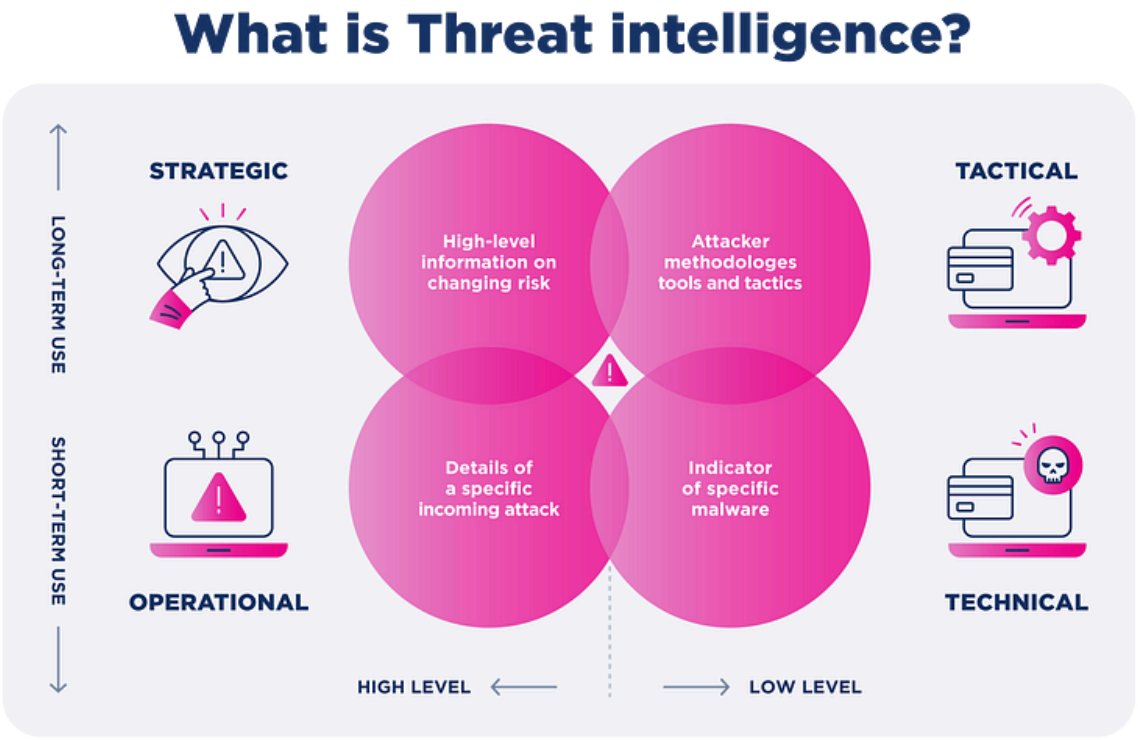
Introduction to Cyber Threat Intelligence (CTI)



What is Cyber Threat Intelligence? Cyber Threat Intelligence (CTI) involves the systematic collection, analysis, and interpretation of data on potential cyber threats. It focuses on understanding the motivations, tactics, and methods of cybercriminals, enabling organizations to proactively defend against potential cyber attacks.

Why Cyber Threat Intelligence Matters

- **Proactive Defense**: Allows organizations to anticipate and mitigate cyber threats before they can cause harm.
- **Risk Management**: Helps to prioritize and address security risks based on intelligence-driven insights.
- **Identification of Threats**: Supports early detection of potential threats, especially emerging ones.
- **Brand Protection**: Safeguards reputation by preventing or limiting the damage of cyber incidents.

Objectives of Cyber Threat Intelligence

- **Proactive Threat Identification**: CTI aims to detect potential threats before they escalate, using data from a variety of sources, including the dark web.
- **Improving Incident Response**: CTI enhances the speed and accuracy of incident response by providing detailed intelligence on threat actors, including their tactics, techniques, and procedures (TTPs).
- **Supporting Strategic Decision-Making**: CTI aligns cybersecurity strategies with broader business objectives by offering valuable insights.
- **Threat Actor Profiling**: A critical CTI objective, profiling enables organizations to understand threat actors' motivations, capabilities, and preferred methods.
- **Reducing the Attack Surface**: By identifying and mitigating vulnerabilities early, CTI minimizes potential entry points for attackers.
- **Promoting Cooperation and Information Sharing**: Collaboration is essential in CTI to strengthen defenses through shared knowledge and collective intelligence.

Types of Cyber Threat Intelligence

- **Strategic Intelligence**: Offers a high-level overview of threats affecting specific geographical areas or industries. It also assesses how threats may evolve over time.
- **Tactical Intelligence**: Focuses on specific attack types, including the TTPs used by threat actors, as well as recommended defensive steps.
- **Operational Intelligence**: Provides day-to-day threat intelligence bulletins, including Indicators of Compromise (IOCs) and Indicators of Attack (IOAs), to inform security teams of ongoing threats.
- **Technical Intelligence**: Involves the analysis of newly discovered malware and vulnerabilities, providing detailed technical insights for mitigating these threats.

Requirements for a CTI Analyst

- **Strong Analytical Skills**: To accurately interpret complex data and identify patterns.
- **Technical Expertise**: Knowledge of network security, malware analysis, and cyber attack methodologies.
- **Awareness of Threat Environment and TTPs**: Familiarity with the specific techniques used by various threat actors.
- **Communication Skills**: The ability to translate complex findings into actionable recommendations for different stakeholders.
- **Critical Thinking and Problem-Solving**: Essential for anticipating and mitigating advanced threats.
- **Knowledge of Intelligence Frameworks and Tools**: Familiarity with frameworks like the MITRE ATT&CK and tools like SIEMs.
- **Continuous Learning and Adaptability**: Given the ever-evolving threat landscape, staying current on threats and technologies is crucial.
- **Understanding Legal and Ethical Considerations**: CTI professionals must respect legal constraints and ethical guidelines in intelligence gathering.

The CTI Lifecycle

1. **Direction**: Begins by defining goals, objectives, and scope. It's essential to plan the collection phase based on specific intelligence requirements.
2. **Collection**: Involves gathering relevant information from multiple sources.
3. **Processing**: Transforms collected information into usable data by filtering out irrelevant data.
4. **Analysis**: Human-led analysis that delves into data details to provide actionable insights.
5. **Dissemination**: Distributes advisory reports and threat intelligence to relevant stakeholders.
6. **Feedback**: The final phase focuses on gathering feedback on the report's timeliness, relevance, and actionability to continuously improve CTI processes.


1. Direction
2. Collection
3. Processing
4. Analysis
5. Dissemination
6. Feedback
Cyber Threat Intelligence Lifecycle