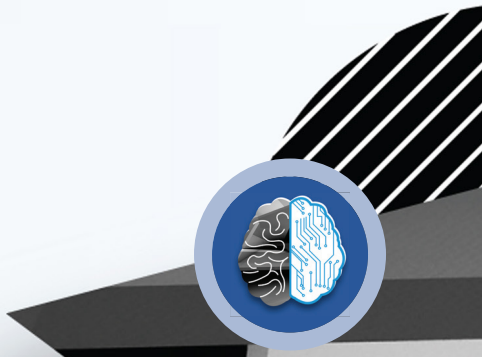
WHITE PAPER

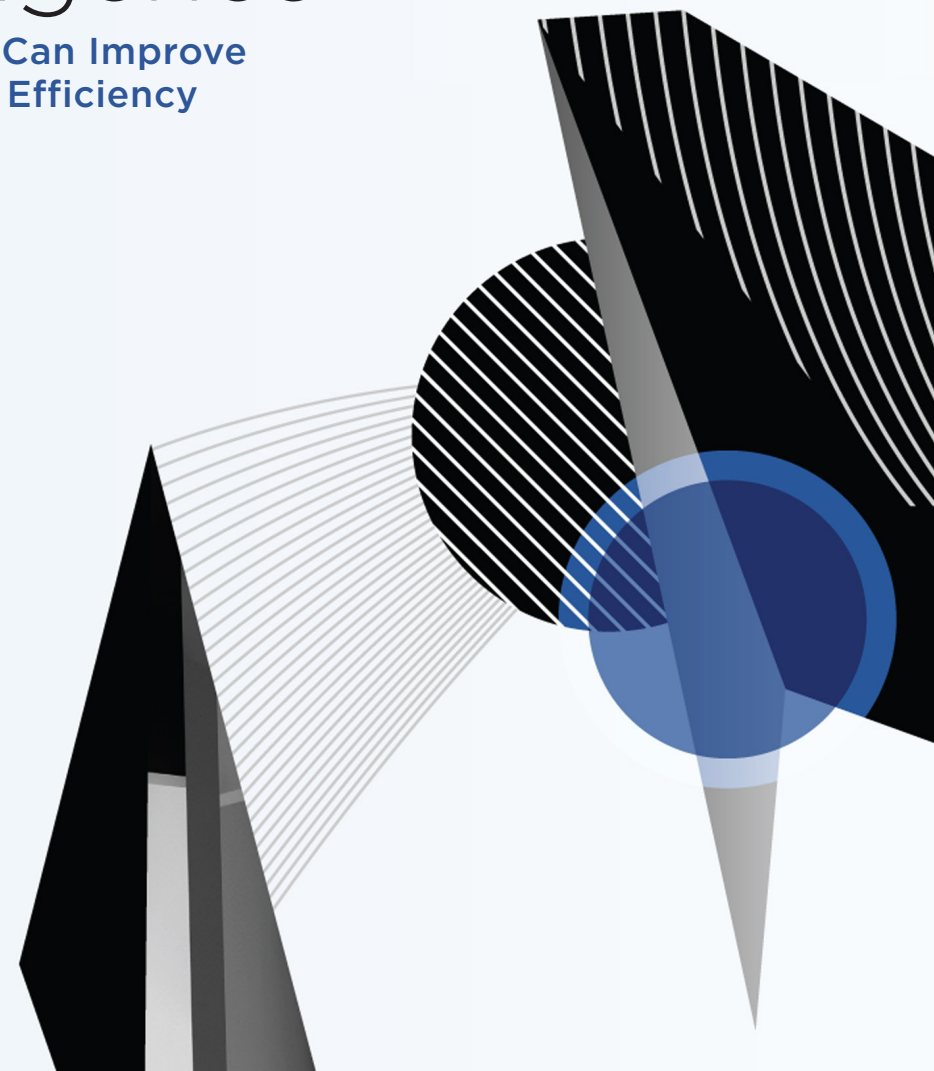


FireEye®

The Cost of No Context:

The Value of True Cyber Threat Intelligence

How Cyber Threat Intelligence Can Improve Risk Management, Operational Efficiency and Strategic Planning



Executive Summary
Sophisticated IT security executives realize that cyber threat intelligence is an essential weapon for detecting and preventing advanced attacks from well-funded attackers with specific agendas and targets. However, even experienced IT executives must navigate through competing vendor claims to evaluate cyber threat intelligence offerings.

This paper will help executives clearly differentiate between threat data feeds and genuine cyber threat intelligence. Overall, cyber threat intelligence is far more useful because it offers:

- Greater visibility into threats.
- Faster response to targeted attacks.
- Better executive communication.
- Improved strategic planning and investment for the security organization.

Distinguishing Between Indicators and Intelligence

Not all companies define cyber threat intelligence in the same way. In fact, there is a spectrum of threat indicators, ranging from signature and reputation feeds to threat data feeds to cyber threat intelligence (Fig. 1). Each of them has a very different definition and offers distinct business value.

Table 1. The spectrum of threat indicators and intelligence.

	Signature and Reputation Feeds	Threat Data Feeds	Cyber Threat Intelligence
Deliverables	Signatures URL Reputations Threat Indicators	Threat frequency data "Anatomy of an Attack" information	Forward-looking analysis of threat actors and methods, customized to client requirements
Value	Increases effectiveness of blocking technologies	Identifies patterns associated with attacks	Extends visibility into threats Speeds response to targeted attacks Clarifies executive communication Informs planning and risk management
Limitations	No insight into patterns Increases alert volume	Passive data collection Backward-looking, generic analysis	

Signature and reputation feeds

Signature and reputation feeds typically provide a stream of malware signatures (file hashes), URL reputation data and intrusion indicators, sometimes supplemented by basic statistics (such as "Today's top 10 malware threats"). This data can be sourced from nonprofit and industry clearinghouses, from vendor security devices at customer sites and from sensors distributed around the web.

The primary value of signature and reputation feeds is to improve the effectiveness of next-generation firewalls (NGFW), intrusion prevention systems (IPS), secure web gateways (SWG), anti-malware and anti-spam packages and other blocking technologies. Up-to-date security data helps these technologies recognize and stop malware and network traffic from web sites known to be controlled or compromised by attackers. A secondary value is to provide raw data to help security information and event management (SIEM) systems detect known threats.

Although signature and reputation feeds are one facet of a traditional defense-in-depth strategy, they have clear limitations:

- They help block mass attacks, but miss targeted attacks for which no signature exists, as well as malware that has been morphed, encrypted, included in downloaded apps or otherwise disguised (a Symantec executive recently estimated that antivirus products now detect only 45% of attacks[1]).
- They provide data on individual threat indicators, but no context to help organizations understand how to put those indicators together to identify a real attack or what action to take.
- They cause NGFWs, IPSs, SWGs, anti-malware packages and SIEM systems to generate more warnings and alerts than the security operations center (SOC) staff and incident response (IR) team can possibly evaluate, concealing important warnings in a barrage of noise.

Threat data feeds

Most information security vendors now offer a "threat lab" or "intelligence network" staffed by a small team of researchers who monitor threat data from vendor devices and sensors and may provide a basic level of human analysis. This analysis usually includes statistical breakdowns of the prevalence, source and targets of malware and attack activities. The lab staff may also publish "anatomy of an attack" discussions that document the details and sequence of actions taken by specific malware or an advanced, multi-stage attack.

Threat data feeds are useful for SOC and IR teams, because they help the teams identify patterns associated with attacks, rather than simply isolated indicators. The information can also provide an understanding of how to remediate compromised systems.

But taken alone, most threat lab analyses are limited:

- Data gathering is passive and often skewed to the geography and industry profile of the vendor's customer base. Example: "What did we see on our firewalls and network sensors?"
- Analysis is backward-looking. Example: "Here is what we observed attacking networks over the past six months."
- They lack intelligence that can help recognize when actors are preparing to attack or the new tactics and techniques they may employ.
- They lack intelligence that reveals successful but undetected breaches. Example: Credit card numbers or customer information associated with the enterprise Is discovered on underground hacker web sites.
- Analysis is generalized across the entire customer base of the vendor or at best across very broad industry groups such as finance, healthcare and manufacturing.

Usually these limitations are simply a result of what some information security product vendors are able to provide. A threat lab or intelligence network is a nice way to differentiate one NGFW or SWG from another, especially since passively-collected data is essentially free to the vendor. But genuine threat intelligence requires serious vendor investments in staff and expertise and includes active data gathering by humans and sophisticated technology, forward-looking analysis and customization based on client needs.

Cyber threat intelligence

Genuine cyber threat intelligence (CTI) often includes signature and reputation feeds and threat data feeds, but goes beyond them in several critical areas.

CTI includes active human and technical information gathering on a global scale. It aggregates data from industry clearing houses and network sensors and continuously monitors hacking groups and underground sites where cybercriminals and hacktivists share ideas, techniques, tools and infrastructure. It requires systematically collecting data based on the location of threats and targets, not the vendor's offices or customer locations. It also involves building a staff with diverse language skills and cultural backgrounds who can understand the motives and relationships of adversaries in China, Russia, Eastern Europe and other hacker havens.

CTI is adversary-focused and forward looking, providing rich contextual data on attackers and their tactics, techniques and procedures (TTPs). It requires a comprehensive understanding of the character and motivation of emerging adversaries, business initiatives that increase the attack surface (opportunities for attacks), the vulnerabilities of new technologies and business practices (mobile devices, virtualization, cloud and SaaS solutions) and how those factors interact. This might include, for example, determining the motivation and targets of a new type of cybercriminal, the vulnerabilities they target, the domains, malware and social engineering methods they use, the structure and evolution of their campaigns and the techniques they are likely to employ to evade current security technologies and practices.

CTI is customized for each client. It gathers situational data and intelligence requirements from each client and provides analyses tailored to the industry, technologies and specific situation of that organization. Top-quality CTI providers offer direct access to analysts so clients can receive in-depth clarification on intelligence. They also allow clients to submit malware samples for analysis. Customized information gives enterprises extra context to set priorities and make optimal decisions based on their specific needs and risk profiles rather than broad industry averages.

The value of cyber threat intelligence

Cyber threat intelligence tends to cost more than threat data feeds. But it also does much more. It allows enterprises to become proactive and prepare themselves for tomorrow's adversaries and threats, rather than reacting to yesterday's news stories. Advantages include not only greater visibility into threats, but also faster response to targeted attacks, better executive communication and improved strategic planning and investment by the security organization.

Greater visibility into threats

Cyber threat intelligence utilizes researchers around the world who speak the native languages, are knowledgeable of the local cultures and familiar with slang and colloquial terms. They are uniquely positioned to uncover new threats and threat actors (cybercriminal gangs, hacktivist organizations and state-sponsored actors) as they collaborate globally to use or develop new campaigns, TTPs, malware variants and social engineering techniques. Consequently, this type of intelligence:

- Gives security staff insight into new indicators of compromise (IOCs) and other clues to help prevent and detect more attacks.
- Gives IT managers, security analysts and others insight into which applications, systems and user populations are most likely to be attacked and how, so security can focus on protecting those high-risk targets from actual threats.

It is difficult to estimate the probability of any particular technology preventing one or more data breaches. However, a recent study by the Ponemon Institute calculated a mean cost per cyber crime of $7.2 million, ranging from an average of $3.0 million for the smallest quartile of companies in the survey to $13.8 million for the largest quartile.[2] Another study found an average cost of $145 per record for lost or stolen records containing sensitive and confidential information.[3]

Faster response to targeted attacks

At major enterprises, NGFWs, IPSs, SIEM systems and other security tools typically generate thousands of alerts and notifications each day. The vast majority of these are unimportant, consisting of potentially suspicious files and activities that turn out to be benign. Many may represent real threats — but only to organizations in a specific industry (finance, retail, government, healthcare), with specific applications (SAP, WordPress) or specific equipment (POS or SCADA systems). Most SOC and IR teams lack the time and expertise to sort through all these alerts or even to perform triage on them intelligently. This means that when attackers gain a foothold inside the network, it typically takes weeks or months to detect them. Statistics paint a distressing picture. According to one study, nearly 100% of successful breaches compromised data within days of initial intrusion while only 16% were detected within the same time table.[4] CTI services improve the operational efficiency of SOC and IR teams by giving them detailed information on which threats are most likely to affect their firm. This shrinks the problem and allows teams to focus on a smaller number of alerts and notifications that represent real threats to their company. The threat analysis provided by CTI services enables SIEM tools to automatically raise the priority of truly meaningful alerts. It also provides the context required for team members to recognize patterns of events that point to attack campaigns.

CTI services can help organizations use information from signature and reputation feeds and threat data feeds. SOC and IR teams can focus on the data and threat reports that are most relevant to their situation and put aside the data and analyses that don't apply.

In fact, some CTI services offer threat data feeds of their own. The best CTI vendors link threat data with context such as adversaries, campaigns, targets and other information that makes intelligence actionable. This rich, contextual intelligence can be fed into SIEM systems and other security products through APIs. Such integrations might allow a SIEM system to correlate events generated by network security tools with indicators of compromise provided by the CTI service. The SIEM system could also use intelligence provided by the CTI service to increase the priority of alerts associated with threats that target the company's industry, geographic locations and major software applications.

Vulnerability patching is another area where CTI can help organizations respond faster to immediate threats. Many enterprises prioritize their patching efforts based on generic rating labels. But an organization can prioritize patches much more effectively if it receives rich information about each vulnerability such as how it works, how hard it is to exploit and whether exploit tools are currently available or under development in the wild. They can also learn whether a specific vulnerability is actually being exploited by adversaries targeting the organization's industry. Better prioritization means less time wasted on "critical" vulnerabilities that actually pose little risk.

By helping prioritize alerts, CTI services increase the operational efficiency of security and incident response staffs and allow them to respond faster to the most serious attacks. Improvements in response can pay big dividends. One study found the cost of cyber attacks averaged $20,758 for each day they were active on the network.[5] At that rate, helping an IR team focus better and identify a threat one week earlier would result in cost savings of over $145,000.

Better executive communication

CISOs often face serious challenges communicating information security issues to business managers, top executives and boards of directors. This makes it extremely difficult to obtain the cooperation — and the funding — justified by actual security threats. A chief financial officer (CFO), for example, is unlikely to increase a budget after hearing "Last week we evaluated 1,000 alerts and blocked 200 pieces of malware, but the frequency of zero-day attacks is increasing."

CTI provides information that can put a face on adversaries and translate cyber threats into business risks, using terms that are meaningful to non-technical executives. CFOs and division general managers respond more favorably to statements such as "Last week we thwarted attacks by a hacktivist group in Eastern Europe trying to degrade our website and damage the corporate brand," or "Companies in our industry are facing a wave of attacks by state-sponsored hackers in Asia who are targeting engineering designs and trade secrets."

Improved strategic planning and investment

CTI services can provide concrete evidence and informed analyses about emerging adversaries and new types of threats. This information can direct enterprises toward planning and investment decisions that improve their security posture while reducing unnecessary risk and spending.

For example, intelligence about new malware types or DDoS attacks can guide investments toward the right technologies to block those new threats. Intelligence about new adversaries and their targets can help security groups allocate resources efficiently and conduct activities more effectively to protect targeted information assets, monitor targeted user groups or scan specific web traffic. Intelligence about the techniques behind new multi-stage attacks can help incident response teams focus on tools and methods that correlate disparate events to expose advanced persistent threats (APTs).

Intelligence can also show that some threats are not relevant to specific industries or company types, saving enterprises from investing scarce resources in the wrong places.

By improving strategic planning and investment and by making security teams more effective and efficient, CTI services can dramatically improve the productivity of security teams. The positive impact can be equivalent to a significant increase in the IT security budget.

Summary

Almost every information security vendor offers some flavor of threat intelligence. Although every form of threat intelligence has value, it is important to recognize the limitations of each offering.

Signature and reputation feeds can make blocking technologies more effective, but they don't provide enough information to identify advanced attacks. They often cause security devices to generate more warnings, alerts and false positives than SOC and IR teams can possibly evaluate.

Threat data feeds help SOC and IR teams understand the anatomy of advanced attacks, but this information alone is often historical and generalized across the entire customer base of the vendor.

Genuine cyber threat intelligence includes active monitoring of underground forums by a staff with diverse language and cultural skills. It provides forward-looking analyses and robust, highly contextual information based on the threats, actors and methods that provide the greatest risk to specific companies, in specific industries, at specific times. Authentic CTI fuses a diverse set of technical and human-derived data sources into intelligence that is actionable across strategic, operational and technical risk management levels.

Cyber threat intelligence services:

- Provide visibility into new types of advanced attacks that could potentially result in multi-million dollar data breaches.
- Help organizations respond faster to real threats and reduce the risk of serious breach consequences by allowing security teams to set aside the vast majority of alerts and focus attention on specific business processes targeted by attackers.
- Help IT managers communicate real security risks and business issues to non-technical business managers and top executives.
- Allow managers to plan risk management strategies and security investments based on current and emerging adversaries and threat types.

These advantages not only reduce the risk of costly security breaches, they also help organizations align security spending with the requirements and risks of the organization.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.

FireEye®