Deep Science Publishing
https://doi.org/10.70593/978-93-49307-75-9_8

DeepScience
Open Access Books

Chapter 8: Designing proactive and intelligent threat detection mechanisms for robust network protection and resilience

8.1. Introduction

Risk management focuses on detecting potential threats, which is in line with our study that explores proactive threat detection mechanisms and potential adversaries of enterprise networks. The telecommunications industry, striving to win customer loyalty, always aims to provide users with higher satisfaction by ensuring seamless data transmission, coverage of service, lower access delay, and minimum packet loss. Because of competitive challenges faced by network vendors, the reduction of capital expenditure and operational costs of operation support subsystems and the network operation center have also played a more substantial role in telecommunications survival. To reach this primary goal of keeping customer satisfaction as high as possible, the achieved network robustness and network resilience are the most valuable criteria. In the past, the research investigated various approaches to enhancing network resilience. The root cause of the single point of failure was revealed, and remedial designs for eliminating the single point of failure were proposed and analyzed. Deployment of diverse routing protocols, protection mechanisms, and facility backup systems contributed to ensuring data transmission and prevented data, traffic, or signaling transmission loss during network failures. To guarantee a minimum grade of data transmission performance, network performance monitoring and failure recovery algorithms were employed. Influences of various network configurations on competitive behaviors of network service providers were also studied.

8.1.1. Purpose and Scope of the Report

This study presents a comprehensive review of traditional proactive threat detection approaches, which are meant to detect malicious activities, as well as advanced persistent threats that are specifically designed to evade existing defense mechanisms. Here, we have analyzed and described a wide range of existing threat detection and timing in networks, and related models that rely on network delay dynamics. Additionally, we propose a novel methodology that bypasses the lack of prior knowledge of the specific values of the APTs' fill dates in delayed interactions and provides efficient real-time estimations of these fill dates over the network's traffic. This study provides a step-by-step overview of the suggested approach and experimentally evaluates its efficiency and accuracy, considering both classical applications and advanced persistent threats.

The increasing complexity, frequency, and sophistication of cyber attacks have forced various stakeholders to reconsider the vulnerability of network infrastructures and to search for mechanisms that will timely detect malicious activities and thus enhance the resilience of these infrastructures against cyber threats. To address this issue, numerous threat detection mechanisms have been proposed; these mechanisms are mainly operable in an active way, solving the problem during or after the realization of the threat in the network. In contrast , proactive detection methodologies have not yet exploited the potential of network delay dynamics, i.e., the delay evolution dependent on the types of messages, traffic, and communication patterns of humans and automated devices.

8.2. Understanding Threat Detection

The goal of any network security mechanism, including intrusion detection, is to prevent unauthorized use, misuse, and abuse of the network and its resources and assets. This includes not only simple thefts but also the installation of logic bombs, Trojan horses, and other software that would give unauthorized control of network resources and thereby enable attackers to cause denial of service attacks, use networks by unauthorized individuals, or engage in other types of network abuse, such as a company representative disclosing proprietary information. Even the seemingly benign use of research resources in a closed institution by outside researchers who logged in solely to write a proposal might represent an abuse of network resources, which are, after all, owned by the community providing support to the institution.

Most attackers' first attacks are detected, in some instances, well before the attacks cause actual harm; failure to collect these detection events almost always means that more subtle and gradually harmful usage attacks will go unnoticed. Unfortunately, it matters little whether the eventual use of a successful attack would cause significant injury, for

an obvious indicator of an attack is always significant. Just as the tools and programs used to initiate attacks can be detected, so can the reconnaissance attackers use to gather information about potential targets.

8.2.1. Definition of Threat Detection

Threat detection is the identification of threat indicators or warning signals that could suggest exposure to some form of danger or harm in an environment. The term is often used in the context of computer or network security. A cyber threat is a sequence of correlated and recurring actions that promote adversarial behavior leading to the loss of data confidentiality, integrity, and computer availability. Detecting the earliest warning signs of an attack, such as reconnaissance, vulnerability scanning, or exploitation, can enable system administrators to respond preemptively to active and passive cyber threats such as viruses, worms, and spyware. The central theme for threat detection is influenced by the observation that potential and actual threats, especially concerning cyber adversaries' actions, their tools, methods used, and their goals to violate network security, are complex by nature. However, one can still detect insider and outsider threat-related suspicious activities generated during the cyber attack process. Such activities identifying pre-penetration, penetration, post-penetration, and finally, an exit of an attacker from a network are referred to as cyber threat-related network indicators. Furthermore, by associating metadata with these suspicious activities, we can fully track attackers' post-penetration activities and identify evidence of secondary and botnet-infested victims, without relying on signature-based malware scanning methods.

Fig 8 . 1 : AI-Enhanced Cyber Threat Intelligence Processing

8.2.2. Importance of Proactive Measures

The importance of proactive measures: Risk assessment methodologies and models used to characterize the security of a network frequently build on probabilistic attack graphs and asset or threat value propositions to help us understand and reason about critical paths and dependencies in the network. Both the attack paths and the asset/threat valuations underlying the formation of the graph tend to become outdated relatively quickly. Thus, approaches that can anticipate and evaluate the effects of such exceptions, model learning and adapting, and eventually contribute to trust models that can help in making autonomous proactive alerting, re-routing, or network actions when exceptions are identified are of high value. Prediction is important to avoid surprises (Javaid et al., 2016; Buczak & Guven, 2016; Diro & Chilamkurti, 2018).

Cyber risk is subjective; we need more ways to reduce uncertainty. A brief look at today's enterprise networks will show that the complexity and dependencies within them have exploded over the last few years. This isn’t all bad - it's also easier now to aggregate data and perform analysis at a broader base. However, not all data is available depending on what subset of management and control responsibilities we choose to observe. Neither is all the data from a single instrument necessarily available nor is that data necessarily accurate or shared by its creator. Most data gets created, gets wrung through server log files, may fall prey to understandable reduction routines due to practical limits of collection, storage, and its complexity to analyze, and then gets erased.

In other words, network structure and measure are related but not perfectly. We believe that we can gain a lot of resilience by being smarter about how we decide to measure and fuse the structure and measurements in a principled fashion. We observe approximations of network trustworthiness rather than total measures. What if a future network could maintain and provide more faithful state information about its configuration, traffic, users, and use to achieve network trustworthiness? This trustworthiness is not just about self-defense - it's about how social networks and human concepts affect this environment, and how the environment responds to behavior.

8.3. Types of Network Threats

Today, the complexity and dynamics of computer networks make them more prone to a wide range of potential threats. How then can a network become infected with a virus? What makes it possible for an attacker to launch a denial-of-service attack against a network asset such as a mail server or a website? And what impact can these attacks have on the services that the network provides? All these questions are basic to understanding network threats and attacks (Yin et al., 2017; Vinayakumar et al., 2019).

To be able to understand how networks can be threatened and attacked, and to grasp how these threats and attacks can be detected, it is useful to classify network threats and to consider some specific examples of them. This categorization can then provide a reference point for the many various threat and attack detection methods that we will introduce in this overview chapter in the following sections. So, what types of electronic threats may disrupt computer network operations and cause losses that may be measured in millions of dollars? In general, computer networks may be threatened and attacked in the following different ways. These combat maneuvers include passing vulnerability scanners and taking advantage of network software weaknesses. In addition, networks may also be subjected to two other classes of attacks: volume attacks and attacks for network resources.

8.3.1. Malware and Ransomware

The malware can be any software that intends to damage systems, user data, servers, or any organization silently. Some examples include ransomware and viruses. Ransomware is widely used today to block unauthorized access to end user's files. It initially encrypts the files stored on hard disks and demands a ransom to decrypt the data. Then it allows users to access the files and spreadsheets. The data are quite large inside the data center environment in the cloud. The criminals do not fear antivirus software at all. Thus, it is essential to protect the data center from ransomware. Any file infected with viruses can propagate to other uninfected files in personal computers, clients, and servers. Constructing the ransom wagon can detect ransomware activities. More advanced architectures can be developed to prevent such activities from occurring. The impacts related to the data center for malware can be categorized as time, affecting hardware, and financial aspects, and influencing user satisfaction, trust, recoverability, and availability. Ransomware attacks happen from the internet, and they usually spread at a fast pace using the server's flaws. Ransomware can infect files hosted anywhere in the internal network, but it especially targets shared machine files. The infection from ransomware can block hospital operations and create significant disruptions, bringing services to a standstill. Ransomware can limit single device access or limit access to the entire site. Any compromised medical devices can create a significant delay or bottleneck. Ransomware can cause denial of service for medical devices that cannot work properly if they lose access to their required infrastructure. The lack of access for devices to medical systems that rely on these servers can cause misdiagnosis and mortalities. Similarly, blocking critical access to the server can weaken the availability pillar. The authorization of access to unauthorized personnel can reduce security.

8.3.2. Phishing Attacks

Phishing is a social engineering scam that uses deception to fraudulently acquire sensitive or valuable information such as username, password, or credit card number. In general, phishing attacks can be categorized into three types, including email phishing, website phishing, and data phishing. Based on the attack platform, phishing falls into two classes: single-stage phishing and two-stage phishing, where the latter offers the ability to specifically harvest sensitive information. In our work, we are interested in both types of phishing.

Data synthesis. The data synthesis framework for phishing contains two types of data, including the artifact data and the attack log. Artifact data is mainly collected from website information as well as a first-stage phishing email and the attachment, which is often designed using an office exploitation framework. To generate a large quantity of artifact data, advanced technologies are created or leveraged to achieve consistent phishing. For instance, we can employ a powerful mobile assistant to load the attachment, and then turn the attachment into image resource files. The generated images could be slightly different; a variety of effect-transformation techniques should be applied to augment the artifact data. Therefore, additional reactions could affect the artifacts, such as watermarking, editing, recoloring, etc.

8.3.3. Denial-of-Service Attacks

Several works deal with denial-of-service (DoS) attacks. In a stable environment, where the fraction of selfish or malicious nodes is below a certain threshold, the probability of routing and service disruptions is kept low. Therefore, exploiting network effects can detect selfish or malicious nodes. Efficient DoS detection mechanisms for ad hoc networks based on inference statistics and a "memory captain" are discussed. By keeping track of request counts and successfully establishing communication, a proactive approach for recognizing and defending against an attack on attribution systems is realized.

Some regions of the Internet are more often used as sources of DoS attacks. Based on monitoring, the topology of regions where DDoS attack sinkholes could be detected. The detection and recovery mechanism utilizes bottlenecks in a distributed service network to detect DoS attacks in secure flows. The proposed new Bottleneck Identifier is capable of reacting to changing conditions and can find long-standing bottlenecks, while nodes use a mechanism to identify previously unsolved bottlenecks to recover service. The concept is based on the observation that in a service network, DDoS attacks can

monopolize significant resources on a single path. Their related design bypasses the requirement of time synchronization by allowing nodes to guess the required switch.

8.3.4. Insider Threats

Insider threats are security risks that come from people within an organization, usually an employee, officer, contractor, or anyone who has insider access to an organization. Insider threats can turn an organization into an easy target for any external threat. It is indeed a challenging problem to deal with insider threats proactively, as employees and other insiders are legally allowed to handle organizational resources. It is negligent to handle potential insiders who work in an organization for an extended period and have a good track record. For most organizations, protecting their systems from external threats and accidental insider threats is the primary concern. Unfortunately, the damage from the intentional insider threat may cause much greater harm. One of the best definitions is that a malicious insider is an entity within an organization's network that possesses some form of privilege and uses that privilege to exceed or abuse their trust in an organization alone or association with one or more external adversaries.

Insiders must first consider both the intelligence cycle and the information security cycle, and second, develop preventive measures to which incumbents should be alerted against unethical conduct. First, the organization must be alerted when an insider violates the intelligence cycle, expanding beyond the traditional insider threat triangle towards the degrading cycle after acts of espionage and sabotage have transpired. Additionally, when organizations and managed security service providers violate the intelligence cycle, cautious attention must be paid to the information security life cycle to identify unethical acts. Providing a methodical level of detail on these matters is vital to improving the knowledge of any organization's situational awareness. Second, the managed security service providers must develop numerous preventive measures to hinder unethical activities. These measures are not solely formed to oversee insider threats; these means combined oversee all major threat agents, including organized crime, nation-states, and hacktivist actors.

8.4. Traditional Threat Detection Methods

Most current models analyzing network traffic are implemented using the three basic data mining tasks of classification, clustering, and association rule mining. Classification assumes data is labeled with a target – in the case of intrusion detection, the classification task is to label traffic as "normal" or "intrusive" – and builds a model to classify future

instances. Support vector machines or one of the many supervised neural network architectures may be used to perform classification tasks. Clustering groups instances without any fixed target in mind and identifies local structure within the underlying data. It can be useful for understanding network traffic in an unsupervised way for which neural networks alone may be ineffective. Association rule mining is used to discover interesting relationships between variables in very large databases with a variety of domains.

Visual data mining and semi-supervised learning are relatively new techniques being applied to threat detection, making up for some of the weaknesses mentioned above. Visual data mining is the field of research that combines human visual perception with computer processing capabilities, mostly that of cluster manipulation and data dimensionality reduction. Data of up to a few dozen dimensions can be presented in two or three dimensions using animation in a way that clusters occur very close together only when their content has a very high similarity. The time dimension can be added to animate the motion of the objects presented – human analysts are better at recognizing patterns in motion than in a static display. Semi-supervised learning methods are machine learning techniques that use a small amount of labeled data and a large amount of unlabeled data for training – an especially advantageous situation for network traffic analysis, where traffic data that is not generated by intrusion events or in general is flawlessly labeled as such generally makes up the vast majority of traffic.

8.4.1. Signature-Based Detection

This is the oldest and most widely used form of intrusion detection, wherein attackers engage with computer systems and networks in response to a stimulus such as a specific known vulnerability. The attacking outcomes are often described as a signature, and detection relies on the transmission, intercept, and comparison of these signatures against configurations, profiles, and rules. Signatures serve as a template, and they can intercept and identify precise matches, partial matches, or similar system capabilities or system behaviors. This implies that a single signature of an attacking event can correspond to multiple profiles of activities or capability/behavior mixtures. The security profile will often contain exploitable resources or critical assets in the same way that the event signature contains interacting addresses.

The primary advantage of the signature-based detection mechanism is the high detection rate. It is often cited as the best approach for detecting known attacks when strict criteria are applied. The signature is applied to simulated profiles and compared for a match, with distinct search terms defining the sort of attack scenario, attributes, and form of

collected footprint evidence needed. Once a match is found, alarms are usually initiated within an incident management system based on adjustable correlation rules or artificial intelligence. The biggest disadvantage of signature-based detection is the requirement to predefine acceptable user behaviors, which impedes the investigation of novel attacks or new combinations of attacks, also known as zero-day attacks, single-action kill chain attacks, or derived capability attacks, which are not outlined in the historical event or scenario results.

8.4.2. Anomaly-Based Detection

When it comes to anomalies, it's always been challenging to verify the idea of 'good behavior.' From a security perspective, implementing anomaly-based systems at organizational scales means making informed guesses about how various systems in the business should ideally operate. Then these guidelines need to be implemented by the organization's IT security department. These challenges seriously add to the deployment time when attempts are made to operationalize internal protective checks and make assumptions around the concept of 'good' behavior - sometimes at odds with enduring system safety norms and safety mechanisms already built within the system. To truly understand 'good' conduct requires a comprehensive study of the system and how it serves the company. To find an anomaly, definition tools such as inference, data mining, and machine learning must be extended to differentiate normal from potentially anomalous behavior. Does a certain bandwidth usage, for example, signify a certain standard?

A capability to detect centralized and decentralized architectures at the network edge seems to be the right way to handle network border cross traffic cost-effectively . Diagnosis mechanisms operate by listening to network traffic and collecting markers for different types of anomalous behavior, such as computer names and usernames, which were not seen before when checking files or system registries and being bombarded with various types of traffic. This data can then be analyzed to generate statistics indicating whether an anomaly has occurred and what decisions (if any) need to be made in response to it. Deployed incident detection mechanisms can either capture the complete material or provide a compressed or summed account before the impact incident occurs. Irrespective of the approach chosen, when enabled and managed, reliable detection mechanisms alert security staff to security incidents in progress or about to happen.

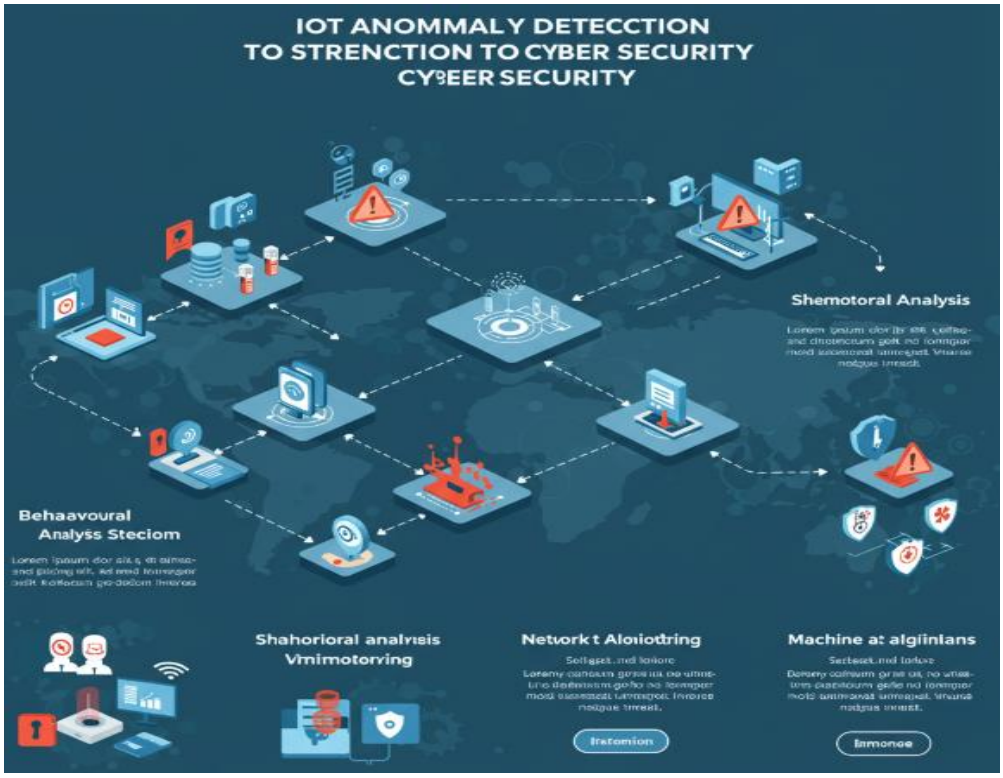

Fig 8 . 2 : IoT Anomaly Detection to Strengthen Cybersecurity

8.5. Limitations of Traditional Approaches

In traditional network security mechanisms, network attacks are engaged to make a network service unavailable. During an attack, the negative impact on the network directly leads to the availability of network services being reduced. This type of negative impact, which is mainly reflected in denial-of-service and distributed denial-of-service attacks, is referred to as passive negative impact. When a traditional security mechanism performs activities, it essentially considers network security and service availability in a reactionary approach. Namely, it operates under a network attack, prevents the attack from succeeding, and promptly handles the resulting consequences. In contrast, network resilience techniques promote active defense as a new guaranteed approach. Proactive defense concentrates on controlling security strategies and green computing. The ultimate goal is to build energy-saving, reliable, and secure networks while minimizing environmental and human costs. Since proactive maintenance has been employed in the network steady state phase for several years, reports indicate that failures and outages have been significantly diminished.

After the implementation of proactive maintenance, future real-time alert reports indicate reduced instances of network security incidents. To ensure the normal operation of network services, once a fault occurs, reactive maintenance is employed to re-establish the normal service state. Although such remedies efficiently minimize any potential negative impacts, they remain predominantly backward-looking and are essentially carried out post-incident following a network failure. Indeed, the actual merit of a proactive approach is realized only when its benefits are recognized, and the allocation of network resources is based on inherent knowledge rather than implementing both passive and reactive approaches to network incidents, which fail to timely uncover and diagnose consequences. Within existing scenarios identifying, diagnosing, and mitigating the negative impacts of network incidents, the timelines of reactive responses vary. Currently, however, no proposal exists that selects a future approach that facilitates the rapid development of proactive responses defending network stability before network security incidents occur.

8.5.1. False Positives and Negatives

The increasing prevalence of network attacks has prompted a variety of intrusion detection mechanisms. In general, these approaches harness proactive techniques using some forms of attack signatures, behavior profiles, statistical anomalies, or correlations to identify suspicious activities and proceed by performing some method of risk assessment to further map out the threats and outputs. This approach raises a couple of issues. Specifically, both false-positive alerts and false negatives for a particular system raise concerns about the lack of reliability of detection for possible cyber threats.

False-positive alerts are those when an alert is considered to be triggered by a legitimate event, while false negatives are issues generated when an alert fails to trigger for a real intrusion. Over the years, a multitude of signature-based IDS has become available on the market, providing a comparable higher rate of detection, albeit at the cost of a highly unreliable detection of polymorphic and metamorphic malware, which work by changing their structure and behavior, making it more difficult to detect them with traditional techniques. Instead, in a majority of cases, the continual bombardment of false-positive alerts generated by current signature-based solutions has caused network administrators to refuse to attend to and eventually neglect IDS alerts as spam. As a consequence, the lack of proper responses represents a significant and ever-growing security threat for almost every organization connected to the Internet.

8.5.2. Slow Response Times

Network resilience is a critical property for the continuing reliable operation of high-assurance systems such as process control networks and sensitive data networks. Although some studies of mechanisms to increase network resilience stretch hundreds of years into the past, modeled threats are not the same as real-world threats, and the cost per absence of industrially occurring network faults is quite high, so further study of alternate methods is called for. In our Fast Worm network testbed, we compare three different network resilience mechanisms to a control. This study extends our previous work by accounting for the theoretical slowest network equilibrium state for a modified implementation of one of the mechanisms that we have developed, along with discussions of how the technology could be used with other network resilience solutions. Our findings indicate that there exists considerable scope for further improvements in the performance of our several proactive protection mechanisms.

Being proactive with information technology enables one to spend a smaller amount of their limited budget of essential resources responding to genuine events. However, one should anticipate both genuine and erroneous slow responses to their proactive measures in some, but certainly not all, of the designs. The most disconcerting of the events that might be anticipated are slower responses to critical real-world, industry-grade threats during a proactive slowdown than would have been expected without any protection in place. We consider the ways that proactive security slowdowns might occur in two of the different classes of proactive vulnerabilities in our Fast Worm network testbed, to refine our experimental procedures for the future testing of slower vulnerable production datasets. We further consider how a protected production acceleration model might be utilized.

8.6. Emerging Technologies in Threat Detection

Security, particularly threat detection, becomes increasingly important when emerging technologies like cloud computing, software-defined networks, social networks, big data, and the Internet of Things develop at a rapid pace. In addition to the security issues, these technologies also bring new challenges to the research and development of new threat detection mechanisms. This chapter studies the opportunities and challenges in IoT, cloud computing, and software-defined networks. We found that these emerging technologies transformed the attack surface and environment, scaled to a huge size, collected or produced a large amount of suspicious data, and created new types of security issues and their characteristics. The Internet of Things (IoT) and cloud computing are becoming widely known and have also achieved rapid development in

mobile scenarios. In addition, software-defined networks (SDN) have become a new trend in future networks, and these technologies have been proven successful in practical designs. Telecom operators and equipment manufacturers are deploying networks or are on the path of infrastructure transformation to accommodate IoT and SDN/cloud. With the rapidly increasing data services, these new systems also bring a huge number of security threats, and traditional security mechanisms do not have the capabilities to identify, trace, and block sophisticated attacks. These new systems are not fully integrated and have some outstanding issues.

8.6.1. Artificial Intelligence and Machine Learning

To address both the lack of global situational awareness and limited proactive defense mechanisms today, we need to improve upon the solutions that we have and develop new techniques that will enable us to discover novel adversaries before any damage to the global infrastructure occurs. One approach to this is through the use of artificial intelligence and machine learning. The algorithms that operate with these approaches can extract characteristic spatial and spectral statistical signatures from disparate data sources to yield statistical modeling or other event prediction for a wide range of applications.

Artificial intelligence and machine learning approaches can automate understanding, prediction, and response. There are two main reasons why these AI/ML approaches are interesting at the current time for network security applications. First, there is an increasing amount of big data generated that is potentially useful for AI/ML approaches. Second, many network security organizations are finding that traditional, signature-based defenses are increasingly ineffective against zero-day attacks and the advanced persistent threat. AI/ML has long been the industry's boogeyman because of its association with classic anomaly-based detection techniques, but in this decade of big data and smarter algorithms, it appears to be ready for something closer to prime time within the cybersecurity industry.

8.6.2. Behavioral Analytics

Behavioral analysis is one of the potential proactive detection research fields, emphasizing accurate detection of malicious behaviors with high resilience against attacks. The detection is not based on predefined malware or malware families; rather, the detection criteria are whether the actual behavior is legitimate or illegitimate and the impact after the behavior, even if caused by legitimate behavior. Known as behavioral

detection or behavioral analysis, the method judges the behaviors by dynamic runtime monitoring, generating static rule motion, or others. The potential cons are the higher proportion of false positive feedback in comparison with static detection and slower response against malicious behaviors while the anti-behavioral detection is installed.

The proposal points out the actual problem of these proactive detection methods and also analyzes the potential research fields, research methods, research objectives, weaknesses, and conciseness, as well as the potential research problem that these existing methods can't tackle. A behavior template collection is established, which is formed by a prior behavior ontology, and ontology classes are defined by analyzing actual malware families, malware behaviors, and advanced persistent threats. Finally, the actual attack scenarios of multiple malware families are provided and proven as convincing demonstration material. The scheme is supposed to work as a module embedded in host-to-network data, and then the scheme judges and responds to all the local network device malicious behavior.

8.6.3. Threat Intelligence Platforms

Threat Intelligence Platforms (TIPs) have emerged as promising solutions, particularly within Security Operations Centers (SOCs), for collecting security-related information from a wide range of sources, aggregating and enriching them, and correlating events to generate high-fidelity alerts. TIPs provide a full lifecycle of threat intelligence activities. It typically includes collection, correlation, collaboration, management, enrichment, and dissemination, and benefits from the context that can be provided by any set of data that underpins a given data lake, thus making the oversight of the general openness and transparency efforts we are targeting particularly relevant to TIPs.

The assignment of managing an organization's TIP might therefore naturally fall within the responsibilities of a team running a SOC. However, the scope and functionality enabled by TIPs span a wider spectrum of data sources, collection, and analysis activities. Complementary technologies are so aligned that we should also consider the organically responsible management of a TIP and the many oversight efforts we target within the introduced transparency and traceability framework. Data sources that are typical within a TIP include but are not limited to, botnets, malware, advanced persistent threats, spyware, vulnerabilities, digital fraud, threat actors, threat feeds, phishing, spam, brute force, payloads, and attack tactics. This would alleviate and bind the history of data originating from any of these sources onto the same historical record as security alerts produced by TIPs that consume the same datasets today.

8.7. Designing Proactive Detection Mechanisms

Network resilience and cyber threat information sharing are not sufficient individually to address the ever-increasing sophistication seen in cyberattacks. The security industry as a whole must get a handle on detecting novel threats and develop timely countermeasures. This applies to network defenders as well, as opposed to more traditional network resilience or security performed by service providers. Service providers typically are responsible for their infrastructure only. The security industry expects daily feed updates to cover new vulnerabilities, attacks, or malware. This daily coverage never seems to be lacking. Security information is available through various publicly accessible sources, third-party threat intelligence platforms, public cybersecurity reports, or deep web monitoring companies. Subscription models are prevalent for commercial threat intelligence feeds from proprietary subscriptions, and a large number of companies offer proprietary options for the delivery of real-time, structured, and processed data suitable for specific business threat environments. Organizations also contribute to the richness and depth of these sources through their data.

It can be argued that not many threat analysis zones exist within traditional enterprise environments. This proposal of extensions to the hyperconnected world seems even more challenging, indeed close to insurmountable. The difficulties involved in analyzing what society's malicious threat broker experts are planning or contemplating through their transactions on the Deep, Dark, and Excluded Web marketplaces are significant. Rather than depending on threat intelligence, it can be suggested that instead, create your own from within the network. Proactively seek and/or detect novel threats as they unknowingly traverse through an organization’s network, or those of its suppliers or partners. Considerable data is known about an organization’s network behavior, meaning that the ability to detect unusual behavior is a gold nugget. Products that capture and store historical network flow data are widely available on the commercial market today. Many of these products historically include algorithms for network threat detection together with the ability to generate structured outputs.

8.7.1. Real-Time Monitoring Systems

Networks dealing with data flows are becoming more complex and also more fragile in the sense that more of their components, which are essential to keep such data flows running, are becoming part of the network. This often presents different types of challenges regarding the implementation and operation of monitoring components and technologies, as they might demand the installation and continuous adaptation of an

increasingly large set of monitoring tools spread through a broadening number of products and vendors, a fact that may pose operational issues and some related overhead. This work focuses on the detection aspects and proposes a way to deliver a homogeneous view of the detection capabilities and provide a multi-source threat information feed aggregated from individual station detections to pruning points or, more specifically, entities defined by the project.

Under these circumstances, the proposed solution will relate and mix the detection information gathered from distinct sources in a way that permits the detection system to detect threats and incidents on the network preemptively and proactively, before any mitigation technologies are put in place to solve the issue, by amplifying some detection system characteristics such as a global and more unified vision of the network for the generic case, and by also promoting special dissemination system characteristics like the transversal network coverage by each of the centralized points where the system stations connect. In this scenario, the solution will cater to three main stakeholder profiles: system operators, mitigation implementers, and finally, attackers.

8.7.2. Automated Response Strategies

The idea of automated response strategies has a strong theoretical basis in the use of radical surgery to stop the epidemic spread of disease. Encouraged by these theoretical underpinnings, many researchers have developed methods to model optimal attack strategies to contain an attack. However, the realization of these theoretical techniques has some practical difficulties. These theoretical methods rely heavily on information about the network; in fact, they usually require exact information about the nodes that are infected. When dealing with multi-agent systems, like the Internet or other communication networks, obtaining this level of information may be a significant constraint. Furthermore, even assuming that our reconnaissance capabilities are good enough, real-time information on the most critical nodes on the network suffers from the extensive time scales for data collection and analysis.

Ad hoc actions, taken directly after experiencing the first symptoms of the spread of a new threat, may slow down to a certain extent the epidemic's spread and allow the introduction of preventive measures. Automated response strategies should be complemented by regular monitoring activities on how the network resilience is behaving in case of analytic performances to detect inconsistencies among theoretical models, detected cause-effect relationships, and real behavior while applying the real-time response strategy.

8.8. Conclusion

Irrespective of the chosen proactive detection mechanism, the ability to detect threats before they can affect the system relies on the successful identification of unusual activity. An important outcome of the research is the provision of a comprehensive compilation of existing proactive detection mechanisms that could easily be implemented in a hybrid fashion to further improve detection success rates. Such refinements can and should be made to ensure that networks can repel malignant actors in the digital realm. A significant future addition to the threat detection process would be the integration with artificial intelligence, specifically machine learning. Deploying an analytics system may allow for the detection of more information, as the system can focus on identifying correlations and previously unseen behavior. The ideal detection system can preempt the creation of threats. While now viewed as an effective part of cybersecurity, techniques to predict malevolent action are still predominantly found within the domain of misinformation and propaganda.

It is beneficial to employ multiple complementary proactive detection mechanisms. Each method specializes in detecting different types of threats, and using multiple methods improves resilience. The inclusion of machine learning within the detection process should be a focus of future work. Intelligence from the detection systems could be used to predict the creation and use of threats, as well as what current trends are developing. This additional phase could then feed into risk assessments for these trends to be classed as emerging threats. The proactive detection mechanisms can be used in the 5G, SCADA, IoT, and industrial control network domains, as well as within organizational networks. The variability of the response mechanisms is also beneficial for integration into these diverse networks. As a result, countless variations on response mechanisms can be used to reduce and remove identified threats from all network types. The techniques are important for maintaining the use of connected digital systems without allowing harmful activities to subvert and disrupt daily routines.

8.8.1. Final Thoughts and Future Directions

The central challenge in network resilience is to thwart the efforts of cyber miscreants to harm network systems and services. While we have seen numerous proactive threat detection mechanisms to achieve this goal, there remains much work to be done in this area. In this chapter, we address some of the overlooked areas, such as the application of thermodynamic concepts to network resilience, as a means to both model attacks and cyber defenses and to measure resilience and vulnerability, as network flow is considerably useful to provide new challenges and deploy an active testbed to validate

whether or not mechanisms work as they were intended. We also make use of a collection of virtualized telecommunication providers. After presenting a summary to provide a point of reference and remind readers of useful contributions, we present some inspiring work – the application of thermodynamic concepts towards resilience and vulnerability assessment of networks and services – in the literature, along with an exploration of its potential and challenges. The majority of effort has been devoted to the study of network profiles and patterns emanating from network flow and the collection of virtualized telecommunication providers by examining the use of such data towards the final evaluation of detection mechanisms. The practical consequences of frequently employing PTDs encompass a shift in focus away from wireless and other unconventional networks or network events that have been discussed to a great extent and are currently addressed both in operational and academic contexts. These future directions describe possible lines of research reflection to assess the practical application and the effectiveness of PTDs for prototyping, training, and development.

Fig 8 . 3 : **Proactive Threat Detection Mechanisms**

References

Buczak, A. L., & Guven, E. (2016). *A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection.* IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). *A Deep Learning Approach for Network Intrusion Detection System.* Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies, 21–26. https://doi.org/10.4108/eai.3-12-2015.2262516

Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2019). *Applying Deep Learning Approaches for Network Traffic Classification and Intrusion Detection.* Computer Communications, 133, 1–9. https://doi.org/10.1016/j.comcom.2018.10.011

Diro, A. A., & Chilamkurti, N. (2018). *Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things.* Future Generation Computer Systems, 82, 761–768. https://doi.org/10.1016/j.future.2017.08.043

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). *A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks.* IEEE Access, 5, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418