Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 1, pp. 65-74
DOI : 10.47974/JIOS-1852

Study of cyber threat intelligence, risk management and methods

Pardeep Singh *
Department of Computer Science & Engineering
Guru Tegh Bahadur 4th Centenary Engineering College
Rajouri Garden 110064
New Delhi
India

Mahesh Kumar †
Department of Information Technology
Bharati Vidyapeeth College of Engineering
Paschim Vihar 110063
New Delhi
India

Neetu Sharma §
Department of Computer Science and Engineering
Galgotias University
Greater Noida
Uttar Pradesh
India

* *ORCID-ID:* **0009-0000-7874-2803**
† *ORCID-ID:* **0009-0004-0560-111X**
§ *ORCID-ID:* **0000-0002-9295-6522**

* *E-mail:* **singh.pardeep@gmail.com (Corrsponding Author)**
† *E-mail:* **maheshmalkani@gmail.com**
§ *E-mail:* **neetush75@gmail.com**

© Taru Publications

Pramod Kumar [‡]
Department of Computer Science and Engineering
Ganga Institute of Technology and Management
Kablana 124104
Jhajjar
Haryana
India

Shweta [@]
Department of Computer Science and Engineering
Bhagwan Parshuram Institute of Technology
Rohini 110089
Delhi
India

Abstract

Cyberattacks by chronic threat actors circumvent network and device security to modify crucial data for companies and people. Cyber threat intelligence (CTI) enables organizations learn about cyber assaults, evidence, threat actors, as well as methodologies. Attacks are mitigated by procedures, methods, and penetration indicators.Minimizing the security gap involves something advanced than data protection in the current cyber threat context. Basic rights include secure internet material. Cyber dangers change often, so recognizing them and how to protect against them is essential. CTI's present situation and challenges are discussed here. It must be handled to maintain early warning. The article covers Cyber Threat Intelligence and associated actions.

Subject Classification: *68M25.*

Keywords: *Cyber security, Cyber threat intelligence, Threat actors, Indicators of compromise (IOC), Techniques, Tactics and procedures.*

I. Introduction

Organizations can utilize data analytics to better understand the motivations of threat actors by gathering and analyzing information on past, present and future cybersecurity risks. Information that an organization utilizes to comprehend all dangers and reduce their impact known as CyberThreat Intelligence(CTI).

[‡] *ORCID-ID:* **0009-0001-0700-4253**

[‡] *E-mail:* **pramod.gill1@gmail.com**
[@] *E-mail:* **shwetagupta@bpitindia.com**

There are mainly four important levels of Cyber Threats Intelligence namely

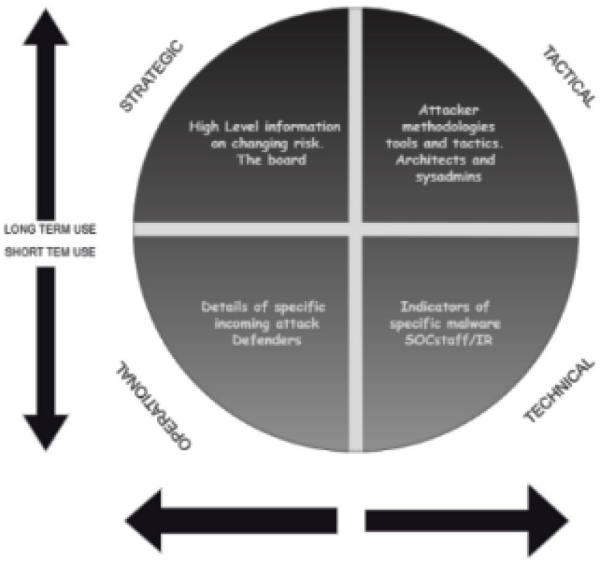


Figure 1

Levels of CTI

1. Operational Cyber Threat Intelligence
2. Tactical Cyber Threat Intelligence
3. Technical Cyber Threat Intelligence
4. Strategic Cyber Threat Intelligence

- Operational Cyber Threat Intelligence – It uses private as well as public sources like social media and dark webs for predicting the cyberattacks.
- Tactical Cyber Threat Intelligence- This type of intelligence refers to tactics, techniques and procedures (as shown in Fig.1) with indicators like URLs and IP's . In just a few hours, IOCs typically become outdated.
- Technical Cyber Threat Intelligence- It examines TTPs to assess network strengths and weaknesses against cyberattacks.

- Strategic Cyber Threat Intelligence-.Thisis employed to highlight and find the "who" alongwith "why", or the idea towards enhancing the performance of the threat actors. Usually, reports, white papers and briefings are developed by Strategic Threat Intelligence.

II. Risk management

The process of recognizing, evaluating, responding to,and putting into practice the operations that control how the organization controls the potential effects of hazards is known as Risk Management. No Cyber attack is random in nature. The dark web sells user account information and registers identical domain names for phishing attempts.

A. *Categories of Risk*

There are various categories that determines the operations caused by the different kinds of risks that affect attaining objectives at the various paradigms of the financial organizations as highlighted in Fig.2



Figure 2

Categories of Risk

- *Types of Risk*

According to [2], Fig. 2 shows inherent and residual hazards for the organization. Development strategy and company goals effect strategic

risk. [1] Financial risk originates from inflation, rate of interest, insurance, taxes, national and regional protectionist policies, and loss minimization.

B. *Process of Risk Management*

Project managers and team members at all levels evaluate and manage risk differently, yet a common risk assessment approach is needed for a full impact assessment.[3]. Since risk management is incremental, each phase must be planned as well as implemented. The steps of risk management are:

1) Risk Management Plan—The author assumes a list of probable sources, risk categories, probability and effect matrix, risk reduction as well as action strategy, intervention plan, and risk and threshold values.
2) Risk identification - A systematic methodology guarantees no severe dangers are ignored. By focusing on key phases, project risks are detected.
3) Risk analysis – Before mitigating risks, they must be identified and studied for their quantitative as well as qualitative consequences for the project. Most risk analysis principles involve frequency, extent, exposure and duration.
4) Risk management – Planned risk response, risk drivers, and risk assessors are part of risk management.
5) Risk monitoring and control-The cutting edgerisks must be identified and needs to planned. Essential hazards must be monitored and more hazards must be handled utilizing risk action plans over time. Some of the tools are licensed to safeguard sensitive data from cyber attacks, while others are open source.Echosec, Cisco umbrella, DeCYFIR, Grey Noise and other important CTI products are listed in the SANS CTI Survey 2021.

I. The XML programming language STIX (Structured Threat Information eXpression) is standardized. Threat analysts use it to examine cyberthreats and activities related to threats [8]. STIX was first got the support from the the Department of Homeland Security (DHS) office of Cybersecurity and Communication in the US. Both manually and automatically using STIX is possible [9]. An XML editor is necessary for manual use and no further tools are needed. Python API's, tools and bindings for Python are needed for

programmatic use. On Github, bindings and associated tools that assist security analysts in processing and using STIX are available as open source[4].

II. **Knowledge-assisted visual analytic system (KAVAS)-**

A form of data analysis software called Knowledge Assisted Visual Analytics System (KAVAS) uses machine learning and artificial intelligence (AI) to help analysts find patterns and insights in huge, complicated datasets.[4].

III. **Trigger Enhanced Discovery System-**

IOC's are often used as investigative proof to identify threats and attacks. Command and control server IP addresses or malicious hash values are IOC's .

Threat intelligence representation alongside transmission specifications including STIX (Structured Threat Information eXpression) (2021) along with MAEC (2021) help security agencies quickly share defense IOCs, while CAPEC and ATT&CK (2021) define attack tactics and threat ontology [5]. TriCTI has 86.99% accuracy on the supplanted dataset, outperforming other cutting-edge models.

IV. **Blockchain-based CTI preventive model for sustainable computing**

Big data management and blockchain fraud prevention are its main purposes.[6].A novel innovation for real-time applications and database transaction systems, blockchain aims to provide consumers with continual transactional transparency. This research proposes benchmarking consensus approaches in an interconnected but dispersed environment[14]. The study [15] uses blockchain technology to construct an immutable, decentralized chronicle of pharmaceutical manufacture to consumption.

V. **CTI framework for Raw Log data extraction**

The availability alongwith accuracy of Indicators of Compromise (IoC), or artifacts like IP addresses which corresponds to malicious system actions for Intrusion Detection Systems (IDS). Protection against various threats [7].

Other Alternatives for CTI

Monitoring the dark web can assist find possible risks because it is a sanctuary for cybercriminals. Threat hunting is the proactive lookout for

potential dangers. To find possible threats before they can cause any harm, threat hunters employ a range of techniques, including log analysis and network traffic analysis

III. Attacks in cybersecurity

The CTI incident response strategy expands and standardizes cyber security. A survey outlines incident response concepts and helps build and assess forms[10]. IoT secures smart machinery and residential devices. Reliable security requires efficient attack detection after heavy attacks [11]. The authors in [12] created PSO as well as Firefly algorithms to find optimal solutions for noisy non-linear and continuous mathematical systems. Each technique was tested extensively on computers. The simulation results showed that the Firefly technique beat the best solutions across every noisy non-linear and mathematical optimization function. The attack detection, prediction, and prevention methods in [13] use stored signatures, patterns, along with strongly connected behavioral profiles.. Fig.3 summarizes cyber security detection, prediction, and

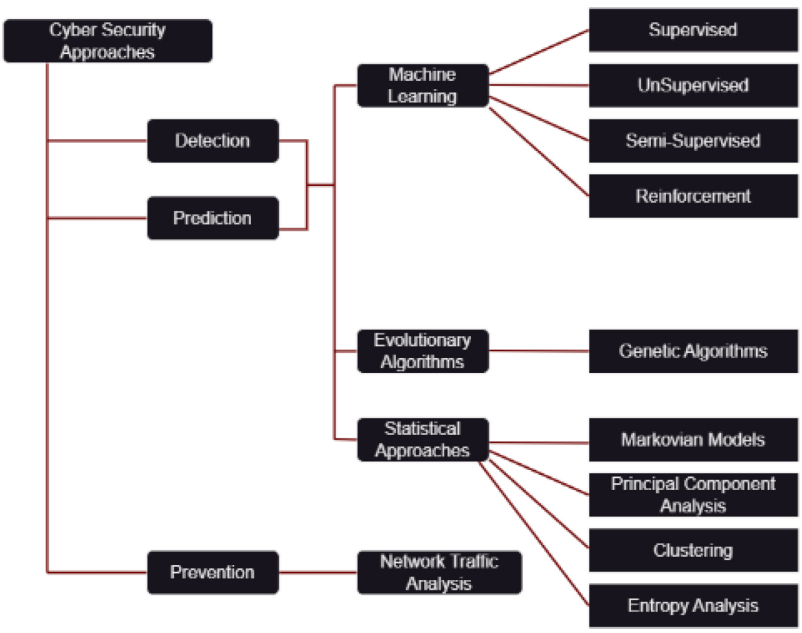


Figure 3

Summary of Cyber Security Approaches

preventive methods. Exploiting computers and IoT devices. DDoS attacks utilize a botnet of computers alongside Internet connections globally, whereas DoS attacks use one machine and one Internet connection to overwhelm an operating system with packets[16].

The three major security needs (CIA) must be considered in every security design: Confidentiality, Integrity, and Availability. The message is confidential and only the selected person may read it. Integrity guarantees information delivery without modification, while availability guarantees user access to services and data at any time[17].

IV. Conclusion

Organizations make smart decisions using Cyber Threat Intelligence. It monitors security and aids incident response to prevent zero-day attacks. Organizations must plan CTI trainings, use blockchain, cloud computing, or machine learning/deep learning to uncover unexpected dangers, and prioritize as well as mitigate cyberattacks to address future problems for comprehensive automation. Signals compromise cyberattacks. This innovative system identifies suspicious log events utilizing log data anomaly detection, enabling iterative clustering, pattern recognition, etc.

References

[1] A. M. Aljuhami and D. M. Bamasoud, "Cyber threat intelligence in risk management," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 10, p. 10 (2021). https://doi.org/10.14569/IJACSA.2021.0121018

[2] I. Croitoru, "RISK MANAGEMENT-BETWEEN NECESSITY AND OBLIGATION," Intern. Audit. Risk Manag., vol. •••, p. 14 (2019).

[3] DOVAL, E. RISK MANAGEMENT PROCESS IN PROJECTS. Review of general management, 29(2) (2019).

[4] F. Böhm, F. Menges, and G. Pernul, "Graph-based visual analytics for cyber threat intelligence," Cybersecurity (Singap.), vol. 1, no. 1, p. 16 (2018). https://doi.org/10.1186/s42400-018-0017-4.

[5] J. Liu, J. Yan, J. Jiang, Y. He, X. Wang, Z. Jiang, et al., "TriCTI: An actionable cyber threat intelligence discovery system via trigger-enhanced neural network," *Cybersecurity* (Singap.), vol. 5, no. 1, p. 8 (2022). https://doi.org/10.1186/s42400-022-00110-3

[6] J. Cha, S. K. Singh, Y. Pan, and J. H. Park, "Blockchain-based cyber threat intelligence system architecture for sustainable computing,"

Sustainability (Basel), vol. 12, no. 16, p. 6401 (2020). https://doi.org/:10.3390/su12166401

[7] M. Landauer, F. Skopik, M. Wurzenberger, W. Hotwagner, and A. Rauber, A framework for cyber threat intelligence extraction from raw log data. In 2019 IEEE International Conference on Big Data (Big Data) (pp. 3200-3209). IEEE (2019, December). https://doi.org/:10.1109/BigData47090.2019.9006328.

[8] F. K. Kaiser, U. Dardik, A. Elitzur, P. Zilberman, N. Daniel, M. Wiens, et al., "Attack hypotheses generation based on threat intelligence knowledge graph," *IEEE Trans. Depend. Secure Comput.,* vol. 20, no. 6, pp. 4793–4809 (2023). https://doi.org/10.1109/TDSC.2022.3233703.

[9] B. Nour, M. Pourzandi, and M. Debbabi, "A survey on threat hunting in enterprise networks," *IEEE Commun. Surv. Tutor.,* vol. 25, no. 4, pp. 2299–2324 (2023). https://doi.org/10.1109/COMST.2023.3299519.

[10] D. Schlette, M. Caselli, and G. Pernul, "A comparative study on cyber threat intelligence: The security incident response perspective," IEEE Commun. Surv. Tutor., vol. 23, no. 4, pp. 2525–2556 (2021). https://doi.org/10.1109/COMST.2021.3117338.

[11] H. A. Alterazi, P. R. Kshirsagar, H. Manoharan, S. Selvarajan, N. Alhebaishi, G. Srivastava, et al., "Prevention of cyber security with the internet of things using particle swarm optimization," *Sensors* (Basel), vol. 22, no. 16, p. 6117, Aug. 16 (2022). https://doi.org/10.3390/s22166117

[12] S. Agarwal, A. P. Singh, and N. Anand, Evaluation performance study of Firefly algorithm, particle swarm optimization and artificial bee colony algorithm for non-linear mathematical optimization functions. In 2013 fourth international conference on computing, communications and networking technologies (ICCCNT) (pp. 1-8). *IEEE* (2013, July). https://doi.org/:10.1109/ICCCNT.2013.6726474.

[13] A. E. Ibor, F. A. Oladeji, and O. B. Okunoye, "A survey of cyber security approaches for attack detection, prediction, and prevention," *Int. J. Security and its Applications,* vol. 12, no. 4, pp. 15-28 (2018). [Online]. Available: https://doi.org/10.14257/ijsia.2018.12.4.02.

[14] V. N. Patil and V. H. Kalmani, "Enhancing security and ensuring secure performance: A performance evaluation of consensus algorithms in a distributed healthcare blockchain system," *J. Stat. & Manag. Syst.,* vol. 26 (2023). [Online]. Available: https://doi.org/10.47974/JSMS-1079.

[15] A. S. Shete, S. Bhutada, M. B. Patil, P. H. Sen, N. Jain, and P. Khobragade, "Blockchain technology in pharmaceutical supply chain: Ensuring transparency, traceability, and security," *J. Stat. & Manag. Syst.*, vol. 27, no. 2, pp. 417-428 (2024). [Online]. Available: https://doi.org/10.47974/JSMS-1266.

[16] N. Anand and K. J. Singh, "A comprehensive study of DDoS attack on Internet of Things network," in Recent Advances in Electrical and Electronic Engineering, B. P. Swain and U. S. Dixit, Eds., Lecture Notes in Electrical Engineering, vol. 1071. Singapore: Springer, pp. 931-943 (2024). [Online]. Available: https://doi.org/10.1007/978-981-99-4713-3_56.

[17] N. Anand and K. J. Singh, "An overview on security and privacy concerns in IoT-based smart environments," in Security, Privacy and Data Analytics, U. P. Rao, M. Alazab, B. N. Gohil, and P. R. Chelliah, Eds., Lecture Notes in Electrical Engineering, vol. 1049. Singapore: Springer, pp. 395-410 (2023). [Online]. Available: https://doi.org/10.1007/978-981-99-3569-7_21.

Received August, 2024