To Strengthen the Cybersecurity Posture of SACCOs in Kenya by Assessing Current Practices, Developing a CTI Sharing Platform, And Formulating Supportive Policy Guidelines

Pius Kiprotich Sigei[1] Dr. Shem Mbandu Angolo[2], Dr. Andrew Omala[3]
School of Computing and Mathematics, Co-operative University of Kenya[123]
Email: sigei.pius@gmail.com/kiprotich24.pius@student.cuk.ac.ke

Abstract

The study investigated to strengthen the cybersecurity posture of SACCOs in Kenya by assessing current practices, developing a CTI sharing platform, and formulating supportive policy guidelines and was based on the following research objective: Creating a platform for sharing Cyber Threat Intelligence (CTI). The research was based on the following research questions: What design and implementation strategies would make a CTI sharing platform viable for SACCOs? The study was based on the Diffusion of Innovations (DoI) Theory developed by Everett M. Rogers in 1962 which explains how, why, and at what rate new ideas and technology spread through cultures, institutions, or organizations and is highly applicable to the design and adoption of a CTI platform because it focuses on how innovation is communicated, the factors influencing adoption, and the roles of various stakeholders issues central to implementing CTI among financial cooperatives like SACCOs. The study targeted 20 Saccos, 120 ICT staffs and 5Management Heads. Census sampling was used to select all the Saccos, the Management Heads and ICT Staff. Anova was used for inferential statistics. Questionnaires and focus group discussions (FGDs). The questionnaires served as structured tools for gathering quantitative data, while the b) from ICT staff while FGDs were used to obtain qualitative insights and more in-depth perspectives on SACCO operations and the challenges they face from Management Heads. This combination allows for a comprehensive understanding of the research subject. Findings indicated Table 3 shows that there was a statistically significant difference between groups as determined by one-way ANOVA (F(4,114) = 18.348, p=.000), (F(4,114) = 15.794, p=.000), (F(4,114) = 12.643, p=.000).Out of the 10 factors used to investigate Creating a platform for sharing Cyber Threat Intelligence. All of them show that there was a strong significance implying that Creating a platform for sharing Cyber Threat Intelligence of Saccos has some influence on improved Cyber security posture.The study recommended: The rollout of the CTI platform should be phased starting with willing SACCOs for pilot testing and refine based on feedback before broader implementation and smaller SACCOs should be supported through partnerships or donor subsidies. Regular cyber briefings, joint simulation exercises, and quarterly feedback sessions should be institutionalized to promote SACCO cooperation.

Keywords: Assessing Cybersecurity posture, CTI sharing Platform, SACCOs
DOI: 10.7176/ISDE/15-05
Publication date: September 30th 2025

1.0 Introduction

In the USA, Truong, et al. (2022) Conducted an empirical study to evaluate the effectiveness of automated CTI sharing using machine learning in U.S.-based security operations centers (SOCs) assessed MISP-based sharing with MITRE ATT&CK tagging across financial and healthcare sectors and found enhanced detection capabilities but noted challenges in trust and real-time correlation. Nweke et al. (2021) investigated user perceptions and adoption factors of CTI platforms across multiple U.S. sectors using the Technology Acceptance Model (TAM) and indicated that system quality and organizational culture significantly influenced usage. In the UK, Hutchings & Clayton, (2021) Conducted a UK-wide analysis of trust dynamics in cyber threat intelligence sharing networks, including law enforcement and private cybersecurity firms through interviews and document analysis, they identified information control and liability concerns as barriers to platform development. Goutam & Buchanan, (2020) Designed and tested a decentralized CTI sharing platform using blockchain and zero-knowledge proofs and showed the system could securely enable sharing between competing entities while maintaining data privacy.

In Canada, Dawson & Rahim, (2019) Canadian scholars conducted a study on the readiness of small and medium enterprises (SMEs) to adopt CTI platforms and found that lack of standards and leadership support limited participation since their work led to recommendations for a national CTI framework in Canada. Ali & Dehghantanha, (2020) proposed and empirically tested a multi-tier CTI sharing platform for Canadian critical infrastructure sectors which integrated anomaly detection tools with a sharing protocol based on STIX/TAXII. Pilot testing demonstrated improved alert correlation and situational awareness. In France, Lévy-Bencheton &

Pignolet, (2018) developed and evaluated a collaborative CTI sharing prototype called SIEVE, in collaboration with French telecom providers and incorporated real-time DNS abuse detection and incident reporting workflows. Their study found increased response times and stakeholder trust. Thales Group (2023) Coordinated a national-level project funded by the French government to develop a federated CTI platform based on privacy-preserving AI which involved 10 partners demonstrated early-stage empirical results showing effectiveness in threat trend detection across sectors.

In Nigeria, Nainna, Bass, and Speakman (2024) conducted a qualitative study using grounded theory to examine the behavior of cybersecurity practitioners regarding CTI sharing and found a positive disposition toward sharing threat data although two main barriers emerged: lack of technical capacity in managing standardized CTI protocols (such as STIX/TAXII) and an absence of data protection frameworks to guarantee trust and confidentiality. Okonkwo (2024) provided evidence of the role of cyber threat intelligence in preventing major attacks on Nigerian banks between 2020 and 2023 and emphasized the necessity of developing a structured national CTI-sharing platform to support proactive cybersecurity measures and pointed out that most organizations rely on informal, email-based exchanges of intelligence, which limits detection timeliness and coordination. In South Africa, Mtsweni, Mutemwa, and Mkhonto (2023), affiliated with the Council for Scientific and Industrial Research (CSIR), proposed and empirically tested a CTI-sharing model based on big data feeds from critical infrastructure which piloted with simulated threat inputs, incorporated advanced analytics to correlate diverse threat indicators and disseminate real-time alerts and demonstrated the potential for sector-wide coordination and significantly improved situational awareness and also emphasized the importance of trust management and legal clarity in CTI sharing among competing infrastructure entities.

In Egypt, El-Kosairy, AbdelBaki, and Aslan (2024) explored the integration of blockchain technology with CTI platforms to enhance data confidentiality and participant anonymity on Egyptian cybersecurity professionals and IT managers, who confirmed that concerns over data leakage and surveillance inhibited participation in CTI exchanges and found that blockchain-based platforms could serve as a trust enabler by allowing traceable but immutable intelligence sharing thus developed a prototype that combined decentralized ledgers with standard CTI feeds such as STIX, and proposed that future systems should focus on hybrid architectures to balance transparency and privacy. In Ghana, Akwei (2025) outlined the pressing need for trust-based regional CTI platforms, especially in the wake of growing attacks on financial and government institutions and proposed a phased approach beginning with low-tech, encrypted CTI mailing lists among key stakeholders, eventually scaling into a digital platform modeled after successful international cases like FS-ISAC.

In Tanzania, Mgaya and Mtenzi (2020) investigated the challenges of information security management in Tanzanian public institutions and found that the absence of centralized intelligence-sharing systems and inter-institutional trust are major obstacles to effective cyber threat mitigation. Further, the Tanzania Communications Regulatory Authority (TCRA) and the Tanzania Computer Emergency Response Team (TZ-CERT) have been instrumental in coordinating cyber threat responses and issuing advisories. A 2023 policy brief from TCRA evaluated the current state of cybersecurity in Tanzania and emphasized the role of public-private partnerships in establishing a centralized threat intelligence exchange system. While not academic, this government-led assessment reflects a growing institutional understanding of CTI's strategic importance.

In Uganda, Tumwesigye and Mbarika (2019) addressed cybersecurity resilience among Ugandan financial institutions and found that while several banks use commercial threat feeds, there was no national or sector-wide CTI-sharing platform and participants in the study expressed concern over the legal liability of sharing breach-related data and a lack of regulatory frameworks to protect contributors and concluded by recommending a multi-stakeholder CTI-sharing framework aligned with international standards like STIX and TAXII. Additionally, the Uganda Communications Commission (UCC) and CERT-UG have continued to build technical capacity for cyber defense. In a 2021 report published by the National Information Technology Authority Uganda (NITA-U), cybersecurity experts outlined a phased plan to develop a national threat intelligence platform, including stakeholder training and infrastructure development. While implementation is ongoing, the report provides foundational empirical insights into the country's capacity for CTI sharing. In Rwanda, Nsengiyumva and Ruhangaza (2022) conducted an exploratory study on digital security risks in Rwanda’s public sector and indicated that public institutions often lack real-time access to threat intelligence, leading to delayed responses and recommended the creation of a centralized threat intelligence coordination platform, hosted by the Rwanda Information Society Authority (RISA), to enable rapid information sharing among government agencies.

In Kenya, Mwendwa (2021), which developed a honeypot-based malware analysis tool tailored to SACCO networks in Kenya. Although not a CTI-sharing platform per se, this prototype demonstrated how honey pot logs including captured malware hashes and associated IP addresses can provide actionable intelligence, potentially usable in cooperative-level sharing systems. Muchilwa (2022) designed and implemented a mobile-centric CTI-sharing platform that enabled stakeholders to report and share fraudulent phone numbers across a broader network which tested via university and regional user groups, provided a proof of concept for crowdsourced threat intelligence that SACCOs could adapt to flag phishing or SIM-swap incidents. Mutua (2023) carried out a case study on fileless malware threat protection in Nairobi SACCOs although focused on memory-forensics detection models, the study employed theoretical frameworks (TAM, PMT) relevant to CTI acceptance and usage and underscored the importance of structured intelligence sharing such as alert dissemination or indicator exchange based on member detection systems. A Apanja & Matabi, (2020) revealed widespread cybersecurity gaps among SACCOs: minimal transaction monitoring, lack of budgets, absence of cybersecurity policy, and infrequent vendor due diligence and stressed the need for Sacco-to-Sacco collaboration platforms to share incident data and vendor risk alerts setting the stage for CTI platform discussions

1.2. Problem statement.

SACCOs are now more at risk from cyber threats due to digital financial services. SACCOs help to build financial inclusion and also encourage economic development. Yet, cybersecurity preparedness and awareness is still not perfect for them. SACCO employees are not well informed about cybersecurity, causing the risk of data breaches, fraud and a loss of member trust to grow. In addition, because there is not one set approach to evaluate cyber readiness, each SACCO manages security in its own way (Oduor & Abong'o, 2023). Through this case study, the cybersecurity readiness of SACCOs in Bomet County was investigated, along with any known gaps, problems and chances for success in cybersecurity. It also reviews how effectively SACCOs are able to identify, block and solve cyber risks as digital security keeps developing. An important weakness is that there isn't a central place where SACCOs can connect, exchange threat knowledge and adapt to industry security practices together. If not for a networked system, each SACCO must handle cybersecurity by itself, using only what they have and acting only after an attack happens, so they face high cybersecurity threats. Banks and microfinance institutions are now ahead of the game because they use collaboration, AI tools and effective cybersecurity.

The GSMA Mobile Money Report (2022) revealed that 1.4 billion individuals across the world do not use banks, proving that getting reliable digital financial services to these people helps increase financial inclusion. The financial ecosystem in Kenya relies heavily on SACCOs which provide credit and transaction services to many farmers and small business owners living in underserved areas (SASRA Annual Report, 2023). It worries me that many companies use digital resources a lot but don't focus enough on cybersecurity or preparation for risks. According to the Serianu report published in 2021, 95% of African SACCOs are so poorly prepared for cyber-attacks that their members' data and finances are at huge risk. Because of this, they do not have the best resources and techniques to defend their networks. In 2009, the Government of Kenya set up SACCO Societies Regulations Authority (SASRA) with guidelines for risk management practices. But apparently, many of our SACCOs seem to put more emphasis on compliance as a means to meet regulatory requirements rather than build their cybersecurity capability. Compliance is thought of as a box ticking exercise where little is invested in building resilience to real time threats. That narrow focus however culminates in crucial gaps in cybersecurity frameworks, creating a massive risk to the economic reliability and integrity of SACCOs. There is an urgent need therefore to assess, not only, this kind of cybersecurity readiness of SACCOs, but also if it is feasible to develop such a compromised or shared cybersecurity information platform. A platform for such a system could enable proactive defense mechanisms, real time incident reporting, knowledge sharing and strategies of collective response. These issues need to be addressed to protect members' financial assets, enhance SACCOs technological resilience and ensure long term sustainability of SACCO operations in a digitally driven financial environment.

1.3 Purpose of the Study

The study investigated to strengthen the cybersecurity posture of SACCOs in Kenya by assessing current practices, developing a CTI sharing platform, and formulating supportive policy guidelines.

1.4 Research Objective

The study was based on the following research objective

1. Creating a platform for sharing Cyber Threat Intelligence (CTI)

1.5 Research Questions.

The research was based on the following research questions:

1. What design and implementation strategies would make a CTI sharing platform viable for SACCOs?

2.0 Literature Review

2.1 Creating a platform for sharing Cyber Threat Intelligence (CTI)

Matanda (2020) carried out a case study on cybersecurity readiness within Nairobi DT SACCOs, identifying vulnerabilities in mobile banking systems and recommended that incident reporting templates and collaborative detection mechanism elements essential to CTI systems. Nambiro et al. (2021) examined cybersecurity challenges in mobile banking for SACCOs and mitigation approaches and stressed the value of shared threat intelligence feeds to counter phishing, malware, and insider attacks. A Serianu and sector-wide survey (2021) in collaboration with KUSCCO and WOCCU highlighted lack of threat sharing, incident reporting, and vendor alert systems among Kenyan SACCOs and recommended establishing cooperative platforms for logging and disseminating threat intelligence. Kamary, (2018) explored Kenya's national cybersecurity context, pointing to institutional weaknesses and the need for collaborative intelligence frameworks elements relevant to future SACCO CTI initiatives. Wachira (2021) studied factors affecting information security in a Kenya National Police SACCO during teleworking and emphasized formal communication channels, incident logging, and shared threat awareness practical features for CTI platform design. Muchilwa (2022) designed and implemented a mobile/web-based CTI-sharing platform for reporting fraudulent phone numbers a common cyber threat vector affecting SACCO members and field evaluations with Nairobi-based user groups confirmed that shared fraud intelligence improved detection and expedited response, offering a usable model for a broader cooperative CTI network infrastructure. Hezron (2024) reported that SACCO cybersecurity strategy adoption rose from 38 percent in 2019 to 55 percent in 2020, with increased budget allocations noted; but the report also called attention to persistent gaps in inter-Sacco information sharing and vendor coordination factors central to CTI platform deployment. The KUSCCO-WOCCU/IRNet survey (2020–2021) documented cybersecurity gaps among 18 SACCOs: five had experienced cyberattacks, most lacked digital transformation or monitoring systems, and many had no cybersecurity policies or budgets respondents recommended shared mechanisms such as blacklist sharing and vendor risk alerts precursors to CTI-sharing function.

2.2 Theoretical Framework

The study was based on the Diffusion of Innovations (DoI) Theory developed by Everett M. Rogers in 1962 which explains how, why, and at what rate new ideas and technology spread through cultures, institutions, or organizations and is highly applicable to the design and adoption of a CTI platform because it focuses on how innovation is communicated, the factors influencing adoption, and the roles of various stakeholders issues central to implementing CTI among financial cooperatives like SACCOs.The Diffusion of Innovations Theory classifies adopters into five categories innovators, early adopters, early majority, late majority, and laggards and posits that adoption is influenced by five key factors: relative advantage, compatibility, complexity, trialability, and observability. When applied to CTI platform development for SACCOs, these factors inform how the platform should be designed, introduced, and communicated to ensure acceptance and widespread use across institutions. The Diffusion of Innovations Theory directly informs the research objective by offering a structured approach to identifying the most effective design and implementation strategies for a CTI platform and understanding how SACCOs perceive new technologies, what influences their adoption decisions, and how information about the innovation spreads within the cooperative sector will be crucial to ensure a successful rollout of such a platform. The theory's focus on communication channels and adopter categories aligns well with SACCOs' varied technological capabilities, cultural norms, and collaborative tendencies.

3.0 Materials and Methods

Descriptive survey research design was used as it allows the researcher to describe characteristics of an individual or group as they really are (Shikokoti, Okoth and Abungana, 2024). Descriptive surveys are only concerned with conditions or relationships that exist, opinions that are held and processes that are ongoing. The study targeted 20 Saccos, 120 ICT staffs and 5Management Heads. Census sampling was used to select all the Saccos, the Management Heads and ICT Staff. Anova was used for inferential statistics. Questionnaires and focus group discussions (FGDs). The questionnaires served as structured tools for gathering quantitative data, while the b) from ICT staff while FGDs were used to obtain qualitative insights and more in-depth perspectives on SACCO operations and the challenges they face from Management Heads. This combination allows for a comprehensive understanding of the research subject.

4.0 Results

4.1 Creating a platform for sharing Cyber Threat Intelligence

The researcher sought to establish an Creating a platform for sharing Cyber Threat Intelligence. Descriptive statistics such as frequencies, percentages, Means and Standard Deviation were utilized. The rating was based on Likert Scale where 1=Strongly Disagree (SD), 2=Disagree (D), 3=Neutral(N), 4= Agree (A), 5= Strongly Agree (SA). The results of objective one were presented in Table 1 which shows Distribution of ICT staff on Creating a platform for sharing Cyber Threat Intelligence

Table 1: Distribution of ICT staff on Creating a platform for sharing Cyber Threat Intelligence

Statement	SD		D		N		A		SA		Mean	Sd
	f	%	f	%	f	%	f	%	f	%		
A CTI sharing platform would significantly improve my SACCO's ability to respond to cyber threats	7	5.9	3	2.5	16	13.4	31	26.1	62	52.1	4.16	1.127
SACCOs should have a standardized protocol for sharing cyber threat intelligence to ensure consistency	4	3.4	2	1.7	20	16.8	23	19.3	70	58.8	4.29	1.026
Implementing a CTI platform requires extensive training for SACCO staff to be effective	4	3.4	2	1.7	14	11.8	25	21.0	74	62.2	4.37	0.990
A CTI sharing platform should include real-time alerts to help SACCO address threats quickly.	2	1.7	3	2.5	10	8.4	25	21.0	79	66.4	4.48	0.882
Privacy concerns could hinder the effective implementation of a CTI sharing platform among SACCOs.	7	5.9	4	3.4	24	20.2	33	27.7	51	42.9	3.98	1.142
Collaboration amongst SACCOs on cyber threat sharing strengthen our collective cybersecurity efforts	3	2.5	8	6.7	16	13.4	19	16.0	73	61.3	4.27	1.087
A CTI platform should be managed by a centralized authority to ensure trust and reliability.	5	4.2	6	5.0	17	14.3	24	20.2	67	56.3	4.19	1.122
SACCOs would benefit from a CTI platform that allows anonymous sharing of	9	7.6	4	3.4	12	10.1	32	26.9	62	52.1	4.13	1.197

threat intelligence.												
The benefits of implementing a CTI sharing platform would outweigh the costs incurred by the SACCOs.	4	3.4	8	6.7	25	21.0	31	26.1	51	42.9	3.98	1.105
Regular updates and feedback mechanisms are essential for a CTI platform to remain effective for SACCOs.	3	2.5	4	3.4	17	14.3	21	17.6	74	62.2	4.34	1.011
Average Mean											**4.22**	**1.069**

Table 1 shows that majority, a total of 62 ICT staff, accounting for (52.1%) of the participants, Strongly Agreed that A CTI sharing platform would significantly improve my SACCO's ability to respond to cyber threats while 31(26.1%) Agreed and 16(13.4%) were Neutral respectively that A CTI sharing platform would significantly improve my SACCO's ability to respond to cyber threats with a mean score of 4.16, with a standard deviation of 1.127. This implies that A CTI sharing platform would significantly improve my SACCO's ability to respond to cyber threats. The findings are in line with Ahmed, (2025) who found that 78% of security teams reported faster incident resolution after integrating CTI into their workflows.

Regarding SACCOs should have a standardized protocol for sharing cyber threat intelligence to ensure consistency in Table 1, Majority a total of 70 ICT staff, accounting for 58.8% of the participants, Strongly Agreed that SACCOs should have a standardized protocol for sharing cyber threat intelligence to ensure consistency while 23(19.3%) Agreed and 20(16.8%) were Neutral that SACCOs should have a standardized protocol for sharing cyber threat intelligence to ensure consistency with a mean score for this question was 4.29, with a standard deviation of 1.026. This implies that SACCOs should have a standardized protocol for sharing cyber threat intelligence to ensure consistency. The findings are consistent with Kayode-Ajala, (2023) who highlighted interoperability challenges and the need for standardized formats to streamline CTI adoption

Table 1 shows on Implementing a CTI platform requires extensive training for SACCO staff to be effective Majority, A total of 74 ICT staff, accounting for (62.2%) of the participants, Strongly Agreed that Implementing a CTI platform requires extensive training for SACCO staff to be effective while 25(21.0%) agreed and 14(11.8%) were Neutral respectively with a mean score of 4.37 and a standard deviation of 0.990. This implies that Implementing a CTI platform requires extensive training for SACCO staff to be effective. The findings concurred with Trocoso-Pastoriza et al. (2022) who demonstrated complexity in privacy-preserving frameworks (e.g., federated sharing) requires staff expertise

Table 1 shows that majority, a total of 79ICT staff, accounting for 66.4% of the participants, Strongly Agreed that A CTI sharing platform should include real-time alerts to help SACCO address threats quickly while 25(21.0%) Agreed and 10(8.4%) Agreed respectively that A CTI sharing platform should include real-time alerts to help SACCO address threats quickly with a mean score of 4.48 and a standard deviation of 0.882. This implies that A CTI sharing platform should include real-time alerts to help SACCO address threats quickly. The findings are in line with Aziz, (2023) who reported CTI-enabled systems deliver real-time threat awareness, enabling proactive defense

Regarding Privacy concerns could hinder the effective implementation of a CTI sharing platform among SACCOs in Table 1, Majority a total of 51 ICT staff, accounting for 42.9% of the participants, Strongly Agreed that Privacy concerns could hinder the effective implementation of a CTI sharing platform among SACCOs while 33(27.7%) Agreed and 24(20.2%) were Neutral respectively that Privacy concerns could hinder the effective implementation of a CTI sharing platform among SACCOs with a mean score of 3.98 and a standard deviation of 1.142. This implies that Privacy concerns could hinder the effective implementation of a CTI sharing platform among SACCOs. The findings are consistent with Albakri, Boiten & Smith, (2020) who modeled CTI-sharing risks including leakage of sensitive data and proposed mitigation techniques. The findings are also in agreement with Jesus, Bains & Chang, (2023) who analyzed 1 million MISP feeds and concluded confidentiality is a major sharing barrier, but can be managed with proper sanitization

Table 1 shows on Collaboration amongst SACCOs on cyber threat sharing strengthen our collective cybersecurity efforts Majority, A total of 73 ICT staff, accounting for (61.3%) of the participants, Strongly Agreed that Collaboration amongst SACCOs on cyber threat sharing strengthen our collective cybersecurity efforts while 19(16.0%) Agreed and 16(13.4%) were Neutral that Collaboration amongst SACCOs on cyber threat sharing strengthen our collective cybersecurity efforts with a mean score of 4.27 and a standard deviation of 1.087. This implies that Collaboration amongst SACCOs on cyber threat sharing strengthen our collective cybersecurity efforts. The findings concur with Trocoso-Pastoriza et al. (2022) who demonstrated that federated, distributed CTI sharing improves collective detection while preserving privacy.

Regarding A CTI platform should be managed by a centralized authority to ensure trust and reliability in Table 1, Majority a total of 67 ICT staff, accounting for 56.3% of the participants, Strongly Agreed that A CTI platform should be managed by a centralized authority to ensure trust and reliability while 24(20.2%) Agreed and 17(14.3%) were Neutral respectively that Staff members are aware of the risks associated with data leakages with a mean score of 4.19 and a standard deviation of 1.122. This implies that A CTI platform should be managed by a centralized authority to ensure trust and reliability. The findings are consistent with Albakri, Boiten & Smith, (2020) who noted structured, policy-driven central oversight builds confidence in CTI ecosystems

Regarding SACCOs would benefit from a CTI platform that allows anonymous sharing of threat intelligence in Table 1, Majority a total of 62 ICT staff, accounting for 52.1% of the participants, Strongly Agreed that SACCOs would benefit from a CTI platform that allows anonymous sharing of threat intelligence while 32(26.9%) Agreed and 12(10.1%) were Neutral respectively that Staff members are aware of the risks associated with data leakages with a mean score of 4.13 and a standard deviation of 1.197. This implies that SACCOs would benefit from a CTI platform that allows anonymous sharing of threat intelligence. The findings are consistent with Jesus, Bains & Chang, (2023) who found anonymized CTI exchanges reduce confidentiality concerns and encourage wider participation

Regarding The benefits of implementing a CTI sharing platform would outweigh the costs incurred by the SACCOs in Table 1, Majority a total of 51 ICT staff, accounting for 42.9% of the participants, Strongly Agreed that The benefits of implementing a CTI sharing platform would outweigh the costs incurred by the SACCOs while 31(26.1%) Agreed and 25(21.0%) were Neutral respectively that The benefits of implementing a CTI sharing platform would outweigh the costs incurred by the SACCOs with a mean score of 3.98 and a standard deviation of 1.105. This implies that The benefits of implementing a CTI sharing platform would outweigh the costs incurred by the SACCOs. The findings are consistent with Okonkwo & Zhang (2024) who found that CTI-enhanced operations in financial firms achieved faster containment with limited overhead, indicating strong cost-effectiveness

Table 1 shows on Regular updates and feedback mechanisms are essential for a CTI platform to remain effective for SACCOs Majority, A total of 74 ICT staff, accounting for (62.2%) of the participants, Strongly Agreed that Regular updates and feedback mechanisms are essential for a CTI platform to remain effective for SACCOs while 21(17.6%) Agreed and 17(14.3%) were Neutral that Collaboration amongst Regular updates and feedback mechanisms are essential for a CTI platform to remain effective for SACCOs with a mean score of 4.34 and a standard deviation of 1.011. This implies that Regular updates and feedback mechanisms are essential for a CTI platform to remain effective for SACCOs. The findings concur with Trocoso-Pastoriza et al. (2022) who highlighted the need for iterative updates and sharing cycles to improve predictive capabilities. Table 2 which shows Distribution of ICT staff on Creating a platform for sharing Cyber Threat Intelligence using Anova

Table 2: Distribution of ICT staff on Creating a platform for sharing Cyber Threat Intelligence using Anova

		Sum of Squares	df	Mean Square	F	Sig.
SACCOs should have a standardized protocol for sharing cyber threat intelligence to ensure consistency"	Between Groups	28.535	4	7.134	8.493	.000
	Within Groups	95.751	114	.840		
	Total	124.286	118			
Implementing a CTI platform requires extensive training for SACCO staff to be effective."	Between Groups	45.326	4	11.331	18.348	.000
	Within Groups	70.405	114	.618		
	Total	115.731	118			
A CTI sharing platform should include real-time alerts to help SACCO address threats quickly."	Between Groups	15.195	4	3.799	5.661	.000
	Within Groups	76.503	114	.671		
	Total	91.697	118			
Privacy concerns could hinder the effective implementation of a CTI sharing platform among SACCOs.	Between Groups	27.243	4	6.811	6.127	.000
	Within Groups	126.723	114	1.112		
	Total	153.966	118			
Collaboration amongst SACCOs on cyber threat sharing strengthen our collective cybersecurity efforts	Between Groups	42.836	4	10.709	12.643	.000
	Within Groups	96.559	114	.847		
	Total	139.395	118			
A CTI platform should be managed by a centralized authority to ensure trust and reliability.	Between Groups	39.453	4	9.863	10.306	.000
	Within Groups	109.101	114	.957		
	Total	148.555	118			
SACCOs would benefit from a CTI platform that allows anonymous sharing of threat intelligence.	Between Groups	52.016	4	13.004	12.661	.000
	Within Groups	117.093	114	1.027		
	Total	169.109	118			
The benefits of implementing a CTI sharing platform would outweigh the costs incurred by the SACCOs.	Between Groups	26.964	4	6.741	6.568	.000
	Within Groups	117.003	114	1.026		
	Total	143.966	118			
Regular updates and feedback mechanisms are essential for a CTI platform to remain effective for SACCOs.	Between Groups	42.986	4	10.746	15.794	.000
	Within Groups	77.569	114	.680		
	Total	120.555	118			

Table 1 shows that there was a statistically significant difference between groups as determined by one-way ANOVA (F(4,114) = 18.348, p=.000), (F(4,114) = 15.794, p=.000), (F(4,114) = 12.643, p=.000), Implementing a CTI platform requires extensive training for SACCO staff to be effective, Regular updates and feedback mechanisms are essential for a CTI platform to remain effective for SACCOs and Collaboration amongst SACCOs on cyber threat sharing strengthen our collective cybersecurity efforts respectively. Out of the 10 factors used to investigate Creating a platform for sharing Cyber Threat Intelligence. All of them show that there was a strong significance implying that Creating a platform for sharing Cyber Threat Intelligence of Saccos has some influence on improved Cyberssecurity posture. Table 2 shows Management Heads' Focus Group Discussion Responses on Cyber Threat Intelligence (CTI) Sharing in SACCOs

Table 2: Management Heads' Focus Group Discussion Responses on Cyber Threat Intelligence (CTI) Sharing in SACCOs

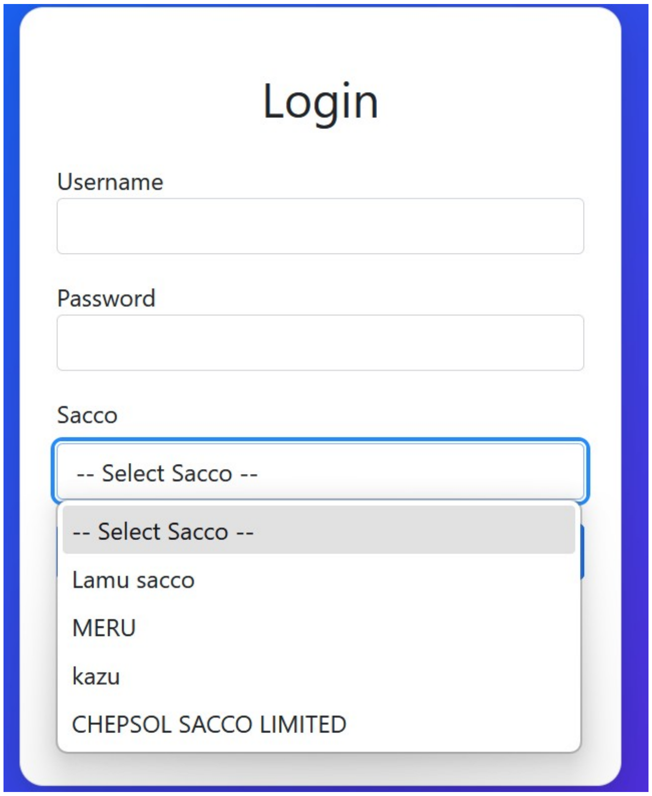
No.	CTI Sharing Statement	Code	Response Summary	Direct Quote
1	A CTI sharing platform would significantly improve my SACCO's ability to respond to cyber threats	P1	Believes a CTI platform would enhance awareness and response time.	"It would give us early warnings and help us respond quickly."
		P3	Agrees strongly; sees it as vital due to increasing cyber attacks.	"We are flying blind without real-time threat sharing."
2	SACCOs should have a standardized protocol for sharing cyber threat intelligence	P2	Agrees; standard protocols will ensure clarity and uniformity across SACCOs.	"We need one approach to make sure all SACCOs follow best practices."
		P4	Supports standardization but cautions about SACCO size differences.	"Smaller SACCOs may struggle if the protocol is too complex."
3	Implementing a CTI platform requires extensive training for SACCO staff to be effective	P1	Agrees; training needed for both technical and non-technical staff.	"Without training, even a good platform will fail."
		P3	Points out the lack of cybersecurity expertise in many SACCOs.	"We would need capacity-building before rolling it out."
4	A CTI platform should include real-time alerts to help SACCO address threats quickly	P2	Strongly agrees; says timely alerts are crucial.	"Real-time alerts are the only way to stop threats before damage is done."
5	Privacy concerns could hinder effective implementation of a CTI sharing platform	P4	Agrees; sensitive data sharing could raise legal issues.	"What happens if shared data leaks? Privacy must be addressed first."
		P1	Suggests encrypted and anonymized data to address concerns.	"Anonymity can help build trust in the system."
6	Collaboration amongst SACCOs on cyber threat sharing strengthens our collective cybersecurity efforts	P3	Strongly agrees; collaboration leads to better defense.	"One SACCO's experience can save many others from attack."
		P2	Advocates for more inter-SACCO forums and regular cyber briefings.	"Cybersecurity is not a competition, we must work together."
7	A CTI platform should be managed by a centralized authority to ensure trust and reliability	P4	Agrees if the authority is neutral and credible.	"KUSCCO or CBK would be ideal managers of the platform."
		P1	Cautions about bureaucracy and data misuse.	"Centralization must not become control or surveillance."
8	SACCOs would benefit from a CTI platform that allows anonymous sharing of threat intelligence	P3	Supports anonymous sharing to encourage openness.	"People are more willing to report if they don't fear repercussions."
		P2	Warns about the possibility of false reports.	"There must be a system to verify threats without revealing identities."
9	The benefits of implementing a CTI sharing platform would outweigh the costs incurred by the SACCOs	P1	Agrees; sees long-term cost savings in reduced cyber incidents.	"It's cheaper to prevent attacks than fix the damage later."
		P4	Cautious; says smaller SACCOs	"Costs are still a burden;

No.	CTI Sharing Statement	Code	Response Summary	Direct Quote
			need financial support.	maybe partner with donors or regulators.”
10	Regular updates and feedback mechanisms are essential for a CTI platform to remain effective for SACCOs	P3	Strongly agrees; feedback builds system trust and improvement.	“Continuous improvement needs ongoing feedback from users.”
		P2	Recommends quarterly review and technical audits of the CTI system.	“Without updates, the platform becomes obsolete quickly.”

From the responses of Management heads in Table 4.2 we can imply that expressed general support for a CTI platform, provided that concerns around cost, privacy, and capacity-building are addressed have a strong agreement on the value of standardization, real-time alerts, and collaboration among SACCOs. Figure 1 shows Security Analytics Dashboard Overview

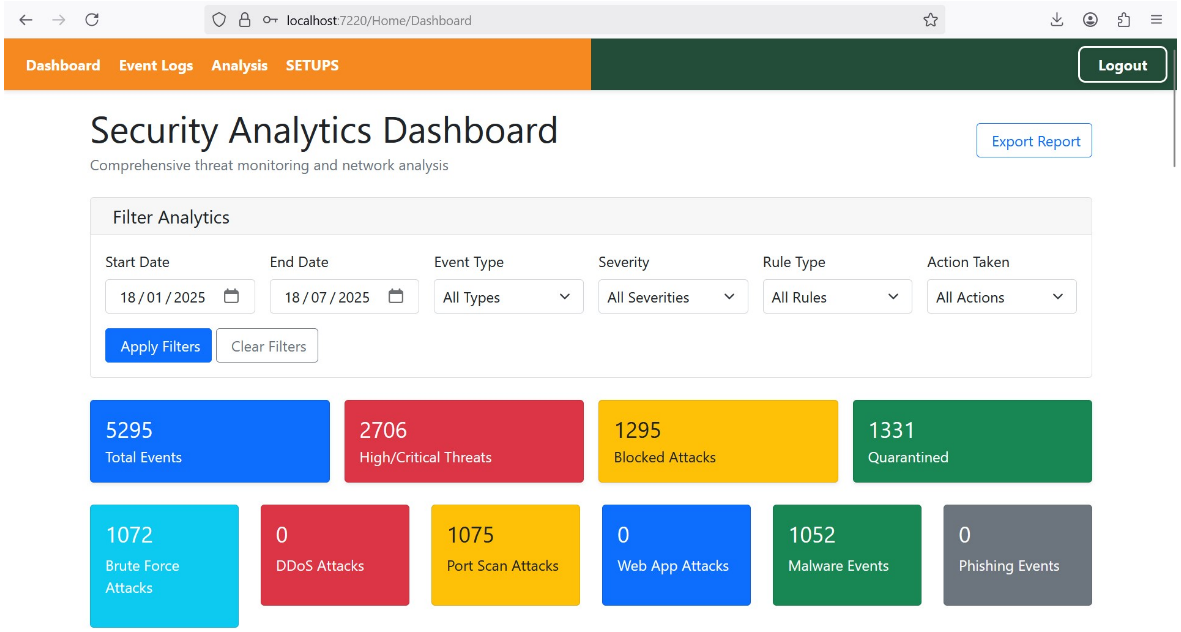
Figure 1 Security Analytics Dashboard Overview

Attribute	Tools	Extensions
LANGUAGE	C#	
DB	MS SQL	
ANALYSIS	PHYTON	APIs



This is used to access the system by inserting your username, password and the sacco a person belongs in. Figure 2 shows the CTI platform Security Analytics Dashboard

Figure 2: CTI platform Security Analytics Dashboard…66



localhost:7220/Home/Dashboard

Dashboard Event Logs Analysis SETUPS Logout

Security Analytics Dashboard

Comprehensive threat monitoring and network analysis

Export Report

Filter Analytics

Start Date	End Date	Event Type	Severity	Rule Type	Action Taken
18 / 01 / 2025	18 / 07 / 2025	All Types	All Severities	All Rules	All Actions

Apply Filters Clear Filters

5295 Total Events

2706 High/Critical Threats

1295 Blocked Attacks

1331 Quarantined

1072 Brute Force Attacks

0 DDoS Attacks

1075 Port Scan Attacks

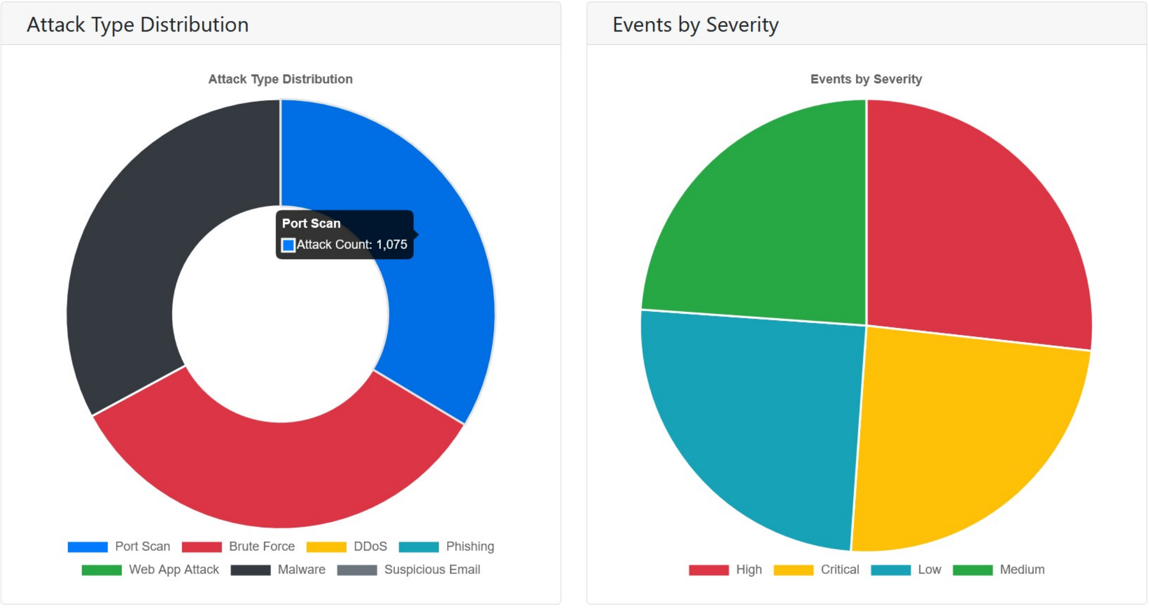
0 Web App Attacks

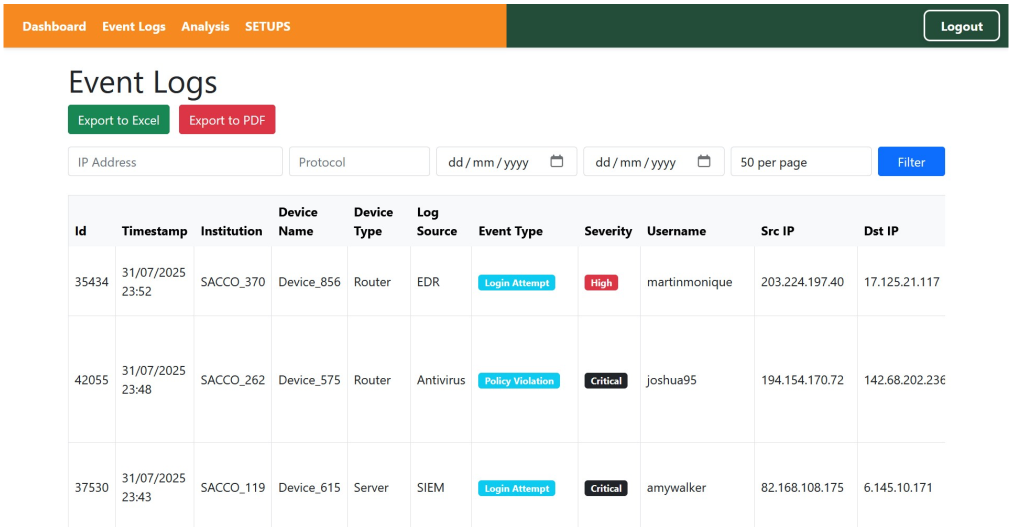
1052 Malware Events

0 Phishing Events

As portrayed in Figure 2 A Security Analytics Dashboard is a centralized visual interface that provides real-time insights and summaries of an organization's cybersecurity posture, based on collected data from various security tools and systems. i.e a total of 5,317 security events were recorded, out of which 2,727 were classified as high or critical threats, indicating a significant threat landscape. From these, 1,296 attacks were successfully blocked, and 1,352 threats were quarantined, helping to contain further risk. Notably, 1,072 instances involved potential breaches or harmful activity, while no brute force attacks were detected during the reporting period. Figure 4 shows the CTI platform Security Analytics Dashboard

Figure 4: CTI platform Attack type Distribution and Event Logs





Event Logs

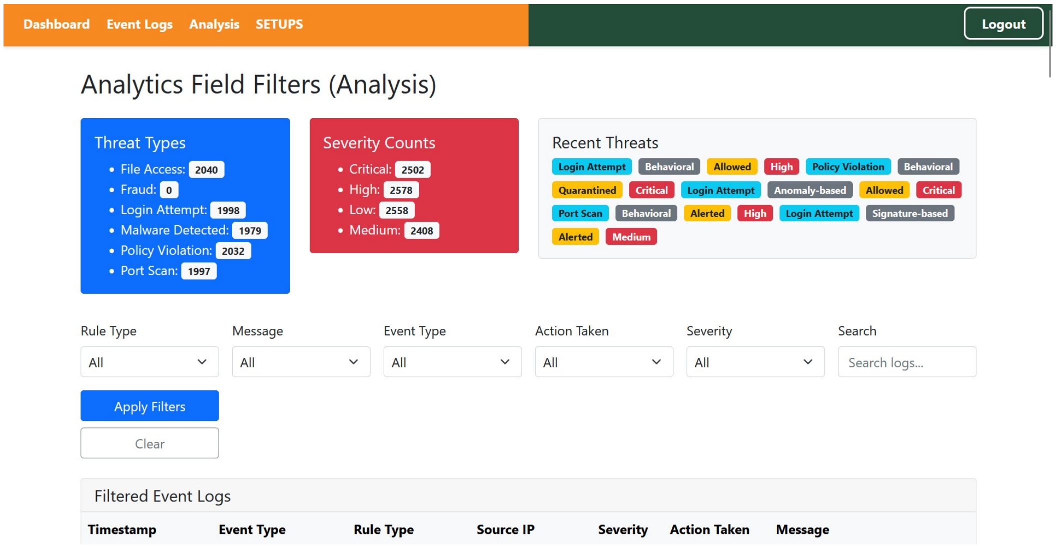
Id	Timestamp	Institution	Device Name	Device Type	Log Source	Event Type	Severity	Username	Src IP	Dst IP
35434	31/07/2025 23:52	SACCO_370	Device_856	Router	EDR	Login Attempt	High	martinmonique	203.224.197.40	17.125.21.117
42055	31/07/2025 23:48	SACCO_262	Device_575	Router	Antivirus	Policy Violation	Critical	joshua95	194.154.170.72	142.68.202.236
37530	31/07/2025 23:43	SACCO_119	Device_615	Server	SIEM	Login Attempt	Critical	amywalker	82.168.108.175	6.145.10.171

These event logs capture detailed records of security-related activities within SACCO networks, highlighting key attributes such as timestamp, event type, source and destination IPs, user involved, and the action taken.

For example, on 31st July 2025 at 23:52, a high-severity login attempt was detected on a router (Device_856) at SACCO_370, involving the user martinmonique. The attempt originated from IP 203.224.197.40 and targeted IP 17.125.21.117 over TCP port 7343, and while the attempt was allowed, further behavioral analysis revealed malware was blocked, resulting in a policy violation marked as critical. The event was categorized under behavioral rules, and no live packet capture (PCAP) was taken. Additional context suggests suspicious activity was identified based on the rule: *"Source check laugh allow nation."* A secondary user account ghill was also flagged, and the final action was to block the event.

Another event logged at 23:48 on the same day from SACCO_262 indicated a critical policy violation detected by the antivirus system on Device_575. The activity involved user joshua95, with traffic between IPs 194.154.170.72 and 142.68.202.236, using TCP ports 33779 and 12670. This event was quarantined, indicating containment action was taken to prevent further threat propagation. Figure 3 shows CTI platform Analytics Field Filters

Figure 3: CTI platform Analytics Field Filters



Analytics Field Filters (Analysis)

Threat Types
- File Access: 2040
- Fraud: 0
- Login Attempt: 1998
- Malware Detected: 1979
- Policy Violation: 2032
- Port Scan: 1997

Severity Counts
- Critical: 2502
- High: 2578
- Low: 2558
- Medium: 2408

Recent Threats

Login Attempt Behavioral Allowed High Policy Violation Behavioral
Quarantined Critical Login Attempt Anomaly-based Allowed Critical
Port Scan Behavioral Alerted High Login Attempt Signature-based
Alerted Medium

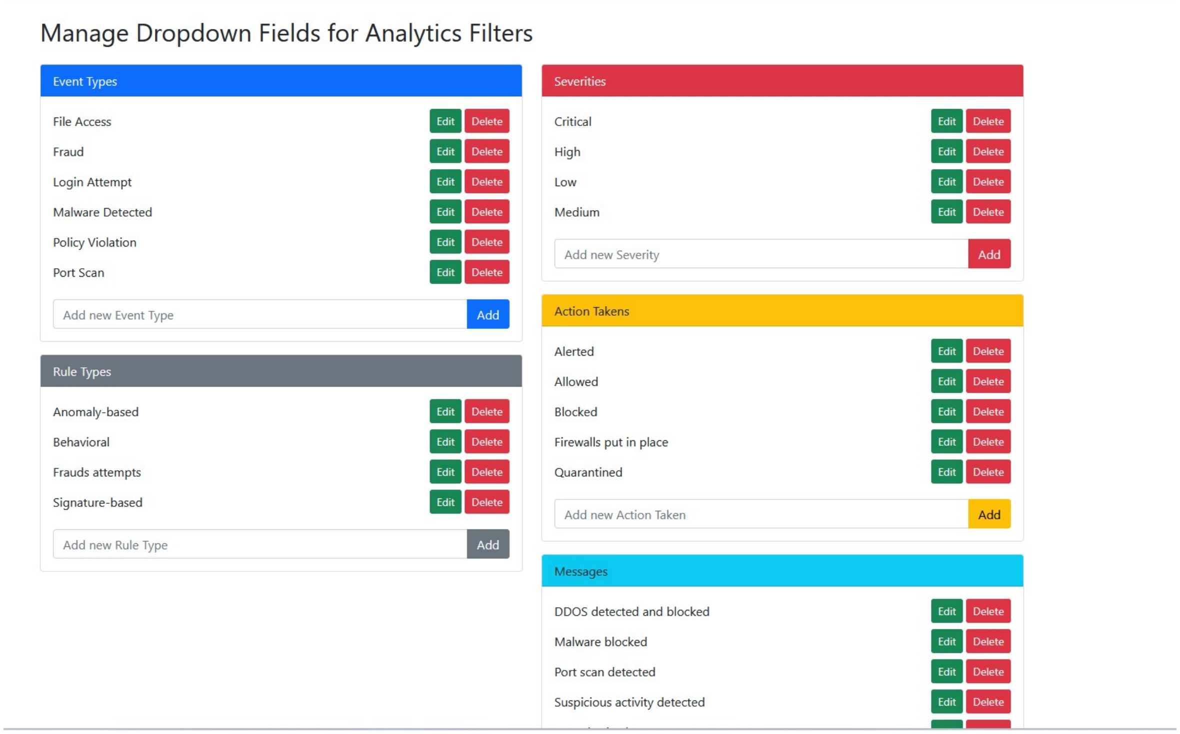
Rule Type	Message	Event Type	Action Taken	Severity	Search
All	All	All	All	All	Search logs...

Filtered Event Logs

Timestamp	Event Type	Rule Type	Source IP	Severity	Action Taken	Message

Figure 4 shows CTI platform Manage Dropdown fields for Analytics filters that has been created

Figure 4: CTI platform Manage Dropdown fields for Analytics filters that has been created



Manage Dropdown Fields for Analytics Filters

Event Types

- File Access
- Fraud
- Login Attempt
- Malware Detected
- Policy Violation
- Port Scan

Add new Event Type

Rule Types

- Anomaly-based
- Behavioral
- Frauds attempts
- Signature-based

Add new Rule Type

Severities

- Critical
- High
- Low
- Medium

Add new Severity

Action Takens

- Alerted
- Allowed
- Blocked
- Firewalls put in place
- Quarantined

Add new Action Taken

Messages

- DDOS detected and blocked
- Malware blocked
- Port scan detected
- Suspicious activity detected

5.0 Discussion and Conclusion

The results of the second objective indicated Table 3 shows that there was a statistically significant difference between groups as determined by one-way ANOVA (F(4,114) = 18.348, p=.000), (F(4,114) = 15.794, p=.000), (F(4,114) = 12.643, p=.000), Implementing a CTI platform requires extensive training for SACCO staff to be effective, Regular updates and feedback mechanisms are essential for a CTI platform to remain effective for SACCOs and Collaboration amongst SACCOs on cyber threat sharing strengthen our collective cybersecurity efforts respectively. Out of the 10 factors used to investigate Creating a platform for sharing Cyber Threat Intelligence. All of them show that there was a strong significance implying that Creating a platform for sharing Cyber Threat Intelligence of Saccos has some influence on improved Cyber security posture.

The Focus Group Discussions painted a more uneven picture highlighting that implementation of security measures is often reactive, driven by incidents rather than proactive planning. Key tools like vulnerability scanners and access controls are frequently missing, and on-site personnel typically lack cyber-specific training. Managers acknowledge cybersecurity risks but often defer responsibility to ICT officers, with limited strategic prioritization or budgetary support. Roles and policies are poorly communicated across the organization, and training for general staff is inconsistent, often occurring only after breaches. Together, these findings underscore the need for SACCOs to move beyond basic compliance and adopt a more cohesive, organization-wide cybersecurity strategy that includes consistent infrastructure upgrades, role clarity, proactive training, and greater institutional commitment

Recommendation

The study was based on the following recommendation:

2. The Government of Kenya through the Central Bank of Kenya (CBK), Communications Authority (CA), or SACCO Societies Regulatory Authority (SASRA) should develop and oversee a centralized CTI platform.

3. Saccos should conduct training on incident reporting, threat analysis, privacy laws, and use of the CTI system. Capacity-building programs must include both technical and non-technical SACCO staff to foster a culture of cyber awareness.
4. SACCOs should establish dedicated cybersecurity committees comprising ICT personnel, management, and compliance officers guiding risk management strategy, and ensuring feedback loops with platform updates.
5. The rollout of the CTI platform should be phased starting with willing SACCOs for pilot testing and refine based on feedback before broader implementation and smaller SACCOs should be supported through partnerships or donor subsidies.
6. Regular cyber briefings, joint simulation exercises, and quarterly feedback sessions should be institutionalized to promote SACCO cooperation.
7. Integrate CTI features into current mobile money, core banking, or digital service platforms already in use by SACCOs. T
8. The CTI platform should include built-in audit tools, dashboards for event trend analysis, and mechanisms for regular system updates and periodic evaluations by SASRA or the National KE-CIRT Coordination Centre should guide improvements.

References

Akwei, E. (2025). *The growing cyber threat landscape in West Africa: A call for regional CTI platforms*. The New Crusading Guide.

Ali, S., & Dehghantanha, A. (2020). Designing an intelligent cyber threat intelligence sharing architecture for Canada's critical infrastructure. *Computers & Security, 89, 101667.*

Apanja, B., & Matabi, M. (2020). *Cybersecurity readiness of SACCOs in Kenya.* KUSCCO & WOCCU / IRNet survey report.

Dawson, M., & Rahim, H. (2019). Cyber threat intelligence sharing: Challenges and enablers within Canadian SMEs. *Journal of Information Warfare, 18(1), 39–50.*

El-Kosairy, A. A., AbdelBaki, M. A., & Aslan, H. A. (2024). Integrating blockchain with cyber threat intelligence sharing: A survey of Egyptian cybersecurity experts. *International Journal of Safety and Security Engineering*, 14(5), 525–534

Goutam, A., & Buchanan, W. J. (2020). A decentralized platform for secure cyber threat intelligence sharing using blockchain and zero-knowledge proofs. *Future Generation Computer Systems, 113, 534–547.*

Hutchings, A., & Clayton, R. (2021). Exploring trust in cyber threat intelligence sharing: A UK case study. *Journal of Cyber Policy, 6(2), 223–242.*

Lévy-Bencheton, C., & Pignolet, Y. (2018). SIEVE: A prototype platform for collaborative cyber threat intelligence sharing among telecom providers. *Computer Networks, 135, 56–70.*

Mgaya, R. & Mtenzi, F. (2020). An Assessment of Information Security Management in Tanzanian Public Institutions. *Journal of Cybersecurity and Information Systems*, 7(2), 35–49

Mtsweni, J., Mutemwa, M., & Mkhonto, T. (2023). Development of a cyber threat intelligence sharing model based on big data sources in South Africa. *Journal of Information Warfare*, 15(3), 45–60

Muchilwa, L. (2022). *Design and Implementation of a Cyber Threat Intelligence Sharing Platform for Reporting Fraudulent Phone Numbers* (Project report). USIU-Africa.

Mutua, I. W. (2023). *A Model for Advanced Analysis of Fileless Malware Threats through*

Memory Forensics in SACCOs in Nairobi County (MSc Thesis). USIU-Africa

Mwendwa, K. M. (2021). *A Honeypot based malware analysis tool for SACCOs in Kenya* (MSc

Thesis). Strathmore University.

Nainna, A., Bass, S., & Speakman, B. (2024). Cyber threat intelligence sharing practices in

Nigeria: A grounded theory perspective. In Adeyemi, O. et al. (Eds.), *Information and Communication Technologies in Africa* (pp. 109–125).

NITA-U. (2021). *National Cybersecurity Strategy (2021–2025)*. Kampala: National Information

Technology Authority - Uganda

Nsengiyumva, J. & Ruhangaza, A. (2022). Cyber Risk Awareness and Security Culture in

Rwanda's Public Sector. *Rwandan Journal of Information and Communications Technology*, 4(3), 77–91

Nweke, J., et al. (2021). Cyber threat intelligence sharing: Understanding user acceptance

through TAM. *Computers & Security, 104, 102466.*

Okonkwo, U. (2024). The role of cyber threat intelligence in preventing attacks in Nigeria: A

case-based assessment. *ResearchGate Working Paper*

Shikokoti, Okoth and Abungana, (2024). *Research Methods in Education.* Aura publishers. ISBN: 978-9914-37-170-3.
TCRA. (2023). *Cybersecurity and Digital Trust in Tanzania: Policy Brief on Threat Intelligence*

Coordination. Tanzania Communications Regulatory Authority

Thales Group. (2023). *Launch of a French cyber threat intelligence platform for secure*

information sharing. Thales Press Release. https://www.thalesgroup.com/en/worldwide/security/press_release/thales-and-10-partners-launch-french-cyber-threat-intelligence

Truong, T. D., et al. (2022). Enhancing cyber threat intelligence sharing with automated context

tagging and threat behavior mapping. *Journal of Cybersecurity, 8(1), tyab019.*

Tumwesigye, A., & Mbarika, V. (2019). Evaluating the Cybersecurity Resilience of Financial

Institutions in Uganda: A Threat Intelligence Perspective. *East African Journal of Information Systems*, 5(1), 12–25