ZEROFOX®

A Buyer's Guide for Threat Intelligence

Selecting threat intelligence that best meets your internal and external cybersecurity requirements

Table of Contents

ZEROFOX

INTRODUCTION

So you're building an Intelligence Program

You lead a security team for a non-security organization. A serious cyberattack has dominated the news cycle for the last month. Your company's executives and board members are now asking each other – and you – about threat intelligence. Do we have the information needed to adequately address cyber risks, both inside and outside the firewall? Where do we get our cyber threat intelligence? Is it current? Is it enough?

What threat intelligence? - you secretly ask yourself. Building a robust intelligence program is on your strategic roadmap, but it has not yet been prioritized or budgeted. Like all business functions, competing priorities challenge security teams. When large-scale events trigger fear and uncertainty (say, for example, a high-profile breach or global pandemic), teams must adapt based on the best information available.

Whether you're starting from scratch or maturing your existing threat intelligence program, building on the right foundation is critical. Intelligence is a broad domain that requires specific skillsets. Can you hire enough talent to meet your needs? Will the required funds to build the right architecture be provided? Can you source intelligence to protect both your critical internal and external assets? It's difficult to measure the Return on Investment (ROI) of an intelligence program – could this impact your position?

You reinforce that an intelligence program will enrich the work your team is doing and that you'll provide a proposal with a recommended strategy, timeline, and resourcing to move forward.

It's time to get to work.

Threat actors have long had the advantage in the digital world, going unnoticed before a cyberattack. Now, leaders across industries view threat intelligence as a vital component of a mature, proactive cybersecurity posture.

Investing in intelligence: where to begin

Although business leaders often focus on the nefarious threat actors operating throughout the Dark Web, an impactful intelligence program must also have the power to collect across the entire internet at scale, monitor social media, and it must be able to maintain visibility in covert communications channels. Security professionals are challenged with how to maintain awareness of the various threat actors, underground forums, vulnerability exploits, and attack vectors and how those threats specifically pertain to their organization, including all critical internal and external assets. From capabilities that are offered "as-a-

service" – such as initial access brokering or ransomware kits – to trafficking of zero-day software exploits in underground markets, the notion that threat actors are all sophisticated, meticulous computer experts is no longer the case. Threat actors have long had the advantage in the digital world, going unnoticed before a cyberattack. Now, leaders across industries view threat intelligence as a vital component of a mature, proactive cybersecurity posture. Even still, they're faced with a skills gap, and without a dedicated in-house team or managed service arrangement with a trusted provider, the challenge of operationalizing intelligence is daunting.

The value of Threat Intelligence Programs

Threat intelligence shifts a company's security posture from reactive to proactive – it provides visibility into cyber-activities that can not only indicate what attackers have done but also what they will likely do next. When configured properly, security teams can more effectively identify and disrupt impending targeted attacks. It can alert teams about relevant, active breaches that are secretly exposing the personal identifiable information (PII) of customers or executives to thousands of earnest cybercriminals.

The right intelligence program also enables teams outside security to make better decisions. Risk exposure slows down business and, whether teams are fundamentally responsible for security or not, disseminating relevant intelligence across the organization can help all teams mitigate risk for the organization itself, its partners, and its customers. Vast amounts of time and energy will be saved through effort reduction against low-level threats, attacks aimed at dissimilar companies, and concerns around vulnerability exploits targeting systems and applications not present in your network. In 2021 alone, there were more than 20,000 common vulnerabilities and exposures (CVEs) reported. It is worth noting that this figure only accounts for known vulnerabilities, meaning zero-day threats represent additional uncalculated risks to organizations.

20K+
CVEs IDENTIFIED IN 2021 ALONE

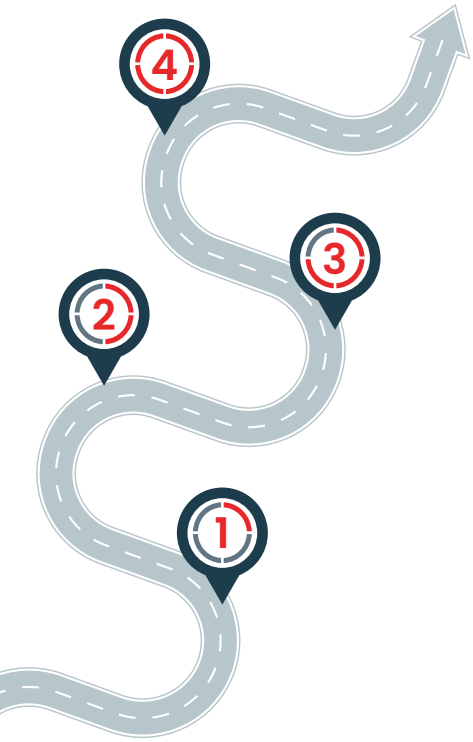
DO YOU CARE?

- Which CVEs relate to my environment?
- Which CVEs have been exploited?
- What's the potential impact?

According to the most recent SANS Institute CTI Survey, only around one-third of respondents had formal, documented intelligence requirements and another one-third said their requirements were created on an ad-hoc basis. Documenting intelligence requirements – aligned to identified stakeholders – is a key starting point for any security organization. Without these requirements as a guide, intelligence collection, analysis, and production are unlikely to yield the expected value. Conversely, stakeholder-approved intelligence requirements enable intelligence teams to track meaningful metrics and measure the impact of the intelligence program. Maturing ad-hoc intelligence processes into a holistic, strategic threat intelligence program that incorporates the intelligence cycle and documented requirements empowers a security organization to put more energy into supporting the growth of their business, rather than wasting valuable resources chasing threats hyped by the media (but not relevant to the business).

ZEROFOX

CRITERIA



Selecting the right threat intelligence

Building a holistic threat intelligence program is a process, and many organizations try to build these programs by dividing threat intelligence responsibilities across various security groups. And while a crawl-walk-run approach is a great strategy to ensure your intelligence program and organizational priorities are aligned, starting on a solid foundation will help avoid common missteps such as tasking traditional security teams with threat intelligence responsibilities. Because of the distinctive skillsets intelligence professionals require, assigning intelligence roles to traditional security teams rarely produces new intelligence. Instead, it yields repackaged open-source information without structured analysis; it does not include the context or recommendations needed that make threat intelligence valuable. Often, the information is only relevant to understanding threats to traditional IT infrastructure under your control, completely ignoring your external footprint on the web, social media, forums and marketplaces, and mobile app stores.

Mature intelligence programs enrich their own security data with the best external data, information, and intelligence to connect internal findings with external context. They also acknowledge the lack of visibility of those external assets, and seek sources of intelligence to illuminate relevant threats. However, this approach requires a substantial amount of time, money, and expertise that many companies are unable to invest. Because the road to building a world-class intelligence team is long, partnering with external intelligence providers is the most efficient and effective way to deliver the right combination of software, people, and information.

Today's threat intelligence market is difficult to navigate, and this guide is designed to help. We've broken down key strategies and tactics to help you avoid common pitfalls and find the right provider(s) and solution(s) for your organization.

In this guide, we will review the following topics

1. Intelligence Requirements Alignment
2. Breadth & Depth of Intelligence Collection
3. Judging the Quality of Intelligence Products
4. Operationalizing Threat Intelligence

Criterion 01

Intelligence requirements alignment

First things first – security professionals must have a well-developed understanding of their organization's intelligence requirements (IRs). These are the specific questions that must be answered to make risk-based security decisions for your organization's unique needs. Mature intelligence vendors assist in developing or reviewing IRs to ensure they're focused on helping protect your most critical assets from the most relevant threats in order of priority.

Alignment among internal stakeholders is just as important as alignment with any external vendors or partners you engage. At most organizations, security operations teams are the primary consumer of threat intelligence. Still, you must not neglect the needs of the teams responsible for network architecture and configuration. You also don't want to leave out your organization's leadership teams that need intelligence to inform strategic plans. In fact, if you're not considering stakeholders from outside the traditional information security team, you're missing a big piece of the puzzle. Revenue and marketing leaders, corporate strategy, and legal counsel are groups that can and should be using threat intelligence. Corporate security and safety teams can benefit from intelligence to help keep executives, employees, facilities, and customers safe from physical threats.

Spend the time identifying particular use cases each team needs and how they plan to employ threat intelligence. You'll set yourself up to create an effective intelligence program, sidestepping some of the most common issues that arise when intelligence programs aren't purpose-built to support a unique set of requirements.

One method to uncover hidden exposures – and potential new threat intelligence stakeholders within an organization – is attack surface visualization. This service can expose attack vectors such as vulnerabilities with active exploits, network security misconfigurations, social media pages for your brand(s), profiles of executives, and potential malicious domains that may otherwise go unnoticed.

KEY TERM

Intelligence requirement

A requirement for intelligence to fill a gap in the knowledge or understanding of the operational environment or threat.

TIP

Ask the vendor about their Standing Intelligence Requirements

Once you've established your intelligence requirements, identifying the right threat intelligence vendor(s) whose capabilities align with those requirements is vital. The most effective vendor will be able to deliver both global intelligence that provides insights on large strategic concerns (geopolitics, threat landscapes, trends, etc.) and packaged intelligence feeds that align with your tactical and operational needs. A good way to communicate with vendors about intelligence requirements is often through use cases. For instance, a financial services company would likely have concerns related to fraud, account takeover, and compromised credentials. In contrast, a manufacturing company will likely be much more concerned with threats to Industrial Control Systems (ICS) or their supply chain.

To meet your needs, threat intelligence vendors also need a mechanism for easily adapting to any of your requirements that aren't necessarily included in their own. Through a process known as a Request for Information (RFI), you're able to ask very specific questions that the analysts can answer, through the intelligence process, with reports that include observations, assessments, and recommendations for actions you can take to mitigate risks. Before onboarding a vendor that provides this service, request sample reports to gauge the quality of their work. You may be able to find examples of these reports on the vendors' websites as well.

INTELLIGENCE REQUIREMENTS EXAMPLES

- What **security threats** may impact the organization's personnel?
- What **fraud defense technologies** are being actively targeted or bypassed by threat actors?
- What are the **emerging or current threats** that target or potentially impact the organization's digital crown jewels?

Criterion 02

KEY TERM

Intelligence feed

A flow of content between machines that has been processed by either humans or machines that were programmed and educated by humans to apply automated analytic processes.

Intelligence collection breadth & depth

A key consideration in selecting threat intelligence providers is understanding their collection sources, historical data retention protocols, and how frequently the data and information are supplemented to satisfy your intelligence requirements. A threat intelligence provider should include the broadest possible range of data sources that align with your objectives. Bear in mind that without processing and analysis, these sources are only data or information– not intelligence. If you don't have an in-house intelligence team, chances are you'll need feeds and complete intelligence reports that add context. Raw data and reshared open-source information lacks the analysis needed to improve decision making around the right actions to mitigate risk.

Breadth of collection

The ecosystem of digital communities and forums is expanding daily. Threat actors are on the move to evade detection, frequenting popular underground forums but also using encrypted communication channels to discuss how to conduct successful cyberattacks. It's important to note that threat actors use "paste sites" – commonly used to share legitimate source code – to post breach data and malware samples.

Additionally, monitoring media outlets provides useful early warning about new threats, but without connection to relevant technical indicators, it is almost impossible to measure actual risk. Your company's leadership and board will also be aware of these news stories so it's important to be prepared to report on your potential exposure. Look for a source that vets them and adds context with a focus on your industry and situation, along with helpful technical information such as attribution, impact, and related indicators of compromise (IOCs).

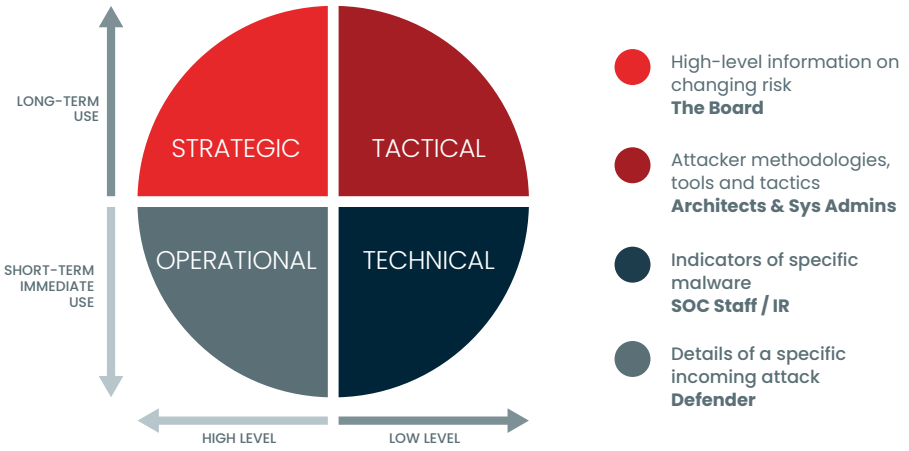
Finally, the most valuable threat intelligence comes from vendors who have a global presence, with expertise across industries and the digital ecosystem. They should offer front-line services that are directly involved in takedowns and incident response. Ideally, these vendors will also have experts with established false identities ("sock puppets") to maintain connections with threat actors themselves. The visibility from first-hand access to threat actors, in-process incidents, and breach response will be invaluable to your defenses and security posture. Whichever TI vendor you choose must be committed to keeping their collection efforts up-to-date and to expanding as new sources appear.

"Organizations are drowning in data and information, which is not the same as intelligence, resulting in poor operational use of the data and information to which they have subscribed."

Source: Gartner

SOURCE CATEGORY CHECKLIST

- Strategic Intelligence
- Tactical Intelligence
- Technical Intelligence
- Operational Intelligence



Source: https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf

Depth of collection

It's important to have access to a broad range of intelligence sources as well as to historical reporting. Established vendors with a robust intelligence library provide deeper insights than those relying exclusively on currently available sources. Your teams should also be able to search for or request historical intelligence reporting via the RFI process to answer any additional intelligence questions.

To address these concerns, it is wise to first have a collection plan built on the foundation of the IRs referenced earlier. Understanding your own needs – the questions you must answer and for which audiences – is the surest way to identify the kinds of data, information, and intelligence you need to collect either for yourselves or through partners.

DANGEROUS DOMAINS

- Threat actors are leveraging internet domain names to conduct attacks against your internal and external assets. Spoofed Domains are used by threat actors who attempt to trick your customers or partners into thinking they're really you, thereby gaining access to login credentials, PII, and other confidential information.
- Attackers create infrastructure they use to conduct operations against your IT stack, known as Command & Control (C2) Domains, in order to gain access to your network or exfiltrate data.

KEY TERM

Botnet

A network of private computers infected with malicious software and controlled as a group without the owners' knowledge.

Source: *Oxford Languages*

TIP

When assessing collection capabilities, ensure sources are kept up-to-date and maintain historical data for at least a year.

For example, if a financial services company determines that their stakeholders include the CSO, the CISO, the SOC, and a team focused on combating financial fraud (among others), they are likely to have IRs that include technical indicators to detect cyber compromises (for the SOC), trends in cyber actors' tactics, techniques, and procedures needed to proactively fortify networks (for the CISO), known or suspected threats to personnel or facilities of the company and those similar in industry and geography (for the CSO), and evidence of compromises of financial account numbers or credentials for accessing financial accounts.

Understanding these stakeholders and their needs results in understanding what needs to be collected. In this example, the financial institution should seek support from one or more vendors that can provide technical and tactical intelligence (for the SOC), strategic intelligence on threat actors and groups (for the CISO), operational intelligence on physical security threats (for the CSO), and intelligence on compromised credentials, credit cards, and cybercrime from the Deep and Dark Web (for the fraud team). In this scenario, while a vendor may be a world leader in threats to Industrial Control Systems (ICS), they would not provide much value for this financial services company. In contrast, a company that specializes in manufacturing would find that same ICS-related intelligence to be vital while likely having little to no interest in the fraud intelligence that the financial services company would consider a high priority.

All of this is to say that there are few absolutes in terms of the value of intelligence. That value is directly related to the needs of the stakeholder. This is why identifying stakeholders and capturing their needs (IRs) is vital to any successful intelligence program.

CATEGORY OF INTELLIGENCE	LEVEL (TACTICAL/OPERATIONAL/STRATEGIC)	STAKEHOLDER(S)
Intelligence Forecasts	Strategic	Board & C-Suite
Threat Landscape/Trends	Operational, Strategic	Directors & Executives
Geopolitical	Operational, Strategic	Directors & Executives
Disinformation/ False Narratives	Operational, Strategic	Directors & Executives
Physical Security	Tactical, Operational, Strategic	CSO, Physical Security, Executive Protection
Fraud Intelligence	Tactical, Operational	Fraud Team
Threat Models	Tactical, Operational	IR, Threat Hunters, Security Engineers & Architects
Technical Indicators (IOCs)	Tactical	SOC Analysts, IR
Brand and Domain Impersonations	Tactical	Brand & Marketing Teams

Criterion 03

Quality of intelligence products

When researching threat intelligence vendors, consider not only the quantity of intelligence sources but also the quality of the intelligence they produce. Automating blocking actions based on expired indicators of compromise (IOCs) or investing heavily based on bad, biased, or incomplete information can have immediate and long-term consequences.

The best way to evaluate the quality of a vendor's intelligence products is to request samples of feed datasets and finished intelligence reports. Share the samples with your security teams to gain their feedback, and review the reports with the following questions found on the next page to keep in mind.

Asking providers questions upfront is an important step to understand if their capabilities can help solve your challenges. Transparency is an important factor to evaluate alignment and if the potential partnership will yield consistent quality. So if a vendor cannot provide you with their analytic tradecraft standards on request, this may be a sign of an immature intelligence production process and could therefore lead to unreliable output.

Conducting brief satisfaction surveys can help assess the value of adding the vendor's threat intelligence products to your arsenal. If your teams aren't getting what they need, they'll let you know.

KEY TERM

Analytic tradecraft standards

Govern the production and evaluation of analytic products, and articulates the responsibility of intelligence analysts to strive for excellence, integrity, and rigor in their analytic thinking and work practices.

Source: dni.gov

Questions to ask when evaluating intelligence products

- Do the feed datasets contain added tagging and contextual information or are they just raw data?
- How often are the datasets updated? Are old indicators aged out?
- Do the reports integrate industry-standard frameworks so your security teams can operationalize the intelligence?
- Does the intelligence dataset or product appear to be something they can utilize in their daily workflow?
- Are the datasets formatted in such a way that the network security team can utilize IOCs to automate firewall rules on malicious IPs or trigger password resets on compromised account credentials?
- Can threat hunters leverage finished intelligence reports to help form new hypotheses in order to expand coverage of their hunts?
- Can vulnerability analysts use the CVE and exploit kits datasets and finished intelligence reports to better prioritize their patching and mitigation efforts?
- Do finished intelligence reports properly use words of estimative probability?
- Do finished intelligence reports clearly distinguish what the analyst knows, doesn't know, and what they think about the threat?

KEY TERM

Words of Estimative Probability (WEP)

Words or terms that can (and should) be used by threat intelligence analysts to produce intelligence products to convey the likelihood of a future event occurring. A well-chosen WEP provides a decision-maker with a detailed estimate upon which to base a decision, and further aids in expressing the extent of confidence in a given conclusion.

Source: medium.com

Criterion 04

Operationalizing threat intelligence

Time-to-value is a common measure in the world of B2B commerce, and it's an important factor when partnering with a threat intelligence provider. How and when you see value depends on your objectives, and it should never depend on the maturity of your threat intelligence program. A good vendor will be able to meet you where you are on your journey, whether you're just getting started or are a high-maturity team interested in supplementing your program. According to Gartner in their Market Guide for Security Threat Intelligence Products and Services, organizations that are just starting out can see quick wins with use cases like telemetry enrichment and vulnerability prioritization. When evaluating a threat intelligence solution, it's critical to understand if it can integrate with your existing solutions and workflows to support your organization's security use cases.

As you establish your organization's threat intelligence stakeholders, it's important to understand how each team wants to access and use this intelligence. If intelligence isn't disseminated to the right people at the right time, it has little value. Find out if your organization uses a Threat Intelligence Platform (TIP), either commercial or open-source. If so, consider integrating the intelligence feeds into that system to enrich and orchestrate the flow to the appropriate people and security tools. Integrating into the existing security stack is an effective way to make the intelligence accessible and usable without overwhelming teams with new technologies or too much data.

The intelligence vendor you choose should also provide other methods of access and distribution that enables users from various security teams to find what they'll need as new IRs arise, without having to go through an intermediary. Email dissemination for finished intelligence and alerts; web interface access for search and alerting capabilities; or, a mobile interface that supports both alert notifications and search functionality for datasets and finished intelligence.

Finally, as stated in the beginning of this report, it's vital to have a competent, experienced threat intelligence analyst in any scenario covered throughout this guide. They'll be able to prepare regular reports on relevant threats, respond to RFIs from internal security teams, assume the point-of-contact role for the vendor relationship, and brief your company's leadership team. Of course, not every organization staffs a full-time threat intelligence analyst. Some threat intelligence vendors offer a service to contract one or more dedicated, named threat intelligence analyst(s) who will act as an extension of your security team.

TIP

Inquire whether vendor enables operationalization with existing tools and methods.

ZeroFox threat intelligence at work

PRODUCT	EXAMPLE CONSUMER (& SECURITY TOOL)	EXAMPLE USE CASES
 **OnWatch Alert**	SOC (using an integration with a SIEM, or Mobile Device)	› Infrastructure Takedown › Incident Response
 **Intelligence Search**	Incident Response/Threat Hunt/Fraud Team (using the ZeroFox platform)	› Threat Hunting › Incident Response › Fraud Management
 **Intelligence Feeds**	SOC/Vulnerability Management (SIEM, SOAR, TIP, VM)	› Automated IOC/IOA Blocking › Telemetry Enrichment › Vulnerability Triage & Management
 **Global Finished Intelligence Advisories**	Security Leadership (TIP)	› Strategic Planning Process › Budgeting Process
 **On-Demand Investigations & Dark Ops Services**	Security Leadership (TIP)	› Executive Threat Assessment › Location Threat Assessment › Digital Asset Recovery
 **OnWatch Expert, Dedicated Analyst**	CTI Team/Director of Security	› Outsourced TI Analyst › Staff Augmentation

CONCLUSION

How to select the right partner for your threat intelligence needs

Threat intelligence is a vital component to a strong security posture. It helps move security from reactive to proactive to best protect your organization. Of course, not all intelligence is created equal and each organization has its own unique needs. Use the information in this guide to make sure you find the right vendor who can support you through all stages of maturity.

To recap the main points this guide covered:

1. **Determine the vendor's alignment with your intelligence requirements** to ensure they have the capacity and tradecraft to focus on the things that matter to you and your organization both inside - and outside - the firewall. Make sure they can answer your security teams' questions. Should you need it, top vendors can help you craft effective intelligence requirements.
2. **Assess the breadth and depth of intelligence collection**, including surface, deep, and dark web, social media, marketplace, and mobile app store sources that are kept up-to-date but also maintain historical data that dates back at least a year. Having the deepest pool of data and historical intelligence typically results in the most context-rich analysis needed for the highest quality intelligence product to inform risk-based decision making.
3. **Evaluate the quality of the intelligence products** by inquiring about the vendor's analytic tradecraft standards. Ask for samples – data sets of IOCs or covert chatter or finished intelligence reports.
4. **Determine how well the vendor enables operationalization** including machine-to-machine integration with existing security tools, multiple dissemination methods to access reports or receive alerts, and, if needed, dedicated TI analyst contracts that ensure swift time-to-value.

About ZeroFox

The leader in External Cybersecurity

ZeroFox (Nasdaq: ZFOX), an enterprise software-as-aservice leader in external cybersecurity, has redefined security outside the corporate perimeter on the internet, where businesses operate, and threat actors thrive. The ZeroFox platform combines advanced AI analytics, digital risk and privacy protection, full-spectrum threat intelligence, and a robust portfolio of breach, incident and takedown response capabilities to expose and disrupt phishing and fraud campaigns, botnet exposures, credential theft, impersonations, data breaches, and physical threats that target your brands, domains, people, and assets. Join thousands of customers, including some of the largest public sector organizations as well as finance, media, technology and retail companies to stay ahead of adversaries and address the entire lifecycle of external cyber risks. ZeroFox and the ZeroFox logo are trademarks or registered trademarks of ZeroFox, Inc. and/or its affiliates in the U.S. and other countries.

See ZeroFox in action

zerofox.com/demo | zerofox.com

Get in touch with us today

sales@zerofox.com | 855.736.1400