Advancing Intelligence-Led Cybersecurity: An Architecture for Cyber Security Intelligence Center

Mehran Mahboubian[1], Amir Hossein Pourshams[1], Mohammad Mahdi Abdian[1]

[1]*R&D Center, Mobile Communication Company of Iran, Tehran, Iran*
{m.mahbubian,ah.pourshams,m.abdian}@mci.ir

Abstract

The swift progression of cyber threats presents significant challenges for organizations striving to safeguard their digital assets through traditional security methods alone. Research shows that relying only on security controls and incident response is insufficient. On the other hand Cyber Threat Intelligence (CTI) has become an essential component of effective cybersecurity strategies, facilitating the proactive identification and coordinated response to threats. This paper proposes a novel architecture for establishing a Cyber Security Intelligence Center (CSIC) within an organization. As the CSIC is a pure novel concept, the first version is implemented in the MCI R&D Office of Security to evaluate its effectiveness and performance. The CSIC would conduct cyber intelligence operations and intelligently integrate with existing security operations and business functions. The proposed CSIC architecture includes CTI lifecycle processes to perform its core functions. In the proposed CSIC intelligence operations would interact closely with security teams, such as those dedicated to prevention, detection and response, aiming to enhance organizational capabilities for preempting and identifying novel cyber threats. Preliminary findings demonstrate establishing a centralized intelligence operation through a CSIC may significantly improve an organization's time to predict, time to detect and time to respond to cybersecurity threats.

Keywords: *Intelligence-Led Security, Cyber Security Intelligence, Cyber Threat Intelligence, Cyber Security Intelligence Center.*

1 Introduction

The digital landscape has revolutionized business operations, opening avenues for growth and innovation. However, this transformation has also introduced new risks, notably in the form of cyber threats. Cybercriminals, nation-state actors, and other malicious entities continually devise new strategies to breach organizational defenses, compromising sensitive data and disrupting critical operations [1]. The traditional approach to cybersecurity, which focuses on deploying security controls and reacting to

incidents as they occur—known as reactive security—is no longer sufficient to address the evolving threat landscape. Organizations must follow Cyber Threat Intelligence (CTI) to adopt a proactive approach to cybersecurity, which involves identifying and responding to threats before they materialize [2].

CTI refers to the collection, processing, and analysis of information aimed at understanding a threat actor's motives, targets, and attack behaviors [3]. It empowers organizations to make informed decisions about their security by anticipating and mitigating potential threats before they can impact business operations. The aim of CTI is not merely reactive; it strives to provide a predictive capability to anticipate potential security incidents based on the tactics, techniques, and procedures of potential threat actors [4]. CTI encompasses a range of intelligence, including strategic, operational, tactical, and technical intelligence [5]:

- Strategic Intelligence: Provides a broad context regarding the cyber threats facing an organization or sector, useful for high-level policy and decision-making.
- Operational Intelligence: Offers insights into specific upcoming or ongoing attacks, suitable for informing operational decisions during incident response.
- Tactical Intelligence: Details the tactics, techniques, and procedures used by threat actors, aiding the development of defensive measures.
- Technical Intelligence: Includes technical indicators of compromise (IOCs) such as hashes, IP addresses, and URLs, which assist in identifying and mitigating attacks.

Despite the recognized importance of CTI and the availability of its essential components, many organizations struggle to establish and integrate it effectively. One of the main challenges is the lack of a comprehensive architecture for performing CTI actions. Hence, the need arises to establish a centralized system such as CSIC that can perform these capabilities. This study aims to address this gap by proposing an architecture for CSIC that can help organizations optimize their CTI capabilities and reduce cybersecurity risk. The proposed CTIC architecture, along with its interactions, will integrate various components of CTI. This includes intelligence collection, processing, analysis, and dissemination, as well as aligning with the organization's security operations and business goals.

2 Related Works

While cyber threat intelligence is crucial for private businesses, numerous academic research studies are also being conducted on this topic. Further advancements in the field made by [6] who developed an enhanced eight-step CTI model, building upon a pre-existing six-step model. This model introduced two additional stages: visualization

and analysis. A tool which applies this model is designed to collect data from various sources, create analytics to expedite threat mitigation time, and improve CTI regarding collection, filtering, sharing, visualization, and analysis. The tool utilizes multiple technologies and protocols, including MySQL, Elastic Search, Log stash, and TAXII. The researchers concluded their work could enhance CTI effectiveness and improve threat mitigation, demonstrating the tool's application using a real-world example.

Gong and Lee proposed a cyber threat intelligence framework aimed at enhancing the security of the energy cloud environment to quickly apply a security model to a large-scale energy cloud infrastructure, and a method for sharing and spreading CTI between the Advanced Metering Infrastructure (AMI) layer and the cloud layer [7]. The framework is designed to include the local AMI layer, the station layer, and the cloud layer. The authors demonstrate that it can effectively respond to cyber threats and also show that the proposed framework can effectively respond to cyber threats by achieving a 0.822 macro-F1 score and a 0.843 micro-F1 score for cyberattack detection in an environment that simulates the model of an attacker and an energy cloud environment.

The study [8] found that CTI tasks are often manual and resource-intensive but can resolved through automation. However, implementing the CTI function is more prevalent in larger organizations due to budget and resources, while smaller organizations rely more on tools. Skills for the CTI function can be learned on the job, but formal education is beneficial. The research also highlights how the CTI function is vital for proactive defense capabilities, enabling organizations to detect and prevent cyber-attacks more effectively. The CTI function provides organizations with insight into the techniques, tactics, and procedures of a threat actor, allowing them to develop proactive detection and mitigation strategies.

The authors of [9] propose that the increasing asymmetry between the cyber-offensive capabilities of attackers and the cyber-defensive capabilities of commercial organizations can addressed by integrating CTI into their defense mechanisms. CTI, which involves the acquisition, processing, analysis, and dissemination of information that identifies, tracks, and predicts cyber threats, can transform organizations' cyber-security behavior from being reactive to proactive, anticipatory, and dynamic.

The paper describes a case study of a large multinational finance corporation's journey to adopt and integrate CTI, transforming its cybersecurity practices. The process involved two phases. Phase 1 considers the adoption of CTI as an innovation within the organization's IT Operations Division. In Phase 2, this innovation translated into a novel solution known as CTI-as-a-service. This service is designed to package and integrate CTI into the broader commercial context for business users. The study illustrates the process of adopting and integrating CTI and provides practical insights into transforming cybersecurity practices.

The ECOSSIAN project [10] introduces a pan-European, three-layered approach to safeguard critical infrastructures (CIs) by detecting cyber incidents and swiftly generating warnings for potentially affected infrastructures. This ecosystem consists of three types of Security Operation Centers (SOCs): Organization SOC (O-SOC), National

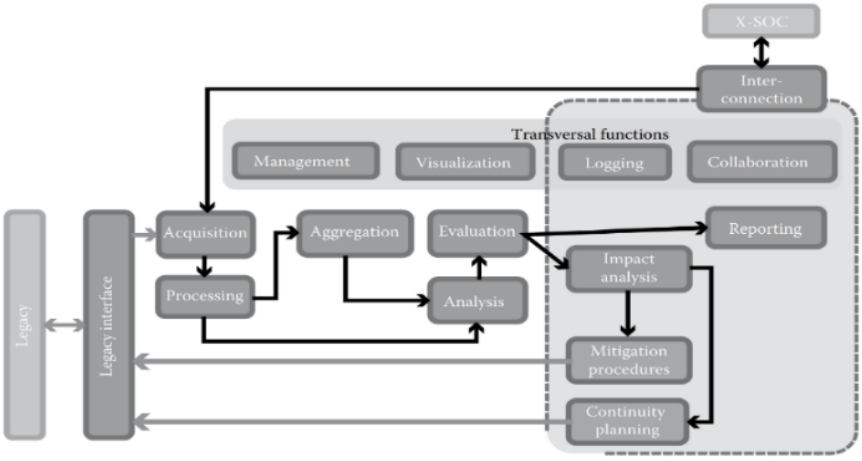

Figure 1: ECOSSIAN project architecture [11]

SOC (N-SOC), and European SOC (E-SOC).

This tri-level incident analysis network allows for flexible, scalable, and technology-independent implementations of SOCs. Functional blocks serve as modular units, facilitating detailed and context-specific functions. The functional blocks include continuity planning, visualization, interconnection, management, collaboration, reporting, impact analysis, mitigation procedure, analysis, evaluation, logging, legacy interface, processing, and aggregation.

Here we propose the CSIC comprising two main sections: the framework and architecture.

2.1 Framework

The framework of the CSIC encompasses the people, processes, and technology needed for its operation. The personnel of the CSIC include intelligence analysts, malware analysts, and forensic experts [5, 11]. The CSIC's processes follow the CTI lifecycle elements, which is necessary to perform cyber intelligence operations.

2.2 Architecture

Our proposed architecture for the CSIC incorporates various internal components and relationships with external relations to the organization's security operations and business objectives.

We classify external security operations into five classes: Asset Management, Prevention, Detection, Response and Recover [12]. These processes serve as the building components of our external stakeholders of the CSIC. The system lifecycle follows four steps: design, build, run, and defend [13]. On the other hand, the CSIC has processes of collection, processing, analysis, and dissemination that are considered to be the building

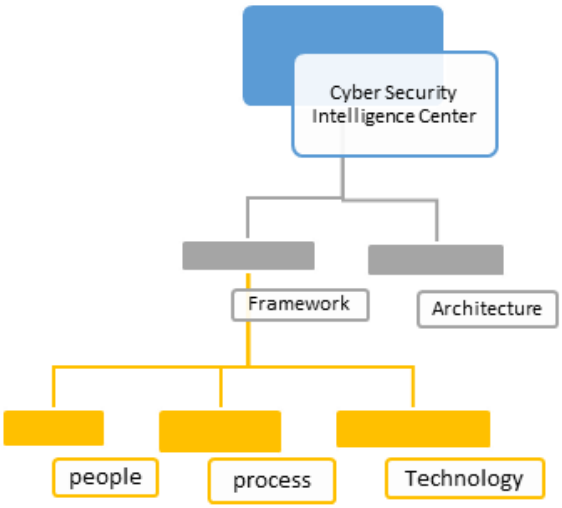

Figure 2: Proposed cyber security intelligence center frame

components of the CSIC as they execute the primary functions of a cyber intelligence operation.

2.2.1 Business and Risk components

As depicted in figure 3 the business component sets the strategic direction and overall security objectives and its interaction influences risk management and security priorities. There are five other security components in the organization:

The Risk component identifies and assesses risks to the organization. Its interaction communicates risk information to the ”Business” and “Asset Management”.

2.2.2 Design, Build, Run and DevSecOps components

DevSecOps ensures that security is considered at every stage of the software development lifecycle. It works with “Design”, “Build”, and “Run” processes.

The Design, Build, and Run components focus on developing and running secure systems and applications, considering vulnerabilities and weaknesses during the design and build phases through the DevSecOps.

2.2.3 Defend component

The Defend component is the central component of the security operations and consists of subcomponents:

- Asset Management: Identifies and inventories assets.
- Prevent: Implements preventive measures.

- Detect: Continuously monitors for threats.
- Response: Respond to detected incidents.
- Recover: Restore normal operations post-incident.

2.2.4 "Vulnerability & Weakness" component

The "Vulnerability & Weakness" component identifies vulnerabilities and weaknesses in systems. It ingests information from "DevSecOps" and "Data Processing" and outputs information into the "threat intelligence analysis" component.

2.2.5 The CSIC components

Collection. Collection within the CSIC refers to gathering information from external sources such as private/public communities, government sources, sector peers, business partners, and vendor alerts. "Collection Sources" are sources of external intelligence and threat information and serve as the input for data processing. They have subcomponents:

a. Governmental sources: Information from government agencies.

b. Sector Peers: Collaboration with other organizations in the same industry.

c. Business partners: Information from industry/business partners.

d. Vendor Alerts: Alerts from vendors about uncovered vulnerabilities and threats.

e. Threat Intelligence Services: Includes free and paid threat Intelligence.

Processing. The processing stage based on the intelligence analyst's diagnosis and intelligence requirements.

"Data Processing and Mining" normalizes, indexes, enriches, filters, and prioritizes information [14] sent from prevention and forensic and malware analysis in "defend" component because this data contains valuable information about blocked intrusion attempts and successful intrusion attempts. It has subcomponents:

a. Actors & Objectives: Understand threat actors and their goals.

b. TTPs (Tactics, Techniques, and Procedures): Identifies common tactics and techniques used by attackers.

c. Observable & Indicator: Detects specific indicators of compromise.

During the analysis phase, we consider assumptions, develop hypotheses based on them, and then evaluate these hypotheses using techniques like ACH matrix and contrarian techniques. For advanced and supplementary analysis, forensic and malware

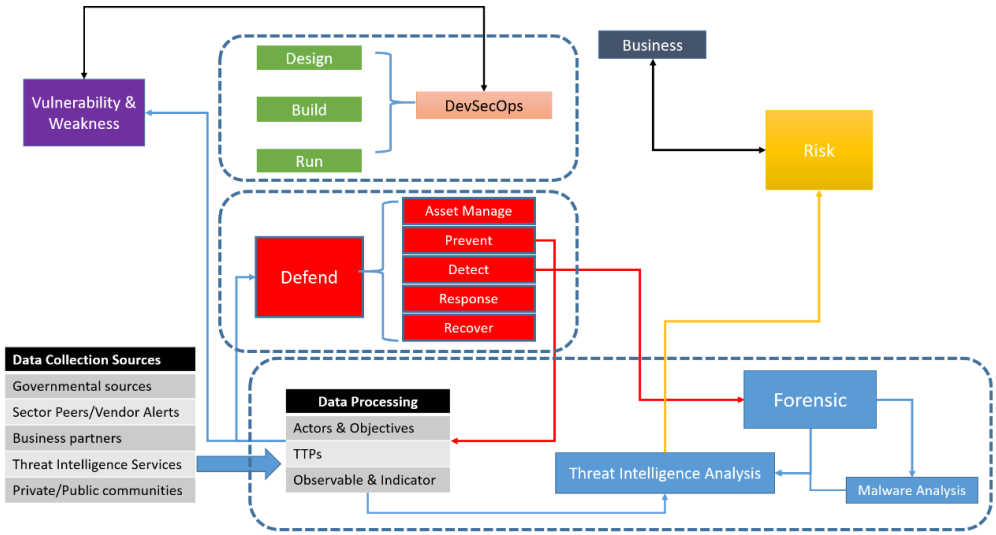

Figure 3: Proposed CSIC architecture

analysis should be done and the dissemination phase is the relations between CSIC and organization components.

The CSIC has five primary components:

Analysis. "Threat Intelligence Analysis" analyzes threat information to provide actionable insights. It ingests information from "Data Processing and Mining" and "Vulnerability & Weakness" to detect real threats and, after analysis, outputs produced intelligence about threats into the risk component.

Forensic. "Network, OS and Memory Forensic" analyzes networks, operating systems, and memory. It ingests information from monitoring and detection about detected attacks and outputs produced intelligence about technical intelligence like IoCs into the "threat intelligence analysis" component.

Malware Analysis. "Malware Analysis" analyzes malware to understand its behavior and impact. It ingests information from "Forensics" and outputs produced intelligence into "threat intelligence analysis" to help analysts know the newest malware and methods.

Relations. In CSIC there are two internal relations:

a. Continuous feedback between "Data Mining & Analytics" and "Threat Intelligence Analysis" refines detection and response strategies.

Table 1: Incident response duration reduction by MCI R&D CSIC

Case name	incident response time in MCI CERT	incident response time with MCI R&D CSIC	incident response duration reduction
RFI attack on RBT portal	two days	one day	50 %
Cerber ransomware	ten days	seven days	33%
Zeus ransomware	six days	four days	33%
Bitcoin email spam	ten days	four days	60%
WAF botnet	sixteen days	six days	62.5%
Fake spam email	three days	two days	33%
LC Trojan	thirteen days	six days	53%

b. Information from “Net-OS-Mem Forensic” and “Malware Analysis” feeds into both “Threat Intelligence Analysis” and “Defend” to improve overall security measures.

3 Results

To evaluate the effectiveness of our proposed architecture, we reassessed multiple past incidents occurred within MCI CERT in 2016. We are allowed to publish seven incidents in this paper. The summary provided in table1.

Table 1 summerizes of duration reduction in presence of MCI R&D CSIC.

The case of Cerber ransomware infection was studied in technical and tactical intelligence. This malware was first detected by virus detection engines in early March 2016, leading to immediate antivirus signature updates. However, due to the lack of a CSIC in MCI CERT and unawareness of Cerber, the malware was only recognized when it infected one of the organization’s laptops in November 2016, with no information on how to clean the malware. The containment of the infection lasted about three days, and eradication and recovery took about two days. With the minimal CSIC implemented in MCI R&D, the requirement considered monitoring security trends and malwares. In the collection phase, we identified this malware in 6-8 days. In processing phase, the indicators and signatures recognized in 1-2 days. The analysis of the malware and the TTPs lasted about 12-16 days in the analysis phase, and the report was disseminated immediately. The entire cyber intelligence operation was completed in 26 days. Thus, the detection and identification time can reduced by about nine months with updated prevention mechanisms, and the time of containment, eradication, and recovery can be reduced by about two days and one day, respectively.

In the following case, we considered operational intelligence about the Zeus Trojan, first identified in 2007. One of Zeus Trojan's variants was detected in MCI CERT in 2016. With our minimal CSIC implementation in MCI R&D, the Requirement considered monitoring security trends and malwares. In the collection phase, we identified this malware in 4-6 days. In processing phase, the indicators and signatures recognized in

1-2 days. In the analysis phase, the time of analysis of the malware and the TTPs lasted about 8-12 weeks because this malware has many variants, and the analysis was very time-consuming. (Our analysis was conducted with the help of the MITRE ATT&CK framework, introduced in 2013 and not present in 2007 at the time of the Zeus attack.) The report was disseminated immediately. The entire cyber intelligence operation was completed in three months. Thus, the detection and identification time can reduced by about two years with updated prevention mechanisms, and the time of containment, eradication, and recovery can reduced by about two days.

Now, nine years after the first case evaluated in MCI CERT, we concluded to invest in establishing CSIC. This decision resulted from the strategic intelligence we created based on our risk management and overall business strategies.

The results indicate that establishing a Cyber Threat Intelligence Center significantly enhances an organization's ability to manage cybersecurity threats more effectively. The data supports the hypothesis that a structured, intelligence-led approach to cybersecurity not only enhances threat detection and response capabilities but also builds a resilient security posture that aligns with business continuity and growth.

4 Conclusion

In this research, we proposed a novel architecture for a CSIC, a crucial and novel concept of the new cybersecurity era, detailing the sub-components necessary to develop and run the CSIC. We also demonstrated how to integrate the CSIC with other security operations within the organization and with the organization's cybersecurity requirements. After evaluating CSIC functionalities, we empirically found that establishing a centralized CSIC could significantly reduce detection and response times. The CSIC with a modular architecture demonstrates scalability, allowing for implementation within the MCI as well as across a range of other organizations, thereby enhancing its applicability and utility.

Acknowledgment We express our sincere gratitude to Mobile Communication of Iran (MCI) for their financial support of this research. Their generous funding enabled us to conduct comprehensive studies and advance our work in Cyber Security Intelligence.

References

[1] "Global Threat Report", Crowdstrike, 2023.

[2] "The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation", Juniper Research, 2022.

[3] D. E. Ozkaya, Practical Cyber Threat Intelligence, 2022.

[4] Kathryn Knerler, Ingrid Parker, Carson Zimmerman, 11 Strategies of a World-Class Cybersecurity Operations Center, The MITRE Corporation, 2022.

[5] Scott J. Roberts & Rebekah Brown, Intelligence Driven Incident Response, O'Reilly Media, Inc, 2017.

[6] Lucas José Borges Amaro , Bruce William Percilio Azevedo , Fabio Lucio Lopes de Mendonca, William Ferreira Giozza, Robson de Oliveira Albuquerque and Luis Javier García Villalba, "Methodological Framework to Collect, Process, Analyze and Visualize Cyber Threat Intelligence Data", *applied sciences,* vol. 12, no. 1205, 2022.

[7] Seonghyeon Gong, Changhoon Lee, "Cyber Threat Intelligence Framework for Incident Response in an Energy Cloud Platform", *Electronics,* 2021.

[8] Anzel Berndt, Jacques Ophoff, "Exploring the Value of a Cyber Threat Intelligence Function in an Organization", in *Information Security Education. Information Security in Action*, 2020.

[9] James Kotsias, Atif Ahmad, Rens Scheepers, "Adopting and integrating cyber-threat intelligence in a commercial organisation", *European Journal of Information Systems,* vol. 32, no. 1, pp. 35-51, 2023.

[10] Tímea Páhi, Giuseppe Settanni, "Real-World Implementation of an Information Sharing Network", in *Collaborative Cyber Threat Intelligence*, Taylor&Francis, 2018.

[11] F. Skopik, Collaborative Cyber Threat Intelligence, CRC Press, 2018.

[12] J. N. M. Dahj, Mastering Cyber Intelligence, Packt Publishing, 2022.

[13] *NIST CYBERSECURITY FRAMEWORK,* 2022.

[14] Scott C. Fitch, Michael Muckin, "Defendable Architectures", Lockheed Martin Corporation, 2019.

[15] DAVID R. MILLER, SHON HARRIS, ALLEN A. HARPER, STEPHEN VANDYKE, CHRIS BLASK, Security Information and Event Management (SIEM) Implementation, McGraw-Hill, 2011.