iGUIDE

ISMS

Information Security Threat Intelligence

iNFOSECBASE

Contents

A Guide to Information Security Threat Intelligence

Introduction

Threat intelligence is a critical component of an organisation's cybersecurity strategy. It involves collecting, analysing and applying information about potential or actual threats to information security. Effective threat intelligence allows organisations to proactively defend against cyber threats, understand their adversaries and strengthen security controls.

This guide will introduce the key concepts, types, benefits and processes associated with information security threat intelligence.

What is Threat Intelligence?

Threat intelligence (TI) is actionable knowledge about existing or emerging threats that enables informed decision-making in response to those threats. It focuses on identifying threat actors, their methods and potential vulnerabilities they may exploit. It is derived from data collection, analysis and dissemination from multiple sources such as open-source intelligence (OSINT), proprietary threat data and industry reports.

Threat intelligence provides insights into:

- Tactics, Techniques and Procedures (TTPs) of attackers
- Indicators of Compromise (IoCs)
- Attack vectors and methods used by cybercriminals
- Emerging threats and vulnerabilities

The Importance of Threat Intelligence

Threat intelligence helps organisations by:

- **Identifying and Preventing Threats**: enables early detection of potential attacks and proactive defence.
- **Enhancing Decision-Making**: provides the necessary context for cybersecurity decisions, such as patching vulnerabilities, investing in tools or adjusting security policies.
- **Reducing Incident Response Time**: with threat intelligence, security teams can detect, respond and mitigate threats faster and more efficiently.
- **Improving Security Posture**: it provides a detailed understanding of the threat landscape, allowing organisations to improve their overall security measures.
- **Supporting Compliance**: many security standards, such as ISO 27001 and NIST, recommend or require organisations to implement threat intelligence programs.

Types of Threat Intelligence

Threat intelligence can be categorised into strategic, tactical, operational and technical levels, each serving a different function:

Strategic Threat Intelligence:

- **Focus**: provides a high-level overview of the threat landscape.
- **Audience**: senior management, board members and decision-makers.
- **Purpose**: helps align security strategies with broader organisational goals.
- **Examples**: industry reports, government advisories and geopolitical analysis affecting cybersecurity.

Tactical Threat Intelligence:

- **Focus**: details the tactics, techniques and procedures (TTPs) of attackers.
- **Audience**: security teams, SOC analysts and IT administrators.
- **Purpose**: helps improve defences by understanding how attackers operate.
- **Examples**: malware analysis, phishing techniques, attack vectors.

Operational Threat Intelligence:

- **Focus**: offers insights into specific, imminent threats to the organisation.
- **Audience**: incident responders and security operations teams.
- **Purpose**: provides actionable intelligence on ongoing or planned attacks.
- **Examples**: information about active campaigns targeting the organisation, threat actor profiles or attack methods.

Technical Threat Intelligence:

- **Focus**: deals with specific technical details such as Indicators of Compromise (IoCs).
- **Audience**: network defenders, threat hunters and IT security personnel.
- **Purpose**: allows security teams to identify and block malicious activity.
- **Examples**: IP addresses, file hashes, URLs, domains, malware signatures.

Sources of Threat Intelligence

There are numerous sources from which organisations can gather threat intelligence:

Internal Sources:

- Logs from firewalls, intrusion detection systems (IDS) and endpoint protection systems
- Incident response reports and forensic investigations
- Vulnerability assessment reports

External Sources:

- **Open-source Intelligence (OSINT)**: publicly available data, such as blogs, news articles or security forums.
- **Commercial Threat Feeds**: paid subscriptions to curated threat intelligence from vendors like FireEye, Recorded Future or CrowdStrike.
- **Government and Industry Sources**: CERTs (Computer Emergency Response Teams), government advisories (e.g. CISA, NCSC) and industry bodies (e.g. ISACs).

- **Dark Web Monitoring**: gathering intelligence from underground forums or dark web marketplaces where attackers exchange tools, services and data.

Threat Intelligence Lifecycle

Threat intelligence follows a structured process known as the intelligence lifecycle. This cycle ensures that the gathered intelligence is relevant, timely and actionable.

Direction:

- Define the objectives and scope of the threat intelligence program.
- Identify the key questions and focus areas (e.g. specific threat actors, attack types or vulnerabilities).

Collection:

- Gather raw data from internal and external sources such as logs, threat feeds, social media or threat-sharing communities.
- Use automated tools, sensors or manual collection methods to capture relevant threat data.

Processing:

- Clean and filter raw data to remove irrelevant information.
- Normalise data to ensure consistency (e.g. standardising IP addresses or domain formats).

Analysis:

- Analyse processed data to identify patterns, trends and potential threats.
- Correlate data from multiple sources to assess the significance and relevance of threats.
- Use tools like threat hunting platforms or machine learning algorithms to detect potential risks.

Dissemination:

- Share the actionable intelligence with relevant stakeholders (e.g. security teams, executives or external partners).
- Tailor the format and level of detail depending on the audience (e.g. technical details for SOC teams, executive summaries for management).

Feedback:

- Collect feedback on the usefulness of the intelligence provided.
- Adjust future intelligence activities based on the feedback and new emerging threats.

Applying Threat Intelligence

Threat intelligence can be applied in various areas of an organisation's security framework:

Proactive Defence:

- Use threat intelligence to predict and prevent attacks by identifying emerging threats before they impact the organisation.

- Update firewall rules, IDS signatures and endpoint protection systems based on new threat indicators.

Incident Response:

- Threat intelligence enables faster detection of attacks and more effective response by providing context on the nature of the attack.
- During an incident, it helps identify threat actor TTPs, enabling quicker containment and eradication.

Vulnerability Management:

- Prioritise patching efforts by identifying the most critical vulnerabilities based on threat intelligence.
- Focus on vulnerabilities that are actively exploited in the wild.

Security Awareness Training:

- Incorporate insights from phishing campaigns or social engineering techniques into security awareness programs.
- Educate employees on the latest tactics used by attackers.

Third-Party Risk Management:

- Assess the security posture of vendors and partners by monitoring threat intelligence for third-party-related breaches or vulnerabilities.

Challenges in Implementing Threat Intelligence

- **Data Overload**: many organisations struggle to process the vast amount of threat data they receive from multiple sources.
- **Relevance and Timeliness**: threat intelligence must be timely and relevant to the organisation's specific risk environment. Irrelevant intelligence can lead to wasted resources.
- **Integration with Security Tools**: ensuring that threat intelligence integrates with existing security tools (SIEM, IDS, EDR) can be challenging but is necessary for automation and actionable response.
- **Skills and Expertise**: threat intelligence analysis requires skilled professionals who can interpret data and apply it effectively. Organisations may need to invest in training or hire specialised talent.

Summary

Threat intelligence is an essential part of modern cybersecurity, providing organisations with the ability to understand, anticipate and defend against the evolving threat landscape. By gathering and analysing threat data from multiple sources, organisations can improve their security posture, respond more effectively to incidents and mitigate risks proactively.

Building an effective threat intelligence program requires a structured approach, the right tools and skilled analysts who can translate intelligence into actionable defence strategies. By incorporating threat intelligence into daily security operations, organisations can stay one step ahead of cyber threats.