence? Intelligence and national security.

https://www.tandfonline.com/doi/abs/10.1080/02684520420003029 67

Heimdal. (2022, February 09). Taking the host intrusion prevention system (HIPS) apart. Cybersecurity basics.

https://heimdalsecurity.com/blog/taking-host-intrusion-prevention-system-hips-apart

Hodigital. (March, 2019). Cyber threat intelligence in government: A guide for decision makers & analysts.

Cybersecurity program. Digital, data & technology.

https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf

Jia, J., Yang, Li., Wang, Y., & Sang, A. (2025, February). Hyperattack graph: Constructing a hypergraph for cyber threat intelligence analysis. Computers & Security.

https://www.sciencedirect.com/science/article/abs/pii/S0167404824004991

Jiang, L., Junping, D., Nan. Z., & Zhe, X. (2020). Bert – bigru – crf: A novel entity relationship extraction model. 2020 IEEE International Conference on Knowledge Graph.

https://www.computer.org/csdl/proceedings-article/ickg/2020/09194542/1n2nkw0yUjm

Johnson, C., Badger, L., & Waltermire, D. (2016, October). Guide to cyber threat information sharing. NIST Special Publication 800-150.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

Mouiche, I., & Saad, S. (2025, January). Entity and relation extractions for threat intelligence knowledge graphs.

Computers & Security.

https://www.sciencedirect.com/science/article/pii/S0167404824004255

Palo Alto. (n.d.). Cyber threat intelligence: A comprehensive guide. Cloud security.

https://www.paloaltonetworks.com/cyberpedia/cyber-threat-intelligence

Sternberg, R. J. (1985). Beyond IQ: A Triarchic Theory of Human Intelligence. Cambridge University Press.

https://archive.org/details/beyondiqtriarchi0000ster

Sigma Cyber Security. (2024, November 16). 6 strategies for integrating cybersecurity threat intelligence.

Cyber intelligence hub.

https://sigmacybersecurity.com/6-strategies-for-integrating-cybersecurity-threat-intelligence/

Threat Intelligence. (2012, April 11). Threat intelligence: Types, benefits, and its lifecycle. Blog.

https://www.threatintelligence.com/blog/threat-intelligence

Torq. (2021, July 27). Automated threat intelligence: An overview. Use cases.

https://torq.io/blog/what-is-automated-threat-intelligence/

Warier, H. (2024, November 22). Understanding cyber threat intelligence: A comprehensive overview.

Knowledge base.

https://www.cloudsek.com/knowledge-base/understanding-cyber-threat-intelligence-a-comprehensive-overview

Wechsler, D. (1944, April). The measurement of adult intelligence. The Williams & Wilkins company.

https://archive.org/details/measurementofadu001469mbp/page/n7/mode/2up

Appendix

Component	Description	Example	References
Humanistic Intelligence.	(IQ) and the ability to formulate ideas.	Quantitative coding and algorithms.	William & Wilkins Company.
Theory of intelligence.	(3) Modern view of intellectual capacity.	Analytical, creative, and practical.	Cambridge University Press.
(ENIAC).	Mechanical calculations.	Large machines for computation.	Computer science history.
Modern systems.	Interactivity and e-commerce.	Formation of technological companies and the formation of (www).	Brokers, intelligence agencies
Threat Intelligence.	Elements of (CTI)	Emergence of threat platforms.	Detection and response.
Types.	Facets and aspects of threat intelligence.	Information Sharing	NIST
Measurements and filtration.	Mathematical implications.	Formulas are required to modify codes and algorithms.	Egyptian informatics journal.

List of figures and tables

Types of Threat Intelligence (Ainslie, 2023).

Threat Intelligence frameworks (Alazab et al., 2024).

Table 1. Most important threat intelligence frameworks.

Framework	Principal ideas and conclusions
DISCLOSE [26]	Utilizes an adversarial tactics, methods, and procedures (TTPs)-based data-driven decision support framework to optimize forensic investigations.
IoV Security [27]	Covers security flaws in the Internet of Vehicles (IoV) and describes explainable AI (XAI) models for intrusion detection.
AI in Cybersecurity [20]	Explains the drawbacks of signature-based methods and looks at deep learning possibilities for challenging cybersecurity jobs.
Emerging Threats [28]	Outlines a methodology for the automatic detection and profiling of new threats through the use of social media and MITRE ATT&CK information.

The sources of intelligence (Alazab et al., 2024).

Table 2. Most important threat intelligence sources.

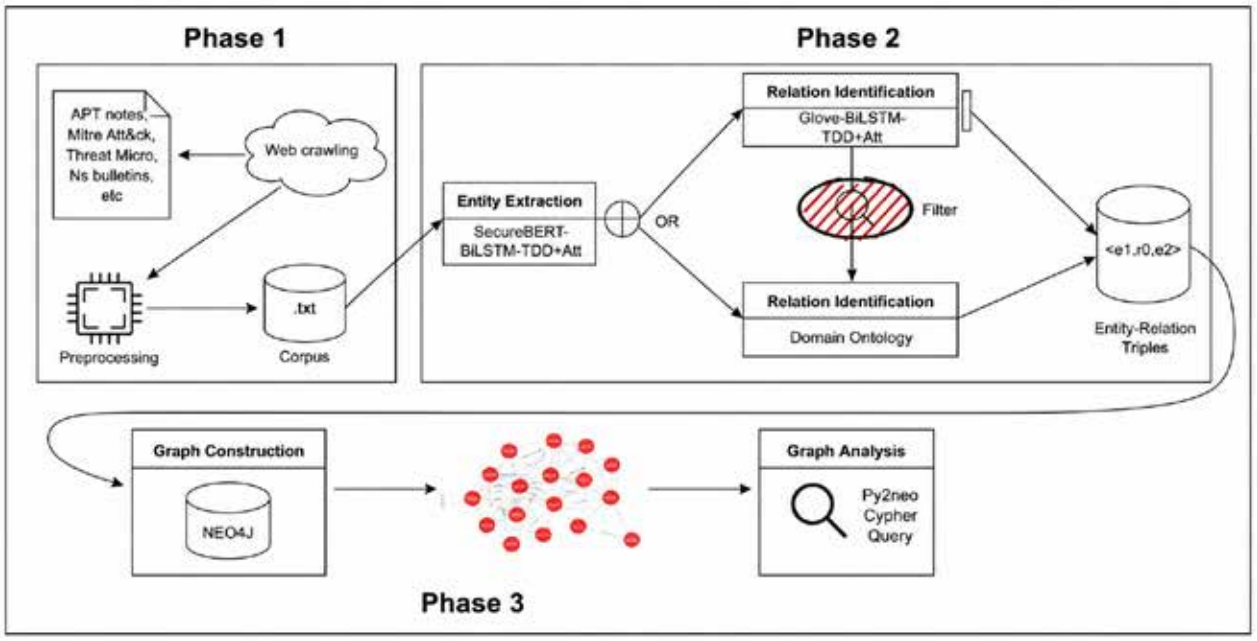
	Source	Principal ideas and conclusions
	**OSINT [38]**	Provides publicly available data for threat detection but requires significant processing for actionable intelligence.
	**Commercial TI [39]**	Offers high-quality, tailored threat feeds but at a cost, suitable for specific industries or threat types.
	**Government Agencies**	Distributes valuable threat intelligence for critical infrastructure protection, essential in sectors like energy and finance.
	**Internal TI [40]**	Uses organization-specific data for targeted threat detection, crucial for identifying internal threats.
	**Dark Web Intelligence [41]**	Provides early warnings of emerging threats and targeted attacks from the hidden part of the internet.
	**Human Intelligence (HUMINT) [38]**	Obtains threat intelligence through interviews; useful for context and qualitative insights.

Detection and mitigation techniques (Alazab et al., 2024).

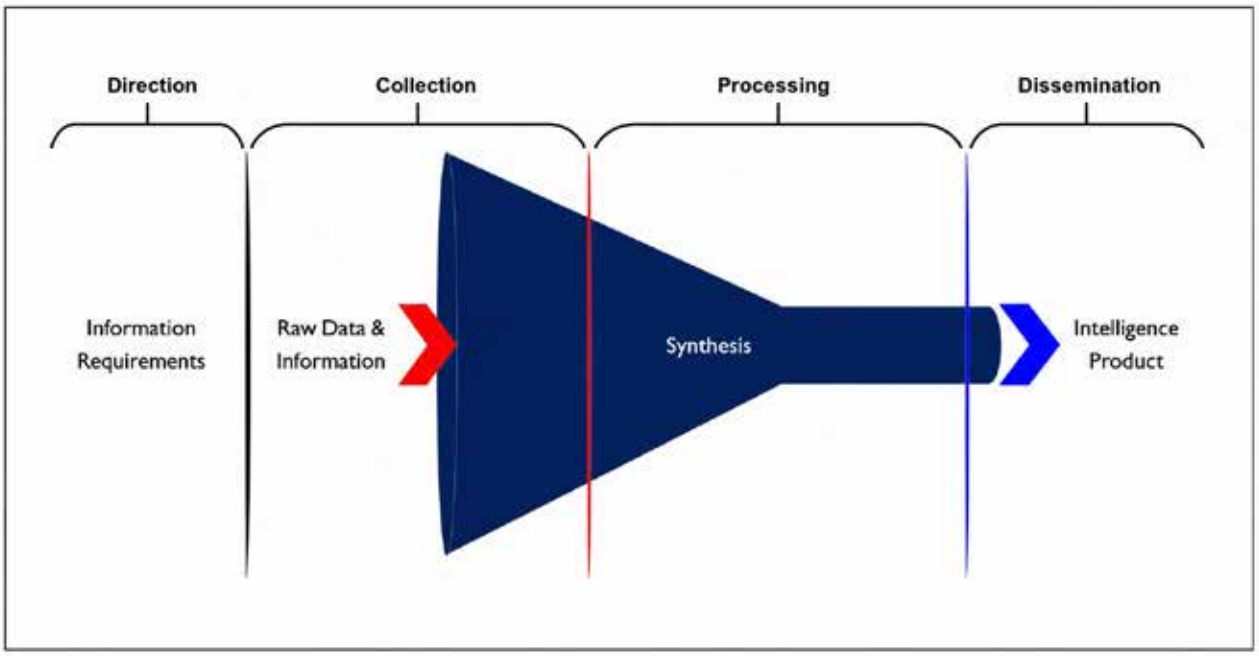
Table 3. Most important threat detection and mitigation techniques.

Technique		Principal ideas and conclusions
	**Machine Learning [42]**	Employing network traffic features, multiclass cyberattack categorization is achieved with great accuracy.
	**Log Analysis [43]**	Applies AI models (XGBoost, RNN, DNN) to analyze log data for efficient cyber-attack detection and identification.
	**Active Defense [44]**	Offers the use of natural language processing in an automated system called CTI View to provide active defense against advanced persistent threats (APTs).
	**IoT Security [2]**	Creates a strong security architecture that integrates fog computing and IoT with healthcare systems (Healthcare 5.0).

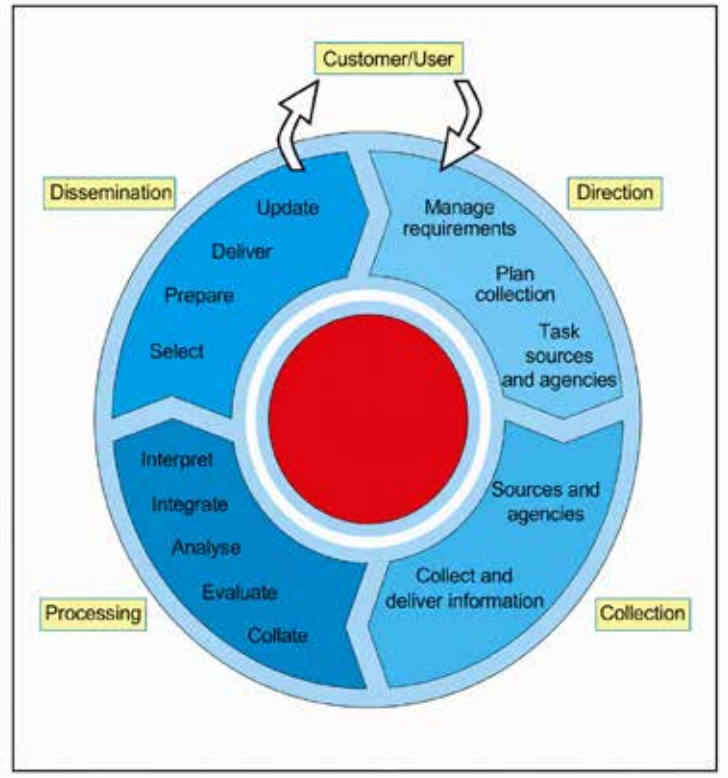
Threat intelligence knowledge graph framework (Mouiche & Saad, 2025).



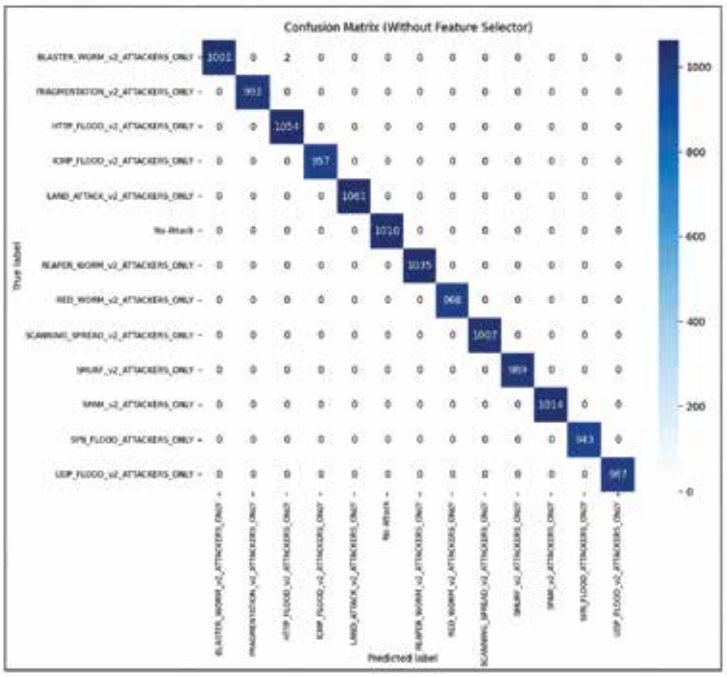
Data transformation into intelligence (Ainslie et al., 2023).



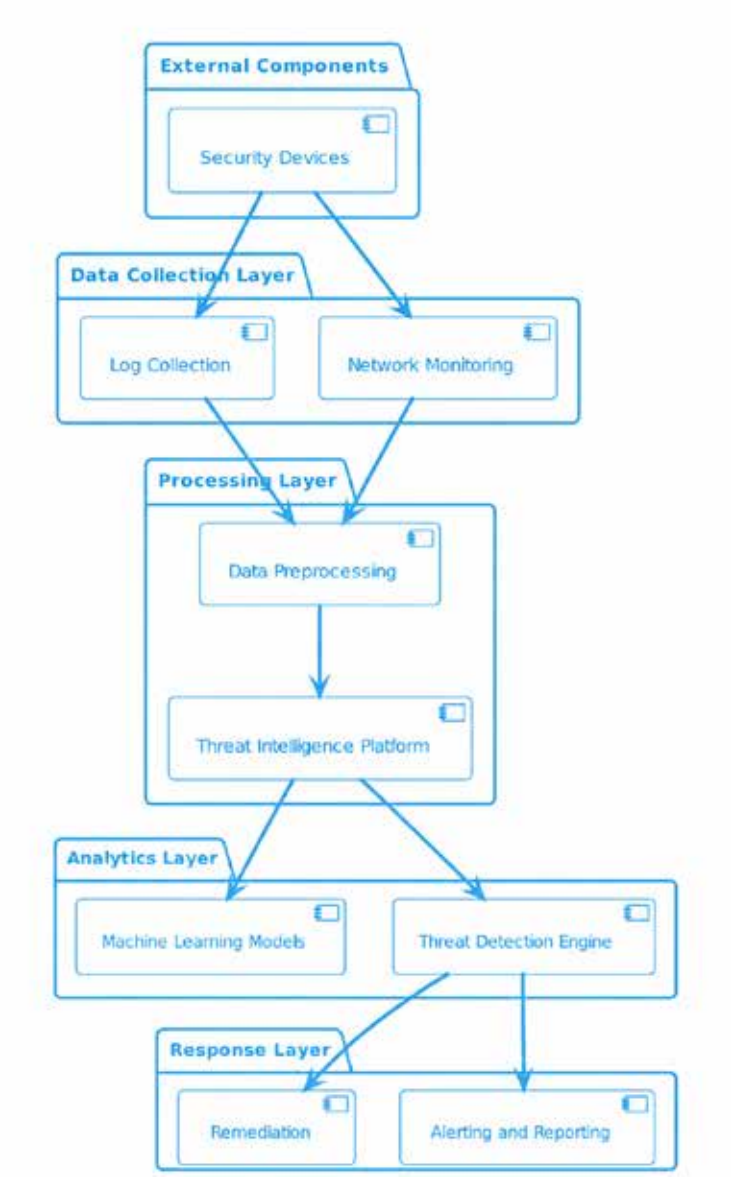
Intelligence cycle (Ainslie et al., 2023).



Different attack categories and their labels (Alazab et al., 2024).



Intelligence cycle (Ainslie et al., 2023).



Index words

Intelligence – psychology – physiology – notions – analysis – abstract – threat -adroit – formulas – graphs - security - algorithms – automation – manual – phases – cycles – models – platforms – code – mathematics – machine learning – AI – legislations – filtration – measurements – detection – mitigation – key - challenges