ISSN: 2634 - 8853

Journal of Engineering and Applied Sciences Technology

SCIENTIFIC Research and Community

Review Article

Open Access

Mitigating Vulnerabilities in Large-Scale Network Environments: Strategies and Best Practices

Udit Patel

USA

ABSTRACT

In the modern world of networks, managing multiple threats in large-scale network environments is an essential goal of organizations to protect their system and essential information. Measures to counter threats and sources of vulnerability and the chances of cyber threats and cyber incidences are the primary focuses of this paper. Vulnerability management, network segmentation, and access controls are the first pillars of a sound cybersecurity program. Vulnerability management is a repeated process of discovering, analyzing, documenting, addressing, and checking general and individual protection flaws before an attacker can. Dividing the network becomes effective in preventing threats from affecting certain highly vulnerable areas of the network, as well as improving the levels of security control. Adopting robust identity and access management solutions, including MFA and RBAC, adds another layer of protection to the network by limiting access to networks and resources to only authorized users. Furthermore, the relevance of repeating vulnerability assessments and penetration testing is underlined, as these activities help update the information on the organization's security and identify insecure positions. However, factors like the increasing pace of vulnerabilities and the necessity to adapt instantly to novel threats show that protection is not easy. Cyber threats are still on the rise, and as a result, the adoption of the spur) advanced technologies like AI in security frameworks boost detection rates and reaction time. The paper concludes by emphasizing the need for constant monitoring and implementing preventive measures to safeguard against emerging and evolving cyber threats.

***Corresponding author**

Udit Patel, Plano, Tx, 75407, USA.

Received: February 05, 2024; **Accepted:** February 12, 2024; **Published:** February 26, 2024

Keywords: Vulnerability Management, Network Segmentation, Threat Detection, Penetration Testing, Patch Management, Zero Trust Architecture, Identity Management, Multi-Factor Authentication, Anomaly Detection, Continuous Monitoring

Introduction

With the increasing technical environment for large-scale networks, threat management, and prevention have emerged as key concerns for organizations. However, newly evolving threats and even more effective types of attacks require leaders to engage in cybersecurity actions more proactively. This article provides the reader with guidelines on identifying, managing, and mitigating threats likely to compromise networks and cause undesired effects on organizations.

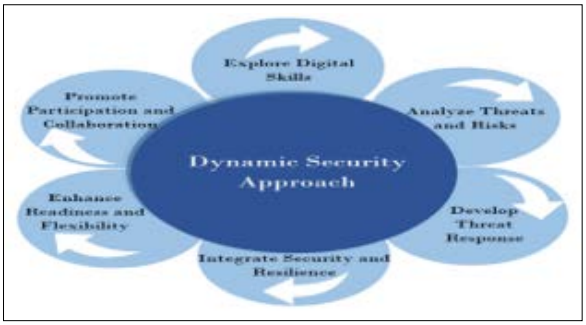

Figure 1: Dynamic Security Approach

The Importance of Proactive Threat Mitigation

Security is another fundamental aspect that seeks to protect the physical structures against all possible hazards [1]. Such losses include money, loss of reputation, and penalties that hackers can make the organization suffer from the regulatory body. It has been argued that the risks arising from hacking attacks, viruses, and threats to information systems can be minimized through early identification of threats. That is where proactive management of risks comes inapposite to a way real response organization, which enables businesses to handle security risks before they exploit the vulnerabilities. Because of this high speed of operation, detection and prevention techniques should be used in real-time to address threats to the most crucial assets.

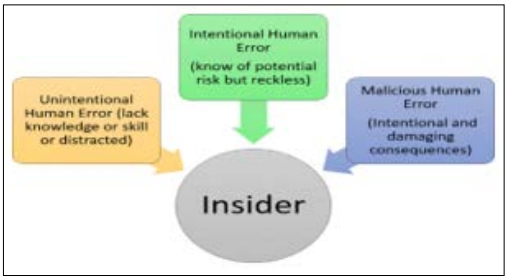

Figure 2: Review and Insight on the Behavioral Aspects of Cybersecurity

Overview of Key Strategies

The rationale of this article is the analysis of many measures aimed at improving the effectiveness of network protection. One of them

is vulnerability management, which is a cyclic process that aims to assess, rate, and handle risk before it turns into a major issue. Realizing vulnerability management would require automation but under the guidance of experts who would identify these weaknesses and correct them. The other measure implemented, as presented in this article, is network segmentation. Organizations can limit the areas of compromise to certain parts of a network and hence limit the movement of an attacker [2]. The logic to justify segmentation is that even if an actor manages to get into one segment of the network, the other segments are impenetrable for all intents and purposes. These are scans that a firm can make to determine other people's opinions on a firm's present system, applications, and networks. These assessments help the management of an organization identify its vulnerabilities and correct them before they are taken advantage of. Implementing strict physical access controls, the identity management system, measures like MFA, and role-based access control means only authorized employees get into the systems. They deny any other person a chance of accessing this network, increasing the security of the entire network [3]. Where applied and incorporated, these measures shall further enhance the organization's protection against cyber attackers and lay down a better network platform with which to work.

Figure 3: Vulnerability Management Strategy

Understanding Vulnerability Management

Definition of Vulnerability Management

Vulnerability management is a continuous process of identifying, assessing, and treating IT asset risks as weaknesses to the corporation's security status [4]. The end option is to lay down measures that assist in assessing, managing, and eradicating the risks to counter the agenda of the attackers. This approach is more holistic than remedial to the issue of cybersecurity. Based on the findings of Poslajko et al, one can highlight that vulnerability management is an essential component of network security since it is designed to evaluate and adjust protection continually [5]. Unlike such practices where the problem is identified and then worked on once the attacker has utilized it, vulnerability management deals with the threat and prevents it from degenerating into a vulnerability that would cause immense damage to the business.

Stages of Vulnerability Management

Vulnerability management follows a structured process, typically broken down into five key stages: The Ditty Cycle refers to discovering, assessing, reporting, remediating, and Verifying.

- **Discover:** The discovery stage is the first of the stages in the vulnerability management life cycle [6]. Here, an organization identifies and catalogs its IT resources like the computers, servers, applications, and networks, among others, that can be referred to when determining the risks. It is critical to have a record of all the resources to verify all the systems and potential flaws in the domain. They also need to account for the devices and systems that are overlooked in their regimes of operations but may still be hacked and breached, although they are inactive. Such obscured assets must be revealed because they are often left unprotected and may open doors to threats [7].
- **Assess:** The assessment process must follow after identifying and categorizing the assets. In this phase, testing is conducted to identify the areas of vulnerability and the extent of the weakness. This refers to penetration testing tools where vulnerabilities are detected and exposed, including common vulnerabilities in the system, devices, and applications. Summers et al, argued that an accurate testing process is critical since it helps security personnel identify the risks to target the firm's most likely impacted strategic systems [8]. None of the identified vulnerabilities are unsafe, although some could be interpreted as such, so there is a need to classify them in a way that would allow for using the limited resources available for risk management to deal with the most severe threats first.
- **Report:** The third activity involves the preparation of a detailed report of all the vulnerabilities that have been identified. In this report, we often define the risks or threats related to certain risks to the organization. In the reporting stage, it also offers remediation plans that make it possible to eliminate the vulnerabilities discussed during the implementation. Following Gupta and Qamar, it is essential to note that reports are much more than technical; they must be accessible to all across the organization [9]. This makes it easy to liaise with other departments and contributes to the non-technical employees' understanding that the vice also has a downside on the business.
- **Remediate:** Once vulnerabilities have been analyzed and a record made, rectification commences. This stage involves implementing corrective measures about the weaknesses that have been identified; this remedial process may in this stage, different steps are taken in order to rectify the vulnerabilities that have been discovered; this can be accomplished through 'curing' such weaknesses by applying patches, updating systems among other procedures that can wipe out the stated vulnerability. The measures that can be involved in the remediation process include patching applications and operating systems, changes in the configuration, or introducing new controls. Organizations may also use compensating controls such as IDS and network segmentation while acknowledging the risk and waiting for a permanent solution [10]. As such, monitoring is always necessary to ascertain that the vulnerabilities have been closed adequately and have not reopened.
- **Verify:** Verification is the final procedure of the vulnerability management process and aims to confirm the outcome of the remediation efforts. This stage ensures that open exposure has been appropriately closed to minimize risk discovery. Verification involves exposing the system, evaluating the remediation activities, and examining the pleasant results. As noted by Pavithra et al, the process also helps to ensure that the heads have received affirmation that mitigation has been effective and can help organizations improve their vulnerability management for future progress [11]. Another essential aspect that should be remembered is the necessity for regular checks and evaluations to maintain solid network security.

Table 1: Stages of Vulnerability Management

Stage	Description	Key Activities
Discover	Identifying and cataloging IT resources, including computers, servers, applications, and networks.	Catalog all IT assets, including overlooked or inactive ones.
Assess	Testing identified assets to discover vulnerabilities and their severity.	Conduct penetration testing, identify vulnerabilities, and classify them based on risk.
Report	Preparing a detailed report of identified vulnerabilities, including risks and remediation plans.	Create accessible reports for all stakeholders, define risks, and suggest remediation plans.
Remediate	Implementing corrective measures to address the identified vulnerabilities.	Apply patches, update systems, change configurations, and use compensating controls.
Verify	Confirming that remediation efforts have effectively closed vulnerabilities and assessing the results.	Evaluate remediation effectiveness, conduct regular checks, and ensure ongoing security.

Tools and Technologies for Vulnerability Management

One of the conclusions that can be made is that vulnerability management needs automated instruments and analysis procedures Rameder et al, some easy tools include Nessus, Qualys, and OpenVAS, which can also conduct the discovery and assessment phase of vulnerability, giving lists of known vulnerabilities on various systems. These are used for significant search sweeps, report compilations, etc. However, it remains clear that such tools sometimes come across fake positives, as Almohri et al, noted [12,13]. Other ancillary tools that may be used in patching include the Microsoft SCCM (System center configuration manager) and IBM BigFix, which has an auto-patching feature that eliminates the patching by a software update and patch deployment. Moreover, for the remediation and verification work, tools such as Security Information and Event Management (SIEM), including Splunk and ArcSight, help in correlating the vulnerabilities with threat intelligence feeds, thereby enabling better judgment in terms of prioritization [14].

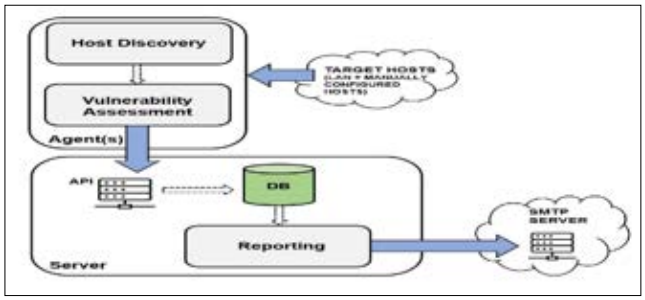

Figure 4: Graphical Representation of the Relationship between this Artifact's Modules (Arrows Depict Data Flow)

Critical Challenges in Vulnerability Management

Vulnerability management has issues as a sub-process of an Information Technology security program. The first one can be defined as an informational challenge per se, which addresses the number of threats that exist for organizations. According to Pavithra et al, security professionals need help to effectively prioritize the numerous threats that AI unveils to identify the most pressing threats that need urgent response [15]. The other challenge is institutionalizing vulnerability management as an ongoing evolving process to meet emerging risks. Since there is an increase in the number of cyberattacks daily, it is apparent that the vulnerability management that needs to be applied today and in the future must also be dynamic. According to Gupta and Qamar, achieving efficiency within organizations in rectifying these shortcomings and simultaneously meeting the operational necessities of applying fixes and testing vulnerabilities in critical systems is always an accomplishment, given the time factor, mainly when system downtime rapidly results in loss of resources. Depending on the model applied, there is the potential for error in assessing vulnerabilities in the sense that false positives and negatives can occur, effectively meaning that resources could be considered inefficient or that threats could actually be overlooked. In order to put up a compelling security necessity, adequate equipment and specially qualified staff must be used to analyze the risks and allocate them suitably [10,16].

As a result, vulnerability management is critical to safeguarding networks and systems in the current world. It means that risks can be prevented before they are exploited, and risks can be identified, evaluated, notified, corrected, and confirmed regarding vulnerabilities Khan et al, therefore, the number of identified vulnerabilities, their priority, and the requirement for qualified estimation demonstrate that the use of automated tools indicates that they are optimal when used to supplement human input to realize the best result [17].

Network Segmentation for Security

Network segmentation is one of the critical security measures that implies the division of an extensive network into yet smaller portions referred to as sub-networks [18]. This practice is applied to minimize the exposure inherent in the access and malware spread so that the network administrators may have nuanced control over data traffic. With new complex networks being deappropriate, models are required to manage such threats and enhance security. It is important to note that the ability to implement network segmentation will lead to better control over traffic and resources used in the network, leading to better security measures and efficient functioning [19].

Concept of Network Segmentation

Network segmentation refers to the act of dividing a network into several parts that are isolated from others in order to restrict access in order to increase security [20]. The idea is to prevent any interaction with the crucial sections of the network, meaning that only approved clients or some gadget should be able to acquire a few specific subnetworks [21]. For instance, by slicing a network, an organization can devote User Groups or applications with different security requirements to deter vulnerability in the aspects of the system from affecting the whole system [22]. The segmentation can be done by using Internet Protocol (IP) techniques such as virtual LANs (VLANs) and firewalls or by using access control lists (ACLs) [23].

Network Key Segments

One of the most typical forms of network segmentation is the division of the company and the external guests. Corporate networks always consist of critical information and assets that are critical to its operations, hence the need for tight security [24]. Guest networks only allow internet connections without connecting with the internal network. This isolation is important in preserving the security of the core network [25]. Guest Wi-Fi should act as a separate network with restricted access to avoid accessing core facilities and corporate resources. One more critical area is the demilitarized zone network (DMZ). DMZ is a neutral ground or an isolated network between a company/organization's internal network and the Internet, where various services such as web, mail, and external-facing applications reside [26]. By positioning such services in DMZ, organizations can regulate traffic from the Internet. Even if one of the servers is compromised, the internal environment will not be compromised [27].

Like CD and CT networks, Development and Testing networks must be separated from production systems. Software development environments provide open access to developers to test new features and, therefore, may contain hostile code. This way, organizations can avoid such loopholes compromising operational systems, as stated by Bocetta et al, following the trend of development networks [28]. It also enables developers to test without affecting the actual environments, offering a safer and more stable production network. Server and departmental segmentation are other significant elements that must be overlooked. Integrated organizations may have various departments, including finance, human resources, and operations, as some may contain sensitive data that must be kept secure. Each of these departments is segmented, and only the authorized staff within the specific department can access this information, which minimizes internal threats [23]. Likewise, servers for sensitive applications should be isolated from general users' networks to reduce exposure.

Physical security and communication systems usually need their own separate community. Computing devices like video monitors, door controls, intercoms, and so on should be kept from the building's standard network Huang et al [29]. This minimizes the risks of tampering with the equipment and means that high bandwidth, which may be required in video and communication systems, does not disrupt the workings of the regular networks [19]. Industrial control systems (ICS) and HVAC systems should also be segmented to enhance their security. These systems constitute part of the physical infrastructure in buildings and have been established to run with little or no security measures in place. When incorporating these systems, isolating them from the other corporate networks is an excellent strategy to avert control of Trojan attacks on OT systems.

Benefits of Network Segmentation

Another huge advantage that comes with network segmentation is the control of the spread of the malware. If a network is not segmented, the malware will infest all the segments, affecting many devices and providing access to many services [26]. Still, suppose a network is compromised into isolated segments. In that case, the infection will remain localized to a specific segment, and the administrator can resolve the problem, although it will not grow into a more significant violation [22]. Another benefit that one can easily associate with such a system is the control of access by unauthorized persons. Separating the network into different subnetworks helps the administrators apply more strict policies concerning data access by assigning the user roles and responsibilities [27]. For instance, an employee in the marketing team is not supposed to access information related to the company's finances, and network segmentation can guarantee the implementation of such restrictions. This principle of least privilege helps minimize the chances of insider threats and every attempt towards unauthorized access.

Another advantage is an increase in monitoring. The administrators can regularly oversee the network traffic by partitioning the network and identifying any malicious activity. This helps implement differentiated IDSs and SIEM systems that can be specific to higher-risk areas and offer improved visibility of threats [26]. Network segmentation is a security strategy that actively supports increasing the efficiency and security of modern networks. Dividing the network into segments minimizes the chances of the disease spreading and hampers the population's access while helping organizations enhance their surveillance. Segmentation also applies to the company'scompany's activities, including corporate and guest Wi-Fi, development networks, and industrial control systems. It should be considered a fundamental element of the security system. An organization needs to develop a sound network segmentation plan, ensuring its security requirements are met to contain critical data and systems.

Regular Vulnerability Assessments and Penetration Testing

The Role of Vulnerability Assessments

Vulnerability assessments are critical in cybersecurity since they help present the blind spots within systems and applications Eshetu et al [30]. A vulnerability assessment's main objective is to systematically examine a network, hardware, or software application to determine which part of it is at risk, what class of threat it falls under, and how soon it is susceptible to risk [31]. The goal is to identify weaknesses the attacker might leverage and derive recommendations to enhance security. Such assessments usually include fully automated and partially automated techniques to identify identified vulnerabilities in systems and applications [32].

As a result, organizations rely on vulnerability assessments to be as prepared as possible for any security threats. In this respect, assessments cover networks' configurations, databases, and software applications to determine appropriate security measures based on the changing threats [33]. Detecting weaknesses in a system, such as old software versions and incorrect firewall settings, helps the organization overcome them before they are exploited [31].

Figure 5: Why is a Cyber Vulnerability Assessment Important

Penetration Testing

Vulnerability assessments are different from penetration testing, otherwise known as ethical hacking, in that while performing the tests, potential threats and risks are imitated to identify weaknesses. A vulnerability assessment may identify where

these are, but penetration testing does more to find out if any of these fractures can be leveraged. A penetration tester uses all the techniques the attacker uses to gain entry to the system, helping an organization understand how an attacker might use a vulnerability. Penetration tests are typically divided into two categories: internal and external. External penetration testing focuses on weaknesses that may be easily exploited from the company's external environment, such as the World Wide Web. Internal tests, in contrast, mimic assaults coming from inside the organization, such as an insider attack or an attacker with access to the targeted network [34].

Figure 6: Factors Demanding the Need for Regular Pentesting

Steps for Conducting Assessments and Penetration Testing

Vulnerability assessments and penetration tests consist of several essential steps that help to make the analysis sufficiently comprehensive. Although these steps differ for each method, they are sometimes parallel in identifying and dealing with weaknesses.

- **Reconnaissance:** Introduction Reconnaissance is the first process in penetration testing and vulnerability assessment Lachkov et al [35]. This phase entails collecting as much information as possible about the target system, including the network structures, the target system's IP addresses, and the open ports [36]. The knowledge-gathering stage is critical because it is easier to take advantage of a weakness when an attacker understands a target. In vulnerability assessments, this information may be obtained using a web vulnerability scanner during screening, while in penetration tests, web research and social engineering may be employed.

- **Scanning:** The second general step of penetration testing consists of groping or sweeping for vulnerabilities in the target network or application. Network vulnerability scanning tools such as Nessus or OpenVAS are normally employed to identify vulnerabilities and assess the security of the system in question [37]. The purpose is to explore opportunities for entry that could be vulnerabilities in the next stage.

- **Exploitation:** In penetration testing, the fourth phase is where the tester looks at how he can invade the vulnerabilities seen during scanning. This might include introducing viruses, using poor passwords, or compromising confidential data [36]. In some vulnerability assessments, this phase may still need to be done since the aim is only to discover the loopholes in the systems.

- **Post-exploitation:** After a weakness is penetrated, the general objective of a tester is to determine the actual impact the exploiter can make. For instance, if the tester attains access to the data, they will identify the amount of data one can steal without being noticed [38]. This stage is helpful for an organization to know the consequences of hacking and assist in finding measures to counter the occurrence.

Table 2: Steps for Conducting Assessments and Penetration Testing

Step	Description	Methods and Tools
Reconnaissance	Collecting detailed information about the target system, including network structures, IP addresses, and open ports.	Use web vulnerability scanners (for assessments), web research, and social engineering (for penetration testing).
Scanning	Sweeping for vulnerabilities in the target network or application.	Employ network vulnerability scanning tools such as Nessus or OpenVAS.
Exploitation	Attempting to exploit identified vulnerabilities to determine their impact.	Introduce viruses, use weak passwords, or access confidential data (more relevant to penetration testing).
Post-exploitation	Assessing the actual impact of the exploited vulnerabilities, including potential data theft or system damage.	Determine the extent of access and data exposure; helps in understanding the impact and developing countermeasures.

Documentation and Prioritization of Findings

Recording of vulnerability assessment and penetration testing results plays a critical role in security procedures and planning [39]. On the same note, the documentation is advantageous in that it captures all the identified risks and potential risks that may come with these vulnerabilities [40]. In vulnerability assessments, there are often automated generated reports that provide overviews of the vulnerabilities discovered and their severity levels so they can be prioritized and addressed in the order of importance. While a scan may come with an email or small report, penetration tests can come with a more in-depth report that details how the vulnerabilities were utilized and the procedures taken during the test. This step must be taken to ensure that the most critical vulnerabilities are addressed first. Some can be highly vulnerable and not easily prone to attack, while others who are low in vulnerability are easily prone to attack [33]. Priority can be assigned to vulnerabilities, which will help identify which issues need immediate attention and resources for fixing them.

Remediation Strategies

Having assessed and recorded vulnerabilities, one has to devise plans to deal with or reduce risks. Remediation can involve installing programs, perhaps as updates or patches for the vulnerability, or making configuration changes [32]. Occasionally, measures that are further reaching, for instance, redesigning part of the network or enhancing the over-access control procedures, may be necessary to counter security vulnerabilities. Organizations must ensure that remediation is continuous to achieve the desired result of eliminating the problem. Each time new threats and risks are identified and the threats come up with enhanced strategies, the organization must upscale the system [34].

Frequency of Assessments

Another set of questions that must be answered is related to the frequency of vulnerability assessments and penetration tests. These assessments should be conducted frequently across organizations. However, the frequency of the assessments will vary depending on factors like the organization's size, the legal requirements of specific industries, and risk tolerance levels [38]. For instance, more sensitive industries, such as the financial or health sector, may need more frequent assessments because of the type of data they process. Another purpose of 'time-based' assessments is to conduct them after a significant shift in the network, for example, after the inclusion of new technologies or redesign of the network frameworks [32]. Penetration tests are usually conducted at least once or twice a year, but more often if required to take more risk due to the nature of the organization's affairs [33].

Figure 7: Network Security Vulnerability Assessment

Learning from Vulnerabilities

The information collected during vulnerability assessment and penetration testing can be considered a knowledge base for enhancing security processes. By assessing underlying risk factors, different prevention mechanisms may be applied to eliminate the system's susceptibilities to future exploitation [37]. These repellants and assessments must be made systematically, with updates on security being made periodically to counter new and improving threats. Moreover, it is crucial to note that learning from vulnerabilities entails multiple teams, including IT, cybersecurity, and management. As argued by Kunz et al, organizations should be adequately prepared to meet the challenges posed by modern-day cyber threats by creating cultures for constant learning and improvement [34].

Implementing Strong Access Controls and Identity Management

In the modern world, where news about hacking, data breaches, and cyber-attacks are standard, an organization must have reasonable access controls and identity management. Comprehensive IAM specifies which people should have access to which resources and enforces the restriction. This process comprises several techniques, for instance, Multi-Factor Authentications (MFA), Role Base Access Control (RBAC), and the Principle of least Privilege. They all work in concert to mitigate risks such as invasion of privacy, theft of data, and inefficient utilization of resources in the organization and, hence, foster a comprehensive and solid organizational structure [41].

Identity and Access Management (IAM)

IAM stands for Identity and Access Management, which is how organizations deal with digital identity and secure their business's resources. These have made IAM crucial as more organizations move to cloud environments and adopt remote working. By implementing IAM, an organization can regulate the authentication procedures and keep track of users' activities to ensure that only the right people are granted access to specific resources [42]. This system means that the users will be well-identified and privileged accordingly to minimize cases of unauthorized access or intrusions. IAM can complement a firm's current security policies and form a multi-layered security system against cyber threats.

Multi-Factor Authentication (MFA)

Multi-factor authentication, or MFA, is one of the fundamentals of effective IAM. This makes the system demand several types of identification from the users from the users to gain access to a system in addition to the standard login identification, such as a password [43]. Research carried out by Aloul shows that MFA can reduce the contraction by up to 99% [44]. It is one of the most effective forms of cybersecurity, with 9% of cyber-attacks being prevented by firewalls. It is attributable to the need for other authentication factors that, in most cases, are in the form of passwords, smart devices, or biometric features such as fingerprint or face recognition [44]. As mentioned earlier, MFA comes in different forms, and some have different security levels. Application-based MFA, for example, employs Google Authenticator, where the user is presented with time-sensitive codes, whereas, for Smartphone-based MFA, the user receives verification codes through an SMS. Despite the frequent use of SMS-based MFA, for example, SIM-swapping attacks remain, which became a problem well described by Cheng et al., 2017. However, because of certain drawbacks related to specific techniques of using MFA, it is still relatively efficient for protecting access to resources.

Role-Based Access Control (RBAC)

Role-Based Access Control, or RBAC, is another way of limiting the access rights of a system depending on the user's position in the institution. Such an approach reduces the likelihood of data misuse since only people with relevant workplace roles are allowed access to the required data resources. The RBAC grants permissions according to already defined and designed roles, thus reducing the chances of encountering undesired permissions or granting more than necessary [45]. Since RBAC restricts access based on job responsibilities, it offers a unique insight into avoiding internal threats and accidental information leakages. While implementing RBAC, several essential measures should be taken to achieve the desired results. Initially, organizations' components must analyze user roles and decide which permissions are required for every position. Subsequently, there is expected to follow role definition and the allocation of responsibilities of each user concerning their roles [46]. As such, organizations should frequently update role assignments to match job modifications and only retain users' privileges when it is essential, helpful, and appropriate. The next step is to map RBAC with security policies and compliance standards integrating methods, guaranteeing that the implemented access controls comply with suitable benchmarks [45]. If these steps are followed, it is possible to ensure RBAC implementation and protect the organization from potential intruders.

Least Privilege Principle

The PoLP is the second significant aspect of access control, which restricts a user's rights and capabilities to only the level necessary to complete their tasks adequately. This Principle states that users should be allowed the few rights they require in their working capacity and that rights should only be temporary [47]. It also prevents the attackers from gaining access to other systems connected to the Internet, and in case of a security breach, PoLP limits the extent of the damage. Even if the attacker can log in to a user's account, his/her actions will be restricted in such a way.

PoLP can only be accomplished by determining the different users and tasks they perform to avoid unnecessarily granting permissions. Also, access should be limited as much as possible, meaning that whenever users require certain privileges, they should only be granted for some time, and then, after some time, review whether the user still requires those privileges. In the case of cloud computing, PoLP becomes even more important because the threat of unauthorized access is even higher due to the distributed nature of the cloud [42]. Thus, implementing PoLP can easily avoid the leakage of sensitive data and decrease security threats.

The best approach in enforcing access controls and identity management to protect an organization's resources is to practice strict measures on people's access. Proper Identity and Access Management (IAM) enables the organization to regulate the access of the systems and data by giving permissions to the right people. MFA stands for multi-factor authentication, hence adding several layers of security, as it is difficult for hackers to breach a secure system. Access control methodologies such as RBAC restrict user privilege to only those resources necessary for work. In contrast, the Principle of least Privilege (PoLP) provides the most minor level of access possible. Altogether, these strategies constitute a coherent concept of access control and identity management that can protect organizations against certain risks.

Zero Trust Architecture

Zero Trust Architecture (ZTA) is a new cybersecurity architecture that adheres to the principle of do not trust and do not assume that everything is valid. This model is crucial in today's environment, especially with the emerging intelligence and complex internal and external threats. While the other security models rely on the concept of secure boundary, Zero Trust postulates that the enemy is already within the network. Hence, maintaining security requires continuous authentication of users, devices, and applications. This architecture has attracted interest because it minimizes the threats of cases and addresses challenges within complex structures and systems in vast networks [48].

Figure 8: Zero Trust Architecture (ZTA)

Definition of Zero Trust

The foundation of Zero Trust is never to trust any entity, internal or external. Classically, network security has been based on the mentality that threats reside outside the network, which caused the exclusive focus on external protection. However, the perimeter model has yet to be effective due to the increasing cases of insider threats, mobility, and cloud computing. Zero Trust recognizes this shift; it postulates that all requests for access to resources should be authenticated, authorized, and encrypted, irrespective of the source. According to NIST, Zero Trust is a security model characterized by the principle that no user or program is trusted by default, and even authorized users and applications must continuously authenticate themselves before they can be granted access to the resources that are within the organization's restricted network [48].

Principles of Zero Trust

Several principles have been defined to distinguish Zero Trust Architecture from traditional models. These include the assumption of breach, continuous verification, and least privilege access.

- **Assume Breach:** In the Zero Trust operation model, organizations assume that the organization's network has already been penetrated. This thinking pattern departs from the view of prevention to that of containment so that the loss is curtailed in the event of a leak. In line with what was noted by one of the pioneers of the Zero Trust concept, Kindervag, no trust is given implicitly to any user or device, thus stopping the transfer of the intrusion into the network [49].
- **Verify Every Device and User Trustworthiness:** Identity and device assurance is at the core of Zero Trust. This process entails authentication not only at the time when a person is requesting a connection but also during the session. This means that dynamic access policies are enforced based on conditions, including the health of the device in use, the behavior of the user, and the level of sensitivity of the resource in question [50]. MFA solutions and EDR systems are essential elements in defining the access of users and devices to the network, which are considered trusted by the network.
- **Enforce Least Privilege and Continuous Verification:** The principle of least privilege implies that users or devices should be provided with the least access rights necessary for their operations. As such, Zero Trust significantly reduces the risks if an unauthorized user infiltrates the network. Another benefit is that it is possible to monitor the activity continuously so that even authorized users would not go beyond their allowed access level [51].

Adaptive Security Concepts and Zero Trust

Another benefit of Zero Trust is the ability to employ adaptive security and thus be more flexible in the face of threats Sarkar et al [52]. Adaptive security is entirely different from the static security models as the former deploys real-time data analysis, including machine learning techniques, to analyze the variations in security parameters. Tightly integrating with traffic analysis, analyzing user activity, and detecting the unhealthy state of the device allows one to recognize threats and prevent them from affecting the organization [53]. By embracing this dynamic approach, one can improve the network's resiliency and maintain security practices proportional to the threats as they emerge.

Benefits of Zero Trust

Zero Trust has many advantages, making it a suitable solution for the present-day company. First, it has boosted the company's security from internal and external threats. Zero Trust works on the principle of trusting that no user and device are harmless and confines the threat moving around in the network. Moreover, since access is constantly checked, the model locks the attackers' ability to horizontally navigate through the network, which is typical in advanced persistent threats [49]. The other potential of zero-trust models is that they help decrease the attack vector. In standard security paradigms, once the user or device gains access to the network, she or he enjoys almost full access, which the attacker can leverage. Zero-trust helps minimize this risk by limiting privileges. Even if the attacker has managed to get inside, their options are pretty limited [48].

In addition, Zero Trust increases the organization's conformity to regulatory frameworks' requirements, especially in terms of data protection and privacy. In this manner, organizations can

prove they are doing everything within their power to guard their assets and minimize the risk of paying hefty fines for failing to adhere to compliance laws [50]. Therefore, Zero Trust Architecture can be best described as a revolutionary paradigm in network protection. Zero Trust, when implemented through assuming breach, continuous user and device verification, and least privilege, minimizes the possibility of attacks and ensuing losses. It has an adaptive security feature that enables it to respond to new emerging threats in the system, making security more effective at any given time. Subsequently, as threats are progressively becoming more sophisticated, organizations must embrace the implementation of Zero Trust to safeguard their respective networks and information assets.

Continuous Monitoring and Incident Response

The Importance of Real-Time Monitoring for Early Threat Detection

Situational awareness is an integral factor in the contemporary approach to cybersecurity, as it allows us to identify threats and respond to them in real-time [54]. The emergence of advanced world cyber threats makes it even more challenging for organizations to prevent proactive measures that enable early detection to reduce effects on sensitive data and systems. Real time enables the detection of such suspicious activities as they occur, an important factor in minimizing the time between the detection of breaches and response to the same [22]. Threats might remain dormant for a while, so the attackers will have ample time to seize on any weaknesses.

Steps in Continuous Monitoring

Continuous monitoring must be thorough so that any prospective threats can be easily identified. Below are the key steps involved: Below are the key steps involved:

- **Event Collection:** The first process of continuous monitoring is event collection, which entails pulling information from one or many media sources together with events originating from system logs, network traffic, and users' activities. These sources yield information that can signal the existence of a malformation or peril [55]. For example, system or network monitoring can show various symptoms, including leakage or unauthorized access. It is necessary to configure the systems to gather all the data from each main asset.
- **Centralized Log Management:** After collecting data must be stored, which is why centralized log management systems are used. SIEM platforms are critical in this process since they help analyze the various messages being generated. SIEMs enable organizations to capture logs from several sources, allowing for the secure single-point viewing of security events [56]. It makes sense to centralize this data and makes identifying possible threats from a large amount of information much more accessible.
- **Log Analysis:** The next step, when all the information is collected, is to study it and look for regularities, variations, or any appearances of the activity of an intruder. This stage is performed by means of the automated tools implemented in the SIEM platforms, based on the set of predefined complex rules and machine learning algorithms, which help to find the traces of the attacks with the help of determination of the unusual big data [57]. For instance, many connections going out could mean the system dumps data outside the organization's network. In contrast, multiple login attempts with invalid credentials might mean the system is undergoing a brute-force attack. Accurate log analysis is the key to identifying specific risks among today's enormous amounts of generated log data.
- **Security Event Correlation:** Security event correlation is the process by which multiple security incidents in different systems are associated to discover additional elaborate attack patterns. Event correlation is, therefore, targeted at analyzing how these and other different events may be connected and implement one part of a more complex attack plan [58]. For instance, associating several login attempts from an unauthorized source with anomalous access to files may signal a concerted attack on a system. Finding such relationships enables an organization to discover attack sequences comprising several stages that remain undetected.
- **Incident Response:** While continuous monitoring centers on risk recognition, incident response is on risk containment once an attack occurs. An effective incident response plan is the only way to reduce the effects of the security incident and avoid other losses.

Steps to Minimize Damage during a Breach

In case of a breach, the focus is made to mitigate the threat and reduce the effect that it may have on the organization [59]. This may include quarantining the compromised systems, controlling access to them, and procedures that could halt the spread of the virus ma, malware, or any other related threats [60]. Data loss has to be addressed at the earliest to avoid much loss and problems for the business. The other thing that the incident response team has to commence is the process of data collection of evidence, which will assist in identifying the level of intrusion and subsequent remedial action.

Role of Incident Response Teams in Mitigating and Resolving Incidents

Security response teams significantly contribute to effectively handling continuing threats and eliminating a security breach problem. These teams, which are usually composed of those with expertise in cybersecurity, are tasked with reporting and working with other departments of the firm to take the proper measures before, during, and after the breach [61]. Some tasks that can be assigned to them are identifying the attack vector, finding workarounds for the situation in the short term, and looking for ways to avoid such an attack in the future. Continuity assessments are essential after an actual event in order to evaluate potential vulnerabilities that may exist in an organization's protection system.

Compliance Monitoring: Ensuring Adherence to Regulatory Standards

Besides threat management, monitoring and response must constantly be carried out to ensure compliance with the set regulations. Some sectors like finance and healthcare have regulations on an organization to scan and detect security violations and to report them in the shortest time possible [55]. Noncompliance with these regulations attracts huge penalties, leading to reputation loss among organizations. There are many reasons why compliance monitoring is essential for organizations, such as maintaining current standard security features and properly documenting incidents. SIEM tools are handy because they retain logs that could be used during regulation assessments to ensure compliance. Unceasing vulnerability scanning and incident reporting are foundational to cybersecurity. Real-time monitoring, centralized log management, and event correlation help the organization identify and contain threats early. Incident response teams are vital for managing risks arising from breaches, preventing disruption of business operations, and meeting legal

mandates. This proves that cyber threats remain relevant, and a monitoring and response framework is necessary.

Patch Management

Patch management is a universally accepted practice in information technology whereby software changes are regularly and systematically made to reverse weaknesses in the system and optimize performance [62]. Patch management is vital for maintaining security against new threats, and improper patch handling is dangerous for organizations. Due to the high complexity of cyber, patching must occur most efficiently and frequently to ensure that IT systems remain secure, protected, and fully operational. This section details the concept of patch management, the components and difficulties inherent in the process, and practical approaches that can aid organizations in overcoming these difficulties.

Figure 9: Patch Management Overview

Importance of Patch Management

Patch management is critical in managing the security IT environments since it deals with software vulnerability. They are produced by vendors to deal with security vulnerabilities, correct program defects, and improve application performance. When systems are not patched on time, the doors are open for cybercriminals to capture the existing opportunity to penetrate, causing massive data and services to be down and leading to financial losses, according to Albert and Doroffee [63]. According to a study by Kaspersky Labs, around 60% of cyberattacks occur because of unpatched vulnerabilities, thus stressing the significance of proper patch management [64]. Patch management addresses risks and caters to many compliances, including the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) compliance that require organizations to protect their systems [65].

Critical Elements of Patch Management

- **Creating an Asset Inventory:** Inventorying potential assets is the first important step of any efficient patch management strategy. From this inventory, organizations can quickly identify all Systems, Apps, and devices on the organizations' network. Alberts & Dorofee point out that having an up-to-date asset inventory is very useful when deciding which assets need a patch or which might be at risk for particular threats [63]. The details that should be in the inventory include the operating systems, software version, and configuration of all the assets to enable one to prioritize applying patches according to the asset's criticality.
- **Risk Analysis and Patch Implementation:** Patch management is not all about urgent patches, but risk analysis is an integral factor to be considered when patching. A risk-based approach focuses on patching to determine the seriousness of the risks and the impact if they are exploited. For example, the patches that resolve the high-severity vulnerabilities that allow attackers to execute code on the user's device must be considered more valuable than the simple bug fixes [66]. In vulnerability management, various organizations employ tools that enable them to identify critical issues that warrant attention and assess risks that require patches to be given high priority. This approach reduces the impact likely to be incurred while patching, enabling the organization to attend to the most severe threats as soon as possible.
- **Patch Announcements and Staying Current o:** Software vendors are constantly issuing patch announcements whenever vulnerabilities have been identified, and one must always be abreast of such announcements. Most vendors have mailing lists, forums, or online pages where they post the availability of patches and the procedures to follow for patching [67]. From the announcements made by organizations, mechanisms must be implemented to track such issues, and patches must be applied as soon as possible. The stream of safety used here does not provide extended periods that hackers can exploit with a list of vulnerabilities present within this type of network.
- **Testing Patches before Deployment:** Such actions must be tested in a more controlled environment when applying patches to all systems. These patches may contain certain incompatibilities that affect other applications that interrelate with them, affect other organizational activities, or cause the system to fail if they are not adequately tested before implementation [68]. Applying patches to noncritical servers or in a test lab environment verifies that the update will not degrade the performance of organizational IT infrastructure. Identifying potential issues ahead of time will help organizations prevent losses through time and disruption of services.
- **Automating Patching Processes:** There is no doubt that automation is of continued importance in improving patch management operations. Some benefits of patch management include capability patches, self-scheduling the patches, and installation within the network with minimal human intervention [69]. Automating patch deployment decreases the possibility of human error and mitigates the variability associated with patch application, freeing resources to work on more critical tasks. Furthermore, using automated systems also ensures that patches can be distributed at certain times of the day and night, thus causing little interference to the business.

Table 3: Critical Elements

Element	Description	Key Points
Creating an Asset Inventory	Catalog all IT resources, including systems, applications, and devices. This helps identify what needs patching and prioritize based on criticality.	Detailed inventory including OS, software versions, and configurations.
Risk Analysis and Patch Implementation	Assess the risks associated with vulnerabilities to prioritize patches. Focus on high-severity issues that can have significant impacts.	Risk-based approach to prioritize urgent patches.

Patch Announcements and Staying Current	Monitor vendor announcements for patches and apply them promptly to avoid exploitation. Keep track of updates and apply patches as soon as available.	Follow vendor updates, track patch availability, and apply patches swiftly.
Testing Patches before Deployment	Test patches in a controlled environment to prevent issues like incompatibilities or system failures. Ensures smooth deployment without disrupting operations.	Verify patches in a test environment before full deployment.
Automating Patching Processes	Use automated systems to deploy patches, reducing human error and ensuring timely updates. Automation improves efficiency and minimizes disruptions.	Automate patch deployment, reduce human error, and minimize operational impact.

Challenges in Patch Management

As with most management practices, patch management has its challenges. One problem that may be observed is the integration of patches into large networks, with numerous patches that seem overwhelming for IT specialists [70]. Further, organizations find it challenging to manage the rate at which patches are released to organizations, particularly mainly when using products from different vendors. Another critical challenge is the co-ordination of the patch release and deployment, without affecting the business operations. This may be especially tricky for organizations with large systems that interconnect with each other [68]. Moreover, it is sometimes challenging to patch a legacy system. A number of organizations still need to start using old software, which is no longer supported by the vendors and thus can barely get patches [60]. In such cases, several compensating controls like network segmentation and intensive monitoring are required to manage the risks associated with unpatched systems.

Remedial Measures for the Difficulties Encountered

Organizations need to consider the following best practices in patch management to address these issues. One of those best practices relates to the patch management policy that defines roles, responsibilities, and processes in patch identification, testing, and application. This policy helps to sustain the patching activities and execute them based on organizational objectives [69]. Further, to ensure all systems are up-to-date with security patches, organizations should occasionally conduct patch audits. Another good practice is implementing Centralized Patch Management, where the systems can be easily monitored and patched from the control console. Centralization simplifies the execution of the patches, brings the least complication, and guarantees unified change throughout the firm [63].

Organizations should promote patching training to employees to increase their understanding of the consequences of not patching. Recurring training ensures that the employees understand how protective they are of their organization's IT business and helps them adhere to patching standards. Patch management plays a significant role in ensuring IT systems' security, functionality, and compliance. An organization's cyber threats can be significantly reduced by using the asset inventory, proper priority of the patches, vendor updates, testing, and automation of the patching process. Despite these challenges, practicing best-of-breed measures like policy and procedure, centralization, and training can minimize these challenges, thus resulting in secure systems.

Table 4: Remedial Measures for Patch Management Challenges

Measure	Description	Key Points
Patch Management Policy	Define roles, responsibilities, and processes for patch management to ensure systematic execution and adherence to organizational goals.	Establish clear policies for patch management.
Centralized Patch Management	Centralize patch management to simplify tracking and deployment across systems, ensuring consistency and efficiency.	Use centralized systems for better management and uniform application.
Employee Training	Educate employees on the importance of patching, the process, and potential impacts of vulnerabilities. Regular training helps maintain awareness and adherence to practices.	Implement ongoing training programs to reinforce the importance of patch management.

Employee Training and Awareness Programs

The Human Element in Cybersecurity: Employees as the Weakest Link

It is widely known that the human factor is one of the main points that can be an object of attack in cybersecurity. Employees, or human resources, perhaps more well-known and the most vital asset of any organization, are often the most vulnerable link in an organization's protection from cyber threats [71]. A critical reason human behavior has been assumed to be a significant source of security threats is unintentional activities or ignorance [72]. The main problem area in this aspect is the absence of adequate training coupled with inadequate knowledge enhancement on matters related to cybersecurity. Exploiters often exploit this area through social engineering and phishing techniques since the employees' awareness level is often low or they are not trapped due to a lapse in judgment. Therefore, training and awareness programs play a vital role in changing employees from being at risk of being unsafe to being shielded against cyber threats.

Table 5: Employee Training and Awareness Programs

Aspect	Description	Benefits
Human Element in Cybersecurity	Employees can be a weak link in cybersecurity due to lack of training or awareness. Addressing this through training helps mitigate risks associated with human errors.	Reduces vulnerability due to unintentional actions or ignorance.
Benefits of Security Training	Training helps in recognizing phishing and social engineering attacks, complying with regulations, reducing mistakes, and creating a security-conscious culture.	Improves detection of phishing, ensures compliance, reduces mistakes, and fosters security culture.
Importance of Continuous Training	Cyber threats evolve, requiring ongoing training and updates to keep employees informed about new threats and security practices.	Keeps employees up-to-date with current threats and best practices.
Engaging Employees	Regular updates and interactive workshops enhance understanding and reinforce security practices among employees.	Improves engagement and reinforces the importance of cybersecurity.

Benefits of Security Training

There is a lot that an organization can do to improve its security position, and security training is critical for this improvement. Training employees on the basics of cybersecurity would deal with many risks.

- **Recognizing Phishing and Social Engineering Attacks:** Phishing and social engineering threats have become complex and formidable threats to most organizations. According to several research, phishing attacks are responsible for about 90% of data breach incidents [73]. Specific training given to the staff can ensure that a person capable of distinguishing between an honest message and a phishing one is trained to avoid being victims of such scams, especially because some appear legitimate from fake sources. It was also suggested that training employees to read emails and links carefully and instructing them to report anything suspicious would significantly diminish the likelihood of a successful phishing attempt [74].
- **Compliance with Industry Standards and Regulations:** Security training also has another significant advantage for an organization. It helps maintain compliance with norms and policies, such as HIPAA. Violating such regulations attracts severe legal consequences in the form of penalties and fines, as well as financial losses in compensation and damage to the business's reputation [75]. Ongoing training guarantees that the employees are conversant with the regulations, its compliance standards, and how data collected is managed and protected, among others. Additionally, such training fosters a workforce more capable of obeying organizational rules, regulations, and external legal requirements.
- **Reducing Risks Associated with Employee Mistakes:** Regardless of the positive attitude and desire to perform their duties, the employees can act in a way that will compromise the organization. For instance, reusing or sharing passwords poses huge risks [76]. Although it may be impossible to ensure that all bad actors are kept out of the system, people can understand appropriate password usage through security training and create passwords fortified by multifactor authentication. Furthermore, the employee can be educated on safety while browsing and the consequences of using outdated operating systems and programs [77].
- **Creating a Security-Conscious Culture:** Cybersecurity is not about occasional training but rather about building a security-oriented culture in the organization.

Table 6: Benefits of Security Training

Benefit	Description	Key Points
Recognizing Phishing and Social Engineering Attacks	Training employees to identify and avoid phishing and social engineering attacks, which are responsible for a significant percentage of data breaches.	Helps employees distinguish legitimate messages from phishing attempts, reducing the likelihood of successful scams.
Compliance with Industry Standards and Regulations	Ensures that employees understand and comply with industry regulations (e.g., HIPAA), avoiding legal penalties and reputational damage.	Keeps employees informed about regulations, data management, and protection to maintain compliance.
Reducing Risks Associated with Employee Mistakes	Educates employees on best practices for password usage, safe browsing, and the risks of outdated software, mitigating potential security breaches caused by human error.	Promotes strong password practices, safe browsing habits, and awareness of software updates.
Creating a Security-Conscious Culture	Fosters an organizational culture where cybersecurity is a priority, not just through periodic training but as an integral part of the company's ethos.	Builds an ongoing, security-focused culture throughout the organization.

Importance of Continuous Training to Adapt to Evolving Threats Cyber threats continue to change frequently, and it is rare to hold a single training session so that employees can be updated on current threats and the measures that need to be taken to counter them van der Kleij et al. It has been established that their nature and threats change over time, thus requiring professional development to provide continuous updates about such threats [78,79]. Continual information on new malware threats, phishing, and other vulnerabilities makes employees knowledgeable about such related threats. It is advised that organizations MUST incorporate several learning methods like e-learning, Workshops, and Simulation to enhance the learning experience and avoid boredom.

Engaging Employees with Regular Security Updates and Workshops

Security can be enhanced by hosting Compulsory Employee Meetings or Workshops on Security and safety concerns within the organization. Employees can prevent such risks when they learn the importance of shielding crucial information and physical infrastructure [80]. Real life, especially when incorporated in an interactive manner, such as presentational or role-play workshops, can be convenient when reinforcing specific lessons. Furthermore, leadership makes periodic announcements to reinforce cybersecurity's significance, increasing awareness of this issue throughout the company [81]. Continuing education and employee training sessions are crucial to reducing human factors threats in an organization's cybersecurity system. In that regard, organizations can enhance their security standing by enhancing the recognition of phishing schemes among their personnel, compliance with the existing standards, and reducing the incidence of errors. Furthermore, providing security consciousness with constant training and engagement is necessary to focus security issues on the organization's agenda at all levels. This proactive approach is essential in a world that is rapidly changing its threats Wong et al [82].

Leveraging Advanced Threat Detection Technologies

The current and evolving nature of the threats requires new and enhanced methods for the security and protection of cyberspace Pandey et al [83]. Of these, the AI-based approach is one of the approaches organizations can use to improve the detection of security threats and risks. Due to the potential of analyzing large volumes of data and providing detection and identification of numerous malicious activities, AI has emerged as a strategic element in cybersecurity. This section looks at some of the uses of AI in threat detection, how it works with existing systems, and some of the issues that arise from this integration.

Figure 10: AI in Cybersecurity: Defending Against Evolving Threats

Using Artificial Intelligence (AI) for Threat Detection

Machine learning is different from traditional computer programs and has improved the detection of cyber threats, mainly through deep learning techniques. Some traditional security measuring tools cannot effectively handle the amount, speed, and type of contemporary cyber threats. AI-based systems are superior to other systems when dealing with an enormous amount of information, recognizing tendencies, and drawing conclusions that are impossible for a human being. In the writings of Berman et al, it is evident that AI provides the means for the automation of tasks such as the detection of threats, allowing the improvement of the efficiency of security operation centers (SOCs) [84]. By drawing on past attack attacks and behavior identification of new trends, AI patterns can quickly identify novel attacks and reduce their impact before they wreak havoc.

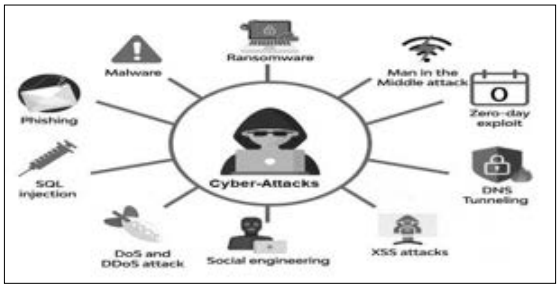

Figure 11: Several common attacks or threats in the context of cybersecurity

Applications of AI in Cybersecurity

AI is utilized in various cybersecurity fields to identify various types of cyber threats. The key applications include phishing detection, anomaly detection, malware detection, and predictive threat intelligence.

Phishing Detection: Phishing continues to be one of the most pronounced types of cyberattacks because it leverages human weaknesses. Such applications of AI can help detect phishing by checking the content of the email, the sender's behavior, and the links in the email. As reported by Khonji et al, it is notable that AI algorithms can summarize and match key attributes of phishing emails and phishing Websites, including domain reputation and abnormal behavior, for detecting phishing emails and Websites with a high degree of accuracy [85]. This automated detection dramatically helps to prevent users from being prey to that kind of attack.

Anomaly Detection: AI performs remarkably well in anomaly detection, a form of threat detection that aims at identifying activities within the network traffic or users' activities that are out of the ordinary. These rule-based solutions can result in many false positives, which burdens security teams. While AI systems use similar definitions, they also distinguish machine learning algorithms for processing big data and setting up norms for typical interaction. AI involves constant surveillance of the network activity to discover that it is out of the ordinary, which may indicate an attack [86]. This capability enables the security management teams to counter threats faster and more efficiently, reducing impacts.

Malware Detection: AI's participation in detecting malware has become more prominent since there are numerous and complicated forms of malware. Traditional methods of identifying the signature slow down with the emerging new variant in the malware. In particular, AI-based systems involve machine learning algorithms that help identify malware by understanding how it works, analyzing the behavioral patterns of benign and malicious codes, and comparing the new unknown malware samples to known ones [87]. AI can also identify zero-day attacks and other malware strains that are hard for conventional techniques to identify.

Predictive Threat Intelligence

It is also instrumental in predictive threat intelligence, which analyzes threat data to identify future attacks. Exploring the possibility of Implementing advanced analytics, cybersecurity systems can then identify new trends characteristic of cyber threats. According to Sommer and Paxson, predictive models allow organization protection to occur before an attacker's strike, offering the organization protection rather than mere detection [88]. The threat intelligence platforms founded on AI similarly evolve and optimize their models and predictions regularly.

Integrating AI into Existing Security Systems

The augmentation of some of these security systems using artificial intelligence most often boosts the security systems' capacity to identify threats and provide accurate time response. As a rule, AI systems can complement SIEM solutions, IDS, and firewalls that improve current solutions for cyber defense. In this case, Buczak and Guven noted that the integration of artificial intelligence posed an enhanced approach to security that includes using conventional security tools to make a multi-layered approach to designing and using a more effective solution proposed in AI solution [89]. Furthermore, it can reduce the workload of mundane tasks like log analysis and threat traffic milking so that analysts can address higher-priority threats. However, incorporating AI into security systems presents some challenges, as this article will illustrate. Managers also need to justify that the solutions offered by AI will be capable of integrating with other tools and procedures used at the organization. This entails prior planning for the models because AI systems require a lot of data to run and may need small adjustments every now and then to adapt to changing risks.

Figure 12: The Role of Artificial Intelligence in Strengthening IT Infrastructure and Security for Federal Agencies

Challenges of AI Implementation: Privacy Concerns and Adapting to New Threats

Even though AI has been found very useful in threat detection, implementing the technology sometimes comes with several challenges Arif et al [90]. There are two significant challenges of AI in cybersecurity: privacy. This is a massive problem for AI systems because collecting and analyzing large quantities of data needed for these systems may violate users' privacy if the information is personal. As Shokri et al, pointed out, these issues can be addressed by implementing privacy-preserving approaches for machine learning that will allow an AI system to learn from the provided data without direct access to it [91]. However, the effectiveness of the identities' threats and security measures remains rather sensitive and will need adjustment. Another issue that might cause potential problems is the ability of AI systems to learn new threats that are yet to be identified. Machine learning algorithms can quickly learn and make connections based on the available data, but the adversaries are constantly improving their approach to remain undetected. That is why the network's AI systems must be updated occasionally to counter new attacks. Barreno et al, explained that an adversarial attack on an AI system involves the attacker modifying input data to make the AI system compromise its decision-making process [92]. Since cyber threats are becoming increasingly complex, the Artificial Intelligence algorithms that work with threat detection must also be complex.

The effectiveness of AI has been observed as the defense mechanism against cyber threats in terms of threat identification and mitigation. Its applications, ranging from the detection of phishing incidents to the ability to predict attacks, serve as an arsenal for organizations as they seek to combat escalating levels of attacks. However, issues like the question of privacy and the question of flexibility make it difficult for AI to be incorporated into the existing security systems. With the ever-increasing threats in cyberspace, the utilization of artificial intelligence in handling cyber threats will also continue to increase [93,94].

Table 7: Challenges of AI Implementation in Cybersecurity

Challenge	Description	Key Points
Privacy Concerns	AI systems require large quantities of data, which may include personal information, raising privacy issues.	Privacy-preserving machine learning approaches can mitigate risks by allowing AI to learn without direct data access.
Adapting to New Threats	AI systems must be frequently updated to address new and evolving cyber threats.	Adversarial attacks can manipulate AI decision-making, necessitating complex and adaptive algorithms.
Complexity of AI Algorithms	The need for sophisticated AI algorithms to keep up with increasingly complex cyber threats.	AI algorithms must be continually refined to remain effective against sophisticated and evolving attacks.

Conclusion

Managing risks and protecting large networks from intrinsic weaknesses can only be accomplished through the proactive use of positive measures, continual evaluations, and the purposeful integration of new technologies. Strategies such as vulnerability management, network segmentation, penetration testing, and access control provide proper mapping and understanding of risks within the network before they progress to higher-level threats. Vulnerability assessments and Penetration testing should be done often in an organization because they offer insight into the effectiveness of an organization's security measures and measures taken to address organizational vulnerabilities. Network segmentation, however, is an efficient approach to controlling the spread of malware and controlling access, which enhances the security of the entire security structure. The many threats in the cyber-space make proactive an essential strategy for network security. It entails constant surveillance, identifying risks before adversaries can take advantage of them, and isolating these threats as early as possible. Security risk tools and mechanisms significantly improve an organization's capability to address risk events when supported by human supervision. Other measures such as RBAC and MFA also supplement access control measures to ensure only the permitted personnel access specific systems and information. Moving to the future, the adoption of complex technologies like artificial intelligence and machine learning in formulating a cybersecurity mechanism will likely assume profound importance. These technologies supply predictive threat intelligence and defense mechanisms capable of changing to respond to continually emergent cyber threats. Consequently, as threats evolve and become more complex, organizations need to adopt continuous improvement, remain alert, and embrace the ever-changing nature of the threat, thus protecting large-scale networks from current and future threats.

References

1. El-Kady AH, Halim S, El-Halwagi MM, Khan F (2023) Analysis of safety and security challenges and opportunities related to cyber-physical systems. Process Safety and Environmental Protection 173: 384-413.
2. Arogundade OR (2023) Network security concepts, dangers, and defense best practical. Computer Engineering and Intelligent Systems 14.
3. Mallaboyev NM, Sharifjanovna QM, Muxammadjon Q, Shukurullo C (2022) Information security issues. In Conference Zone 241-245.
4. Nikumaa T (2022) Vulnerability Management Process https://www.theseus.fi/bitstream/handle/10024/750130/Nikumaa_Tiina.pdf;jsessionid=2E4C05CA79045666F45260EE48E50E75?sequence=2.
5. Poslajko K, Mroczek M, Wójcik R (2020) Frameworks for improving vulnerability management in large-scale network environments. Cybersecurity Journal 12: 131-149.
6. Humayun M, Jhanjhi N, Almufareh MF, Khalil MI (2022) Security threat and vulnerability assessment and measurement in secure software development. Comput. Mater. Contin 71: 5039-5059.
7. Almohri HM (2019) Security challenges in segmented networks. IEEE Security & Privacy 17: 64-71.
8. Summers A (2019) Implementing network segmentation to mitigate cybersecurity risks. Computer Security Journal 38: 45-58.
9. Gupta A, Quamar A (2021) Best practices for enterprise-level vulnerability management. Computers & Security 99: 102051.
10. Alfandi O (2021) Network segmentation for enhanced security in corporate environments. Journal of Cybersecurity 14: 22-35.
11. Pavithra M (2020) Segmentation and isolation techniques in securing critical infrastructures. Journal of Network and Computer Applications 45: 52-67.
12. Rameder H, Di Angelo M, Salzer G (2022) Review of automated vulnerability analysis of smart contracts on Ethereum. Frontiers in Blockchain 5: 814977.
13. Almohri H, Oliveira D, Hamlen K (2019) Assessing the role of automated tools in vulnerability management. Journal of Cybersecurity Practices 6: 48-62.
14. Poslajko P (2020) Proactive strategies for network segmentation. Information Security Journal: A Global Perspective 29: 9-23.
15. Pavithra P, Kumar S, Natarajan R (2020) Overcoming challenges in vulnerability management for small and medium enterprises. Information Security Journal: A Global Perspective 29: 223-234.
16. Alfandi O, Almomani I, Gupta P (2021) Vulnerability management and mitigation techniques for cloud-based applications." International Journal of Information Security 10: 87-96.
17. Khan RA, Khan SU, Khan HU, Ilyas M (2022) Systematic literature review on security risks and its practices in secure software development. ieee Access 10: 5456-5481.
18. Alabbad M, Khedri R (2022) Dynamic Segmentation, Configuration, and Governance of SDN. J. Ubiquitous Syst. Pervasive Networks 16: 7-22.
19. Zhu B, Jajodia S (2016) Network Security Techniques for Critical Infrastructure Protection. Springer Publishing.
20. Farooq M, Khan R, Khan MH (2023) Stout Implementation of Firewall and Network Segmentation for Securing IoT Devices. Indian Journal of Science and Technology 16: 2609-2621.
21. Cheng W, Liang J, Liu J (2017) SMS-based two-factor authentication schemes and phishing attacks. International Journal of Security and Networks 12: 148-159.
22. Scarfone K, Mell P (2017) Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology https://csrc.nist.gov/pubs/sp/800/94/final.
23. Tariq M, Butt AH, Khalid M (2018) Network Segmentation Techniques for Enhancing Cybersecurity. Journal of Computer and Network Communications 10: 78-90.
24. Knapp ED (2024) Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Elsevier.
25. Barik S, Bhardwaj A, Ghosh A (2020) A Review on Wi-Fi Network Security and Its Segmentation Techniques. International Journal of Network Security & Its Applications 12: 23-36.
26. Xu L, Zhang Y, Luo W (2016) Demilitarized Zone Network Security Architecture for Modern Enterprises. Journal of Information Security 8: 52-61.
27. Gonzalez-Granadillo G, Astorga-Paliza F, Nespoli P (2018) Threat Detection and Mitigation in DMZ Networks Using Adaptive Segmentation. Journal of Computer Networks and Communications 9: 56-63.
28. Bocetta S, De Vincenti A, Morreale P (2021) Securing Development and Testing Networks through Segmentation. Journal of Information Security and Applications 65: 102475.
29. Huang HY, Fanjiang YY, Hung CH, Lee CA (2022) Design and Implementation of a Smart Intercom System through Web Services on Web of Things. In Telecom 3: 675-691.
30. Eshetu AY, Mohammed EA, Salau AO (2024) Cybersecurity vulnerabilities and solutions in Ethiopian university websites. Journal of Big Data 11: 118.
31. Scarfone K, Grance T, Masone J (2008) Guide to Enterprise Telework and Remote Access Security. NIST https://csrc.nist.rip/library/alt-SP800-46r1.pdf.
32. Stanger J (2016) CompTIA Security+ Study Guide. Sybex https://www.netwrix.com/comptia_security_plus_study_guide.html.
33. Saleem S, Ahmad H (2017) Cybersecurity Frameworks and Network Vulnerability Assessments. Journal of Computer Networks and Communications.
34. Kunz A, Ottersbach G, Mohmeyer P (2015) Practical Penetration Testing. Springer.
35. Lachkov P, Tawalbeh LA, Bhatt S (2022) Vulnerability assessment for applications security through penetration simulation and testing. Journal of Web Engineering 21: 2187-2208.
36. Skoudis E, Liston T (2006) Counter Hack Reloaded. Pearson https://www.counterhack.net/Counter_Hack/Welcome.html.
37. Scarfone K, Souppaya M, Cody A (2008) Guide to Enterprise Patch Management Technologies. NIST Special Publication https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-40r3.pdf.
38. Fischer S (2020) Penetration Testing Essentials. Wiley.
39. Ravindran U, Potukuchi RV (2022) A Review on Web Application Vulnerability Assessment and Penetration Testing. Review of Computer Engineering Studies 9.
40. Whitaker S, Newman C (2006) Penetration Testing and Network Defense. Cisco Press https://www.ciscopress.com/store/penetration-testing-and-network-defense-9781587052088.
41. Taherdoost H (2023) E-Business Security and Control. In E-business essentials: Building a successful online enterprise. Cham: Springer Nature Switzerland 105-135.
42. Zissis D, Lekkas D (2012) Addressing cloud computing

security issues. Future Generation Computer Systems 28: 583-592.

43. Muddychetty NS (2024) A Comparative Analysis of SecurityServices Using Identity and AccessManagement (IAM) http://search.ndltd.org/show.php?id=oai%3Aunion.ndltd.org%3AUPSALLA1%2Foai%3ADiVA.org%3Abth-26014&back=http%3A%2F%2Fsearch.ndltd.org%2Fsearch.php%3Fq%3Dsubject%253A%2522multi%2Bfactor%2Bauthentication%2522.
44. Aloul F (2010) Two factor authentication using mobile phones. 2010 IEEE/ACS International Conference on Computer Systems and Applications https://doi.org/10.1109/AICCSA.2010.5587030.
45. Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chandramouli R (2001) Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security 4: 224-274.
46. Hu VC, Ferraiolo DF, Kuhn DR (2006) Assessment of access control systems. NIST Special Publication 800: 1-118.
47. Saltzer JH, Schroeder MD (1975) The protection of information in computer systems. Proceedings of the IEEE 63: 1278-1308.
48. Rose S, Borchert O, Mitchell S, Connelly S (2020) Zero Trust Architecture. National Institute of Standards and Technology (NIST) Special Publication 800-207.
49. Kindervag J (2010) No More Chewy Centers: Introducing the Zero Trust Model of Information Security. Forrester Research.
50. Garcia M (2019) Implementing Zero Trust Security in Cloud and On-Premise Environments. Cybersecurity Journal 8: 215-230.
51. Sahib A (2019) The Role of Least Privilege in Cybersecurity: A Zero Trust Approach. Journal of Information Security 6: 312-326.
52. Sarkar S, Choudhary G, Shandilya SK, Hussain A, Kim H (2022) Security of zero trust networks in cloud computing: A comparative review. Sustainability 14: 11213.
53. Sawyer R (2018) Adaptive Security and Zero Trust: Dynamic Defenses in Modern Cybersecurity. InfoSec Quarterly 12: 149-161.
54. Onwubiko C (2022) CyberOps: Situational Awareness in Cybersecurity Operations. arXiv preprint arXiv: 2202.03687.
55. Cichonski P, Millar T, Grance T, Scarfone K (2012) Computer Security Incident Handling Guide. NIST.
56. Souppaya M, Scarfone K (2013) Guide to Malware Incident Prevention and Handling for Desktops and Laptops. NIST https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-83r1.pdf.
57. Feng Q, Purohit H, Dong X, Han Q (2019) Automated log analysis for network intrusion detection. Journal of Network and Computer Applications 136: 89-98.
58. Jouini M, Rabai LBA, Aissa AB (2014) Classification of security threats in information systems. Procedia Computer Science 32: 489-496.
59. Ou CX, Zhang X, Angelopoulos S, Davison RM, Janse N (2022) Security breaches and organization response strategy: Exploring consumers' threat and coping appraisals. International Journal of Information Management 65: 102498.
60. Scarfone K, Mell P (2007) Guide to Intrusion Detection and Prevention Systems (IDPS). NIST https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf.
61. Killcrece G, Kossakowski KP, Ruefle R, Zajicek M (2003) Organizational Models for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon University.
62. Korir FC (2023) Software security models and frameworks: an overview and current trends.
63. Alberts CJ, Dorofee A (2013) Managing Information Security Risks: The OCTAVE Approach. Addison-Wesley.
64. Kaspersky Labs (2019) IT Threat Evolution Q2 2019. Kaspersky Labs Report.
65. Sadri M (2024) HIPAA: A Demand to Modernize Health Legislation. The Undergraduate Law Review at UC San Diego 2.
66. Gartner (2020) Best Practices for Vulnerability and Patch Management. Gartner Research.
67. Mell P, Kent K (2007) A Framework for the Development and Publication of Security Patches. NIST Special Publication 800-840.
68. McGraw G (2006) Software Security: Building Security In. Addison-Wesley https://www.abebooks.com/book-search/isbn/0321356705/.
69. Kerravala Z (2020) Automated Patch Management: Efficiency in Security. ZK Research.
70. Lefdal JB, Reisæter DW (2022) Security patch management-an overview of the patching process and its challenges in norwegian businesses.
71. Hadlington L (2017) Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky online behaviors. Heliyon 3: e00346.
72. Torten R, Reaiche C, Boyle S (2018) The impact of Information Security Awareness Training on employee compliance: A pilot study. Journal of Information Systems 32: 123-141.
73. Abawajy J (2014) User preference of cybersecurity awareness delivery methods. Behaviour & Information Technology 33: 236-247.
74. Bauer S, Bernroider EW, Chudzikowski K (2017) Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Computers & Security 68: 145-159.
75. Davis R, Peppet S (2017) Regulating Privacy: Data Protection and the Law. Fordham Law Review 86: 121-145.
76. Alotaibi F, Furnell S, Stengel I (2016) A Survey of Password Use and Management. Journal of Information Security and Applications 27: 22-31.
77. Sommestad T, Hallberg J, Lundholm K, Bengtsson J (2014) Variables influencing information security policy compliance: A systematic review of quantitative studies. Information Management & Computer Security 22: 21-38.
78. van der Kleij R, Schraagen JM, Cadet B, Young H (2022) Developing decision support for cybersecurity threat and incident managers. Computers & Security 113: 102535.
79. Bada M, Sasse MA, Nurse JRC (2019) Cyber security awareness campaigns: Why do they fail to change behavior? Computers & Security 79: 133-145.
80. Tikk E, Kaska K, Vihul L (2017) International Cybersecurity Law. Cambridge University Press.
81. McIlwraith A (2016) Information Security and Employee Behaviour: How to Reduce Risk through Employee Education, Training and Awareness. Routledge https://www.researchgate.net/publication/352868892_Information_Security_and_Employee_Behaviour_How_to_Reduce_Risk_Through_Employee_Education_Training_and_Awareness.
82. Wong LW, Lee VH, Tan GWH, Ooi KB, Sohal A (2022) The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. International Journal of Information Management 66: 102520.
83. Pandey AB, Tripathi A, Vashist PC (2022) A survey of cyber

security trends, emerging technologies and threats. Cyber Security in Intelligent Computing and Communications 19-33.

84. Berman DS, Buczak AL, Chavis JS, Corbett JT (2019) A survey of deep learning methods for cyber security. Information 10: 122.
85. Khonji M, Iraqi Y, Jones A (2013) Phishing detection: A literature survey. IEEE Communications Surveys & Tutorials 15: 2091-2121.
86. Kim Y, Kim H, Lee E (2018) Deep learning-based anomaly detection in real-time for cybersecurity. IEEE Access 6: 51691-51706.
87. Sharma S, Sabitha AS, Rao A (2020) Machine learning-based approaches for malware detection: A survey. Journal of Information Security and Applications 54: 102531.
88. Sommer R, Paxson V (2010) Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy 305-316.
89. Buczak AL, Guven E (2016) A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials 18: 1153-1176.
90. Arif H, Kumar A, Fahad M, Hussain HK (2024) Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research. International Journal of Multidisciplinary Sciences and Arts 3: 242-251.
91. Shokri R, Stronati M, Song C, Shmatikov V (2017) Membership inference attacks against machine learning models. Proceedings of the 2017 IEEE Symposium on Security and Privacy 3-18.
92. Barreno M, Nelson B, Joseph AD, Tygar JD (2010) The security of machine learning. Machine Learning 81: 121-148.
93. Cheng W, Zhang Y, Xiao S (2017) Advanced Network Segmentation for Improved Cybersecurity in Industrial Control Systems. International Journal of Critical Infrastructure Protection 17: 23-35.
94. Summers A, Brown M, White J (2019) Vulnerability assessments in evolving network architectures. Security Engineering Journal 8: 297-312.