How To Integrate Threat Intelligence Into Your Security Program

Reducing Risk And Uncertainty To Your Organization With Threat Intelligence

by Brian Kime

January 15, 2021

Why Read This Report

An effective security architecture requires insights into your organization's threat landscape, but many S&R professionals are disappointed in the results of their threat intelligence efforts. This report offers examples of intelligence products and processes for each level of intelligence and how S&R pros can integrate those outputs into the SOC, incident response (IR), engineering, architecture, budgeting, planning, and risk management functions to reduce overall cyber risks and help develop an effective intelligence-driven security strategy.

Key Takeaways

Strategic Decision-Makers Need To Consume Threat Intelligence

To help drive the compelling cyber risk management processes, business leaders need strategic threat intelligence. Recent high-profile data breaches such as Equifax have demonstrated how the lack of strategic cyber risk management at the board and C-suite levels can cause real long-lasting harm to the businesses, customers, and employees.

Use Internal Security Telemetry First

Successful threat intelligence programs prioritize collection and analysis of their business's internal security telemetry. Procuring more external threat intelligence does not always lead to increased cybersecurity and privacy maturity.

Measure Effectiveness, Not Performance

Metrics that drive improved decision-making and help build greater resilience against cyberthreats are superior to performance metrics about the number of indicators of compromise collected by the threat intelligence team.

How To Integrate Threat Intelligence Into Your Security Program

Reducing Risk And Uncertainty To Your Organization With Threat Intelligence

by Brian Kime
with Merritt Maxim, Benjamin Corey, and Peggy Dostie

January 21, 2021

Table Of Contents

2 Cyber Threat Intelligence Is Immature

4 Align Threat Intelligence To Your Stakeholders

7 An Effective Program Supports Stakeholders Throughout The Firm

13 Use Metrics To Track Threat Intelligence Effectiveness

Recommendations

14 Start With Tactical, Progress To Operational And Strategic Intelligence

16 Supplemental Material

Related Research Documents

Five Dangerous Ways Social Media Is Exploited For Profit

Job Description: Director Of Threat Intelligence

Now Tech: External Threat Intelligence Services, Q4 2020

FORRESTER®

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

Cyber Threat Intelligence Is Immature

Of all the cybersecurity domains and specialties, cyber threat intelligence (CTI) is one of the newest and least understood by stakeholders. Threat intelligence is defined as assessing the intent, capabilities, and opportunities of threat actors in response to stakeholder requirements. Stakeholders use threat intelligence to inform business decisions and reduce risks, both physical ones and cyberthreats. However, there is a separation between decision-makers and intelligence producers that Matthew Olney, director at Cisco's Talos intelligence and interdiction team, consistently observes in his interactions with clients and partners.[1] Research at Carnegie Mellon has shown that lower performing threat intelligence capabilities tend to report to security operations centers (SOC), limiting the intelligence analysts to reactive tasks and support.[2]

Threat Intelligence Capabilities Are Some Of The Least Supported In Cybersecurity

The SANS Institute's 2020 Cyber Threat Intelligence (CTI) Survey shows that less than half of organizations have a dedicated threat intelligence team.[3] Additionally, Carnegie Mellon's research shows that high-performing security organizations have the personnel to support their threat intelligence needs.[4] Organizations that just add threat intelligence responsibilities onto existing security staff generally struggle to derive substantial value from that staffing strategy.

Vendors And Internal Teams Struggle To Elicit Intelligence Requirements

In addition to threat intelligence being poorly understood by business leaders, many organizations have immature processes around their organization's intelligence requirements. For example, less than half of respondents to the SANS CTI Survey reported they had documented intelligence requirements. While that number increased significantly from 2019, the lack of a process to elicit and refine intelligence requirements is a major factor inhibiting the closure of the gap between stakeholders and intelligence teams. Furthermore, when SANS asked who contributed to the intelligence requirements, the top two results were tactical defenders, while senior risk managers and strategists in the boardroom and C-suite were at the bottom of the results.[5]

Immature Intelligence Tooling

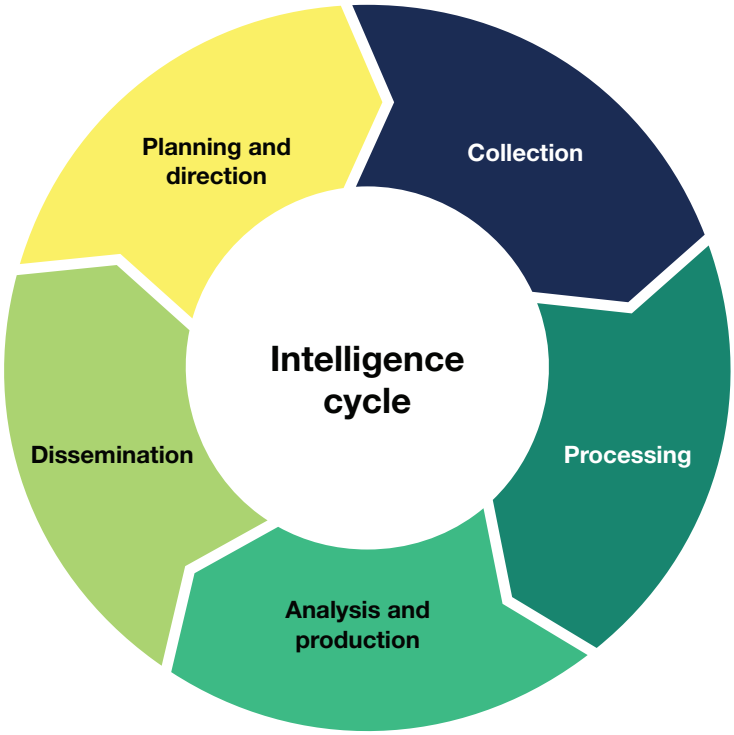
Organizations should always prioritize people and process over tools. Poor tools can hold back a well-trained team. The SANS CTI Survey shows that non-CTI specific (e.g., SIEM, email, and spreadsheets) and free open source tooling remain the most commonly used tools to manage threat intelligence information.[6] Spreadsheets, while useful for many business tasks, are not conducive to automation. Email is a poor database for deriving insights out of information. Not using automation to handle many of the low-risk, repeatable tasks like moving data between systems only hampers your threat intelligence efforts.

To integrate a robust threat intelligence capability that helps all levels of stakeholders manage cyber risk, follow the intelligence cycle (see Figure 1):

- **Planning and direction.** This stage is most frequently overlooked by stakeholders and intelligence teams. Often, one stakeholder decides the organization threat intelligence needs and goes immediately to vendor selection. Organizations should start first by identifying threat intelligence stakeholders throughout the enterprise — within the security team and elsewhere in the organization. Whoever is responsible for providing intelligence needs to elicit intelligence requirements from each stakeholder. Once requirements are defined, the intelligence capability can create a collection plan (which should always exhaust all internal data sources before going to external sources) and an intelligence architecture to enable teams to quickly complete the full cycle.
- **Collection.** Once a team has a raw intelligence collection plan, they can begin acquiring data. Much of the internal data needed should already be available. This raw intelligence data overlaps with the data a SOC needs but often includes security events (e.g., blocked phishing emails, firewall blocks) that don't get escalated to a SOC threat analyst. Getting the right security telemetry into a threat intelligence platform is crucial. But remember, internal security telemetry is already paid for and is high fidelity. Exercise due diligence for the gaps in your collection plan that require placement and access to sources outside your network that you don't control. Regularly evaluate open source feeds for accuracy and timeliness. Outsource human intelligence collection in criminal forums and communities to vendors who specialize in that due to the resources and risks involved.
- **Processing.** Before human intelligence analysts can derive an assessment of a threat or automatically feed IOCs into a security control or analytics platform, raw intelligence information needs processing. The intelligence systems should extract and collate technical details. Timestamps should be normalized, ideally to UTC. Lastly, the system should automatically apply threat intelligence frameworks like the Diamond Model of Intrusion Analysis, a kill chain (e.g., Lockheed Martin's or the two-stage ICS Kill Chain), and MITRE's ATT&CK framework.[7]
- **Analysis and production.** This stage is where raw intelligence is evaluated and synthesized into finished intelligence that answers stakeholder requirements. Intelligence analysts use various techniques or tradecraft to detail the who, what, when, where, why, and how of threats. Vendors and internal intelligence teams model known and emerging threats to help stakeholders reduce risk to the organization. Critical thinking and controlling for biases are important skills to produce accurate intelligence.
- **Dissemination.** Intelligence that never makes it to a stakeholder has no value. Dissemination of intelligence should use any medium or format the stakeholder requires such as STIX, CSVs, PDFs, phone calls, or deskside briefs. Use automation when appropriate to disseminate intelligence to human stakeholders and security controls. Some stakeholders, like executives, may prefer briefings. Don't forget, the information on a slide or received via an API integration is likely only a fraction of what the analyst knows about the threats.

- **Feedback.** While not a stage within the cycle, feedback is critical throughout the process. Feedback can be collected automatically (e.g., script or API failures, report viewership, surveys) or via informal mechanisms like interviews or focus groups. Feedback is used to refine intelligence requirements, improve the collection plan, upgrade the intelligence architecture, enhance analytical tradecraft, expand dissemination, and more.

FIGURE 1 The Threat Intelligence Cycle



Align Threat Intelligence To Your Stakeholders

Not all threat intelligence is relevant to every stakeholder. Some threat intelligence stakeholders lack the skills or access to put IOCs to work. At the same time, there is little a SOC threat analyst could do with a strategic forecast to address the new vulnerability scan alert on their screen. Integrating threat intelligence throughout a security program is much more than addressing one or two intelligence use cases.

The Three Levels Of Threat Intelligence

The construct of tactical, operational, and strategic levels of threat intelligence helps stakeholders and producers visualize the flow of intelligence from one level to another. The levels of intelligence are related to organizational hierarchy — strategic leaders like the C-suite and board of directors

are strategic threat intelligence stakeholders. This construct supports stakeholder identification, intelligence production, and allocation of intelligence resources. The levels of intelligence are defined as follows:

- **Tactical.** Security professionals at the tactical level are involved in the daily struggle to protect the organization's assets. SOC threat analysts triage new alerts from the organization's various security controls. Incident responders contain and eradicate threats so that the organization can quickly recover from a data breach or attack. Tactical threat intelligence helps the SOC threat analysts completely and quickly triage security events. It also helps incident responders focus their investigation and reduce adversary dwell time and mean-time-to-recovery.
- **Operational.** Security and risk professionals at the operational level are responsible for ensuring efficient allocation of information technology (IT) and operational technology (OT) systems and security controls and capabilities to maintain the confidentiality, integrity, availability of information, and the safety and reliability of industrial processes. Operational threat intelligence at this level includes indications that a threat is likely to attack the organization, trend analysis of the organization's threat landscape, assessments of the threat's tactics, techniques, procedures (e.g., MITRE ATT&CK techniques), and information that enables defenders to detect and stop threats before reaching their objectives.
- **Strategic.** Primarily used by the C-suite and board of directors, strategic threat intelligence helps those stakeholders align the organization's risk management program to assessments of likely threats. Based on an inventory of the organization's critical assets, the strategic threat intelligence function must evaluate which threats are likely to target the organization and why.[8] Threat intelligence must be included in the calculus so that strategic level decision-makers can understand the threats that may inhibit or prevent obtaining their strategic objectives.[9]

Effective Threat Intelligence Has Four Primary Qualities

In our research, we discovered that less mature organizations focus on "actionable" intelligence. This manifests itself in teams seeking to acquire as many IOCs as possible and pushing those into a security information and event management (SIEM) product for IOC detection purposes. In practice, this typically worsens the signal-to-noise ratio in the SOC. The bias toward actionability also forces intelligence producers to focus on serving tactical defenders at the expense of delivering good-quality intelligence to senior stakeholders whose decisions have a longer effect. A security practitioner at a global pharmaceutical company noted their threat intelligence counterparts at an acquired European company embodied the problem with actionable intelligence. By collecting as much external data to make those security controls as effective as possible, they predictably created many false-positive and low-value alerts in the security operations center. To reduce risk and uncertainty, S&R pros should seek to produce intelligence that meets these four qualities:

- **Completeness.** Good threat intelligence possesses all the necessary parts to provide the consumer what they need to take an appropriate action to reduce risk. For example, atomic indicators without context (e.g., a CSV with only a list of IP addresses) are incomplete and, generally, unhelpful for defenders.[10] Atomic and computed indicators become IOCs with added context (e.g., MITRE ATT&CK technique, first and last seen timestamps, behavior observed, etc.).[11]
- **Accuracy.** Threat intelligence must save organizations more in success than it costs them in wasted resources.[12] Inaccurate intelligence may lead to unfavorable signal-to-noise ratios in your SOC or placing security controls in the wrong location or with the wrong configuration. Tracking the number of false-positive alerts generated by poor threat intelligence in your SIEM is a good indicator of the accuracy of threat intelligence at the tactical level.
- **Relevance.** Threat intelligence must address a threat within that organization's landscape. For example, intelligence on threats to electric generation are irrelevant to a financial services organization at the tactical level. Strategically, though, a financial services organization should consider backup electric generation as part of its disaster recovery planning in the event of multiple, successful coordinated attacks on the electric grid. Additionally, intelligence delivered in a manner which is unusable (for example STIX files in an organization that uses a different standard) can do more harm than good.[13]
- **Timeliness.** Consumers must receive and operationalize intelligence fast enough to make an impact more valuable than the cost of the threat intelligence itself.[14] Delivering a warning of an attack after the attack has begun has little value.

Use Internal Security Telemetry First

Forrester Analytics survey data shows organizations use, on average, almost 18 external intelligence sources, a sizable increase from about 12 to 13 sources in 2019 (see Figure 2).[15] Despite procuring more threat intelligence, Forrester cybersecurity and privacy maturity assessment data shows a negligible improvement from 2019 to 2020 despite acquiring about one-half more of external threat intelligence sources.[16] SANS survey results show internal sources — that your organization has already paid for — are less valued than external, often paid, sources.[17] Internal data sources are free, more reliable and available, and tell you exactly what a threat is doing to your organization.

FIGURE 2 Organizations Are Overwhelmed With Threat Intelligence

"How many of each of the following does your organization currently subscribe to?"

Source type	Average number of sources
Commercial threat intelligence feeds that we pay for	6.31
Information sharing communities that we belong to	5.82
Open sources of threat intelligence and/or blocklists that are free	5.54

Base: 1,137 global security decision-makers with network, data center, app security, or security ops responsibilities who have seniority level of manager or above
Source: Forrester Analytics Business Technographics® Security Survey, 2020

An Effective Program Supports Stakeholders Throughout The Firm

Approximately only 10% of CISOs have military and law enforcement experience.[18] Businesses that recruited the core of their cybersecurity staff from those career fields have built out more-holistic threat intelligence teams, while businesses that built their security function from IT staff have smaller, less mature threat intelligence capabilities. For those enterprises that built their security and risk functions from staff within the CIO's organization, the focus of any threat intelligence capability skews heavily towards support to security operations and incident response. However, threat intelligence stakeholders span the entire organization from individual SOC threat analysts to the board of directors (see Figure 3 and see Figure 4). Contrary to what many technology leaders see as a technical data integration problem, threat intelligence products become less technical and increasingly forward-looking as the seniority of the stakeholder increases. A successful approach to threat intelligence must span tactical, operational, and strategic levels to help stakeholders best mitigate risk.

FIGURE 3 Functions Of A Fully Integrated Threat Intelligence Team

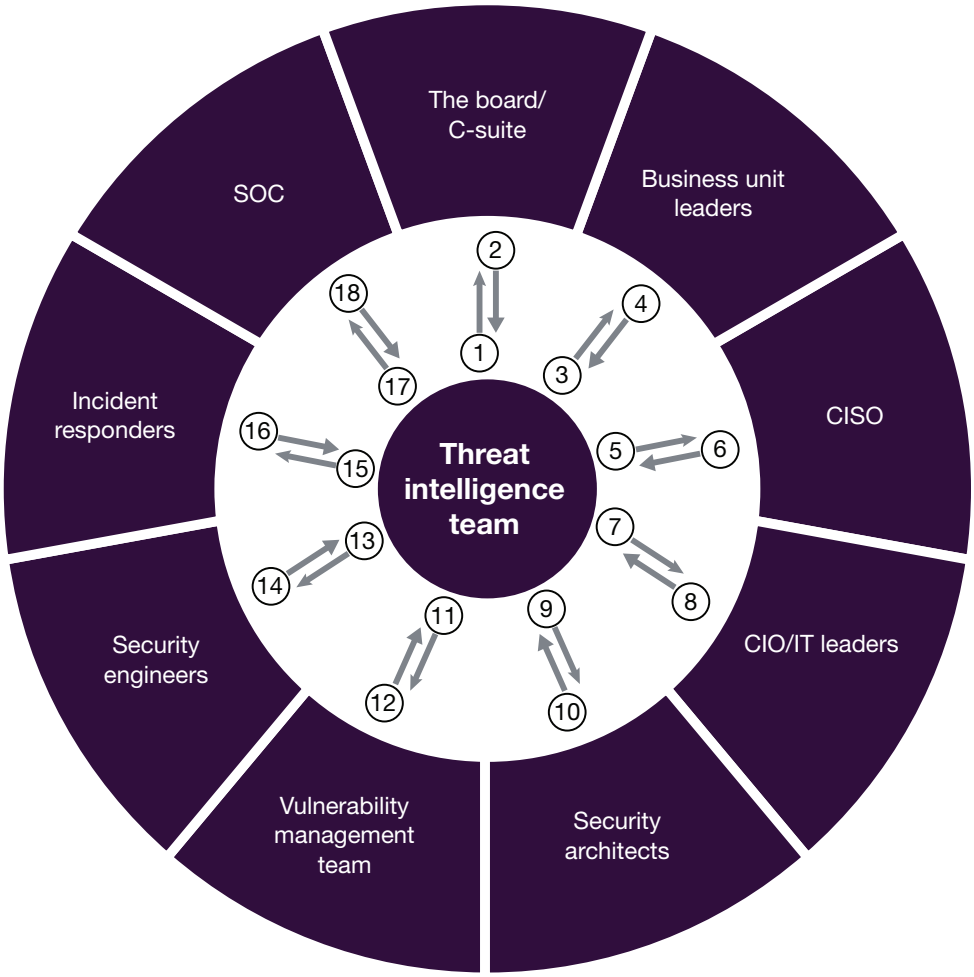


FIGURE 4 Threat Intelligence Teams Have Give-And-Take With Other Teams In The Organization

1	Strategic intelligence and forecasts	**10**	Security architectures, requirements, RFIs, feedback
2	Requirements, RFIs, corporate strategy, feedback	**11**	Vulnerability intelligence
3	Strategic intelligence and forecasts	**12**	Requirements, RFIs, feedback
4	Requirements, RFIs, business unit strategy and technology vendors, feedback	**13**	IOCs, threat models, detections
5	Threat landscape/models, campaigns, metrics	**14**	Metrics, RFIs, feedback
6	Requirements, RFIs, security and risk strategy, feedback	**15**	IOCs/historical threat activity
7	Threat landscape/models, metrics	**16**	Incident reports and forensic artifacts, RFIs, feedback
8	Requirements, RFIs, IT strategy, CMDB, network architectures, feedback	**17**	IOCs/historical threat activity
9	Threat models, campaign analysis	**18**	Resolved security events, RFIs, feedback

Integrating Threat Intelligence At The Tactical Level

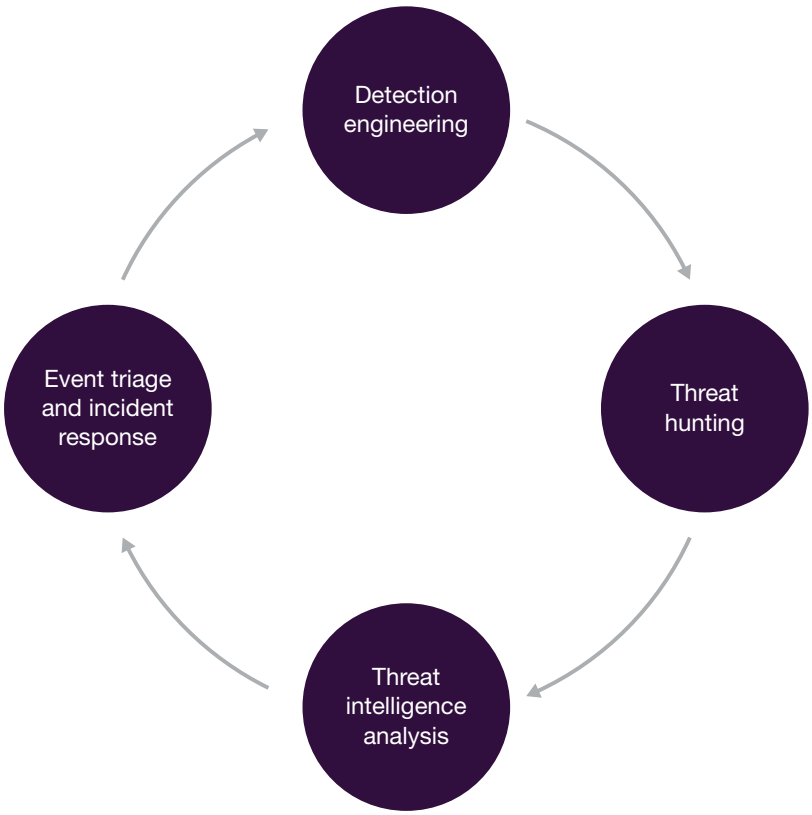
To help the organization secure its assets and information, tactical threat intelligence should focus on providing information to detect new threats, more completely and accurately triage new security alerts, and focus incident responders to quickly and completely contain and eradicate threats during a breach response. Use threat intelligence information from your internal threat library and vendors like DomainTools, GreyNoise, Recorded Future, and VirusTotal to enrich the information on a SOC threat analyst's screen.

Threat Intelligence Supports Threat Hunting

Additionally, to fully integrate threat intelligence at the tactical level, threat intelligence should drive threat hunting and detection engineering (see Figure 5). Threat hunting, to be clear, is not querying for IOCs from an intelligence report — that is historical IOC detection. Threat hunting should begin with a hypothesis based on an intelligence assessment: the who, what, where, when, why, and how of a threat actor. Threat hunters scour the organization's vast security logs to identify which controls and

logs can answer that hypothesis. Engineers create new, permanent detection rules and correlations once threat hunters have identified where they can detect a specific adversary. New detections will trigger new SOC alerts, and the intelligence team leverages that feedback to update threat models.

FIGURE 5 Threat Intelligence Integration At The Tactical Level



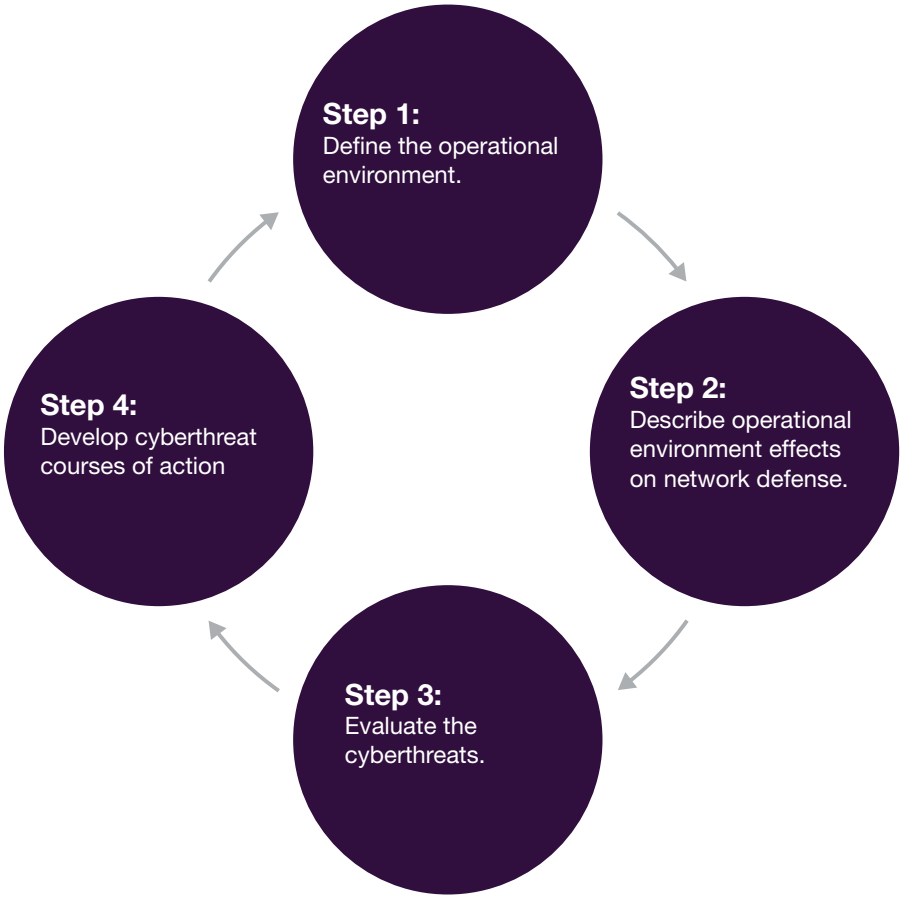
Integrating Threat Intelligence At The Operational Level

Intelligence activities at the operational level focus on serving the needs of CISOs and CIOs and their respective directors. This is the level of intelligence driving the design of security architectures against the threats known or likely to be targeting an organization. The more intelligence teams can inform CISOs and CIOs about threat objectives and capabilities the better they can posture their organization to be more resilient against state-affiliated or criminal threats.[19] Thus, the major goal of operational threat intelligence is gaining awareness of your organization's total threat landscape to optimize the allocation of those technology assets and security controls.

Use Intelligence Prep Of The Cyber Environment To Understand Your Threat Landscape

Intelligence teams can achieve and maintain awareness of an organization's threat landscape via a process like Intelligence Preparation of the Cyber Environment (IPCE) (see Figure 6). IPCE is a continuous process of analyzing an organization's potential threats to detect a pattern of activities that may indicate risks to the organization's processes, networks, information, employees, or customers. IPCE provides a means of visualizing and analyzing internal security telemetry and closed and open source information to infer likely threat courses of action. The outputs of IPCE support the organization's risk management strategy and security decision-making.[20]

FIGURE 6 Intelligence Preparation Of The Operational Environment



Use MITRE ATT&CK To Aid Attribution

Business leaders often want to identify the criminals who broke into the network and stole sensitive data. Attributing an intrusion to the perpetrator is typically out of reach for most private sector organizations. To gain the benefits of attribution without expending significant resources, intelligence teams must exploit the organization's existing security telemetry from your security stack. External data from industry-specific information sharing and analysis centers and intelligence services add additional context and can confirm internal analysis. The MITRE ATT&CK framework provides us a shared lexicon for modeling cyberthreats. Using ATT&CK across all your cloud, network, and endpoint security controls, your SOC and IR team, provides an intelligence team a common lexicon to see patterns or clusters of activity. Focusing on clustering security events — like multiple phishing emails from the same threat — based on shared infrastructure, malware, and artifacts allows intelligence teams to enumerate the myriad of threats targeting an organization and better express the nature of emerging threat activity to improve all aspects of a security organization.

Integrating Threat Intelligence At The Strategic Level

To help the board and C-suite manage strategic risks, threat intelligence must be included in conversations at that level so those stakeholders can understand the threats that may inhibit the company's strategic objectives.[21] Boards of directors are concerned with managing the greatest strategic risks — reputational and regulatory — to preserve shareholder value. The board hires a CEO who best manages those risks and takes advantages of opportunities in the market to grow shareholder value. Data breaches and cyberattacks can affect both of those strategic risks and harm shareholder value.

M&A Risk Assessments Must Consider Cyberthreats

Mergers, acquisitions, and divestitures affect a business's threat landscape. Failing to appreciate how cyberthreats perceive the business as a target can lead to devastating data breaches and harm to consumers, customers, and stockholders. Equifax leadership, for example, grew the business on acquiring other data brokers and building an extremely attractive database for state-affiliated cyberthreats to steal for their own counterintelligence and espionage purposes.[22] Failing to appreciate the company's growing cyberthreat landscape caused the company $650 million in settlements and government fines.[23] The effects to US national security are harder to quantify, but the theft of Equifax data benefitted the country responsible for the data breach and could harm the national security of the United States longer term.

Disinformation Is A Threat To Brand Reputation

Disinformation is an emerging risk in the private sector that boards and C-suites need to pay particular attention to. In the past couple of years, governments and businesses are increasingly using disinformation to deceive consumers and business leaders and negatively affect their decision-making. "One of our clients suffered a nine-figure loss as a result of a disinformation campaign. This wasn't

due to one tweet. It was a sustained, coordinated campaign against that brand over several months. The lack of visibility into these manipulated narratives leaves organizations exposed and unable to effectively defend their [reputations],” said Wasim Khalid, CEO of Blackbird.ai. Senior business leaders need to have the ability to detect indications of emerging false narratives earlier in the campaign to counter the narrative and reduce the harm to their brand’s reputation. To prevent brands from making decisions based on false narratives, senior leaders need to have intelligence capabilities that can monitor disinformation threats alongside more traditional physical and cyberthreats.

Boards Should Ask Tough Questions About the Company’s Threat Landscape

As corporate fiduciaries, boards of directors are responsible for overseeing management strategy, as well as for their identification and planned response to enterprisewide risks impacting the company and its shareholders.[24] Boards should ask the corporate management how they obtain and use intelligence on the cyberthreats to the business to drive the cyber risk management strategy. Forecasts like the National Intelligence Estimates prepared for US government policy makers or the Estonian Foreign Intelligence Service’s annual report, “International Security and Estonia” are appropriate for the board.[25] One effective structured analytic technique for forecasting is alternate futures analysis. Alternate futures analysis is useful when the situation (e.g., a cyberthreat landscape) is too complex to trust one single assessment. Involving the board and C-suite in an alternate futures exercise is the most effective way to communicate the results and explore the alternative outcomes and key uncertainties.[26] Forecasting is a vital part of strategic intelligence, offering business leaders indications about probable future conditions and aiding sound decision-making.[27]

Use Metrics To Track Threat Intelligence Effectiveness

SANS’s survey revealed only 4% of their respondents have processes in place to measure the effectiveness of threat intelligence.[28] Many organizations capture measures of performance, rather than effectiveness, when evaluating their threat intelligence program. As Charlie Munger famously said, “Show me incentive and I will show you the outcome.”[29] Organizations that use measures of effectiveness for threat intelligence will see better outcomes and lower cyber risk.

Measures Of Performance Don’t Reduce Risk

Measures of performance answer the question, “Are we doing things right?”[30] These measures tell us, for threat intelligence, that data is successfully being acquired and processed. Examples of threat intelligence measures of performance are:

- **Number of IOCs acquired.** Threat intelligence is not a volume game. The European threat intelligence team we spoke with acquired as many IOCs from external sources as possible because that was a key KPI their management measured them by. Collect what you need to answer your intelligence requirements and continually verify that information is being acquired and processed according to your intelligence architecture.

- **Number of reports read.** While intelligence analysts must consume raw and finished intelligence to maintain their knowledge of threats, reading reports alone does not reduce risk.

Measures Of Effectiveness Show Security And Intelligence Maturity

Measures of effectiveness answer the question, "Are we doing the right things?" These measures tell us, for threat intelligence, that all the resources used to understand the organization's cyberthreats have been used to reduce risk. Examples of measures of effectiveness are:

- **Detections created from threat intelligence.** Threat intelligence should be used to engineer new threat detection rules and correlations.
- **Incidents discovered from threat intelligence.** While answering stakeholder intelligence requirements, a threat intelligence team may discover leaked data or a threat selling access to the organization's network.
- **SOC signal-to-noise ratio.** False positives and low severity alerts lead to SOC threat analyst burnout and wasted resources. Threat intelligence should increase the quality of alerting in the SOC so that threat analysts have more time triaging high severity alerts.
- **Adversary dwell time.** The time from when a threat successfully achieves access to an organization's systems until it is eradicated should decrease with improved detections throughout a threat's activity and overall greater knowledge of threat TTPs.
- **Mean-time-to-recovery.** The recovery phase of the incident handling lifecycle should decrease as incident responders use threat intelligence to better scope their investigation and eradicate the threat from the environment.
- **Mean cost of a breach.** As organizations become more aware of their threat landscape and make quicker, better security decisions, the costs of data breaches and cyberattacks should decrease.

Recommendations

Start With Tactical, Progress To Operational And Strategic Intelligence

Planning and managing intelligence stakeholder interaction is key to the intelligence program's success. Start by identifying intelligence stakeholders (SOC, CISO, and board of directors). Once that's completed, the next step is determining initial intelligence requirements and creating an initial collection plan that links each requirement to a data source (such as IDS logs, malware repositories, email filters, or underground communities). To build an effective threat intelligence program, S&R pros should:

- **Make strategic intelligence a long-term goal.** Given that much of tactical intelligence can be automated, organizations should begin producing intelligence at this level before progressing to the operational level. Once the threat intelligence capability has mastered the tactical level, add requirements to cluster tactical activity into campaigns and threat groups. We recommend a

process such as the IPCE to model threats likely targeting your organization, data, and customers. The outputs of IPCE allow the organization to build a robust intelligence collection plan.[31] Lastly, use the campaign and threat group assessments to forecast long-term trends in the organization's threat landscape. Structured analytic techniques such as scenario planning and alternate futures analysis are useful for helping senior business leaders reduce long-term risk to the organization.

- **Use internal data first.** Before paying a vendor for threat intelligence, leverage your own organization's security telemetry — like email security, SOC events, and postincident reports. You've already paid for it! Once you've exhausted all your internal data, you can then evaluate external threat intelligence services from vendors like CrowdStrike, FireEye, Secureworks, and others to complete your intelligence collection plan. Start with sources that help protect your organization's brand and reputation.
- **Remember that threat intelligence is not a volume game.** Threat intelligence is only a volume game when showing the billions of IOCs you have available. Too much data leads to analysis paralysis. As Alex Nikolai Steffen wrote, "More is not better. Better is better."[32] Fill out your threat intelligence collection plan with internal sources first. Then fill in the gaps with high-quality external sources — free or paid. Collect only what you need to answer your stakeholders' requirements.
- **Use measures of effectiveness.** Threat intelligence helps organizations make better security decisions and reduce risk. This requires focusing on metrics that demonstrate the value stakeholders are realizing from applying threat intelligence to their decision-making. Metrics like mean cost of a breach, adversary dwell time, and mean-time-to-recover better show whether your intelligence capability is improving decision-making and reducing risk.

Supplemental Material

Survey Methodology

The Forrester Analytics Business Technographics® Security Survey, 2020, was fielded from June to August 2020. This online survey included 3,691 respondents in Australia, Canada, China, France, Germany, India, the UK, and the US from companies with two or more employees.

Forrester Analytics' Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services and in marketing efforts. Dynata fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Analytics' Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

For Technographics Clients: How To Get More Technographics Data Insights

Forrester's Business Technographics Security Survey 2020 of 1,137 global security decision-makers includes many additional questions and parameters by which you can analyze the data contained in this report.

We can provide additional insights about the consumers highlighted in this report:

- Who they are (e.g., demographics, lifestyle, and interests).
- What they do (e.g., digital, mobile, social behaviors).
- Affiliations they have (e.g., brands used, products owned).
- How they feel (e.g., attitudes, interests).

If you wish to subscribe to Forrester's Consumer Technographics services, please contact your account manager or data@forrester.com. If you are an existing Technographics client, please contact your data advisor at data@forrester.com.

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Blackbird.ai
Cisco
CrowdStrike
Dragos
FireEye

Endnotes

[1] Source: Interview with Matthew Olney, director, Talos threat intelligence and interdiction at Cisco, August 19, 2020.

[2] Source: Jared Ettinger, et. al., "Cyber Intelligence Tradecraft Report: The State of Cyber Intelligence Practices in the United States (Study Report and Implementation Guides)," Carnegie Mellon University, May 21, 2019 (https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=546578).

[3] Source: Robert M. Lee, "2020 SANS Cyber Threat Intelligence (CTI) Survey," SANS Institute, February 10, 2020 (https://www.sans.org/reading-room/whitepapers/threats/paper/39395).

[4] Source: Jared Ettinger, et. at., "Cyber Intelligence Tradecraft Report: The State of Cyber Intelligence Practices in the United States (Study Report and Implementation Guides)," Carnegie Mellon University, May 21, 2019 (https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=546578).

[5] Source: Robert M. Lee, "2020 SANS Cyber Threat Intelligence (CTI) Survey," SANS Institute, February 10, 2020 (https://www.sans.org/reading-room/whitepapers/threats/paper/39395).

[6] Source: Robert M. Lee, "2020 SANS Cyber Threat Intelligence (CTI) Survey," SANS Institute, February 10, 2020 (https://www.sans.org/reading-room/whitepapers/threats/paper/39395).

[7] The model establishes the basic atomic element of any intrusion activity, the event, composed of four core features: adversary, infrastructure, capability, and victim. These features are edge-connected representing their underlying relationships and arranged in the shape of a diamond, giving the model its name: the Diamond Model. It further defines additional meta-features to support higher-level constructs such as linking events together into activity threads and further coalescing events and threads into activity groups. These elements, the event, thread, and group all contribute to a foundational and comprehensive model of intrusion activity built around analytic processes. It captures the essential concepts of intrusion analysis and adversary operations while allowing the model flexibility to expand and encompass new ideas and concepts. Source: Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, "The Diamond Model of Intrusion Analysis," Active Response, July 2013 (https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf).

Developed by Lockheed Martin, the Cyber Kill Chain framework is part of the intelligence driven defense model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective. Source: "Cyber Kill Chain," Lockheed Martin (https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html).

ICS-custom cyberattacks capable of significant process or equipment impact require adversaries to become intimately aware of the process being automated and the engineering decisions and design of the ICS and safety system. Gaining such knowledge enables an attacker to learn the systems well enough to cause predictable effects on systems in a way that circumvents or impacts safety mechanisms and achieves a true cyber-physical attack rather than an attack characterized as espionage, ICS disruption, or intellectual property theft. To accomplish such an attack requires adversaries to initiate a two-stage attack against an ICS. The multiple stages, or exaggerated kill chain, provide additional opportunities for defenders to increase the adversary's cost of an attack and to position themselves to detect and disrupt attackers before they reach their goal. Source: Michael J. Assante and Robert M. Lee "The Industrial Control System Cyber Kill Chain," SANS Institute, October 2015 (https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297).

See the Forrester report "The Forrester MITRE ATT&CK Evaluation Guide."

[8] Source: Kristen Dennesen, John Felker, Tonya Feyes, and Sean Kern, "Strategic Cyber Intelligence," Intelligence and National Security Alliance, March 25, 2014 (https://www.insaonline.org/wp-content/uploads/2017/04/INSA_StrategicCyberIntel_WP.pdf).

[9] Source: Steven Hengel Jr, Sean Kern, and Andrea Little Limbago, "Operational Cyber Intelligence," Intelligence National Security Alliance, October 8, 2014 (https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_Op_Cyber_FIN.pdf).

[10] Source: Sergio Caltagirone, "CART: The 4 Qualities of Good Threat Intelligence," Active Response, July 1, 2015 (http://www.activeresponse.org/the-4-qualities-of-good-threat-intelligence/).

[11] IOC = Observable + Context. Within information sharing standards, this context is traditionally found in the description field of an IOC. I recommend a little Golden Rule of CTI: Provide as much context as you wish other sharing partners would provide to you. Seriously, picture another analyst receiving your IOC through an information sharing program; they run those IOCs through their SIEM and get a match to an event and they have the description you wrote. Did you give them enough information to determine if this is a false positive? Did you give them enough information to pivot into other event types to search for related IOCs? Or did you share another frustratingly contextless "observable"? Source: Andy Piazza, "CTI is Better Served with Context: Getting better value from IOCs," Medium, June 14, 2020 (https://klrgrz.medium.com/cti-is-better-served-with-context-getting-better-value-from-iocs-496343741f80).

[12] Source: Sergio Caltagirone, "CART: The 4 Qualities of Good Threat Intelligence," Active Response, July 1, 2015 (http://www.activeresponse.org/the-4-qualities-of-good-threat-intelligence/).

[13] Source: Sergio Caltagirone, "CART: The 4 Qualities of Good Threat Intelligence," Active Response, July 1, 2015 (http://www.activeresponse.org/the-4-qualities-of-good-threat-intelligence/).

[14] Source: Sergio Caltagirone, "CART: The 4 Qualities of Good Threat Intelligence," Active Response, July 1, 2015 (http://www.activeresponse.org/the-4-qualities-of-good-threat-intelligence/).

[15] Source: Forrester Analytics Business Technographics Security Survey, 2020.

[16] Sources: Forrester Analytics Business Technographics Security Survey, 2020, and Forrester Analytics Global Business Technographics Security Survey, 2019.

[17] Source: Robert M. Lee, "2020 SANS Cyber Threat Intelligence (CTI) Survey," SANS Institute, February 10, 2020 (https://www.sans.org/reading-room/whitepapers/threats/paper/39395).

[18] See the Forrester report "CISO Career Paths: Plot Your Course For Advancement."

[19] Source: Steven Hengel Jr, Sean Kern, and Andrea Little Limbago, "Operational Cyber Intelligence," The Intelligence and National Security Alliance, October 8, 2014 (https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_Op_Cyber_FIN.pdf).

[20] Source: Brian Kime, "Threat Intelligence: Planning and Direction," SANS Institute, March 29, 2016 (https://www.sans.org/reading-room/whitepapers/threatintelligence/paper/36857).

[21] Source: Steven Hengel Jr, Sean Kern, and Andrea Little Limbago, "Operational Cyber Intelligence," The Intelligence and National Security Alliance, October 8, 2014 (https://www.insaonline.org/wp-content/uploads/2017/04/INSA_WP_Op_Cyber_FIN.pdf).

[22] A federal grand jury in Atlanta returned an indictment in February 2020 charging four members of the Chinese People's Liberation Army (PLA) with hacking into the computer systems of the credit reporting agency Equifax and stealing Americans' personal data and Equifax's valuable trade secrets. Source: "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax," US Department of Justice, February 10, 2020 (https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking).

[23] Source: David Yaffe-Bellany, "Equifax Data-Breach Settlement: Get Up to $20,000 If You Can Prove Harm," The New York Times, July 22, 2019 (https://www.nytimes.com/2019/07/22/business/equifax-data-breach-claim.html).

[24] Source: Larry Clinton, "Cyber-Risk Oversight 2020: Key Principles and Practical Guidance for Corporate Boards," Internet Security Alliance, February 2020 (http://isalliance.org/wp-content/uploads/2020/02/RD-3-2020_NACD_Cyber_Handbook__WEB_022020.pdf).

[25] Estonia's Foreign Intelligence Service publishes this annual report — "International Security and Estonia" — to ensure the best possible threat assessments to Estonian leadership. Source: "International Security and Estonia 2020," Estonian Foreign Intelligence Service (https://www.valisluureamet.ee/pdf/raport-2020-en.pdf).

[26] Source: United States Government, A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis, CreateSpace Independent Publishing Platform, 2012.

[27] Source: David R. Mandel and Alan Barnes, "Accuracy of forecasts in strategic intelligence," PNAS, July 29, 2014 (https://www.pnas.org/content/111/30/10984).

[28] Source: Robert M. Lee, "2020 SANS Cyber Threat Intelligence (CTI) Survey," SANS Institute, February 10, 2020 (https://www.sans.org/reading-room/whitepapers/threats/paper/39395).

[29] Charlie Munger is the vice chairman of Berkshire Hathaway and considered by Warren Buffet to be his partner at the company.

[30] Source: "Joint Operations," Joint Chiefs of Staff, October 22, 2018 (https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf).

[31] Source: Brian Kime, "Threat Intelligence: Planning and Direction," SANS Institute, March 29, 2016 (https://www.sans.org/reading-room/whitepapers/threatintelligence/paper/36857).

[32] Source: Alex Nikolai Steffen, "The Next Green Revolution," Wired, May 1, 2006 (https://www.wired.com/2006/05/green/).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

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.

160276