WHAT IS THREAT INTELLIGENCE (TI)?

Actionable information that empowers organizations to predict and prevent/mitigate cyberthreats and attacks

Terminology

(APT) Advanced Persistent Threat
(CTI) Cyberthreat intelligence
(MRTI) Machine Readable Threat Intelligence
(CISO) Chief Information Security Officer
(CIRT) Computer Incident Response Team
(CERT) Computer Emergency Response Team
(TIP) Threat Intelligence Platform
(CND) Computer Network Defense
(MF) Management Framework
(DNS) Domain Name System
(DoS) Denial of Service
(DDoS) Distributed Denial of Service
(XSS) Cross Site Scripting
(RAT) Remote Access Trojan
(ICS) Industrial Control System
(IoC) Indicators of Compromise
(IPS) Intrusion Prevention System
(IDS) Intrusion Detection System
(UTM) Unified Threat Management
(VPN) Virtual Private Network
(SIEM) Security Information and Event Management System

Terminology

TI in numbers:

US$6 trillion
estimated US$6 trillion annual cyber losses by 2021

US$12.9 billion
estimated size of the TI market by 2023

18.42%
forecast annual growth of the TI market to 2025

US$5.2 trillion
total value at risk from cybercrime over next 5 years

85%
Ponemon survey respondents rating TI highly important to security operations

79%
Ponemon survey North American respondents implementing TI

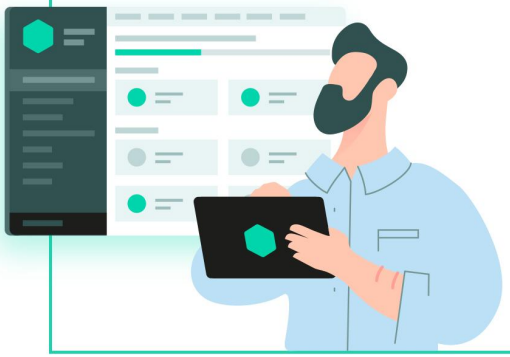
Who consumes "actionable" TI

Strategic - Senior executives, board level and CISOs

Tactical – CISOs, security decision makers, security personnel, system architects

Technical/Operational – Security operations centre (SOC) teams, vulnerability management teams, malware researchers and analysts

Consumers



INDICATORS OF COMPROMISE (IoCs)

WARNING SIGNALS OF CYBERSECURITY INCIDENTS

1. Unexplained account behavior, unusual network activity
2. Unknown new files, suspicious configuration or registry changes
3. Malicious domains, URLs, IP addresses
4. File hashes, enterprise vulnerabilities

IoC

kaspersky BRING ON THE FUTURE

Types of Threat Intelligence

Strategic - Clarify cyberthreat risk for organization decision-makers, enabling them to prioritize security investments correctly to safeguard the strategic goals of the organization

Tactical - Specific reports on types of threats/attacks, likely attackers, exploits leveraged, vulnerabilities targeted, detection avoidance strategies

Technical/Operational – Detailed insights into threat indicators including IP addresses, domains and hashes enabling effective detection of threats and showing what organizations need to focus on when responding to incidents

Benefits of Threat Intelligence (TI)

TI IMPROVES:

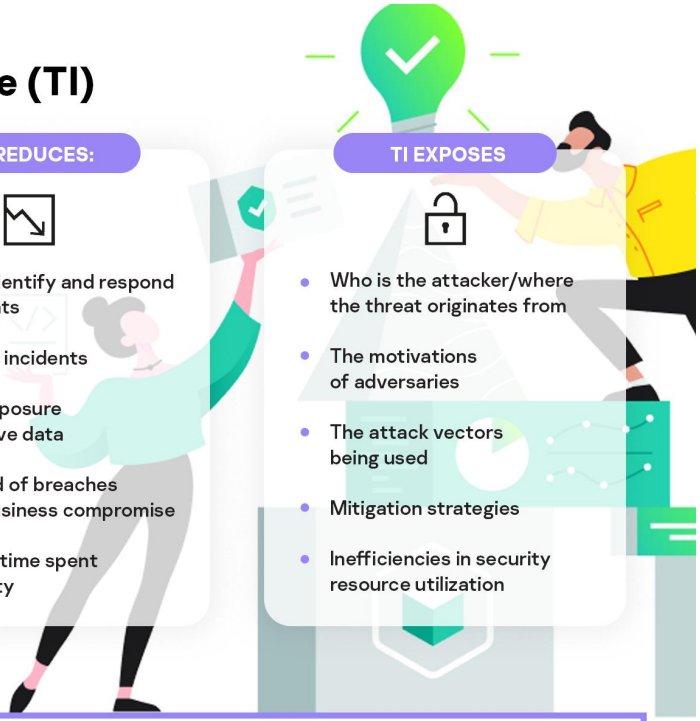
- Risk analysis
- Detection of unknown threats
- Detection accuracy with fewer false positives
- Visibility into threats and attack methodologies
- Security prioritization and resource utilization

TI REDUCES:

- Time to identify and respond to incidents
- Impact of incidents
- Risk of exposure of sensitive data
- Likelihood of breaches and/or business compromise
- Cost and time spent on security

TI EXPOSES

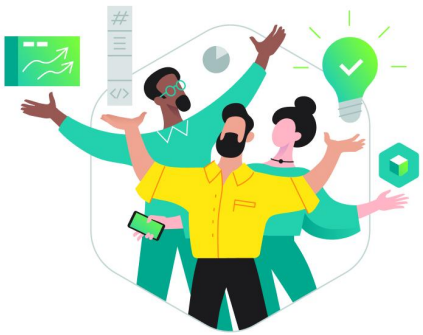
- Who is the attacker/where the threat originates from
- The motivations of adversaries
- The attack vectors being used
- Mitigation strategies
- Inefficiencies in security resource utilization



Stages of Threat Intelligence

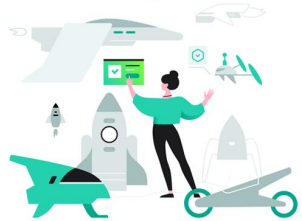
1. Define and prioritize Threat Intelligence goals → **2. Collect raw data to meet Threat Intelligence goals** → **3. Structure and analysing data** → **4. Integrate and act on analysed conclusions**

- Vision and expected results
- Quantifiable measures
- How to transform results into action



- Internal sources – SIEM including DNS, event and firewall logs, security incident response reports
- Open external sources – internet, social media, shared intelligence feeds
- Proprietary external sources - access to the dark web, criminal forums, geographical, multilingual, business and technical sector specializations
- External source collection techniques - anonymous proxies, Crawlers (programs scanning web servers), Honeypots (to lure attackers and record activities), Internet Relay Chat (IRC) protocol, spam traps, Botnet Monitoring services (24/7/365 monitoring of botnets, their targets and activities) etc.

- Automated filter eliminates false positives and redundant information
- Sorting metadata - time, source, geolocation, category etc. to calculate 'score' – what is the likelihood of the threat/attack
- Classifying data for human analysis beyond machine learning capabilities



- Actionable intelligence sources that seamlessly integrate with organization's existing security
- Prioritizing relevant data for specific security requirements to accelerate decision-making
- Timely insights into emerging threats indicating how to prioritize alerts, maximize resources and defend against attacks