FORRESTER®

The Forrester Tech Tide™: Threat Intelligence, Q2 2021

Fifteen Technologies And Services Underpin Threat Intelligence

by Brian Kime and Elsa Pikulik

April 13, 2021 | Updated: April 22, 2021

Why Read This Report

Threat intelligence is increasingly critical to firms' ability to manage cyber risk and build resilient security programs. To accelerate their threat intelligence performance, firms are evaluating and adopting multiple services and technologies. This Forrester Tech Tide™ report presents an analysis of the maturity and business value of the 15 service and technology categories that enable an effective threat intelligence-driven security program. Security and risk pros should read this report to shape their firm's investment approach to these technologies.

The Forrester Tech Tide™: Threat Intelligence, Q2 2021

Fifteen Technologies And Services Underpin Threat Intelligence

by Brian Kime and Elsa Pikulik
with Alla Valente, Salvatore Schiano, Merritt Maxim, Benjamin Corey, and Peggy Dostie

April 13, 2021 | Updated: April 22, 2021

Leverage Threat Intelligence To Manage Risk And Reduce Breaches

Cyberbreaches often result in financial losses and harm to brands, forcing firms to spend precious resources on incident response, breach notifications, possible regulatory fines, lawsuits, as well as lost employee productivity and reduced customer confidence. Security and risk professionals must build resilient cultures and architectures. Critical to building that resiliency is an understanding of threat intent and objectives and using that knowledge and forecasts to improve decision-making. By building a robust threat intelligence capability, security and risk professionals can reduce risk to intellectual property and business processes and ensure trust and confidence in customers and partners.

Curate A Set Of Technologies That Enable Threat Intelligence

Forrester surveyed technology decision-makers, suppliers, and other subject matter experts in our search for the most important threat intelligence technologies. Each of the technology categories analyzed in this Forrester Tech Tide meets three criteria and:

- **Is an important contributor to understanding threats and managing risk.** Each technology and service is fundamental to understanding threats regardless of domain (physical or cyberspace) and helps S&R pros detect and monitor said threats from the tactical level to the strategic level. Additionally, we focused on technologies that help threat intelligence teams manage stakeholder requirements, efficiently aggregate raw threat intelligence, analyze and derive insights from internal and external security telemetry, and disseminate finished intelligence to stakeholders.
- **Is commercially available at enterprise scale.** Vendors included in this report are both established and recent market entrants. They offer products that vary in size, technical scope, regional focus, and market approach.
- **Has (or will have) market traction.** The technologies and services listed in this report vary in market maturity. We included technologies that clients are using today and those they should use in the future.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Select Threat Intelligence Technologies That Offer High Business Value

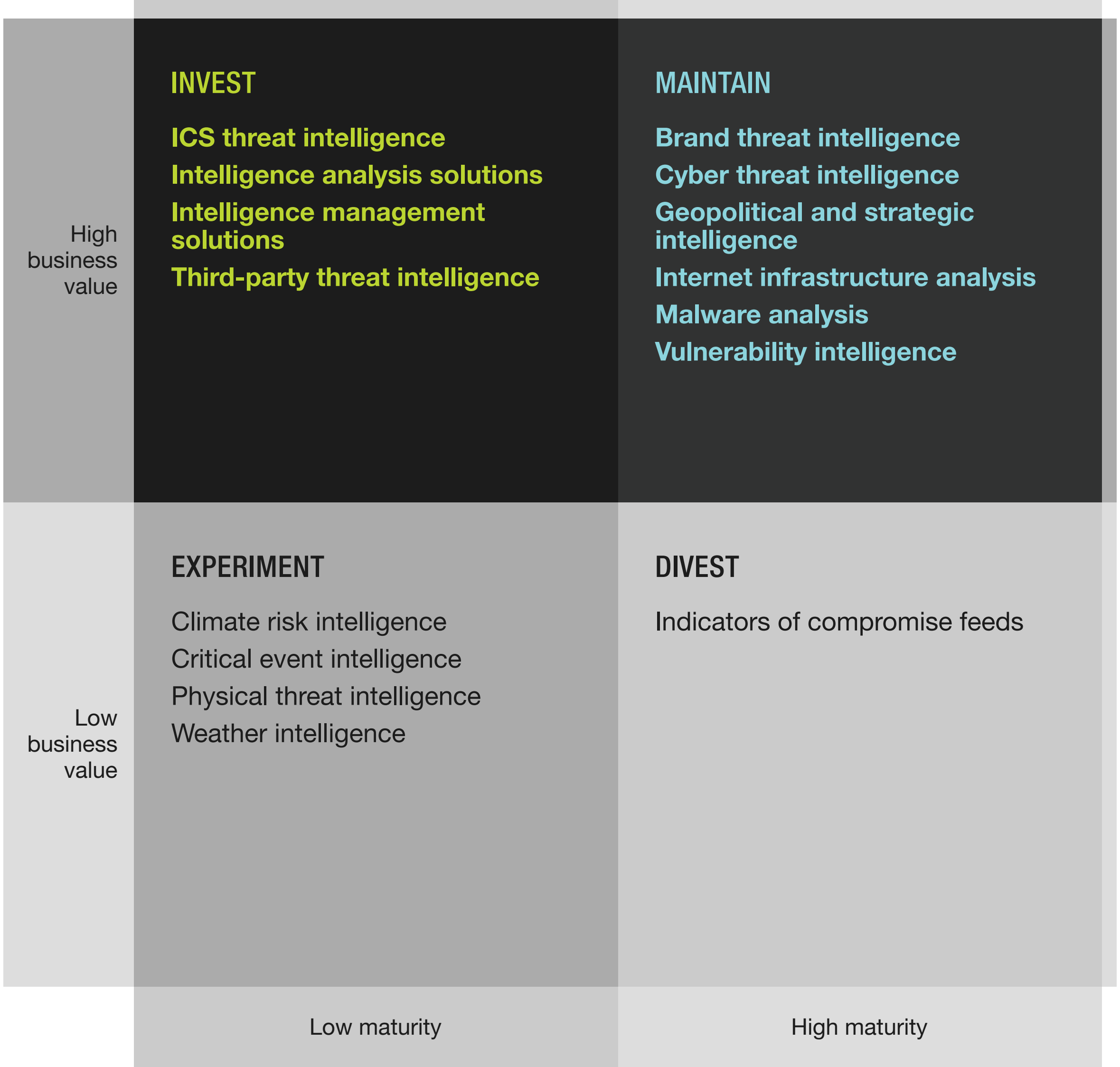
The central 2x2 graphic offers a summary of the state of the technology categories that make up threat intelligence (see Figure 1).

FIGURE 1 Tech Tide™: Threat Intelligence, Q2 2021

TECH TIDE

Threat Intelligence

Q2 2021



	Low maturity	High maturity
High business value	**INVEST** ICS threat intelligence Intelligence analysis solutions Intelligence management solutions Third-party threat intelligence	**MAINTAIN** Brand threat intelligence Cyber threat intelligence Geopolitical and strategic intelligence Internet infrastructure analysis Malware analysis Vulnerability intelligence
Low business value	**EXPERIMENT** Climate risk intelligence Critical event intelligence Physical threat intelligence Weather intelligence	**DIVEST** Indicators of compromise feeds

Evaluate Business Value And Maturity For Each Threat Intelligence Technology And Service

We plot the categories on two dimensions:

- **Business value.** This translates to the estimated return on investment for the threat intelligence capability over the whole lifetime of the technology. We evaluated business value for threat intelligence technologies and services based on: 1) how successful the technology will be over its lifetime; 2) how the technology reduces business risk across tactical, operational, and strategic interests; and 3) the ability to improve intelligence capabilities without having to hire additional staff.
- **Maturity.** We derived the maturity for each threat intelligence product by evaluating inputs such as the rate of product innovation, the type of vendors that are dominant in each market, enterprise adoption, and our own knowledge and understanding of the intelligence types and use cases.

Determine Strategies For Threat Intelligence Based On Business Value And Maturity

The business value and maturity dimensions, in turn, position each category in one of four quadrants:

- **Experiment.** Low maturity and low business value characterize technologies in the Experiment zone. Most enterprises should limit their exposure to these technologies to bounded experiments, waiting for the expected business value of these newer categories to improve before investing.
- **Invest.** Low maturity and high business value characterize technologies in the Invest zone. These new technologies have ripened to the point where enterprises can confidently invest.
- **Maintain.** High maturity and high business value characterize technologies in the Maintain zone. These are the bread-and-butter technologies that most enterprises rely on to run their business. They're generally stable, well-understood technologies that continue to have high returns to the business. Most enterprises should maintain their installations and usage of these technologies.
- **Divest.** High maturity and low business value characterize technologies in the Divest zone. These older technology categories have reached a point where their business value has dropped. Most enterprises should be looking for newer, higher-value replacements and divesting from these categories.

Invest In And Maintain Threat Intelligence Technologies With High Business Value

In mapping the futures of the technologies and services in the threat intelligence ecosystem, we found that:

- **New intelligence categories are emerging to help evaluate new threats such as physical security.** Traditionally, organizations would have to rely on weather reports to get weather intelligence, newspapers for geopolitical intelligence, and security cameras for physical intelligence.

Emerging capabilities in climate risk intelligence, critical event intelligence, physical threat intelligence, and weather intelligence allow organizations to get tailored data and insights for their specific location and unique circumstances.

- **Multiple threat intelligence services are required to address different types of threats.** It's rarely the case that one size fits all in terms of threat intelligence technologies and services. While many organizations would love a single pane of glass from which to view their entire threat landscape, the reality is organizations are investing in an arsenal of products to account for each unique type of risk. For example, a vendor that excels in the critical event intelligence capability may not have capabilities as strong in malware analysis and vice versa.
- **IOC feeds should be features of more valuable intelligence services.** Standalone IOC feeds lack the context needed to make better tactical security decisions. Many security control vendors include IOC feeds as part of their threat detection capabilities.

Experiment With Climate Risk Intelligence And Others

Four of the threat intelligence technologies fall into the Experiment quadrant of the Tech Tide, with low maturity and low current business value. We see the possibility for each tech category to reach higher maturity levels and a larger range of business value but without a guarantee for future success. Forrester predicts that many of these experimental threat intelligence products may be pulled into bigger integrated solutions.

Climate Risk Intelligence

Enterprises and public organizations alike use climate risk intelligence technologies to assess their unique exposure to the impacts of climate change. These solutions use spatial, socioeconomic, financial, and climate data to inform users of future climate hazards that threaten to disrupt their business across their supply chains, partners, and assets. As the climate crisis accelerates, these solutions will become critical for climate risk management (see Figure 2).

FIGURE 2 Experiment: Climate Risk Intelligence

Strategy:
EXPERIMENT

MATURITY
↓ Low

BUSINESS VALUE
↓ Low

LIFECYCLE COST
$$$

SAMPLE VENDORS
ClimateAI; The Climate Service; Jupiter Intelligence; One Concern; Senscity; XDI Systems

Climate risk intelligence

Definition
Climate risk intelligence services use advanced analysis methods such as predictive analytics and scientific modeling to assess and anticipate climate-related risks and opportunities under different scenarios. Common features include hazard impact analysis, vulnerability assessments, and climate risk scores.

Maturity rationale
Vendors in this space are emerging and primarily focused on financial services. Enterprise adoption outside of the finance vertical will increase as awareness of climate change risks grows.

Business value rationale
These solutions help business and government leaders adapt and build resilience to the chronic and acute physical risks associated with climate change. They will increasingly add value for short- and long-term strategic planning relating to ongoing climate change.

Critical Event Intelligence

Organizations in nearly every industry can benefit from critical event intelligence to help mitigate supply chain risk, contribute to business continuity and crisis response efforts, and protect employees' and customers' physical safety. In the current pandemic, critical event intelligence has gained new use cases in detecting COVID-19 hotspots (see Figure 3).

FIGURE 3 Experiment: Critical Event Intelligence

Strategy:
EXPERIMENT

MATURITY
↓ Low

BUSINESS VALUE
↓ Low

LIFECYCLE COST
**$**$$

SAMPLE VENDORS
AlertMedia; Babel Street; Dataminr; DigitalStakeout; Echosec Systems; Geospark Analytics; OnSolve

Critical event intelligence

Definition
Critical event intelligence utilizes real-time data from sources such as social media, blogs, news feeds, online forums, IP addresses, latitude and longitude, and device GPS to assess potential threats from location-specific events, especially for physical risk.

Maturity rationale
Prior to COVID-19, critical event intelligence was primarily used for physical safety and risk mitigation in areas such as public safety, military and defense, and corporate security. The pandemic has accelerated the use case of critical event intelligence in areas such as contact tracing and real-time crowd intelligence.

Business value rationale
Global events can affect the safety and security of your people, locations, and operations. Organizations unaware of critical events can suffer significant financial losses and unaddressed risks to their employees and customers. Critical event intelligence helps security teams reduce risk from unforeseen events.

Physical Threat Intelligence

Organizations subscribe to physical threat intelligence services to monitor closed and open internet sources for threats targeting executives, employees, or physical assets. Threats include criminal and terrorist activity as well as the loss of physical data. Mitigating physical threat incidents improves business resiliency, employee productivity, and brand reputation (see Figure 4).

FIGURE 4 Experiment: Physical Threat Intelligence

Strategy:
EXPERIMENT

MATURITY
↓ Low

BUSINESS VALUE
↓ Low

LIFECYCLE COST
$$$

SAMPLE VENDORS
Armored Things; Babel Street; Echosec Systems; Everbridge; Flashpoint; Geospark Analytics; OnSolve; Ontic; Proofpoint; RiskIQ

Physical threat intelligence

Definition
Physical security services monitor open and closed internet channels for indications and warnings of threats targeting an organization's people (including VIPs) and physical locations. Threats monitored include malicious insiders, violent extremists, criminals, and terrorists.

Maturity rationale
Deriving complete, accurate, relevant, and timely indicators of threats to your people and assets is extremely difficult. Detecting and understanding a potential threat's intent and objectives toward their targets is still a highly human-driven (and expensive) service.

Business value rationale
As social media and underground forums are used to overtly and covertly plan and coordinate physical attacks, it is becoming more necessary for corporate security teams to leverage physical threat intelligence to protect an organization's locations and people.

Weather Intelligence

Improvements in data analytics, internet of things (IoT), and satellite technology have contributed to enhancing the rigor of the intelligence that is collected compared to traditional weather forecasting. The efficiency of collecting insights from weather data helps organizations make business risk decisions, plan for extreme weather events, and improve business continuity (see Figure 5).

FIGURE 5 Experiment: Weather Intelligence

Strategy:
EXPERIMENT

MATURITY
↓ Low

BUSINESS VALUE
↓ Low

LIFECYCLE COST
$$$

SAMPLE VENDORS
Baron; ClimaCell; DisasterAWARE Enterprise; Earth Networks; IBM The Weather Company

Weather intelligence

Definition
Weather intelligence services deliver forward-looking data and real-time insights from sensors, satellites, drones, and other sources to help organizations plan and make operational decisions based on weather and climate.

Maturity rationale
Mature weather forecasting firms compete with an emerging class of vendors that use advanced analytics to improve the accuracy and efficiency of their models.

Business value rationale
These add significant business value to organizations in weather-sensitive industries, such as insurance, energy, and agriculture, and will grow in importance as climate change fuels the severity of extreme weather events and weather variability.

Invest In ICS Threat Intelligence And Others

Four of the threat intelligence technologies fall into the Invest quadrant of the Tech Tide, with low maturity and high current business value. When evaluating technologies in this category, keep in mind that they offer value now but should have bold innovation roadmaps to increase capabilities and interoperability.

ICS Threat Intelligence

Organizations in the manufacturing, utilities, energy, and transportation industries use ICS threat intelligence capabilities to protect physical and digital assets, find indicators of compromise (IOCs), learn about emerging ICS threats, ensure safety, and prevent unplanned shutdowns. As threats increasingly target and affect industrial processes, CISOs will better manage risk to their firm's core business with products designed for these environments (see Figure 6).

FIGURE 6 Invest: ICS Threat Intelligence

Strategy:
INVEST

MATURITY
↓ Low

BUSINESS VALUE
↑ High

LIFECYCLE COST
$$$

SAMPLE VENDORS
Dragos; FireEye; Kaspersky

ICS threat intelligence

Definition
Industrial control system (ICS) threat intelligence services provide tactical, operational, or strategic threat intelligence regarding cyberthreats that attack industrial controls systems in operational technology (OT) environments.

Maturity rationale
ICS security (and the analysis of OT-specific threats) is a rapidly maturing area of cybersecurity. As visibility improves in OT environments, our knowledge of OT cyberthreats increases, making this threat intelligence very valuable for firms in heavy industries such as manufacturing, logistics, and utilities.

Business value rationale
As more and more industrial control systems automate our businesses, the threats to industrial automation continue to multiply with potential to cause financial and physical risks to any organizations utilizing ICS systems.

Intelligence Analysis Solutions

Intelligence analysis solutions make visualizations using raw threat data to help evaluate risks. Use cases include geopolitical intelligence, antifraud, cyberthreats, criminal intelligence, and social media. Intelligence analysts at companies that belong to industries ranging from high-tech to finance and professional services use these solutions to contextualize and prioritize business risks (see Figure 7).

FIGURE 7 Invest: Intelligence Analysis Solutions

Strategy:
INVEST

MATURITY
↓ Low

BUSINESS VALUE
↑ High

LIFECYCLE COST
$$$

SAMPLE VENDORS
Cambridge Intelligence; IBM i2 Analyst's Notebook; Linkurious; Maltego; Palantir; Siren; Visallo

Intelligence analysis solutions

Definition
Intelligence analysts use link analysis and visualization solutions to turn cybersecurity, social network, geospatial, and temporal data into intelligence. Clients use these solutions to analyze cyberthreat, criminal, fraud, and physical threats.

Maturity rationale
Solutions in this category are evolving from the traditional law enforcement, counterterrorism, and counterinsurgency missions to support cybersecurity use cases. These solutions should soon be able to scale effectively for analysts to visualize exceptionally large security data sets to begin automatically clustering activities by threat group.

Business value rationale
Intelligence analysis solutions help analysts present security data in a manner that tells a story to a stakeholder. They also help analysts see patterns and linkages between data that are not possible with spreadsheets or databases.

Intelligence Management Solutions

Security professionals can become overwhelmed with the amount of data and alerts they receive. Intelligence management solutions provide processes for intelligence professionals to manage stakeholder requirements, automate intelligence collection, maximize data analysis, and operationalize the intelligence (see Figure 8).

FIGURE 8 Invest: Intelligence Management Solutions

Strategy:
INVEST

MATURITY
↓ Low

BUSINESS VALUE
↑ High

LIFECYCLE COST
$$$

SAMPLE VENDORS
Analyst Platform; Anomali; Cyware; D3 Intelligence; EclecticIQ; Elemendar; King & Union; LookingGlass Cyber Solutions; Polarity; ThreatConnect; ThreatQuotient; TruSTAR

Intelligence management solutions

Definition
Intelligence teams use these solutions to aggregate, process, and disseminate raw and finished intelligence products. These solutions may also manage intelligence requirements and help orchestrate and automate intelligence workflows.

Maturity rationale
The intelligence management solutions currently support only a minority of steps in the intelligence cycle. Most solutions here aggregate data collected by other sources, perform some processing and deduplication, and then disseminate that technical and tactical security information to other security controls.

Business value rationale
While intelligence analysts can begin aggregating data in spreadsheets for free, they will quickly find those solutions limiting. Management solutions relieve analysts from manually entering new reports and raw data. They also help make that data available to other stakeholders and security controls.

Third-Party Threat Intelligence

Organizations use third-party threat intelligence to continually monitor their partners, vendors, and suppliers to detect breaches, domain and social media spoofing, and other threats. Common use cases include vendor management, regulatory compliance, and business continuity (see Figure 9).

FIGURE 9 Invest: Third-Party Threat Intelligence

Strategy:
INVEST

MATURITY
↓ Low

BUSINESS VALUE
↑ High

LIFECYCLE COST
$$$

SAMPLE VENDORS
BitSight; Panorays; Recorded Future; Risk Based Security; RiskIQ; RiskRecon; SecurityScorecard

Third-party threat intelligence

Definition
Third-party threat intelligence vendors enrich internal assessment data with information from external sources to help clients reduce risk from compromised vendors, suppliers, partners, and software libraries. They enhance due diligence in the areas of financial viability, cybersecurity posture, regulatory changes, geopolitical risk, and others.

Maturity rationale
This is a somewhat mature market with many established vendors as well as new entrants. The wave of new regulations, evolving compliance requirements, new and emerging risks, and vulnerabilities surrounding the third-party and supply chain ecosystem will continue to sustain this market.

Business value rationale
Security pros rely on these technologies to continuously monitor for risk events in real time, add multidimensional context for decision-making, and respond to regulatory mandates.

Maintain Brand Threat Intelligence And Others

Six of the threat intelligence technologies fall into the Maintain quadrant of the Tech Tide, with high maturity and high current business value. These are core threat intelligence technologies that continue to evolve to help detect reputational threats, track cyberthreats, and improve decision-making in the cybersecurity organization. When evaluating technologies in this category, keep in mind that they offer value now; review other options first, especially in the Invest or Experiment quadrants, and invest when there is a clear gap.

Brand Threat Intelligence

Every organization, from global Fortune 100 names to small businesses, are concerned with protecting their brand and reputation. Brand threat intelligence scrapes social media, the web, closed forums, and other sources to find instances of disinformation, impersonation, or exposure of brand assets. Common use cases include takedowns of fake accounts and credentials exposed on the dark web (see Figure 10).

FIGURE 10 Maintain: Brand Threat Intelligence

Strategy:
MAINTAIN

MATURITY
↑ High

BUSINESS VALUE
↑ High

LIFECYCLE COST
$$$

SAMPLE VENDORS
Blackbird.AI; Cybersprint; Digital Shadows; FireEye; Flashpoint; Intel 471; IntSights; PhishLabs; Proofpoint; Recorded Future; RiskIQ; Secureworks; Sixgill; ZeroFOX

Brand threat intelligence

Definition
Brand threat intelligence services collect and analyze data from a range of digital channels, including social, mobile, and web sources. Vendors in this space deal with exposure of digital assets, accounts, and disinformation online, offering quick detection and remediation.

Maturity rationale
This market is relatively new, as the digital channels where disinformation spreads online is constantly growing, but it is applicable for every organization. Most large players in the threat intelligence space offer these services, but there are also some smaller niche players whose sole focus is brand and reputation.

Business value rationale
All organizations, regardless of size and vertical, need to protect their reputation. Misinformation, disinformation, counterfeiting, brand impersonation, and more negatively influence a brand's reputation. Brands must keep their trademarks out of risky areas of the internet to build and retain customer trust and preserve brand value.

Cyber Threat Intelligence

Stakeholders across the organization utilize cyber threat intelligence to track threat actors and their campaigns. Intelligence from these vendors helps clients build more-resilient security architectures and reduce the frequency and impact of intrusions. Client organizations are members of nearly every industry, including financial services, retail, consumer packaged goods, public and governmental organizations, transportation, utilities, and more (see Figure 11).

FIGURE 11 Maintain: Cyber Threat Intelligence

Strategy:
MAINTAIN

MATURITY
↑ High

BUSINESS VALUE
↑ High

LIFECYCLE COST
$$$

SAMPLE VENDORS
CrowdStrike; Digital Shadows; DomainTools; ESET; FireEye; Flashpoint; Group-IB; IBM; IntSights; Intel 471; Kaspersky; Recorded Future; RiskIQ; Secureworks; ZeroFOX

Cyber threat intelligence

Definition
Cyber threat intelligence services provide tactical, operational, and strategic all-source intelligence on cyberthreats (including state-sponsored, criminal, hacktivist groups) and their activities and campaigns to drive security and business decisions.

Maturity rationale
Cyber threat intelligence is a developed market; most enterprises now subscribe to multiple intelligence services. There continues to be innovation in the category, and many vendors are expanding the types of threat intelligence (e.g., third parties, vulnerabilities, brands) they provide to clients to help improve security decision-making.

Business value rationale
Cyber threat intelligence is important for stakeholders across the organization including those working in the SOC, security engineering, security architects, as well as CISOs. Finished cyber threat intelligence reports answer intelligence requirements, which ultimately drives better security and business decisions.

Geopolitical And Strategic Intelligence

Geopolitical and macroeconomic events, fluctuations, and trends often drive the actions of criminal and state-nexus threat actors. Reduce risk to your organization by monitoring the global threat landscape and incorporating strategic threat intelligence into long-term planning at the board and C-suite levels (see Figure 12).

FIGURE 12 Maintain: Geopolitical And Strategic Intelligence

Strategy:
MAINTAIN

MATURITY
↑ High

BUSINESS VALUE
↑ High

LIFECYCLE COST
$$$

SAMPLE VENDORS
Economist Intelligence Unit; Emergent Risk International; Recorded Future; The Soufan Group; Stratfor; Wikistrat

Geopolitical and strategic intelligence

Definition
Geopolitical intelligence services produce global security and risk forecasts and insights into geopolitical events and macroeconomic indicators to drive long-term and strategic decision-making.

Maturity rationale
While geopolitical intelligence is a mature market, the players and the threat landscape are constantly changing. This type of intelligence is also often supplemented by government or industry sources.

Business value rationale
Firms with global operations now face exposure to geopolitical risks. These tools and services can help security professionals protect their operations abroad. Additionally, understanding the long-term goals of criminal, activist, and state-sponsored adversaries helps security leaders make long-term risk management decisions.

Internet Infrastructure Analysis

Intelligence analysts use internet infrastructure analysis, which provides technical intelligence, to analyze and hunt for threats. Common use cases include proactive monitoring, identifying exposed or vulnerable assets, DNS analytics, and protecting against phishing and DDoS attacks (see Figure 13).

FIGURE 13 Maintain: Internet Infrastructure Analysis

Strategy:
MAINTAIN

MATURITY
↑ High

BUSINESS VALUE
↑ High

LIFECYCLE COST
**$**$$

SAMPLE VENDORS
Censys; DomainTools; Farsight Security; GreyNoise Intelligence; RiskIQ; Team Cymru

Internet infrastructure analysis

Definition
Internet infrastructure analysis services provide access to metadata of IP addresses, domains, encryption certificates, registration information, and more and are used by threat intelligence analysts and hunters to analyze and hunt for potentially malicious internet infrastructure.

Maturity rationale
Vendors that scan for cyberthreat infrastructure have mature solutions to observe changes to infrastructure in near real time and to make that data available to threat hunters and intelligence analysts.

Business value rationale
Cyberthreats can abuse legitimate administration solutions, but they must maintain their own infrastructure to command and control their malware and implants. Intelligence analysts can spot indications of emerging threat activity by monitoring for new threat infrastructure.

Malware Analysis

Intelligence analysts use malware analysis, which provides technical intelligence, to analyze and hunt for malware such as malicious code. Common use cases include detecting malware, discovering indicators of compromise (IOCs), research, and incident response (see Figure 14).

FIGURE 14 Maintain: Malware Analysis

Strategy:
MAINTAIN

MATURITY
↑ High

BUSINESS VALUE
↑ High

LIFECYCLE COST
**$**$$

SAMPLE VENDORS
ANY.RUN; Broadcom; Cisco; Comodo; CrowdStrike; Cyren; FireEye; Forcepoint; Intezer; Joe Sandbox; McAfee; OPSWAT; Palo Alto Networks; ReversingLabs; VirusTotal; VMRay; Webroot

Malware analysis

Definition
Malware analysis services are used by threat intelligence analysts and threat hunters to analyze suspicious files and hunt for new malicious code, documents, programs, and scripts.

Maturity rationale
Enterprises often have multiple malware analysis capabilities built in throughout their security stack through solutions such as email security gateways and antivirus. However, there continues to be innovations in malware analysis, and many enterprises add an additional layer of malware analysis for hunting purposes.

Business value rationale
Cyberthreats are constantly innovating to evade detections. Malware analysis solutions help add depth to an enterprise's security stack and provide additional context about malware. These solutions can help intelligence analysts cluster threat activity via greater knowledge of malware.

Vulnerability Intelligence

Vulnerability intelligence is critical to lower the risk of vulnerability exploitation and reduce the frequency of unplanned maintenance and interruptions of business processes. The sheer volume of vulnerabilities (18,000 in 2020) is too much for any enterprise to handle, and CVSS scores lead to poor prioritization. The best services here fuse security telemetry, malware analysis, underground criminal communications, and more to go beyond CVSS and narrow the number of vulnerabilities that security and risk pros should focus on (see Figure 15).

FIGURE 15 Maintain: Vulnerability Intelligence

Strategy:
MAINTAIN

MATURITY
↑ High

BUSINESS VALUE
↑ High

LIFECYCLE COST
$$$

SAMPLE VENDORS
FireEye; Flashpoint; Kenna Security; Recorded Future; Risk Based Security; Snyk

Vulnerability intelligence

Definition
Vulnerability intelligence services monitor the cyberthreat environment for vulnerability exploits to help organizations prioritize vulnerability remediation.

Maturity rationale
Specialty vendors and pure threat intelligence vendors began creating specific analytics around vulnerability exploitation several years ago. These vendors can now provide the insights needed to transform vulnerability management analysts into risk advisors — saving countless hours of productivity while reducing the risk of vulnerability exploitation.

Business value rationale
The greatest challenge for vulnerability risk management teams is advising their organization's asset owners how to prioritize vulnerability remediation. Vulnerability intelligence is a crucial component in helping manage the business calculus of determining which production systems to take offline for security patching.

Divest From IOC Feeds

One of the threat intelligence technologies fall into the Divest quadrant of the Tech Tide, with high maturity and low current business value. When evaluating technologies in this category, keep in mind that they have already reached their business value ceiling, review alternatives first, and invest only if there is a critical threat intelligence need.

Indicators Of Compromise Feeds

Indicators of compromise (IOC) feeds provide a list of capabilities that are used in malicious activity and attacks. We classified IOC feeds in Divest, as these solutions are increasingly being built into other enterprise security controls such as enterprise firewalls, endpoint detection and response, and security analytics platforms. Common use cases for IOC feeds include asset inventory, prioritization, threat detection, and mitigating data loss (see Figure 16).

FIGURE 16 Divest: Indicator Of Compromise Feeds

Strategy:
DIVEST

MATURITY
↑ High

BUSINESS VALUE
↓ Low

LIFECYCLE COST
$$$

SAMPLE VENDORS
AT&T; Bad Packets; Cyren; ESET; IBM; Infoblox; Neustar; OPSWAT; Proofpoint; Recorded Future; Secureworks; Spamhaus; Team Cymru; Webroot

Indicators of compromise feeds

Definition
Indicators of compromise (IOC) feeds provide lists of IOCs (infrastructure and capabilities used in intrusions and attacks) for use to block, detect, or search for additional malicious activities.

Maturity rationale
IOC feeds have existed for a long time in security and are increasingly built into network, cloud, and endpoint security controls.

Business value rationale
IOCs tend to have short lifespans as threats shift infrastructure and capabilities frequently. IOC detection has a lower signal-to-noise ratio than behavioral detection. And to detect or prevent threat activity based on IOC detections, vendors must prioritize speed over accuracy and completeness, leading to lower-value raw intelligence.

Supplemental Material

Methodology

The purpose of the lists of sample vendors we include in the figures about each category is to further clarify the nature of the category — not to serve as a vendor selection shortlist for readers seeking to choose a vendor in that category. The fact that a vendor isn't included in a list does not indicate that Forrester believes it isn't worth considering. For guidance about vendor selection, Forrester publishes separate research (Now Tech and Forrester Wave™ reports) in which Forrester analysts offer customized advice to our clients.

We help business and technology leaders use customer obsession to accelerate growth.

PRODUCTS AND SERVICES

- › Research and tools
- › Analyst engagement
- › Data and analytics
- › Peer collaboration
- › Consulting
- › Events
- › Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO

B2B Marketing

B2C Marketing

Customer Experience

Customer Insights

eBusiness & Channel Strategy

Technology Management Professionals

CIO

Application Development & Delivery

Enterprise Architecture

Infrastructure & Operations

● Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.