ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SIENCE

DESIGNING A SECURITY OPERATIONS FRAMEWORK TO IMPROVE INFORMATION SECURITY MONITORING: THE CASE OF ETHIOPIAN BANKS

By

Muluberhan Embafrash

August 2021

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SIENCE

DESIGNING A SECURITY OPERATIONS FRAMEWORK TO IMPROVE INFORMATION SECURITY MONITORING: THE CASE OF ETHIOPIAN BANKS

A Thesis Submitted to College of Graduate Studies of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information Science

By: Muluberhan Embafrash

Advisor: Million Meshesha (PhD)

August 2021

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SIENCE

DESIGNING A SECURITY OPERATIONS FRAMEWORK TO IMPROVE INFORMATION SECURITY MONITORING: THE CASE OF ETHIOPIAN BANKS

By: Muluberhan Embafrash

Name and Signature of Members of the Examining Board:

Million Meshesha (PhD)	_____	_____
Advisor	Signature	Date
Dereje Teferi (PhD)	_____	_____
Examiner	Signature	Date
Lemma Lessa (PhD)	_____	_____
Examiner	Signature	Date

DECLARATION

I declare that this thesis is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references. A list of references is appended. Moreover, this thesis has not previously been accepted for any degree and is not being concurrently submitted in candidature for any degree in any university.

Signature: _____

Muluberhan Embafrash

This thesis has been submitted for examination with my approval as a university advisor

Advisor: _____

Million Meshesha (PhD)

ACKNOWLEDGEMENT

First and foremost, I would like to thank the almighty God for giving me all the strength and blessings I need in my life.

My heartfelt gratitude goes to my advisor Dr. Million who have provided me unreserved guidance and direction. You have been always kind and cooperative to me whenever I come to your office with my issues. Thank you!

I would also like to thank to all IT security managers, supervisors and staff in all banks, who have spared their precious time to discuss and share me valuable feedbacks about the existing Security Operations practices and gaps while doing this research.

I would also to thank all my family, sisters and brothers especially; Dork, Kidist, Abel, Hailemichael and Abadi who always loves, supports and pushes me to be a better person. I wouldn't be where I am today without you.

Finally, I would like to thank all my classmates, my teachers, colleagues and friends, who have inspired and encouraged me during the course of this research.

ABSTRACT

Ethiopian banks have continued investing heavily in Information technology to expand their banking services and products to their customers using different digital channels. However, this wide use of IT-based services in the banking sector has brought increased concern of information security threat from all involved stakeholders including customers, management, employees, shareholders and regulatory bodies. To overcome this concern, financial institutions have significantly strengthened their defenses in protecting their critical assets against cybersecurity threats using different mechanisms. Regulatory bodies such as National Bank of Ethiopia (NBE), and Information Network Security Agency (INSA) are also playing key roles in facilitating and pushing financial institutions to be equipped with the right information security technology, people, policies and procedures. However, assessment of existing security operation practices reveal, too little attention is given to proactive threat detection and information security continuous monitoring. Having continuous information security monitoring practices by establishing standard Security Operations Center (SOC) is crucial in proactively detecting and responding to cybersecurity attacks directed to this mission-critical banking infrastructure. This study has tried to fill this gap by proposing a comprehensive security operations framework for the Ethiopian banking industry using design science research methodology.

Document analysis and expert discussions have been used to collect and understand the current practices and gaps in security operations. Unavailability of common security operations framework, inadequate security threat monitoring practices, lack of skilled cybersecurity analysts, budget constraints and insufficient collaboration and communication with national and international cybersecurity threat intelligence bodies are some of the gaps and obstacles preventing the SOC team and management in implementing effective and efficient security operations.

Finally, threat detection and monitoring part of the designed artifact is sufficiently demonstrated and evaluated by simulating open-source SIEM solution in a virtual environment. The evaluation result also shows that the design artifact has adequately addressed the people, process and technology aspects. However, secured configurations, forensics and incident response procedures have not been covered in this research, even though they are part of the SOC main functions. Thus, these areas require further study. The financial institutions are also required to assess their readiness in adopting the designed SOC framework and information security monitoring.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

APT	Advanced Persistent Threats
CERT	Cyber Emergency Response Team
CII	Critical Information Infrastructure
CIRT	Cybersecurity Incident Response Team
CISO	Chief Information Security Officer
CND	Computer Network Defense
CONOPS	Concept of Operations
CSIRT	Computer Security Incident Response Team
CSOC	Cybersecurity Operations Center
DDOS	Distributed Denial of Service
DSRM	Design Science Research Methodology
EDR	Endpoint Detection and Response
ENISA	European Network and Information Security Agency
IDS	Intrusion Detection System
INSA	Information Network Security Agency
IPS	Intrusion Prevention System
IR	Incident Response
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
KALI	Kernel Auditing Linux
MDR	Managed Detection and Response
MSSP	Managed Security Services Provider
NIST	National Institute of Standards and Technology
NOC	Network Operation Center
PCAP	Packet Capture
PCI-DSS	Payment Card Industry Data Security Standards
SANS	System Administrator, Audit, Network and Security
SIEM	Security Information and Event Management
SO	Security Onion
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations
SOC-CMM	Security Operations Capability and Maturity Model
SPAN	Switch Port Analyzer
TIP	Threat Intelligence Platform
TTP	Tools, Techniques, and Procedures
UEBA	User and Entity Behavior Analytics
VA	Vulnerability Assessment
VM	Virtual Machine

CHAPTER ONE

INTRODUCTION

1.1. BACKGROUND

As pointed out by Zimmerman (2014) Security Operation Center (SOC) is defined primarily by what it does – Computer Network Defense (CND). Thus, the definition is adapted from characterizing CND as the practice of defense against unauthorized activity within computer networks, including monitoring, detection, analysis, response and restoration activities. A SOC is a team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents (Zimmerman, 2014).

As more businesses and institutions are becoming digital, data and information security is one of the top concerns that needs to be addressed. According to Mugari et al (2016) cybercrime is a serious threat to all the facets of any nation's economic activity and this threat is more pronounced in financial institutions as they have continued to use non-cash based payment systems.

Tebikew (2013) has stated that modern banking increasingly relies on the Internet and computer technologies to operate their business and market interactions. Banks are on the way of using the state-of-the-art technologies to increase efficiency and effectiveness in service-delivery. However, these benefits do not come without risks for information being misused, service disrupted or any other attacks interrupting the normal operation of computer-based information systems. The threats and security breaches are highly increasing in recent years globally, which is with no exception for Ethiopia.

Nowadays, the Ethiopian banking sector has not only deployed Internet banking, but also different digital services such as Core banking, Mobile banking, POS, ATMs to enhance service-delivery and customer's convenience. However, as different channels are added to enhance customer experience, so does the security attack surface has widened. Siddique & Rehman (2011) also have identified the following cybercrimes prevalent in the banking industry, credit card fraud, ATM frauds, money laundering, phishing, identity theft and denial of service.

To defend themselves, financial institutions and the banking industry is implementing different Information Security Programs to counter attacks originating from inside and outside of the organization without affecting customers convenience.

Different studies have been conducted related to information security in the Ethiopian banking industry including Information Security Framework by Tebikew (2013), security practices & policies by Nigussie (2015), information security awareness programs by Bogale (2018) and disaster recovery and incident response management plans by Berhanu (2017). However, they did not address the day-to-day security operations and traffic flow visibility to proactively monitor suspicious activities happening in the banks' IT infrastructure. Maintaining complete traffic flow visibility and continuous security monitoring enables cybersecurity analysts to proactively monitor and detect malicious network traffic before it reaches and compromises sensitive bank systems.

As operations continue to evolve beyond traditional borders, utilizing IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service) in public or private cloud environments, solutions need to evolve ensuring visibility and control of organizational data is maintained. Having visibility of every device and how they are meant to behave on a network is crucial to understand what constitutes a normal traffic and what could be considered a deviation. Network data provides a rich source of information about the traffic moving across a network to find threats passing between servers and troubleshoot application performance problems. Once we have an intelligent view of how the network should behave and what the user behaviors within it looks like, we can monitor activities not fitting those patterns to detect and respond to threats (Raynolds, 2020).

In this research, an attempt is made to formulate a security operations framework for the Ethiopian banking industry based on assessment of the current practice and literature review.

1.2. STATEMENT OF THE PROBLEM

A Security Operations Centre (SOC) functions as a team of skilled people operating with defined processes and supported by integrated security intelligence technologies. The SOC specifically focuses on cyber threat monitoring, forensic investigation, incident management and reporting (IBM, 2013) under the umbrella of an overall security operations environment and clear executive support.

Ethiopian banks have continued highly investing in IT and Security infrastructure to avail their services through different technologies and channels. However, continued investments in IT security equipment alone will not make them secure from different security attacks and financial fraud. Thus, in addition to IT and security infrastructure investments, continuous monitoring and investigation of suspicious traffic entering and exiting critical systems should be conducted to take proactive measures before an active breach occurs. Skilled IT security analysts are also required to monitor and investigate security violations 24x7 to ensure critical systems are not compromised. Banks and financial institutions should also work in close collaborations with national and international information security threat intelligence organizations as banks are no longer separate entities due to the adoption of mobile and Internet for digital banking services.

Currently, Commercial Bank of Ethiopia has already implemented a SOC solution in their premises. The rest are also in the process of acquiring and implementing a SOC center fulfilling local and international legal and compliance requirements.

Security event visualization is still rare in most organizations today. Many security professionals conduct manual log reviews or perform 'spreadsheet' analyses, and for some, implementation of basic Security Information and Event Management (SIEM) technology is as far as they go. However, the ultimate goal should be to develop an environment in which security events are discovered by security professionals within the organization. Data aggregation or correlation as seen in a SIEM is assumed to be beneficial to real-time security event visualization and notification Trustwave (2013).

Attacks have grown significantly in complexity, rendering the majority of 'Off the Shelf' detection solutions ineffective Trustwave (2013). Ethiopian banks who have limited budget might be tempted to use opensource SOC solutions as commercial solutions are becoming expensive options. However, today's sophisticated security threats require highly skilled security analysts equipped with tailor-made security solutions and tools to effectively secure critical systems.

There are few studies that assess the development of SOC frameworks in literature. Onwubiko (2015) studied Cybersecurity Operations Center (CSOC) as essential business control mechanism aimed to protect ICT systems and support organization's cyber defense strategy. He has also stated

that SOC's main purpose is to ensure incidents are identified and managed to resolution swiftly. Muniz et al. (2015) noted that 60 percent of businesses being breached happened within minutes or less, however half of these incidents took anywhere from months to even years before being uncovered. These indicates the importance of having an effective security operations program in which a mature SOC plays a significant role.

Some researchers have also tried to study information security in the Ethiopian banking industry from different angles. These studies include information security management framework proposal by Tebikew (2013). Nigussie (2015) also has tried to study practices, challenges and prospects of information security policy. Gebrehawariat (2017) made an assessment of the effectiveness of security with a focus on Card Banking. Berhanu (2017) also has assessed IT Disaster Recovery Practices. Yohannes (2018) has also studied the gaps in Information Security Incident Management Practices in a selected bank. Bogale (2018) has also proposed Information Security Awareness Program for a private bank in Ethiopia. Kindie (2018) has studied mobile banking security from customers' perspective in one of the government commercial banks. Amare (2015) has tried to assess insider security threats in the Ethiopian Banking Industry.

As we can clearly see from the above related studies, almost all of them predominantly focus on overall IT Security Management, IT Security Policy, IT Disaster Recovery practices and IT Security incident management practices in the Ethiopian financial industry.

However, previous researchers did not try to assess the operational side of IT Security in the Ethiopian banking industry. After laying-out all the plans, frameworks and policies, ensuring whether the services and IT infrastructure is used properly and is in compliance with the organizations policies and plans is very critical. Hence, this research is intended to explore the current Security Operations practices and propose a holistic SOC framework for the Ethiopian Banking industry. Schinagl et al. (2015) also has stated that a number of papers from leading security suppliers, describe specific implementations and are written with a commercial intention. An organization that has to build its own SOC has little benefit from these papers, since they contain no general guidance.

As a result, this study is intended to develop customized Security Operations framework for Ethiopian banks which will enable them to proactively and continually monitor cyber-threats and ensure compliance to the Information Security Program in place.

Thus, the research questions this study attempted to explore and answer includes the following:

1. What are the current **security operation and threat monitoring practices, gaps and challenges** in the Ethiopian Banking industry?
2. What are the **major functions** of a SOC?
3. What is the **suitable SOC framework** that enhances the Security Operations of the banks in mitigating cyberattacks and financial fraud?
4. What is **suitable SOC implementation model** for the Ethiopian banks.
5. What are the **options** available to **implement information security detection and monitoring** in Ethiopian banks with the limited budget and skillset?

1.3. OBJECTIVE OF THE STUDY

1.3.1. General Objective

The general objective of this study is to formulate a Security Operations framework for the Ethiopian Banking industry so as to enhance proactive prevention and mitigation of cyber-attacks and financial fraud through continuous threat detection and monitoring.

1.3.2. Specific Objectives

To achieve the general objective of this study, the following specific objectives are formulated:

- To assess the current Security Operation and information security monitoring practices, gaps and challenges in the Ethiopian Banking industry.
- To identify the main functions and requirements of a modern SOC.
- To propose a comprehensive SOC framework for effective and efficient implementation of security operations for Ethiopia banks.
- To propose suitable SOC implementation models for the Ethiopian banks.
- To assess options of implementing continuous information security threat detection and monitoring as a part of the SOC main functions.
- To demonstrate and evaluate the framework focusing on proactive threat detection and monitoring

1.4. SCOPE AND LIMITATIONS OF THE STUDY

The study is intended to cover the Security Operation practices and development of comprehensive Security Operations framework for Ethiopian financial institutions with specific focus on proactive information security threat detection and monitoring.

This demonstration of the artifact doesn't does not cover security hardening, incident management plans and recovery. In addition, due to resource and time limitation; compliance and penetration testing are not also covered even though they are main functions of the SOC.

For this study, primary data about current security operation and threat monitoring practices have been gathered from selected samples of private and government commercial banks using domain expert discussions. Secondary data is collected from different documents including brochures, annual reports and strategic plans of respective banks. In addition, national cybersecurity assessment reports conducted by INSA have been reviewed. However, site visits to existing SOC centers and threat intelligence have not been conducted in this research due to permission issues.

The study has assessed the current practices and activities, identified and measured their effectiveness and performance, and analyzed the gaps and challenges customized security operations framework and model have been developed based on common characteristics to solve the identified problems.

Finally, information security threat detection and monitoring have been also demonstrated and evaluated as part of the SOC major functions to emphasize the need to implement proactive prevention of cybersecurity threats in the Ethiopian banking sector.

1.5. SIGNIFICANCE OF THE STUDY

This study is believed to have a great contribution to the Ethiopian Banking industry in designing as well as enhancing the effectiveness of security operations including in proactively detecting, mitigating and defending their critical IT infrastructure from cyber-attacks and financial fraud.

The designed framework is also significant in that, in defining and identifying the SOC implementation models, core functions and overall components appropriate for the Ethiopian banking industry.

This research is also demonstrated and evaluated options of using open-source SIEM solutions for the Ethiopian banks who have limited budget and skilled cybersecurity professionals.

This research is also helpful to practitioners who are responsible in designing and implementation of SOC solutions in the Ethiopian financial sector. This study is also expected to be used as an initial guide to inspire future researchers who wants to pursue further study in the field, so as to enhance the result of this study.

In addition, it is believed to create and enhance an overall awareness of SOC and proactive cybersecurity threat detection and monitoring in other sectors as well, such as the health sector, defense and other national security agencies who operates mission-critical IT infrastructure.

CHAPTER TWO

LITERATURE REVIEW AND RELATED WORKS

2.1.OVERVIEW

In this chapter both conceptual literatures and related works are reviewed. In the conceptual literature review; overview of Information Security, Information security management in the banking industry, overview of a SOC and Security Operations practices in the financial sector, skill-sets required by a SOC team, international best practices, standards and guidelines to be followed while building effective and efficient Security Operations and continuous information security threat detection and monitoring are discussed.

2.2.INFORMATION SECURITY

According to (Zimmerman, 2014), todays cybersecurity challenges to business and government organizations include:

- Threat Landscape: - the security landscape is continually evolving, new and automated offensive tools (such as Backtrack, Kali Linux) are becoming readily available for attackers with little knowledge and skills to launch sophisticated attacks.
- Business challenges: - in addition to the technical security threat landscape, legal and business-imposed decisions impact the way organizations operate information security. Such decisions include moving services and information to the cloud, meeting compliance requirements, the proliferation of bring your own devices (BYOD); and the rise of Internet of Everything (IoT).
- Privacy and data protection laws: - in addition to business-centric standards, organizations must adhere to country-specific laws and regulations related to privacy and data protection.

The author added that developing security operations capabilities is critical supporting an organizations compliance with such regulations and react appropriately to security incidents that impact availability, integrity, authentication and confidentiality of information.

According to Bogale (2018) the most well-known theoretical model which treats information security is the CIA triad which includes the following three aspects as shown in Figure 1.

Figure 1:- CIA Triad (Bogale, 2018)

- Confidentiality – is described as the protection of information, application, system and network from unapproved access. It relies to the safeguard of information by illegal admission regardless in what form is stored.
- Integrity – is described as the protection of information, application, system and network from unauthorized change, be intentional or accidental.
- Availability – is the affirmation that information, assets and resources are available only to those authorized.

In addition, Bogale (2018) has stated that effective Information Security incorporates security products, technologies, policies and procedures.

Organizations invest much in technology innovation and upgrading the existing infrastructure to support the business and address their customer need. However, if not the technology and the infrastructure is supported by security at an acceptable level, investing much only in technology and infrastructure wouldn't bring the expected result Gebrehawariat (2017).

Gebrehawariat (2017). has also stated that a successful organization should have the following multiple layers of security in place for the protection of its operations:

I. Physical Security: To protect the physical items, objects, or areas of an organization from unauthorized, access and misuse.

II. Personal Security: To protect the individual or group of individuals who are authorized to access the organization and its operations.

III. Operations Security: To protect the details of a particular operation or series of activities.

IV. Communications Security: To protect an organization's communications media, technology, and content.

V. Network Security: To protect networking components, connections, and contents.

VI. Information Security: To protect information and its critical elements, including the systems and hardware.

According to Nigussie (2015) information security is concerned with protecting information in all its forms, whether written, spoken, electronic, graphical, or using other methods of communication. Defence, Detection and Deterrence (the three Ds) are the three aspects of security that can be applied as a security strategy within an organization.

- Defence aims to protect information assets prior to an attack by prohibiting unauthorized access, modification, destruction or disclosure. Defensive measures reduce the likelihood of a successful compromise of valuable assets, thereby lowering risk and potentially saving the expense of incidents that otherwise might not be avoided.
- Detection on the other hand is an operational level strategy which aimed at identifying specific security behaviour or incident. Various security technologies can be applied within this strategy like network detection devices, network and system scanners, video surveillance systems, misuse and anomaly detectors, antivirus software, etc. A security breach may go unnoticed for hours, days, or even forever without proper detection mechanism.
- Deterrence is another aspect of security which is aimed at influencing human behaviour and attitude in their disciplinary action. It is effective in guiding employees towards legitimate, acceptable use behaviour, in discouraging weakly motivated internal

perpetrators, in reducing insider abuse and misuse of information systems, and in influencing employee intentions.

2.3.INFORMATION SECURITY MANAGEMETN IN THE BANKING INDUSTRY

Due to technology transformation and national information security policy in today's Ethiopian banking business, Information security has become one of the key points for customer attraction, retention and profitability. Ethiopian banking industry is one of the rapidly growing industries in the country (Nigussie, 2015).

Tebikew (2013) has also stated that the banking service has shifted from local branch banks to national and global presence and anywhere-anytime banking. The banking business competition has motivated the advancement of services enabled by IT which in turn increased the information security risk. From Information security aspect, each bank has applied some component of the comprehensive Information Security Policy such as: Acceptable use policy for computers and equipment, conventional key backup policy, antivirus, etc. The researcher further stated that even though many banks have invested on IT security devices as part of CORE banking solution project, managing these devices may be challenging since they don't have overall or comprehensive ISM framework which serve as a guide to develop and implement their own Information security policy based on their requirement in line with the national information security policy.

Nigussie (2015) further stated that management lack of awareness, lack of industry best practices and standards in the country, lack of professionals in the area are among the major challenges Ethiopian banks are facing. Information security is not only a problem that technology can address alone, but also a problem the management to solve. Therefore, legal frameworks in the form of policy and standards are the most prerequisites to establish efficient and reliable security governance systems. The scholar identified the main challenges in formulating, implementing and compliance of Information Security Policy in Ethiopian Banks as lack of management's commitment and support, lack of specialized training to Information security personnel, complexity of the subject matter, no specific education/curriculum in the country, the regulatory body i.e., no developed standard by NBE, resistance with employees to comply with Information Security Policy and lack of continuous awareness training. Nowadays, NBE is forcing each bank

to recruit dedicated information security personnel so that he/she directly engage in the process of protecting the organization's information assets. However, since information security industry needs such a huge initial infrastructure investment and personnel technical efficiency, banks face similar challenges when trying to secure their organization.

Amare (2015) have stated that insider attacks pose a serios information security threat costing Ethiopian banking industry millions of Birr in lost revenue. In addition, the researcher has indicated that critical information assets in the commercial banks are vulnerable to insider attacks and incidents that originate from the inside are often difficult to detect and profile. Installation of unauthorized software and financial fraud are considered as the main insider threats to the Ethiopian banking industry. Concerned bodies should take responsible measures to reduce the threat by monitoring user's computer log and group policy withing a specified domain.

Accroding to Gebrehawariat (2017), the financial sectors are expected to be compliant to the security standard such as PCI DSS in order to be connected to the international payment brands. Being compliant to the security standard will enable the financial sector to protect their valuable asset from the current internal and external attacks. However, the scholar pointed out that most banks and electronic payment processors in Ethiopia often fail complying PCI-DSS security standard in time due to improper security settings, incorrect configurations, low levels of encryption and poor policies and procedures. Assessing those controls using PCI-DSS standard checklist could have prevented costs in business disruption as well as monetary fines and makes the financial sectors competitor in the international market by enabling them to provide international card services such as VISA International, MasterCard, Union Pay and the like.

In addition, Gebrehawariat (2017) identified that, even though different technologies are implemented to protect the organizations from information security risk, there is no regular control and management of the security tools. Periodic risk assessment is not maintained in the organizations to assess and identify risks based on its level (critical, high, medium) and take action accordingly before it affects the system and business.

Bogale (2018) stated that it is a must for the banking industry to pay more attention to the information security issues within the organization nowadays. The banks should establish information security governance framework and organize information security awareness program.

Bogale (2018) also added that existing security frameworks and awareness programs are contextual and are not customized for Ethiopia. Contextual factors such as organizational, national and environment affect the design of such programs.

Woretaw and Lessa (2012) explained that the level of information security awareness in Ethiopian banking sector is unsatisfactory. One of the greatest threats to information security could actually come from within a company or organization.

Yohannes (2018) stated that even though banks are deploying prevention mechanisms to keep out hackers and attempts of cyber-attacks, incidents occur occasionally. This indicates a need for an effective and efficient management of information security incidents. The scholar identified that one Ethiopian bank has a team that work in the security operations center who also acts as incident response team and as IT staff when required in contrary to the ISO/IEC 27035 standard; which recommends assignment of dedicated team for Incident Response.

According Nigussie (2015) the proclamation of Federal Democratic Republic of Ethiopia No. 592/2008 on Federal Negarit Gazeta states that NBE is the regulatory body in any Ethiopian financial sector, which is responsible for the supervision of the following information security related issues in financial institutions:

- Assess whether Ethiopian banks have a disaster recovery site for their data center.
- Assess whether there is a central directory services to authenticate users.
- Assess whether there is an information security personnel in the bank
- Assesses their IT audit reports.
- Assess their fraud registries or logs. All microfinance institutions shall have a well-written monitoring and control policies, approved by the board, and procedures for fraud detection, mitigation and reporting as stated in the licensing and supervision of the businesses of microfinance institutions Fraud Monitoring Directive No. MFI/26/2014

2.4.SECURITY OPERATIONS OVERVIEW

A SOC is defined primarily by what it does – Computer Network Defense (CND). Thus, the definition is adopted from characterizing CND as the practice of defense against unauthorized activity within computer networks, including monitoring, detection, analysis, response and restoration activities. A SOC is a team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents (Zimmerman, 2014). The author further stated that even though practices of CND and incident response is more than 20 years old, SOCs are still facing with fundamental issues related not just to the technologies but with larger issues related to people and processes, from how to handle incident escalation to where the SOC belongs in the organizational structure.

Onwubiko (2015) describes SOC as a center that comprises People (Analyst, Operators, and Administrators etc.) who monitor ICT systems, infrastructure, applications and services using Processes, Procedures and Technology in order to deter computer misuse and policy violation, prevent and detect cyber-attacks, security breaches, and abuse, and respond to cyber incidents.

As 21st century businesses and organizations continue to expand their digital presence and online services, it makes them susceptible to cybercrime and cyber-attacks. In addition, PCI DSS and ISO/IEC 27001:2013, along with other information security and privacy standards, demand that security controls be properly monitored, and that information security events and incidents be appropriately handled. Failure to comply with standards may lead to large fines or jail time for all persons held accountable for information assurance.

Thus, to comply with these security standards and best practices requires establishing effective security operations procedures equipped with the right tools, processes and security professionals to proactively monitor and respond to security incidents.

Triage is the process of sorting, categorizing, and prioritizing incoming events and other requests for SOC resources.

An **incident** is: - an assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores,

or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.

To determine the nature of the attack, the SOC often must perform advanced **forensic analysis** on artifacts such as hard drive images or full-session packet capture (PCAP), or **malware reverse engineering** on malware samples collected in support of an incident.

A SOC provides services to a set of customers referred to as a **constituency** a bounded set of users, sites, IT assets, networks, and organizations. Combining definitions constituency can be established according to organizational, geographical, political, technical, or contractual demarcations.

SOC authority are classified in to two stages of the incident life cycle:

1. **Reactive.** Responsive measures taken after an incident is either suspected or confirmed. Actions are usually more tactical in nature - they are temporary and impact only those constituents and systems that are directly involved in an incident. Examples include logical or physical isolation of a host, log collection from a server, or an ad hoc collection of artifacts.

2. **Proactive.** Measures taken in preemption of a perceived threat, before direct evidence of an incident is uncovered. These actions are more strategic in nature - they are usually durable and impact substantial portions of the constituency

Situational Awareness

For a SOC to effectively provide a set of capabilities to constituents, it must understand the environment in which it executes the CND mission, both at a macroscopic and microscopic level. A large portion of a SOC's job, whether intentionally or by accident, is to maintain and provide this understanding of the constituency's defensive posture back out to its constituents. This understanding is referred to as situational awareness (SA).

Incident Tip-offs

A SOC's number one job is to find and respond to security incidents. Potential incident reports, or "tippers," can come from a number of parties, including:

- Constituents with normal, unprivileged system access
- Constituency system and network administrators
- Constituency help desk
- Constituency ISSOs and ISSMs
- Legal counsel or compliance entities
- Peered, subordinate, coordinating, or national SOCs
- Law enforcement or other investigatory entities
- Other organizations somehow involved in the incident.

These tip-offs can be delivered through a variety of methods, typically:

- Email messages
- Phone calls
- Walk-in reports
- Incident reporting form on SOC website
- Cyber tip feeds (from other SOCs).

Incidents reported through these means should usually be regarded as high-value, especially in comparison to unconfirmed IDS alerts. Because they were evaluated in the context of these parties' own missions and systems, they are almost certain to be worthy of attention.

Cyber Attack Life Cycle Phase	Description	Example
Recon(naissance)	The adversary identifies and investigates targets.	Web mining against corporate websites and online conference attendee lists.
Weaponize	The set of attack tools are packaged for delivery and execution on the victim's computer/network.	The adversary creates a trojanized Portable Document Format (PDF) file containing his attack tools.
Deliver	The packaged attack tool or tools are delivered to the target(s).	The adversary sends a spear phishing email containing the trojanized PDF file to his target list.
Exploit	The initial attack on the target is executed.	The targeted user opens the malicious PDF file and the malware is executed.
Control	The adversary begins to direct the victim system(s) to take actions.	The adversary installs additional tools on the victim system(s).
Execute	The adversary begins fulfilling his mission requirements.	The adversary begins to obtain desired data, often using the victim system as a launch point to gain additional internal system and network access.
Maintain	Long-term access is achieved.	The adversary has established hidden backdoors on the target network to permit regular reentry.

Table 1:- Cyber Attack Life-Cycle (Zimmerman, 2014)

Tools and Data Quality

The CND mission succeeds or fails by the SOC analysts' ability to collect and understand the right data at the right time in the right context. Virtually every mature SOC uses a number of technologies that generate, collect, analyze, store, and present tremendous amounts of security-relevant data to SOC members.

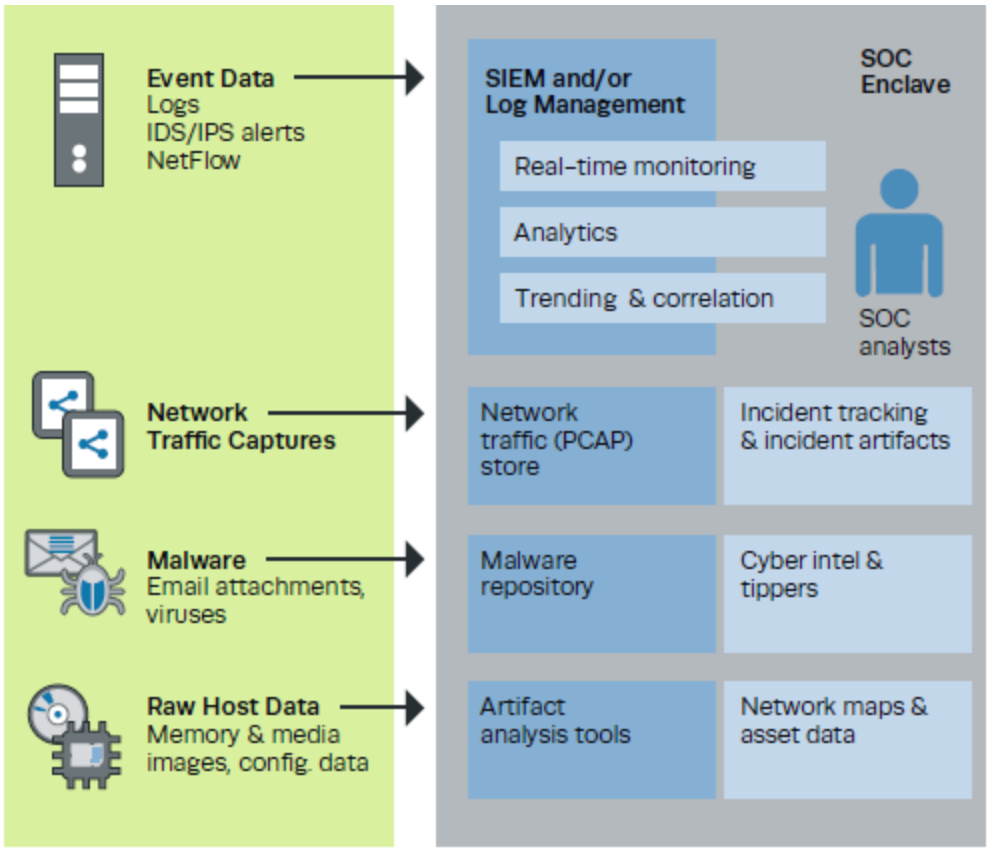

Figure 2:- Typical SOC Tool Architecture (Zimmerman, 2014)

No matter how severe, a single raw event by itself does not provide sufficient evidence that an incident actually occurred.

Agility

If the SOC has a worst enemy, some might say that it is the APT. However, as the adversary acts, reacts, and changes strategies quickly; so, should organizations need to respond fast to maintain the same pace of advancement as the adversary.

2.4.1. SOC Team

Acquiring complex technology and world-class automated systems will fail if not monitored and maintained by the right people. Good SOC team members should have a combination of deeply specialized skills and general security knowledge who are able to interpret and investigate potential security incidents as fast as possible and with high accuracy (Muniz et al., 2015).

A SOC typically will designate a set of individuals devoted to real-time triage of alerts, as well as fielding phone calls from users and other routine tasks. This group is often referred to as **Tier 1**.1 If Tier 1 determines that an alert reaches some predefined threshold, a **case** is created and **escalated** to Tier 2. This threshold can be defined according to various types of potential "badness" (type of incident, targeted asset or information, impacted mission, etc.). Usually, the time span Tier 1 has to examine each event of interest is between 1 and 15 minutes. It depends on the SOC's escalation policy, concept of operations (CONOPS), number of analysts, size of constituency, and event volume. Tier 1 members are discouraged from performing in-depth analysis, as they must not miss events that come across their real-time consoles. If an event takes longer than several minutes to evaluate, it is escalated to Tier 2.

Tier 2 accepts cases from Tier 1 and performs in-depth analysis to determine what actually happened—to the extent possible, given available time and data—and whether further action is necessary. Before this decision is made, it may take weeks to collect and inspect all the necessary data to determine the event's extent and severity. Because Tier 2 is not responsible for real-time monitoring and is staffed with more experienced analysts, it is able to take the time to fully analyze each activity set, gather additional information, and coordinate with constituents. It is generally the responsibility of Tier 2 (or above) to determine whether a potential incident occurred (Zimmerman, 2014).

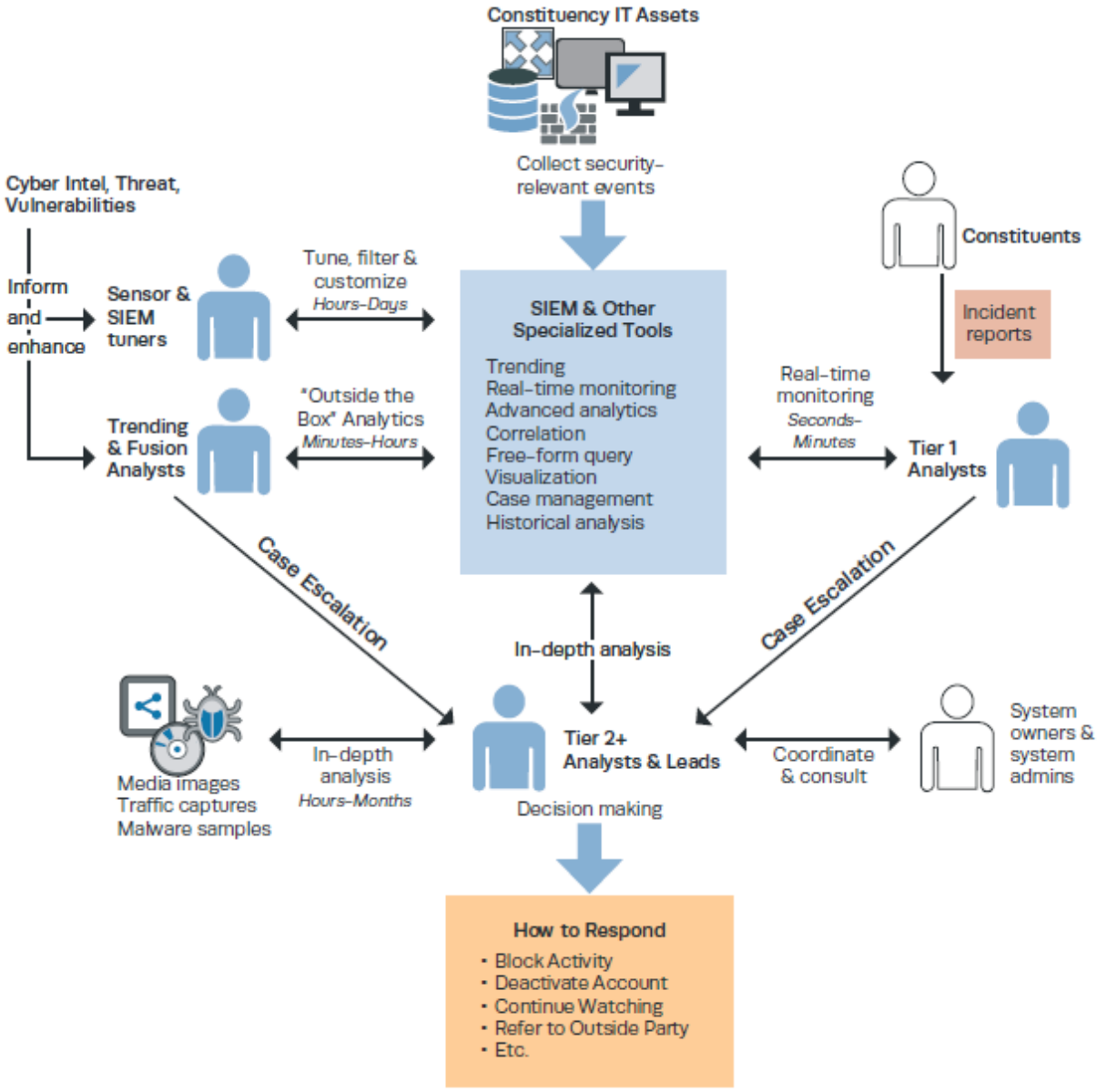

Figure 3:- SOC Roles and Incident Escalation (Zimmerman, 2014)

2.5.BEST PRACTICES, STANDARDS AND GUIDELINES RELATED TO SECURITY OPERATIONS

2.5.1. SANS

The SANS Security Operations guide by Hubbard (2020) divides SOC functions into Core functions and Auxiliary functions as shown in Figure 4. The core functions are drawn in solid boxes while the auxiliary functions are in dashed outlines.

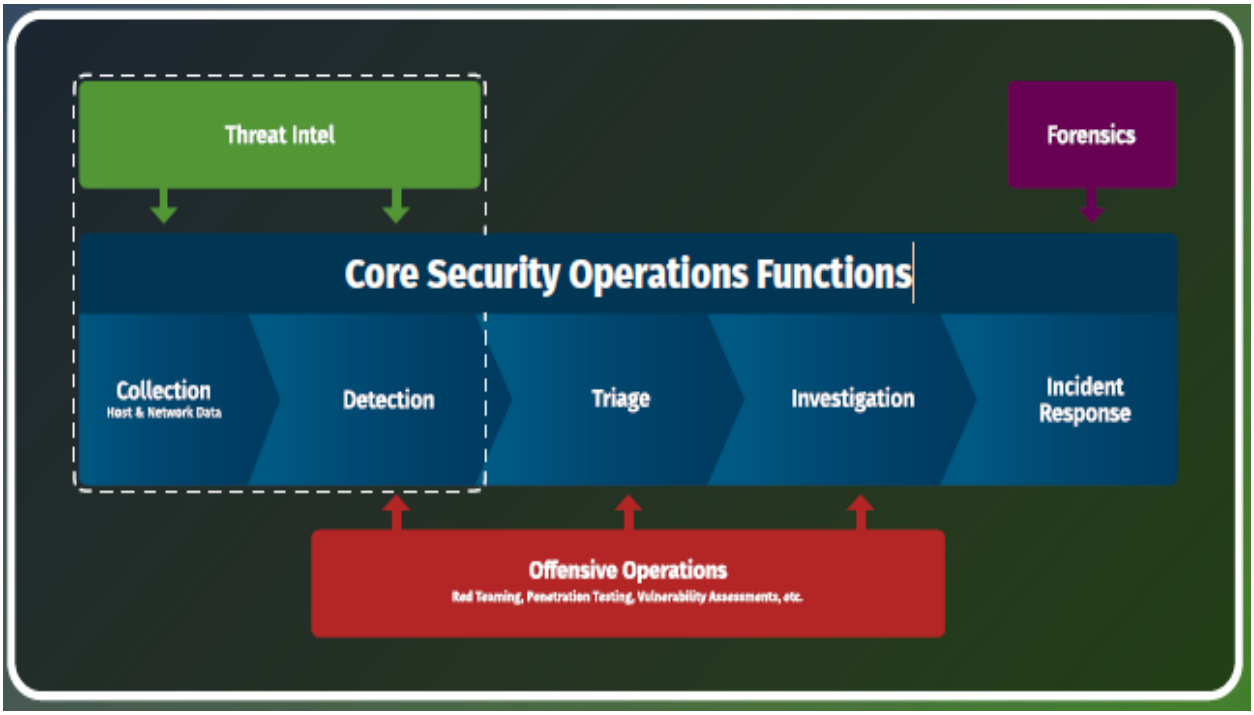

Figure 4:- SOC functions Diagram (Hubbard, 2020)

SOC Core Functions

- **Collection** – involves recording security-relevant events (any useful and observable but not necessarily malicious activity) in the environment. Recording all events such as web traffic, logins and more is required for spotting anomalous activity that may be used to identify attacks in progress. Specific data types to be collected should be guided by your threat intelligence, which should inform you of what types of events and logs are required to detect attacks.

The output of this stage is events that may be logs, network traffic metadata, or other derived information about what occurred on a given device or network segment. This data is typically generated either on an endpoint device as a log or gathered/generated from network traffic that is observed directly by a network appliance or via network tap or switch mirror port.

- **Detection-** after collection stage comes the detection stage to accurately identify (without missing anything or generating false positives), all observed events that may indicate a potential attack. This can happen either reactively through automatic detections using SIEM analytics engines, network or endpoint sensors or through proactive by searching through the data using threat-hunting. The main goal of this stage is to find all truly malicious activity and get an alert related to it into the triage for action by the security team. The effectiveness of a SOC in this stage is correlated with the quality of the tools employed as well as the strength of the SOC's threat-hunting capabilities, threat intelligence information, and detection engineering functions.

- **Triage** – once the detection stage has generated alerts on the events of interest these alerts are all forwarded to one or more queues for triage. In this stage, SOC analysts must sort through all the potentially malicious activity that has been generated by the detection function and determine the order of importance in which to assess each alert. Triage order is often based on factors such as how far the attack may have progressed, the criticality of the system being attacked, the privilege of account that may be compromised, and whether it appears to be a unique or targeted attack.

- **Investigation** – after alert is selected from the triage queue, SOC analysts investigate the alert in more detail to verify if something bad is truly happened. As many SOCs suffer from overly sensitive analytics and untuned alert logic, this step can often lead to a false positive determination and dismissal or the alert. Thus, it may involve gathering data from additional network sensors or logs from multiple sources or performing open-source intelligence research. The main goal of this stage is the accurate verification of whether an alert is true or false positive.

- **Incident Response** – receives notification or alerts that have been investigated and qualified as a situation that must be dealt with. The goal of this stage is to scope, contain, and eradicate the problem as quickly as possible, and ultimately recover from the incident with a minimum of damage. Depending on the severity of the issue, this activity may range anywhere from minor virus removal to month-long investigation with forensics, law enforcement involvement, and more.

  The output of an incident response function should be both the remediation of the incident and lessons learned on how to prevent that type of issue in the future by categorizing the attack details into profiles of threat groups and threat intelligence.

SOC Auxiliary Functions

The following groups are often either part of the SOC organization or work closely with it to help accomplish the cyber defense mission.

- **Threat intelligence** – teams must work closely with the SOC to inform them of what adversity groups exist, what they want, and which ones are likely to be interested in the organization. This helps prioritize controls, defensive tools and detection strategies, and ensure that the team focuses on the right areas for defensive tools and detection strategies.
- **Forensics** – largely focused on assisting the incident response stages, forensics team and specialists help find the ground truth during an incident using specialized knowledge of how activity on a machine may leave datable evidence.
- **Penetration Testing/Vulnerability Management –** works closely with the SOC, largely to make the results of scans available such that the SOC can detect when an exploit has been attempted against a system that may be vulnerable to it.

2.5.2. NIST

According to NIST 800-53 (2020), the fundamental concepts associated with security and privacy controls includes the relationship between requirement and controls. The term requirement is explained as a guideline used in both legal and policy requirements, as well as expressions of the

broader set of stakeholder protection needs that may be derived from different sources (e.g., such as laws, directives, regulations, policies, standards, mission and business needs, or risk assessment).

Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and reflecting the protection needs of organizational stakeholders. Controls are selected and implemented by the respective organization in order to satisfy the system requirements and can include administrative, technical, and physical aspects. For ease of use in the security and privacy control selection and specification process, controls are organized into 20 families.

NIST 800-53 Rev. 5 IR-14 (2020) recommends establishing and maintaining a security operation center.

A Security Operation Center (SOC) is the focal point for security operation and computer network defense for an organization. The purpose of SOC is to defend and monitor an organization's systems and networks (i.e., cyber infrastructure) on an ongoing basis. The SOC is responsible for **detecting**, **analyzing**, and **responding** to cybersecurity incidents in a timely manner. The organization staffs the SOC with skilled technical and operational personnel (e.g., security analysts, incident response personnel, system security engineers) and implements a combination of technical, management, and operational controls (including monitoring, scanning, and forensic tools) to monitor, fuse, correlate, analyze, and respond to threat and security-related event data from multiple sources. These sources include perimeter defenses, network devices (e.g., routers, switches) and endpoint agent data feeds. The SOC provides a holistic situational awareness capability to help organizations determine the security posture of the system and organization. A SOC capability can be obtained in a variety of ways i.e., larger organizations may implement a dedicated SOC while smaller organizations may employ third-party organizations to provide such capability.

NIST (2014) has identified five cybersecurity core functions which are Identify, Protect, Detect, Respond, and Recover to form continuous and concurrent cybersecurity operation culture to address information system risks and threats.

Figure 5:- NIST CSF (NIST, 2014)

2.5.3. PCI-DSS

The Payment Card Industry Data Security Standard (PCI DSS), a standard set by the PCI Security Standards Council (PCI SSC) that applies to all entities that store, process, and/or transmit cardholder data, mandates a number of technical and operational security requirements. The standard mandates, under the "regularly monitor and test networks" control objective mapped to PCI DSS requirements 10 and 11, that organizations must regularly monitor and test networks to find and fix vulnerabilities.

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

PCI DSS Requirements	Testing Procedures	Guidance
10.3 Record at least the following audit trail entries for all system components for each event:	**10.3** Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following:	By recording these details for the auditable events at 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when, and how.
10.3.1 User identification	**10.3.1** Verify user identification is included in log entries.	
10.3.2 Type of event	**10.3.2** Verify type of event is included in log entries.	
10.3.3 Date and time	**10.3.3** Verify date and time stamp is included in log entries.	
10.3.4 Success or failure indication	**10.3.4** Verify success or failure indication is included in log entries.	
10.3.5 Origination of event	**10.3.5** Verify origination of event is included in log entries.	
10.3.6 Identity or name of affected data, system component, or resource.	**10.3.6** Verify identity or name of affected data, system component, or resources is included in log entries.	
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. *Note: One example of time synchronization technology is Network Time Protocol (NTP).*	**10.4** Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.	Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach). For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised.
10.4.1 Critical systems have the correct and consistent time.	**10.4.1.a** Examine the process for acquiring, distributing and storing the correct time within the organization to verify that: • Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time, • Systems receive time information only from designated central time server(s).	

Table 2:- PCI-DSS Requirement 10.3 (PCI-DSS, 2018)

PCI DSS Requirements	Testing Procedures	Guidance
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	**10.6.1.a** Examine security policies and procedures to verify that procedures are defined for reviewing the following at least daily, either manually or via log tools: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	Checking logs daily minimizes the amount of time and exposure of a potential breach. Daily review of security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file-integrity monitoring (FIM) systems, etc. is necessary to identify potential issues. Note that the determination of "security event" will vary for each organization and may include consideration for the type of technology, location, and function of the device. Organizations may also wish to maintain a baseline of "normal" traffic to help identify anomalous behavior.
	10.6.1.b Observe processes and interview personnel to verify that the following are reviewed at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	

Table 3:- PCI-DSS Requirement 10.6.1 (PCI-DSS, 2018)

Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI DSS Requirements	Testing Procedures	Guidance
11.3.1 Perform *external* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	**11.3.1.a** Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows: • Per the defined methodology • At least annually • After any significant changes to the environment.	Penetration testing conducted on a regular basis and after significant changes to the environment is a proactive security measure that helps minimize potential access to the CDE by malicious individuals. The determination of what constitutes a significant upgrade or modification is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant. Performing penetration tests after network upgrades and modifications provides assurance that the controls assumed to be in place are still working effectively after the upgrade or modification.
	11.3.1.b Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	
11.3.2 Perform *internal* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	**11.3.2.a** Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows. • Per the defined methodology • At least annually • After any significant changes to the environment.	
	11.3.2.b Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	**11.3.3** Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected.	

Table 4:- PCI-DSS Requirement 10.3 (PCI-DSS, 2018)

11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	**11.4.a** Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic: • At the perimeter of the cardholder data environment • At critical points in the cardholder data environment.	Intrusion detection and/or intrusion prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known "signatures" and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and send alerts and/or stop the attempt as it happens. Without a proactive approach to unauthorized activity detection, attacks on (or misuse of) computer resources could go unnoticed in real time. Security alerts generated by these techniques should be monitored so that the attempted intrusions can be stopped.
	11.4.b Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises.	
	11.4.c Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection.	
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	**11.5.a** Verify the use of a change-detection mechanism by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: • System executables • Application executables • Configuration and parameter files • Centrally stored, historical or archived, log and audit files • Additional critical files determined by entity (for example, through risk assessment or other means).	Change-detection solutions such as file-integrity monitoring (FIM) tools check for changes, additions, and deletions to critical files, and notify when such changes are detected. If not implemented properly and the output of the change-detection solution monitored, a malicious individual could add, remove, or alter configuration file contents, operating system programs, or application executables. Unauthorized changes, if undetected, could render existing security controls ineffective and/or result in cardholder data being stolen with no perceptible impact to normal processing.

Table 5:- PCI-DSS Requirement 11.4 & 11.5 (PCI-DSS, 2018)

2.5.4. ENISA

According to the ENISA (European Network and Information Security Agency), a SOC provides an incident detection service by observing technical events in networks and systems and can also be responsible for incident response and handling. In large enterprises, SOCs sometimes focus only on monitoring and detection services and then handover incident handling to separate CSIRT. In smaller organizations, CISRT and SOCs are often considered to be synonymous.

Typically, SOC teams operate from SOC rooms, where analysts sit at their workstations in front of a video wall that projects a summary of the current situation. SOC teams typically evolves from IT security teams automating their work using security information and event management (SIEM) and other security automation and orchestration technology for security monitoring. SOC teams usually focus their Key Performance Indicators (KPIs) around quality indicators – detection speed, detection breadth, coverage, false-positive rates – as well as incidents handled, the ratio of alerts/events/incidents, number of escalation and workload per incident.

CSIRT/SOC Service Areas

- Information Security Incident Management – includes Information Security Incident report acceptance, incident analysis, artifact and forensic evidence analysis, mitigation & recovery
- Vulnerability Management – vulnerability discovery/research, report, analysis, coordination, disclosure and response
- Situational Awareness – data acquisition, analysis and synthesis, communication
- Knowledge Transfer – awareness building, training and education, technical and policy advisor
- Information Security Event Management – monitoring and detection, event analysis.

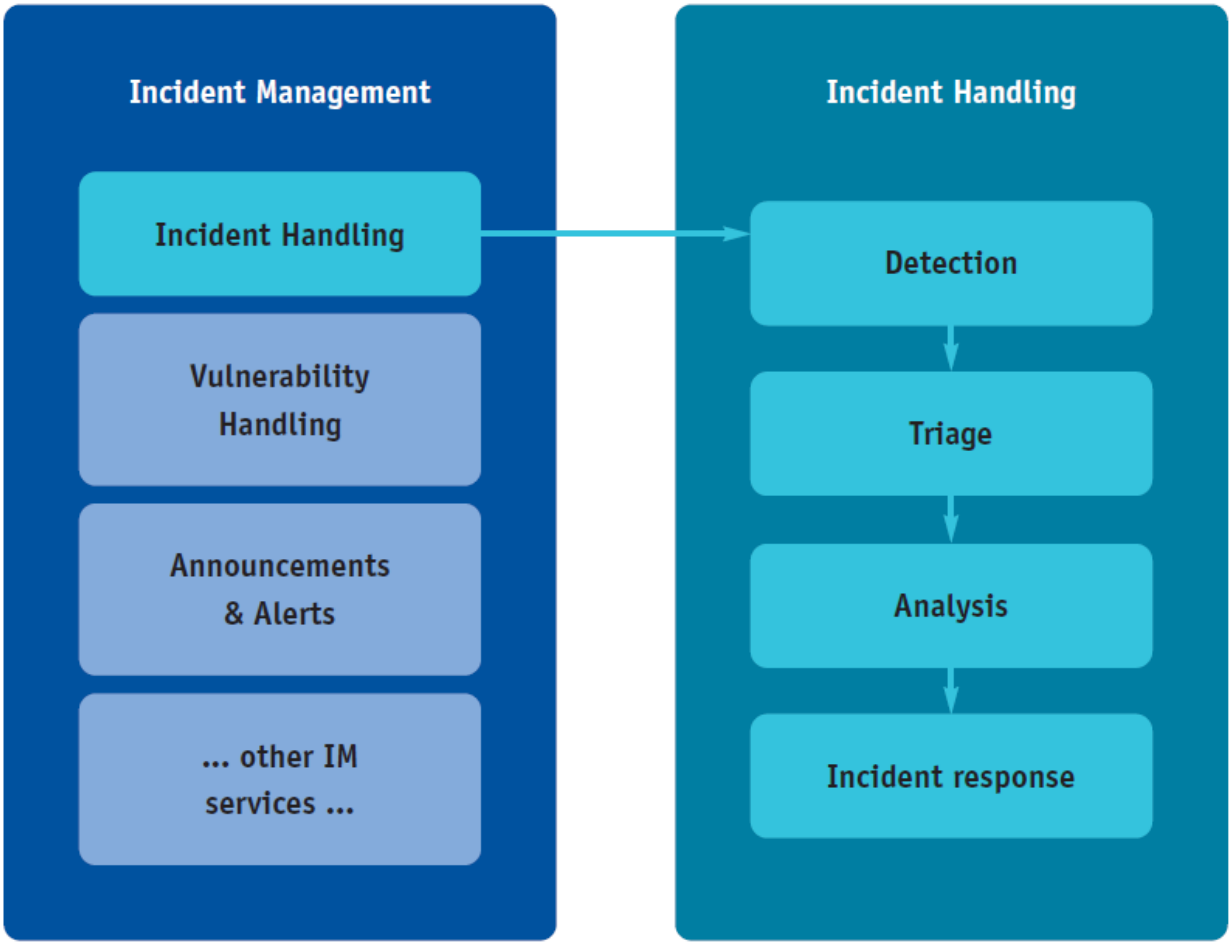

Figure 6:- Incident Management and Incident handling (ENISA, 2010)

2.5.5. MITRE ATT&CK

A SOC satisfies the constituency's network monitoring and defense needs by offering a set of services. The main capabilities/functionalities of a SOC even though it may not cover all.

Real-Time Analysis – includes call center used for tips, incident reports, and requests for CND services from constituents received via phone, email, SOC website postings, or different methods. It also includes real-time monitoring and triage analysis of real-time data feeds (such as system logs and alerts) for potential intrusions. After a specified time, threshold, suspected incidents are escalated to an incident analysis and response team for further study. Usually, synonymous with SOC's Tier 1 analysis, focusing on real-time feeds of events and other data visualizations.

Intel and Trending – collection, consumption, and analysis of cyber intelligence reports, cyber intrusion reports, and news related to information security, covering new threats, vulnerabilities, products, and research. Intel can be culled from coordinating SOCs, vendors, news media websites, online forums, and email distribution lists. Extracting data from cyber intel and synthesizing it into new signature, content and understanding of adversary TTPs, thereby evolving monitoring operations. It also includes long-term analysis of event feeds, collected malware, and incident data for evidence of malicious or anomalous activity or to better understand the constituency or adversary TTPs. This function also includes threat assessment i.e., holistic estimation of threats posed by various actors against the constituency, its enclaves, or lines of business, withing the cyber realm by leveraging existing resources such as cyber intel feeds and trending along with the enterprise's architecture and vulnerability status.

Incident Analysis and Response – prolonged, in-depth analysis of potential intrusions and tips forwarded from other SOC members. This capability is usually performed by analysts in tiers 2 and above within the SOC's incident escalation process. It usually involves analysis of various data artifacts to determine the who, what, when, where, and why of an intrusion – its extent, how to limit damage, and how to recover. It also involves working with affected constituents to gather information about an incident, understanding its significance, and assess mission impact and countermeasures to deter and block adversary presence or damage.

Artifact Analysis – gathering and storing forensic artifacts related to an incident in a manner that supports its use in legal proceedings. This function also includes malware and implant analysis also known as reverse engineering to extract malware (viruses, Trojans, implants, droppers, etc.)

from network traffic, or media images and analyzing them to determine their nature. SOC members typically looks for initial infection vector, behavior and informal attribution to determine the extent of an intrusion and detailed timeline of events.

Scanning and Assessment – this SOC functionality includes Network Mapping, Vulnerability Scanning & Assessment and Penetration Testing. Network mapping activities include regular mapping of constituency networks to understand the size, shape, makeup, and perimeter interfaces through automated or manual techniques. Vulnerability scanning and assessment is also conducted to check vulnerability status, usually focusing on each system's patch level and security compliance, examining system configuration and review of system design documentation to produce report and findings along with recommended remediation. In addition, penetration testing is performed by conducting a simulated attack against a segment of the constituency to assess the target's resiliency to an actual attack using different tools. These operations usually are conducted only with the knowledge of and authorization of the highest-level executives within the constituency without the forewarning system owners.

Outreach – this SOC capability involves providing product assessment, security consulting and training and awareness and media relation services to constituents. In addition, it involves Situational Awareness i.e., regular, repeatable repackaging and redistribution of the SOC's knowledge of constituency assets, networks, threats, incidents, and vulnerabilities to constituents. This capability goes

2.5.6. SOC-CMM

The SOC-CMM is open source SOC maturity assessment model composed of five domains which are Business, People, Process, Technology and Services. A set of assessment questions was developed for objective and self-assessment to be performed to determine if a specific SOC has implemented the identified elements. Each SOC also may weigh the importance of elements of the SOC-CMM, indicating that some elements are not appropriate for the organization's requirement or culture.

The SOC is where log information collected throughout the enterprise is gathered, processed and analyzed by skilled individuals to find indicators of cyber threats in the infrastructure. Thus, the

SOC adds value to business by increasing the resilience of the organization against cyber threats and minimizing damage resulting from cyber-attacks.

Capability maturity measurement is a SOC management tool that can be used to determine strengths and weaknesses of the SOC. Furthermore, it provides a means for measuring growth of the SOC, thereby demonstrating the return on investment in the SOC.

Maturity level	Description
0. Non-existent	At this level, the aspect is extremely ad-hoc or incomplete. Thus, delivery is not assured.
1. Initial	The aspect is delivered in an ad-hoc fashion.
2. Managed	The aspect is documented and delivered consistently.
3. Defined	The aspect is managed using ad-hoc feedback on the quality and timeliness of deliverables.
4. Quantitatively Managed	The aspect is systematically being measured for quality, quantity and timeliness of deliverables.
5. Optimizing	The aspect is continuously being optimized and improved upon.
Capability level	**Description**
0. Incomplete	At this level, the aspect is incomplete. Thus, the SOC has insufficient capability to deliver this aspect.
1. Performed	There is sufficient capability to deliver the aspect at a basic level.
2. Managed	The capability for the aspect is delivered consistently.
3. Defined	The capability for this aspect is optimized and well-documented and delivers true added value.

Table 6: SOC-CMM capability and maturity levels

2.6. RELATED WORKS

2.6.1. Description

Different related research works have been done by local as well as foreign scholars in the information security field.

The local research works reviewed include, different studies related with Information Security management in the Ethiopian banking industry; such as Information Security Management Framework, Information Security Policy and Awareness, Incident Response Management, Insider Threats, Card Banking and Mobile Banking Security and Disaster Recovery practices.

Different foreign research works, which are related with this research have also been critically reviewed to assess strengths and gaps.

2.6.2. Local Works

In this section, the researcher tried to refer and review local research works conducted on the area of information security in the financial sector. Gebrehawariat (2017) assessed information security management practices in the financial sector with special focus on card banking using PCI-DSS security standard as a benchmark to identify gaps and recommend best security practices. The researcher followed quantitative research methodology and used questioners to collect data. In addition, observation and document viewing approaches are used to strengthen the research. The research findings indicate that most of the essential security practices and management activities in the financial sector does not comply with international security standards. In addition, most of the critical security requirements that would address the financial sector from security risk is below acceptable level. The researcher concluded by identifying the major security factors that are prohibiting the financial sector from complying to PCI-DSS security standard and suggesting actions items and directions. However, the study is limited to card banking security compliance and didn't address overall IT infrastructure security compliance requirements. In addition, the overall organizational performance enhancements it brings to Ethiopian banking sector by complying to international card-banking security standards is not justified.

Amare (2015) also attempted to assess current insider threat management in the Ethiopian banking industry with particular emphasis on insider threat, motivational factors and mitigation strategies. The researcher used surveys to conduct the research and questionnaires were used to collect data from selected samples. Based on the study findings, insider threats such as installation of unauthorized software and financial frauds are identified as the most prevalent malicious activities in the Ethiopian banking industry. Dissatisfaction with immediate managers, monetary gain, desire for recognition and emotional distress are also indicated in the research as the motivation factors behind insider threats. Finally, the researcher suggested different ways of mitigating insider threats and recommended best practices to be followed. However, the research doesn't cover proactive mechanisms of detection and monitoring of insider threats.

Kindie (2018) studied customers' perception towards mobile banking security at Commercial Bank of Ethiopia. The researcher adopted Protection Motivation Theory (PMT) and Technology Acceptance Model (TAM) theoretical research models to formulate the research. A survey questionnaire and interview were used to collect data from customers and internet banking

managers respectively. The findings of the research indicate that factors such as perceived ease of use, trust belief, self-efficacy, perceived risk and perceived vulnerability affecting customers' perception towards mobile banking security. However, the researcher pointed out the need to explore additional constructs that can predict customers perception more accurately. New measures such as attitude, demographic variables and prior computing experience has been suggested to be considered by the researcher in future studies.

Tebikew (2013) has studied and developed Information Security Management framework for the Ethiopian banking industry by assessing current practices and international security standards. Qualitative and quantitative research approaches were used. Questionnaire surveys, document analysis and interviews were used also to collect the necessary data while conducting the research. The study results show that the banks are using diverse mechanisms to manage information systems security with low compliance level to Information Security Management best practices and standards. Sixteen Information Security Management domains which have been classified into three main categories have also been identified. However, metrics of security management effectiveness and the impact of organizational security culture, trust-level and ethical conduct have not been addressed in the research.

Nigussie (2015) has also studied the practices, challenges and prospects of Information Security policy in the Ethiopian banking industry by assessing the current issues. The study used qualitative research methodology; using interview and observation to collect primary data. Secondary data is also collected from journal articles, published statistical resources and bulletins. Lack of awareness of the Management, lack of local best practices and standards and lack of professionals in the area are also identified among the major challenges facing the Ethiopian banking industry. Impact assessment of following a specific standard, formulation of a standard information security policy, detail challenges in each of the policies and awareness levels are areas that are not discussed in depth in the research.

Bogale (2018) has proposed information security awareness program for Enat bank by reviewing existing awareness programs and practices. The researcher followed a quantitative research approach with case study methods. Findings of the study showed that information security awareness level of the bank's employees is unsatisfactory. The researcher proposed a comprehensive awareness program and good practices to be followed organization-wide in order

to strengthen the overall security posture and security vulnerabilities mitigation. Face-to-face and multi-media based awareness programs, and inexpensive tools such as posters, do and do not lists and warning banners are among the proposed information security awareness programs and techniques by the researcher. However, the research is limited to only one financial institution.

Yohannes (2018) also assessed Information Security Incident Management practices in an Ethiopian bank using qualitative case study research methods. Findings of the study revealed that the bank does not have a predefined and separate incident management plan; even though to some extent, it was compliant with international incident management standards, guidelines and procedures. In addition, the study's findings indicate that the bank never conducted incident management rehearsals and lack of awareness, lack of skilled and experienced incident handlers and advancement of security threats were identified among the major challenges. The research is limited to one bank and made limited discussion on how the identified challenges can be resolved. In addition, the researcher didn't propose information security incident management framework that suits to all Ethiopian banks.

2.6.3. International Works

Different foreign research works related with cybersecurity operation practices have also been reviewed in this study. Some of the related research works conducted by foreign scholars are summarized in Table 7 below.

Author	**Problems and objective of the study**	**Key findings**	**Observed gaps that require further study**
(Schinagl et al., 2015)	Developing a framework for Designing a Security Operation Center	Identified and defined the generic building blocks of a SOC design Developed effectiveness of a SOC measurement method	Doesn't address SOC Incident escalation process and funding mechanisms

(Onwubiko, 2015)	Developing Cyber Security Operations strategy to protect business and monitor security	Identified Cybersecurity Operations strategy and framework People, processes are key to CSOC	CSOC delivery model/methods not covered
(Michail, 2015)	Assess whether Security Operation Center goals & capabilities can benefit organizations' businesses	Well-managed SOCs can enable bring substantial business benefit & increase organizational performance	• The research is done on US SOCs • The research doesn't include for outsourced services • Doesn't include metrics for evaluating SOC performance
(Janos et al., 2018)	Assess security concerns and challenges of a SOC	With well-managed SOC, security concerns can be mitigated with different countermeasures Creating and operating a SOC is worthy and efficient	The countermeasures proposed doesn't include ways to mitigate new and future cyber threats
(Dempsey, 2011)	Develop an ISCM Strategy to enhance threat/vulnerability awareness and visibility	Defining, establishing, implementing, analyzing, responding and reviewing security monitoring program and strategy.	Doesn't cover the people and technology aspects of continuous security monitoring program

Table 7: Related Foreign Works

As shown in Table 7, different foreign researchers have tried to assess current best practices, benefits and gaps of security operations centers in different organizations by comparing it against international standards.

Schinagl et al. (2015) have pointed out in their research that there is no standard framework available in literature reviews and no clear scope or vision on SOCs. Hence, they have tried to develop a security operations framework by identifying and defining the building blocks of a SOC using a case study research design method. The researchers have consolidated the SOC building blocks into five functions i.e., the Intelligence or CERT function which exchanges cybersecurity information with the internal and external parties, baseline security function which handles the vulnerability assessment and compliance scans, monitoring function which proactively monitors security threats using SIEM, penetration testing function to determine how systems react to an attack and the forensic function who assist in collecting electronic evidence for law enforcement bodies. They have also emphasized the need to have shared SOC among multiple user organizations as there might be scarcity of skilled analysts and maintaining and tooling of separate SOCs is expensive and time-consuming process.

Onwubiko (2015) has tried to develop a cyber SOC framework as a means to protect organization's critical business operations, ICT systems and support Cyber Defense Strategy. The developed CSOC framework consists of Log Collection, Analysis, Incident Response, Reporting, Personnel and Continuous Monitoring. However, the SOC delivery model is not discussed in his research.

Michail (2015) has assessed whether Security Operation Center goals & capabilities can benefit organizations' businesses and found out that well-managed SOCs can enable bring substantial business benefit & increase organizational performance. However, the research is conducted in SOCs which are located in the US. In addition, the research doesn't include for outsourced services and metrics for evaluating SOC performance

Janos et al. (2018) assessed security concerns and challenges of a SOC and explained that with well-managed SOC, security concerns can be mitigated with different countermeasures and creating and operating a SOC is worthy and efficient. However, the countermeasures proposed in the research doesn't include ways to mitigate new and future cyber threats.

Dempsey et al. (2011) have developed an Information Security Continuous Monitoring (ISCM) strategy to enhance threat/vulnerability awareness and visibility into organizations assets. This strategy enables to provide support to implemented security controls with accordance to the risk tolerance and provide the necessary information to respond to risks. However, the research did not cover the people and technology aspects; which play a critical role in effective and efficient security risk monitoring.

2.6.4. Summary

The fundamental concepts related to Security Operations practices and threat including from local and foreign research works has been reviewed and discussed thoroughly in this chapter. Guidelines, international best practices and standards assessing security operation and continuous threat monitoring have been also presented in this literature review.

According to NIST (2014) cybersecurity framework has five core functions i.e., Identify, Protect, Detect, Respond and Recover. Moreover, this research predominantly focuses on detection and monitoring major functions of the SOC.

Thus, the SOC-CMM model is found suitable and effective in evaluating and measuring the SOC framework's effectiveness and efficiency as it is also derived from the NIST CSF.

Existing security operations frameworks in the reviewed literatures are contextual and are not customized for Ethiopian context. Contextual factors such as organizational, national and cultural constraints affect the design of such programs. There is also a local research gap in this area.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.1. INTRODUCTION

This chapter discusses the research methodologies used. The research methodologies used to develop the framework are Design Science and Qualitative research. This chapter also explains the different approaches and views in which these methodologies have been used and why the specific methodology has been selected to carry out the research.

The research uses Design Science Research Methodology (DSRM) to develop the framework for overall information systems security operations by taking into consideration the existing security operation practices, tools, skillset, effectiveness and gaps before trying to develop a viable and usable framework.

3.2. RESEARCH DESIGN

This research used DSRM (Design Science Research Methodology) to formulate the SOC framework which is widely used in Information Systems Research.

Design Science Research (DSR) methodology in the Information Systems field is a discipline in which new knowledge is produced by the construction and evaluation of artifacts such as software, composite systems of software, users and use processes and IS-related organizational methodologies and interventions Kuechler et al. (2012), models, frameworks, theories Hevner et al (2004). The fundamental principle of design-science research is that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artifact. Thus, design science research methodology addresses research through the building and evaluation of artifacts designed to meet the identified business need (Hevner et al., 2004).

Peffers et al. (2006) has stated that a common framework is necessary for DS research in IS and mental model or template for readers and reviewers to recognize and evaluate the results of such research. Accordingly, Peffers et al. (2006) has divided research in IS into six typical steps i.e., **i)** problem identification & motivation, **ii)** definition of objectives for a solution, **iii)** design and development, **iv)** demonstration, **v)** evaluation and **vi)** communication is used while developing the framework in this research.

Figure 7, below shows details of Design Science Research Methodology (DSRM) process model

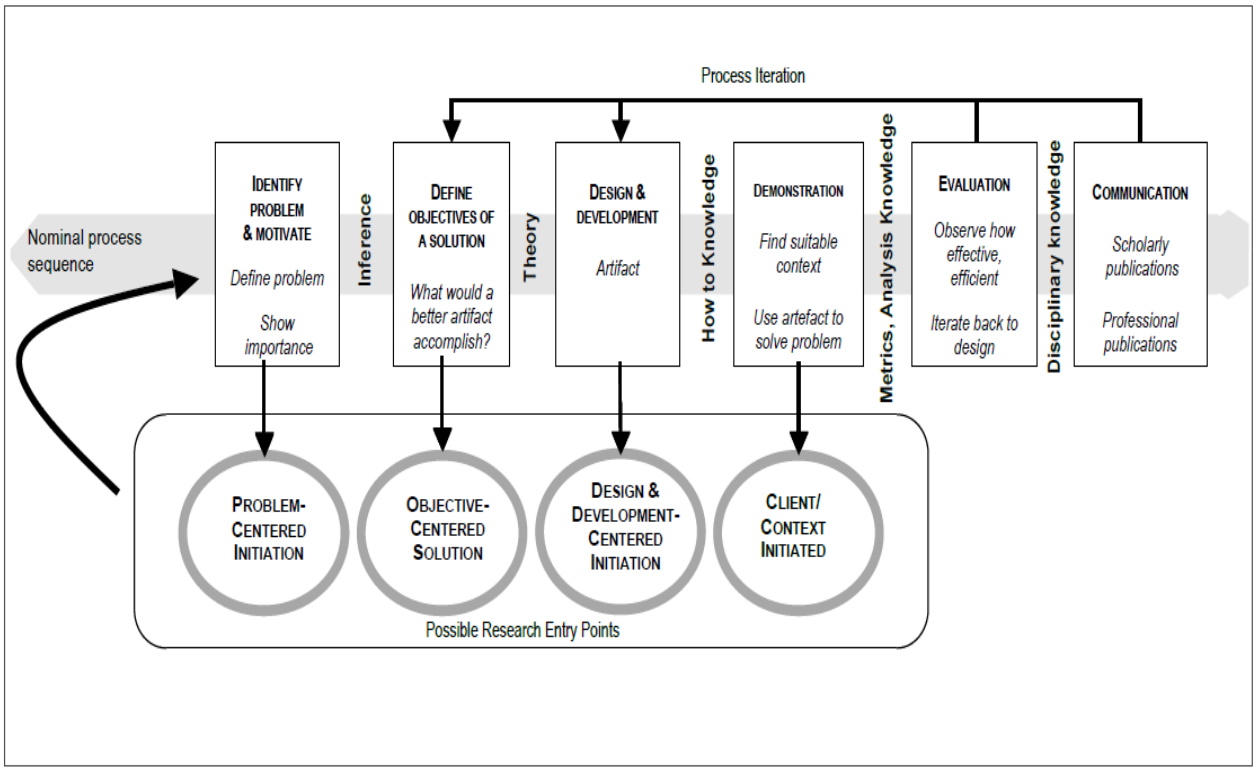

Figure 7:- Design Science Research Methodology Process Model (Peffers et al., 2006)

Thus, this DSRM process model has been followed to design a SOC framework for the Ethiopian banking industry to enhance proactive threat detection and monitoring as summarized in Table 8:

Processes/Steps	**Guidelines** (Peffers et al., 2006)	**Application of Design Science for: Designing of SOC Framework to Improve Information Security Continuous Monitoring**
Activity 1: Problem identification and motivation	Define the specific research problem and justify the value of a solution to develop an artifact.	Inadequate measures on proactive cyber-attacks, financial frauds monitoring and prevention in Ethiopian financial institutions
Activity 2: Define the objectives for a solution	Infer the objectives of a solution from the problem definition and knowledge of what is possible and feasible.	The specific research problem is to assess the current Security Operation practices, evaluate its effectiveness and design a SOC framework for the Ethiopian Banking industry to enhance proactive threat detection and monitoring.

Activity 3: Design and development	Create an artifact such as potential constructs, models, methods, or instantiations	The research project produced a practical artifact i.e., SOC framework design for the Banking industry in Ethiopia.
Activity 4: Demonstration	Demonstrate the use of the artifact to solve one or more instances of the problem	The threat detection and monitoring function of SOC framework will be demonstrated for its viability and effectiveness using an experimental approach to simulate and test it in a controlled environment.
Activity 5: Evaluation	Observe and measure how well the artifact supports a solution to the problem.	The designed SOC framework is evaluated against the objectives of the research versus the actual observed effectiveness of the framework using questionnaire and feedbacks from domain experts. The conceptual framework evaluation will iterate back to activity 3 until acceptable empirical evidence or logical proof is met to improve its effectiveness.
Activity 6: Communication	Communicate the problem and its importance, the artifact, its utility and novelty, the rigor of its design, and its effectiveness to researchers and other relevant audiences, such as practicing professionals, when appropriate.	The research will be communicated through various publication mediums including thesis. The work has also been presented to selected banking industry domain experts and received feedbacks using virtual meeting.

Table 8:- Designing of SOC framework using Design Science process model

3.3. PROBLEM IDENTIFICATION AND MOTIVATION

3.3.1. Motivation

The main motivation of conducting this study is the unavailability of a common security operations framework and references in the Ethiopian banking industry which is critical in designing and implementing efficient and effective SOC.

The other reason that goes hand in hand with the above motivation is the gaps observed in the Ethiopian banks in proactive security threat detection and monitoring. when it comes to securing their mission-critical services, a paradigm shift is required from reactive and firefighting-like

cybersecurity operation practices (such as incident management) to proactive security monitoring and prevention.

In addition, there is no local research done on designing a SOC framework; indicating the topic is open and with many problem domains to be addressed by this study and future researchers.

Moreover, Ethiopian banks who have limited budget to invest in building custom-made SOC tools might consider other options such as open-source solutions; as it enables them to have the necessary tools without spending huge amount of money or the need for sophisticated expertise.

3.3.2. Problem Identification

Design science begins its research process by identifying the problem the research needs to solve. Thus, the problems and challenges will be identified and discussed in this section.

As Ethiopian banks continued to expand their services through different digital channels such as ATM, POS, Internet and Mobile banking to enhance service-delivery and customer satisfaction; they also need to give equal attention to the concerns of exposure to cybersecurity threats. By implementing a standard SOC and proactive security threat prevention will enable them build trust and confidence among their customers. In addition, implementing international security standards and best practices will enable them to better prepare themselves by providing competitive and secured services before the financial sector open up to the rest of the world.

After the problems are clearly identified this paper showed the specific importance of the work by providing the solutions to the challenges. In order to come up with the solution, the researcher followed qualitative data collection instruments.

To fully understand and figure out the current security operation and threat detection practices discussions and questionnaire play critical role. The expert interviews and discussions with industry experts provides useful insights into the current SOC facilities being assessed and considered for this research. However, additional data that could have been gathered using onsite observation and inspection to the banks that have already implemented SOC was not possible due to permission issues. Thus, data into the current practices was collected using expert discussion by preparing questionnaires. The interview questions were designed based on SOC-CMM open standard which is used to measure the capabilities and maturity of a given SOC. According to Rob (2020) SOC-CMM is a SOC management tool that can be used to determine strengths and

weaknesses of the SOC. Furthermore, it provides a means for measuring growth of the SOC, thereby demonstrating the return on investment. The questionnaire adopted has been modified to include questions that were left out or were not included in the original model. The modification was made to include factors that were unique to the Ethiopian banking sector and also to cover the expertise part. The questionnaire was distributed and shared for the selected sample banks using E-mails and Telegram application. The questionnaire used has been attached in Annex-1 of this research for reference.

The researcher has used purposive sampling method to select the sample banks for expert-discussions.

In addition, document analysis has been conducted to assess and better understand the underlying cybersecurity issues in the Ethiopian banking industry. A document prepared by INSA (2020) which assesses the overall national cybersecurity landscape of the country's critical infrastructure, including financial institutions have been reviewed in this study.

3.4. DEFINING THE OBJECTIVES FOR A SOLUTION

Defining the objectives of the solutions is the second major step in Design Science Research Methodology process. In this stage, the study aims to identify the main requirements for developing a SOC framework and improving information security continuous monitoring. It tries to provide a way to show how the designed framework could be useful by enhancing the observed challenges after identifying and evaluating their relevance. Qualitative data is used to show how the proposed framework is expected to alleviate the existing gaps and challenges that were not considered by previous similar studies. After the required data is collected, analysis and interpretation are made using Qualitative data analysis method. Finally, thematic coding analysis technique is used to group the collected data based on the current categories of SOC design methods. Summarization of results of the qualitative data is made and presented accordingly to narrate and interpret the existing practices and situations.

3.5. DESIGN AND DEVELOPMENT

As per Design Science research, a viable and feasible artifact is developed in this phase. After problems and objectives of the research are clearly identified in the previous phases using different data gathering techniques such as domain expert discussions and document analysis and further

referring and reviewing international security operations standards and best-practices, a suitable framework is developed for the Ethiopian banking industry.

The developed framework shows each component with its corresponding functionalities to solve the identified challenges in designing SOC and security continuous monitoring. The framework is developed based on the three ITIL pillars i.e. People, Processes and Technology supported by key SOC definitions and typologies referred from literature reviews, international best practices and standards, inputs from domain expert discussions and from document analysis. Each of the components of the framework is discussed in detail in the consecutive chapters.

Microsoft Visio 2019 is used to design and draw the proposed SOC framework and architecture. In addition, Microsoft Excel have been used to illustrate the findings in graphs during the problem identification and discussion of results sections.

Besides SOC framework design, the main focus of this research is demonstrating the need for proactive security threat detection and monitoring. Thus, an open-source SIEM tool i.e., Security Onion along with Kali Linux, Windows 7 machines installed on Oracle VirtualBox virtual machine are used in this research. The Security Onion SIEM solution is used to demonstrate the need to continuously collect, detect and monitor security events occurring inside the banks' IT infrastructure by consolidating them into a single dashboard.

3.6. DEMONSTRATION AND EVALUATION OF THE FRAMEWORK

3.6.1. Demonstration of the Framework

This is a phase where the researcher shows the usability of the developed artifact or framework in solving the challenges of designing and implementing effective and efficient SOC.

Due to the findings and gaps observed in implementing a standard information security continuous monitoring and proactive threat detection practices in the banks assessed the research will focus on demonstration of one of the core functions of SOC i.e., threat detection and monitoring.

Thus, the artifact i.e., threat detection and monitoring is demonstrated using Security Onion installed on Oracle VirtualBox virtualization software to simulate a real-world proactive threat detection and mitigation scenario. Kali Linux, also installed on Oracle Virtual Box is used to

simulate the cyberattacks such as Nmap network scan, Zeus malware attack and gaining unauthorized access to an FTP server hosted on Windows 7 using Metasploit Framework exploit. Security Onion and Kali Linux are chosen as a demonstration tool for this study, because both are open-source software available for free and their ability to simulate real-world SIEM solution and by launching cyberattacks using the pre-packaged tools. After completion of the demonstration, the researcher showed that the each of the cybersecurity attacks launched from the Kali Linux tools are accurately detected and monitored. This is done using Security Onion's SIEM tools including log collection and threat detection tools found pre-installed on the Security Onion such as Sguil IDS, Squert and Kibana. These tools are very critical for the cybersecurity analysts in helping automate the detection, monitoring, analyzing and responding to security threats before they affect and disrupt mission-critical services and daily business operations.

3.6.2. Evaluation of the Security Operations Framework

Design science research relies upon the application of rigorous methods in both the construction and evaluation of design artifact. Hevner et al. (2004) describes different design evaluation Methods used in Design Science Research methodology which are summarized in Table 9 below. From these methods, the experimental approach is followed in this research to evaluate the artifact's utility and performance by comparing the objectives the research against the observed results in a controlled environment.

1. Observational	Case Study: Study artifact in depth in business environment
	Field Study: Monitor use of artifact in multiple projects
2. Analytical	Static Analysis: Examine structure of artifact for static qualities (e.g., complexity)
	Architecture Analysis: Study fit of artifact into technical IS architecture
	Optimization: Demonstrate inherent optimal properties of artifact or provide optimality bounds on artifact behavior
	Dynamic Analysis: Study artifact in use for dynamic qualities (e.g., performance)
3. Experimental	Controlled Experiment: Study artifact in controlled environment for qualities (e.g., usability)
	Simulation – Execute artifact with artificial data
4. Testing	Functional (Black Box) Testing: Execute artifact interfaces to discover failures and identify defects
	Structural (White Box) Testing: Perform coverage testing of some metric (e.g., execution paths) in the artifact implementation
5. Descriptive	Informed Argument: Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artifact's utility
	Scenarios: Construct detailed scenarios around the artifact to demonstrate its utility

Table 9:- Design Evaluation Methods (Hevner et al., 2004)

Moreover, the framework is evaluated to further check it suitability by presenting the it to selected domain-experts of respective banks using Zoom virtual meeting and collecting feedbacks.

3.7. COMMUNICATION

The research is communicated through various publication mediums including thesis. The work has also been presented to selected banking industry IT Security personnel. In addition, it will be communicated by producing journal articles and conference paper.

CHAPTER FOUR

PROBLEM IDENTIFICATION, OBJECTIVES AND DESIGN OF FRAMEWORK

4.1. OVERVIEW

Document analysis and domain-expert discussions have been conducted to understand the existing situation and factors affecting Ethiopian banks security operations and continuous security monitoring.

4.1.1. Document Analysis

According to INSA (2020) national cybersecurity assessment document in which it studied current cybersecurity situation, actors and next action plan; the financial sector is one of the critical institutions which could bring critical impact to the national economy and development. These financial institutions include all banks, insurance companies and microfinance institutions. According to the study, security assessment made on 14 of the 17 banks and associated payment institutions that work collaboratively with them; total of 224 vulnerabilities have been found in their 24 mobile banking applications and internet banking systems, out of which 111 vulnerabilities are categorized as high impact vulnerabilities.

The study added that Ethiopia has drafted five-year Digital Strategy that will enable the ICT industry to contribute its part to the national economy. International studies have pointed out that cybersecurity attacks will accelerate in high rate due to the increase in ICT usage by organizations and society and continued reliance on ICT by different economic sectors.

Thus, providing assistance to financial institutions establish 24x7 security monitoring and response capabilities is one of the short-term action plans put forward to counter the increase in cyberattacks. The long-term action plan is to create a financial sector which is capable of handling and preventing complex and sophisticated cyberattacks and who can contribute to national Cybersecurity Emergency Response Team (CERT) and cybersecurity forum.

The banking sector is categorized as high priority sector among the financial institutions as it highly relies on ICT to provide different banking services to the customers.

According to the document, the following short-term action plans have been made in seven Ethiopian private and government banks in order to strengthen their cybersecurity defenses:

- Providing security awareness training
- Preparing cybersecurity strategy and structure
- IT infrastructure and payment system security audit
- Deploying SIEM and other security solutions
- Cybersecurity awareness level and governance audit
- Connecting respective SOCs to national CERT center

As it can be inferred from the document analysis and the short-term action plans, almost all banks weren't connected to the national CERT center which enables them to get the latest security vulnerabilities and feeds and supporting them to protect their mission-critical assets from zero-day and advanced cyberattacks that are not detected by their local SOC analysts and tools.

In addition, even though SIEM solution is one of the most critical technologies that should be deployed in the SOC; the findings indicate that it is missing in some of the Ethiopian private banks. The SIEM solution enables security analysts to get real-time security alerts by analyzing logs collected from different sources including the IT infrastructure and payment systems. Thus, this shows that there is a major gap in proactive threat detection and monitoring which is one of the core SOC functions.

4.1.2. Expert Discussions

Selected discussion points have been prepared by the researcher prior to arranging discussion sessions with the cybersecurity domain experts of the respective banks. The discussion points have been customized based on SOC-CMM model with special emphasis given to the technology used, and processes as well as SOC team sections of the model. In addition, cybersecurity intelligence gathering practices, analyst skill-levels, management commitment and overall TTPs (Tools, Practices and Procedures) used have been discussed with the practitioners.

According to the discussions made the following findings and best practices have been identified that can be useful inputs during SOC design and implementations:

- Almost all banks have dedicated IT Security team who are responsible of overseeing the overall security of their respective banks. This might be partly due to NBE's encouragement of banks to establish IT Security structure in their governance.

- All banks have cybersecurity policies and risk management practices in place
- Some of the bigger banks with better resources have already implemented SOC equipped with SIEM and other cybersecurity monitoring tools.
- In addition, PCI-DSS compliance and certification is driving some of the banks to implement SOC solutions.

According to domain expert discussions made with IT Security officers and managers from public and private banks in Ethiopia; the following critical current security operations issues and gaps have been raised:

- Unavailability of SOC framework for the Ethiopian banking industry – there is no comprehensive cybersecurity operations strategy and overall framework that could serve as a reference and guideline while implementing standard SOC. Even though most banks have cybersecurity policy, it does not include in depth and detail discussions of security operations and tools to be used.
- Lack of continuous security monitoring – even though some of the bigger banks have invested in security solutions and SOC tools, they have no adequate security analysts that can monitor and respond to alerts on 24x7 basis.
- Inadequate automation and tools – one of the main SOC tools i.e., SIEM solution is expensive and requires robust time and resources to implement it. Only few resourceful banks are investing in implementing commercial SIEM solutions.
- Inadequate collaboration with local and international cybersecurity organizations – security operations require working closely with national and international cybersecurity organizations CERT organizations such as INSA, MITRE CK&ATT
- Lack of skilled cybersecurity analysts and professionals – SOC needs not only security monitoring tools but should be complemented by highly skilled cybersecurity analysts.
- Inadequate management commitment and awareness to invest in SOCs – management commitment is required in the implementation of an effective and efficient SOC staffed with skilled cybersecurity analysts.
- Ineffective communications and collaborations among SOC analysts and other IT departments – the SOC team should be able to communicate with other IT department such as CIRT, NOC, IT helpdesk, Service providers team to be able to function effectively. This

will enable them to get the latest updates about changes made to the IT infrastructure and have better understanding of traffic flow and detect anomalies or vulnerabilities easily. Impacts to the daily business and services of the bank should also be analyzed before applying fixes and patches to security vulnerabilities.

- Lack of adequate budget - required to acquire necessary SOC tools and recruit skilled SOC analysts.
- Lack of awareness about the national cybercrime law and legal processes – bank IT Security management and analysts should clearly know the details the Ethiopian computer crime laws and enforcement process such FDRE Negarit Gazette Computer Crime Proclamation No. 958/2016 in order to report incidents and successfully prosecute individuals involved in cybersecurity attack.

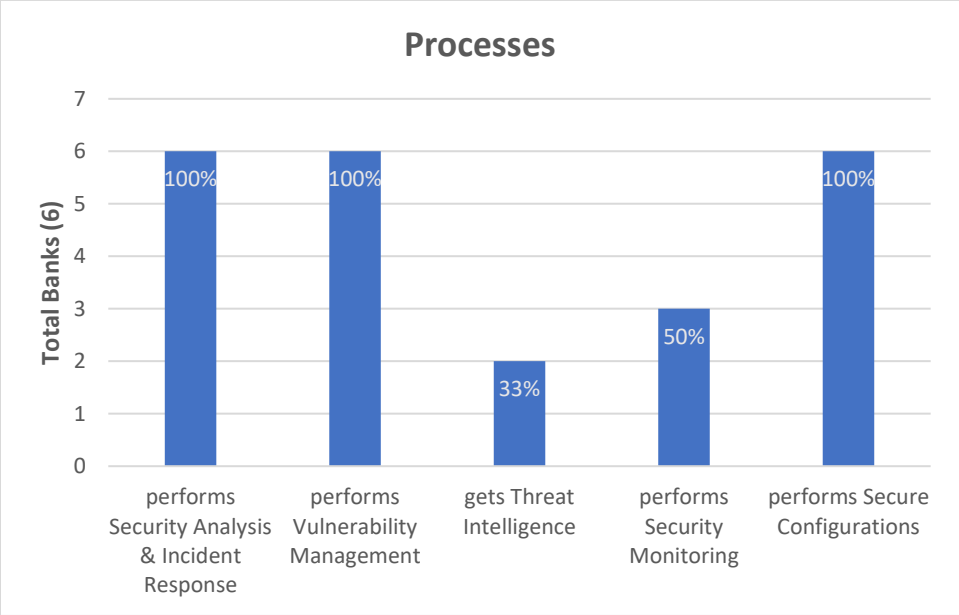

Figure 8:- Experts' discussion summary of SOC Processes

Figure 8, shows that only 50% and 33% of the assessed banks performs proactive security monitoring and gets threat intelligence respectively. However, the experts responded that they perform regular vulnerability management and secure configuration activities in their IT infrastructure. In addition, all of the experts responded they perform security analysis and incident

response activities whenever exceptional security violations and behaviors are observed in the IT environment.

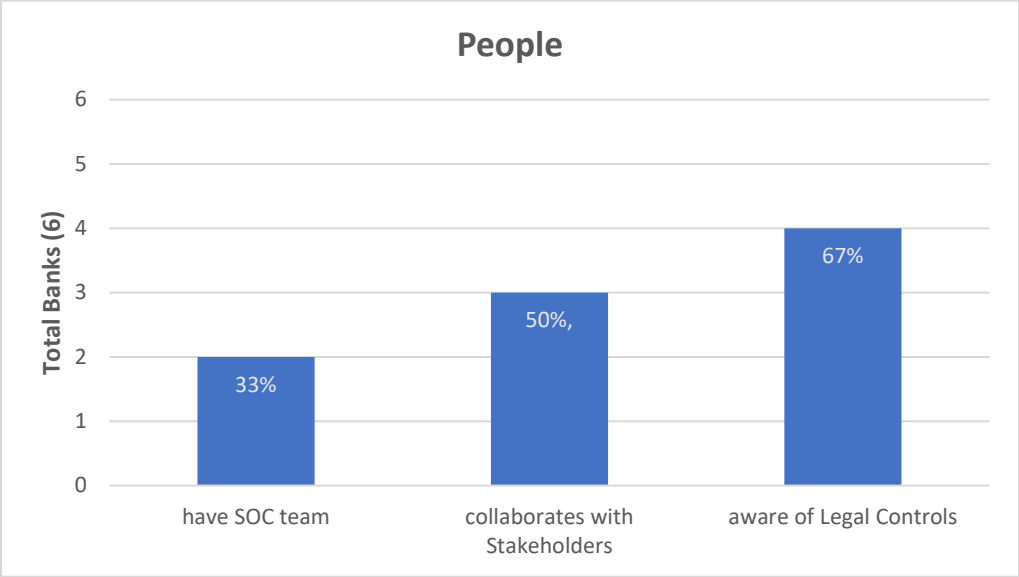

Figure 9:- Experts' discussion summary of SOC People domain

Figure 9 shows 33% of the assessed banks have dedicated SOC security analysts while 50% of them respond that they collaborate with internal and external stakeholders. In addition, 67% of the respondents have awareness about the national and international cybercrime laws.

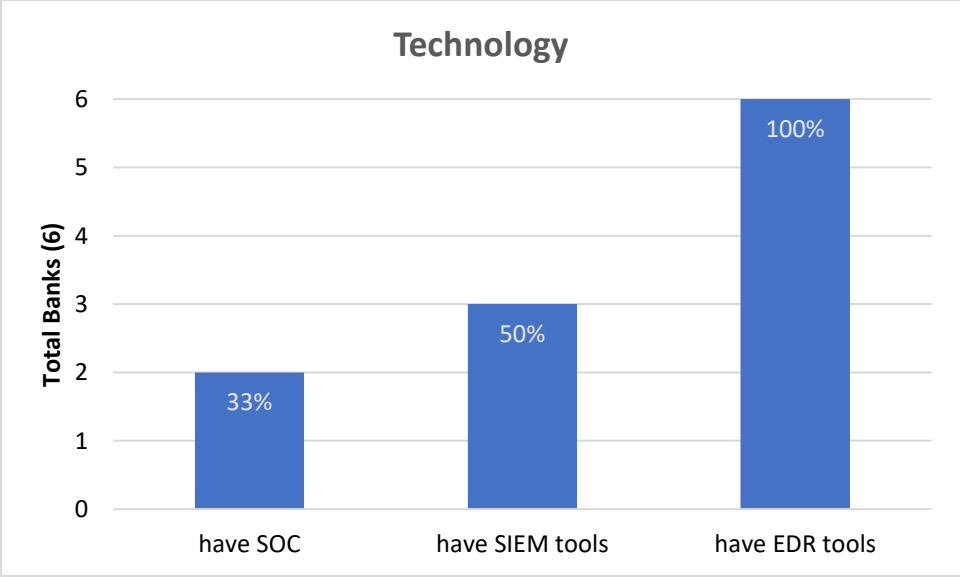

Figure 10:- Experts' discussion summary of SOC Technology

Figure 10 above, shows only 33% of the banks assessed have standard SOC facilities while 50% have implemented a SIEM solution and are performing proactive threat detection and monitoring. Moreover, all of the experts responded that their respective banks have deployed EDR (Endpoint Detection and Response) tools such as antivirus and other endpoint security posture assessment tools.

4.2. OBJECTIVES OF THE FRAMEWORK

The objective of this design is to formulate a Security Operations framework for the Ethiopian Banking industry to be used as a reference by the banking industry on how to plan, design, build and operate effective and efficient SOC to secure their mission-critical services from cybersecurity attacks and financial frauds. Major building blocks and components of the framework are also identified and discussed in this research. The designed framework will enable bank executives and Chief Cybersecurity Officers to make better decisions regarding the requirements for building a SOC in terms of expected functional objectives, budget and staffing requirements.

Implementing a standard SOC enables banks and financial institutions to:

- Improve threat management – in order to achieve maximum effectiveness, proactive threat detection and prevention technologies must be centrally consolidated and monitored in real time. Additionally, resources should be available to investigate and respond to suspicious activities and incidents.
- Reduce time-to-detect incidents – integrated monitoring gives security better visibility and enables the function to correlate patterns and detect suspicious activities. Effective detection and escalation of incidents and close coordination between teams improves response outcomes and response time.
- Centralize and consolidated security functions – consolidating security functions in a SOC can provide cost efficiencies while maximizing available expertise, skills and resources when an organization operates in multiple locations.
- Comply with regulatory bodies and laws – a SOC is often the operational model of choice for large and some midsize enterprises to meet regulatory requirements mandating security monitoring, vulnerability management or incident response functions.

Major gaps have been identified in implementing continuous threat detection and monitoring; indicating some banks does not have SIEM solution and the findings of 111 high impact vulnerabilities during the problem identification phase.

Thus, besides designing a SOC framework, improving proactive cybersecurity threat detection and monitoring practices in the banking industry is one of the main objectives of this research. Applying continuous information security practices enables the financial institutions in detecting and mitigation of cybersecurity attacks and frauds before the mission-critical banking services are disrupted or hacked; hence, enhancing trust and image building among their customers which are very crucial requirements in the banking business.

Thus, the objectives of the solution are as summarized below: -

- Develop a Security Operations framework for the Ethiopian banking industry by identifying the major components required for building effective and efficient SOC. The framework is intended to incorporate remediations to the gaps and challenges observed during the problem identification phases. The SOC is detrimental and foundation in proactively stopping and preventing cybersecurity attacks and financial fraud targeted at mission-critical banking assets and services from different types of actors with varying motivations.
- Identify suitable SOC model for the Ethiopian banking industry by taking into consideration budget and cybersecurity analyst limitations.
- Identify major SOC functions and services required to effectively secure banks' mission-critical services.
- The research objectives also focus on the evaluation and demonstration of proactive security threat detection through the implementation of continuous monitoring mechanisms rather than a reactive way of security threat mitigation i.e., incident management and recovery.
- Filling local research gap in this area of study and inspiring fellow researchers.

4.3.DESIGN REQUIREMENTS

In order to build a viable and usable artifact that meets Ethiopian banks cybersecurity operation needs and that achieves objectives of this research, a set of design requirements has been identified.

These requirements include technical as well as business goals. The business requirements include enhancing revenue and building customer trust by implementing highly secured and available banking services.

The technical design requirements considered in this research are based on the ISO/IEC 25000:2014 (2014) Software Quality Requirements Engineering, SQuaRE model for software quality. The ISO/IEC 25010 standard has extensive features that a quality software artifact should include. However, not all these features are applicable for SOC framework design, as the standard is mainly intended for software design and requirement elicitation purposes.

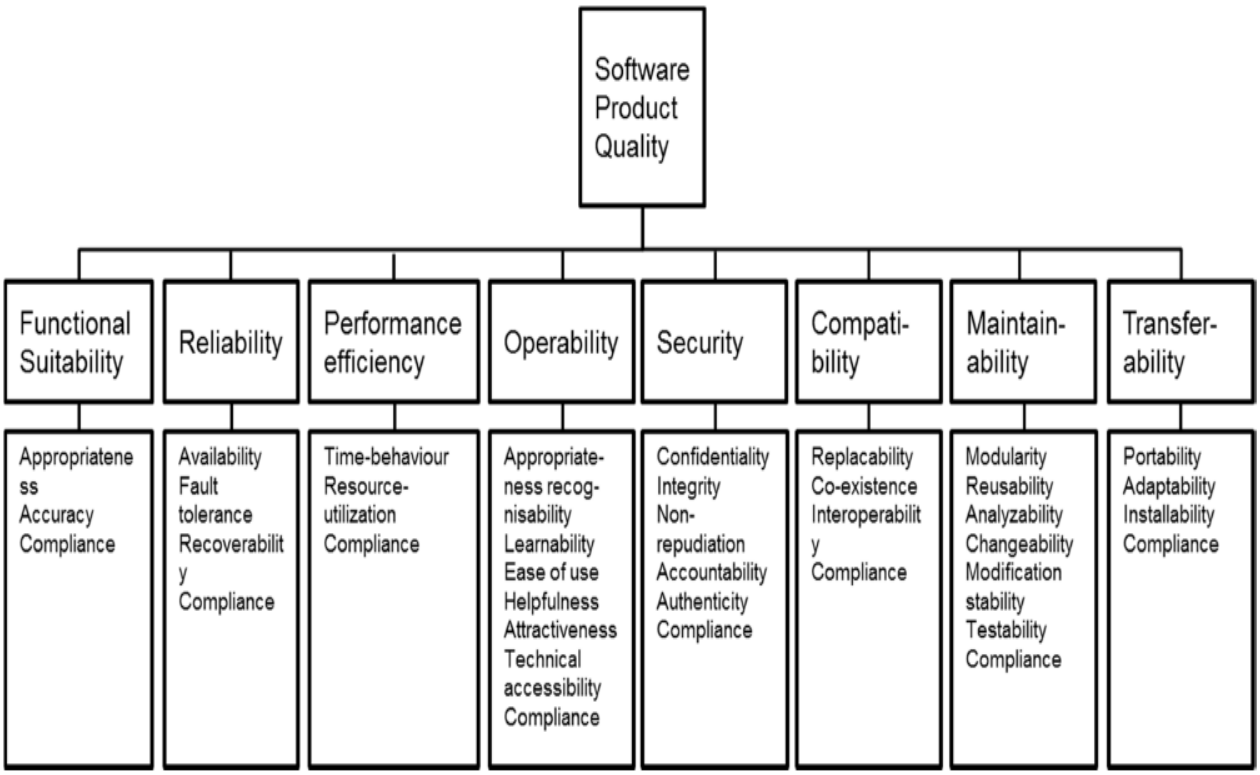

Figure 11:- ISO/IEC SQuaRE Model (ISO/IEC 25000:2014, 2014)

The researcher has discussed the following features of the SQuaRe model to be used as important inputs while designing the SOC artifact: -

Functional suitability

The appropriateness feature indicates how well the designed artifact is capable of performing its primary functions by determining the strengths and weakness of the designed SOC framework using maturity and capability levels. This feature is determined during the artifact demonstration phase of this research.

Accuracy is also an important aspect in determining the designed artifact's ability to prevent cybersecurity threats before critical systems are compromised.

Reliability

In this attribute, the designed artifact is required to be fault tolerant by limiting false positives while detecting cybersecurity threats.

Performance and efficiency

The performance of the artifact depends on the effectiveness and efficiency of the SIEM system and SOC analysts' skills in detecting and stopping threats.

Operability

Several aspects within the operability quality area apply to the artifact the ability to recognize appropriateness of security alerts and incident response. In addition, the artifact should be easily learnable and straightforward in using and guiding SOC analysts in using the SIEM solution. Ease of use of the SOC tools is also goes hand-in-hand with the learnability parameter. For this purpose, Graphical User Interface based monitoring tools are also used while demonstrating the artifact. Attractiveness of the SOC tools is also critical to easily perceive and visualize the security alerts. In this case, the Security Onion SIEM tool displays alerts in attractive formats including graphs.

Security

The main function of artifact is to ensure confidentiality, integrity and authenticity of in collaboration with other security technologies and tools. In order to ensure confidentiality of logs and data collected by the SIEM solution secure protocols should be used and should also be encrypted to prevent tempering. Connectivity with central Network Time Protocol (NTP) servers

should be properly authenticated using password. Strong encryption and hashing algorithms should also be used to secure communication with the time server.

Compatibility

The tools used while designing a SOC should also be interoperable with the existing IT infrastructure and payment systems so that logs can be pulled and correlated to detect and prevent security threats. International standards and practices have been used to design and demonstrate the compatibility of the various SOC tools and processes with the existing commonly used IT systems. Standards such as NIST and ITIL have been used in designing the framework.

Maintainability

The designed artifact should also be simple to maintain by modularizing the main functional components to accommodate additional services and technologies when required. The framework is designed in a modular way based on People, Processes and Technology components. The artifact is also designed in a way that can be reused and adopted by all the financial institutions in Ethiopian including other organizations with mission-critical infrastructure that needs to be protected from cybersecurity threats by building standard SOC services.

4.4. PROPOSED SOC FRAMEWORK FOR THE BANKING INDUSTRY

This framework aims to be useful and relevant to public and private banks in Ethiopia by formulating a security operations baseline that solves the specified gaps and challenges and meets objectives of the research. The designed framework is expected to be used in implementing and maintaining effective and efficient Security Operations strategy. In addition, it is required to enhance and to fill the observed gaps observed during the problem identification phase.

Accordingly, the framework is designed based on: -

- Gaps observed from the problem identification phase of this study i.e., unavailability of SOC framework, unsatisfactory collaboration with local and international CERT, inadequacy of awareness about cybersecurity laws and regulations, unavailability of monitoring tools and the increase in undetected vulnerabilities in the assessed banks.

- Design requirements specified in section 4.3
- Literature review, international best practices and standards used in SOC i.e., hardening & Secured configurations, monitoring, penetration testing, forensics & security incident management.
- Required SOC tools and techniques to proactively monitor security information and events
- Gaps observed in accessing and collaboration with national and international threat intelligence feeds and advisories

In addition, ITIL framework has been used to divide the SOC framework into 3 major domains i.e., the People, Processes and Technology domains for ease of understanding and clarity.

The services and functions provided by the SOC are included in the Processes domain. This SOC services identified from literature review and industry standards and best practices have been further categorized into the following main technical and operational functions:

1. **Hardening and Secured Configurations –** Secured configuration and development
2. **Threat Intelligence –** Threat and vulnerability feeds/Advisories
3. **Forensics –** Incident Management & investigation
4. **Penetration Testing –** periodically test and patch loopholes and vulnerabilities
5. **Detection and Monitoring** – Log Collection, Detection and Analysis

Thus, the application of ITIL pillars to design this SOC framework, implementation models (presented at the end of this section) and the introduction of legal control are new to this research, that has been added and customized based on the observed gaps in the problem identification phases.

Based on the above inputs from the problem identification phase, design requirements, literature reviews and assessment of international standards and best practices, the below SOC framework is designed and proposed for the Ethiopian banking industry. The detail definitions and roles of each of the framework's components are also discussed in subsequent sub-sections.

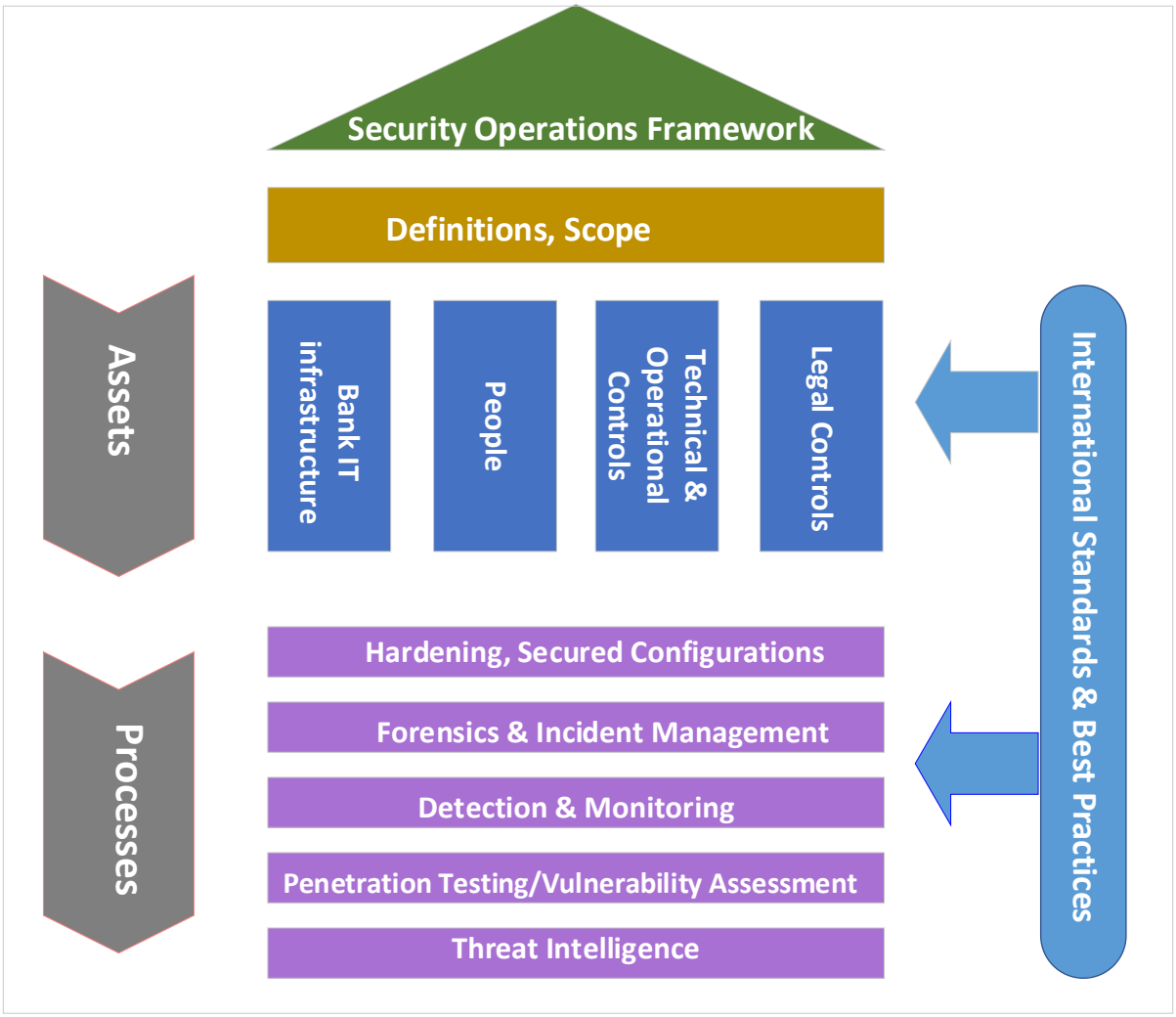

Figure 12:- Proposed Security Operation Framework

Successful adoption of the framework depends upon effective and efficient cross-domain interaction to deliver value and service within the SOC.

According to Davis (2004) the entire or partial loss or compromise of the critical national infrastructure can cause large-scale loss of life, serious implications on the national economy and grave social consequences for the community and be of immediate concern for the national government. As financial institutions are part of the Critical Information Infrastructure (CII) ensuring and protecting the banking and financial services should be one of the top priorities.

The assets part in the proposed design includes both people and the technology in the Ethiopian banking industry.

4.4.1. Technology

The technologies used in the Ethiopian banking industry include different IT infrastructure and cybersecurity systems. The SOC is part of the cybersecurity solutions that should be implemented to protect the critical IT infrastructure from attacks by continuously monitoring for malicious intrusions.

- Core banking systems
- Payment Applications Systems such as Switch Systems, Internet Banking, Mobile Banking, International Money Transfer Organizations
- Network Infrastructure extending from the HQ to Branches, Third-Party networks and Agents
- Process automation application systems such as HR Management System, Finance & Budget Management Systems, etc.
- System infrastructure Active Directory, Antivirus, Email, File Sharing, etc...
- Telecommunication links such as Data, Internet and USSD gateways
- Data Center facilities such as Air conditioner, Door Access Control, CCTV, Fire Suppression, Electric Power Systems
- NOC, ticketing and support systems
- Security products, SOC

General SOC Tools

A small SOC could start to operate with SIEM tool only. However, as the size and complexity of the IT environment increase, additional tools, especially those providing visibility become necessary to allow the SOC to effectively provide its services. Table 10, summarizes general SOC tools that are most commonly used in modern SOCs that are divided into three categories i.e., visibility, analysis, action and management (Chuvakin et al., 2018).

	Tool	**Typical Use**
Visibility	• EDR	• Investigation of alerts related to endpoints or indicators coming from threat intelligence

		• Also used as a hunting tool, and sometimes as a primary threat detection tool on the endpoints
	• Network traffic analysis (NTA), network forensics tools and other network visibility tools	• Investigation of alerts and obtaining additional context about suspect activity in the network • Also used as a hunting tool • Occasionally, network flow collection tools may be used in place of full Layer 7 packet capture tools; flows may also be collected inside a SIEM
	• VA tools	• Identifying existing vulnerabilities in the environment • Used for vulnerability management or just for additional context for monitoring as well as asset inventory
	• Cloud access security broker (CASB)	• Delivering threat detection, cloud service discovery and overall visibility for cloud, primarily in the form of SaaS, but increasingly infrastructure as a service (IaaS) environment as well
Analysis	• SIEM	• Used to consolidate and correlate events and logs coming from different technologies and sources, generate alerts to be investigated, or report on suspicious or privileged use activities • Provides a single point to search log data and can be used for investigations and hunting activities

		• The SIEM is often seen as the primary tool for a SOC
	• User and entity behaviour analytics (UEBA)	• Used to identify suspicious behaviours by users and other entities • Can be used as a source of alerts, a means to refine and enrich alerts or to provide context for the SIEM
	• Malware analysis and sandboxing	• Used for investigations when suspicious software is identified in the environment • Access to a set of cloud sandboxes may also be used
Action and Management	• Security orchestration, automation and response (SOAR)	• Supports monitoring and response workflows, case management and automation, response and triage orchestration, and reporting • Enables security operations teams to automate and prioritize security operational activities and report data to inform better business decision making
	• Threat intelligence platform (TIP/SOAR)	• Used to facilitate collection, consolidation, refinement and sharing of TI (Threat Intelligence) • A threat intelligence platform (TIP) may be used by a SOC • As TIP capabilities are increasingly being incorporated into SOAR, organizations may opt to rely on the SOAR tool for this function
	• Collaboration and Unified communications	• Used to facilitate communication and interaction between SOC personnel

		• Some SOCs will use simple chat rooms to allow communication and collaboration, but more mature environments may integrate these tools with SOAR and other technologies, such as chatbots, allowing interactive and ad hoc incident investigation, response, and TI consumption and sharing

Table 10:- General SOC Tool Categories (Chuvakin et al., 2018)

While both SOAR and SIEM platforms aggregate data from multiple sources; SIEM systems collect data, identify deviations, rank threats and generate alerts while SOAR solutions handle additional tasks and capabilities such as integrations with wider internal and external security and non-security applications. In addition, SOAR platforms use automation, AI and machine learning to provide greater context and automated response to threats. However, it should be noted that both systems are not a replacement for human security analysts, but instead augment their skills and workflows.

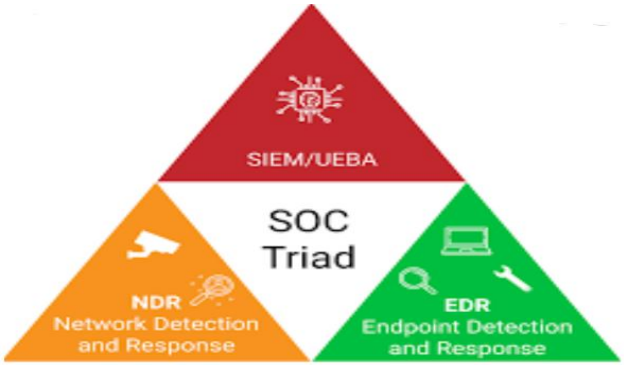

Figure 13:- Gartner SOC Visibility Triad

4.4.2. People & Stakeholders

The bank management and executives are considered as the primary stakeholders as they are responsible for the allocation of the required resources and personnel to drive this initiative along with CISO, Security Managers and Security Officers adopting this cybersecurity Operations Framework.

Governmental Cybersecurity and CERT (Cyber Emergency Response Teams) agencies such as INSA, NBE, local and international security solutions suppliers are also some of the stakeholders in the Security Operations in the Ethiopian Banking industry.

Hackers, the threat landscape and customers have also to be taken into consideration while designing the framework.

SOC Team Composition

The SOC team roles and required skills are directly related to the services and functions performed by the group. If the SOC is responsible for vulnerability management, for example, it is expected to have staff performing VAs and VA tools. The staff model below assumes that the SOC will focus on core detection and response tasks.

As security monitoring is the core function of the SOC, most common roles are related to this process. Many organizations with traditional SOCs have the monitoring team split into at least two levels:

- Level 1: These less-skilled SOC analysts usually handle basic alert triage and are the initial contact of the SOC via telephone, email or other workflow tools. This is the most important role to be structured in a 24x7 manner. Different techniques and best practices should be used to analyze the most frequent tasks of the L1 analysts and to automate them via SOAR tool playbooks.
- Level 2: These are usually more skilled SOC analysts who perform investigation and response to alerts handed off by Level 1 analysts. Some organizations may prefer to assign the Levl 2 analysts “on call” basis in order to keep basic 24x7 operations to save expenses for the more skilled and more expensive analysts.

Other optional SOC roles may include:

- SOC team manager – responsible for defining and managing analyst shifts to keep continuous SOC operations

- Threat Intelligence analyst – responsible for consuming and eventually producing threat intelligence and providing guidance to the other roles on changes required to adapt to threats that are relevant to the organization.
- Incident Response – organizations that include IR as part of the SOC would add roles related to the CIRT to the SOC team. IR is sometimes represented as Level 3 SOC personnel/analyst.

Skills shortage is one of the most challenging issues for building an effective and efficient SOC. Appropriate compensation, such as retention incentives, training, benefits and workload management, including shift assignments, are also critical to retaining SOC analysts.

Some banks may also prefer to work with IT and security vendors such as MSSPs (Managed Security Services Providers), MDR (Managed Detection Response) providers, consultants, integrators and so forth to outsource certain security operation functions.

4.4.3. Processes of Security Operations Framework

Key processes of the Security Operations Framework include Secure Configurations and Hardening, Forensics & Incident Response Management, Security Intelligence feeds & advisories, Penetration Testing, Monitoring and Analysis.

In addition, NIST (2014) has identified five cybersecurity core functions which are Identify, Protect, Detect, Respond, and Recover.

Identify – developing the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Protect – developing and implementing the appropriate safeguards to ensure delivery of critical infrastructure services. This function supports the ability to limit or contain the impact of a potential cybersecurity event.

Detect – developing and implementing the appropriate activities to identify the occurrence of a cybersecurity event. This function enables timely discovery of cybersecurity events.

Respond – developing and implementing the appropriate activities to take action regarding a detected cybersecurity event.

Recover – developing and implementing appropriate activities to maintain plans for resilience by restoring services that were impacted by a cybersecurity event.

However, processes involved in the detection, response and recovery complemented by threat intelligence advisories are the main focus of this research.

Detailed discussions of each of the security operations functional components and processes i.e., Log Collection, Analysis and Response as identified by (Onwubiko, 2015) are presented as follows:

i. Log Collection

Log collection is an essential aspect of the security monitoring. Without events logs it will be challenging to detect when an asset is compromised, or when an attempt or intrusion is carried on the asset. A good SOC ought to have very low false positives if the monitoring is tuned, trained and baselined appropriately (Onwubiko, 2015).

Thus, we need to configure all of the IT infrastructure in the bank such as workstation, network devices, application systems, etc. to send logs to a central repository. In addition, all devices are required to synchronize with centralized NTP (Network Time Protocol) server so that we can have consistent time source across all IT infrastructure. This will be helpful during event investigation and correlation as all events have corresponding timestamps.

Logs can be collected through a number of mechanisms or protocols such as Syslog (IETF 5424), SNMP (IETF 5343), traffic flow (i.e., netflow), streaming data, such as Packet Capture (PCAP), DPI (Deep Packet Inspection) and Audit log (logs produced when system audit policy is enabled).

Logging levels should be also configured appropriately according to the risk level and security sensitivity of (Syslog RFC5424, 2015) – Logging Levels.

ii. Analysis

After collecting the next most critical functions in Security Operations monitoring is the Log Analysis.

Log Analysis can be done through different ways including manual, semi-automated, fully automated, and hybrid methods. Manual analysis is performed by security analysts without relying on technology while Automated analysis makes use of full use of technology to analyze security events and logs without human intervention. Hybrid analysis is fully automated analysis combined with human decision making (security analysts) in the loop. This analysis method is suitable and recommended for protecting and continuous monitoring of security in the banking industry. Automated log analysis uses technologies such as Security and Event Management (SIEM) systems such as RSA Analytics, QRadar, HP Arcsight, AlienVault, Security Onion etc. to normalize, correlate and analyze data (structure and semi-structured data) swiftly. The latest technologies employ non-signature based systems such as machine learning and algorithms to detect anomalies and stealth events.

iii. Monitoring

Security events monitoring are performed by security analysts and operators 24x7. The security monitoring can be automated to trigger an alert and display or forward it to security analysts when an incident or attack occurs.

iv. Response

Incident response is one of the main functions of security operations which ensures incidents are contained or mitigated as there is no guarantee security breaches will not occur regardless of how much we have invested in securing our critical systems. Thus, every financial institution should have mature incident response plan in place which will enable it to resume its banking services with minimal disruption after a security breach.

A typical incident includes:

- Traffic originating entity (source IP address of event or group of events),
- Entity name (hostname, fully qualified domain name),
- Traffic type (RDP, SSH, FTP, HTTP, HTTPS, TLS, SSL etc.),

- Protocol (TCP/UDP)
- Payload information,
- Suspected attack payload / attack vector (provided by the log source that raised the alert, e.g., known signature or heuristics),
- Target asset (IP address of the target endpoint), and occasional the
- GeoIP location1 information (this is geographic information associated to the origin of the source IP address used in the attack. E.g., IP address originating from a country/city)

While most of the cyber incidents can be handled by the local security operations team, exceptional cyber-attacks that are beyond the team's skills and expertise requires seeking the assistance of national CERT agencies like INSA or other international cyber security institutions.

Vulnerability Assessment/Penetration Testing

Penetration testing/vulnerability assessment is one of the key SOC functions that is responsible for evaluating and reviewing an information system if it is susceptible to any known vulnerabilities, assigning severity levels and recommends remediation actions accordingly. According to NIST Special publication 800-40 by Mell et al. (2013), patch and vulnerability management duties and activities include:

- Create a System Inventory – to maintain inventory of hardware equipment, operating system and software applications used within the organization.
- Monitor for vulnerabilities, remediations and threats. Vulnerabilities are software flaws or misconfigurations that can be exploited by malicious entity to gain unauthorized access. Threats are attacks that exploit vulnerabilities such as exploit scripts, worms, viruses, rootkits and Trojan horses. remediation: installation of a software patch, adjustment of a configuration setting, and removal of affected software. There are several types of resources available for monitoring the status of vulnerabilities, remediations, and threats. The most common types of resources are vendor website, third-party websites, newsgroups, vulnerability scanners and databases, enterprise patch management tools and other notification tools.

- Prioritize vulnerability remediation – to determine the significance of the threat or vulnerability with a focus on systems that are essential for the operation. In addition, determining the extent of damage caused and the risks involved while applying the patch and non-patch remediation are the main tasks in this phase.
- Test and deploy remediations – test patches and non-patch remediations on IT systems that use standardized configuration management. Downloaded patch should be checked against authenticity methods vendors provide using cryptographic checksums, PGP and digital certificates. In addition, patches should be scanned for viruses before installation and tested on non-production systems to avoid unintended consequences. Remediation can be deployed in the form of security patch installation, adjustment of configuration setting and removal of the affected software using enterprise patch, update and configuration management tools.
- Verify vulnerability remediation through vulnerability scanning and penetration testing using either network scanners or host vulnerability scanners.

Forensics and Incident Management

Some organizations operate incident response activities from a group separate from the SOC. This unit is usually called Computer Incident Response Team (CIRT). There are advantages and disadvantages of merging IR and SOC functions into one unit.

Advantages of IR as a part of the SOC team includes tighter integration between detection and response, reduced resource requirements and more options for career progression and job rotation. On the other hand, the disadvantages are overlapping duty issues when investigating alerts related to SOC personnel, lack of independence while identifying issues related with initial alert handling by the SOC and makes IR complex to outsource.

However, when IR is handled by a separate CIRT team, the advantages are independence of investigating incidents involving SOC resources, easier to outsource SOC monitoring function as IR activities are handled separately. The disadvantages of this option are that it requires duplication of effort and resources and reduces career progression options within the SOC.

Regardless of where the IR function resides, the interaction between it and the monitoring function is a defining factor for SOC success. They need to work collaboratively continuously.

The forensics function consisting of forensics team and specialists largely focuses on assisting during the incident response stages by finding the ground truth and evidence of an intrusion.

Threat Intelligence

Large organizations usually have separate Threat Intelligence function apart from the SOC and CIRT functions with main duties involving threat database creation and consumption. This enables to inform the SOC team about the latest threats, techniques and vulnerabilities which in turn will be used to design defensive tools and detection strategies accordingly.

Technical and Operational controls

The technical and operational measures include security operations activities that will enable the banks proactively monitor and prevent cyber-attacks and frauds. Some of the measures include:

- Standards and best practices from other countries' banking industry and financial services
- Comprehensive security configurations and incident response management plan
- Continuous training and capacity building to security officers and analysts
- Cooperating with national and international threat intelligence centers

Legal Control

The framework should also take into consideration national and international cybercrime laws and regulations to facilitate effective and efficient security operations. Thus, security officers and analysts should keep custody of cybercrime evidences properly, which will help prosecute hackers and cybercriminals according to the national and international law.

4.4.4. Proposed SOC Model

Each SOC has a unique design and implementation. Since no generally accepted framework exists, each SOC is formed through organic growth. The effectiveness of each SOC is based mainly on executive commitment. Without such commitment, competent resources and sufficient budgets, a SOC can provide security in name only (Schinagl et al., 2015).

According to Gorka et al. (2018) published by one of the leading global research and advisor firm i.e., Gartner; have summarized the typical SOC implementation forms as shown in Table 11 below:

SOC Model	Attributes	Typical Adopter
Virtual SOC	• No dedicated facility • Part-time and geographical distributed team members • Reactive, activated when a critical alert or incident occurs • Primary model when fully delegated to an MSSP	Small to upper-midmarket organizations
Multifunction SOC/NOC	• Dedicated facility with a dedicated team performing not just security, but some other critical 24x7 IT operations from the same facility to reduce costs	Small, midsize and low-risk large enterprises where network and security functions are already performed by the same, or an overlapping, group of people and teams
Hybrid SOC	• Dedicated and semi-dedicated staff, either internally or externally • Security operations can be performed by the organization's • Security operations can be performed by the organization's internal staff 24 hours per day, 7 days a week; 8 hours per day, 5 days a week; or 8 hours per day, 7 days a week with some responsibilities offloaded to an external provider • Control of processes and effectiveness will vary according to how much stays inside vs. how much goes to the external provider	Small to midsize Enterprises
Dedicated SOC	• Dedicated facility	Large enterprises, service

	• Dedicated team • Fully in-house • 24/7 operations	providers, high-risk organizations
Command SOC	• Coordinates other SOCs • Provides threat intelligence, situational awareness and additional expertise • Rarely directly involved in day-to-day operations	Very large enterprises and service providers, governments, military, intelligence

Table 11:- SOC Models (Gorka et al., 2018)

Dedicated SOC is proposed as the best model for the Ethiopian Banking industry as they are considered as large enterprises with branch offices ranging from hundreds to thousands spread across different regions of the country. In addition, Ethiopian banks are considered as high-risk organization as they are involved in financial services sector which is highly exposed to fraud and cyber-attacks.

However, banks who have limited resources and budget constraints can choose to establish a command SOC/Shared SOC. INSA with collaboration with Ethiopian central bank i.e., NBE are planning to establish a shared SOC that can be used by all Ethiopian financial sectors. EthSwitch S.C, which is the National Payment operator interconnects all of the Ethiopian banks; is chosen to be managing the Shared SOC. This SOC model will enable smaller banks to have a SOC at significantly less budget and expenses than building their own dedicated SOC.

CHAPTER FIVE

DEMONSTRATION AND EVALUATION

5.1.OVERVIEW

The designed artifact requires further demonstration and evaluation to prove its suitability and usability in solving real world problem. Thus, the designed SOC framework is demonstrated and evaluated so that it can be adopted by the Ethiopian banking industry to build and operate effective and efficient SOC solutions.

Some of the major gaps identified during the problem identification phase of this research include: SIEM solution not implemented in some banks, findings of high impact vulnerabilities that were not detected by respective banks and inadequate budget allocations for building standard SOC that is equipped with the necessary technology and skilled professionals.

In addition, threat detection and monitoring plays key role in preventing cybersecurity threats proactively. With all the technical and procedural measures in place, financial institutions cannot guarantee security. Thus, complementing security controls with continuous threat detection and monitoring practices greatly enhances the overall security posture and effectiveness. The continuous threat detection and monitoring activities should also be supported by national CERT centers and other trusted threat intelligence feeds to be able to get the latest vulnerabilities and exploits.

Hardening/Secure Configurations, Penetration Testing/Vulnerability Assessments and Threat Detection/Monitoring are the SOC functions that are useful in proactively preventing security attacks. The first two functions are frequently addressed and mentioned as part of security controls in different studies; whereas the later getting inadequate attention by practitioners and researchers. Other functions of the SOC such as Forensics and Incident Management are reactive in nature, which are ineffective in preventing security breaches from happening.

Prioritizing proactive threat monitoring and prevention over reactive i.e., incident management practices enable banks to maintain their reputation and build strong trust among customers which are key requirements in sustaining the banking business.

Thus, one of the core functions of SOC i.e., threat detection and monitoring is demonstrated in this research along with threat intelligence; to fill the major gap observed during the problem

identification phase as well as to emphasize the need for proactive cybersecurity threat prevention.

In addition, the three major domains of the SOC framework, i.e., People, Processes and Technology are implicitly demonstrated, while demonstrating the threat detection and monitoring Process of the SOC function. The threat detection and monitoring (**Process**) demonstration has used a SIEM tool (**Technology**) to proactively detect and monitor security threats and a security analyst (**People**) takes action to remediate the security vulnerability.

5.2. DEMONSTRATION

Demonstration is practical exhibition and explanation of how an artifact works and is performed. To demonstrate the adopted framework, open-source SIEM tool called Security Onion is used in this research. Security Onion is leading open-source operating system for network security monitoring, IPS, log management and threat hunting.

This SIEM tool is installed on Oracle VirtualBox virtualization software to collect logs and monitor security alert in real-time. To perform these tasks, the SIEM tool uses the various tools found integrated in it such as Kibana, Squert, Sguil and Snort IDS rules. Kali Linux is also used as part of the demonstration to generate security attacks, capture the alerts in real-time by the Security Onion SIEM tool.

The above tools were selected because of their ability to simulate a real-world log aggregation, analysis and detection of security alerts. It also allows to visualize security alerts in an aggregated way using different graphs in a single dashboard.

The major Security Onion tools and packages that are used for demonstrating the framework include:

- **SNORT** – Security Onion can be integrated with Intrusion Detection System such as Snort which enables custom-rules and signatures configuration.
- **KIBANA** – is an open-source data visualization and exploration tool used for log and time-series analytics, application monitoring, and operational intelligence use cases. It offers powerful and easy-to-use features such as histograms, line graphs, pie charts, heat maps, and built-in geospatial support.

- **SGUIL** - is a collection of free software components for Network Security Monitoring and event driven analysis of IDS alerts. Sguil is built by network security analysts for network security analysts.
- **SQUERT** - Squert is a web application that is used to query and view event data stored in a Sguil database (typically IDS alert data). Squert is a visual tool that attempts to provide additional context to events through the use of metadata, time series representations and weighted and logically grouped result sets. The hope is that these views will prompt questions that otherwise may not have been asked.
- **CyberChef** - Used by cybersecurity analysts to perform various tasks tools while scanning vulnerabilities in Web Applications

In addition to the above Security Onion tools the below tools and operating systems are used to demonstrate the framework:

- **Oracle VirtualBox –** is used to simulate the entire demonstration used in this research by creating three Virtual Machines i.e., Security Onion VM, Windows 7 VM and Kali Linux VM.
- **KALI LINUX** – which is designed for digital forensics and penetration testing will be used to simulate attacks using some of its more than 600 pre-installed powerful penetration testing tools such as Nmap, Metasploit and Wireshark. In this research, Metasploit will be used for ethical penetration testing purposes in a simulated virtual environment to attack the Windows 7 workstation, which generates security alerts on the Security Onion SIEM tool. In addition, network scans and TCP replay attacks will be performed on the Windows host machine. Network scans are usually conducted by cyber hackers to gather network information such as IP addresses, ports and version information before launching sophisticated attacks. TCP replay attack also known as playback attack is also a form of is a type of man-in-the-middle attack; in which data is re-transmitted in a malicious way by intercepting it. Zeus malware attack has been also been used as part of the demonstration of real-time security threat detection and monitoring. In real-world scenario where SOC facilities are properly implemented, the security analyst will take appropriate response to remediate the security alert immediately upon detection of the event.

- **Windows 7 Machine –** is used as a target machine to demonstrate the different security exploits using the Kali Linux.

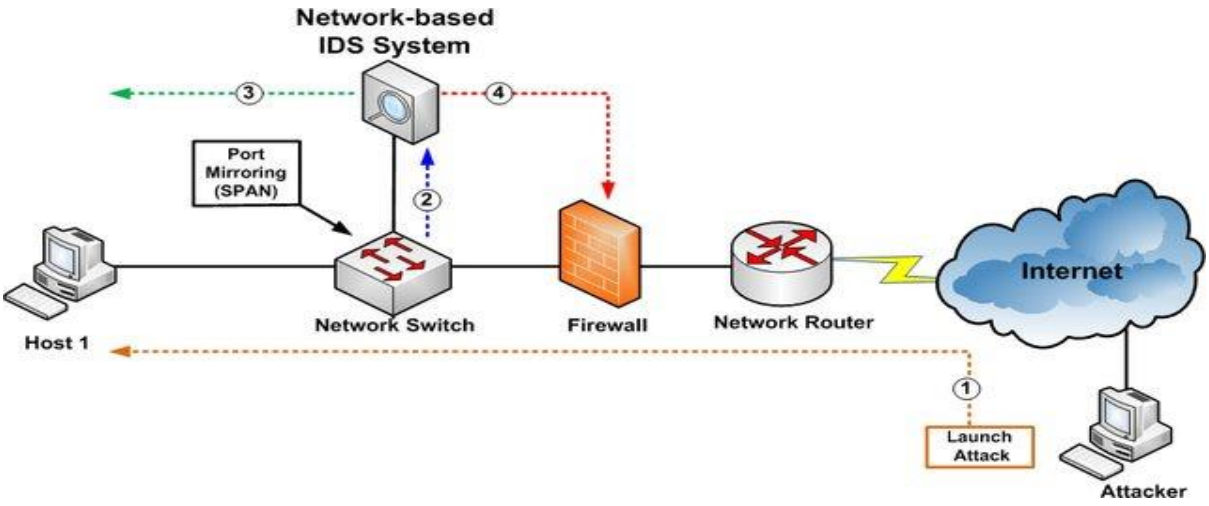

Figure 14:- Typical Security Onion Deployment Scenario

5.2.1. Security Onion Overall Simulation Architecture and Configuration

The below overall Security Onion Architecture is used to simulate the SIEM solution along with Kali Linux loaded with different attacking features and Window 7 machine to be targeted using Oracle Virtual Machine. A computer hardware with 1Gigabits interface speed, 16GB RAM and 1TB hard disk is used for this simulation purposes.

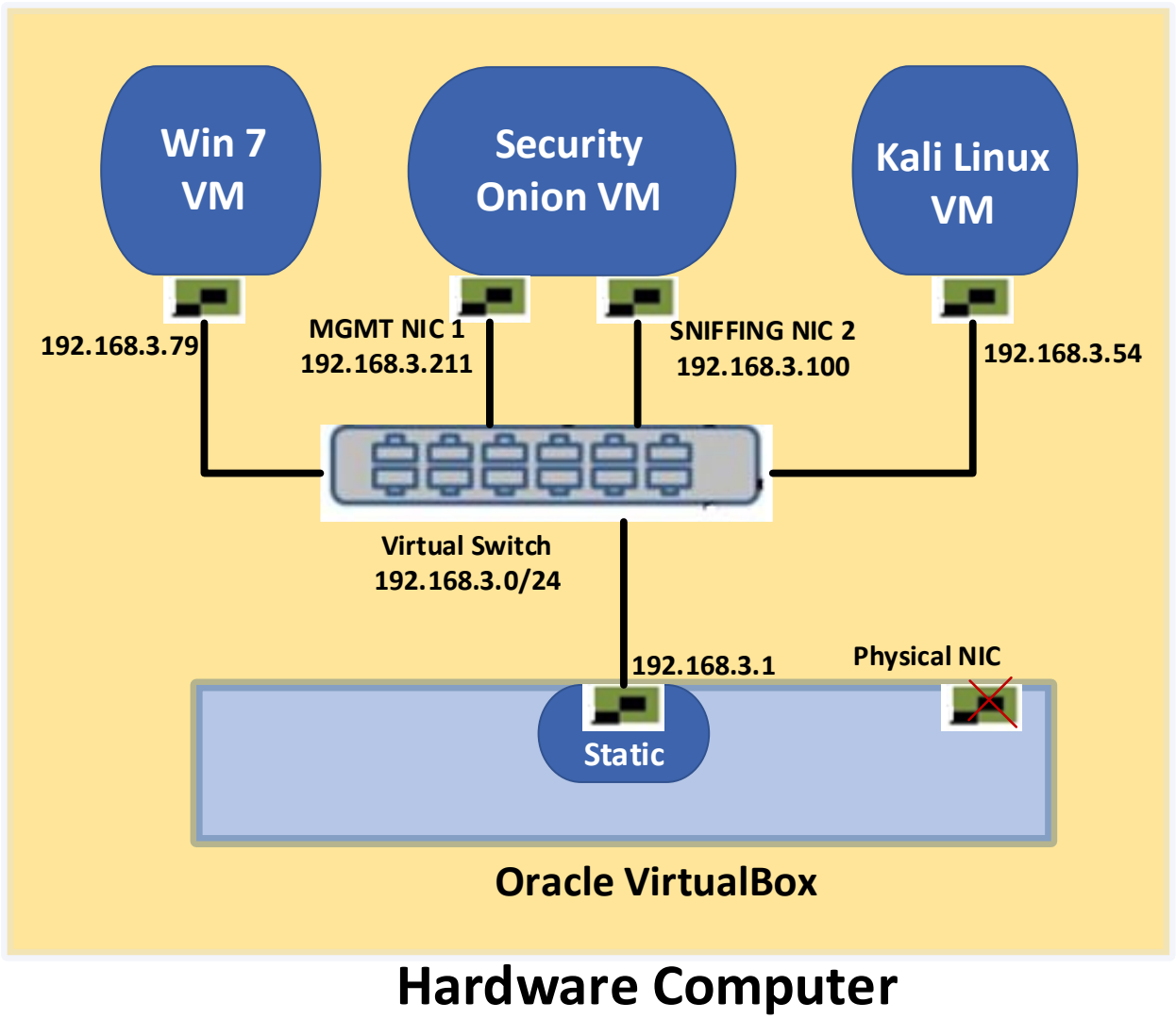

Figure 15:- Security Onion Simulation on Oracle Virtual Box – Overall architecture

As shown in the above Figure 15, the Security Onion SIEM requires two interfaces, i.e., Management interface and Sniffing interface. The management interface is used to manage the Security Onion's different security monitoring tools, while the Sniffing interface is used to capture logs and malicious network traffic.

The Security Onion's interfaces can be shown below in Figure 16 after installing and configuring it on the Oracle Virtual machine according to the planned simulation design shown in Figure 15 above.

```
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:16:d2:e2
          inet addr:192.168.3.211  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe16:d2e2/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:120 errors:0 dropped:0 overruns:0 frame:0
          TX packets:205 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13034 (13.0 KB)  TX bytes:12607 (12.6 KB)

enp0s8    Link encap:Ethernet  HWaddr 08:00:27:9b:b1:a4
          inet addr:10.0.3.15  Bcast:10.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::b66c:9a57:6fa1:c301/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1180 (1.1 KB)  TX bytes:1744 (1.7 KB)
```

Figure 16:- Security Onion Sniffing and Management interface details

Figure 17:- Security Onion setup installation wizard

The setup wizard shown in figure 17 above installs all services of the security onion including Elasticsearch, Logstash, Kibana, Squert, Sguil, Bro, Snort and netsniff-ng that we will use them for different purposes such log management and aggregation, intrusion detection, and for monitoring of security alerts.

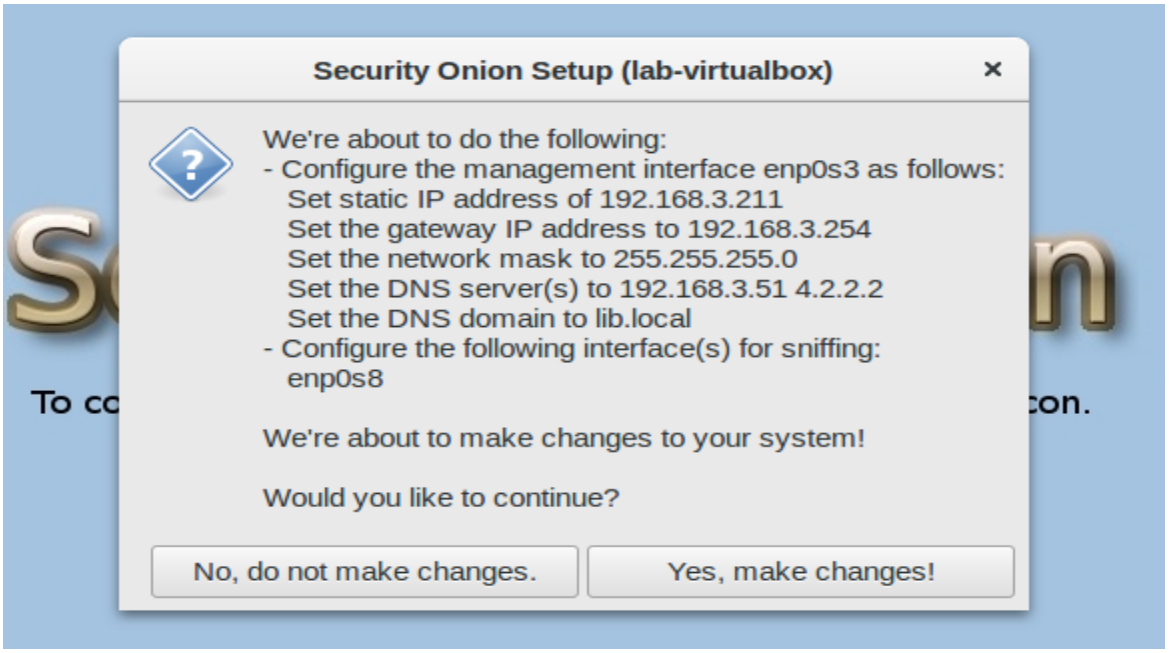

Figure 18:- Security Onion setup installation wizard

IP address, gateway, network mask and DNS are also required to be configured in the setup wizard as shown in figure 18 above which will be used for managing the Security Onion GUI-based tools.

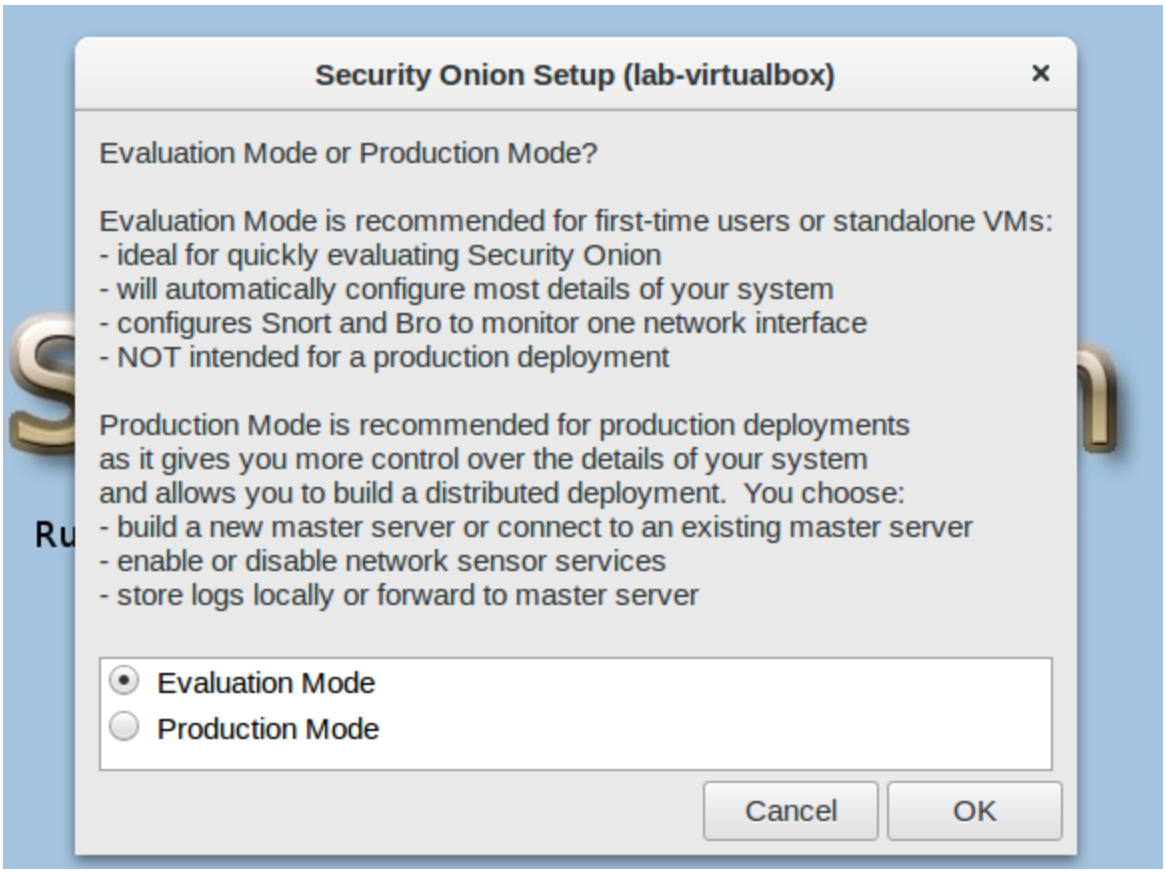

Figure 19:- Security Onion setup installation wizard

Evaluation mode is selected as shown in figure 19, while deploying the security onion to demonstrate this research work. This mode is selected because it simplifies the configuration and setup. In addition, the production mode is used in complex deployment scenarios. In our case it is required to monitor traffic in a simple network consisting of three machines i.e., Windows 7, Kali Linux and Security Onion nodes.

Figure 20:- Security Onion security tools

Overview of the security onion tools are shown in figure 20, after logging in in to the virtual machine.

After completing the Security Onion installation and setup, we need to open the Sguil security monitoring tool is opened using the proper credentials to detect security attacks and IDS alerts that generated from the Kali Linux virtual machine in real-time.

As shown in Figure 21 below, the Squil's sniffing interface is selected to monitor security notifications and alerts.

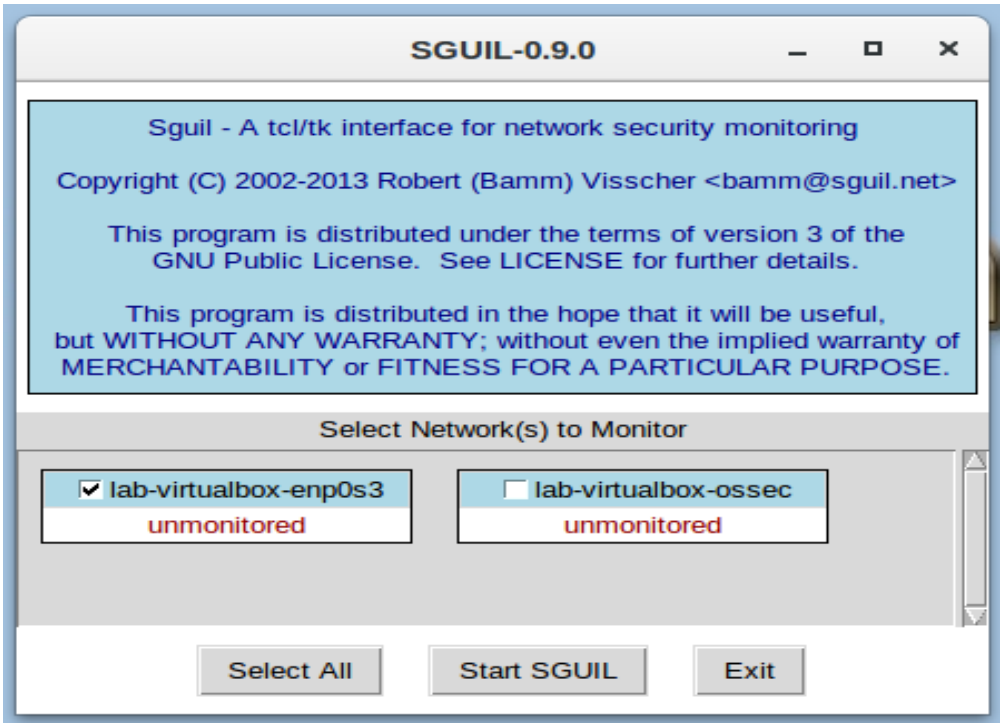

Figure 21:- Sguil Sniffing/Monitored interface selection

5.2.2. Network Scan Attacks using Nmap

After opening Sguil and selecting the Sniffing/Monitored interface or adapter network scan attack is run using Nmap network scanning tool which is found pre-installed on the Kali Linux virtual machine by default as shown in Figure 22 below. A network scanning attack is usually used to discover detail information in a target system; such as IP addresses, operating system, services running on the target machines; before launching further security attack.

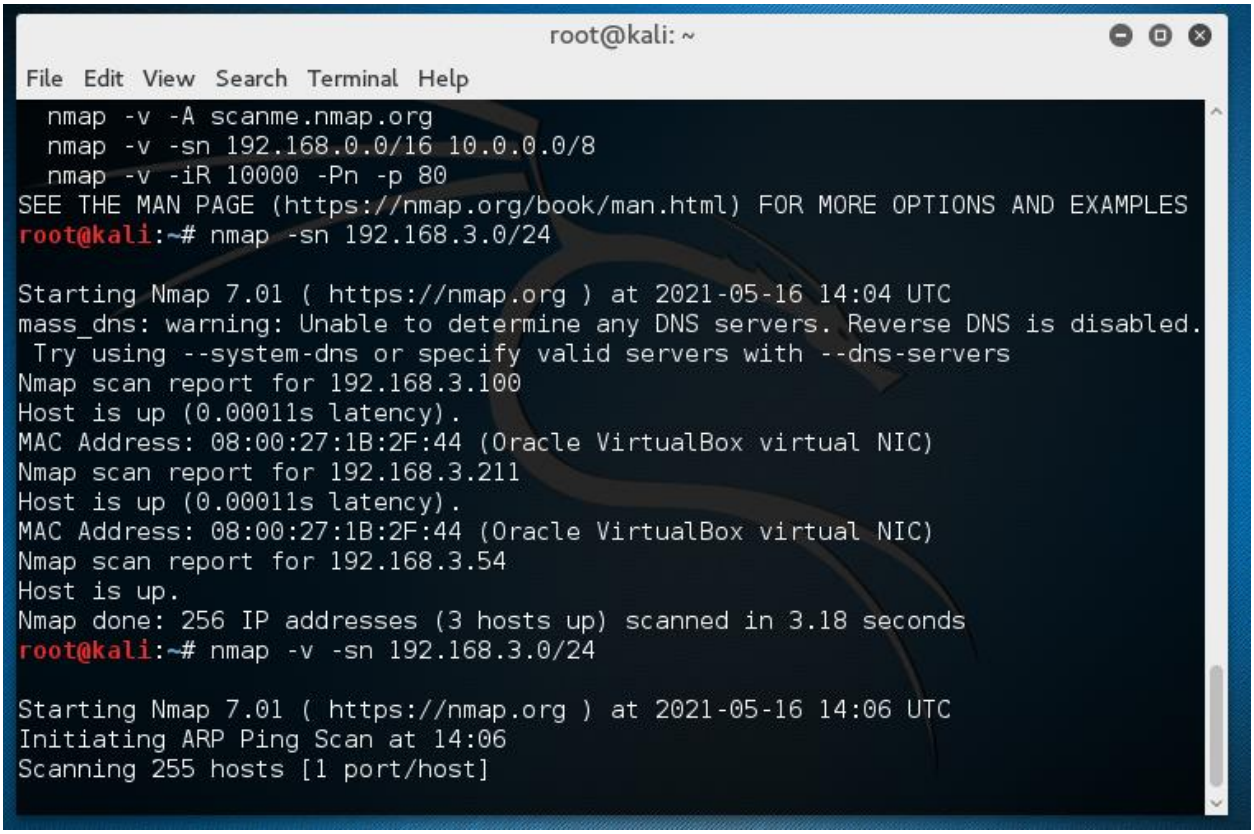

Figure 22:- Kali Linux - Nmap Network Scan attack

A network scan attack is launched using Nmap network scanning tool which is found installed on the Kali Linux machine. The network scanning attack is launched on the 192.168.3.0/24 subnet. As it can be observed from Figure 22, three host machines or IP addresses are up and running.

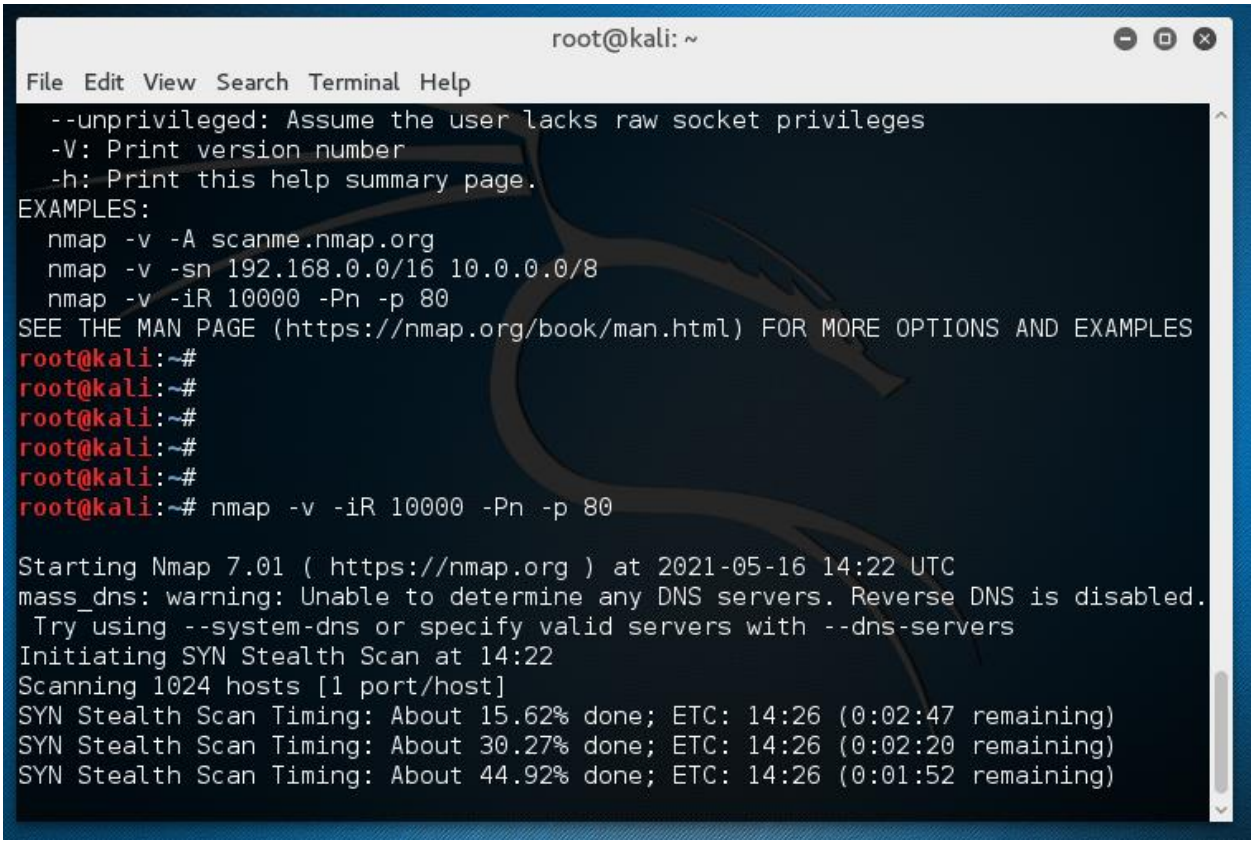

Figure 23:- Nmap SYN Stealth Scan attack on port 80

Syn stealth scan attack have also been demonstrated in figure 23 above using Nmap. Syn stealth scan attacks are usually used to launch DDoS attack on mission-critical servers with the aim of disrupting services and access to it.

After the Nmap network scan and SYN stealth scan is completed, network reconnaissance and stealth SYN scan attack that was run previously is detected by the IDS system i.e., Sguil as shown in Figure 24 below.

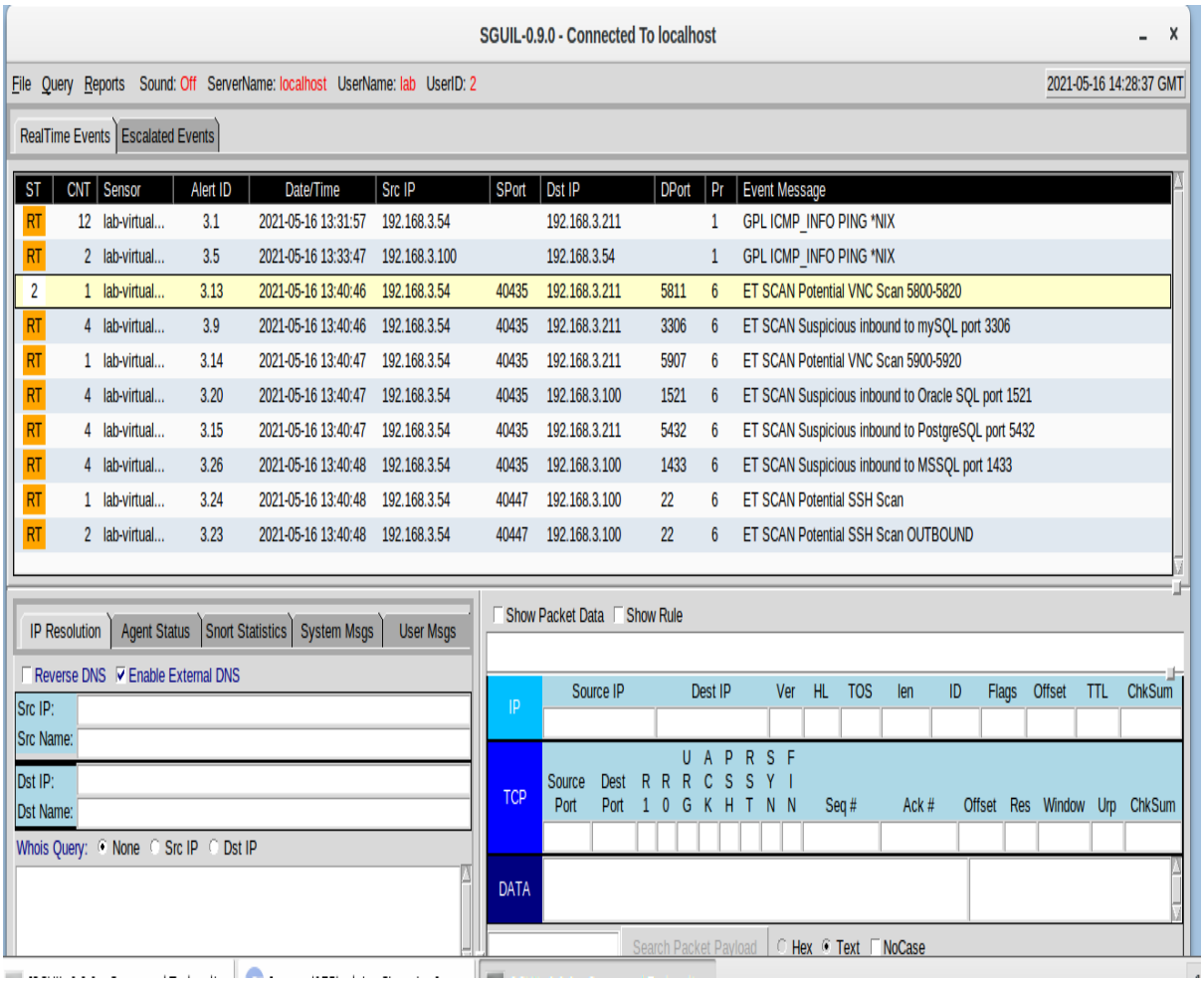

Figure 24:- Sguil IDS alerts - for the Nmap network scan attacks

The Nmap network scan attack and SYN stealth scans have been accurately detected by the Security Onion Intrusion Detection System i.e., Sguil as shown in Figure 24 above.

5.2.3. Zeus Malware Attack

In addition to the Nmap network scan attacks that we launched from the Kali Linux virtual machine above, Zeus malware attack have been also tested in the simulation, to further test and evaluate the threat detection capability of the Security Onion SIEM tool.

Zeus, also called Zbot is a Trojan-horse malware package that runs on versions of Microsoft Windows; which is identified for the first time back in 2007. While it can be used to carry out many malicious and criminal acts, it is often used to steal banking information by commonly

known security attacks such as Man-In-The-Browser, Keystroke logging and form grabbing. It usually spreads through drive-by-downloads, phishing and malicious email-links. The Trojan malware installs itself on the victim computer, secretly capturing passwords, account numbers, and other sensitive data used to login into online banking accounts. It is also very difficult to detect even with up-to-date antivirus and other endpoint security software solutions as it hides itself using stealth techniques.

The Security Onion has built-in sample Zeus packet captures as it is shown in Figure 25 below. In this case, it will be used to attack the Windows 7 machine in the virtual machine.

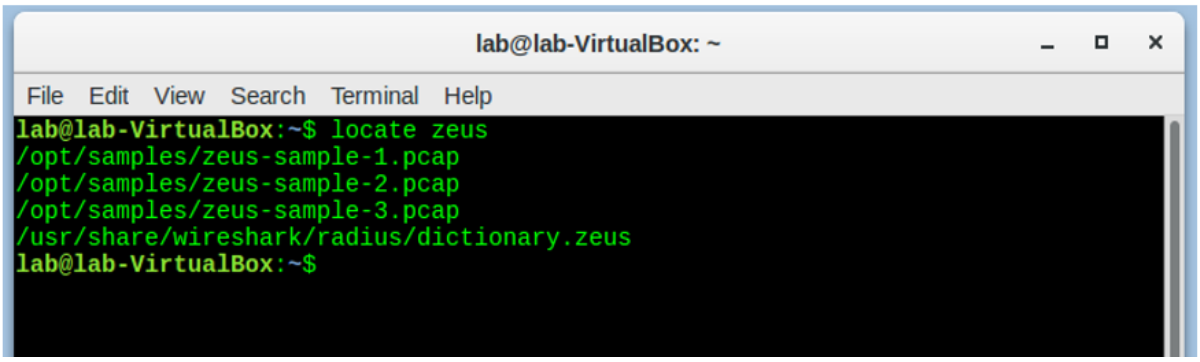

Figure 25:- Zeus Malware - Sample PCAPs on the Security Onion

A TCP replay command is used to replay the Zeus malware sample 20 times at high speed on the security onion's sniffing interface as shown below in Figure 26.

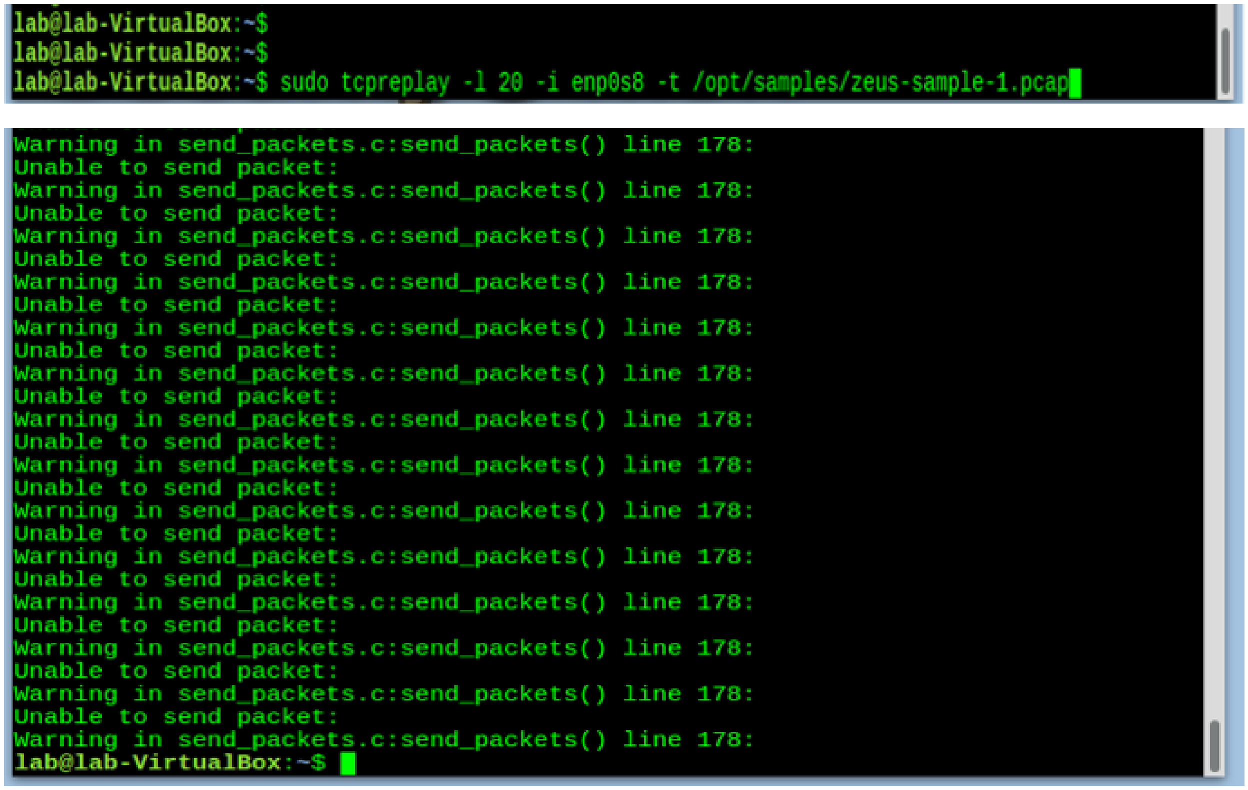

Figure 26:- Launching the Zeus Malware attack

The Trojan malware attack has been accurately detected and displayed by the Security Onion's Sguil module security/IDS alerts as shown in Figure 27 below.

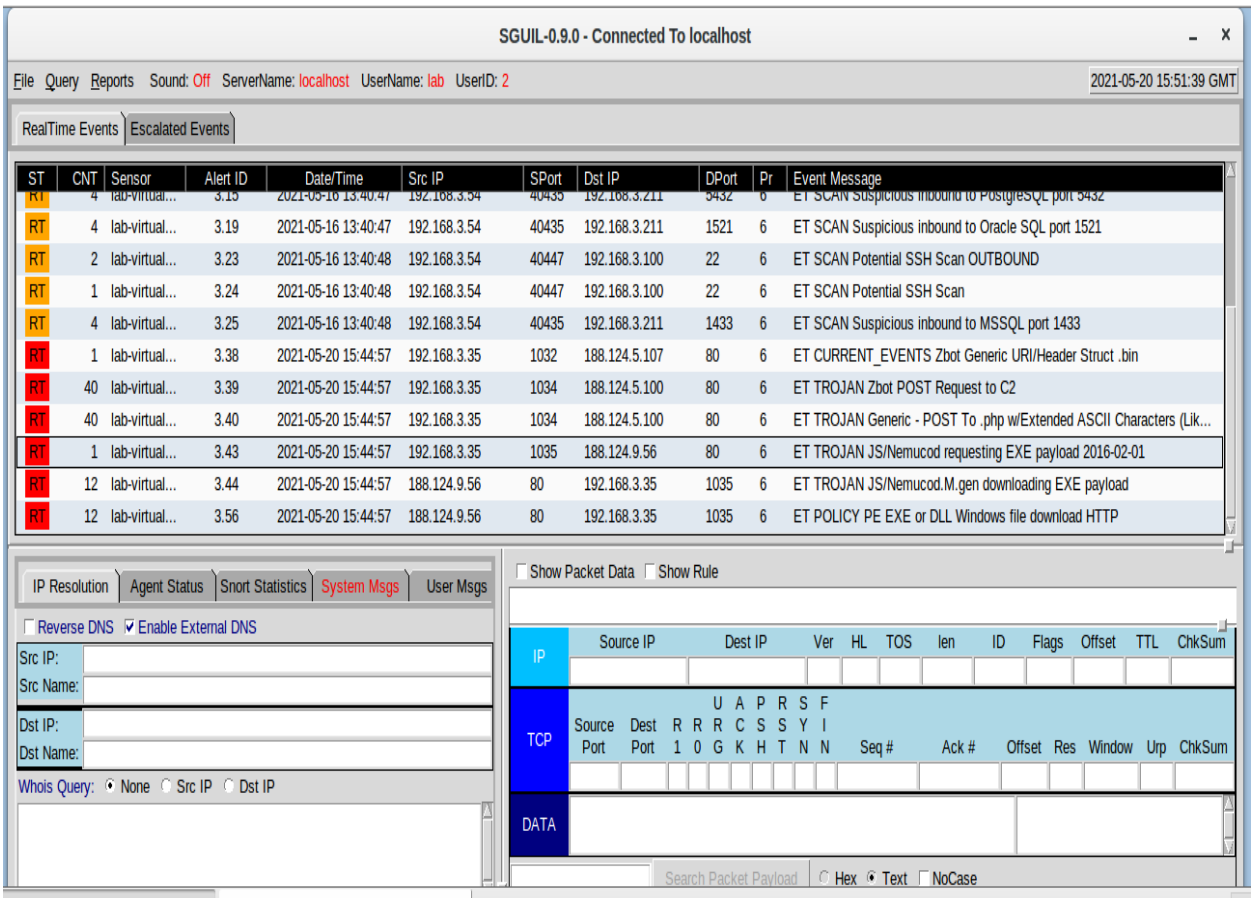

Figure 27:- Zeus Trojan-horse malware Sguil IDS alerts

5.2.4. Penetration Testing using Metasploit

The Metasploit framework is a very powerful penetration testing tool, which can be found pre-installed on the Kali Linux. It is widely used by cybercriminals as well as by ethical hackers to test vulnerabilities on networks and servers. In this simulation we will uses Metasploit to get unauthorized access by exploiting the FTP server on the Windows 7 machine.

The FTP server is setup and simulated in the Windows 7 machine as shown below in Figure 28. The FTP server is assumed to store some sensitive corporate files and documents.

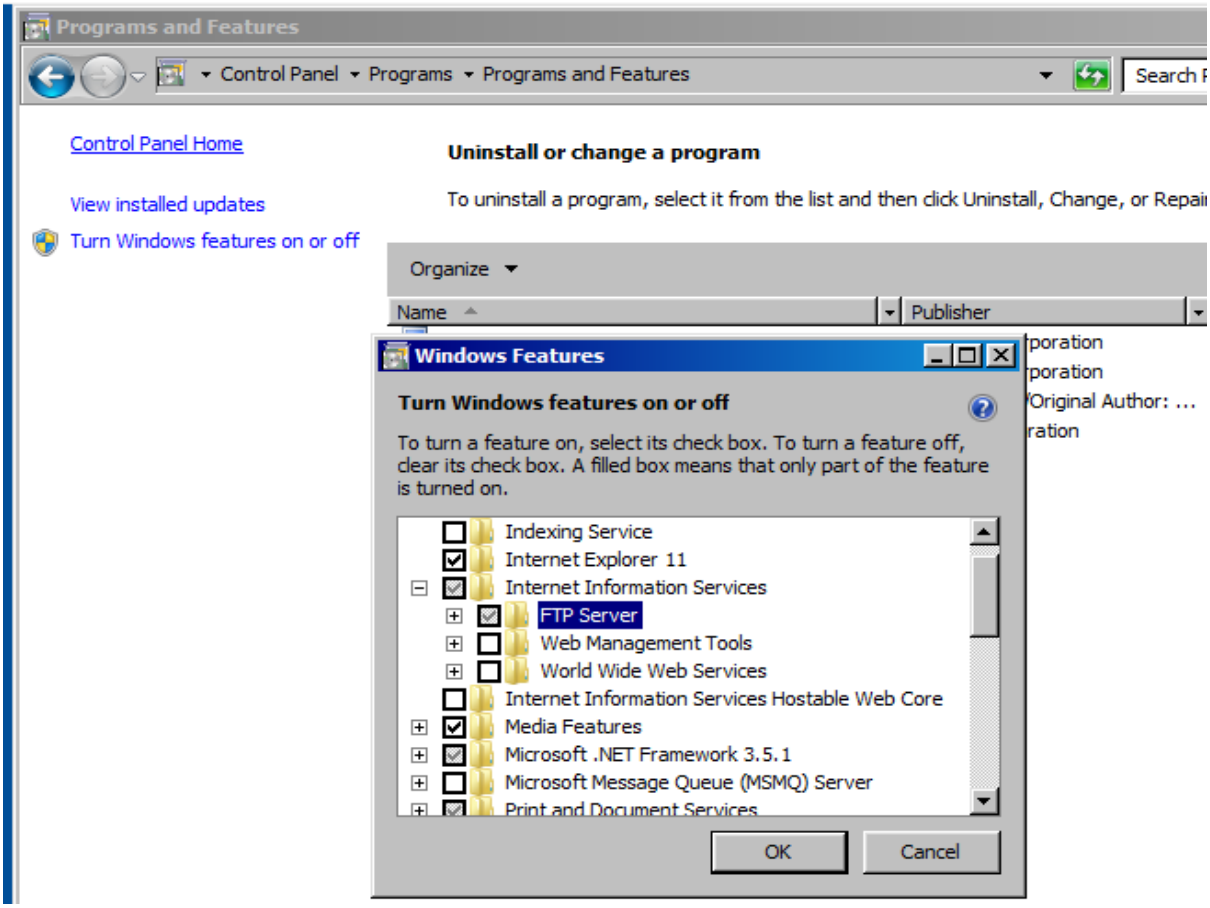

Figure 28:- Enabling FTP Server

After setting up the FTP server, Nmap scan is run on the target Windows 7 machine to make sure the FTP service is opened on TCP port 21, before launching a Metasploit attack.

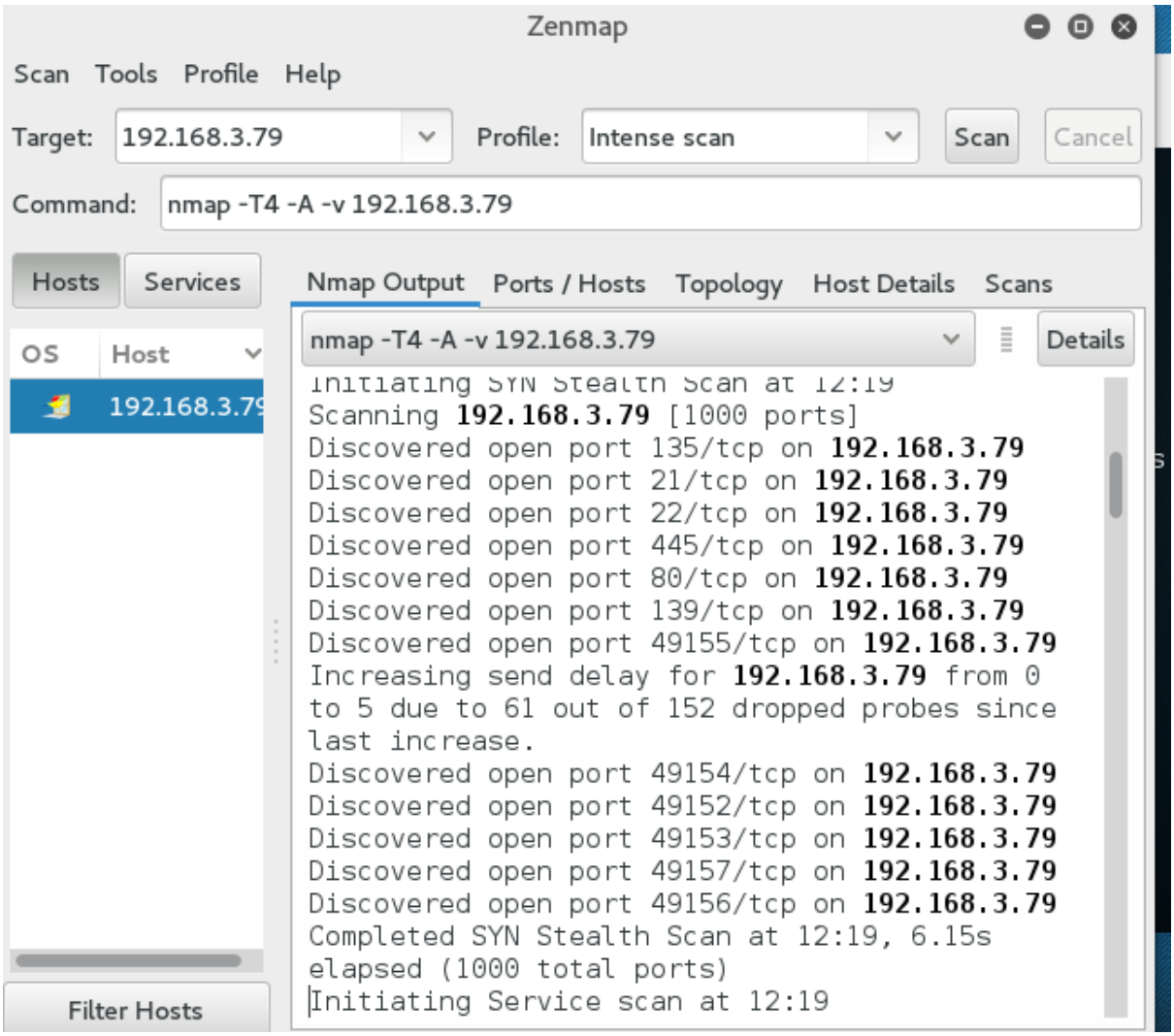

Figure 29:- Scanning opened ports of the Windows 7 machine using Zenmap/Kali Linux

The Windows 7 machine is now setup with FTP and is listening on TCP port 21, as it can be shown in the Nmap port scan output of Figure 29 above.

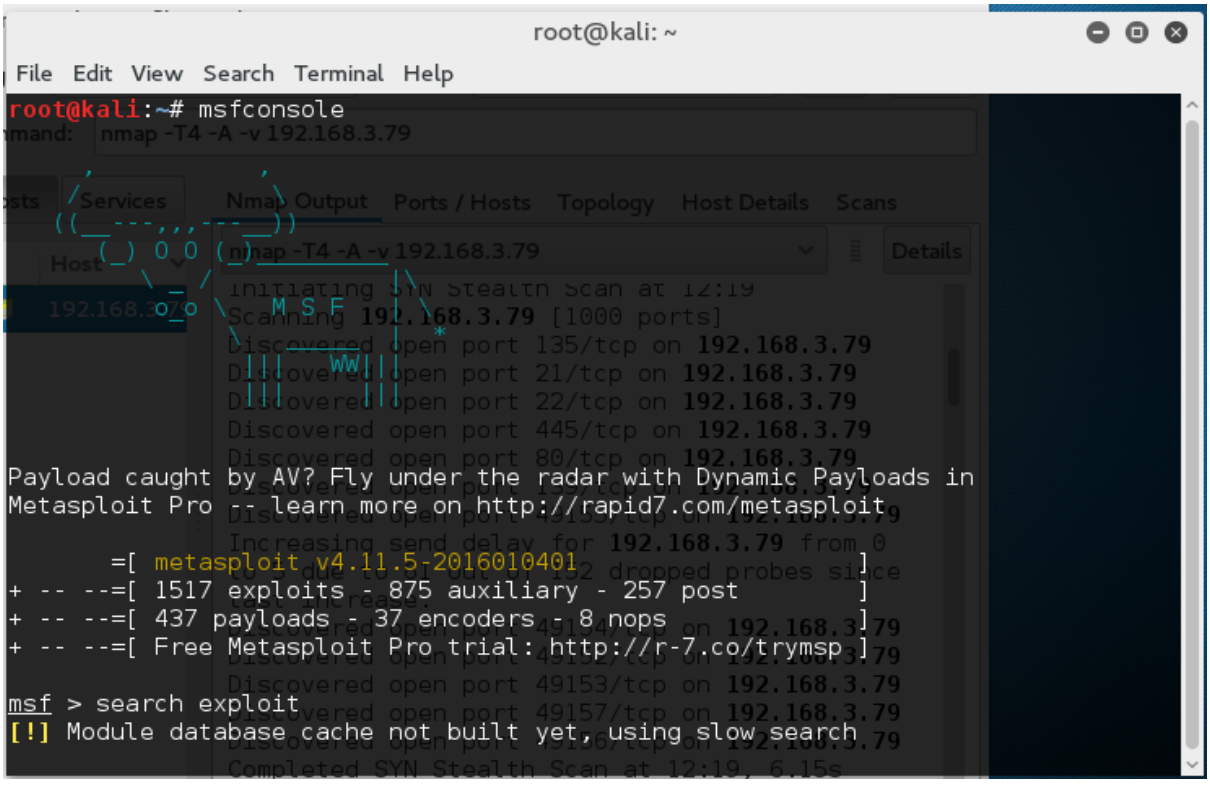

Figure 30:- Running Metasploit Console

The Metasploit Framework console is run to search for built-in FTP exploits that we will use in this simulation as shown in Figure 30 above.

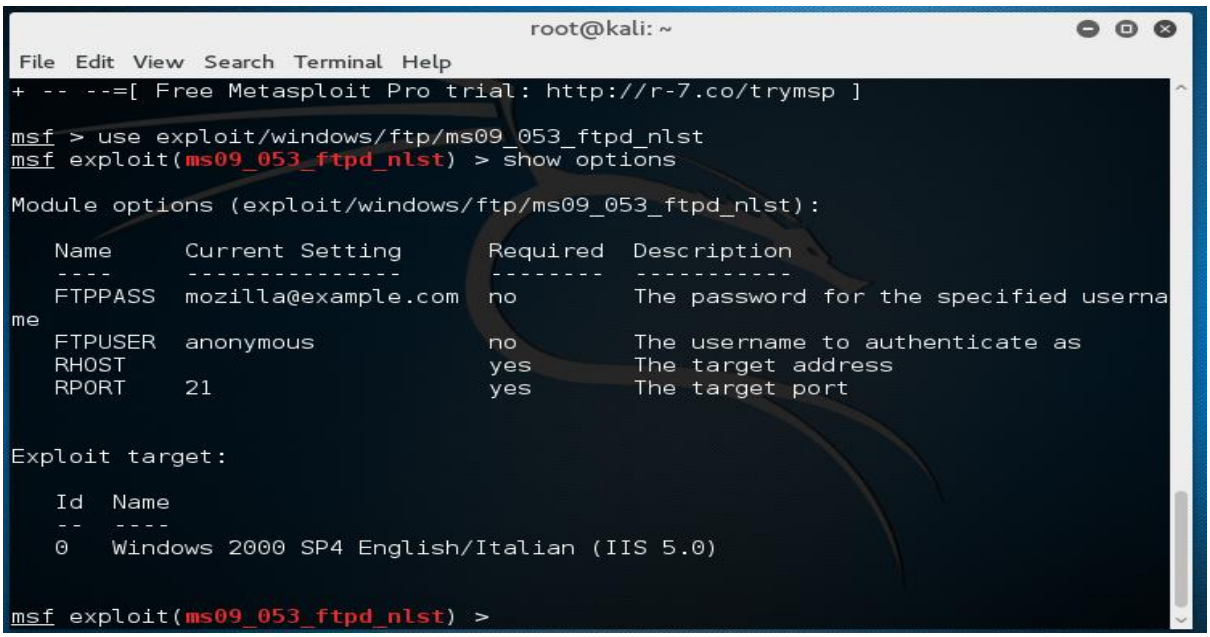

Figure 31:- Selecting Exploit type

The FTP exploit to be used is selected and options required to launch the ack are displayed in the Metasploit Framework (MSF) console shown in Figure 31 above.

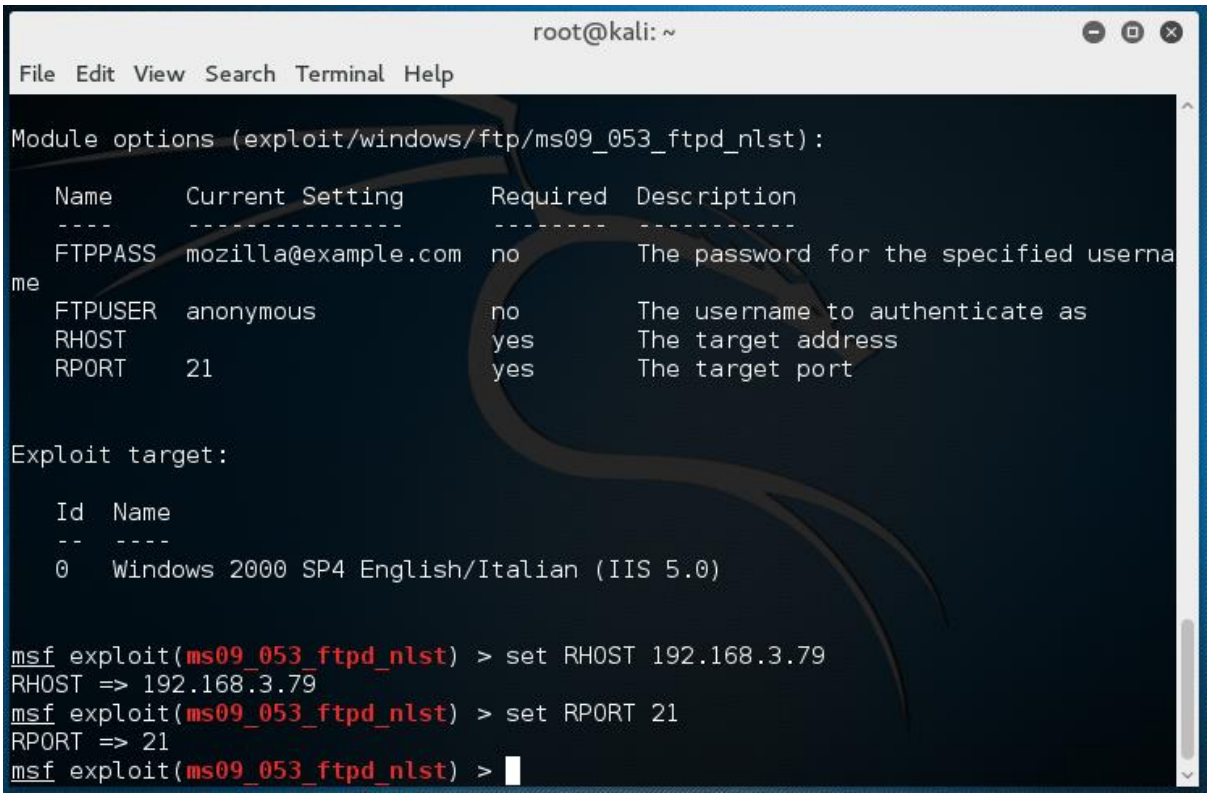

Figure 32:- Setting Targets to be Exploited

After setting up the target's i.e., FTP server's IP address and port address on the MSF console as shown in Figure 32 above; the exploit is successfully launched as shown in Figure 33 below to get unauthorized access to the FTP server.

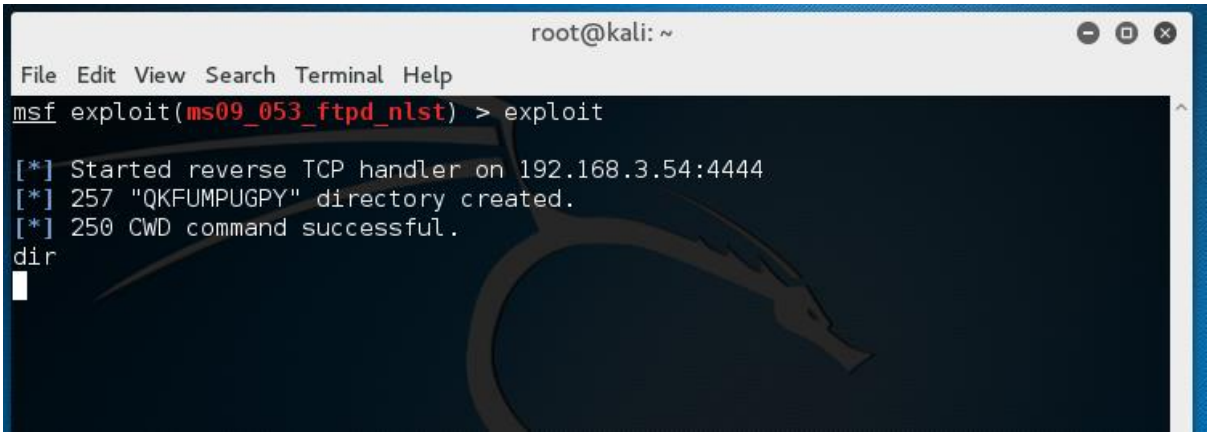

Figure 33:- Launching Exploit on the FTP

Malicious files have been written to the FTP server after gaining unauthorized access using the Metasploit exploit as shown in Figure 34 below. Initially, only the text files have been created by the researcher on the FTP server to represent as sample confidential corporate files. The rest of the directory files are created after gaining unauthorized access using the exploit. This demonstration shows that the attacker/hacker has managed to get unauthorized access and write some malicious files or codes that might also be used to launch further attacks on other targets.

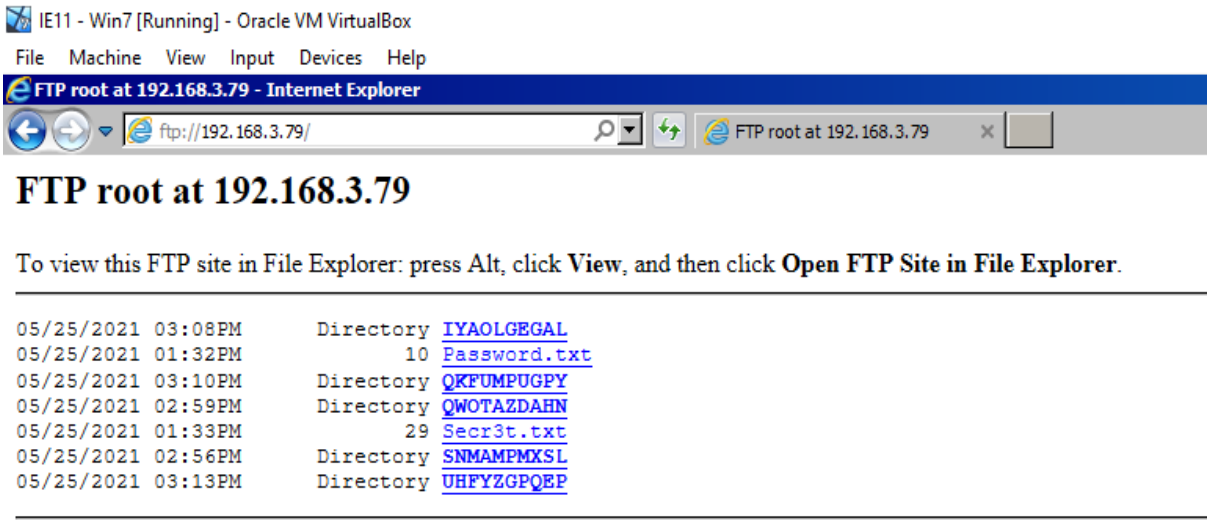

Figure 34:- FTP Files Created by the Exploit

The unauthorized access to the FTP server using Metasploit exploit has been successfully detected and displayed by the SGUIL Intrusion Detection System as shown in Figure 35 below. The IDS alerts contain useful information such as source IP address, source port, destination IP address, destination ports and other details. These information are critical inputs for security analysts to trace, investigate and stop the attack by applying necessary configuration changes.

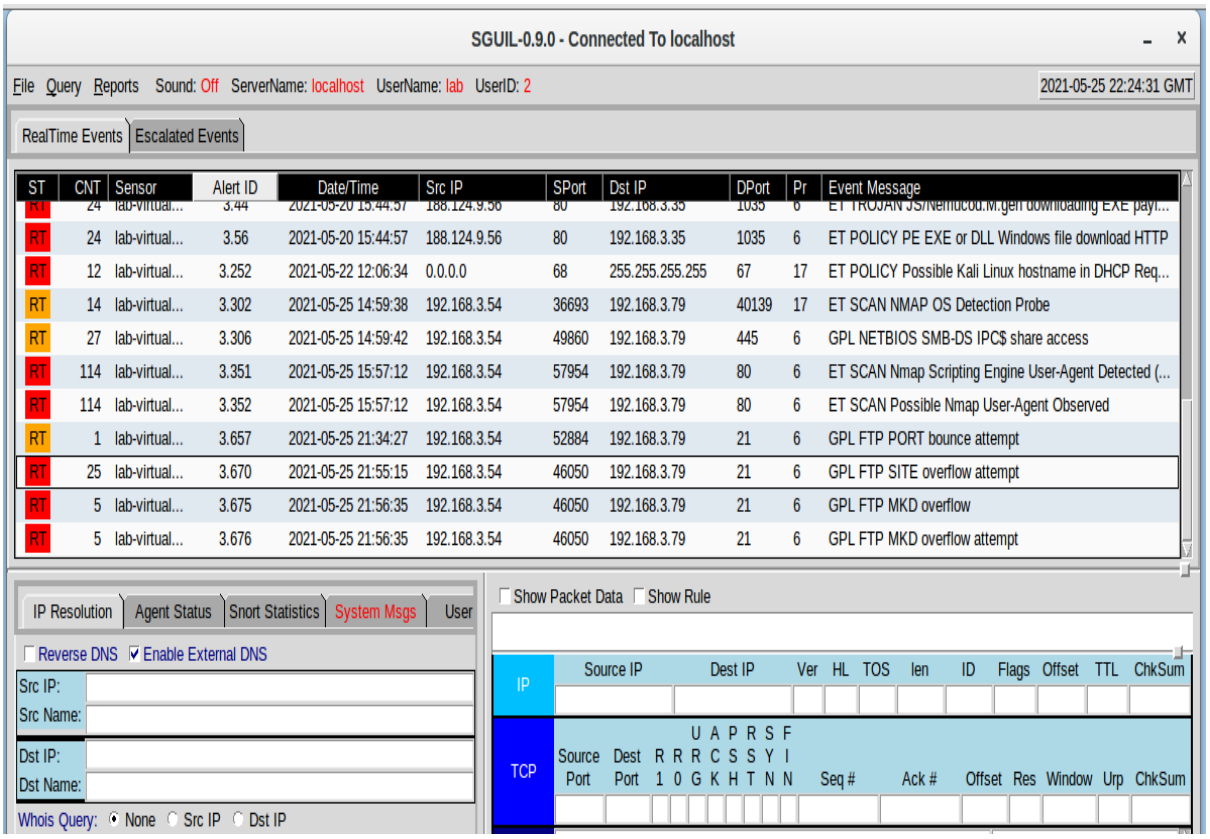

Figure 35:- Squert IDS alerts of FTP Exploit

5.2.5. Summary of Result of Threat Monitoring

The threat monitoring results summary is demonstrated using KIBANA and SQUERT open-source Graphical User Interface (GUI) tools. These tools are some of the Security Onion tools used for threat alert visualization and statistics consolidated in one Dashboard. This is suitable for the security analysts to perform daily security alert detection, monitoring and response activities.

The summary of threat alerts and log counts, which are generated from the previously launched attacks are shown below in Figure 36, by the Kibana dashboard.

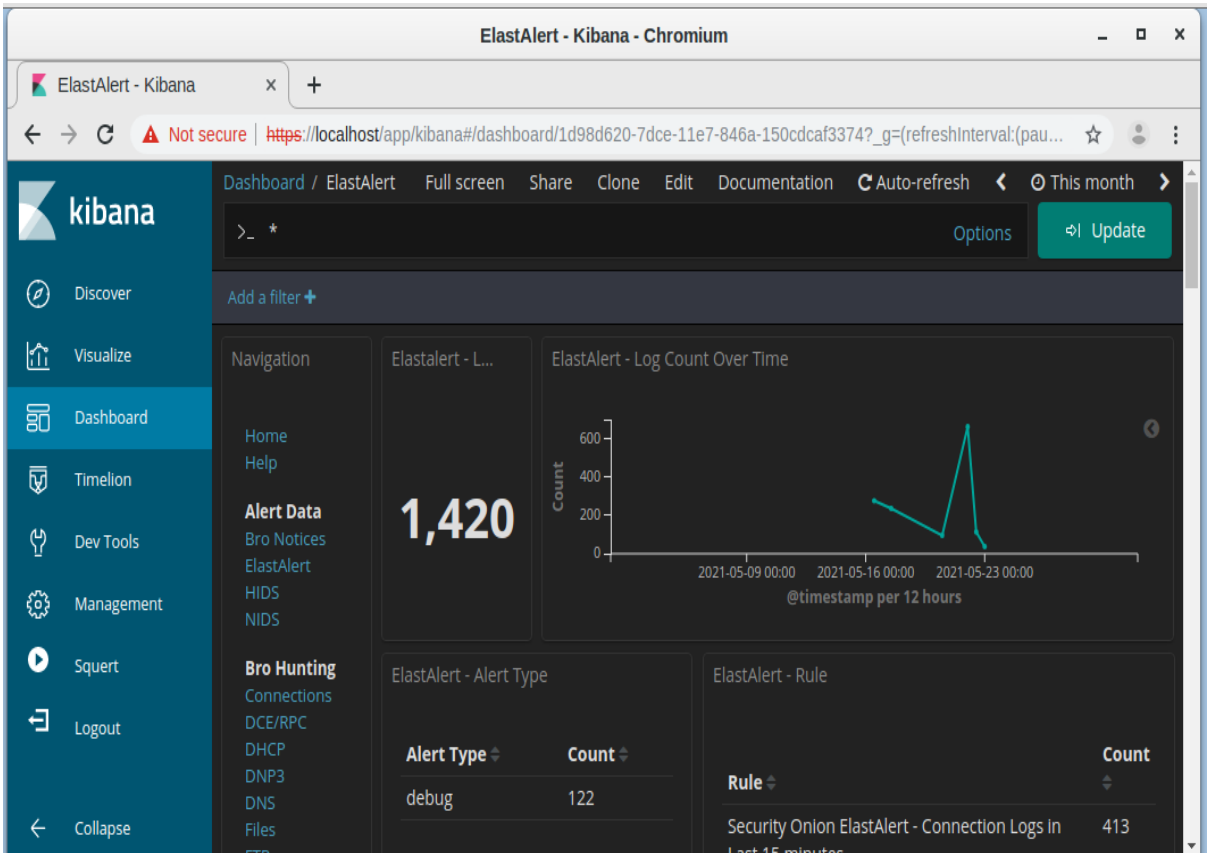

Figure 36:- Kibana main dashboard with security logs and alerts summary

Kibana Ealsticsearch rule alerts which are fired by the previous security attacks can also be shown in Figure 37 below, categorized into Connection logs, IDS events and User logins.

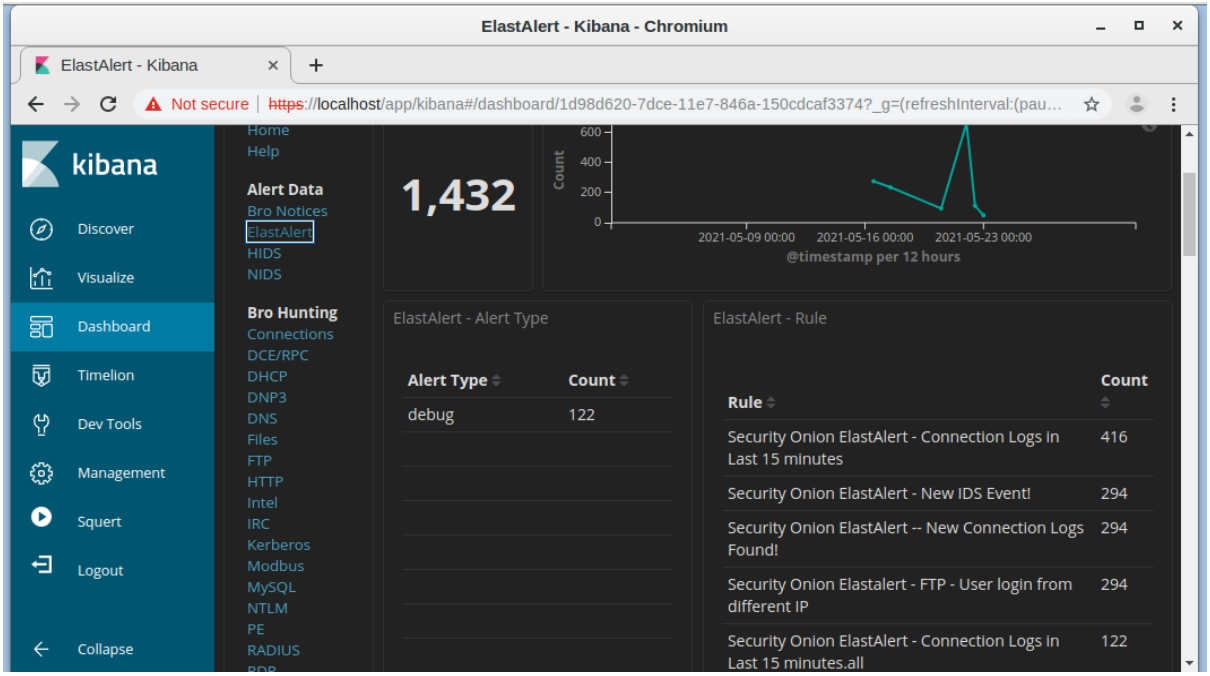

Figure 37:- Kibana - Security Alert Types and Counts

Intrusion Detection using SQUERT

The IDS alerts from Sguil can also be found summarized by Squert in a GUI (Graphical User Interface) format as shown below in figure 38.

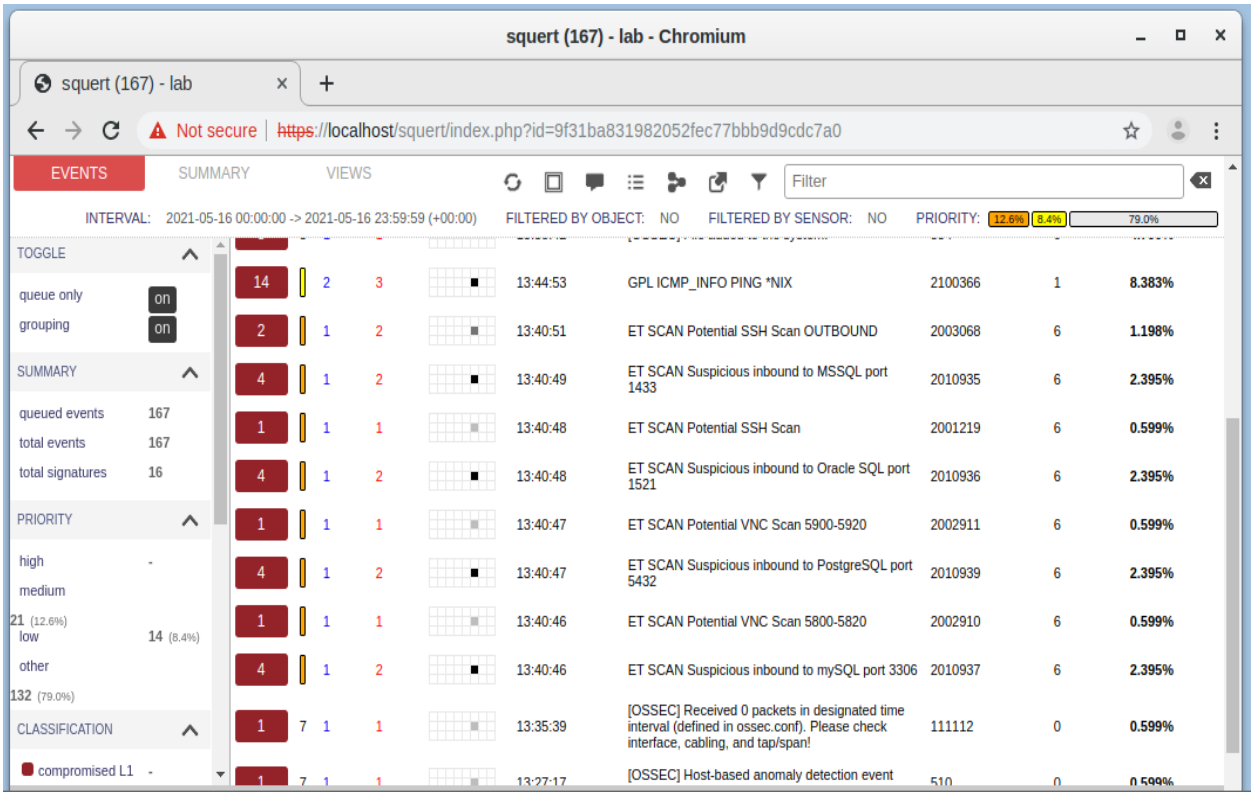

Figure 38:- Squert IDS alerts

Squert alerts can also be further investigated using reputable threat intelligence sites such as VirusTotal, ZeusTracker, MalwareDomainList and etc. to study about the security alert details, vulnerabilities it exploits and remediation recommendations as shown in Figure 39 below.

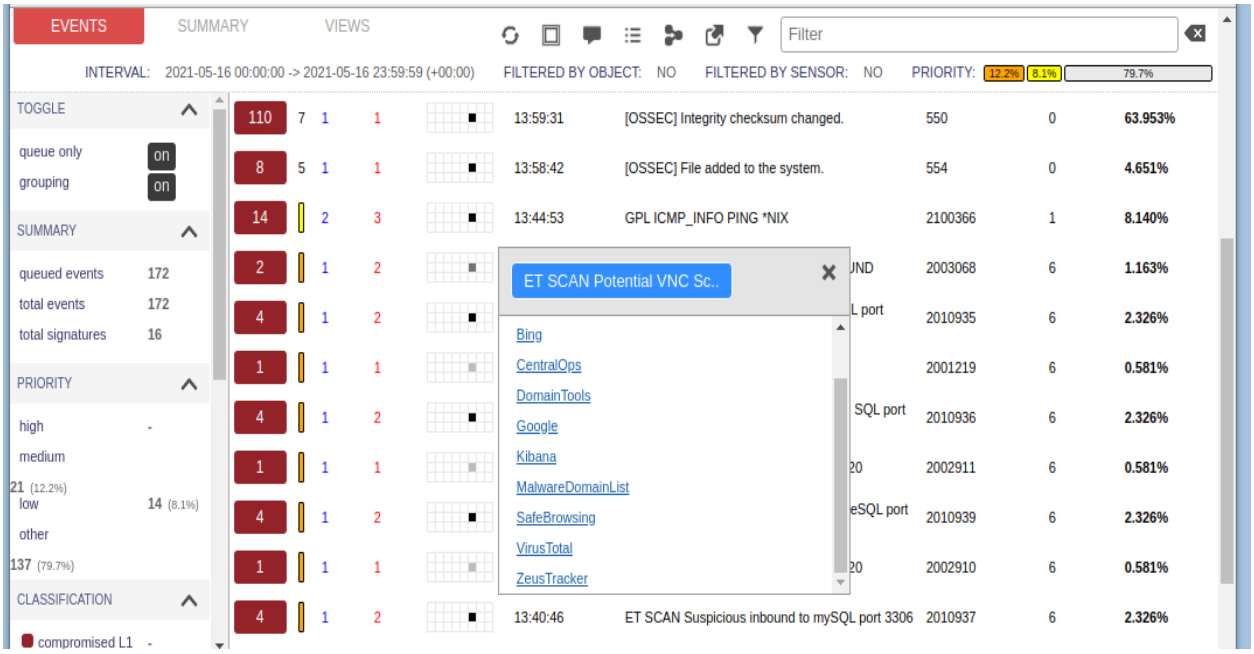

Figure 39:- Squert alerts investigation using reputable threat intelligence sites

After implementation, performance testing has been conducted using varied payloads on the Security Onion using Kali Linux powerful offensive tools.

All network scan and SYN flood attacks and Trojan-Horse malware that we have run from the Kali Linux were correctly detected and generated alerts accordingly. This has been consistently demonstrated by the various Security Onion tools such as Sguil, Squer and Kibana; displaying the security alerts in different formats.

In addition, the demonstration indirectly covers three major components of the designed SOC framework i.e., Processes (threat detection and monitoring), Technology (SIEM tool) and People (when security analysts take action to remediate the detected security threat).

In summary, the designed framework is sufficiently demonstrated according to the research objectives and expectations of precisely detecting and responding to security threats and attacks proactively to prevent compromise of critical infrastructure and service disruption thereby enabling financial institutions maintain trust and confidence among their customers.

5.3. EVALUATION

Evaluation is the systematic investigation of the merit, worth, or significance of the artifact. Evaluation practices varies across researchers as new methods and approaches has been developed and used for diverse projects and researches. In this regard, experimental approach is used to study the artifact in a controlled environment. In addition, presentation and demonstration is conducted to domain experts from six banks using Zoom virtual meeting to evaluate the framework. Virtual meeting is preferred due to time and resource constraints to conduct the demonstration by arranging a workshop. Moreover, COVID-19 restrictions made it difficult and challenging to arrange a workshop and meet physically.

Thus, a focus group of practitioners have been used here as alternative evaluation method to evaluate the developed SOC framework, as intended users of the artifact. However, getting practitioners' opinion in a matter of hours wouldn't be feasible to draw meaningful and thoughtful feedbacks as they have limited time.

After the demonstration of the proposed framework, questionnaires consisting of the three ITIL domains i.e., People, Process and Technology have been used to collect their feedbacks and evaluate the overall effectiveness and usability of the framework. The practitioners' response to the 5-point Likert scale based questionnaire is summarized in Table 12 below; showing the total number of respondents for each scale.

Evaluation Parameters	***Strong Agree (5)***	***Agree (4)***	***Neutral (3)***	***Disagree (2)***	***Strongly Disagree (1)***
People					
The designed framework covers all relevant topics in the people domain including stakeholders, analysts, roles, knowledge management and training and governance aspects required to run an effective and efficient SOC.	*8*	*2*	*2*	-	-

Process					
The designed framework has covered all relevant topics in the Processes domain required in a typical SOC to provide necessary functions and services.	*7*	*3*	*2*	-	-
Technology			.		
The designed framework has covered all relevant topics of the Technology domain that can be used in the Ethiopian banks to build a SOC.	*9*	*2*	*1*	-	-
Threat Detection and Monitoring					
Threat detection and monitoring part of the artifact is demonstrated adequately and can be used to build an effective and efficient SOC to proactively stop and mitigate security threats.	10	1	1	-	-

Table 12:- Evaluation Response Summary

Total of 12 experts i.e., 2 IT Security experts from each of the six banks has been participated in evaluating this framework. The evaluation parameters People, Processes, Technology and Threat Detection and Monitoring demonstration have been evaluated by the respective experts with average points of 4.08, 4.41, 4.67 and 4.75 results respectively out of a 5-point Likert Scale.

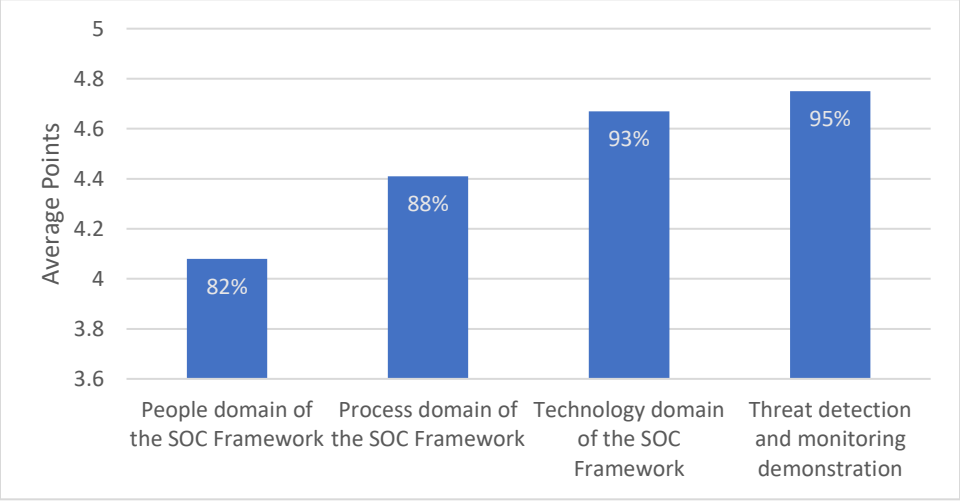

Figure 40: Summary of results of the SOC framework evaluation

5.4. DISCUSSION OF RESULTS

From the evaluation results of the framework discussed in the above section, it clearly shows that relevant topics of the three pillars i.e., People, Processes and Technology aspects of the SOC framework have been adequately covered in this research. Satisfactory result has been recorded by the way the threat detection and monitoring part of this artifact has been demonstrated followed by SOC Technology, Processes and People domains.

Thus, the overall results show that the designed framework can be used as solution by the banking industry with further enhancements and improvements, especially in People and Processes aspects of the artifact.

CHAPTER SIX

CONCLUSION AND RECOMMENDATIONS

6.1. OVERVIEW

A SOC framework is designed for the banking industry, which will be used as a reference and guideline while implementing efficient and effective security operations to prevent the ever-increasing cyberattacks and financial fraud. The framework is designed by identifying the current problems, gaps and challenges facing the financial institutions in regards to proactively securing their mission-critical IT infrastructure. In addition, previous literature, international standards and best practices have been reviewed to come up with a custom-made framework for the Ethiopian banking industry. Document analysis and expert discussion instruments have been used to gather data and assess the current security operation practices. The main purpose of this chapter is to conclude and summarize key points of the study and to indicate areas that need further study by future researchers and practitioners.

6.2. CONCLUSION

As Ethiopian financial institutions accelerate the adoption of cutting-edge technologies to provide and expand their banking services using different digital channels including ATM, POS, Card banking, Internet banking and Mobile banking; so does the concerns of vulnerability to cybersecurity crimes and fraud. Hence, proactive monitoring of security threats and vulnerabilities is required to protect these mission-critical services by adopting a customized SOC framework.

A design science research methodology is used to design the artifact. The framework is proposed by identifying the current practices and gaps in the Ethiopian banking industry using qualitative research methods. Thus, document analysis and expert interviews have been used to collect the necessary data and understand the problem at hand. The framework is designed based on the three ITIL pillars i.e., People, Processes and Technology.

The proposed framework makes it unique as compared to other SOC frameworks in that, new sub-components such as Legal Controls, Threat Intelligence and Typology of SOC have been added to fill the gaps observed in the Ethiopian financial institutions' security operations. In addition, the development of the framework using ITIL components is new approach in this research.

Finally, one of the core SOC functions, identified in the research i.e., threat detection and monitoring complemented with threat intelligence have been demonstrated and evaluated to fill the gap observed in proactive prevention and mitigation of cyberattacks and frauds in the Ethiopian banking industry. Open-source SIEM tool i.e., Security Onion installed in a virtual environment with real-world scenarios have been used to demonstrate this part of the artifact. Hence, the designed artifact demonstration comprises one of the **Processes** (threat detection and monitoring), **Technology** (SIEM tool) and **People** (security analysts) to remediate and act upon the detected security incidents.

To simulate the different cyberattacks, Kali Linux penetration testing tools have been used. Network scan attacks, Zeus Malware/Trojan horse and Metasploit exploit tools have been tested in the virtual environment. These cyberattacks have been correctly identified and detected by the Security Onion various tools including Sguil IDS system and GUI-based Kibana and Squert tools.

To assess the usability and functions of the designed SOC framework, it has been also evaluated by presenting it to focus group domain experts from six banks and high-level questionnaire have been used to collect their feedbacks. The results from the evaluation of the artifact shows that the overall aspects of the artifact are adequately covered, consistent with the objectives of the research.

The research has successfully achieved it goals of designing a viable and usable artifact that can be adopted by the Ethiopian banking industry to implement effective and efficient security operations. The artifact is designed based on different industry standards and best practices to ensure the functional and non-functional requirements are met. In addition, this research has sufficiently demonstrated that open-source SOC tools can be used to proactively analyze and detect cybersecurity attacks which can be cost-effective options to financial institutions who have limited budgets. This study is also expected to fill the gap in local literatures in the field. In addition, it is intended to inspire future researchers and practitioners to further strengthen the artifact.

However, the areas of security hardening, forensics and incident response procedures are not covered and demonstrated in this research even though they are part of the SOC's major functions. As a result, these topics require further study.

6.3.RECOMMENDATIONS

Based on the findings of this research, the following recommendations are made for improving the proposed framework.

- In this study, the threat detection and monitoring part of the designed framework is simulated in a lab environment with limited traffic. For practical reasons there is a need to demonstrate it in real-world setup with high traffic sources to its effectiveness in detecting and analyzing cybersecurity threats.
- The SOC analysts' skill level and gaps were not assessed in detail and needs further work.
- The researcher recommends Ethiopian banks to study the way to implement standard security operation procedures to enhance visibility, proactively monitor and deter cybersecurity threats to their mission-critical IT infrastructure
- Ethiopian banks should also assess and evaluate their readiness in terms of the overall SOC components i.e., People, Processes and Technology as they are critical ingredients in implementing an effective and efficient security operations.
- Using SOAR (Security Orchestration, Automation and Response) instead of a SIEM would have been effective as it uses Artificial Intelligence and Machine learning algorisms to automate the detection, analysis and response to cybersecurity threats.

REFERENCE

Amare, B. (2015). Assessment of Insider Threat in Ethiopian Banking Industry. *(Unpublished Master's Thesis), Addis Ababa University, Ethiopia*.

Barclay et al. (2013). Developing a National CyberSecurity Framework for Jamaica: A Design Science Approach. *12th International Conference of IFIP working group*.

Berhanu, N. (2017). Assessment of IT Disaster Recovery Practices in Ethiopian Commercial Banks. *(Unpublished Master's Thesis), Addis Ababa University, Ethiopia*.

Bogale, M. (2018). Proposing Information Security Awareness Program for Enat Bank in Ethiopia. *(Unpublished Master's Thesis), Addis Ababa University, Ethiopia*.

Chuvakin et al. (2018). How to Plan, Design, Operate and Evolve a SOC. *Gartner*.

Davis, P. (2004). Cyber security and implications for national infrastructure. *IEE Seminar on Developments in Control in the Water Industry.*

Dempsey, K. L. (2011). Information Security Continous Monitoring (ISCM) for Federal Information Systems and Organizations. *NIST Secial Publication 800-137*.

ENISA. (2010). Good practice guide for incident management. *ENISA*.

Gebrehawariat, D. (2017). Assessment of the Effectiveness of Card Banking Security in the Ethiopian Financial Sector. *(Unpublished Master's Thesis), Addis Ababa University, Ethiopia*.

Gorka et al. (2018). Selecting the Right SOC model for your Organization. *Gartner*.

Hevner et al. (2004). Design science in information systems research. MIS quarterly. 75-105.

Hubbard, J. (2020). Guide to Security Operatins. *SANS*.

IBM. (2013). Strategy Considerations for Building a Security.

INSA. (2020). Cybersecurity current situation, actors and next action plans.

ISO/IEC 25000:2014. (2014). Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Guide to SQuaRE. *ISO/IEC JTC 1/SC 7*.

Janos et al. (2018). Security Concerns Towards Security Operations Centers.

Kindie, H. (2018). Customers' Perception towards Mobile Banking Security: The Case of Commercial Bank of Ethiopia. *(Unpublished Master's Thesis), Addis Ababa University, Ethiopia*.

Kuechler et al. (2012). A Framework for Theory Development in Design Science Research: Multiple Perspectives. *Journal of the Association of Information Systems*, 395-423.

Mell et al. (2013). Creating a Patch and Vulnerability Management Program. *NIST Special Publication 800-40 Version 2.0*.

Michail, A. (2015). Security operations centers: A business perspective . *(Master's thesis)*.

Mugari et al. (2016). The Emerging Threat to the Financial Services Sector in Zimbabwe. *Mediterranean Journal of Social Sciences*.

Muniz et al. (2015). Security Operations Center: Building, Operating, and Maintaining Your SOC. *Cisco Press*.

Nigussie, A. (2015). Practices, Challenges and Prospects of Information Security Policy in Ethiopian Banking Industry. *(Unpublished Master's Thesis), Addis Ababa University, Ethiopia*.

NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity. *Cybersecurity Framwork*.

NIST 800-53. (2020). Security and Privacy Controls for Information Systems and Organizations. *Special Publication Revision 5*.

Onwubiko, C. (2015). Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, 1-10.

PCI-DSS. (2018). Requirement and Security Assessment Procedures Version 3.2.1. *PCI Security Standards Council*.

Peffers et al. (2006). The design science research process: A model for producing and presenting information systems research. *Proceedings of First International Conference on Design Science Research in Information Systems and Technology* (pp. vol. 24, pp. 83–106.). DESRIST.

Raynolds, L. (2020). Network Visibility and Threat Detection Survey. *SANS*.

Rob, O. v. (2020). Measuring Capability Maturity in Security Operations Centers. *SOC-CMM* .

Schinagl et al. (2015). A Framework for Designing a Security Operations Centre (SOC). (pp. 2253-2262). HICSS.

Siddique, & Rehman. (2011). Impact of Electronic Crime in Indian Banking Sector: an overview. *International Journal of Business and Information Technology*.

Syslog RFC5424. (2015). The Syslog Protocol. *IETF*.

Tebikew, K. (2013). Information Security Management Framework for Banking Industry in Ethiopia. *(Unpublished Master's Thesis), Addis Ababa University, Ethiopia*.

Trustwave. (2013). *Global Security Report.*

Woretaw, & Lessa. (2012). Information Security Culture in The Banking Sector in Ethiopia. *5th ICT 2012 Ethiopia Conference*.

Yohannes, T. (2018). Assessment of Information Security Incident Management Practices in Ethiopian Bank. *(Unpublished Master's Thesis), Addis Ababa University, Ethiopia*.

Zimmerman, C. (2014). Ten Strategies of a World-Class Cybersecurity Operations Centre. *The Mitre Corporation*.

APPENDICES

Domain Expert Interview Questionnaires

1. Do you get enough local references and best practices while implementing your SOC?

   _____

2. If you have a SOC currently, can you please list all the challenges you are facing while implementing and operating a SOC?

   _____

3. Do you continuously monitor your IT infrastructure for any possible intrusions and cyber-attacks?

   _____

4. Do you have automation tools such as SIEM to continuously monitor cybersecurity events happening in your IT environment?

   _____

5. Do you have contacts established within the local and international cybersecurity CERT organizations for assistance in case of cybersecurity incidents and to get up to date information about the latest vulnerabilities in the financial industry?

   _____

6. Does your organization have enough skilled cybersecurity analysts working in the SOC?

   _____

7. Is there management commitment and awareness about the need to invest in SOC?

   _____

8. Please specify and list the best practices and standards you are using currently to manage your SOC (if any)?

_____

9. Does your SOC team closely collaborate and communicate with other teams such as NOC and IT teams?

_____

10. Does your SOC receive the latest cybersecurity threat and vulnerability information from known national and international sources?

_____

11. Does the SOC security analysts also performs additional tasks such as in the IT Security department or other IT department functions?

_____

12. Does the SOC team identified which critical IT infrastructure and assets to monitor using SIEM?

_____

13. Does the SOC team also perform cybersecurity Risk Management, Penetration Testing, Forensics tasks?

_____

14. Does your organization has approved incident response plans?

_____

15. Do you conduct detail forensics to investigate security incidents after they occur?

_____

16. Does the SOC team monitor and investigate security alerts and notifications detected by the SIEM systems on timely basis?

_____

17. Do you receive and share security threat intelligence with external stakeholders to achieve broader cybersecurity situational awareness?

_____

18. Does the day-to-day SOC team's coordination with stakeholders occurs consistent with response plans?

_____

19. Do all your SOC personnel know their roles and order of operations when a response is needed and to ensure accountability?

_____

20. Does your SOC team has a baseline of network operations and expected data flows for users and systems in your bank?

_____

21. Is event data collected and correlated from multiple sources and sensors and events are analysed to understand attack targets and methods?

_____

22. Does your SOC team monitor unauthorized personnel, connections, devices, and software in your bank?
23. How are incidents and notifications reported in your bank?

_____

24. Is activity of SOC personnel monitored to detect potential unauthorized access to critical systems of your bank?

_____

25. How does the SOC team determine the impact of security events and establish incident alert thresholds?

_____

26. Does your bank have legal controls and procedures in place that is adopted from the national and international cybercriminal laws to prosecute individuals and entities who may commit cybercrimes or financial frauds.

_____