Security Onion as a Network Auditing Tool at the San Cristóbal de Huamanga National University

Kimberlly Nena Barraza Tudela[1], Hubner Janampa Patilla[2]
San Cristóbal De Huamanga National University, Ayacucho, Perú[1]
Information Technology Office, San Cristóbal De Huamanga National University, Ayacucho, Perú[2]

***Abstract*—In a context of evolving cyber threats, the San Cristobal de Huamanga National University (UNSCH) faces the need to improve its network security infrastructure. This study implements Security Onion as a network auditing tool at this institution with the objective of evaluating its effectiveness in three key areas: security monitoring, log management, and intrusion detection. The study employs an applied, descriptive, and experimental approach to demonstrate that Security Onion is a robust solution for incident detection. It enables comprehensive analysis of network logs and early identification of suspicious activities, providing a holistic view of the network. Based on the results, the study suggests best practices for protecting institutional information and the network, and contributes to understanding Security Onion's capabilities in similar network infrastructures. Furthermore, it provides a replicable model for other institutions.**

***Keywords*—Network security; network auditing; Security Onion; IDS; CIS Controls**

I. Introduction

During the course of 2023, a significant increase in cyber threats was recorded globally, with organizations across all sectors facing unprecedented challenges in protecting their digital assets [25]. According to the IBM Cost of a Data Breach Report 2024, the average cost of a data breach reached an all-time high of $4.88 million, underscoring the financial and operational impact of these incidents [36]. Although ransomware incidents decreased, other threats, such as the misuse of valid credentials and data theft, rose considerably, highlighting the evolving nature of cyber risks [35]. The exploitation of vulnerabilities in web applications due to poor security configurations and the spread of malicious information-stealing programs (infostealers) also reflect a concerning trend in the exploitation of sensitive data [9].

This threat landscape has not spared Latin America, a region increasingly targeted by cybercriminals due to its growing digitalization and limited investment in cybersecurity infrastructure. It is estimated that 27% of organizations in the region fell victim to multipurpose malware in 2023, with prevalent threats such as FakeUpdates and Qbot [53]. Additionally, trojans and phishing attacks have tripled compared to previous years, further exacerbating the region's cybersecurity challenges [55]. Peru, in particular, has faced a surge in cyberattacks targeting both citizens and institutions, exposing confidential information and undermining trust in digital systems [24] [56].

Educational institutions, including universities, have become prime targets due to their open network environments, vast amounts of sensitive data, and often limited cybersecurity resources. San Cristóbal de Huamanga National University (UNSCH) is no exception. Although the university campus has not suffered ransomware attacks, its administrative headquarters fell victim to such an incident in 2022, affecting critical systems like SIGA and SIAF and causing significant disruptions to administrative processes. This event underscored the urgent need to strengthen the institution's cybersecurity posture through proactive measures, including advanced threat detection and response capabilities.

In this context, network auditing emerges as a fundamental mechanism to assess and enhance the security of technological infrastructure. Security Onion, an open-source platform, offers a comprehensive solution for this purpose, combining advanced security monitoring, log management [47], and intrusion detection systems. Its implementation enables real-time monitoring of security events, facilitating swift responses to anomalies and potential attacks [26] [33] [43]. Moreover, its scalability and cost-effectiveness make it an ideal choice for institutions like UNSCH, which often operate with limited budgets [28] [32].

The objective of this study is to implement Security Onion as a network auditing tool at UNSCH, evaluating its effectiveness in threat detection and its potential to improve the institution's cybersecurity framework. By doing so, this research aims not only to strengthen UNSCH's resilience against cyber threats but also to provide a replicable model for other educational institutions facing similar challenges. In an era where cyberattacks are becoming increasingly sophisticated, proactive measures like network auditing are essential to safeguarding sensitive data and ensuring operational continuity.

II. Theoretical Basics

A. Security Onion

Security Onion is an intrusion detection-oriented platform based on the Ubuntu distribution that comprises a multitude of IDSs, including host-based (HIDS) and network-based (NIDS) variants [17] [30] [48], in addition to other tools for logging, management, and visualization of data [21] [22] [23] [27] [41] [51] [57] [59] [65] [68] [70]. The configuration of the system can be implemented on a master server with multiple nodes or as a standalone or hybrid deployment, thereby demonstrating its remarkable adaptability.

The primary deployment types are categorised as follows: Import, Evaluation, Standalone, and Distributed [61], as shown in Table I and illustrated in Fig. 1 and Fig. 2.

TABLE I. SECURITY ONION DEPLOYMENT TYPES AND THEIR MINIMUM REQUIREMENTS

Type of deployment	Minimum requirements			
	N° of cores	*RAM*	*Storage (SSD preferred)*	*N° of network interfaces*
Import	2	4GB	50GB	1
Evaluation	4	8GB	200GB	2
Independent	4	16GB	200GB	2
Distributed*	2-8	4-16GB	12-200GB	1-2

*The minimum requirements of the distributed deployment type vary according to the subtype, since there is a master node and the others are remote nodes with different functionality.

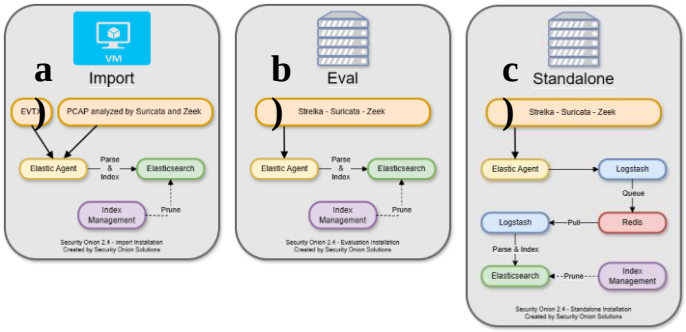

Fig. 1. Security Onion deployment types (a) Import, (b) Evaluation, (c) Standalone.

B. Network Auditing

Auditing is not merely the deployment of a multitude of hacking tools with the objective of breaching network security. The term "audit" itself denotes a process of collecting, examining, and evaluating network data to assess its status [49] [50]. This enables organizations to determine the effectiveness of their network monitoring and management operations, particularly in terms of compliance with internal and external standards.

1) Computer network: It is defined as a set of wired and wireless communication links through which various hardware and software components exchange data and information [3] [20] [62].

2) Network security: Network security: The field of network security encompasses the design of protocols and the establishment of best practices with the objective of safeguarding data within computer networks. The overarching objective is to establish a secure environment that safeguards the network, its components, stored and transmitted data, and its users [4] [38]. It is imperative to acknowledge that security should be regarded as a continuous process, rather than a standalone solution [37] [60]. Security can be conceptualized in two distinct states: physical and theoretical. In the physical domain, security is achieved through the implementation of barriers, the designation of secure areas, and the resistance of intruders. Conversely, the theoretical state of security, also referred to as security through obscurity, is predicated on the fallacious assumption that secrecy can provide absolute security. This approach is predicated on the assumption that, as long as an object remains unknown to those outside a core group, it is inherently secure [35]. However, this perspective is often regarded as a flawed philosophy.

a) Network security attacks: A campus network, such as that of the UNSCH, is vulnerable to a wide range of network attacks. Chakraborty et al. (2020) define network security attacks as illicit activities perpetrated by unauthorized actors against private, corporate, or governmental computing assets with the goal of destroying, modifying, or stealing sensitive data [8]. To provide a more illustrative example, please refer to Table II, which presents the types of attacks and some respective examples.

b) Malware: This software is designed to disrupt the operation of computers, collect sensitive information, and gain access to private computer systems [18]. It is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software that spreads in various ways to create havoc and steal sensitive information.

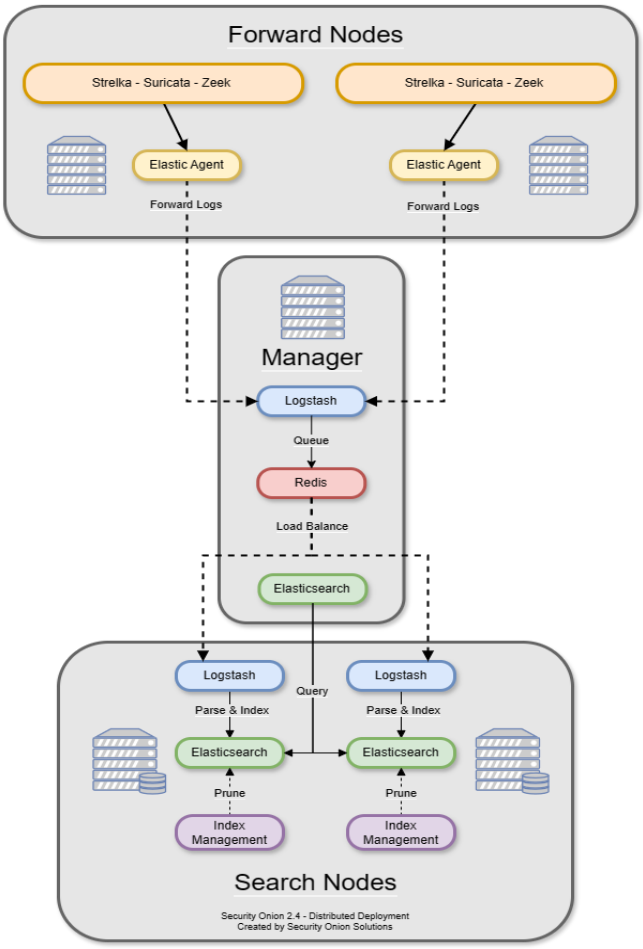

Fig. 2. Distributed deployment type.

TABLE II. CLASSIFICATION OF NETWORK SECURITY ATTACKS

Types of attack	Description	Examples
Passive attack	The primary objective of such attacks is to surreptitiously procure sensitive information, often with the aid of sophisticated malware. These attacks are challenging to detect and therefore pose a significant challenge to network protection [39].	Traffic analysis. Monitoring. Spying.
Active attack	These systems are engineered to alert users to potential security breaches. Consequently, the victim is able to disrupt communication with the other party [67].	Modification. Wormhole attack. Fabrication. Impersonation. Denial of service. Sinkhole (service attack). Sibyl.
Advanced attack	This is defined as an attack in which an unauthorized user gains access to a network and remains on it for an extended period without being detected. These incursions pose a heightened risk to corporate entities, as external actors gain persistent access to their confidential information [58].	Black hole attack. Rushing attack. Replay attack. Byzantine attack. Location disclosure attack. Man-in-the-middle attack (Man-in-the-middle attack).

III. METHODOLOGY

A. Type, Level and Design of the Research

This research is classified as applied, given its objective to generate new knowledge applicable to addressing practical problems [52]. It builds on previous theoretical contributions and employs appropriate methodologies to achieve the proposed objectives [5] [46]. The research is descriptive in nature, aiming to provide an accurate description of the implementation and results obtained [6] [45] by Security Onion. Regarding the research design, a non-experimental and cross-sectional approach was selected. The cross-sectional design, in contrast to experimental research, permits the observation of behaviors or variables of interest in a natural context and at a specific time [14] [31] [44]. Consequently, the research can be characterized as cross-sectional, non-experimental, and descriptive.

B. CIS Controls

The Center for Internet Security, Inc. (CIS) defines CIS Controls as a set of best practices designed to protect organisations from the most common attacks and real threats [7]. As the name suggests, these controls are designed to identify the most critical points that require protection in order to prevent the most significant attacks. The latest version, CIS Controls v8.1, comprises 18 controls and 153 safeguards, which are distributed across three implementation groups (IGs). These IG groups are tailored to the cybersecurity maturity level of organisations, as illustrated in Fig. 3 and Table III.

In this research project, network auditing has been aligned with the CIS Controls version 8 due to their practical and accessible approach. Unlike standards such as ISO 27001 and COBIT, which require a more exhaustive and complex framework, the CIS Controls provide precise guidance based on real-world threats and a detailed analysis of security incidents. For example, CIS Control 13: Network Monitoring and Defense is critical for UNSCH, as it enables the detection and response to malicious activities in real time. Security Onion, with its advanced network traffic monitoring and intrusion detection capabilities, aligns perfectly with this control, facilitating the identification of anomalies and the mitigation of threats before they escalate.

Similarly, CIS Control 07: Continuous Vulnerability Management plays a vital role in protecting the university's technological infrastructure. This control emphasizes the importance of proactively identifying, prioritizing, and remediating vulnerabilities.

Furthermore, the CIS Controls are organized into three implementation groups (IGs), enabling organizations to select the maturity level most appropriate for their context. In the case of UNSCH, the IG2 profile was determined to be the most suitable, given that the university has specialized IT personnel but faces challenges in protecting sensitive information and managing risks associated with operational disruptions.

TABLE III. IMPLEMENTATION GROUPS (IG'S)

Denomination	Characteristics
IG1 (Small to medium-sized organizations)	Organizations with limited IT and cybersecurity expertise. Their primary concern is maintaining business operations, as they have low tolerance for downtime. The sensitivity of the information they protect is low, primarily including employee data and financial information.
IG2 (Medium to large organizations)	They employ specialized IT and cybersecurity personnel. They store sensitive customer and business process information and can withstand brief service interruptions. Their main concern is the loss of public trust in the event of a breach.
IG3 (Organizations with high cybersecurity maturity)	They employ security experts specializing in areas such as risk management, penetration testing, and application security. Their assets contain highly sensitive information subject to regulatory oversight. The materialization of attacks can cause significant harm to public well-being.

Fig. 3. CIS Controls version 8.1.

C. Security Tool

In the domain of network monitoring and intrusion detection, there exists a plethora of widely utilised tools, each exhibiting distinct strengths and limitations. The ensuing discourse aims to provide a comparative analysis of Suricata, Snort, Zeek (Bro IDS) and Security Onion, with the objective of substantiating the selection of Security Onion for network auditing at the San Cristóbal de Huamanga National University.

1) Suricata: Suricata is a high-performance intrusion detection and prevention system (IDS/IPS) known for its ability to analyze network traffic in real time using signature-based rules and anomaly detection. It is particularly efficient in handling high volumes of traffic and supports modern protocols.

a) Advantages:

- High performance in environments with heavy traffic.
- Support for deep packet inspection (DPI).
- Compatibility with Snort rules, facilitating migration.

b) Disadvantages:

- Requires manual configuration and rule management.
- Lacks an integrated graphical interface, which can complicate its use for non-specialized teams.

2) Snort: Snort is one of the oldest and most widely used intrusion detection systems. Rule-based and highly customizable, it is effective at detecting known threats. However, its traditional approach makes it less suitable for detecting advanced or unknown threats.

a) Advantages:

- Large user community and extensive availability of rules.
- Lightweight and easy to deploy in small environments.

b) Disadvantages:

- Limited in detecting advanced threats (e.g., zero-day attacks).
- Requires manual rule management and configuration.

3) Zeek (Bro IDS): Zeek (formerly known as Bro IDS) is a network traffic analysis tool focused on generating detailed logs and forensic analysis. Unlike Suricata and Snort, Zeek does not rely on signature-based rules but instead uses customizable scripts to analyze network behavior.

a) Advantages:

- Generates detailed, context-rich logs, ideal for forensic analysis.
- Highly customizable through scripts.

b) Disadvantages:

- Requires a high level of expertise for configuration and use.
- Not a real-time detection system on its own but rather a tool for post-incident analysis.

4) Security onion: Security Onion is a comprehensive security monitoring platform that integrates multiple open-source tools, including Suricata, Zeek, Wazuh, and Elastic Stack.

a) Advantages:

- Integration of multiple tools into a single platform.
- User-friendly and centralized graphical interface.
- Advanced event correlation and data visualization capabilities.
- Scalable and adaptable to environments of varying sizes.

b) Disadvantages:

- Requires moderate hardware resources due to its comprehensive nature.
- Initial learning curve for advanced configurations.

The selection of Security Onion for network auditing at UNSCH is based on its ability to integrate the functionalities of tools like Suricata, Zeek, and Wazuh into a single platform, simplifying management and reducing operational complexity. Unlike Suricata and Snort, which require manual configuration and rule management, Security Onion provides a centralized graphical interface that facilitates the monitoring and analysis

of security events, even for teams with limited cybersecurity expertise.

Furthermore, Security Onion offers advanced event correlation and data visualization capabilities through Elastic Stack, enabling faster and more effective incident response [12]. This is particularly important for UNSCH, where early threat detection and the protection of sensitive information are key priorities. While Zeek provides detailed forensic analysis, its complexity and lack of real-time detection capabilities make it less suitable for a comprehensive implementation in an institution with limited resources.

IV. Results

A. Description of the Existing Network on the University Campus

1) Network topology: The local area network (LAN) of the university campus employs a structured cabling configuration with a star topology, wherein the main node is the OTI office (formerly CTI) and the remote nodes are distributed among the faculties and laboratories of the different schools [11], as illustrated in Fig. 4.

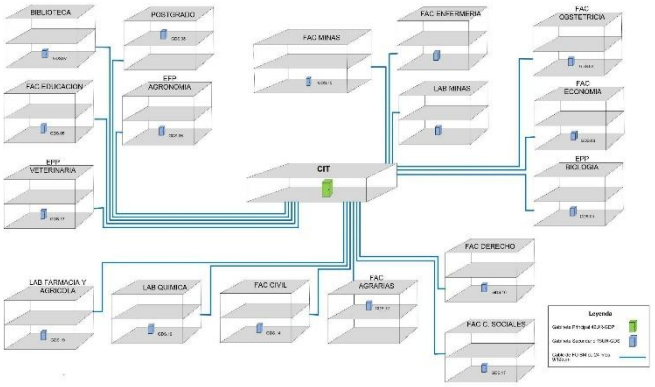

Fig. 4. Network topology on the university campus.

2) Perimeter security system: The perimeter security system is composed of a Checkpoint firewall that is integrated into the network through the connection to the Cisco core switch [11] and to the Internet provider's equipment.

B. Audit Methodology with Security Onion

1) Security onion installation and configuration: Security Onion installation is divided into two main stages [69]. The initial stage covers the preliminary steps of installing from a bootable USB stick. These steps adhere to the standard procedures outlined in the official Security Onion documentation. Once the initial stage of the installation is complete, the system will prompt for a reboot. It is imperative to remove the bootable USB memory stick before rebooting the computer to avoid restarting the installation process from the removable media. Security Onion will be configured according to the needs of each organization or available resources.

It is imperative to note that the deployment of Security Onion necessitates the presence of two network interfaces on the equipment. The primary interface facilitates access to the web console, whereas the secondary interface is responsible for traffic collection from the SPAN port of the switch, as illustrated in Fig. 5. Furthermore, it is imperative to emphasise that an IP address or a network segment from which the system can be accessed must be authorised for access to the web console, see Fig. 6.

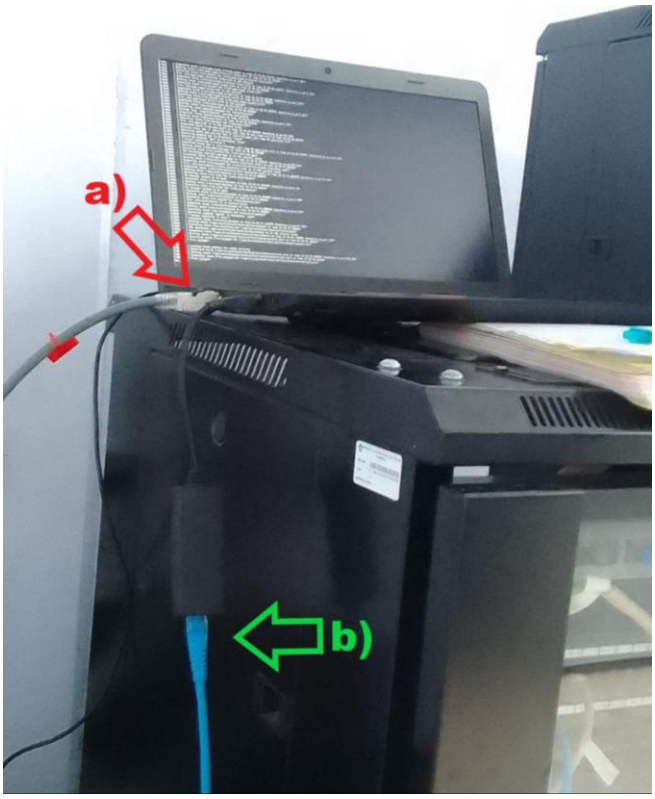

Fig. 5. The Computer on which Security Onion is installed must be connected to the network via a (a) Network cable that is connected to the SPAN port of the switch. In addition, (b) The network interface through which the Security Onion web console will obtain an IP must be determined.

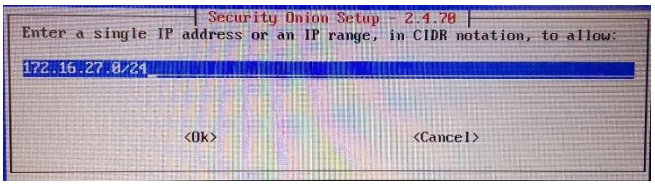

Fig. 6. Authorized network for Security Onion web console login.

2) Node verification: In order to ensure proper network monitoring, it is necessary to verify the status of the node. This process entails entering the IP address of the Security Onion web console from the web browser of an external device connected to the authorized network. Subsequently, the configured credentials are entered. Upon successful authentication, the welcome interface is displayed, presenting the user with a left-side menu comprising several options. The "Grid" option is selected to view the node status and the services that are currently operational. This facilitates the user's ability to verify the successful deployment of the system, as illustrated in Fig. 7.

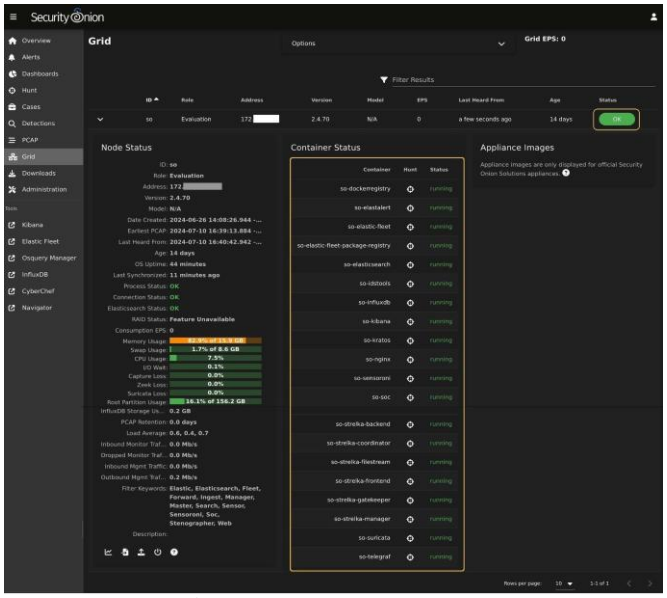

Fig. 7. Status of the Security Onion node that has been deployed.

3) Detections in the network using security onion: In order to access the logs of Security Onion detections, it is necessary to click on the "Detections" option, which is located in the left menu of the interface. This will display data such as name, severity, date, type, and other relevant information regarding the detections made in a specific time period, as illustrated in Fig. 8.

It is important to note that Security Onion has only one set of rules enabled by default. To obtain a comprehensive overview, it is necessary to activate the remaining rules (Fig. 9), or at least those that are relevant to the university campus network. Subsequent to this activation, the interface will consequently display the new records, as illustrated in Fig. 10.

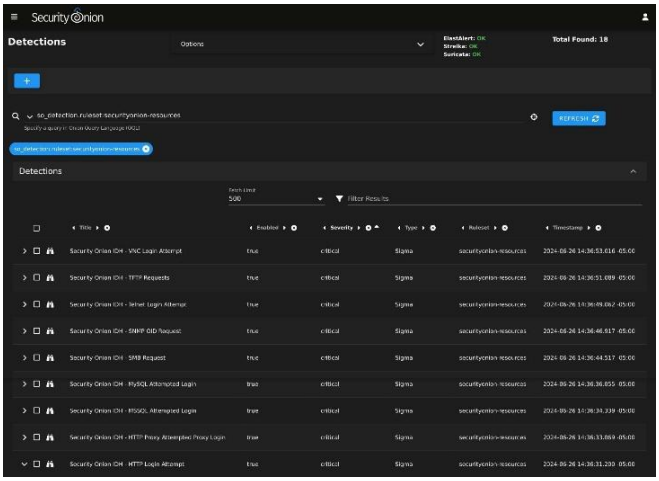

Fig. 8. Network detections according to security onion monitoring.

C. Integration and Documentation of Results

1) Documentation of findings: Over the course of approximately three weeks, Security Onion obtained a total of 500 logs from a segment of the university campus network. Of these logs, 485 were classified as informative, while the remaining 15 were categorized as critical and high severity. Fig. 11 shows the detections along with brief descriptions.

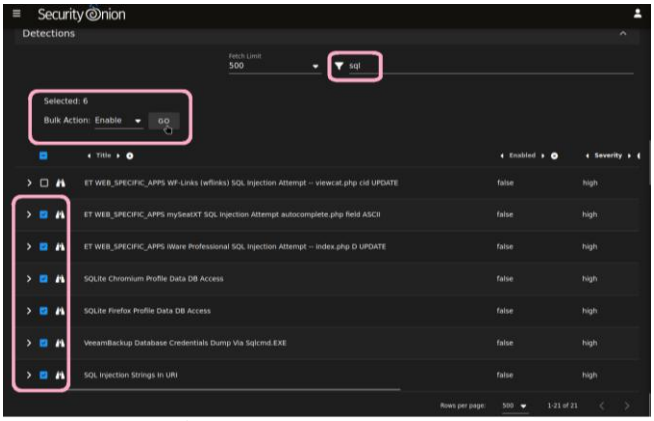

Fig. 9. Activation of rules that have been deemed pertinent to the network.

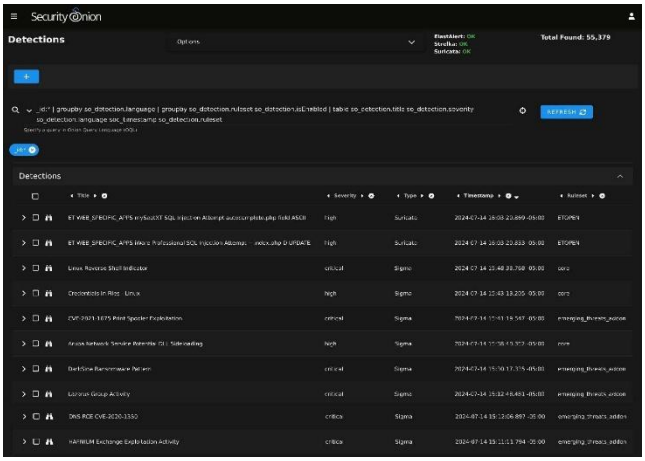

Fig. 10. Detections registered by security onion subsequent to the enablement of certain rules.

Fig. 11. Detections in the network grouped by severity.

2) Observed patterns:

a) Prevalence of informative detections: The majority of detections, specifically 97%, are informative and tend to be lower priority. However, it is crucial to obtain a comprehensive understanding of network traffic and potential misconfigurations or minor anomalies.In this research work, the detection "ET TOR TOR Known Tor Relay/Router (Not Exit) Node Traffic group 184-668" indicates traffic originating from known Tor relay nodes. These nodes may not be inherently malicious; however, they could be utilized to conceal other activities.

b) Critical and high severity detections: Although only 3% of the detected cases are critical or high severity, the potential for damage is concerning. This set of detections encompasses a variety of cyber threats, including SQL injection, ransomware, and Advanced Persistent Threat (APT) group-targeted attacks [1]. Attempts of SQL injection, as evidenced by detections in "mySeatXT," "iWare Professional," and injection strings in URIs, can compromise critical databases. The detection of the "DarkSide Ransomware" pattern indicates the presence of highly destructive ransomware, associated with actors using techniques such as phishing and exploitation of externally accessible services [10, 16].In addition, the traffic identified on TOR relay nodes, as mentioned in the previous point, suggests a possible connection with ransomware activities, as TOR is commonly used to hide command and control operations.

Conversely, the detection of activities attributed to APT groups, such as the "Lazarus Group" [40] and the exploitation of Exchange by "HAFNIUM" [29], point to sophisticated intrusion attempts. In these cases, the objective of the groups appears to be the obtaining of confidential information through advanced tactics and persistence in compromised networks. Furthermore, there have been endeavors to exploit well-documented vulnerabilities, including "CVE-2021-1675 Print Spooler Exploitation" [15] and "CVE-2020-1350 DNS RCE" [19]. These vulnerabilities could potentially enable attackers to execute arbitrary code or compromise critical systems.

Finally, detections related to post-exploitation techniques, such as "Aruba Network Service Potential DLL Sideloading" [2] and "Linux Reverse Shell Indicator" [42], suggest attempts to maintain persistence and move laterally in the network. Data exfiltration [34] is also evident, with alerts such as "Credentials In Files - Linux" [13] and unauthorized database accesses such as "VeeamBackup" [66] and "SQLite" [64].

This series of detections underscores the necessity for constant vigilance against these cyber threats.

D. Relationship of findings to CIS Controls

In this section, we delineate the manner in which the detections made by Security Onion align with the security controls established by the Center for Internet Security (CIS). It should be noted that some findings may be associated with multiple controls; however, the focus will be on those most relevant and representative for each case. As illustrated in Table IV, this relationship is demonstrated.

Furthermore, a double-entry table (see Table V) is presented that visually summarizes these relationships, marking with an "X" the intersection between each finding and the relevant CIS controls. This graphical representation facilitates the expeditious identification of the safety critical points addressed by each finding.

TABLE IV. RELATIONSHIP BETWEEN DETECTIONS AND CIS CHECKS

Detections	CIS Controls	Relation
- ET WEB_SPECIFIC_APPS mySeatXT SQL Injection Attempt - ET WEB_SPECIFIC_APPS iWare Professional SQL Injection Attempt - SQL Injection Strings In URI [63]	CIS 02 Control: Inventory and control of software assets	These detections are directly related to the need to maintain software integrity by updating it to address vulnerabilities in applications where SQL injection can be performed.
	CIS Control 04: Secure Configuration of Assets and Enterprise Software	The implementation of secure configurations has been demonstrated to be an effective measure in preventing the exploitation of SQL injection attacks.
- Linux Reverse Shell Indicator - CVE-2021-1675 Print Spooler Exploitation - Lazarus Group Activity - DNS RCE CVE-2020-135 - HAFNIUM Exchange Exploitation Activity - Potential OWASSRF Exploitation Attempt - Proxy	CIS 07 Control: Continuous vulnerability management	Designed to facilitate the identification and mitigation of vulnerabilities that could be exploited to create reverse shells or by APTs. It is intended to detect and remediate specific vulnerabilities, including CVE-2021-1675, CVE-2020-1350, and those that have been exploited by HAFNIUM. Additionally, it is designed to detect and mitigate attempts to exploit OWASSRF vulnerabilities [54].
	CIS Control 13: Network Monitoring and Defense	● The detection of suspicious activity from APT groups such as Lazarus and reverse shell is essential for continuous monitoring and active network defense. ● The monitoring of attempts to exploit critical vulnerabilities or malicious activity related to Exchange server exploitation.
- Credentials In Files - Linux - SQLite Firefox Profile Data DB Access - VeeamBackup Database Credentials Dump Via Sqlcmd.EXE	CIS 03 Control: Data protection	The protection of sensitive information in databases or browser profiles, including credentials, is imperative to prevent its extraction.
	CIS Control 13: Network Monitoring and Defense	Monitor activities that attempt to access credentials in files, unauthorized access to sensitive databases and suspicious activities that attempt to dump credentials.
Aruba Network Service Potential DLL Sideloading	CIS Control 04: Secure Configuration of Assets and Enterprise Software	Safe configurations to prevent DLL side-loading.
	CIS Control 13: Network Monitoring and Defense	Monitor suspicious DLL side-loading activity.
DarkSide Ransomware Pattern	CIS 10 Control: Malware Defenses	The detection and prevention of the ransomware's execution.

Detections	CIS Controls	Relation
	CIS Control 13: Network Monitoring and Defense	Monitor malicious activity related to ransomware.
Security Onion IDH - SSH Accessed	CIS 06 Control: Access control management	Manage and monitor authorized and unauthorized access to systems.
	CIS 13 Control: Network monitoring and defense	Monitor any suspicious access to SSH services.
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic traffic group 184-668	CIS Control 13: Network Monitoring and Defense	Monitor traffic from Tor relay nodes to identify potential suspicious activity.

TABLE V. SUMMARY OF THE RELATIONSHIP BETWEEN DETECTIONS AND CIS CONTROLS

Detections	CIS Controls						
	02	*03*	*04*	*06*	*07*	*10*	*13*
ET WEB_SPECIFIC_APPS mySeatXT SQL Injection Attempt autocomplete.php field ASCI0049	X		X				
ET WEB_SPECIFIC_APPS iWare Professional SQL Injection Attempt -- index.php D UPDATE	X		X				
Linux Reverse Shell Indicator					X		X
Credentials In Files - Linux		X					X
CVE-2021-1675 Print Spooler Exploitation					X		X
Aruba Network Service Potential DLL Sideloading			X				X
DarkSide Ransomware Pattern						X	X
Lazarus Group Activity					X		X
DNS RCE CVE-2020-1350					X		X
HAFNIUM Exchange Exploitation Activity					X		X
Security Onion IDH - SSH Accessed				X			X
Potential OWASSRF Exploitation Attempt - Proxy					X		X
SQLite Firefox Profile Data DB Access		X					X
VeeamBackup Database Credentials Dump Via Sqlcmd.EXE		X					X
SQL Injection Strings In URI	X		X				
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic traffic group 184-668							X

E. Recommendations and Action Plan

1) Recommendations: The following recommendations are based on the safeguards in the CIS controls and are ordered according to the number of related detections.

a) CIS control 13: Network monitoring and defense

- Centralization and monitoring
  - Centralize security event alerts.
  - Collect network traffic flow logs.
- Intrusion detection
  - Implement a host-based intrusion detection solution.
  - Implement an intrusion detection solution in the network.
- Traffic and access management
  - Perform traffic filtering between network segments.
  - Manage access control for remote assets.

b) CIS 07 control: Continuous vulnerability management

- Management and remediation processes
  - Establish and maintain a vulnerability management process.
  - Establish and maintain a remediation process.
- Automation and vulnerability analysis
  - Perform automated operating system and application patch management.
  - Perform automated vulnerability scans of internal organizational assets and externally exposed business assets.
- Remediation of detected vulnerabilities

c) CIS Control 04: Secure Configuration of Assets and Enterprise Software

- Establish and maintain a secure configuration process for enterprise assets, software and network devices.
- Asset and software security

- Configure automatic session blocking on enterprise assets.
- Implement and manage a firewall on servers and user devices.
- Manage default accounts in enterprise assets and software.
- Uninstall or disable unnecessary services on enterprise assets and software.

- Device security
  - Configure reliable DNS servers on enterprise assets.
  - Apply automatic device locking on laptops and mobile devices.
  - Implement remote wipe capability on portable end-user devices.

d) CIS 02 Control: Inventory and control of software assets

- Software inventory and management
  - Develop and keep the software inventory up to date.
  - Ensure that authorized software is supported.
  - Treatment of unauthorized software.
- Tools and lists
  - Use automated software inventory tools.
  - Use allowed list for authorized software and authorized libraries.

e) CIS 03 Control: Data protection

- Establish and maintain a data management process, data inventory and data classification scheme.
- Access and encryption
  - Configure data access control lists.
  - Encrypt data on user devices, removable media, in transit and at rest.
- Retention and disposal
  - Apply data retention.
  - Securely delete data.
- Segmentation and documentation
  - Document data flow.
  - Segment data processing and storage according to sensitivity.

f) CIS 06 Control: Access control management

- Establish a process for granting access and a process for revoking access.
- Authentication and centralized control
  - Require MFA for externally exposed applications, remote network access and administrative access.
  - Establish and maintain an inventory of authentication and authorization systems.
  - Centralized access control.

g) CIS 10 Control: Malware Defenses

- Implementation and maintenance
  - Implement and maintain anti-malware software.
  - Configure automatic updates of anti-malware signatures.
- Preventive measures
  - Disable autorun and autoplay for removable media.
  - Configure automatic anti-malware scanning of removable media.
  - Enable anti-exploitation functions.
- Centralized management
  - Centrally manage anti-malware software.
  - Use behavior-based anti-malware software.

2) Implementation priority: To achieve an effective improvement in the security of UNSCH, it is proposed that a phased approach be adopted to implement security measures. This approach will be based on the CIS Controls related to network detections. The implementation of safeguards corresponding to IG1 will be prioritized, as these form the fundamental foundations for protecting the organization. Subsequently, the implementation of those corresponding to IG2 will be addressed, as they complement the initial measures and effectively address the additional risks and complexities associated with an organization with a higher risk profile and data sensitivity.

The prioritization of these measures should also be informed by the number of detections associated with each control. For instance, CIS Control 13 has been associated with 13 detections, a figure that positions it as a top priority. CIS Control 07 follows closely with 6 detections, while other controls such as CIS 04 (4 detections), CIS 02 and CIS 03 (3 detections each), and CIS 06 (1 detection) also warrant consideration.

However, a specific consideration must be taken into account in the case of Control 13. Given that its safeguards are not intended for institutions from IG2 and this control has the highest number of associated detections, it is recommended to implement it simultaneously with the safeguards of IG1. This strategy will enable the early mitigation of the most critical vulnerabilities, thereby fortifying the organization's security infrastructure in a comprehensive manner.

3) Action plan: The action plan commences with a comprehensive audit of the IT and security infrastructure to identify gaps and ascertain protection needs. Concurrently,

security policies will undergo a process of updating, based on CIS controls and adapted to the specific needs of the university network. Subsequent to the formulation of policies, the security solutions will be implemented, prioritizing the safeguards of the aforementioned controls. During this implementation phase, training of IT staff and end users on the use of and response to the new security measures will commence.

Throughout the process, a continuous monitoring system will be established to evaluate the effectiveness of the implemented measures and adjust policies and practices as new threats or changes in the IT environment arise. This continuous improvement process will begin as soon as the first safeguards are implemented, ensuring that any gaps detected are addressed immediately. To optimize time and resources, some actions can be carried out in parallel. For instance, while the comprehensive audit is underway, security policies can undergo updates, and concurrently, the training of staff can be initiated for the implementation of the solutions. This ensures that all phases of the action plan are executed in an efficient and coordinated manner.

V. Discussion

The implementation process of Security Onion at UNSCH proved to be an enriching and insightful experience, allowing for the identification of both the strengths and challenges associated with using this tool in a real-world environment. Initially, a commercially available device widely used in the country was selected, which met the minimum requirements for an Evaluation deployment. However, during the second stage of the installation, specifically after confirming the configurations, the device began to experience recurrent failures. These failures consisted of the device shutting down during the subsequent process. This issue was resolved by replacing the device with one that had greater RAM capacity, which allowed the installation to be completed without further issues. This incident highlights the importance of having adequate hardware to ensure the proper functioning of advanced security tools.

The choice of Security Onion as an open-source platform proved to be a strategic decision, especially in a context where the university's administrative authorities are reluctant to invest in cybersecurity solutions or do not prioritize their importance. Security Onion not only provided a robust and scalable solution but also minimized associated costs. This experience reinforces the viability of open-source tools as effective alternatives for institutions with limited resources but growing needs for protection against cyber threats.

On the other hand, a significant limitation of the study was the inability to obtain network traffic directly from the main switch of the university campus. This switch did not have available ports to configure it as a SPAN (Switch Port Analyzer) port, which would have allowed for more comprehensive traffic capture and analysis. Although a partial analysis was achieved with the available resources, this restriction prevented more exhaustive network monitoring.

In summary, this experience not only demonstrated the effectiveness of Security Onion as a network auditing tool but also highlighted the importance of having adequate hardware, available network infrastructure, and the support of institutional authorities to ensure the success of cybersecurity initiatives.

VI. Conclusions and Recommendations

The implementation of Security Onion at UNSCH has demonstrated that it is an effective tool for network auditing, thanks to its capabilities in security monitoring, log management, and intrusion detection. Security Onion has enabled the identification and mitigation of suspicious activities and anomalies within the network of the university campus of the UNSCH, such as SQL injection attempts, ransomware, and traffic associated with advanced threat actors. Additionally, it facilitated the collection, storage, and analysis of logs, which helped identify unusual patterns that will be instrumental in taking preventive actions and avoiding greater damage. Security Onion's ability to centralize these functions contributes to better event traceability and strengthens defense measures against emerging cyber threats.

However, this study has also identified areas for improvement and opportunities for future work. First, it is recommended to implement a Standalone deployment instead of the Evaluation deployment used in this research, as the latter limits the use of certain tools and advanced functionalities. A Standalone deployment would allow for the full utilization of Security Onion's capabilities and improve the accuracy of threat detection.

Second, it is suggested to deploy complementary tools such as Zeek and Snort to compare and enrich the obtained logs. These tools could provide a more comprehensive view of network traffic and help identify threats that might go unnoticed with a single solution. Finally, it is recommended to closely monitor and analyze TOR traffic on the network, given the observed correlation between detections such as "DarkSide Ransomware Pattern" and "ET TOR Known Tor Relay/Router (Not Exit) Node Traffic." This analysis could reveal hidden threats and further strengthen UNSCH's security posture.

In conclusion, while Security Onion has proven to be a valuable tool for network auditing, its implementation can be enhanced through a more robust deployment, the integration of additional tools, and a deeper focus on analyzing encrypted traffic. These recommendations would not only benefit UNSCH but could also serve as a guide for other institutions facing similar cybersecurity challenges.

References

[1] AO Kaspersky Lab. “¿Qué es una amenaza avanzada persistente (APT)?” Kaspersky, https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats. Accessed 20 July 2024.

[2] “Aruba Network Service Potential DLL Sideloading.” DETECTION.FYI, 1 February 2024, https://detection.fyi/sigmahq/sigma/windows/image_load/image_load_side_load_aruba_networks_virtual_intranet_access/. Accessed 17 July 2024.

[3] Beasley, Jeffrey S., and Pilyasat Nilkaev. NETWORKING ESSENTIALS: SIXTH EDITION A COMPTIA NETWORK+ N10-008 TEXTBOOK. Edited by Mark Taber, 6 - Instructor Edition ed., Pearson Education, 2022.

[4] Bejtlich, Richard. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press, 2013.

[5] Bernal Torres, César Augusto. Metodología de la investigación: Administración, economía, humanidades y ciencias sociales. Pearson Educación de Colombia S.A.S., 2016.

[6] Carrasco Díaz, Sergio. Metodología de la investigación científica: pautas metodologicas para diseñar y elaborar el proyecto de investigación. San Marcos, 2015.

[7] Center for Internet Security, Inc. Controles CIS Versión 8. Critical Security Controls versión 8. 8, Español ed., Center for Internet Security, Inc., May 2021.

[8] Chakraborty, Mohuya, et al., editors. The "Essence" of Network Security: An End-to-End Panorama. Springer Nature Singapore, 2020.

[9] Check Point Software Technologies. Check Point 2024 Cyber Security Report. Check Point Research, 2024.

[10] Cibersecurity & Infraestructure Security Agency (CISA). "DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks." CISA, 8 July 2021, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a. Accessed 20 July 2024.

[11] Cloud IT. Informe técnico final. Contratación del servicio de instalación de equipos y cableado estructurado para el proyecto "Mejoramiento de las herramientas tecnológicas para las actividades académicas en la ciudad universitaria de la Universidad Nacional de an Cristóbal de Huamanga". 1, Enero 2022, pp. 1-304.

[12] Cozzupoli, Joe, et al. "How can you choose relevant information security standards?" Linkedin, 15 March 2024, https://es.linkedin.com/advice/0/how-can-you-choose-relevant-information-security-eplrc?lang=en. Accessed 26 Mayo 2024.

[13] "Credentials In Files - Linux." DETECTION.FYI, 30 April 2023, https://detection.fyi/sigmahq/sigma/linux/auditd/lnx_auditd_find_cred_in_files/. Accessed 17 July 2024.

[14] Creswell, John W., and J. David Creswell. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. SAGE, 2023.

[15] "CVE-2021-1675 Print Spooler Exploitation." DETECTION.FYI, 20 June 2023, https://detection.fyi/sigmahq/sigma/emerging-threats/2021/exploits/cve-2021-1675/win_exploit_cve_2021_1675_printspooler_operational/. Accessed 17 July 2024.

[16] "DarkSide Ransomware Pattern." DETECTION.FYI, 20 June 2023, https://detection.fyi/sigmahq/sigma/emerging-threats/2021/malware/darkside/proc_creation_win_malware_darkside_ransomware/. Accessed 17 July 2024.

[17] Deuble, Ashley, and David Shinberg. Using and Configuring Security Onion to detect and prevent Web Application Attacks. Detecting and preventing web applications attacks with Security Onion. SANS Institute, 26 July 2012.

[18] Disso, Jules Pagna, and Muhammad Younas. "The world of malware: an overview." 2018 IEEE 6th International Conference on Future Internet of Things and Cloud - FiCloud 2018: 6-8 August 2018, Barcelona, Spain : Proceedings, IEEE, 2018, pp. 420–427.

[19] "DNS RCE CVE-2020-1350." DETECTION.FYI, 20 June 2023, https://detection.fyi/sigmahq/sigma/emerging-threats/2020/exploits/cve-2020-1350/proc_creation_win_exploit_cve_2020_1350/. Accessed 17 July 2024.

[20] Dos Santos de Carvalho Ribeiro, Thatiane Cristina. Fundamentos de redes de computadores. Editora e Distribuidora Educacional S.A., 2016.

[21] Elasticsearch B.V. "Kibana: Explora, visualiza y descubre datos." Elastic, https://www.elastic.co/es/kibana/. Accessed 26 April 2023.

[22] Elasticsearch B.V. "¿Qué es Elasticsearch? - Elasticsearch: Motor de búsqueda y analítica distribuido oficial." Elastic, https://www.elastic.co/es/what-is/elasticsearch. Accessed 26 April 2023.

[23] Ertel, Jason. "ElastAlert 2 - Automated rule-based alerting for Elasticsearch — ElastAlert 2 0.0.1 documentation." ElastAlert 2, https://elastalert2.readthedocs.io/en/latest/elastalert.html#overview. Accessed 26 April 2023.

[24] Forbes Perú. "El Perú sufrió 5.000 millones de intentos de ciberataques en 2023, reportó Fortinet." Forbes, 2024, https://forbes.pe/tecnologia/2024-03-25/el-peru-sufrio-5-000-millones-de-intentos-de-ciberataques-en-2023-reporto-fortinet.

[25] Fortinet. Outbreak Alerts Annual Report 2023. FortiGuard Labs Outbreak Alerts provide a unique analysis of the threat landscape throughout the tech ecosystem. FortiGuard Labs.

[26] Gonzáles, Ronald, et al. Using Security Onion for Hands-On Cybersecurity Labs. American Society for Engineering Education/Pacific South West Conference, 2015, pp. 1-6.

[27] Google Open Source. "Stenographer is a packet capture solution which aims to quickly spool all packets to disk, then provide simple, fast access to subsets of those packets. Discussion/announcements at stenographer@googlegroups.com." GitHub, 4 November 2022, https://github.com/google/stenographer. Accessed 26 April 2023.

[28] Gupta, Sunil, and Kees Leune. Logging and Monitoring to Detect Network Intrusions and Compliance Violations in the Environment. SANS Institute, 4 July 2012.

[29] "HAFNIUM Exchange Exploitation Activity." DETECTION.FYI, 28 November 2023, https://detection.fyi/sigmahq/sigma/emerging-threats/2021/ta/hafnium/proc_creation_win_apt_hafnium/. Accessed 17 July 2024.

[30] Heenan, Ross, and Naghmeh Moradpoor. Introduction to Security Onion. Paper presented at The First Post Graduate Cyber Security Symposium. The First Post Graduate Cyber Security Symposium - Edinburgh Napier University, Edinburgh, United Kingdom, 10 May 2016, Edinburgh, United Kingdom. Introduction to Security Onion-AbertayUniversity, http://thecyberacademy.org/wp-content/uploads/2016/05/PGCS-symposium_2016_paper_6.pdf. Accessed 23 April 2023.

[31] Hernández Sampieri, Roberto, et al. Metodología de la investigación. Edited by Roberto Hernández Sampieri, McGraw-Hill Education, 2014.

[32] Hickman, Alfredo, and Rich Graves. Gaining Visibility on the Network with Security Onion: A Cyber Threat Intelligence Based Approach. GIAC (GSEC) Gold Certification, SANS Institute, 1 February 2016.

[33] Hjelmvik, Erik. Hands-on Network Forensics. Swedish Armed Forces CERT FIRST, Forum of Incident Response and Security Teams, 14 June 2015, https://www.first.org/resources/papers/conf2015/first_2015_-_hjelmvik-_erik_-_hands-on_network_forensics_20150604.pdf. Accessed 23 April 2023.

[34] IBM. "¿Qué es la exfiltración de datos?" IBM, https://www.ibm.com/es-es/topics/data-exfiltration. Accessed 20 July 2024.

[35] IBM, et al. X-Force Threat Intelligence Index 2024 Resumen ejecutivo. IBM, Febrero 2024.

[36] IBM, and Ponemon Institute. Cost of a Data Breach Report 2024. July 2024.

[37] Jackson, Chris. Network Security Auditing. Cisco Press, 2010.

[38] Kizza, Joseph Migga. Guide to Computer Network Security. Springer International Publishing, 2020.

[39] Laurent, Maryline, and Samia Bouzefrane. Digital Identity Management. Edited by Maryline Laurent and Samia Bouzefrane, Elsevier Science, 2015.

[40] "Lazarus Group Activity." DETECTION.FYI, 20 June 2023, https://detection.fyi/sigmahq/sigma/emerging-threats/2020/ta/lazarus/proc_creation_win_apt_lazarus_group_activity/. Accessed 17 July 2024.

[41] THE LINUX FOUNDATION PROJECTS. "osquery." Welcome to osquery, https://osquery.readthedocs.io/en/stable/. Accessed 26 April 2023.

[42] "Linux Reverse Shell Indicator." DETECTION.FYI, 28 August 2023, https://detection.fyi/sigmahq/sigma/linux/network_connection/net_connection_lnx_back_connect_shell_dev/. Accessed 17 July 2024.

[43] Lockheed, Martin. Gaining the advantage: Applying Cyber Kill Chain® Methodology to Network Defense. 2015.

[44] Maier, Christian, et al. "Cross-sectional research: A critical perspective, use cases, and recommendations for IS research." International Journal of Information Management, vol. 70, no. 102625, 2023. https://doi.org/10.1016/j.ijinfomgt.2023.102625.

[45] Manjunatha, N. "Descriptive Research." Journal of Emerging Technologies and Innovative Research (JETIR), vol. 6, no. 6, 2019, pp. 863-867.

[46] Marotti de Mello, Adriana, and Thomaz Wood Jr. "What is applied research anyway?" Revista de Gestão, vol. 26, no. 4, 2019, pp. 338-339. 10.1108/REGE-10-2019-128.

[47] Meyer, Royer, and Carlos Cid. Detecting Attacks on Web Applications from Log Files. SANS Institute, 26 January 2008, p. 45.

[48] Mobeen, Nazar, et al. "A Review on Security Onion Tools for Intrusion Detection." International Journal of Scientific & Engineering Research, vol. 12, no. 3, 2021, pp. 599-607.

[49] N-able Solutions ULC and N-able Technologies Ltd. "How to Perform a Network Audit: A Step-By-Step Guide." N-able, 1 October 2020, https://www.n-able.com/blog/how-to-perform-network-audit. Accessed 29 April 2023.

[50] NexTReT Ciberseguridad S.L. "Monitorización de Seguridad." Spidernext, https://spidernext.com/monitorizacion-de-seguridad/. Accessed 29 July 2024.

[51] Open Information Security Foundation (OISF). "Suricata User Guide." Suricata 6.0.11 documentation, https://suricata.readthedocs.io/en/suricata-6.0.11/. Accessed 24 April 2023.

[52] Organización para la Cooperación y el Desarrollo Económicos. Manual de Frascati 2015: Guía para la recopilación y presentación de información sobre la investigación y el desarrollo experimental. OECD Publishing, Paris/FEYCT, Madrid ed., 2018, https://doi.org/10.1787/9789264310681-es.

[53] Perù21. "Perú fue el objetivo de más de 3.000 millones de intentos de ciberataques en el 2023." Peru21, 30 Agosto 2023, https://peru21.pe/cheka/tecnologia/ciberseguridad-ciberataques-fortinet-peru-fue-el-objetivo-de-mas-de-3000-millones-de-intentos-de-ciberataques-en-el-2023-noticia/.

[54] "Potential OWASSRF Exploitation Attempt - Proxy." DETECTION.FYI, 26 February 2024, https://detection.fyi/sigmahq/sigma/emerging-threats/2022/exploits/cve-2022-41082/proxy_cve_2022_36804_exchange_owassrf_exploitation/. Accessed 17 July 2024.

[55] Quispe, Julio. "Pymes fueron las más afectadas por ciberataques en el 2023: los ataques más comunes." Gestión, 23 Noviembre 2023, https://gestion.pe/tecnologia/pymes-fueron-las-mas-afectadas-por-ciberataques-en-el-2023-por-que-empresas-peruanas-emprendimientos-negocios-noticia/.

[56] Rodríguez, Guillermo. "Perú es el cuarto país de América Latina con más ciberataques." América Retail, 2023, https://www.america-retail.com/peru/peru-es-el-cuarto-pais-de-america-latina-con-mas-ciberataques/.

[57] Russinovich, Mark, and Thomas Garnier. "Sysmon - Sysinternals." Microsoft Learn, 10 April 2023, https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon. Accessed 27 April 2023.

[58] Saini, Sukhpreet Kaur, et al. 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom). Edited by M. N. Hoda, IEEE, 2016.

[59] Sanders, Chris. Intrusion Detection Honeypots: Detection Through Deception. Applied Network Defense, 2020.

[60] Schwartau, Winn. "It's About Time: The Unappreciated Fundamental Metric for Security." Cyber Defense Magazine, 2021. https://winnschwartau.com/wp-content/uploads/2021/12/TBS-Overview-Metrics-12Dec2021.pdf.

[61] Security Onion Solutions. "Introduction — Security Onion Documentation 2.4 documentation." Security Onion Documentation, https://docs.securityonion.net/en/2.4/introduction.html. Accessed 27 April 2023.

[62] Shin, Bongsik. A Practical Introduction to Enterprise Network and Security Management. Auerbach Publishers, Incorporated, 2021.

[63] "SQL Injection Strings In URI." DETECTION.FYI, 6 September 2023, https://detection.fyi/sigmahq/sigma/web/webserver_generic/web_sql_injection_in_access_logs/. Accessed 17 July 2024.

[64] "SQLite Firefox Profile Data DB Access." DETECTION.FYI, 1 December 2023, https://detection.fyi/sigmahq/sigma/windows/process_creation/proc_creation_win_sqlite_firefox_gecko_profile_data/. Accessed 17 July 2024.

[65] Target. "Strelka: Real-time, container-based file scanning at enterprise scale." GitHub, https://github.com/target/strelka. Accessed 27 April 2023.

[66] "VeeamBackup Database Credentials Dump Via Sqlcmd.EXE." DETECTION.FYI, 13 February 2023, https://detection.fyi/sigmahq/sigma/windows/process_creation/proc_creation_win_sqlcmd_veeam_dump/. Accessed 17 July 2024.

[67] Vinod, Michael, et al. CCNA Security 210-260 Certification Guide: Build Your Knowledge of Network Security and Pass Your CCNA Security Exam (210-260). Packt Publishing, 2018.

[68] Wazuh Inc. "Getting started with Wazuh." Wazuh documentation, https://documentation.wazuh.com/current/getting-started/index.html. Accessed 27 April 2024.

[69] Z3R0th. "Setting up Security Onion at home | by Z3R0th | Medium." Medium, 16 February 2020, https://z3r0th.medium.com/setting-up-security-onion-at-home-717340816b4e. Accessed 21 May 2024.

[70] The Zeek Project. "About Zeek — Book of Zeek." Zeek Documentation, https://docs.zeek.org/en/master/about.html. Accessed 27 April 2024.