LTIMindtree

Enhance **Operational Efficiency** with **Cyber Threat Intelligence**

Index

With ever-increasing reliance on IT systems, and convergence of IT-OT, enterprises are witnessing an exponential surge in cybersecurity threats. Malware, data breach attacks, phishing exploits, ransomware, crypto-jacking, and many other threats are on an upward spiral in sheer volume and level of sophistication.

The best-of-breed firewalls, intrusion prevention and detection systems, anti-malware, and other high-end security systems, are not able to provide sufficient coverage to enterprises from these threat vectors with a traditional approach. The reason can be attributed primarily to two factors which are:

- **The sheer volume**
- **Discrete nature of security threats which can overwhelm security teams**

To cope up with these challenges, enterprises need to re-align their cyber-security strategy. Embedding pre-emptive protection mechanisms in their security systems can provide real-time intelligence and enable multi-layered protection against known and unknown threat vectors. This can be achieved by leveraging **Threat Intelligence** feeds, along with human analysis backed by thorough research.

What is Threat Intelligence?

Threat Intelligence can be described as evidence-based knowledge, including context, mechanisms, indicators, impact, and actionable insights about an existing or emerging threat to the enterprise assets. It can be leveraged by the security teams to decide the next course of action. Threat intelligence solutions gather raw data about emerging or existing threat actors from a number of sources including open, dark web, and technical sources — to form the most robust picture possible. The data is then analyzed and filtered to produce threat intelligence feeds and management reports that contain information which can be used by automated security control solutions.

Threat feeds can be straightforward, such as a malicious domain name, or complex, such as an in-depth profile of a known threat actor. However, threat intelligence has a maturity curve represented by the three levels listed below:

Tactical intelligence | **Operational intelligence** | **Strategic intelligence**

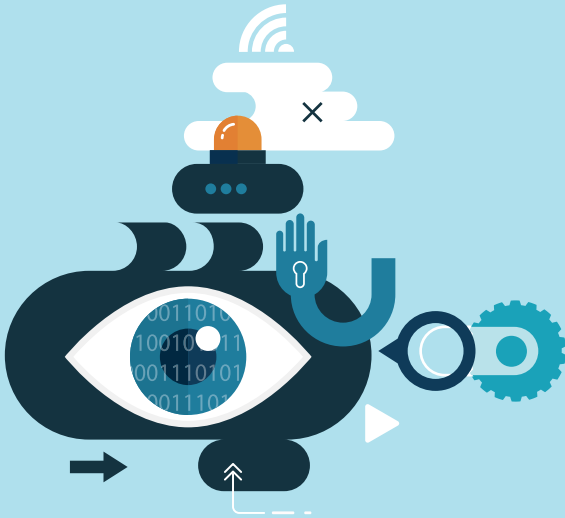
With each level, the context and analysis of threat intelligence becomes deeper and more sophisticated with different set of audiences, and the changes in cost of feeds.

Why Threat Intelligence

Security leaders often find it difficult to articulate the adverse impact of threats and justify cost-benefit analysis for deploying effective countermeasures to the executive board. Threat intelligence provides powerful ammunition and helps in contextualizing the impact of threat vector or potential vulnerability. This is done by providing visibility about organizations of the same size in other industries or trends and intelligence from the dark web indicating that the enterprise is likely to be targeted. Threat intelligence also helps security leaders to make informed decision and prioritize the vulnerabilities and weaknesses in their existing network which the threat actors are most likely to target. Additionally, it insights to the Security team on the **tactics, techniques, and procedures (TTPs)** threat actors can use.

Visibility & Control

Enterprises find it extremely difficult to identify leading indicators of risk because adversaries, including their capabilities, motives, and actions are unknown. Security leaders have neither visibility nor direct control over threats to their organization and can at-best be cognizant of them and be prepared. Threat intelligence solutions enable security leaders with a real-time pivot of the latest threats, trends, and events, which helps them respond to a threat or communicate the potential impact of a new threat type to business leaders and board members in a timely and coherent manner.



Addressing Security Skills Gap

Security Operations Centre (SOC) teams need to deal with huge volumes of alerts generated by the networks 24*7. Triaging these alerts is a time-consuming process, and many alerts can slip through the crack in this process. Manual intervention leads to "alert fatigue" amongst analysts, which impacts on the quality of delivery.

Threat intelligence automates some of the most labour-intensive tasks, rapidly collecting data and correlating context from multiple intelligence sources, prioritizing risks, and reducing unnecessary alerts. Powerful threat intelligence helps security professional to quickly "upskill" their expertise and experience.

Defining the Goal

This is the first stage in the threat intelligence life cycle because it sets the roadmap for the entire operation. In this stage, the team will agree on the goals and objective, and define the methodology of the intelligence program based on the stakeholder requirement. Some of the critical attributes for evaluation are:

- Identify potential attackers are and their motivations
- Have an idea on the attack surface
- What specific line of defence and strategy can be adopted to deflect future attack

Feedback

The final stage of the threat intelligence lifecycle involves getting feedback on the provided report to determine whether adjustments need to be made for future threat intelligence operations. Stakeholders may have changes to their priorities, the cadence at which they wish to receive intelligence reports, or how data should be disseminated or presented.

Dissemination

The dissemination phase requires the threat intelligence team to translate their analysis into a digestible format and present the results to the stakeholders. How the analysis is presented depends on the audience. In most cases the recommendations should be presented concisely, without confusing technical jargon, either in a one-page report or a short slide deck.

Analysis

Once the dataset has been processed, the team must then conduct a thorough analysis to find answers to the questions posed in the requirements phase. During the analysis phase, the team also works to decipher the dataset into action items and valuable recommendations for the stakeholders.

Information Accumulation

Once the requirements are defined, the team then sets out to collect the raw data required to satisfy those objectives. Depending on the goals, the team will usually seek out traffic logs, publicly available data sources, relevant forums, social media, and industry or subject matter experts.

Processing

After the raw data has been collected, it is processed into a format suitable for analysis. Most of the time, this entails organizing data points into spreadsheets, decrypting files, translating information from foreign sources, and evaluating the data for relevance and reliability.

The threat Intelligence Value Proposition

Organizations are increasingly recognizing the value of threat intelligence, with more than 70 percent planning to increase threat intelligence spending in upcoming quarters. However, most organizations are focusing only on the basic use cases, such as integrating threat data feeds with existing network, IPS, firewalls, and SIEMs — without taking full advantage of the insights that intelligence can offer. Organizations, in order to reap the complete benefit from Threat Intelligence solutions, should leverage the expertise of the Service Integrators, consultants who have built core expertise in this space. When implemented well, threat intelligence can help to achieve the following objectives:

Operational efficiency

- Keeps organization updated with contextualized information including methods, vulnerabilities, targets and bad actors; 86% reduction in unplanned downtime due to security events.
- Reduces "Alert Fatigue" in SOC team with by filtering information, events and curtailing redundant process; 34% reduction in time spend on regular reporting, 63% faster resolution of security threats.

Risk containment

- Empowers cyber security stakeholders by revealing adversarial motives and their tactics, techniques, and procedures (TTPs); 22% more threats identified before actual impact.
- Helps security professionals better understand the threat actor's decision-making process; helps to achieve 10x faster identification of threats.

Top-line indicators

- Enables business stakeholders, such as executive boards, CISOs, CIOs and CTOs to invest wisely, mitigate risk, become more efficient and make faster decisions.
- Efficiency of sec-ops team increases by 32%; more the 250% ROI in three years.

Conclusion

OAs demand for cyber threat intelligence tools is on all-time high with the growing number of threats, security marketplace is swamped with threat intelligence providers. However, organizations must be meticulous about choosing the right-fit solution catering to their specific needs. For threat intelligence to work well, organization must embrace a philosophy to be embed on cyberthreat intelligence into the DNA. Threat intelligence solution, if leveraged deftly can act as the first line of defense against potential cyber-attacks. It provides insights that can be consumed by analysts and integrated with security systems to proactively reduce security risks, increase efficiency and reduce cost of security operations.

About the Author

Rohit Vyas | Senior Specialist, Cyber Security, **LTIMindtree**

Rohit Vyas is a Senior Cyber Security Specialist with diverse experience in Network Security, Threat Intelligence, and Consulting. He has worked extensively in Cyber Security Solution Design and Implementation for global clients across various domains, including banking and Insurance, Retail, Telecom, Govt. Sector and Healthcare. At LTIMindtree, Rohit Vyas is responsible for identifying customers' technical and business requirements to design Cyber Security solutions as per industry standards and assist team in implementation in accordance with standards.