MANDIANT

EBOOK

THE VALUE OF CONTEXT

How cyber threat intelligence can help you disrupt adversaries

Combating The Unknowns

Security leaders are fighting an asymmetric battle. Fast moving adversaries (known unknowns) use seemingly limitless resources to launch increasingly sophisticated attacks. To level the playing field, security leaders must continually assess every aspect of their security program to maximize the effectiveness of people, processes and technologies. This in turn helps ensure that every critical component is optimized to combat stealthy attackers.

Cyber threat intelligence (CTI) is an essential capability in an organization's security program. Used properly, CTI can enable better-informed security and business decisions, and ultimately allow organizations to take decisive action to protect their users, data and reputation against adversaries. Unfortunately, threat intelligence is a broad term used inconsistently through the cyber security community. Simplification and misuse of various threat intelligence options can make it more expensive or provide a false sense of security for cyber security leaders.

Teams need to be able to distinguish between the threat feeds, which are exhaustive lists showing indicators of compromise (IOCs), and the comprehensive CTI derived from actors, discovered and tracked in the wild.

The Threat Actor Knowledgebase

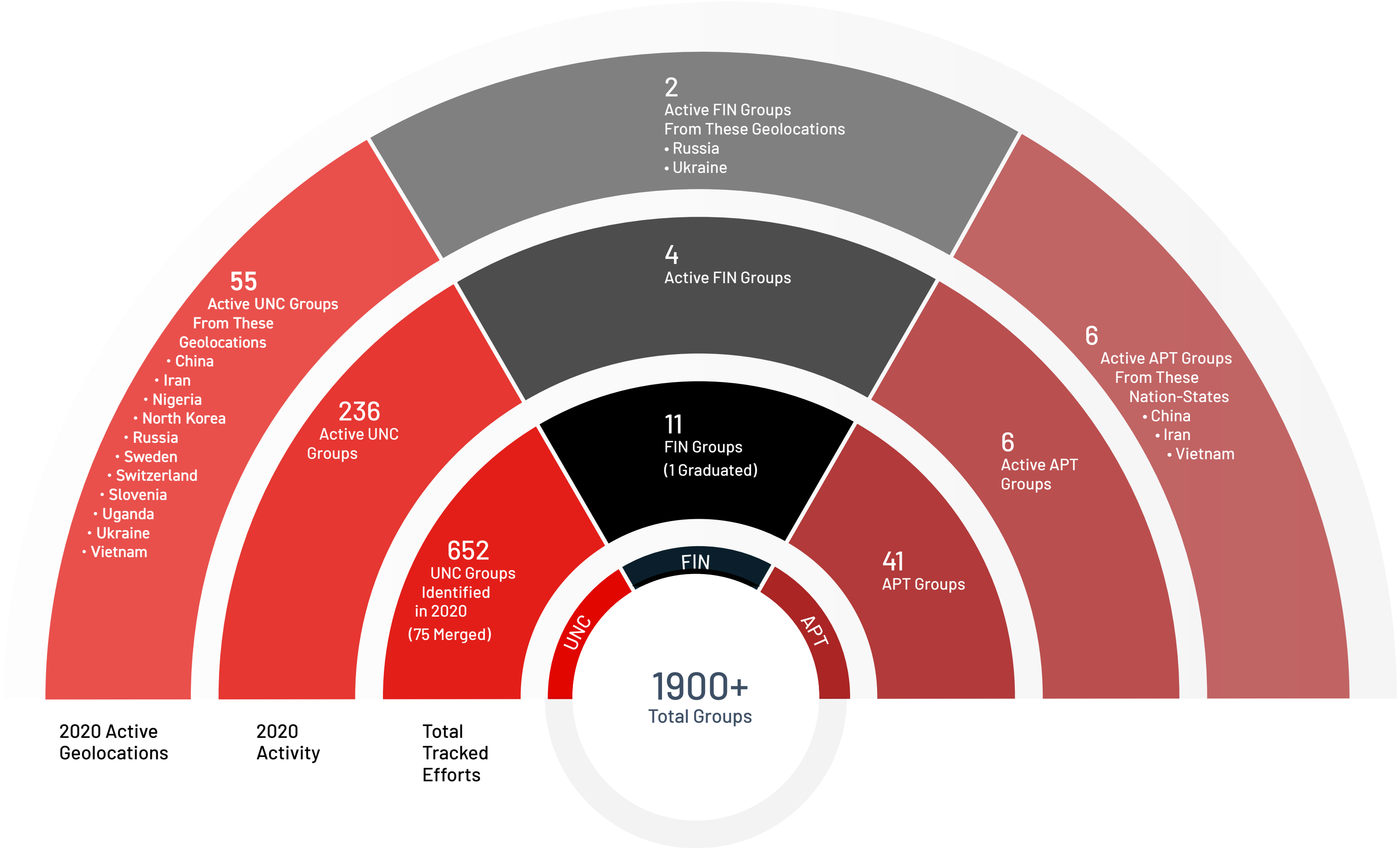
Unlike threat feeds that only reference potential security risks, comprehensive CTI is a constantly expanding and refined threat actor knowledgebase that supports a broad spectrum of investigations while maintaining fidelity within that dataset.

Threat expertise is at the core of this indispensable dataset. Refined threat knowledge makes it possible to transform this data into reliable results that security teams can put into action so that your organization can make informed decisions, ultimately solidifying your organization's security posture.

Organizations invested in a robust CTI program will quickly experience its value with to-the-minute data and around-the-clock support from a provider that can equip security teams with critical insights.

Putting the Value of Data in Context

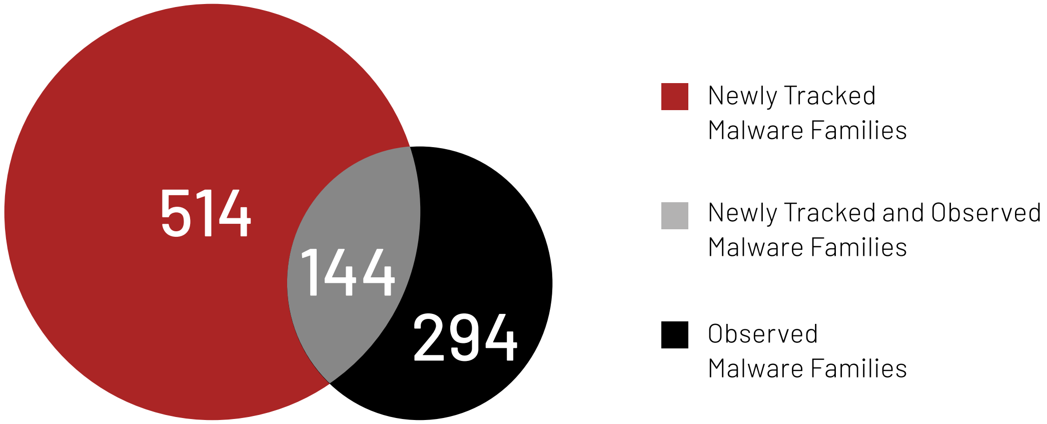
CTI is more than crunching numbers and getting data dumps. The true value of CTI data can be expressed in the context of its evolution from the wild—the known unknowns — to the refined knowledgebase that enables organizations to make informed business and security decisions.



How Mandiant Categorizes Attack Groups

Nearly 50% of observed malware families were newly tracked.

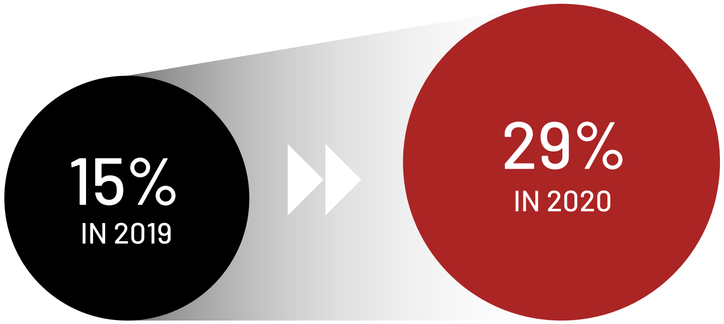
Over 500 malware families were newly tracked in 2020, and Mandiant observed 144 of them during their investigations. Adversaries continually add to their malware libraries to retain their status as active threats.



93% increase in number of threat groups per investigated environment.

In 29% of cases in 2020, Mandiant identified more than one distinct threat group in an environment—nearly twice the percentage noted in 2019. Adversaries are frequently working together to complete their mission. Organizations need to do likewise and choose strong security partners for stronger defenses.

Multiple Threat Groups Identified (Per Environment)

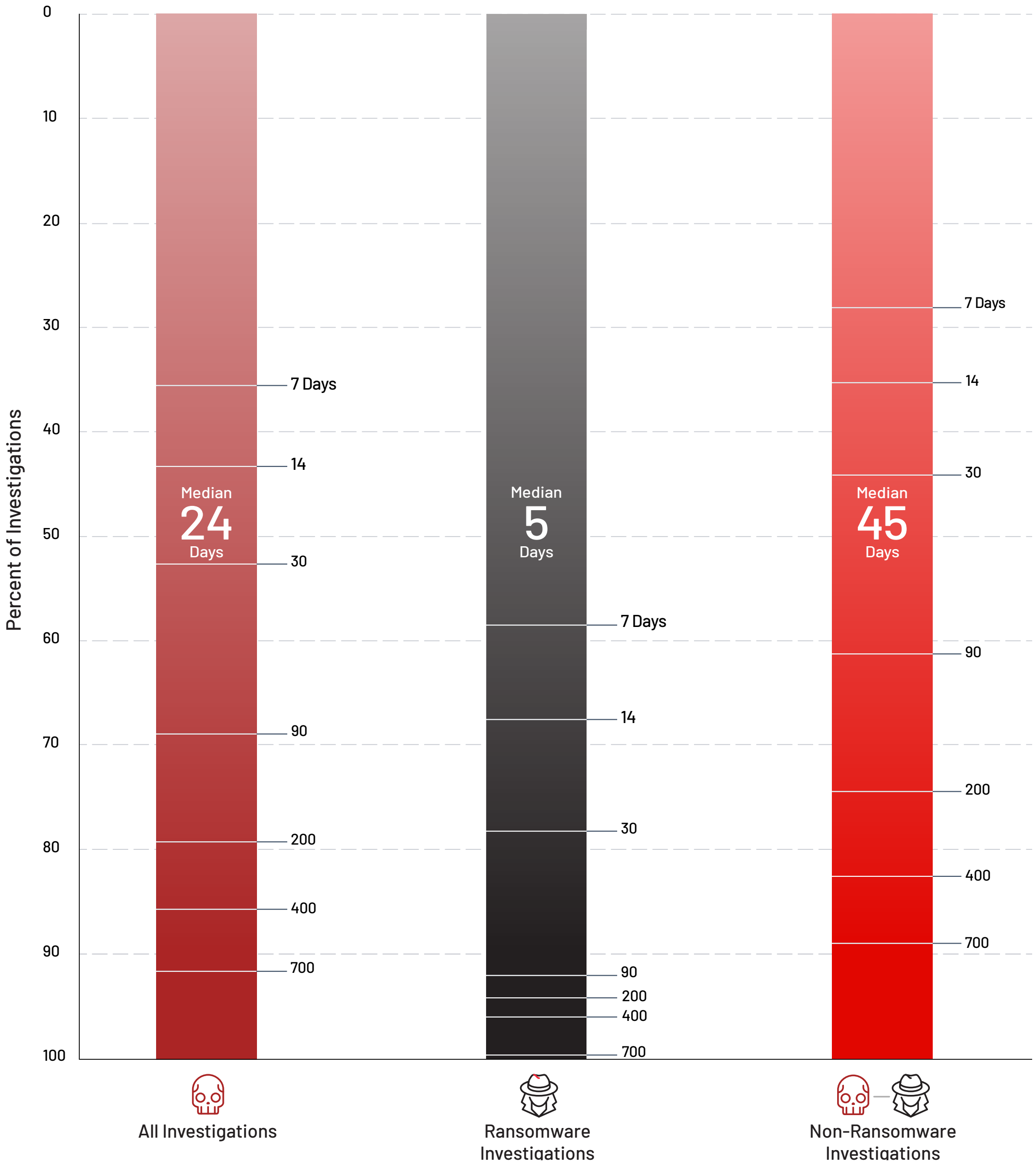


The global median dwell time for ransomware is just five days.

Ransomware is a major, rapidly growing threat with a very short dwell time compared to other attack types.

Without rapid detection and response, organizations may continually be at the mercy of ransomware threats. Comprehensive CTI can directly contribute to better threat visibility, giving users a chance to respond before malware takes hold of their systems.

Global Dwell Time by Investigation Type, 2020



The Elements of Reliable CTI

Approximately 85% of organizations subscribe to some form of threat intelligence. However, to deliver value, data from a reliable CTI program should be trustworthy, timely and actionable.

Trustworthy

There is a plethora of threat feeds and more feeds does not deliver immediate value. Not only can adversaries access many of these feeds and use them for counter intelligence, but the attacker may also be the source of some feeds. Security leaders and threat analysts must know who supplies their data to make reliable and critical decisions.

Timely

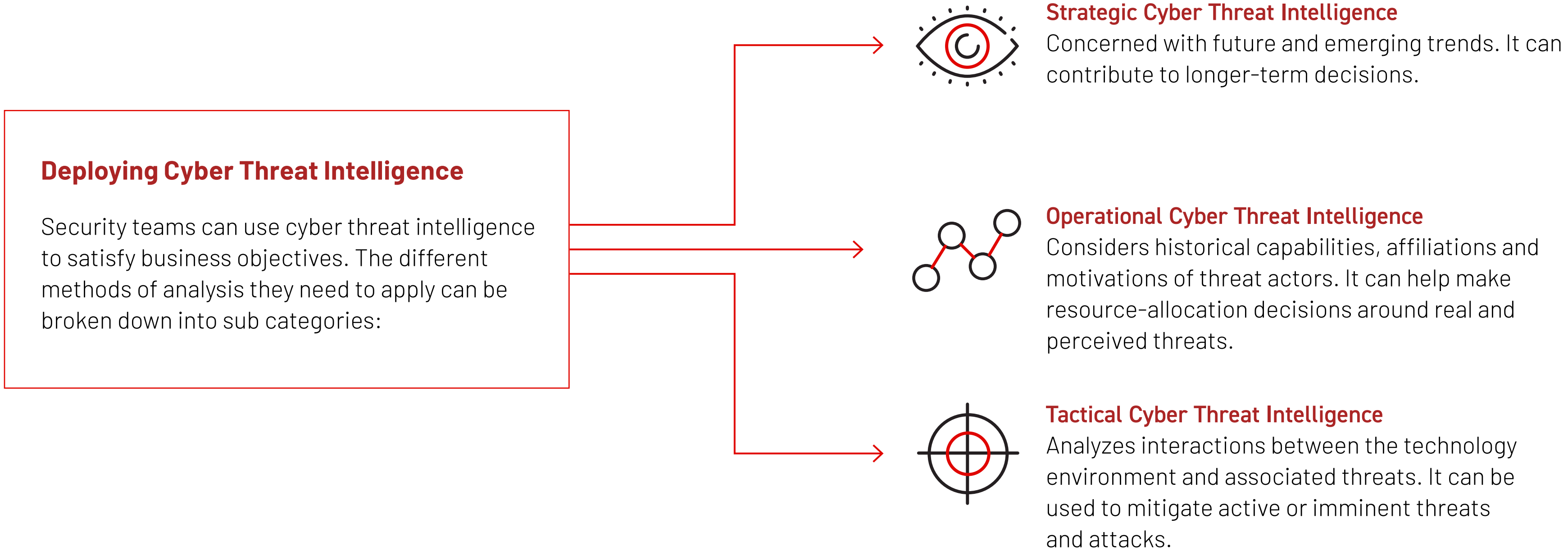
IOCs are easy to get and may be reused many times by others. Today, 45% of CTI consumers are dissatisfied with identification and removal of expired IOCs. And another 30% complain about the timeliness of threat intelligence data. "IOCs tend to have short lifespans as threats shift infrastructure and capabilities frequently."

Without timely insights on current threats, organizations may consume the wrong insights and hunt for activities that are no longer relevant while a bad actor injects malicious code into their systems.

Enemy Disruption Through CTI

Unlike natural disasters, cyber threats are driven by human beings. A comprehensive CTI program should provide actionable data that offers insight into the adversary, its motives, and its tactics, techniques and procedures. Knowing what drives the enemy can empower security teams to quickly identify threats that matter and prevent cyber attacks.

CTI must provide tactical, operational and strategic all-source intelligence on malicious actors (including state-sponsored, criminal and hacktivist groups), their activities and campaigns to drive optimal security and business decisions.



Deploying Cyber Threat Intelligence

Security teams can use cyber threat intelligence to satisfy business objectives. The different methods of analysis they need to apply can be broken down into sub categories:

Strategic Cyber Threat Intelligence
Concerned with future and emerging trends. It can contribute to longer-term decisions.

Operational Cyber Threat Intelligence
Considers historical capabilities, affiliations and motivations of threat actors. It can help make resource-allocation decisions around real and perceived threats.

Tactical Cyber Threat Intelligence
Analyzes interactions between the technology environment and associated threats. It can be used to mitigate active or imminent threats and attacks.

Examples and Use Cases

Strategic CTI to develop or maintain a holistic threat profile

Organizations develop cyber threat profiles to maintain holistic situational awareness on threats, vulnerabilities and risks. Adversary-based intelligence should include threat actors and their motivations, campaign trends, malware and capabilities. This is used to inform and guide cyber defense operations or risk teams by tracking threat actors and their activity, while gaining a better understanding of their potential impact to the business.

Operational CTI to prioritize alerts

Alert fatigue plagues security operations. Threat analysts routinely receive tens of thousands of alerts they will never be able to address. They need automatic correlation between intelligence and alerts that streamline prioritization of alerts to make faster triage decisions. They also need intelligence to develop alert criteria such as SIEM detection rules that better reflect the potential impact and sophistication of a threat. Analysts are unlikely to have time to read detailed intelligence reporting; they only want to know if an alert is related to malicious activity.

Tactical CTI to optimize vulnerability management with threat scoring

Organizations rely on intelligence to support their judgments on the relevance and impact of vulnerabilities. Critical elements of high-value intelligence include comprehensive insight on your organization’s vulnerable assets, the probability of attempted or successful exploitation within your environment or against specific assets, the adversary’s ability to weaponize and exploit those vulnerabilities, and the perceived threat or impact on your services and sensitive assets.

CTI Selection Criteria

Security organizations and threat analyst looking to consume threat intelligence or evaluating CTI subscriptions must ask several questions to help select an appropriate CTI solution:

- Are my current and future threat feeds providing information about the actors, threats my organization is facing and what I should prioritize?
- Who are the internal stakeholders? Who will need and use threat intelligence within the organization? Are the current threat feeds or subscriptions helping these stakeholders?
- Are there specific intelligence requirements or threat formats that best serve the needs of stakeholders? Will the CTI program produce the latest, to-the-minute, actionable intelligence?

These guidelines are critical to building a successful CTI program. Neglecting due diligence can complicate the alignment of intelligence capabilities to business needs and diminish your organization's ability to become an intelligence-led cyber security leader in your industry.

The Value of Comprehensive Cyber Threat Intelligence

Comprehensive CTI allows organizations to be proactive and prepare themselves for tomorrow's adversaries and threats, rather than reacting to yesterday's news stories. Without the ability to consider all risks and options available to them, cyber security professionals cannot make the best possible security decisions for their organization. In addition and perhaps most importantly, comprehensive CTI can help the organization prepare for attacks and manage risks, creating a more effective security and risk management program and process.

Benefits of Cyber Threat Intelligence:

Valuable insight and context

Detailing information on which threats are most likely to affect an organization or industry and indicators to help prevent, direct and detect more attacks.

Improved incident response times

Prioritizing alerts which enables an organization to respond faster to real threats and reduce the risk of serious breach consequences.

Improved communication, planning and investment

Security teams can communicate real risks to the business and focus on protecting high-risk targets from actual threats via additional security investment and planning.

> 93% of global organizations reported some form of successful cyber attack in the past 12 months.[1]

[1] FireEye (November 2019). Cyber Trendscape 2020.

Learn more at **www.mandiant.com/intelligence**

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant

Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.