ISSN: 2754-6705

Journal of Mathematical & Computer Applications

SCIENTIFIC Research and Community

Review Article

Open Access

Leveraging Threat Intelligence for Compliance Strategies

Haritha Madhava Reddy

USA

ABSTRACT

As cyber threats become increasingly sophisticated, organizations are compelled to adopt proactive measures to safeguard their assets and comply with regulatory requirements. Threat intelligence has emerged as a vital component in both cybersecurity and compliance strategies. As such, this paper explores the role of threat intelligence in helping organizations meet evolving regulatory standards, such as GDPR, CCPA, and the NIS2 Directive, and also outlines how it can be leveraged to improve risk assessment, incident response, and reporting. Moreover, this paper categorizes threat intelligence into four main types: strategic, operational, tactical, and technical, each serving distinct purposes from shaping long-term strategies against cyberattacks. By integrating threat intelligence into compliance frameworks, organizations can enhance their ability to proactively detect and mitigate threats, streamline regulatory reporting, and align their security efforts with business objectives.

***Corresponding author**

Haritha Madhava Reddy, USA.

Received: November 15, 2022; **Accepted:** November 20, 2022, **Published:** November 29, 2022

Keywords: Threat Intelligence, Cybersecurity, Compliance Strategies, Cyber Threats, Threat Intelligence Platforms (TIPs), Open-Source Intelligence (OSINT), Dark Web Monitoring, Machine Learning, GDPR, CCPA, NIS2 Directive, Risk Assessment, Incident Response, Reporting, Strategic Intelligence, Operational Intelligence, Tactical Intelligence, Technical Intelligence, Threat Intelligence Lifecycle

Introduction

Emerging technological innovations and globalization have increasingly reshaped industries across the globe, which also has led to an increased reliance on data and connected systems. However, as businesses continue to shift their operations online, they face an escalating number of cybersecurity threats. At the end of 2022, cybercrime damages are predicted to cost the world $8.15 trillion annually by 2022, compared to $1.16 trillion in 2019 [1]. As a result, the proliferation of these threats has compelled numerous regulatory bodies to enforce significantly more strict cybersecurity guidelines. Moreover, one of the critical components to defending against cyber threats and adhering to regulatory requirements is threat intelligence. Threat intelligence, more specifically, is the practice of collecting and analyzing information about current and potential future cyber threats to improve security posture and regulatory compliance [2]. It helps organizations move from a reactive to a proactive stance by effectively identifying potential attacks before they occur. Given the increasing complexity of cyber threats and the evolving regulatory landscape, being able to leverage threat intelligence is crucial for effective compliance strategies.

Understanding Threat Intelligence

By leveraging threat intelligence, organizations gain a clearer understanding of their adversaries, the techniques they use, and the vulnerabilities they seek to exploit. This intelligence allows businesses to make informed, strategic decisions regarding their security posture and to effectively mitigate potential attacks. The primary goal of threat intelligence is to provide actionable insights that enable organizations to anticipate and respond to cyber threats before they can cause significant damage. Threat intelligence can take many forms and can be derived from a wide range of sources, including threat feeds, incident reports, malware analysis, security blogs, and even the dark web. When properly analyzed, this information can help organizations not only react to cyberattacks but also adopt a more preventative approach [3]. Threat intelligence is typically classified into several categories, each serving distinct purposes. These include strategic intelligence, operational intelligence, tactical intelligence, and technical intelligence. By understanding these categories, organizations can effectively integrate threat intelligence into their security strategies.

Strategic Intelligence

Strategic intelligence provides high-level, long- term insights into global threat trends, geopolitical factors, and broader cybersecurity developments. It is typically aimed at senior executives, board members, and decision-makers who are responsible for shaping the organization's overall security strategy. This can also be used for understanding the variety of social, political, and cultural motives of an attacker [4]. Strategic intelligence helps organizations understand the broader context of the threats they face, which might include nation-state actors, cybercriminal organizations, or economic competitors seeking to disrupt their operations. This type of intelligence, therefore, is particularly valuable for businesses that operate in multiple regions, as it offers insights into how geopolitical changes might affect their security posture. For example, tensions between countries can lead to an increase in state- sponsored cyberattacks, targeting industries that are critical to national infrastructure, such as in areas of healthcare, finance, or energy. Strategic intelligence can moreover help executives make informed decisions about resource allocation,

investments in new security technologies, and partnerships with third-party vendors. By understanding global trends, organizations can anticipate potential threats that may not yet be directly impacting them but could pose a risk in the future. Additionally, strategic intelligence informs regulatory and compliance decisions, as organizations must adapt their strategies to meet continuously evolving legal frameworks.

Operational Intelligence

Operational intelligence is focused on specific, real-time threats that are actively targeting or could soon target an organization. Unlike strategic intelligence, which provides long-term insights, operational intelligence is immediate and actionable [5]. It is primarily used by security teams to monitor current threats, track emerging vulnerabilities, and thereafter taking appropriate action to prevent a cybersecurity attack. This type of intelligence is particularly useful in managing incident response efforts and ensuring that the organization's defenses are aligned with the latest threat vectors. As such, operational intelligence provides real-time information about malware campaigns, phishing attacks, or ransomware trends that are circulating. With this information, organizations can adjust their security protocols, update firewall rules, and monitor their networks for any signs of compromise. An example of operational intelligence would be identifying a new strain of malware that is rapidly spreading through phishing emails. Security teams can leverage operational intelligence to immediately flag and block emails containing malicious attachments or links, preventing users from interacting with the malware [6]. Additionally, operational intelligence is vital for threat hunting, where security analysts proactively search for indicators of compromise (IOCs) in their environment, reducing the window of time in which an attacker could exploit a vulnerability [7].

Tactical Intelligence

Tactical intelligence refers to the detailed understanding of the tactics, techniques, and procedures (TTPs) that threat actors use to carry out their attacks. It provides security professionals with granular, actionable data that can be applied directly to improve an organization's defenses. Tactical intelligence often includes malware signatures, known bad IP addresses, attack methods, and patterns of behavior commonly exhibited by specific threat groups [8]. Tactical intelligence is particularly important for creating defense mechanisms that can stop threats before they infiltrate the organization's network. For example, by analyzing the TTPs of a known hacker group, security teams can configure their security systems to detect and block these attack methods. For instance, if a group is known to exploit a specific vulnerability in a web application, tactical intelligence allows organizations to patch that vulnerability and implement additional monitoring to detect similar behavior in the future. This type of intelligence is critical for preventing both widespread and targeted attacks. While operational intelligence helps organizations understand the current threat landscape, tactical intelligence enables them to actively defend against specific attack methods. It is commonly shared among organizations within the same industry through information-sharing platforms, helping to improve collective security efforts.

Technical Intelligence

Technical intelligence involves highly detailed, technical data about specific indicators of compromise (IOCs), such as malware hashes, malicious IP addresses, or command and control (C2) domains used by attackers [9]. This intelligence is used primarily by security operations teams to detect and block threats at the technical level. It often includes data from past attacks and helps organizations identify suspicious activity within their networks. For example, if an organization detects an IP address that has been flagged by technical intelligence sources as being associated with malware distribution, the security team can thereafter block that IP from accessing the network. Similarly, if a new malware strain has been identified, its hash value can be added to an endpoint protection system to prevent the malware from executing on any machine within the network. Technical intelligence is therefore particularly useful for security tools that rely on automated detection and prevention, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and endpoint detection and response (EDR) platforms [10]. By feeding IOCs into these systems, organizations can detect potential attacks more efficiently and respond before significant damage occurs. Moreover, technical intelligence often serves as the foundation for threat hunting, allowing security teams to proactively search for signs of malicious activity based on known attack patterns.

The Threat Intelligence Cycle

The threat intelligence lifecycle is a structured process that ensures that the data collected is relevant, actionable, and effective. This lifecycle involves several stages, each of which is crucial to converting raw threat data into actionable insights that can be applied to protect the organization. The process begins by identifying the specific intelligence needs of the organization. This could involve focusing on specific types of threats (such as ransomware or insider threats) or targeting intelligence that helps the organization comply with regulatory requirements. The intelligence requirements should align with the organization's strategic goals and risk management framework. After defining the intelligence needs, the next step is gathering raw data from a variety of sources. These sources can include public threat feeds, information sharing platforms, dark web monitoring, proprietary threat intelligence services, and internal logs. The goal of this step is to gather as much relevant data as possible to gain a comprehensive understanding of the current and emerging threats.

Once the data is collected, it needs to be organized and filtered to remove irrelevant or duplicate information. This is an essential step in ensuring that only high-quality data is analyzed. During this stage, threat data is also categorized based on its relevance to specific security needs. In this stage, security analysts review the processed data to derive actionable insights. The analysis may involve identifying patterns in the data, correlating information from multiple sources, and assessing the potential impact of the threats on the organization. Advanced analytics tools, including machine learning models, are often employed to automate parts of this process and detect patterns that may not be immediately obvious to human analysts.

After the analysis, the resulting threat intelligence must be shared with the appropriate stakeholders within the organization. This could include the security operations center (SOC), executive leadership, or specific teams responsible for implementing defensive measures. The intelligence is typically shared through reports, dashboards, or automated alerts that help relevant teams make informed decisions. The final stage of the lifecycle is the feedback loop, where the effectiveness of the intelligence is evaluated [11]. Organizations continuously assess whether the threat intelligence is accurate, timely, and useful in preventing or mitigating attacks. This feedback helps refine the intelligence-gathering process for future iterations, ensuring that it remains aligned with the organization's evolving needs and the dynamic

threat landscape. By following the threat intelligence lifecycle, organizations can ensure that their threat intelligence efforts remain focused, efficient, and impactful. This process enables businesses to stay ahead of emerging threats, respond to ongoing attacks, and continuously improve their security posture to meet compliance and operational goals.

The Evolving Compliance Landscape

The regulatory landscape for cybersecurity has become increasingly stringent as cyberattacks grow in both frequency and sophistication. Organizations must navigate a variety of frameworks aimed at protecting personal data, securing critical infrastructure, and ensuring business continuity. Regulations like the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the NIS2 Directive, and ISO 27001:2022 set the standard for data protection and cybersecurity practices globally [12]. These regulations underscore the importance of adopting robust, proactive security measures, placing greater emphasis on threat identification and mitigation. One of the most prominent shifts in regulatory expectations is the move towards risk-based approaches [13]. Rather than relying solely on reactive security protocols, modern regulations encourage organizations to assess the risks they face from cyber threats and implement controls accordingly. For instance, GDPR mandates that organizations deploy "appropriate technical and organizational measures" to protect personal data, requiring a thorough assessment of potential risks and proactive defenses. Similarly, the NIS2 Directive calls for organizations in critical sectors such as healthcare, energy, and transportation to adopt proactive cybersecurity measures.

The increased focus on risk-based compliance emphasizes the need for threat intelligence. By leveraging real-time threat data, organizations can better understand the risks they face and align their security practices with regulatory demands. Furthermore, many regulations require organizations to demonstrate compliance through documented evidence of proactive threat mitigation efforts—an area where threat intelligence plays a vital role.

INTEGRATING THREAT INTELLIGENCE INTO COMPLIANCE STRATEGY

Threat intelligence can play a pivotal role in helping organizations meet compliance requirements by providing real-time insights into the evolving threat landscape. Modern regulations, such as GDPR and CCPA, mandate that organizations take proactive steps to protect sensitive data and ensure privacy [14]. Leveraging threat intelligence allows businesses to stay ahead of emerging threats and align their security strategies with regulatory requirements.

For example, GDPR requires organizations to implement appropriate security measures based on the risks to the data they control. Threat intelligence helps organizations assess these risks by identifying new attack vectors, vulnerabilities, and threat actors. By understanding these specific risks that are most relevant to their operations, organizations can tailor their security controls to ensure compliance with GDPR's stringent data protection mandates.

CASE STUDY: NIS2 DIRECTIVE AND THREAT INTELLIGENCE

The NIS2 Directive, introduced by the European Union, serves as an update to the original NIS Directive and focuses on enhancing the cybersecurity of critical infrastructure sectors,
including energy, health, and transport. One of the key elements of the directive is the emphasis on proactive cybersecurity risk management, with threat intelligence playing a central role in achieving compliance. This directive applies to operators of essential services and digital service providers, requiring them to manage cybersecurity risks and report significant incidents to the relevant authorities. Threat intelligence is essential in helping organizations comply with the NIS2 Directive by providing the information needed to identify, assess, and mitigate risks before they escalate into incidents that require reporting. Organizations subject to the NIS2 Directive are required to take measures to identify and mitigate risks to their essential services[15]. Threat intelligence enables these organizations to assess potential threats, such as ransomware attacks targeting critical infrastructure, and take the necessary steps to protect their systems. Furthermore, the directive mandates that organizations report incidents that could have a significant impact on the continuity of their services. Threat intelligence platforms (TIPs) provide the information necessary to identify and report such incidents accurately and promptly, ensuring compliance with the directive[16]. By incorporating threat intelligence into their compliance strategies, organizations can meet the requirements of the NIS2 Directive while improving their overall cybersecurity resilience. Threat intelligence allows them to stay informed about emerging threats, prioritize risks, and implement targeted security measures to protect their critical infrastructure.

1. Risk Management And Assessment

Risk assessment is a critical component of both compliance and cybersecurity. By understanding the risks they face, organizations can take appropriate actions to mitigate them and ensure compliance with relevant regulations. Threat intelligence plays a vital role in the risk assessment process, providing valuable insights into the threat landscape and helping organizations identify potential risks.

Threat intelligence allows organizations to conduct threat modeling and attack surface analysis. Threat modeling involves identifying potential adversaries, their motivations, and the tactics they might use to compromise an organization's systems [17]. Attack surface analysis, on the other hand, maps out all potential entry points into an organization's network, allowing security teams to identify and close vulnerabilities [18].

Aligning threat intelligence with an organization's business objectives and regulatory requirements ensures that security efforts are focused on the most critical risks. This alignment allows organizations to not only meet compliance requirements but also prioritize the protection of their most valuable assets. By integrating threat intelligence into their risk management frameworks, organizations can create a comprehensive approach to mitigating cyber risks while ensuring regulatory compliance.

Incidence Response And Reporting

Incident response is a critical aspect of cybersecurity, and threat intelligence can significantly enhance an organization's ability to detect and respond to incidents quickly. By providing real-time insights into potential threats, threat intelligence allows organizations to identify incidents earlier, reducing the time it takes to contain and remediate them.

In the context of compliance, many regulations require organizations to report certain types of incidents to regulatory authorities within specific timeframes. For example, GDPR mandates that organizations report data breaches within 72 hours of discovery [19]. Threat intelligence can help organizations meet these reporting requirements by providing the necessary information to assess the scope and impact of an incident. By

leveraging threat intelligence, organizations can ensure that they report incidents accurately and on time, avoiding potential fines or penalties for noncompliance [20].

Furthermore, modern cybersecurity platforms often integrate threat intelligence into automated incident response workflows. These workflows use threat intelligence to trigger alerts, block malicious IP addresses, isolate infected systems, and initiate other predefined actions to mitigate the impact of an attack. Automating certain aspects of incident response improves an organization's ability to respond to threats quickly and efficiently, ensuring compliance with incident reporting requirements.

Threat Intelligence Platforms And Compliance

Threat Intelligence Platforms (TIPs) are specialized tools that collect, analyze, and distribute threat intelligence across an organization. One of the core functions of TIPs is data aggregation, which involves gathering threat intelligence from a diverse range of inputs. These sources can include open-source intelligence (OSINT), such as public threat feeds, blogs, and cybersecurity research reports, as well as intelligence from security vendors, who provide premium threat feeds that contain valuable, often exclusive, information about the latest cyber threats [21]. Additionally, TIPs can collect data from dark web monitoring, were information about cybercriminal activities, such as stolen credentials or discussions about exploiting vulnerabilities, can be found.

Once this data is collected, advanced analytics tools are employed to process and analyze it. TIPs use machine learning algorithms and data correlation techniques to sift through the vast amounts of threat data, identifying patterns and trends that could indicate emerging threats or ongoing campaigns. For example, if multiple organizations report phishing attacks using a similar set of IP addresses or domains, a TIP can flag this as part of a broader, coordinated attack campaign. This capability allows organizations to move from a reactive to a proactive security stance by predicting potential attacks before they occur.

TIPs are not standalone solutions; rather, they integrate seamlessly with an organization's existing security infrastructure to enhance the overall effectiveness of its cybersecurity strategy [22]. TIPs can be integrated with tools such as firewalls, which control the flow of traffic into and out of the organization's network. By feeding the latest threat intelligence into firewalls, organizations can automatically block IP addresses or domains associated with malicious activity.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are also enhanced by TIPs [23]. These systems monitor network traffic for suspicious behavior or known attack patterns. With up-to-date threat intelligence from a TIP, these systems can identify and stop emerging threats more effectively. Additionally, Security Information and Event Management (SIEM) platforms, which collect and analyze security- related data from across an organization's IT infrastructure, can be integrated with TIPs to provide real-time insights [24]. SIEM platforms benefit from TIPs by correlating events with known threats, enabling faster detection and response to incidents.

Collaboration and information sharing are critical components of a robust threat intelligence strategy. TIPs facilitate the exchange of threat intelligence both within an organization and with external partners, such as industry peers, regulatory bodies, and information-sharing organizations like Information Sharing and Analysis Centers (ISACs) [25]. By sharing threat data, organizations can contribute to a collective defense, allowing others to benefit from the intelligence they have gathered.

For internal collaboration, TIPs enable security teams to share threat intelligence with relevant stakeholders, such as IT administrators or executive leaders. This ensures that everyone within the organization is aware of potential threats and can take appropriate action to mitigate risks. Externally, sharing threat intelligence can help organizations stay informed about broader industry trends and emerging threats, contributing to a stronger overall security posture.

Conclusion

As cyber threats continue to evolve, organizations face increasing pressure to not only defend their networks but also comply with stringent regulatory requirements designed to protect sensitive data and critical infrastructure. Threat intelligence has emerged as a critical tool in meeting these challenges, offering organizations the ability to proactively identify, assess, and mitigate risks before they escalate into significant security incidents.

The integration of threat intelligence into compliance strategies enables organizations to move beyond reactive security postures and adopt a more comprehensive approach to risk management. By leveraging the different types of threat intelligence—strategic, operational, tactical, and technical—organizations can align their security efforts with both their business objectives and the regulatory frameworks that govern their operations.

The threat intelligence lifecycle plays a key role in ensuring that the data collected is relevant and actionable. This structured process allows organizations to gather threat data from a variety of sources, process it effectively, and share it with stakeholders to make informed decisions. Threat Intelligence Platforms further streamline this process by aggregating data from open-source intelligence, security vendors, and dark web monitoring, then using advanced analytics to identify trends and patterns that indicate potential threats.

Moreover, TIPs can integrate with existing security tools, such as firewalls, IDS/IPS, and SIEM platforms, to enhance the overall security posture of an organization. They also facilitate collaboration and information sharing, both within the organization and with external partners, improving collective security and ensuring that threat intelligence is used to its fullest potential.

In conclusion, as regulatory frameworks become more complex and cyberattacks more sophisticated, organizations must leverage threat intelligence to not only protect their systems but also ensure compliance with global standards. By investing in TIPs and integrating threat intelligence into every aspect of their security strategy, organizations can better anticipate threats, streamline compliance efforts, and safeguard their business in today's ever-evolving threat landscape.

REFERENCES

1. Statista (2022) Estimated cost of cybercrime worldwide 2018-2029 (in trillion U.S. dollars) [Graph]. In Statista. Retrieved from https://www.statista.com/forecasts/1280009/cost- cybercrime-worldwide
2. Tounsi W (2019) What is cyber threat intelligence and how is it evolving? Cyber- Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT 1-49.
3. Koloveas P, Chantzios T, Alevizopoulou S, Skiadopoulos S, Tryfonopoulos C (2021) intime: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence. Electronics 10: 818.
4. Keim Y, Mohapatra A K (2022) Cyber threat intelligence framework using advanced malware forensics. International Journal of Information Technology 14: 521-530.
5. Flashpoint (2022) Three types of threat intelligence and how to use them. Flashpoint. https://flashpoint.io/blog/three-types-of-threat-intelligence/
6. Dudley T (2020) Users are an intelligence source: Are you leveraging them in your detection strategy?. Cyber Security: A Peer-Reviewed Journal 4: 40-47.
7. Lejonqvist G, Larsson O (2018) Improving the precision of an intrusion detection system using indicators of compromise:-a proof of concept.
8. Montasari R, Carroll F, Macdonald S, Jahankhani H, Hosseinian-Far A, Daneshkhah A (2021) Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence. Digital forensic investigation of internet of things (IoT) devices 47-64.
9. Borges E (2018) Technical threat intelligence: What it is and how it helps stop cyberattacks. Recorded Future. https://www.recordedfuture.com/blog/technical- threat-intelligence
10. Haakila A (2022) Implementing Security Monitoring at Small and Medium sized Businesses.
11. Recorded Future (2020) Threat intelligence lifecycle phases. Recorded Future. https://www.recordedfuture.com/blog/threat- intelligence-lifecycle-phases
12. Baik J S (2020) Data privacy against innovation or against discrimination? The case of the California Consumer Privacy Act (CCPA). Telematics and Informatics 52.
13. Hutter B M (2005) The attractions of risk-based regulation: accounting for the emergence of risk ideas in regulation (33) London: CARR.
14. Newman M, Swift M, Gladicheva V (2020) gdpr and ccpa Start to Bare Teeth as Privacy Protection Goes Global. Bus. L. Int'l 21: 267.
15. Wallis T, Johnston C, Khamis M (2021) Interorganizational cooperation in supply chain cybersecurity: a cross-industry study of the effectiveness of the UK implementation of the NIS directive. Information and Security: An International Journal 48: 36-68.
16. Wagner T D, Mahbub K, Palomar E, Abdallah A E (2019) Cyber threat intelligence sharing: Survey and research directions. Computers & Security 87: 101589.
17. Hutchins E M, Cloppert M J, Amin R M (2011) Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research 1: 80.
18. Manadhata P K, Wing J M (2010) An attack surface metric. IEEE Transactions on Software Engineering 37: 371-386.
19. Grey O R, Brown R (2020) GDPR Compliance: Incident Response and Breach Notification Challenges. In Cyber Security Practitioner's Guide 275-302.
20. White A E (2014) Threat assessment of cyber attacks on retail and financial organizations (Master's thesis, Utica College).
21. Evangelista J R G, Sassi R J, Romero M, Napolitano D (2021) Systematic literature review to investigate the application of open source intelligence (osint) with artificial intelligence. Journal of Applied Security Research 16: 345- 369.
22. Cybersecurity and Infrastructure Security Agency. (n.d.). Securing network infrastructure devices. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/news/securing- network-infrastructure-devices
23. Ashoor A S, Gore S (2011) Difference between intrusion detection system (IDS) and intrusion prevention system (IPS). In Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India 4: 497-501.
24. Rassam M A, Maarof M, Zainal A (2017) Big Data Analytics Adoption for Cybersecurity: A Review of Current Solutions, Requirements, Challenges and Trends. Journal of Information Assurance & Security 12.
25. Gordon L A, Loeb M P, Lucyshyn W (2003) Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy 22: 461-485.