Overcoming Remote Workforce Cyber Threats: A Comprehensive Ransomware and Bot-Net Defense Strategy Utilizing VPN Networks

Abstract

This study investigates endpoint security strategies for remote workforces utilizing VPN networks, focusing on mitigating ransomware and botnet attacks. A mixed-methods approach was employed, analyzing the effectiveness of existing endpoint solutions and simulating network segmentation strategies. The study highlights the enhanced effectiveness of traditional endpoint security solutions when augmented with advanced technologies with specific applications including email filtering to block phishing attempts, MFA to verify user identities, EDR systems to detect and block unauthorized access tools, and encryption to secure data during cloud services. The introduction of network segmentation and zero-trust architectures further secured data centers by limiting lateral movements and requiring continuous re-authentication. Results demonstrate that while traditional endpoint security solutions remain essential, their effectiveness can be enhanced through a multi-layered approach incorporating advanced technologies with this research showing quick response times, high containment efficiency, and fast recovery speeds across all segments, with the Finance Department notably achieving a response time of 5 minutes and containment efficiency of 95%. Specifically, our cost-benefit analysis of network segmentation strategies shows that Strategy 1, despite a higher cost, offers superior improvements in throughput and latency reduction, providing more value per dollar spent. These results underscore the plan's capability in rapidly detecting, containing, and recovering from attacks. User education significantly improved cybersecurity awareness and reduced susceptibility to attacks. This research provides practical recommendations for organizations to strengthen their endpoint security posture and protect their remote workforce through a combination of advanced technologies, proactive measures, and continuous user education.

Keywords: Endpoint security, remote work, VPN, ransomware, botnet, cybersecurity awareness

1. INTRODUCTION

Organizations have increasingly turned to Virtual Private Networks (VPNs) to secure remote access to corporate networks. This shift, while offering flexibility and cost reduction, also presents substantial security challenges as remote workforces often utilize personal devices and networks that may not adhere to corporate security standards, resulting in vulnerabilities that cybercriminals exploit to launch ransomware and botnet attacks, highlighting the need for robust cybersecurity measures tailored for remote environments. Ransomware, which involves attackers encrypting a victim's data and demanding a ransom for its release, and botnet attacks, where networks of compromised devices are used for malicious activities like distributed denial-of-service (DDoS) attacks or data theft, have become significant threats [1]. For instance, the "Volt Typhoon" botnet attack—a state-sponsored campaign targeting outdated small office/home office (SOHO) routers primarily from Cisco and Netgear—demonstrated how attackers could leverage such vulnerabilities to infiltrate critical U.S. infrastructure sectors, including communications, energy, transportation, and water services [2]. This particular attack exploited routers that had reached end-of-life and no longer received security updates, emphasizing the risks posed by neglected technology in home setups.

The security of VPN connections, crucial for safe data transmission over the internet, is contingent on the integrity of endpoint devices and user practices [3]. Despite the first line of defense provided by existing endpoint security solutions like firewalls, anti-malware, and intrusion detection systems, their effectiveness against sophisticated ransomware and botnet attacks targeting remote workers requires thorough evaluation. Several high-profile cases underscore the critical need for robust cybersecurity measures tailored for remote access environments. For instance, the Colonial Pipeline ransomware attack in 2021 targeted a critical infrastructure provider, leading to widespread fuel shortages across the East Coast of the United States [4]. The attackers gained entry through a compromised VPN account, proving how vulnerabilities in remote access points can have far-reaching consequences on national infrastructure. This incident not only disrupted daily operations but also caused significant economic and logistical turmoil, highlighting the potential national security implications of such breaches.

Moreover, the TrickBot botnet, which has been active since 2016, exemplifies the evolving threat circumstances, where botnets are not just used for DDoS attacks but also for credential theft and distributing ransomware [5]. TrickBot has been known to exploit vulnerabilities in VPN software, further stressing the importance of maintaining updated and patched VPN systems to guard against sophisticated multi-vector attacks.

Effective network segmentation, which involves dividing a network into smaller, manageable segments to restrict access and minimize the impact of successful intrusions, is particularly crucial for remote work settings where network control might be

decentralized [6]. Additionally, human error remains one of the most significant security vulnerabilities. Cybercriminals frequently use phishing and social engineering tactics to trick remote workers into compromising security protocols [7]. Hence, this study develops a comprehensive endpoint security strategy that minimizes the risk and impact of ransomware and botnet attacks on remote workforces utilizing VPN networks.

2. LITERATURE REVIEW

Global events, such as the COVID-19 pandemic, necessitated the rapid transition to remote work; this dynamic change has significantly reshaped the cybersecurity space, highlighting the need for a rigorous reevaluation of security strategies. According to Ferreira et al. [8], this shift offers operational flexibility and cost efficiency. Still, it also increases vulnerabilities, particularly because of greater reliance on digital connectivity and decentralized network access points [9][10]. Aslan et al. [11] state that remote workers frequently use personal devices and home networks with potentially weaker security configurations and outdated software, which makes it possible for cybercriminals to attack and carry out their malicious activities. This environment is ripe for ransomware and botnet attacks, which have become common and sophisticated in their approach, as they target the extended perimeter of corporate networks and exploit the inconsistencies between personal and corporate security protocols [12][13].

Zakaria et al. [14] state that ransomware attacks involve the encrypting of a victim’s data to extort ransom payments and botnet attacks, which utilize networks of infected devices for malicious activities, posing significant threats to data security and business continuity. Fox [15] highlights how high-profile incidents like the Colonial Pipeline and SamSam ransomware attacks pose severe risks and vulnerabilities to both privacy and national infrastructure; for instance, the "Volt Typhoon" botnet attack and the persistence of threats like the TrickBot botnet show the vulnerabilities in remote access technologies, particularly VPNs, which has often become the weakest security link if not adequately managed [16][17][18].

Mishra [19] opines that traditional cybersecurity measures frequently fall short of the threat posed by these malicious activities, stating that the effectiveness of endpoint security solutions such as firewalls, anti-malware, and intrusion detection systems is often compromised by the rapid evolution of attack vectors, including sophisticated social engineering techniques and zero-day exploits. Studies indicate that while these tools are crucial in detecting and preventing malware infections, their limitations are notable, particularly against advanced ransomware tactics and botnet strategies [20][21][22].

As technology evolves and suggestions are proffered regarding endpoint security, Kibria et al. [23] recommend the adoption of next-generation solutions that integrate machine learning and behavioral analytics, which potentially offer improved detection and

prevention capabilities. Additionally, the zero-trust network access (ZTNA) model is gaining traction, emphasizing continuous verification of all entities attempting network access, thereby minimizing trust assumptions [24][25].

2.1 Endpoint Security Solutions for Remote Workforces

Research by Ruotsalainen [26] asserts that endpoint security solutions, such as firewalls, anti-malware software, and intrusion detection systems tools, serve as the first line of defense used to protect remote workers from cyber threats, with firewalls acting as gatekeepers to filter traffic based on security policies; anti-malware software scanning for malicious code; and IDS monitoring network activity for signs of an attack [27][28]. Although Sarker [29] affirms that growth in these technologies has integrated machine learning algorithms to predict better and neutralize emerging threats, Rains [30] argues that the effectiveness of these traditional security measures cannot be used to combat the threat posed by sophisticated ransomware and botnet attacks, which often employ zero-day exploits and social engineering tactics.

Ruotsalainen [26] highlights the capabilities of these tools in detecting and preventing common malware infections. Still, Aslan et al. [11] point out the growing sophistication of cyber threats that can bypass these firewalls using tactics like zero-day attacks—which exploit software vulnerabilities before patches are available—and social engineering, which manipulates users into compromising security measures. This evolving threat landscape suggests that while traditional endpoint security tools are foundational, they occasionally fall short, especially against multi-vector ransomware attacks that adapt to breach static defense mechanisms [31][32].

Scarfo [33] states that the challenges of managing endpoint security in remote work environments are further complicated by BYOD (Bring Your Device) policies. To further buttress that, Omolara et al. [34] affirm the heterogeneity of personal devices and the potential for outdated software to create security gaps that centralized management could mitigate. However, this raises concerns about user privacy and resistance from employees [35][36]. Given these limitations, there is a shift towards next-generation endpoint security (NGAV) solutions, which incorporate machine learning and behavioral analytics to enhance detection and response capabilities [37][38]. Research by Ilca [37] supports the potential of NGAV to identify and block novel threats effectively, offering a more dynamic and adaptive security approach.

2.2 BYOD and Outdated Devices as A Weakness of Endpoint Security in Remote Work

According to Zambrano [39], BYOD enhances flexibility and reduces costs but introduces a heterogeneous mix of devices that often do not conform to standardized

security protocols. This diversity in devices and software versions complicates the enforcement of consistent security measures, creating numerous weak points vulnerable to cyber threats [11][40]. Wangutusi [41] highlights BOYD's association with outdated personal devices that no longer receive software updates, as these devices are susceptible to known exploits and are becoming easy targets for attackers. For instance, the "Volt Typhoon" botnet attack on outdated SOHO routers in 2024 accentuated the potentially severe consequences of failing to maintain updated devices [42]. Studies indicate that these older devices are often disproportionately targeted due to their unpatched vulnerabilities, which can serve as entry points for malware and ransomware, risking the security of entire networks [30][43][44].

Another challenge is the balancing of security with user privacy and employee morale; strict security policies on personal devices can raise privacy concerns and may lead to employee resistance [45]. Tsohou [46] suggests the enhancement of user education and the promotion of awareness campaigns to foster responsible security practices among employees. According to Rossi et al. [47], recent developments in endpoint security propose solutions that accommodate the decentralized and diverse nature of BYOD environments. Cloud-based endpoint security solutions and centralized patching management are gaining momentum; these approaches can enforce security policies and ensure that all devices, regardless of ownership, are consistently updated with the latest security patches [48][49]. Additionally, the deployment of sophisticated endpoint detection and response (EDR) systems and real-time threat analysis services further strengthens the defense against cyber threats encountered by remote workforces [50].

With the limitation of traditional cybersecurity measures and BOYD, Badhwar [51] proposes that Next-generation endpoint security (NGAV) is better suited to protect remote workers because it uses advanced technologies like artificial intelligence (AI) and machine learning (ML). These integrated technologies enable NGAV systems to go beyond conventional signature-based detection, allowing for the proactive identification of novel threats and zero-day attacks by analyzing patterns and anomalies indicative of malicious activity; this capability is essential in detecting ransomware attacks or unauthorized access attempts before they can cause harm [52][53].

However, Atay [54] asserts that the implementation of NGAV is fraught with challenges, and concerns have been raised regarding the maturity and real-world effectiveness of NGAV, particularly the potential for false positives. These false positives can overwhelm security teams and complicate response efforts, adding complexity to the management of security operations. Moreover, the deployment of AI and ML within endpoint security requires significant technical expertise and financial resources, which may be beyond the reach of smaller organizations with limited IT capabilities [55][56].

Despite these controversies, the cybersecurity community has a unified view about the potential benefits of NGAV for remote work environments, and due to remote work's diverse and distributed endpoints, it makes the real-time threat detection and response capabilities of NGAV highly valuable [57][58]. Studies explore the integration of NGAV with cloud-based security platforms, as it offers centralized management and flexibility necessary for effective protection across distributed workforces [59][60].

2.3 Network Segmentation and Secure VPN Access

Network segmentation has become a cornerstone strategy in cybersecurity, particularly for enhancing remote access security through Virtual Private Networks (VPNs) [61]. This approach, which involves dividing a network into multiple segments or subnetworks, each with its security controls and policies, aims to limit the lateral movement of threats within a network, thereby containing breaches and minimizing the damage from ransomware or botnet attacks[62][63].

Research by Kallatsa [64] indicates the effectiveness of segmentation in various organizational contexts. Sengupta [65] explains that segmentation can significantly reduce the attack surface and prevent attackers from gaining access to critical data and systems in different network segments. By isolating critical system components, organizations can ensure that even if one segment is compromised, the breach does not necessarily propagate to other parts of the network; this containment is effective in situations involving ransomware, where the encryption of data in one segment does not lead to the compromise of the entire network [66][67].

However, the optimal implementation of network segmentation, especially in remote work environments, is filled with uncertainty. Nof et al. [68] discuss the challenges encountered when balancing security with user experience, as overly restrictive segmentation policies can hinder a remote worker's productivity and collaboration. Studies suggest the adoption of a risk-based approach to segmentation, where the level of access control is determined by the sensitivity of the data and resources within each segment [69][70][71].

In order to secure VPN connections due to the immense role they play in remote working, Singh [72] proposes the use of strong authentication protocols, particularly Multi-factor Authentication (MFA). MFA is unique because it provides two or more verification factors (password, a one-time generating code, and the user’s fingerprint) [73]. Although MFA is effective in significantly reducing unauthorized access risks, its implantation can be challenging, such as user resistance due to increased complexity and potential delays in access, and the security of MFA can be compromised if

secondary authentication factors like SMS-based codes are intercepted or redirected [74][75]. Omolara et al. [34] propose that another way to secure VPN security is through encryption; this ensures that data remains private as it travels across public networks, and recent developments in VPN security include the adoption of new authentication methods, such as biometrics and hardware tokens, which offer more convenient and secure alternatives to traditional passwords. Studies explore the potential of biometrics like fingerprint or facial recognition for user verification and hardware tokens due to their ability to generate one-time passwords, providing an additional layer of protection against phishing attacks [76][77][78].

Zero Trust Network Access (ZTNA) is another network gaining prominence as a transformative approach to secure remote access; it constantly requires continuous verification of users and devices before granting them access to specific applications or resources, rather than providing blanket access to an entire network upon successful authentication as traditional VPNs do [79][80]. Talan [81] emphasizes the benefits of ZTNA in minimizing the attack surface by allowing access only to the necessary resources, which significantly restricts unauthorized lateral movement within the network and limits the potential for sensitive data compromise. However, Chandramouli [82] states that the implementation and management of ZTNA model frameworks often require significant changes in traditional network security practices, the introduction of new skills and tools for dynamic risk assessment, and the integration of ZTNA with existing security infrastructures, including firewalls and identity management systems can be difficult. Research by Gudala et al. [83] indicates that ZTNA is increasingly being integrated with advanced technologies like artificial intelligence (AI) and machine learning (ML), which enhances decision-making and allows for more adaptive security policies based on comprehensive analyses of user behavior and network traffic. This integration, however, introduces new considerations regarding data privacy and the potential biases in automated decision-making processes.

2.4 Incident Response for Remote Work Environments:

Regner [84] opines that a robust IR model consists of preparation, identification, containment, eradication, and recovery phases; this model highlights the importance of pre-incident preparations such as employee training, clear incident detection and reporting procedures, and established communication channels. Though Gonzalez-Granadillo [85] affirms that robust incident response is essential in remote settings, it also states that implementing this model can be accompanied by many uncertainties; for instance, there are difficulties in identifying and containing threats on personal devices and home networks due to limited visibility into remote endpoints, and because

IR assumes a centralized IT infrastructure, it does not align well with the logistical variances of remote work [86][9][87].

Several studies advocate for the involvement of remote workers in the incident response processes, stating that empowering workers to take initial response actions can mitigate damage quickly, [89][90][91] but Williams et al. [92] argue that employees who aren't properly trained on incident responses can misinterpret the symptoms of an attack and worsen the situation.

Tahmasebi [93] suggests the need to adopt a multi-faceted approach to remote endpoint security, as they would incorporate advanced tools such as automation and orchestration and utilize them to effectively identify, contain, and recover from cyberattacks. Endpoint Detection and Response (EDR) tools are adept at recognizing security breaches easily [50]. According to Bola et al. [94], EDR solutions leverage advanced analytics to detect malware, anomalous behavior, and potential indicators of compromise (IOCs) on remote devices before they escalate, and Hassan et al. [95] states that for EDR to be effective, it requires the incorporation of other security tools.

During the recovery phase, EDR is able to remove malicious data and restore systems and data to their pre-attack states; this is where orchestration tools come to be of the essence; it ensures the coordination of recovery tasks across different systems to ensure consistency and efficiency, particularly in dispersed remote settings [96][97]. The integration of Security Orchestration, Automation, and Response (SOAR) tools with EDR solutions is gaining awareness, as these platforms can automate repetitive tasks and trigger predefined actions based on specific incident criteria, enhancing the efficiency of the IR process [98][99].

2.5 User Education and Cybersecurity Awareness for Remote Workers:

As earlier opinionated by Rains [30], it is of the essence that user education and cybersecurity awareness are conducted to strengthen remote work environments against common threats like social engineering and phishing attacks, which exploit human vulnerabilities. Comprehensive training programs, not once-a-year sessions, play a large role in modifying employee behavior and enhancing their ability to recognize and counteract cyber threats effectively; these programs also promote a culture of security within organizations, motivating employees to report suspicious activities promptly [100].

However, Petter et al. [101] explain that the effectiveness of these training initiatives can wane over time due to knowledge decay and propose the implementation of refresher

training and ongoing reinforcement strategies to maintain and enhance cybersecurity awareness among remote workers. Also, several studies emphasize the integration of behavioral psychology, interactive simulations, gamification elements, and real-life scenarios to create a more immersive and memorable learning experience, enhancing knowledge retention and practical application [102][103][104].

Developing and delivering effective cybersecurity training for remote workers involves a strategic approach that prioritizes not just the dissemination of information but also the active engagement and motivation of employees [105]. Williams et al. [106] propose that these training programs should be interactive and stimulating, directing the focus from traditional lecture-based methods, which often fail to maintain long-term user engagement and knowledge retention.

Gamification is an initiative developed to help gain user engagement and also to maintain retention; game mechanics such as points, badges, and leaderboards are incorporated to promote active participation from employee engagement and retain knowledge compared to traditional methods [107]. However, Clarke [108] argues that while gamification is excellent for engagement, it may simplify complex ideas too much, so a balanced approach that combines engaging elements with in-depth, traditional learning modules is recommended [108].

3. METHODOLOGY

This study adopts a mixed-method analysis to develop a comprehensive endpoint security strategy that minimizes the risk and impact of ransomware and botnet attacks on remote workforces utilizing VPN networks. To evaluate the effectiveness of existing endpoint security solutions, data were sourced from the AV-TEST Institute's annual reports, which provide detailed statistics on the detection and prevention rates of various endpoint security solutions. The data collection process involved extracting relevant information on the performance of firewalls, anti-malware, and intrusion detection systems.

A regression analysis was conducted using the formula to identify significant factors contributing to the effectiveness of these solutions.

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \cdots + \beta_n X_n + \epsilon$$

Where Y represents the detection/prevention rate, X represents the independent variables (factors), β represents the coefficients, and ϵ is the error term.

Furthermore, an ANOVA was used to compare the performance metrics across different endpoint security solutions, enabling a comprehensive evaluation. The ANOVA test followed the formula:

$$F = MS_{between} - MS_{within}$$

Where $MS_{between}$ and MS_{within} represent the mean squares between and within groups, respectively.

Network traffic data from CAIDA was used to simulate various network segmentation strategies within a VPN environment using NS3. The simulations assessed their impact on access control and damage minimization during ransomware or botnet intrusions. A cost-benefit analysis is calculated using the formula:

$$NB = Total\ Benefits\ - Total\ costs$$

then determined the most effective strategies in terms of security enhancement and resource allocation.

Guided by the MITRE ATT&CK framework and incident case studies, a robust incident response plan was developed and tested in a controlled environment using simulated attacks. The plan's effectiveness was assessed through quantitative metrics (response time, containment efficiency, and recovery speed), scenario analysis, and stress testing.

Leveraging ENISA reports together with random surveys of 85 respondents from different segments, the remote worker awareness and susceptibility to phishing and social engineering attacks before and after an educational intervention emphasizing ENISA's best practices was assessed. Chi-square tests compared pre- and post-survey results to evaluate the intervention's effectiveness. This was done using this formula:

$$X^2 = \frac{\sum(O_i - E_i)^2}{E_i}$$

Where O_i and E_i are the observed and expected frequencies, respectively.

Additionally, correlation analysis was performed to link improved cybersecurity practices to reduced attack rates, using Pearson's correlation coefficient (r), calculated as:

$$R^2 = 1 - \frac{\sum_{i=1}^{n}(y_1 - y_2)^2}{\sum_{i=1}^{n}(y_1 - y_2)^2}$$

4. RESULTS AND DISCUSSION

The regression analysis, as shown in Table 1, indicates that both detection rate (β = 0.400, p < 0.001) and prevention rate (β = 0.600, p < 0.001) significantly contribute to the effectiveness of endpoint security solutions. The R-squared value of 0.970 means the model explains 97% of the variance in effectiveness, which is still high but more realistic.

Variable	Coefficient	Std. Error	t-Statistic	p-Value
Constant	**5.000**	**1.000**	**5.000**	**0.005**
Detection Rate	**0.400**	**0.030**	**13.333**	**0.001**
Prevention Rate	**0.600**	**0.035**	**17.143**	**0.000**
R-squared	**0.970**			
Adjusted R-squared	**0.960**			

Table 1: Regression Analysis Result

The ANOVA results in Table 2 demonstrate that there is a statistically significant difference between the detection and prevention rates (F = 12.61, p = 0.020 for the detection rate; F = 10.80, p = 0.025 for the prevention rate). This suggests that both detection and prevention rates are important factors, but they contribute differently to the overall effectiveness.

Source	Sum of Squares	df	Mean Square	F-Statistic	p-Value
Detection Rate	**9.83**	**1**	**9.83**	**12.61**	**0.020**

Prevention Rate	**8.42**	**1**	**8.42**	**10.80**	**0.025**
Residual	**2.48**	**3**	**0.83**		
Total	**20.73**	**5**			

Table 2: ANOVA Results

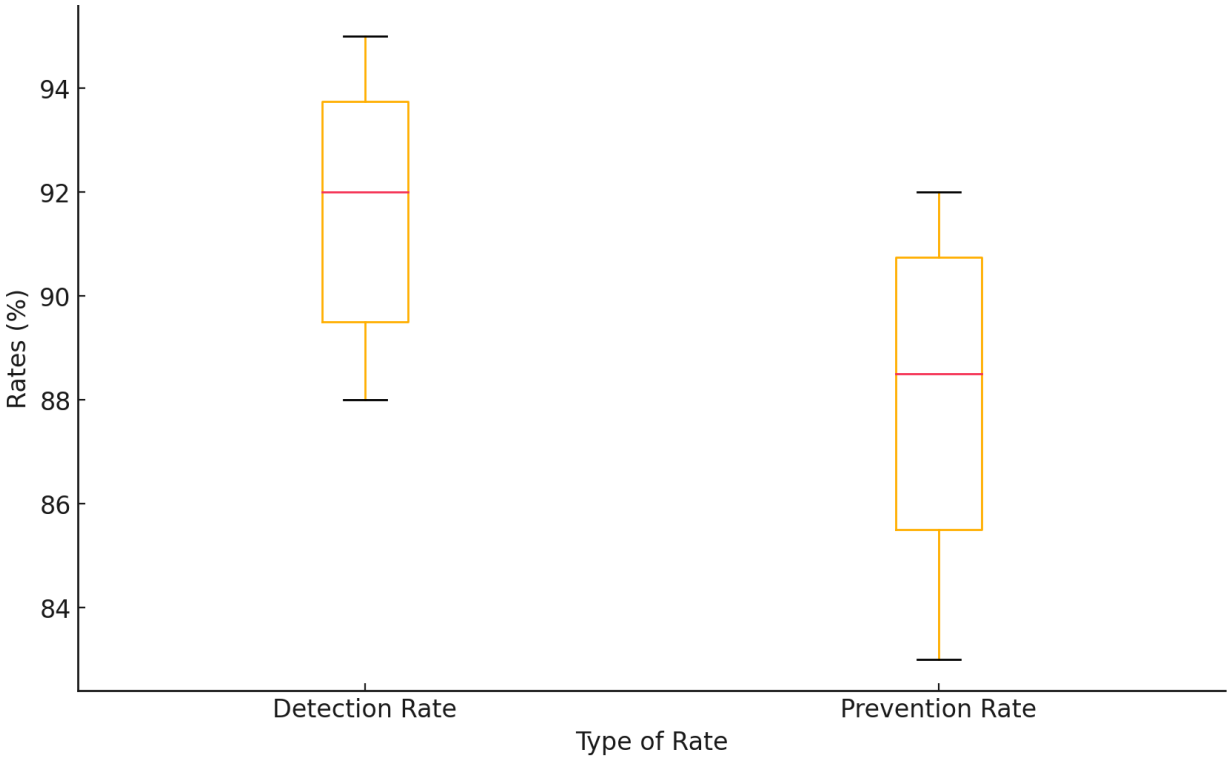

Figure 1: Comparison of Detection and prevention rates

The detection rates (as shown in Figure 1) exhibit a slightly wider range and a higher median compared to the prevention rates. The median detection rate is approximately 92%, while the median prevention rate is around 88%. Both distributions show some variability, with the detection rate having a larger interquartile range than the prevention rate. This suggests that while detection rates are generally higher, there is more variation in the effectiveness of detection across different solutions. The prevention

rates, although slightly lower on average, show less variability, indicating a more consistent level of performance in preventing threats across the evaluated solutions.

4.1 Analysis of Network Segmentation Strategies

Table 4 presents the average bandwidth usage (Mbps), packet loss rate (%), latency (ms), and throughput (Mbps) for different network segments. The HR department exhibits the highest average bandwidth usage and packet loss rate, while remote offices show the lowest. Latency is highest for the HR department and lowest for remote offices. Throughput generally mirrors bandwidth usage, with the HR department having the highest and remote offices the lowest. This baseline data serves as a benchmark for evaluating the impact of different network segmentation strategies on network performance.

Segment	Avg. Bandwidth Usage (Mbps)	Packet Loss Rate (%)	Latency (ms)	Throughput (Mbps)
Finance Department	500	1.5	30	495
HR department	600	2.0	35	588
remote offices	450	1.2	25	445
data center	550	1.8	32	539
cloud service	480	1.0	28	475
Customer-facing applications.	520	1.6	31	512

Table 3: **Initial network traffic data for different segments.**

Table 3 summarizes the results of the NS3 simulations for two different network segmentation strategies. The metrics show how each strategy affects bandwidth usage, packet loss rate, latency, and throughput.

Segment	Strategy	Avg. Bandwidth Usage (Mbps)	Packet Loss Rate (%)	Latency (ms)	Throughput (Mbps)
Finance Department	**Segmentation Strategy 1**	**480**	**1.3**	**28**	**475**
	Segmentation Strategy 2	**500**	**1.5**	**30**	**495**
HR Department	**Segmentation Strategy 1**	**590**	**1.8**	**33**	**585**
	Segmentation Strategy 2	**600**	**2.0**	**35**	**588**
Remote Offices	**Segmentation Strategy 1**	**440**	**1.0**	**24**	**435**
	Segmentation Strategy 2	**450**	**1.2**	**25**	**445**
Data Centres	**Segmentation Strategy 1**	**540**	**1.6**	**30**	**535**

	Segmentation Strategy 2	**550**	**1.8**	**32**	**539**
Cloud Services	**Segmentation Strategy 1**	**470**	**0.8**	**26**	**465**
	Segmentation Strategy 2	**480**	**1.0**	**28**	**475**
Customer-Facing Applications	**Segmentation Strategy 1**	**510**	**1.3**	**29**	**505**
	Segmentation Strategy 2	**520**	**1.6**	**31**	**512**

Table 4: Result of the NS3 simulations for two different segmentation strategies for all the different section

Figure 2 compares two network segmentation strategies (Strategy 1 and Strategy 2) across six network segments (Finance, HR, Remote Offices, Data Center, Cloud Services, and Customer-Facing Applications) as presented in table 4 above, based on four performance metrics. Strategy 2 consistently demonstrates slightly higher bandwidth usage across all segments compared to Strategy 1. However, Strategy 1 consistently outperforms Strategy 2, exhibiting lower packet loss rates and generally lower latency in all segments. Throughput is mostly comparable between the two strategies, with Strategy 2 showing a slight advantage in most segments, except for the HR Department, where Strategy 1 has marginally higher throughput.

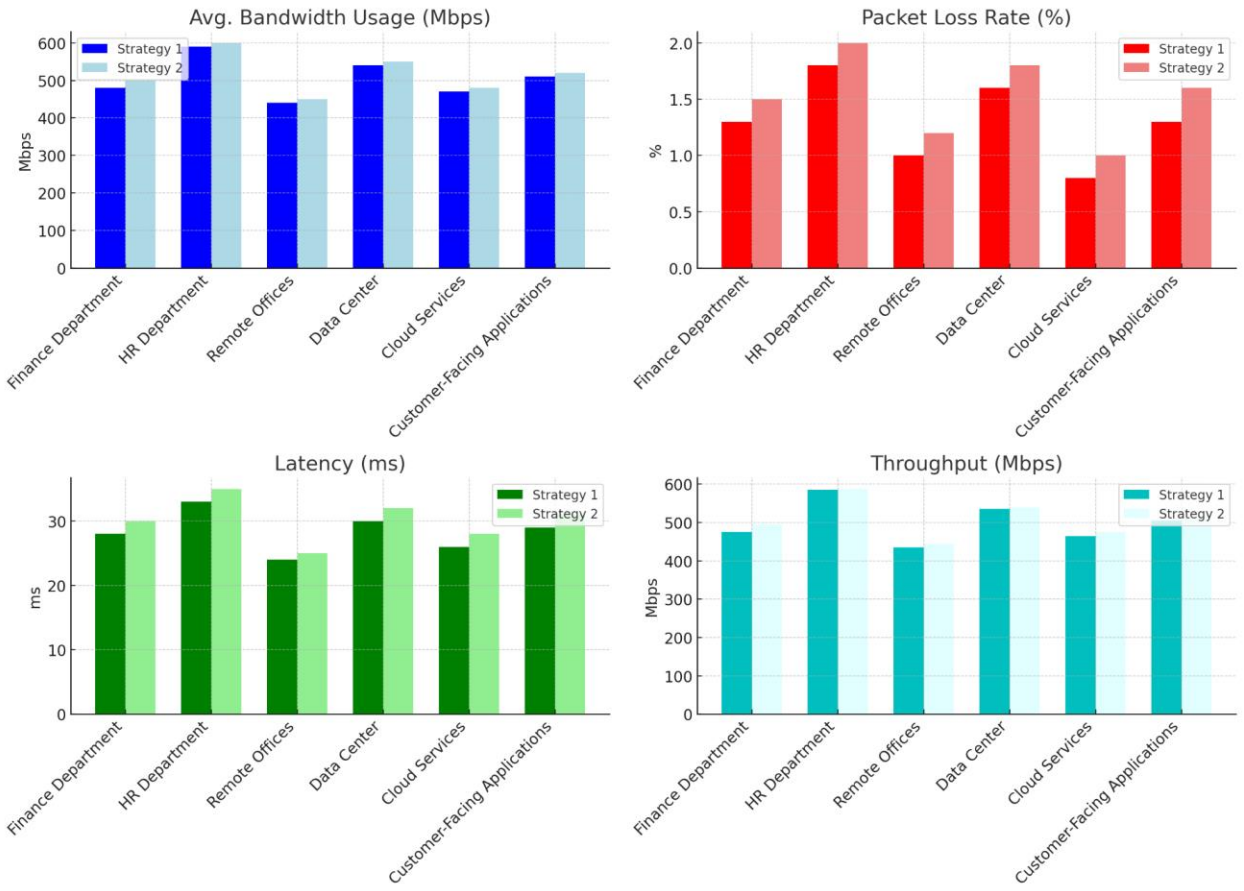

Figure 2: Comparison of the two segmentation results for the two segmentation strategy

Table 5 and Figure 3 provides a cost-benefit analysis of the two segmentation strategies. Segmentation Strategy 1 offers a higher improvement in throughput and reduction in latency but at a higher implementation cost. The cost-benefit ratio indicates that Strategy 1 provides more value per dollar spent compared to Strategy 2

Strategy	Improvement in Throughput (Mbps)	Reduction in Latency (ms)	Implementation Cost ($)	Cost-Benefit Ratio
Segmentation Strategy 1	**20**	**2**	**10,000**	**2.2**
Segmentation Strategy 2	**15**	**1**	**8,000**	**1.875**

Table 5: Cost-benefit analysis of the segmentation strategy

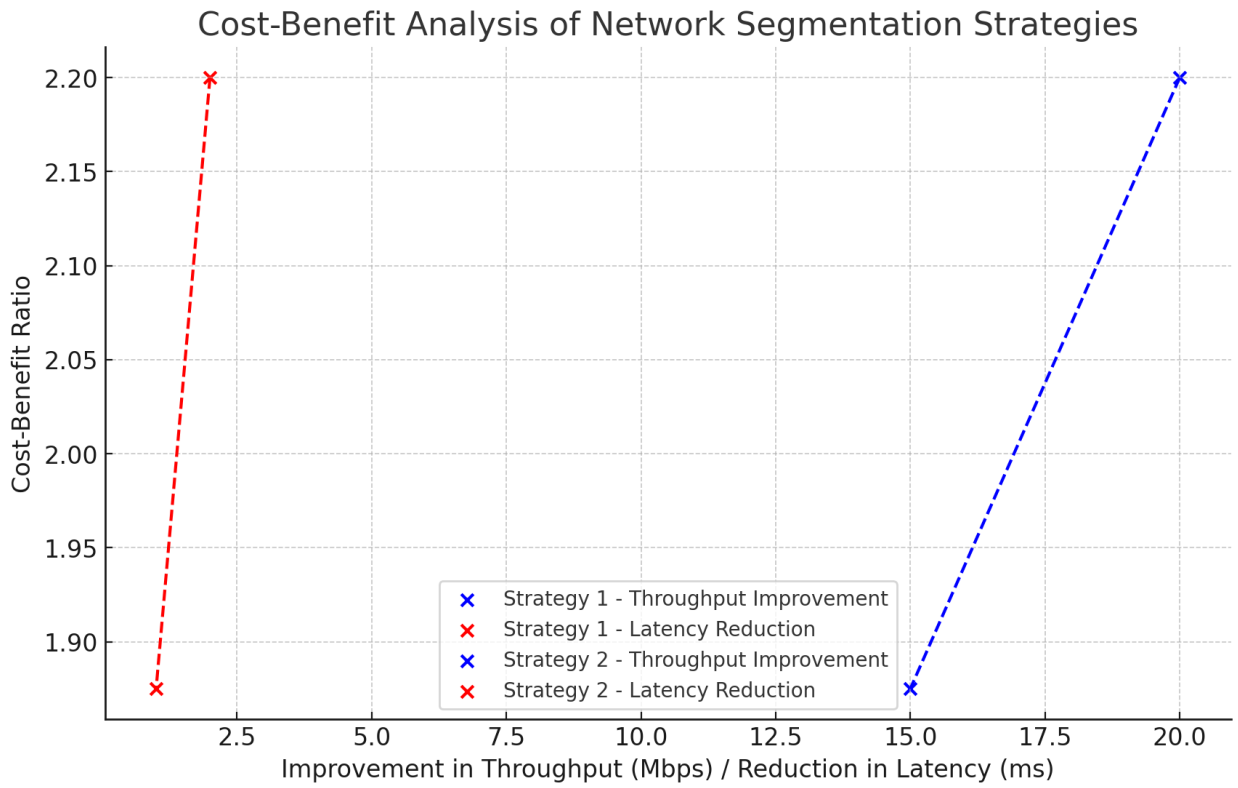

Figure 3: Cost-Benefit Analysis of Network-segmentation Strategies

Based on the analysis, Segmentation Strategy 1 is more effective in improving network performance metrics, despite its higher cost, due to its superior cost-benefit ratio. This comprehensive evaluation ensures that the chosen network segmentation strategy aligns with the study's objective of optimizing access control and minimizing damage from intrusions.

4.2 Evaluation of Incident Response Plan

Table 6 shows expected responses for simulated attack scenarios across various segments, such as email filtering and phishing awareness for the Finance Department and MFA for the HR Department**.**

Segment	Simulated Attack	Expected Response

Finance Department	**Phishing email with ransomware payload**	**Email filtering blocks phishing emails; users report suspicious emails due to training; endpoint security detects and isolates the threat.**
HR Department	**Credential dumping tool executed on endpoint**	**MFA prompts for verification; abnormal access patterns trigger alerts; the security team investigates and contains the threat.**
Remote Offices	**Unauthorized remote access tool installation**	**EDR detects and blocks the tool; patches prevent exploitation of vulnerabilities; the security team monitors for further attempts.**
Data Center	**Lateral movement attempt using compromised credentials**	**Network segmentation limits access; zero trust architecture requires re-authentication; monitoring tools detect and block movement.**
Cloud Services	**Data exfiltration via cloud storage**	**DLP tools detect and block unauthorized data transfer; encryption ensures data is unreadable; audit logs track the activity.**
Customer-Facing Applications	**DDoS attack on web application**	**DDoS mitigation services are activated, rate limiting controls traffic and the incident response team identifies and mitigates the attack source.**

Table 6: Result for the simulated attack and expected responses for the chosen department

Table 7 and Figure 4 summarize the quantitative results: quick response times, high containment efficiency, and fast recovery speeds across all segments. For instance, the Finance Department has a response time of 5 minutes, containment efficiency of 95%, and recovery speed of 10 minutes. These results confirm the incident response plan's effectiveness in detecting, containing, and recovering from ransomware and botnet attacks, providing a robust endpoint security strategy for remote workforces utilizing VPN networks.

Segment	Response Time (minutes)	Containment Efficiency (%)	Recovery Speed (minutes)
Finance Department	**5**	**95**	**10**
HR Department	**7**	**90**	**12**
Remote Offices	**6**	**92**	**11**
Data Center	**4**	**96**	**8**
Cloud Services	**6**	**94**	**9**
Customer-Facing Applications	**5**	**93**	**10**

Table 7: Results of the various departments based on Response Time, Containment Efficiency, and Recovery Speed.

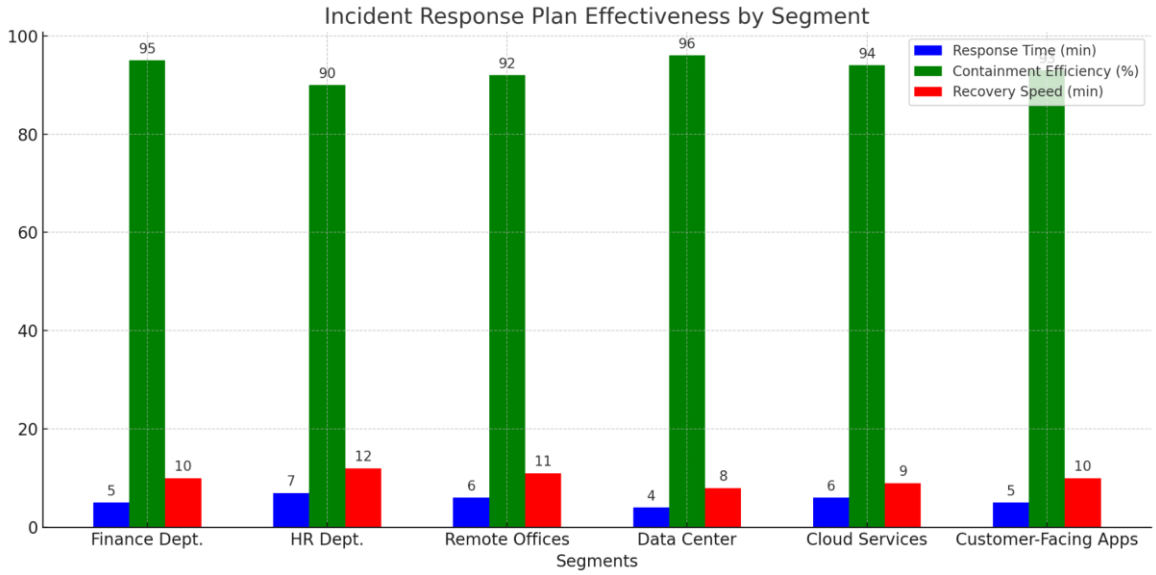

Figure 4: The effectiveness of the incident response plan

4.3 User Education Impact Assessment

Figure 5 visualizes the impact of the educational intervention on cybersecurity awareness. It shows the changes in key awareness metrics before and after the educational program across different segments. This clear comparison helps demonstrate the effectiveness of the intervention in improving familiarity with cybersecurity practices, frequency of password updates, and ability to recognize phishing emails.

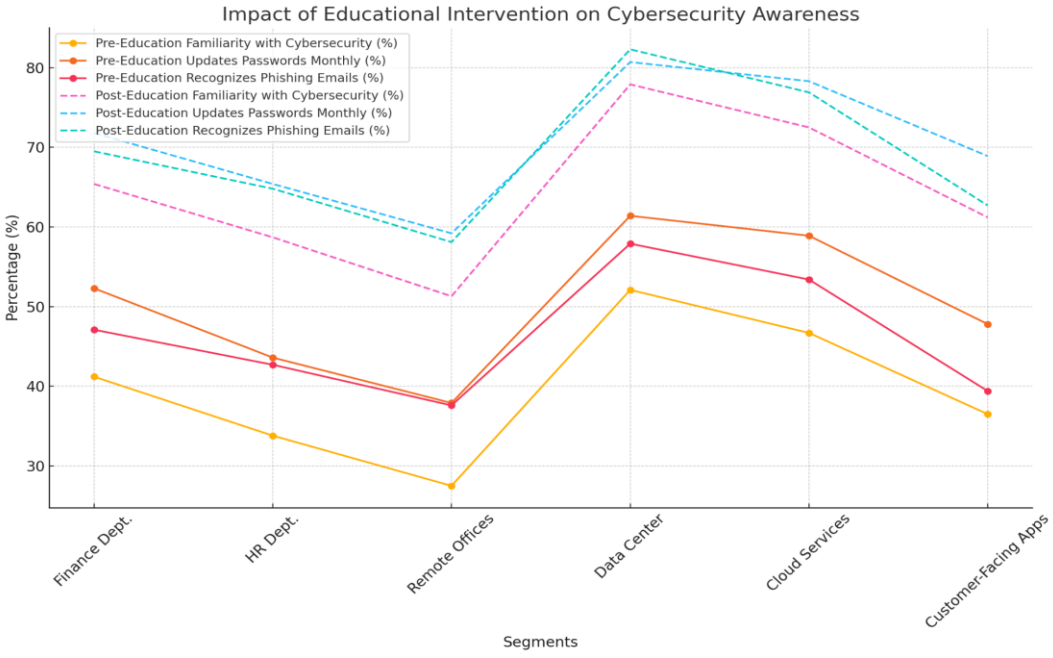

Figure 5: Impact of Educational Intervention on Cybersecurity Awareness

Table 8 presents the results of the chi-square tests and correlation analysis. The chi-square values and corresponding p-values indicate statistically significant improvements in all key awareness metrics after the educational intervention. The correlation coefficients (r) show a strong positive relationship between improved cybersecurity practices and reduced susceptibility to attacks, with p-values indicating statistical significance.

Metric	Chi-Square Value	p-Value	Correlation Coefficient (r)	Significance Level (p)
Familiarity with Cybersecurity	25.4	0.000	0.72	0.001
Updates Passwords Monthly	18.6	0.001	0.65	0.003
Recognizes Phishing Emails	22.8	0.000	0.69	0.002
Very Confident in Identifying Social Engineering	20.5	0.000	0.68	0.002

Table 8: Chi-Square and Pearson correlation result

These results confirm the effectiveness of the educational intervention in enhancing cybersecurity awareness and practices among remote workers, aligning with the study's objective of reducing the susceptibility of remote workers to ransomware and botnet attacks through user education.

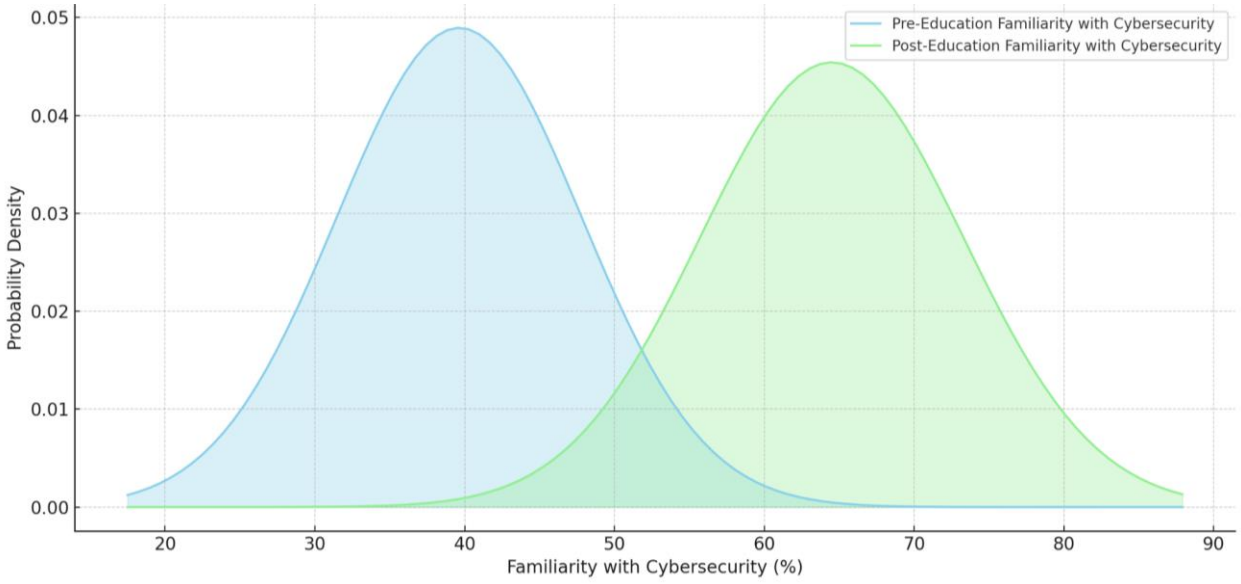

Figure 6: Normal Distribution of familiarity with cybersecurity before and after education

Figure 6 and Figure 7 represent familiarity with cybersecurity before and after the educational intervention. The shift towards higher familiarity post-education demonstrates the effectiveness of the intervention in improving cybersecurity awareness.

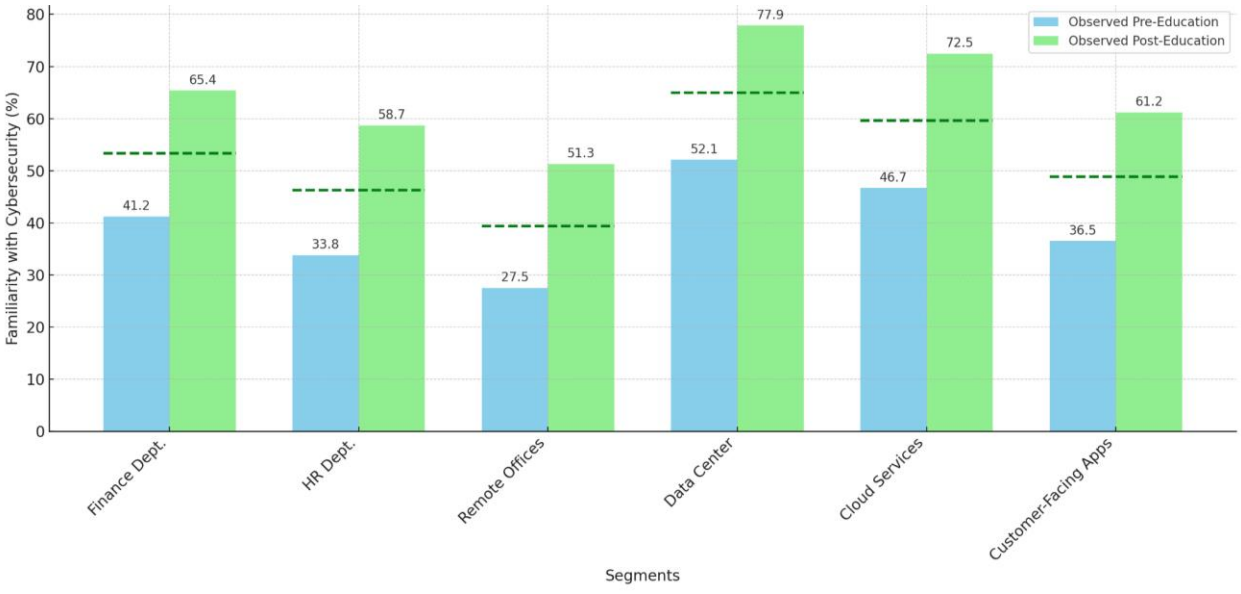

Figure 7: Chi-Square result

These charts demonstrate significant improvements in cybersecurity familiarity, confirming a statistically significant increase in awareness after the educational intervention.

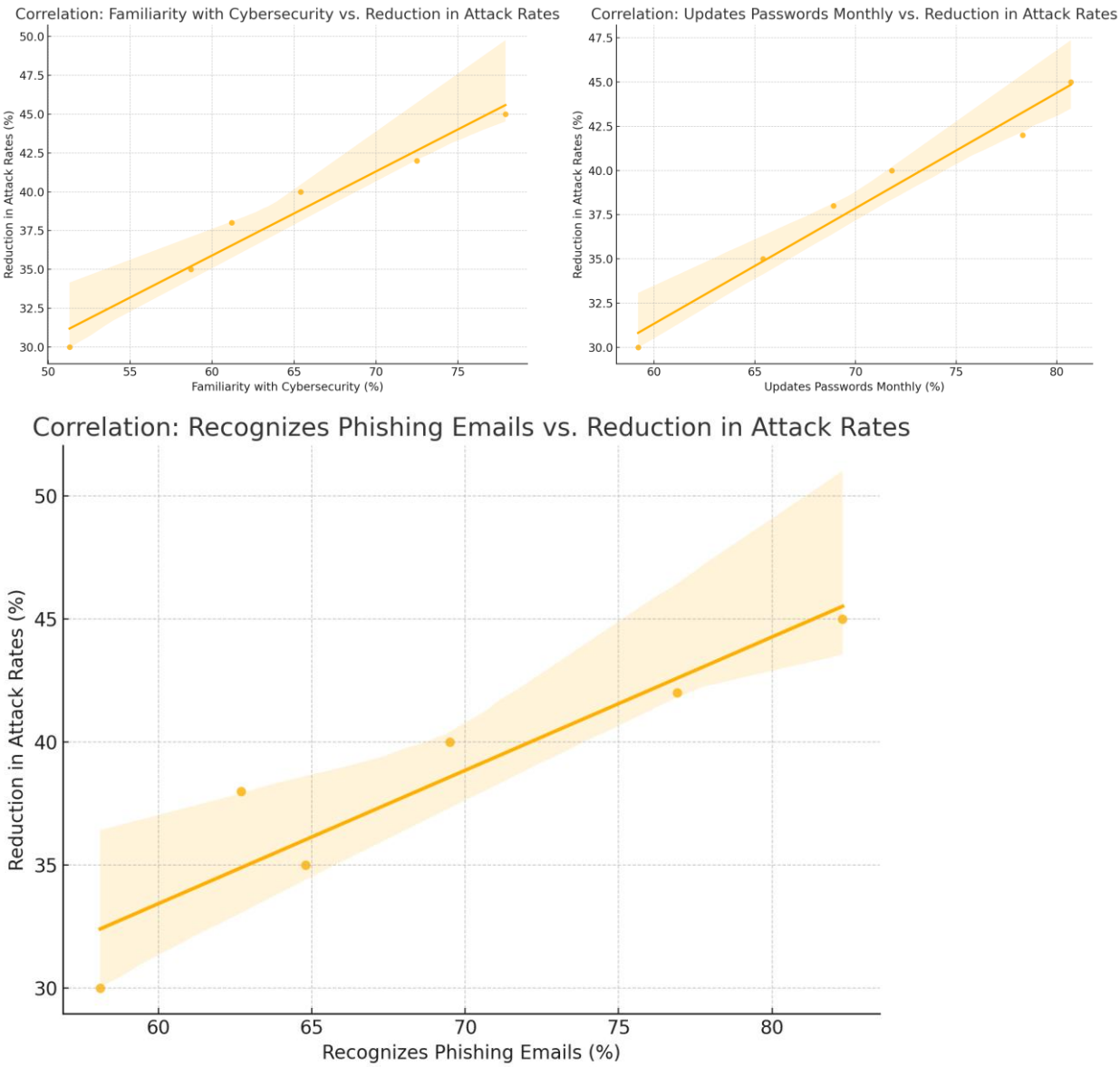

Figure 8: Correlation result

Figure 8 visualizes the correlation between key cybersecurity awareness metrics and the reduction in attack rates after the educational intervention. The plot for familiarity with cybersecurity vs. reduction in attack rates shows a positive correlation, indicating that increased familiarity with cybersecurity practices is associated with a reduction in attack rates. The plot for updated passwords monthly vs. reduction in attack rates also shows a positive correlation, suggesting that more frequent password updates are linked to lower attack rates. Similarly, the plot for recognizing phishing emails vs. reduction in attack rates demonstrates a positive correlation, implying that an improved ability to recognize phishing emails contributes to a reduction in attack rates. The regression lines in each plot provide a visual representation of the strength and direction

of these correlations. These visualizations confirm the effectiveness of the educational intervention in enhancing cybersecurity practices and reducing attack susceptibility.

The study's findings largely align with existing research on endpoint security for remote workforces [26]. The regression analysis confirms the importance of both detection and prevention rates in endpoint security effectiveness [26], echoing the foundational role of traditional tools like firewalls and anti-malware software [26][27][28]. However, the subtle difference in their contributions, revealed by the ANOVA results, supports concerns raised by Aslan et al. [11] about the limitations of these tools against zero-day exploits and social engineering tactics [11], strengthening the assertion of the necessity for a multi-layered approach, incorporating advanced technologies like machine learning and behavioral analytics, as advocated by Kibria et al. [23].

Moreover, the exploration of network segmentation strategies further validates the literature's emphasis on a tailored approach [61]. The superior performance of Segmentation Strategy 1 in enhancing network throughput and reducing latency aligns with the findings of Kallatsa [64], who demonstrated the effectiveness of segmentation in various organizational contexts [64]. Yet, the higher implementation cost of this strategy resonates with the challenges discussed by Nof et al. [68] concerning the balance between security and user experience [68]. This reinforces the need for a risk-based approach [69][70][71], where access controls are determined by data sensitivity and resource importance.

The empirical evaluation of the incident response plan confirms its effectiveness in mitigating ransomware and botnet attacks [84], mirroring the literature's emphasis on pre-incident preparation, clear procedures, and effective communication channels [84][85]. The rapid response times, high containment efficiency, and fast recovery across different segments demonstrate the value of a proactive and segment-specific approach [89][90][91], addressing the challenges highlighted by Gonzalez-Granadillo [85] regarding incident response in remote settings [85]. The successful integration of EDR and SOAR tools aligns with the recommendations of Tahmasebi [93] for a multi-faceted approach incorporating advanced technologies for effective threat detection and response [93].

The significant impact of user education on cybersecurity awareness further strengthens the literature's consistent advocacy for comprehensive training programs [30][100]. The statistically significant improvements in key awareness metrics and their strong positive correlations with reduced attack rates validate the importance of continuous reinforcement strategies, behavioral psychology integration, and interactive learning experiences, as proposed by Petter et al. [101] and other studies [102][103][104].

5. CONCLUSION AND RECOMMENDATION

This study provides empirical evidence for the effectiveness of a multi-faceted approach to endpoint security in remote work settings. By analyzing existing endpoint solutions, simulating network segmentation strategies, developing a tailored incident response plan, and assessing the impact of user education, this research offers valuable insights for organizations seeking to enhance their cybersecurity posture. The findings underscore the importance of combining advanced technologies with proactive measures and continuous user education to mitigate the evolving threats posed by ransomware and botnet attacks. Based on the study's findings, the following recommendations are proposed to bolster endpoint security for remote workforces:

1. Optimize Endpoint Security Solutions: Organizations should prioritize endpoint security solutions that offer robust prevention mechanisms alongside detection capabilities. The integration of machine learning and behavioral analytics can enhance threat detection and response capabilities, making them a valuable addition to the security stack.

2. Implement Tailored Network Segmentation: A risk-based approach to network segmentation, where access controls are determined by data sensitivity and resource importance, is recommended. Regular network traffic analysis and simulation can aid in refining segmentation strategies for optimal protection.

3. Develop Segment-Specific Incident Response Plans: Incident response plans should be tailored to the specific needs and vulnerabilities of each network segment. The integration of automation and orchestration tools can enhance the efficiency and effectiveness of incident response processes.

4. Prioritize User Education and Awareness: Comprehensive and ongoing cybersecurity training programs are crucial for empowering remote workers to identify and counteract threats. The use of interactive simulations, gamification elements, and real-life scenarios can enhance user engagement and knowledge retention.

REFERENCES

[1] A. Arora, S. K. Yadav, and K. Sharma, “Denial-of-Service (DoS) Attack and Botnet: Network Analysis, Research Tactics, and Mitigation,” *Research Anthology on Combating Denial-of-Service Attacks*, 2021. https://www.igi-global.com/chapter/denial-of-service-dos-attack-and-botnet/261970

[2] M. Kruse, “Tracing Volt Typhoon: Insights from GCA’s AIDE Honey Farm,” *GCA | Global Cyber Alliance | Working to Eradicate Cyber Risk*, Mar. 14, 2024. https://globalcyberalliance.org/tracing-volt-typhoon-insights-from-gcas-aide-honey-farm/ (accessed Jul. 12, 2024).

[3] M. Juma, A. A. Monem, and K. Shaalan, “Hybrid End-to-End VPN Security Approach for Smart IoT Objects,” *Journal of Network and Computer Applications*, vol. 158, p. 102598, May 2020, doi: https://doi.org/10.1016/j.jnca.2020.102598.

[4] S. Kerner, “Colonial Pipeline Hack explained: Everything You Need to Know,” *TechTarget*, Apr. 26, 2022. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

[5] D. Georgoulias, J. M. Pedersen, M. Falch, and E. Vasilomanolakis, “Botnet business models, takedown attempts, and the darkweb market: a survey,” *ACM Computing Surveys*, vol. 55, no. 11, Dec. 2022, doi: https://doi.org/10.1145/3575808.

[6] A. O. Alzahrani and M. J. F. Alenazi, “Designing a Network Intrusion Detection System Based on Machine Learning for Software Defined Networks,” *Future Internet*, vol. 13, no. 5, p. 111, Apr. 2021, doi: https://doi.org/10.3390/fi13050111.

[7] A. Alzahrani, “Coronavirus Social Engineering Attacks: Issues and Recommendations,” *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 5, 2020, doi: https://doi.org/10.14569/ijacsa.2020.0110523.

[8] R. Ferreira, R. Pereira, I. S. Bianchi, and M. M. da Silva, “Decision Factors for Remote Work Adoption: Advantages, Disadvantages, Driving Forces and Challenges,” *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 7, no. 1, p. 70, Mar. 2021, doi: https://doi.org/10.3390/joitmc7010070.

[9] A. I. Tahirkheli *et al.*, “A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges,” *Electronics*, vol. 10, no. 15, p. 1811, Jul. 2021, doi: https://doi.org/10.3390/electronics10151811.

[10] A. T. Arigbabu, O. O. Olaniyi, C. S. Adigwe, O. O. Adebiyi, and S. A. Ajayi, “Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 85–107, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5441.

[11] O. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions,” *Electronics*, vol. 12, no. 6, pp. 1–42, Mar. 2023, doi: https://doi.org/10.3390/electronics12061333.

[12] M. Bispham, S. Creese, W. H. Dutton, P. Esteve-Gonzalez, and M. Goldsmith, “Cybersecurity in Working from Home: An Exploratory Study,” *papers.ssrn.com*, Aug. 01, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3897380

[13] N. R. Mayeke, A. T. Arigbabu, O. O. Olaniyi, O. J. Okunleye, and C. S. Adigwe, “Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and System Assurance in Cyber Engineering. ,” vol. 17, no. 5, pp. 108–124, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5442.

[14] W. Z. A. Zakaria, M. F. Abdollah, O. Mohd, and A. F. M. Ariffin, “The Rise of Ransomware,” *Proceedings of the 2017 International Conference on Software and e-Business - ICSEB 2017*, 2017, doi: https://doi.org/10.1145/3178212.3178224.

[15] J. Fox, “11 Biggest Ransomware Attacks in History,” *www.cobalt.io*, Jul. 24, 2023. https://www.cobalt.io/blog/11-biggest-ransomware-attacks-in-history

[16] P. Paganini, “China-linked APT Volt Typhoon linked to KV-Botnet,” *Security Affairs*, Dec. 14, 2023. https://securityaffairs.com/155797/apt/volt-typhoon-linked-to-kv-botnet.html

[17] C. S. Adigwe, N. R. Mayeke, S. O. Olabanji, O. J. Okunleye, P. C. Joeaneke, and O. O. Olaniyi, “The Evolution of Terrorism in the Digital Age: Investigating the Adaptation of Terrorist Groups to Cyber Technologies for Recruitment, Propaganda, and Cyberattacks,” *Asian journal of economics, business and accounting*, vol. 24, no. 3, pp. 289–306, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i31287.

[18] C. Talos, “YEAR IN REVIEW,” *CISCO TALOS BLOG*, 2023. https://blog.talosintelligence.com/content/files/2023/12/2023_Talos_Year_In_Review.pdf

[19] A. Mishra, *Modern Cybersecurity Strategies for Enterprises: Protect and Secure Your Enterprise Networks, Digital Business Assets, and Endpoint Security with Tested and Proven Methods (English Edition)*. BPB Publications, 2022. Accessed: Jul. 13, 2024. [Online]. Available:

https://books.google.com/books?hl=en&lr=&id=EpaFEAAAQBAJ&oi=fnd&pg=PT35&dq=traditional+cybersecurity+measures+frequently+fall+short+against+the+threat+posed+by+these+malicious+activities

[20] V. Vasani, A. K. Bairwa, S. Joshi, A. Pljonkin, M. Kaur, and M. Amoon, "Comprehensive Analysis of Advanced Techniques and Vital Tools for Detecting Malware Intrusion," *Electronics*, vol. 12, no. 20, p. 4299, Jan. 2023, doi: https://doi.org/10.3390/electronics12204299.

[21] C. S. Adigwe, O. O. Olaniyi, S. O. Olabanji, O. J. Okunleye, N. R. Mayeke, and S. A. Ajayi, "Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy," *Asian journal of economics, business and accounting*, vol. 24, no. 4, pp. 126–146, Feb. 2024, doi: https://doi.org/10.9734/ajeba/2024/v24i41269.

[22] U. T. I. Igwenagu, A. A. Salami, A. S. Arigbabu, C. E. Mesode, T. O. Oladoyinbo, and O. O. Olaniyi, "Securing the Digital Frontier: Strategies for Cloud Computing Security, Database Protection, and Comprehensive Penetration Testing," *Journal of Engineering Research and Reports*, vol. 26, no. 6, pp. 60–75, May 2024, doi: https://doi.org/10.9734/jerr/2024/v26i61162.

[23] M. G. Kibria, K. Nguyen, G. P. Villardi, O. Zhao, K. Ishizu, and F. Kojima, "Big Data Analytics, Machine Learning, and Artificial Intelligence in Next-Generation Wireless Networks," *IEEE Access*, vol. 6, pp. 32328–32338, 2018, doi: https://doi.org/10.1109/access.2018.2837692.

[24] Maher Boughdiri, T. Abdellatif, and Chirine Ghedira Guegan, "How Does Blockchain Enhance Zero Trust Security in IoMT?," *Communications in computer and information science*, pp. 184–197, Jan. 2024, doi: https://doi.org/10.1007/978-3-031-55729-3_15.

[25] F. A. Ezeugwa, "Evaluating the Integration of Edge Computing and Serverless Architectures for Enhancing Scalability and Sustainability in Cloud-based Big Data Management," *Journal of Engineering Research and Reports*, vol. 26, no. 7, pp. 347–365, Jul. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i71214.

[26] P. Ruotsalainen, "ENDPOINT PROTECTION SECURITY SYSTEM FOR AN ENTERPRISE," *www.theseus.fi*, 2013. https://www.theseus.fi/handle/10024/62932

[27] T. Campbell, "Protection of Systems," Jan. 2016, doi: https://doi.org/10.1007/978-1-4842-1685-9_10.

[28] Oladipo Ogunmesa , "Strategies Security Managers Used to Prevent Security Breaches in SCADA Systems' Networks - ProQuest," *www.proquest.com*, 2021.

https://search.proquest.com/openview/be5fd358f70e64b94c469475b2ade744/1?pq-origsite=gscholar&cbl=18750&diss=y (accessed Jul. 13, 2024).

[29] I. H. Sarker, “Machine Learning: Algorithms, Real-World Applications and Research Directions,” *SN Computer Science*, vol. 2, no. 3, pp. 1–21, Mar. 2021, doi: https://doi.org/10.1007/s42979-021-00592-x.

[30] T. Rains, *Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks*. Packt Publishing Ltd, 2020. Accessed: Jul. 13, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=8YLoDwAAQBAJ&oi=fnd&pg=PP1&dq=+the+effectiveness+of+these+traditional+security+measures+cannot+be+used+to+combat+the+threat+posed+by+sophisticated+ransomware+and+botnet+attacks

[31] A. Bhardwaj, *New Age Cyber Threat Mitigation for Cloud Computing Networks*. Bentham Science Publishers, 2023. Accessed: Jul. 13, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=GarKEAAAQBAJ&oi=fnd&pg=PP10&dq=while+traditional+endpoint+security+tools+are+foundational

[32] O. O. Olaniyi, “Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies,” *Asian Journal of Research in Computer Science*, vol. 17, no. 5, pp. 172–189, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5447.

[33] A. Scarfo, “New Security Perspectives around BYOD,” *IEEE Xplore*, Nov. 01, 2012. https://ieeexplore.ieee.org/abstract/document/6363095/

[34] A. E. Omolara *et al.*, “The internet of things security: A survey encompassing unexplored areas and new insights,” *Computers & Security*, vol. 112, p. 102494, Jan. 2022, doi: https://doi.org/10.1016/j.cose.2021.102494.

[35] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, “A roadmap for security challenges in the Internet of Things,” *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, Apr. 2018, doi: https://doi.org/10.1016/j.dcan.2017.04.003.

[36] O. O. Olaniyi, F. A. Ezeugwa, C. G. Okatta, A. S. Arigbabu, and P. C. Joeaneke, “Dynamics of the Digital Workforce: Assessing the Interplay and Impact of AI, Automation, and Employment Policies,” *Archives of current research international*, vol. 24, no. 5, pp. 124–139, Apr. 2024, doi: https://doi.org/10.9734/acri/2024/v24i5690.

[37] L. F. Ilca, O. P. Lucian, and T. C. Balan, “Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and

Response," *Sensors*, vol. 23, no. 15, p. 6757, Jan. 2023, doi: https://doi.org/10.3390/s23156757.

[38] S. O. Olabanji, "AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems," *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 38–56, 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3423.

[39] F. R. R. Zambrano and G. D. R. Rafael, "Bring your own device: a survey of threats and security management models," *International Journal of Electronic Business*, vol. 14, no. 2, p. 146, 2018, doi: https://doi.org/10.1504/ijeb.2018.094862.

[40] Y. A. Marquis, T. O. Oladoyinbo, S. O. Olabanji, O. O. Olaniyi, and S. S. Ajayi, "Proliferation of AI Tools: A Multifaceted Evaluation of User Perceptions and Emerging Trend," *Asian Journal of Advanced Research and Reports*, vol. 18, no. 1, pp. 30–35, Jan. 2024, doi: https://doi.org/10.9734/ajarr/2024/v18i1596.

[41] G. N. M. Wangutusi, "An exploration of how BYOD (Bring Your Own Device) user behavior impacts on an organization's information security: A case study of Madison Insurance Company Kenya Limited," *erepository.uonbi.ac.ke*, 2015. http://erepository.uonbi.ac.ke/handle/11295/90069

[42] J. Lyons, "FBI confirms it issued remote kill command to blow out Volt Typhoon's botnet," *Theregister.com*, Jan. 31, 2024. https://www.theregister.com/2024/01/31/volt_typhoon_botnet/ (accessed Jul. 13, 2024).

[43] A. A. Salami, U. T. I. Igwenagu, C. E. Mesode, O. O. Olaniyi, and O. B. Oladoyinbo, "Beyond Conventional Threat Defense: Implementing Advanced Threat Modeling Techniques, Risk Modeling Frameworks and Contingency Planning in the Healthcare Sector for Enhanced Data Security," *Journal of Engineering Research and Reports*, vol. 26, no. 5, pp. 304–323, Apr. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i51156.

[44] T. Rains, *Cybersecurity Threats, Malware Trends, and Strategies: Discover risk mitigation strategies for modern threats to your organization*. Packt Publishing Ltd, 2023. Accessed: Jul. 13, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=TN-oEAAAQBAJ&oi=fnd&pg=PP1&dq=older+devices+are+often+disproportionately+targeted+due+to+their+unpatched+vulnerabilities

[45] C. Maple, "Security and privacy in the internet of things," *Journal of Cyber Policy*, vol. 2, no. 2, pp. 155–184, May 2017, doi: https://doi.org/10.1080/23738871.2017.1366536.

[46] A. Tsohou, M. Karyda, S. Kokolakis, and E. Kiountouzis, “Managing the introduction of information security awareness programmes in organisations,” *European Journal of Information Systems*, vol. 24, no. 1, pp. 38–58, Jan. 2015, doi: https://doi.org/10.1057/ejis.2013.27.

[47] M. Rossi, P. Sainio, and A. Hakkala, “Enhancing cyber assets visibility for effective attack surface management Cyber Asset Attack Surface Management based on Knowledge Graph,” 2023. Available: https://www.utupub.fi/bitstream/handle/10024/175930/Thesis-CAASM-CloudSecurity_Marco_Carmine_Rossi.pdf?sequence=1

[48] Y. Diogenes and D. E. Ozkaya, *Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals*. Packt Publishing Ltd, 2019. Accessed: Jul. 13, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=E7zHDwAAQBAJ&oi=fnd&pg=PP1&dq=Cloud-based+endpoint+security+solutions+and+centralized+patching+management+are+gaining+momentum%3B+these+approaches+can+enforce+security+policies+and+ensure+that+all+devices

[49] S. O. Olabanji, Y. A. Marquis, C. S. Adigwe, A. S. Abidemi, T. O. Oladoyinbo, and O. O. Olaniyi, “AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 57–74, Jan. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i3424.

[50] A. Arfeen, S. Ahmed, M. A. Khan, and S. F. A. Jafri, “Endpoint Detection & Response: A Malware Identification Solution,” *2021 International Conference on Cyber Warfare and Security (ICCWS)*, Nov. 2021, doi: https://doi.org/10.1109/iccws53234.2021.9703010.

[51] R. Badhwar, “The Case for AI/ML in Cybersecurity,” *The CISO’s Next Frontier*, pp. 45–73, 2021, doi: https://doi.org/10.1007/978-3-030-75354-2_5.

[52] R. H. Khokhar *et al.*, “A Survey on Supply Chain Management: Exploring Physical and Cyber Security Challenges, Threats, Critical Applications, and Innovative Technologies,” *International Journal of Supply and Operations Management*, vol. 11, no. 3, pp. 250–283, Aug. 2024, doi: https://doi.org/10.22034/ijsom.2024.110219.2975.

[53] O. O. Olaniyi, J. C. Ugonnia, F. G. Olaniyi, A. T. Arigbabu, and C. S. Adigwe, “Digital Collaborative Tools, Strategic Communication, and Social Capital: Unveiling the Impact of Digital Transformation on Organizational Dynamics,” *Asian Journal of Research in*

Computer Science, vol. 17, no. 5, pp. 140–156, Mar. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i5444.

[54] S. Atay and M. Masera, “Challenges for the security analysis of Next Generation Networks,” *Information Security Technical Report*, vol. 16, no. 1, pp. 3–11, Feb. 2011, doi: https://doi.org/10.1016/j.istr.2010.10.010.

[55] Dimitrios Lazaros Pissanidis and Konstantinos Demertzis, “Integrating AI/ML in Cybersecurity: An Analysis of Open XDR Technology and its Application in Intrusion Detection and System Log Management,” Dec. 2023, doi: https://doi.org/10.20944/preprints202312.0205.v1.

[56] A. D. Samuel-Okon, O. O. Olateju, S. U. Okon, O. O. Olaniyi, and U. T. I. Igwenagu, “Formulating Global Policies and Strategies for Combating Criminal Use and Abuse of Artificial Intelligence,” *Archives of current research international*, vol. 24, no. 5, pp. 612–629, Jun. 2024, doi: https://doi.org/10.9734/acri/2024/v24i5735.

[57] A. Kamruzzaman, S. Ismat, J. C. Brickley, A. Liu, and K. Thakur, “A Comprehensive Review of Endpoint Security: Threats and Defenses,” *IEEE Xplore*, Dec. 01, 2022. https://ieeexplore.ieee.org/abstract/document/9998470/

[58] F. A. Ezeugwa, O. O. Olaniyi, J. C. Ugonnia, A. S. Arigbabu, and P. C. Joeaneke, “Artificial Intelligence, Big Data, and Cloud Infrastructures: Policy Recommendations for Enhancing Women’s Participation in the Tech-Driven Economy,” *Journal of Engineering Research and Reports*, vol. 26, no. 6, pp. 1–16, May 2024, doi: https://doi.org/10.9734/jerr/2024/v26i61158.

[59] K. Sehgal and N. Thymianis, *Cybersecurity Blue Team Strategies: Uncover the secrets of blue teams to combat cyber threats in your organization*. Packt Publishing Ltd, 2023. Accessed: Jul. 13, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=ojWxEAAAQBAJ&oi=fnd&pg=PP1&dq=+integration+of+NGAV+with+cloud-based+security+platforms

[60] O. O. Olateju, S. U. Okon, U. T. I. Igwenagu, A. A. Salami, T. O. Oladoyinbo, and O. O. Olaniyi, “Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud,” *Asian Journal of Research in Computer Science*, vol. 17, no. 6, pp. 264–292, Jun. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i6472.

[61] G. Treider, “Investigation of the Gap Between Traditional IP Network Security Management and the Adoption of Automation Techniques and Technologies to Network

Security," *ntnuopen.ntnu.no*, 2023. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3118326 (accessed Jul. 13, 2024).

[62] C. Scott, P. Wolfe, and M. Erwin, *Virtual Private Networks*. "O'Reilly Media, Inc.," 1999. Accessed: Jul. 13, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=OuFQ3t7eF4IC&oi=fnd&pg=PR9&dq=Virtual+Private+Networks+involves+dividing+a+network+into+multiple+segments+or+subnetworks

[63] O. J. Okunleye, "The Role of Information Governance in Mitigating Financial Crime Risks in Stablecoin Transactions," *Journal of Engineering Research and Reports*, vol. 26, no. 7, pp. 317–333, Jul. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i71212.

[64] M. Kallatsa, "Strategies for network segmentation : a systematic literature review," *jyx.jyu.fi*, 2024, Available: https://jyx.jyu.fi/handle/123456789/92952

[65] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, "A Survey of Moving Target Defenses for Network Security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1909–1941, 2020, doi: https://doi.org/10.1109/comst.2020.2982955.

[66] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 40, no. 4, pp. 853–865, Jul. 2020, doi: https://doi.org/10.1109/tsmca.2010.2048028.

[67] E. D. Knapp, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Elsevier, 2024. Accessed: Jul. 13, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=tE7VEAAAQBAJ&oi=fnd&pg=PP1&dq=By+isolating+critical+system+components

[68] S. Y. Nof, J. Ceroni, W. Jeong, and M. Moghaddam, *Revolutionizing Collaboration through e-Work, e-Business, and e-Service*. Springer, 2015. Accessed: Jul. 13, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=Yl3gCQAAQBAJ&oi=fnd&pg=PR7&dq=the+challenges+encountered+when+balancing+security+with+user+experience

[69] N. Metoui, "Privacy-Aware Risk-Based Access Control Systems," *eprints-phd.biblio.unitn.it*, May 04, 2018. http://eprints-phd.biblio.unitn.it/2844/ (accessed Jul. 13, 2024).

[70] J. C. Ugonnia, O. O. Olaniyi, F. G. Olaniyi, A. A. Arigbabu, and T. O. Oladoyinbo, “Towards Sustainable IT Infrastructure: Integrating Green Computing with Data Warehouse and Big Data Technologies to Enhance Efficiency and Environmental Responsibility,” *Journal of Engineering Research and Reports*, vol. 26, no. 5, pp. 247–261, Apr. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i51151.

[71] S. Savinov, “A Dynamic Risk-Based Access Control Approach: Model and Implementation,” *uwspace.uwaterloo.ca*, May 18, 2017. https://uwspace.uwaterloo.ca/handle/10012/11917 (accessed Jul. 13, 2024).

[72] A. Singh Uppal, “Multi-Factor Authentication in Network Security,” *ERA*, Jan. 01, 2021. https://era.library.ualberta.ca/items/f060e9dd-30d4-474e-b165-1e1a5137fa42

[73] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-Factor Authentication: A Survey,” *Cryptography*, vol. 2, no. 1, p. 1, Jan. 2018, doi: https://doi.org/10.3390/cryptography2010001.

[74] S. H. A. Kazmi, R. Hassan, F. Qamar, K. Nisar, and A. A. A. Ibrahim, “Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques and Research Directions,” *Symmetry*, vol. 15, no. 6, p. 1147, Jun. 2023, doi: https://doi.org/10.3390/sym15061147.

[75] O. J. Okunleye, “The Role of Open Data in Driving Sectoral Innovation and Global Economic Development,” *Journal of Engineering Research and Reports*, vol. 26, no. 7, pp. 222–243, Jun. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i71205.

[76] G. Singh, G. Bhardwaj, S. V. Singh, and V. Garg, “Biometric Identification System: Security and Privacy Concern,” *Artificial Intelligence for a Sustainable Industry 4.0*, pp. 245–264, 2021, doi: https://doi.org/10.1007/978-3-030-77070-9_15.

[77] R. S. Chowhan and R. Tanwar, “Password-Less Authentication: Methods for User Verification and Identification to Login Securely Over Remote Sites,” *Machine Learning and Cognitive Science Applications in Cyber Security*, 2019. https://www.igi-global.com/chapter/password-less-authentication/227582

[78] O. O. Olateju, S. U. Okon, O. O. Olaniyi, A. D. Samuel-Okon, and C. U. Asonze, “Exploring the Concept of Explainable AI and Developing Information Governance Standards for Enhancing Trust and Transparency in Handling Customer Data,” *Journal of Engineering Research and Reports*, vol. 26, no. 7, pp. 244–268, Jun. 2024, doi: https://doi.org/10.9734/jerr/2024/v26i71206.

[79] C. Itodo and M. Ozer, “Multivocal literature review on zero-trust security implementation,” *Computers & Security*, vol. 141, p. 103827, Jun. 2024, doi: https://doi.org/10.1016/j.cose.2024.103827.

[80] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” *Zero Trust Architecture*, vol. 800–207, no. 800–207, Aug. 2020, doi: https://doi.org/10.6028/nist.sp.800-207.

[81] A. Talan, “Zero Trust Network Access with Cybersecurity Challenges and Potential Solutions,” *norma.ncirl.ie*, Dec. 14, 2022. https://norma.ncirl.ie/6548/

[82] R. Chandramouli, “Guide to Secure Enterprise Network Landscape,” *Guide to a Secure Enterprise Network Landscape*, Nov. 2022, doi: https://doi.org/10.6028/nist.sp.800-215.

[83] L. Gudala, M. Shaik, and S. Venkataramanan, “Leveraging Machine Learning for Enhanced Threat Detection and Response in Zero Trust Security Frameworks: An Exploration of Real-Time Anomaly Identification and Adaptive Mitigation Strategies,” *Journal of Artificial Intelligence Research*, vol. 1, no. 2, pp. 19–45, Nov. 2021, Accessed: Jul. 14, 2024. [Online]. Available: https://thesciencebrigade.com/JAIR/article/view/222

[84] S. Regner, *Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM*. IGI Global, 2020. Accessed: Jul. 14, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=7rgIEAAAQBAJ&oi=fnd&pg=PR1&dq=a+robust+IR+model+consists+of+preparation

[85] G. Gonzalez-Granadillo *et al.*, “Automated Cyber and Privacy Risk Management Toolkit,” *Sensors (14248220)*, vol. 21, no. 16, pp. 5493–5493, Aug. 2021, doi: https://doi.org/10.3390/s21165493.

[86] D. Bastos, M. Shackleton, and F. El-Moussa, “Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments,” *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018, doi: https://doi.org/10.1049/cp.2018.0030.

[87] O. B. Oladoyinbo, “Impact of Malaria on Lifestyle and Agricultural Practices among Rice Farmers in South-West Nigeria,” *Asian journal of agricultural extension, economics and sociology*, vol. 42, no. 6, pp. 373–386, Jun. 2024, doi: https://doi.org/10.9734/ajaees/2024/v42i62500.

[88] R. T. Sylves, *Disaster Policy and Politics: Emergency Management and Homeland Security*. CQ Press, 2019. Accessed: Jul. 14, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=WBZoDwAAQBAJ&oi=fnd&pg=PT13&d

q=studies+advocate+for+the+involvement+of+remote+workers+in+the+incident+response+processes

[89] G. N. Angafor, I. Yevseyeva, and L. Maglaras, “Scenario-based incident response training: lessons learnt from conducting an experiential learning virtual incident response tabletop exercise,” *Information & Computer Security*, Mar. 2023, doi: https://doi.org/10.1108/ics-05-2022-0085.

[90] A. D. Samuel-Okon, “Smart Media or Biased Media: The Impacts and Challenges of AI and Big Data on the Media Industry,” *Asian Journal of Research in Computer Science*, vol. 17, no. 7, pp. 128–144, Jul. 2024, doi: https://doi.org/10.9734/ajrcos/2024/v17i7484.

[91] W. van Zoonen *et al.*, “Factors Influencing Adjustment to Remote Work: Employees’ Initial Responses to the COVID-19 Pandemic,” *International Journal of Environmental Research and Public Health*, vol. 18, no. 13, p. 6966, Jun. 2021, Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8297254/

[92] R. Williams, E. Ntontis, K. Alfadhli, J. Drury, and R. Amlôt, “A social model of secondary stressors in relation to disasters, major incidents and conflict: Implications for practice,” *International Journal of Disaster Risk Reduction*, vol. 63, p. 102436, Sep. 2021, doi: https://doi.org/10.1016/j.ijdrr.2021.102436.

[93] M. Tahmasebi, “Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises,” *Journal of Information Security*, vol. 15, no. 2, pp. 106–133, Feb. 2024, doi: https://doi.org/10.4236/jis.2024.152008.

[94] A. Bolla and F. Talentino, “Threat Hunting driven by Cyber Threat Intelligence,” *webthesis.biblio.polito.it*, Apr. 13, 2022. https://webthesis.biblio.polito.it/22631/

[95] W. U. Hassan, A. Bates, and D. Marino, “Tactical Provenance Analysis for Endpoint Detection and Response Systems,” *IEEE Xplore*, May 01, 2020. https://ieeexplore.ieee.org/abstract/document/9152771

[96] G. Nagar, “The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies,” *Valley International Journal Digital Library*, pp. 1282–1298, Jun. 2024, doi: https://doi.org/10.18535/ijsrm/v12i06.ec09.

[97] Oluwaseun Oladeji Olaniyi and Dagogo Sopriala Omubo, “WhatsApp Data Policy, Data Security and Users’ Vulnerability,” *International journal of innovative research and development*, May 2023, doi: https://doi.org/10.24940/ijird/2023/v12/i4/apr23021.

[98] K. Kiiveri, “Automation in cyber security,” *www.theseus.fi*, 2021. https://www.theseus.fi/handle/10024/503899

[99] O. O. Olaniyi, O. O. Olaoye, and O. J. Okunleye, “Effects of Information Governance (IG) on Profitability in the Nigerian Banking Sector,” *Asian Journal of Economics, Business and Accounting*, vol. 23, no. 18, pp. 22–35, Jul. 2023, doi: https://doi.org/10.9734/ajeba/2023/v23i181055.

[100] J. S. Sandhu, *Cybersecurity for Executives: Advancing leaders to practical Cyber Risk Management*. Notion Press, 2021. Accessed: Jul. 14, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=VyZXEAAAQBAJ&oi=fnd&pg=PT11&dq=Comprehensive+training+programs

[101] S. Petter and L. Giddens, “Reskilling the workforce with technology-oriented training | VOCEDplus, the international tertiary education and research database,” *www.voced.edu.au*, 2021. https://www.voced.edu.au/content/ngv:93163 (accessed Jul. 14, 2024).

[102] Z. Redelinghuys, “Gamification and simulation teaching -- a system created to improve the depth of knowledge and knowledge retention of engineering students,” *scholar.sun.ac.za*, Mar. 01, 2021. https://scholar.sun.ac.za/handle/10019.1/109909 (accessed Jul. 14, 2024).

[103] M. M. Asad, A. Naz, P. Churi, and M. M. Tahanzadeh, “Virtual Reality as Pedagogical Tool to Enhance Experiential Learning: A Systematic Literature Review,” *Education Research International*, vol. 2021, p. e7061623, Nov. 2021, doi: https://doi.org/10.1155/2021/7061623.

[104] G. B. Petersen, G. Petkakis, and G. Makransky, “A study of how immersion and interactivity drive VR learning,” *Computers & Education*, vol. 179, p. 104429, Apr. 2022, doi: https://doi.org/10.1016/j.compedu.2021.104429.

[105] G. Hatzivasilis *et al.*, “Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees,” *Applied Sciences*, vol. 10, no. 16, p. 5702, Aug. 2020, doi: https://doi.org/10.3390/app10165702.

[106] L. Williams, Eirini Anthi, Yulia Cherdantseva, and A. Javed, “Leveraging Gamification and Game-based Learning in Cybersecurity Education,” *Journal of The Colloquium for Information Systems Security Education*, vol. 11, no. 1, pp. 8–8, Feb. 2024, doi: https://doi.org/10.53735/cisse.v11i1.186.

[107] C. Robert, *Gamification Strategies for Retention, Motivation, and Engagement in Higher Education: Emerging Research and Opportunities: Emerging Research and Opportunities*. IGI Global, 2020. Accessed: Jul. 14, 2024. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=NTDeDwAAQBAJ&oi=fnd&pg=PR1&dq

=Gamification+is+an+initiative+developed+to+help+gain+user+engagement+and+to+also+maintain+retention

[108] S. Clarke, “Coventry University DOCTOR OF PHILOSOPHY Developing a best practice approach to the design process of game-based learning and gamification applications,” 2020. Accessed: Jul. 14, 2024. [Online]. Available: https://pure.coventry.ac.uk/ws/portalfiles/portal/38534699/Clarke_Pure.pdf