Borneo International Journal eISSN 2636-9826; Vol. 7 (2); 2024; 12-26
Published by *Majmuah Enterprise*
www.majmuah.com

Security Challenges in SCADA Systems: A Comprehensive Penetration Testing Approach

HELMY HANYFF HAIRUDIN RUZAILI and MOHAMAD FADLI ZOLKIPLI
School of Computing, College of Arts and Sciences, Universiti Utara Malaysia, Sintok, Kedah, Malaysia

Email : hlmyanip86@gmail.com

Received: April 02, 2024
Accepted: May 01, 2024
Online Published: June 04, 2024

Abstract
This paper examines the cybersecurity weaknesses in Supervisory Control and Data Acquisition (SCADA) systems, which play a crucial role in the infrastructure of many industrial sectors. By employing a comprehensive penetration testing framework, the study uncovers significant vulnerabilities like protocol deficiencies, difficulties in integrating with IT networks, and security flaws related to human factors. The article assesses the efficacy of existing security measures and identifies the specific areas that require enhancement. This resource provides a thorough examination of the possible cyber threats that SCADA systems may encounter and evaluates their ability to withstand these threats. Suggestions for strengthening system security involve implementing focused vulnerability patching, enhancing security knowledge among staff, and developing strong defence methods. This work enhances the field of cybersecurity by offering a systematic method for recognising, evaluating, and reducing the dangers linked to SCADA systems. As a result, it aids in protecting vital infrastructure against sophisticated cyber assaults.

Keywords: Supervisory Control and Data Acquisition (SCADA) Systems, IT Network Integration, Cyber Threats

1 Introduction

A SCADA system is an essential element of industrial automation that oversees and regulates operations in diverse sectors such as water distribution, energy, and manufacturing. These systems gather live data from sensors and equipment in distant areas and transmit it to a central control system. This system facilitates effective process management, data analysis, and prompt decision-making to address evolving circumstances or irregularities, ensuring uninterrupted operations and safety in critical infrastructure scenarios. According to (Sonali Priya, 2020), SCADA systems are critical because they support downtime mitigation, efficiency maintenance, data processing for informed decision-making, and communication of system faults. The extensive utilization of SCADA (Supervisory et al.) systems in critical infrastructure sectors underscores the essential requirement for cybersecurity measures in safeguarding vital services from cyber threats. SCADA systems, which enable the monitoring and control of industrial processes, have been increasingly integrated with IT networks, making them more vulnerable to cyberattacks. The importance of security in SCADA environments cannot be overstated, given their role in overseeing water treatment facilities, energy generation and distribution, and other critical utilities. This research aims to methodically identify and assess the inherent vulnerabilities present in SCADA systems. This will be achieved by utilizing sophisticated penetration testing techniques like the Shodan search engine to detect potential security issues. This project aims to provide practical security innovations and effective strategies for strengthening SCADA systems against advanced cyber-attacks. By doing so, it will contribute to enhancing the resilience and dependability of critical infrastructure operations.

2 Literature review

2.1 Overview of SCADA Security Challenges

SCADA security challenges are multifaceted, stemming from their critical role in infrastructure and inherent vulnerabilities. Key issues include outdated systems, lack of encryption, inadequate authentication, and reliance on proprietary protocols. These challenges are compounded by the systems' exposure to network threats due to increased connectivity. According to (Janusz Hajda, Ryszard Jakuszewski, & Ogonowski, 2021) the advent of the 20th century witnessed a second revolution that revolved around the utilisation of electrical energy to generate significant amounts of work. Subsequently, throughout the 1970s, the utilisation of electronics and internet technologies prompted the commencement of the third industrial revolution, leading to automated production. The current implementation of the fourth industrial revolution, commonly referred to as Industry 4.0, is now in progress.

2.2 Risk management

Risk management in SCADA systems is a crucial framework designed to identify, evaluate, and reduce risks related to these vital infrastructures' operational and cybersecurity elements. Significant issues occur due to inherent vulnerabilities, such as old technology, insufficient encryption, and weak authentication systems. According to (Halima Ibrahim Kure, Islam, & Haralambos Mouratidis, 2022) regardless of their size, especially those involved in critical infrastructure, must comprehend the risks involved. This understanding is crucial to implement appropriate measures to ensure overall business continuity and the delivery of key services. In addition, SCADA systems are vulnerable to a range of external threats such as malware, phishing, and advanced cyberattacks, including Advanced Persistent Threats (APTs) and targeted incursions akin to Stuxnet. Internal risks, which encompass unintentional human errors and deliberate harmful activities by personnel, introduce additional complexity to the risk environment. Furthermore, failing to adhere to industry norms and government rules can result in significant legal and financial repercussions, posing compliance concerns. Gaining a comprehensive understanding of these complex hazards is essential to formulating efficient strategies for safeguarding SCADA systems against potential disruptions and guaranteeing the security and dependability of critical infrastructure operations.

2.3 Risk Identification

- System Vulnerabilities: Identify inherent vulnerabilities in SCADA systems, such as outdated hardware and software, lack of encryption, and inadequate authentication mechanisms.
- External Threats: Consider the range of cyber threats, including targeted attacks like Stuxnet, malware, phishing, and Advanced Persistent Threats (APTs).
- Internal Threats: Acknowledge risks posed by insider threats, whether intentional or accidental, due to human error or malicious actions by employees.
- Compliance Risks: Identify potential non-compliance with industry standards and government regulations, which could lead to legal and financial repercussions.

The process of identification underscores the significance of recognising and enumerating the diverse hazards that SCADA systems must confront. According to (Wali, 2022) software attacks have been approached from a distinct perspective, recognising them as vulnerabilities and hazards to cyber security that could have an impact on SCADA systems in terms of patching and human factors. Applying patches to systems, particularly ones that need uninterrupted operation around the clock, might potentially expose previously unknown vulnerabilities or even result in system crashes. Nevertheless, human factors can also give rise to social engineering, which can result in deliberate attacks targeting both internal and external systems, as well as human errors, which can lead to intentional attacks. These encompass insider risks, compliance concerns, and external cyber threats, alongside internal weaknesses. To ensure the security of critical infrastructure and safeguard SCADA systems from disruptions, it is imperative to identify and acknowledge potential threats.

2.4 Risk Assessment

- Threat Analysis: Evaluate the likelihood of different types of cyber-attacks and their potential impact on SCADA systems' integrity and the continuity of critical operations.

- Vulnerability Assessment: Use tools and methodologies to assess the security posture of SCADA systems, identifying and prioritizing vulnerabilities.
- Impact Analysis: Assess the potential consequences of successful attacks on SCADA systems, considering both direct impacts (e.g., operational disruptions) and indirect impacts (e.g., reputational damage).

The process of quantifying and ranking the hazards posed to SCADA systems relies significantly on risk assessment. According to (Yulia Cherdantseva et.al, 2022) for risk assessment and management to be effective, it is necessary to collaboration and communication with a diverse group of professionals from various fields, such as network and hardware engineers, software developers, system operators, Human Resources (HR) administrators, and floor managers (this list is not exhaustive). By evaluating the likelihood and potential ramifications of various cyber threats, organisations can improve their understanding of their security position. This information facilitates the implementation of targeted measures to enhance defences against critical vulnerabilities and potential attack vectors.

2.5 Risk Mitigation Strategies

- Layered Defense Mechanisms: Implement a multi-layered security approach, including firewalls, intrusion detection systems, and encryption, to protect against various attack vectors.
- Regular Updates and Patch Management: Ensure timely application of security patches and updates to mitigate known vulnerabilities.
- Access Control and Authentication: Strengthen access control measures and authentication mechanisms to restrict system access to authorized personnel only.
- Network Segmentation: Segment SCADA networks from corporate networks and the internet to minimize the attack surface and contain potential breaches.
- Employee Training and Awareness: Conduct regular training sessions for employees to recognize potential cyber threats and understand best practices for cybersecurity.

To safeguard a SCADA system, it is necessary to use several risk mitigation strategies, including network segmentation, regular upgrades, layered defence mechanisms, stringent access controls, and personnel training. According to (Ghandi Rouainia, Mounira Rouainia, & Abderrezak Metatla, 2020) applying risk mitigation strategies will enhance emergency response capabilities and facilitate the development of comprehensive maintenance strategies based on long-term predictive risk assessments. These preventive activities are crucial for minimising the attack surface, enhancing system resilience, and ensuring business continuity in the presence of cyber threats.

2.6 Continuous Monitoring and Incident Response

- Real-Time Monitoring: Implement real-time monitoring tools to detect suspicious activities and potential security breaches.
- Incident Response Plan: Develop and regularly update an incident response plan to ensure a coordinated and effective response to security incidents.
- Disaster Recovery and Business Continuity: Establish disaster recovery plans and business continuity strategies to ensure the rapid restoration of SCADA operations in the event of a cyber-attack.

The timely detection and immediate response to security incidents rely on continuous monitoring and a robust incident response system. SCADA systems can mitigate operational downtime and ensure system integrity in the face of cyberattacks by integrating structured incident response plans, disaster recovery plans, and real-time monitoring capabilities. According to (Smith, R et.al, 2021) incident response planning involves creating strategies to address the adverse impacts on critical equipment and operations, regardless of the crisis's origin. ICS operators often have contingency plans in place for power, supply, and output failures. However, the potential impact of cyber-attacks on these plans has only recently started to be considered.

2.7 Regular Reviews and Audits

- Security Audits: Conduct regular security audits to assess the effectiveness of existing security measures and identify areas for improvement.
- Risk Management Policy Updates: Regularly review and update the risk management policy to reflect the evolving threat landscape and incorporate lessons learned from past incidents.

Given the dynamic nature of cyber threats, it is imperative to regularly assess and audit security protocols and risk management principles. To enhance the overall security of SCADA systems, it is crucial to consistently assess and modify security practices. This encompasses the tasks of tackling newly identified risks, rectifying vulnerabilities in security, and using knowledge gained from past incidents. According to (Henriques,J et.al, 2024) Compliance audit frameworks can aid in the detection of misconfigurations. They can be utilised to monitor the security levels of both individual and group account access and generate detailed reports that track security improvements. The compliance auditing process concludes with a report that includes conclusions and other information about fulfilled standards and any instances of non-compliance (if identified). Additionally, it can bring awareness to the hazards and consequences of non-compliance and provide corrective actions to prevent its recurrence.

2.8 Historical Incidents and Case Studies

Notable incidents like the Stuxnet attack highlight SCADA systems' susceptibility to targeted cyber-physical attacks. According to (Mohee, 2022) the Stuxnet virus surreptitiously infiltrates and takes over industrial control systems intending to sabotage normal industrial operations. The malicious computer worm is inserted via a 'hole' in the industrial control system through a removable device such as a USB memory stick. Studies of these incidents reveal that attackers often exploit specific vulnerabilities, such as unpatched software or insecure network configurations, leading to significant operational disruptions.

2.9 Current Security Measures and Gaps

Current security measures for SCADA systems involve layered defenses, including network segmentation, encryption, and intrusion detection systems. According to (T.Goh, 2020) Security awareness training should not be treated as a singular event, but rather as an essential ongoing practice. Goh (2020) argues that safeguarding organisational assets necessitates the following actions: (a) providing training and education to all stakeholders, irrespective of their positions; (b) performing an internal cybersecurity audit to identify knowledge deficiencies across the organisation and track improvement; and (c) mandating cybersecurity training courses for executives and managers in all departments to set a precedent. Every individual has to prioritise security, as seemingly harmless activities can have significant consequences. However, gaps remain, particularly in areas like real-time threat detection and response, legacy system integration, and the human factor in security. The dynamic nature of cyber threats requires ongoing vigilance and adaptation of security strategies.

3 Methodology

The methodology used in this study is a meticulous and systematic approach to penetration testing specifically tailored for the complex and unique environment of SCADA systems. An effective cybersecurity plan necessitates the inclusion of penetration testing, a process that replicates a system attack to assess its vulnerabilities and the efficacy of its safeguards. Protecting SCADA systems from escalating cyber-attacks is imperative due to their crucial function in overseeing and managing critical infrastructure and industrial activities. This section outlines a three-part method designed to address the complex issue of security in SCADA systems. To safeguard the operational integrity of these critical systems, we develop a "Comprehensive Penetration Testing Framework" that adapts classic penetration testing phases to the specific requirements of SCADA environments. The subsequent part, titled "Selection of Test Cases," delves into the systematic approach of identifying and prioritising vulnerabilities, with a focus on those that pose the greatest risk to the reliability and security of the system. The "Tools and Techniques" section provides a concise overview of the specific equipment required for SCADA system penetration testing. This covers both widely used tools often used in the industry, as well as custom-designed solutions specifically tailored to address the unique challenges posed by these systems.

The study aims to enhance the security stance of these critical systems by offering cybersecurity experts a structured plan for conducting thorough, effective, and secure penetration testing in SCADA environments. The technique employed in this study will be delineated to achieve this objective.

3.1 Comprehensive Penetration Testing Framework

This meticulously constructed framework is specifically designed to tackle the unique challenges presented by critical infrastructures such as SCADA systems. The framework is built around a comprehensive comprehension of SCADA architectures, their significance to operations, and the potential consequences of disruptions or unauthorised access. Our technique is extensive and includes a series of well-planned processes that ensure thorough review while maintaining system integrity.

- **Planning Phase:** The penetration testing method starts with precisely defining the scope, objectives, and bounds of the test to have a comprehensive understanding of its breadth and limitations. Operational safety is prioritised, employing practices designed to avoid adverse impacts on physical processes, considering the potential hazards associated with testing active systems. An all-encompassing strategy is made possible by forming a multidisciplinary team consisting of operational personnel, cybersecurity experts, and SCADA engineers. This guarantees that all possible consequences and weaknesses are adequately considered.
- **Reconnaissance Phase:** During the reconnaissance phase, it is crucial to gather intelligence to effectively carry out a successful penetration test. The objective of this phase is to get a comprehensive comprehension of the target SCADA system, encompassing its communication protocols, device connections, and network topology. This covert phase aims to replicate the stealth and tactics of potential assailants, to acquire crucial information without triggering internal security measures.
- **Vulnerability Assessment Phase:** After deeply comprehending the system, attention turns to finding any weaknesses in the SCADA environment. This step combines automated equipment with manual inspection methods to find procedural and technological flaws. The goal is to gather as much data as possible on vulnerabilities that attackers might be able to exploit.
- **Exploitation Phase:** Once vulnerabilities are identified, they are methodically and ethically utilised to assess their exploitability and understand the potential ramifications of a breach. To mitigate any potential harm to the system, this critical procedure is executed meticulously, with the primary objective of evaluating the extent and severity of possible security breaches.
- **Post-Exploitation Phase:** Once vulnerabilities are identified, they are methodically and ethically utilised to assess their exploitability and understand the potential ramifications of a breach. To mitigate any potential harm to the system, this critical procedure is executed meticulously, with the primary objective of evaluating the extent and severity of possible security breaches.
- **Reporting Phase:** The penetration test concludes with a comprehensive report that details the findings, such as identified vulnerabilities, the extent of potential system compromise, and evidence of the test's impact on system functionality. The study also contains prioritised suggestions for enhancing the resilience of the system, mitigating identified risks, and improving response strategies.

This Comprehensive Penetration Testing Framework is designed to be iterative, allowing for the continuous evolution and refinement of penetration testing strategies in response to the ever-changing landscape of cyber threats. According to (Hiter, 2023) employing a well-organized penetration testing framework is crucial for attaining efficient outcomes in security assessments. These frameworks guarantee that testing procedures can be done again and adjusted to fit the changing environment of an organization's infrastructure and its vulnerabilities. These frameworks remove ambiguities in the testing process by offering explicit standards and techniques. This enables a more targeted approach to discovering and resolving security vulnerabilities. This strategic method improves the effectiveness of penetration tests and also supports a more comprehensive vulnerability management plan, optimising resource allocation towards strengthening security measures. It underscores the need for a balanced approach that rigorously assesses system vulnerabilities while ensuring the continuous, safe operation of these critical systems.

3.2 Selection of Test Cases

This section outlines the strategic process of test case selection, emphasizing a risk-based approach tailored to SCADA systems. It focuses on identifying vulnerabilities by assessing system components' criticality and susceptibility to attacks, ensuring the penetration tests are both targeted and effective. The creation of realistic attack scenarios, based on potential threats identified during threat modeling, enhances the testing's relevance and efficacy.

- **Risk Assessment**: Begin by doing a comprehensive examination to identify the critical SCADA system components that are vital to operations and the ones that are most vulnerable to cyberattacks. By establishing priorities, it becomes more feasible to allocate resources towards areas where security breaches could have the most significant impacts.
- **Vulnerability Identification:** It is crucial to carefully identify specific areas of weakness in these fundamental components. This involves assessing possible vulnerabilities, such as software glitches or insecure network setups, that an attacker could take advantage of.
- **Targeted Testing:** Develop penetration tests specifically designed to concentrate on the identified vulnerabilities. This ensures thorough and efficient testing by focusing resources on the most susceptible areas.
- **Realistic Scenarios:** Generate test cases that replicate genuine attack situations by utilising the risks identified during the threat modelling process. This approach ensures that the testing is highly relevant and replicates the strategies and actions of a potential opponent.
- **Relevance and Efficacy:** Aim to enhance the penetration testing process by ensuring that all test cases are directly related to real and practical security challenges faced by SCADA systems, thus improving the overall effectiveness of the security measures being tested.

The selection of test cases inside a SCADA system penetration testing framework is a vital step in guaranteeing precise and effective examinations. This technique significantly enhances the importance and efficiency of testing efforts by emphasising vulnerability identification, realistic attack scenario building, and the utilisation of a risk-based methodology. To ensure the security of SCADA systems against constantly changing cyber-attacks, it is crucial to carefully identify test cases that are based on a comprehensive understanding of system weaknesses and potential threats.

3.3 Tools and Techniques

The "Tools and Techniques" part of this article delves into the precise set of tools required for doing effective SCADA system penetration testing. To provide comprehensive coverage, it is crucial to utilise open-source and commercial solutions that support SCADA-specific protocols such as DNP3 and Modbus. The section emphasises the likely requirement for developing specialised tools to thoroughly assess exclusive or distinctive elements inside these complex networks, as well as the crucial significance of conducting testing on operating systems to prevent disruptions

- **Commercial and Open-Source Tools:** These tools are essential for probing SCADA systems. They range from network scanners to protocol analyzers, specifically tailored or adaptable to SCADA protocols such as Modbus and DNP3, offering a mix of depth and flexibility in testing.
- **Safety in Live Systems Testing:** Emphasizes the critical need for tools and methodologies that ensure tests do not disrupt the operational integrity of live SCADA environments, maintaining system availability and safety.
- **Custom Tool Development:** Highlights the often-required development of bespoke tools to address the unique configurations and proprietary technologies embedded within SCADA systems, ensuring a thorough and tailored security assessment.

Table 1: Tools used for SCADA Pentest

Tools	Technique
Google Dorks	This tool helps with reconnaissance by using sophisticated search queries to locate precise information about target systems that may be unintentionally disclosed online.
SHODAN IO	Serves as a device and system search engine for internet-connected devices, making it possible for testers to identify components of SCADA networks.
Metasploit	An environment for creating and running exploits against a distant target computer, helpful for assessing security holes in systems.
Default Passwords	This method of detecting lax authentication procedures involves trying to gain access using frequently used or factory-set passwords.

- **Google Dorks:** Google Dorks refers to the utilisation of sophisticated search queries on Google to identify potentially susceptible systems or discover exposed sensitive information within targeted systems. By employing skillfully formulated queries, testers might uncover inadvertently exposed data, such as configuration files or vulnerable endpoints, which can provide vital information during the reconnaissance phase.
- **SHODAN IO:** SHODAN operates as an Internet of Things (IoT) search engine, enabling penetration testers to locate internet-connected devices and systems, including SCADA components. Testing enables testers to gather information regarding potential points of access and the security status of a SCADA network by examining devices with specific attributes or vulnerabilities.
- **Metasploit:** Metasploit is a versatile tool used for developing and executing attack code on identified vulnerabilities. The exploitation phase of penetration testing relies on the simulation of real-world assaults to confirm vulnerabilities and assess the potential impact of an exploit on the target system.
- **Default Passwords:** This strategy makes use of well-known default passwords to attempt to gain access to devices or systems; this is a typical security error. It is particularly valuable in identifying devices that were not properly secured after being put into operation, highlighting the importance of implementing robust password regulations and protocols in SCADA systems.

Table 1 shows the “Tools and Techniques" section highlights the crucial importance of utilising a combination of commercial and open-source tools specifically intended for SCADA-specific protocols like Modbus and DNP3 to conduct efficient penetration testing on SCADA systems. According to (Marwan Albahar, Dhoha Alansari, & Anca Jurcut, 2022) penetration testers must ensure that attackers are unable to identify and exploit any vulnerabilities that could lead to the destruction, exploitation, or disclosure of information. This highlights the necessity of creating specialised tools to address the unique characteristics of SCADA networks and the significance of conducting non-disruptive tests on operational systems. The key tools for SCADA penetration testing are emphasised, which include utilising Google Dorks for initial reconnaissance to discover exposed sensitive data, employing SHODAN IO to identify internet-connected SCADA components, utilising Metasploit to exploit known vulnerabilities and utilising default passwords to identify weak authentication mechanisms. These tactics are crucial for doing a comprehensive security assessment while also ensuring the uninterrupted functioning and safety of SCADA installations.

4 Security Challenges Identified

The following section explores the various security vulnerabilities found in SCADA systems, with a focus on the specific risks associated with weaknesses in SCADA protocols, human factors that contribute to security breaches, and the challenges that arise from integrating SCADA systems with standard IT infrastructures. Its objective is to offer a comprehensive comprehension of the security environment that is unique to SCADA systems.

4.1 Selected industries

The state of cybersecurity in many different economic sectors today shows how cybercriminals focus on specific targets. Certain industries like manufacturing, oil and gas, and building automation, appear explicitly targeted because of their operating traits and vulnerabilities rather than being assaulted randomly. The industries have responded proactively, as shown by the higher-than-usual rates of blocked harmful objects. Each industry requires a different defence strategy due to this deliberate targeting.

Table 2: 2022 ICS Cybersecurity Incident in Industry

Industry	Malicious Block Percentage
Building Automation	42.2%
Oil & Gas	39.6%
Manufacturing	33.3%
Engineering & ICS	33.6%
Energy	33.5%
Automotive	32.3%

Table 2 shows the H1 2022 industry-specific figures show that the industrial sector has a highly developed cyber defense strategy. Building Automation has the most significant block rate, which may be related to its higher risk profile and resulting in more robust cyber defenses. According to (Alexander, Belisle, & Steele, 2020) when additional incidents occurred, trends related to the adversaries' attack life cycle targeting ICS emerged. For example, the enemies used information technology (IT) infrastructure to access control systems, their ultimate goal. Every industry has a different relationship with cyber dangers based on how it operates and the viruses it is susceptible to. These percentages represent a complex battlefield where vigilante and sophisticated cybersecurity measures are essential for business operations rather than just a precaution.

- **Human-Related Risks:** Despite advancements in technology, humans remain a significant factor in SCADA system security. Human errors, such as misconfigurations or failure to follow security best practices, can inadvertently expose SCADA systems to cyber threats. Moreover, malicious insiders pose a significant risk, as they may intentionally exploit vulnerabilities or misuse privileged access to compromise system integrity. There is a few of Human Factors and System Vulnerabilities in SCADA Security
- **Human-Related Threats and Insufficient Access Control:** It mentions human-related threats to physical infrastructure, such as theft and damage, and points out the logical perspective of SCADA security threats related to people, such as insufficient access control processes in place to verify user-issued commands This underscores the need for comprehensive security training and awareness programs to ensure that SCADA system operators and personnel adhere to security policies and protocols.
- **Segmented Environment and Differing Mentalities:** The document describes a segmented environment with no clear demarcation between operational duties, leading to incongruences and differing mentalities regarding SCADA systems. It notes that SCADA operators prioritize safety and continuity of the process over the application of IT security technologies, which can lead to vulnerabilities.
- **Interconnectivity and Increased Exposure:** The increased interconnectivity and integration of SCADA systems have amplified network exposure to more access points, compounding the complexity of the environment. This makes older security beliefs, such as the 'air gap' or security through obscurity, obsolete and highlights the need for greater understanding and security measures to mitigate human-related risks

- **Legacy Systems and 'Set and Forget' Mentality:** The document also discusses how legacy systems, often left under patch management with factory standard settings or default passwords, coexist with modern solutions. This 'set and forget' mentality, along with the inability to make changes that could breach contractual obligations or vendor warranty specifications, exposes SCADA systems to manipulation or exploitation

The security vulnerabilities of SCADA systems are complex, involving unique weaknesses in protocols, human mistakes and difficulties arising from interaction with traditional IT frameworks. Industries such as manufacturing, oil and gas and building automation have implemented complex cyber defences in response to being targeted by cybercriminals. According to (Alsharif, Mishra, & Alshehri, 2022) it has been discovered that over 39% of security risks are attributed to human factors, and 95% of successful cyber-attacks are a result of human error, primarily from insider threats. A significant human element problem in cybersecurity is the absence of user consciousness regarding cyber risks. This is because these industries have inherent vulnerabilities in their operations, which is evident from the different rates at which they block hostile activity. The presence of humans greatly exacerbates these risks, as misconfigurations, failure to adhere to security best practices and insider threats all contribute to the vulnerability of the system. In addition, inadequate access control and segregated operational environments worsen security discrepancies. The growing interconnectedness of SCADA and IT networks amplifies vulnerability, making classic security solutions such as air gaps outdated. The risk of cyber intrusions is increased by the use of legacy systems that are maintained with a 'set and forget' approach, as well as obsolete security methods. This situation highlights the urgent requirement for continuous system updates, strict password management, and the use of proactive security techniques to successfully protect SCADA environments.

5 Penetration Testing Results

This section thoroughly examines the results of penetration testing, specifically looking at cases where vulnerabilities were effectively exploited. According to (Ralethe, 2014) as is standard for all SCADA systems and other systems that were not categorized. The results of these trials yielded suggestions for addressing the identified weaknesses, emphasizing the significance of penetration testing in evaluating the effectiveness of current security measures and the ability of SCADA systems to withstand cyber-attacks. The significant findings from the first half of 2022 might be expanded upon by penetration testing results, highlighting the widespread nature of cybersecurity vulnerabilities across industrial control systems worldwide. Draw attention to the trend of fewer harmful object detections, contrasting with the different effects in different areas, suggesting a complex threat landscape. Examine the variety and ubiquity of malware families, the remarkable occurrence of ransomware attacks in particular sectors and the notable presence of spyware and cryptocurrency miners. These indicators point to an increasing problem for cybersecurity defenses. Identifying the threat sources malicious email attachments and the improper use of removable media, for example may highlight the crafty strategies used by adversaries and emphasize the necessity of solid cybersecurity defenses and ongoing monitoring to protect industrial automation systems from potentially dangerous developments.

- **Successful Exploit:** Nowadays, where technology and connection permeate every aspect of our lives, industrial control system's resilience to cyberattacks is a safeguard for vital infrastructures. Vigilant cybersecurity tactics are essential as these systems become more digitalized, increasing the likelihood that cyber attackers may exploit vulnerabilities. According to (Jae-Myeong Lee, Sugwon Hong, 2020) The sophistication and intelligence of cyberattacks directed against Supervisory Control and Data Acquisition (SCADA) systems is increasing. The three security measures currently being considered for SCADA systems are security monitoring, communication message security, and physical/logical network separation. This analysis clarifies the sophisticated nature of cyber threats by thoroughly examining successful exploits. It emphasizes the necessity of ongoing security protocol innovation to protect critical operations from the always-changing cyber risk landscape.

Table 3: Global Statistics Related to SCADA Exploit

Metric	Global Percentage (H1 2022)
ICS Computers with Malicious Blocks	31.8%
Spyware Blocks	8.6%
Ransomware Blocks	0.65%
Malicious Email & Phishing Blocks	7% (14.4% in Building Automation)
Threats from Removable Media	3.5% (10.4% in Oil and Gas)
Network Folder Malware Blocks	0.6% (1.2% in Oil and Gas)
Cryptocurrency Mining Malware Blocks	2.3%
Blocks of Malicious Documents (MS Office + PDF)	5.5%
ICS Computers with Malicious Blocks	31.8%

Table 3 shows the H1 2022 data summary on ICS computer exploits, about one-third of these systems saw hostile activity, with different dangers depending on the industry. The two most important were ransomware and spyware, which affected a tiny but noteworthy proportion of systems. Malicious emails pose a severe risk, particularly in building automation. Network folders and removable media were also identified as vectors, especially in the oil and gas industry. A rise in malicious document detection indicates a surge in sophisticated phishing attempts, whereas a decrease in virus and worm incidences demonstrates that preventive measures are working better.

Table 4: H1 2022 ICS Cyber Threat Detection Statistics

Types	Global Percentage
Malware Blocks on ICS Computers	31.8%
Spyware Blocks on ICS Computers	8.6%
Ransomware Blocks on ICS Computers	0.65%
Malicious Document Blocks (MS Office + PDF)	5.5%

Table 4 shows nearly a third of industrial control systems show a significant engagement with malware defense, as the table indicates that threats are widespread and diverse. While it is less common than other malware, spyware impacts a sizable portion of systems, suggesting that it is specifically designed to target sensitive data. Ransomware poses a severe threat because of its disruptive potential, even if it affects fewer users. Identifying malicious documents indicates a persistent threat from seemingly innocuous routes, requiring extensive security protocols.

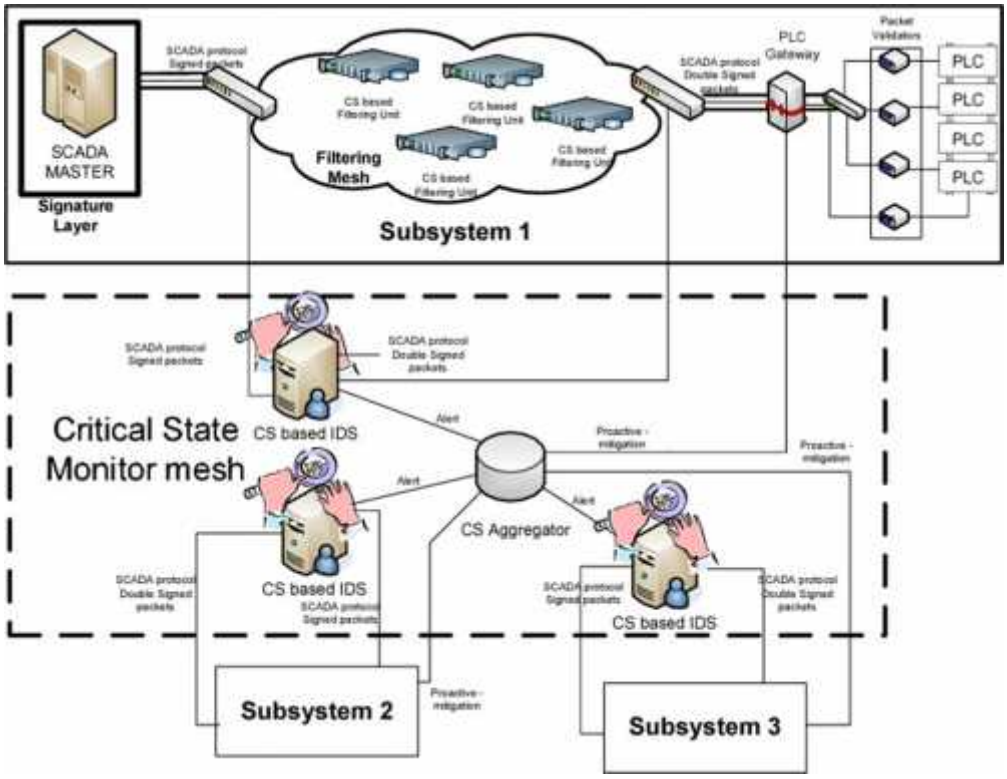
Table 5: Regional ICS Cybersecurity Threat Overview

Types	Global Percentage
Africa	41.5%
Southeast Asia	40.0%
East Asia	38.1%
Central Asia	37.2%
Middle East	36.2%
Latin America	32.4%
South Asia	31.8%
Russia	30.2%
Eastern Europe	28.7%
Southern Europe	27.4%
Australia and New Zealand	23.6%
USA and Canada	18.1%
Western Europe	14.4%
Northern Europe	12.8%

Table 5 shows an examination of H1 2022 data on worldwide ICS cyber threats, the situation is complex, with more than 38% of ICS computers in East Asia, Southeast Asia, and Africa thwarting harmful attempts, suggesting a more significant risk of cyber threats. However, the United States and Canada, Western Europe and Northern Europe have demonstrated lower percentages, potentially due to more robust cyber defences or fewer attacks overall. The year-over-year variations that have been noticed point to different regional trends in threat activity or detection capacities. This calls for a cybersecurity plan that considers local conditions and encourages international collaboration to strengthen the protection of vital infrastructure against the pervasive threat of cyberattacks.

- **Resilience of SCADA Systems:** This evaluation assesses the overall robustness and resilience of SCADA systems in response to security incidents and breaches. It encompasses the system's ability to detect, contain, and recover from cyber-attacks while maintaining operational continuity and ensuring the integrity of critical processes. According to (Germanus, Abdelmajid Khelil, & Suri, 2010) the susceptibility to cyber threats, which can lead to decreased accessibility or compromised data accuracy, presents hazards to public safety. To address these risks, the document proposes improving the dependability and safety of SCADA system operations by implementing Peer-to-Peer (P2P) approaches. P2P networks provide intrinsic resilience features, like path redundancy and data replication, that can enhance the resilience of SCADA systems. These capabilities enable the systems to bypass failed nodes and identify tampered control data.

Figure 1: A K / N Attack-Resilient ICT Shield for SCADA Systems, with State Based Attack Detection



5.1 Features from the perspective of resilience

- **SCADA Master Signature Layer:** This layer indicates that all communication packets within the SCADA protocol are signed, likely to ensure data integrity and authenticity. This helps protect against data tampering and spoofing attacks, ensuring that only verified commands and data are processed.
- **Filtering Mesh for Subsystem 1:** This mesh consists of units that use cryptographic signatures (CS) for filtering. This suggests an added layer of security where only messages with valid signatures are allowed through, which is crucial for preventing unauthorized commands from reaching critical control systems.

- **PLC Packet Validators:** Programmable Logic Controllers (PLCs) are equipped with packet validators, implying that each PLC checks the signature of incoming packets. This step is essential to ensure that even if a malicious packet bypasses previous security layers, it won't be executed at the PLC level.
- **Critical State Monitor Mesh:** This mesh includes IDS (Intrusion Detection Systems) that are signature-based, monitoring the network for any signs of intrusion. Upon detecting a potential threat, these systems can send out alerts for proactive mitigation. This is crucial for a quick response to threats and maintaining system availability.
- **CS Aggregator:** The aggregator appears to coordinate alerts and information from various IDS units, which could allow for a centralized view of security threats across different subsystems. This would enable a rapid and coordinated response to incidents, enhancing the overall resilience of the system.
- **Proactive Mitigation:** The presence of proactive mitigation measures at different points suggests that the system can not only detect threats but also take pre-emptive action to counteract potential attacks, minimizing downtime and ensuring continuity of operations.
- **Subsystem Segmentation:** The system appears to be segmented into at least three subsystems, each with its own security measures. This segmentation is a key resilience strategy, as it prevents a breach in one part of the system from easily spreading to others.

By examining the system's response to simulated threats during penetration testing, cybersecurity professionals can gauge its effectiveness in mitigating the impact of security breaches and minimizing disruptions to essential services. This analysis helps organizations identify strengths and weaknesses in their incident response capabilities, informing strategic improvements to enhance the resilience of SCADA systems against evolving cyber threats. The outcomes of penetration testing offer vital insights into the weaknesses and resilience of SCADA systems against cyber threats. According to (Fovino et.al, 2017) successful utilisation of system vulnerabilities during these tests highlights the significance of continuous security assessments and the implementation of robust protection mechanisms. Examining effective vulnerabilities enables cybersecurity professionals to focus and customise repair actions, thereby enhancing the protection of vital infrastructure. Moreover, evaluating the resilience of SCADA systems when confronted with simulated attacks offers a valuable understanding of their capacity to maintain operational integrity and rebound from security breaches. This study provides a basis for enhancing incident response methods and improving the overall resilience of SCADA systems, ensuring the uninterrupted and dependable provision of key services in the presence of cyber challenges.

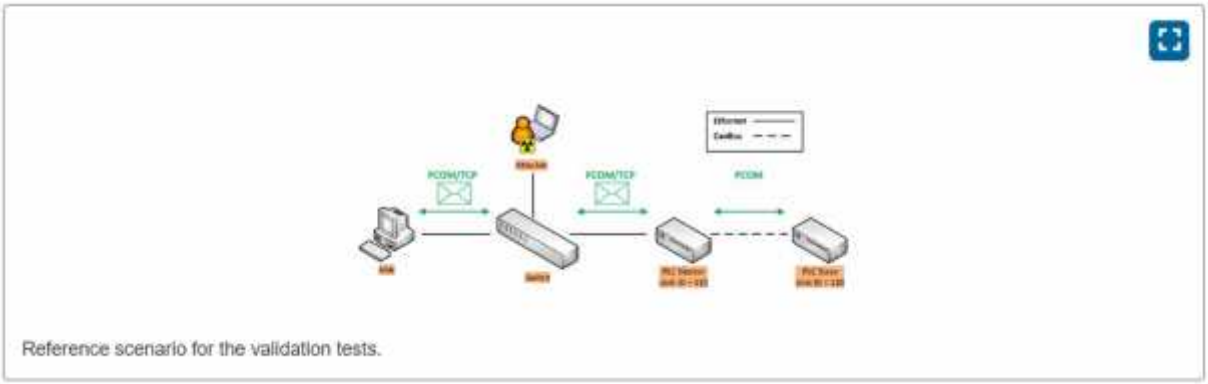
6 Mitigation Strategies

This part outlines strategic recommendations and actionable steps to address and remediate vulnerabilities identified during the penetration testing process. Emphasis is placed on developing robust patching strategies to fortify system defenses and initiatives aimed at enhancing the security awareness and preparedness of personnel involved in the operation and maintenance of SCADA systems.

- **Recommendations for Vulnerability Patching:** This aspect entails providing specific and actionable recommendations for patching and remediation to address the vulnerabilities identified during the penetration testing process. These recommendations are tailored to the unique characteristics and requirements of SCADA systems, aiming to bolster their security posture and resilience against cyber threats. Recommendations may include prioritizing critical patches, establishing patch management processes, and implementing timely updates to mitigate known vulnerabilities effectively. By adopting a proactive approach to vulnerability patching, organizations can minimize the risk of exploitation and enhance the overall security of their SCADA environments.
- **Enhancing Security Awareness:** This component focuses on developing initiatives and programs aimed at elevating security awareness among SCADA system operators and associated personnel. These initiatives seek to cultivate a culture of security consciousness and vigilance, empowering individuals to recognize and respond effectively to potential security threats. Strategies for enhancing security awareness may include conducting regular training sessions, disseminating educational materials on cybersecurity best practices, and

fostering open communication channels for reporting security incidents and concerns. By investing in security awareness initiatives, organizations can strengthen their human defences and create a more resilient security posture against evolving cyber threats.

Figure 2: Analysis of Possible Mitigation Strategies



According to (Rosa et.al, 2017) employing firewalls or network intrusion detection systems (NIDS) is a potential method to prevent, identify, or alert against such attacks. However, such systems need to possess the capability of performing Deep Packet Inspection (DPI) to gain insight into the activities occurring on the network. For instance, one may be given read-only privileges, whereas write-only and administrative privileges may be limited and documented. Repositories like as have compilations of Snort rules for many SCADA protocols including Modbus, DNP3 and S7. These rules can be employed to discern various operations, such as network queries and endeavours to reprogram Modicon PLCs. These rules correlate predetermined values (the protocol signatures) with particular sections of the TCP payload (based on the offset and depth Snort keywords). It is crucial to design mitigation measures based on the findings of penetration testing to address the vulnerabilities identified in SCADA systems. A proactive defence posture is built upon the foundation of targeted vulnerability patching and enhanced security understanding among staff. The purpose of tailored patching recommendations is to enhance system defences by mitigating the risk posed by known vulnerabilities and preventing potential exploitation. Simultaneously, it is crucial to implement measures that enhance the understanding and readiness of SCADA system operators and related personnel to foster a vigilant and proactive security mindset. Together, these strategies emphasise the importance of taking a comprehensive approach to cybersecurity, integrating technical solutions with human elements to establish a strong and durable defence against the various threats to SCADA systems.

7 Discussion

Industrial control systems (ICS) are essential for managing critical infrastructures in various industries in today's networked environment. However, as these systems become more digital, there is a greater chance that cyberattacks targeting Supervisory Control and Data Acquisition (SCADA) systems may occur. The increasing sophistication of cyberattacks targeting SCADA systems presents a severe risk to vital operations. Cybersecurity methods like physical/logical network separation, communication message security and security monitoring are being examined to improve the resilience of ICS against cyber threats in response to these growing challenges.

Table 6: Comparison of Global and Regional ICS Cybersecurity Threats

Metric	Global Percentage (H1 2022)	Regional Percentage
CS Computers with Malicious Blocks	31.8%	Africa: 41.5%
Spyware Blocks	8.6%	Southeast Asia: 40.0%
Ransomware Blocks	0.65%	East Asia: 38.1%
Malicious Email & Phishing Blocks	7% (14.4% in Building Automation)	Central Asia: 37.2%
Threats from Removable Media	3.5% (10.4% in Oil and Gas)	Middle East: 36.2%

Network Folder Malware Blocks	0.6% (1.2% in Oil and Gas)	Latin America: 32.4%
Cryptocurrency Mining Malware Blocks	2.3%	South Asia: 31.8%
Blocks of Malicious Documents (MS Office + PDF)	5.5%	Russia: 30.2%
Malware Blocks on ICS Computers	31.8%	Eastern Europe: 28.7%
Spyware Blocks on ICS Computers	8.6%	Southern Europe: 27.4%
Ransomware Blocks on ICS Computers	0.65%	Australia and New Zealand: 23.6%
Malicious Document Blocks (MS Office + PDF)	5.5%	USA and Canada: 18.1%

Table 6 shows global data for the first half of 2022 shows an alarming trend in cyberattacks against industrial control systems (ICS), especially SCADA (Supervisory Control and Data Acquisition) systems. Malicious blocks affected around one-third of ICS PCs globally; 8.6% of systems were affected by malware, and 0.65% by ransomware. Mainly when establishing automation, phishing and fraudulent emails were a serious concern. Moreover, network folder malware and removable media threats were common, especially in the oil and gas sector. According to (Yaman Roumani, 2020) since zero-day attacks continue to affect businesses, the results highlight several important issues. Organizations must first improve the order in which they prioritize patch development. For instance, enterprise software vendors ought to be more watchful when it comes to patching delivery delays than for other kinds of software. Furthermore, considering vulnerability type, the data might help decision-making as organizations rank which zero vulnerabilities need immediate attention. Regionally, ICS cyber risks were found in much higher percentages in Africa, Southeast Asia, and East Asia. This emphasises how much more likely cyberattacks are in these areas. Conversely, lower percentages were seen in the USA, Canada, Western Europe, and Northern Europe, which may indicate better cyber defences or fewer attacks. However, the year-over-year variations show how dynamic regional threat landscapes are, underscoring the need for international cooperation and customised cybersecurity strategies to effectively reduce cyber risks and protect vital infrastructure from potential threats.

8 Conclusion

Strong security measures are necessary for vital infrastructure, as the paper thoroughly examines cybersecurity flaws in SCADA systems. It discusses the difficulties with human factors, SCADA integration with IT networks, and protocol weaknesses. Identifying and addressing these vulnerabilities, along with proposing fixes like patching vulnerabilities and raising security awareness, are done using a thorough penetration testing framework that is given. To ensure the safe functioning of vital services, the objective is to increase the resilience of SCADA systems against cyber threats.

Acknowledgement

The authors would like to thank all members of the School of Computing who participated in this study. This study was carried out as part of the Hacking and Penetration Testing Project. This work was supported by Universiti Utara Malaysia

Reference

Sonali Priya. (2020, July 29). What is SCADA Systems? Retrieved April 2, 2024, from Schneider Electric Blog website: https://blog.se.com/industry/machine-and-process-management/2020/07/29/what-is-scada-systems.

Janusz Hajda, Ryszard Jakuszewski, & Ogonowski, S. (2021). Security Challenges in Industry 4.0 PLC Systems. *Applied Sciences (Basel)*, *11*(21), 9785–9785. https://doi.org/10.3390/app11219785.

Halima Ibrahim Kure, Islam, S., & Haralambos Mouratidis. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing & Applications (Print)*, *34*(18), 15241–15271. https://doi.org/10.1007/s00521-022-06959-2.

Wali, A. M. (2022, July 14). Analysis of Security Challenges in Cloud-Based SCADA Systems: A Survey. Retrieved April 2, 2024, from ResearchGate website: https://www.researchgate.net/publication/367605287_Analysis_of_Security_Challenges_in_Cloud-Based_SCADA_Systems_A_Survey.

Yulia Cherdantseva, Burnap, P., Simin Nadjm-Tehrani, & Jones, K. (2022). A Configurable Dependency Model of a SCADA System for Goal-Oriented Risk Assessment. *Applied Sciences (Basel)*, *12*(10), 4880–4880. https://doi.org/10.3390/app12104880.

Ghandi Rouainia, Mounira Rouainia, & Abderrezak Metatla. (2020). Over Pressure Risk Mitigation with SCADA in a Natural Gas Distribution System. *Universal Journal of Mechanical Engineering*, *8*(1), 21–28. https://doi.org/10.13189/ujme.2020.080103.

Smith, R., Janicke, H., He, Y., Ferra, F., & Albakri, A. (2021). The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework. *Computers & Security*, *109*, 102398–102398. https://doi.org/10.1016/j.cose.2021.102398.

Henriques, J., Caldeira, F., Cruz, T., & Paulo Simões. (2024). A Survey on Forensics and Compliance Auditing for Critical Infrastructure Protection. *IEEE Access*, 1–1. https://doi.org/10.1109/access.2023.3348552.

Mohee, A. (2022, March). A Realistic Analysis of the Stuxnet Cyber-attack. Retrieved April 2, 2024, from ResearchGate website: https://www.researchgate.net/publication/359125549_A_Realistic_Analysis_of_the_Stuxnet_Cyber-attack.

Goh, T., & Bailey, M. P. (2020). Making cybersecurity training a priority. Chemical Engineering, 127(2), 32-37.

Hiter, S. (2023, July 5). What Is a Pentest Framework? Top 7 Frameworks Explained. Retrieved April 2, 2024, from eSecurity Planet website: https://www.esecurityplanet.com/networks/pentest-framework.

Marwan Albahar, Dhoha Alansari, & Anca Jurcut. (2022). An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities. *Electronics*, *11*(19), 2991–2991. https://doi.org/10.3390/electronics11192991.

Alexander, O., Belisle, M., & Steele, J. (2020). *MITRE ATT&CK ® for Industrial Control Systems: Design and Philosophy McLean, VA*. Retrieved from https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf.

Alsharif, M., Mishra, S., & Alshehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering*, *40*(3), 1153–1166. https://doi.org/10.32604/csse.2022.019938.

Ralethe, S. (2014). *Investigating Common SCADA Security Vulnerabilities Using Penetration Testing CORE Metadata, citation and similar papers at core.ac.uk Provided by Wits Institutional Repository on DSPACE*. Retrieved from https://core.ac.uk/download/pdf/39676184.pdf.

Jae-Myeong Lee & Sugwon Hong (2020). Keeping Host Sanity for Security of the SCADA Systems.Retrieved March 5, 2024, from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9046797.

Germanus, D., Abdelmajid Khelil, & Suri, N. (2010). Increasing the Resilience of Critical SCADA Systems Using Peer-to-Peer Overlays. *Lecture Notes in Computer Science*, 161–178. https://doi.org/10.1007/978-3-642-13556-9_10.

Fovino, I. N., Carcano, A., Guglielmi, M., & M. Masera. (2017). A K / N Attack-Resilient ICT Shield for SCADA Systems , with State Based Attack Detection. Retrieved April 2, 2024, from https://www.semanticscholar.org/paper/A-K-N-Attack-Resilient-ICT-Shield-for-SCADA-Systems-Fovino-Carcano/b7d50645a80bcea44bd12c3ae3f64503f12e647f.

Rosa, L., Borges, M., Mazo, S., Monteiro, E., Cruz, T., & Paulo Simões. (2019). A Comprehensive Security Analysis of a SCADA Protocol: From OSINT to Mitigation. *IEEE Access*, *7*, 42156–42168. https://doi.org/10.1109/access.2019.2906926.

Yaman Roumani. (2021). Patching zero-day vulnerabilities: an empirical analysis. *Journal of Cybersecurity (Oxford)*, *7*(1). https://doi.org/10.1093/cybsec/tyab023.