Vendor Landscape: S&R Pros Turn To Cyberthreat Intelligence Providers For Help

CTI Providers Must Support Every Phase Of The Intelligence Cycle

by Rick Holland

November 3, 2015

Why Read This Report

The overwhelming threat landscape, coupled with the desire to transition from reactive to proactive security, is driving interest in cyberthreat intelligence. Organizations are looking to complement internally developed threat intelligence with external threat intelligence. In this report, we give S&R pros the tools to evaluate cyberthreat intelligence providers along with analysis of 20 of the top players in the space.

Key Takeaways

Cyberthreat Intelligence Provides Tactical And Strategic Value

S&R pros want to better understand the threat landscape and use that knowledge to inform strategic business decisions. At the same time, they want to integrate tactical CTI into their controls to provide better protection and detection.

The Intelligence Cycle Should Be The Framework For Evaluating CTI Providers

In an effort to better understand and differentiate CTI providers, S&R pros should frame their vendor analysis using the intelligence cycle and determine how the vendor supports: 1) planning and direction; 2) collection; 3) processing; 4) analysis and production; and 5) dissemination.

S&R Pros Must Be Prepared To Quantify Threat Intelligence Benefits

The resources required to invest in internal and external threat intelligence can be significant. It's imperative that S&R leaders develop a plan to measure the return on investment in cyberthreat intelligence.

Vendor Landscape: S&R Pros Turn To Cyberthreat Intelligence Providers For Help

CTI Providers Must Support Every Phase Of The Intelligence Cycle

by Rick Holland
with Stephanie Balaouras, Claire O'Malley, and Peggy Dostie

November 3, 2015

Table Of Contents

Notes & Resources

Forrester interviewed Bitsight Technologies AnubisNetworks, CrowdStrike, Cyjax, Cytegic, Cyveillance, Digital Shadows, Emerging Threats, FireEye/Mandiant, Flashpoint, IID, Intel 471, iSight Partners, Norse, Recorded Future, SurfWatch Labs, Symantec, Verisign iDefense, Wapack Labs, Webroot, and ZeroFox.

Related Research Documents

Know Your Adversary

The State Of The Cyberthreat Intelligence Market

Top 11 Trends S&R Pros Should Watch: 2015

FORRESTER®

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

S&R Pros Turn To CTI Providers For External Threat Intel

In the past 12 months, the five largest breaches (based on the number of breached customer records) accounted for 93% of all breached records.[1] US home improvement retailer Home Depot took the top spot with a breach that affected 109 million records, followed by US health insurance provider Anthem Blue Cross Blue Shield. This concentration demonstrates the targeted nature of today's cyberattacks. Attackers are carefully picking their victim organization, learning its business, understanding its partner relationships, and testing for weaknesses and vulnerabilities. This is why there is strong demand for cyberthreat intelligence (CTI). S&R pros want as much warning as possible of threat actors targeting their region, industry, or, specifically, their firm. The hope is that with a little more warning, or at least an understanding of the adversaries targeting their firm, S&R pros can adjust security accordingly and reduce the likelihood of a successful attack. Forrester defines CTI as:

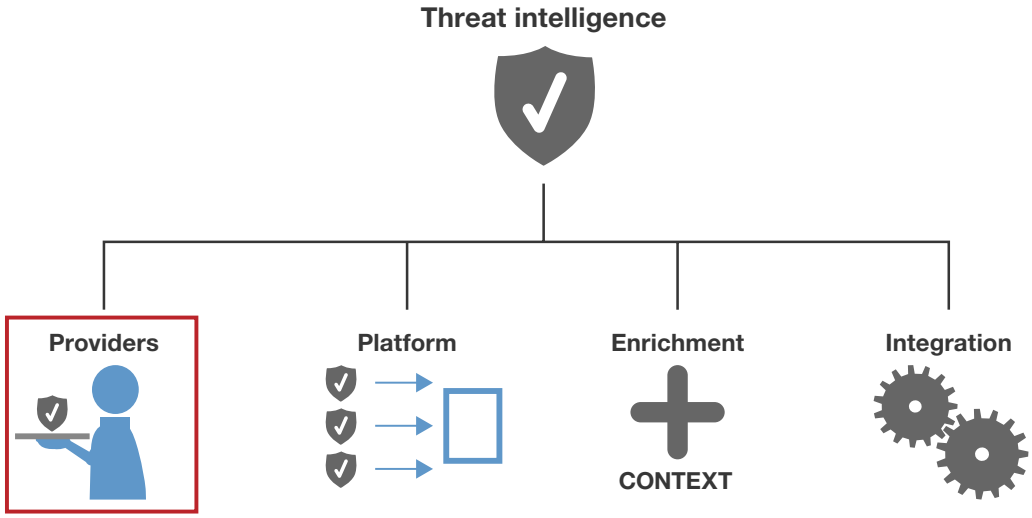
> *"The details of the motivations, intent, and capabilities of internal and external threat actors. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats."*

CTI consists of four distinct categories of technology capabilities: providers, platforms, enrichment, and integration (see Figure 1). The research in this report focuses on CTI providers that use a variety of collection capabilities to gather information on external threat actors. These providers then use automated and/or human analysis to produce machine-readable CTI and analyst-written intelligence reports. CTI providers help S&R pros:

- **Better understand the threat landscape.** CTI provides insights into the threat landscape that aid in determining appropriate courses of action that reduce risks to business operations. The understanding of threats needs to balance internal perspective based on actual intrusions with external threat actor activity.
- **Enhance the effectiveness of other security controls.** As one S&R pros told us: "We are able to take a threat intelligence feed and integrate it directly into our Palo Alto Networks firewalls. We are blocking malicious traffic and reducing the number of intrusions we have to respond to."

That customer testimonial brings up a significant point: Threat feeds can provide value. The point is often made that without human analysis threat data isn't intelligence and provides no value.[2] This client didn't have a threat intelligence team, much less dedicated incident response staff. From a traditional intelligence perspective, threat data isn't threat intelligence. However, for the majority of organizations this doesn't matter, and value can still be gained. Many organizations lack the resources to invest in the more expensive analyst-driven finished intelligence products and are happy to integrate threat feeds into their security controls.

FIGURE 1 Cyberthreat Intelligence Technology Categories



CTI Provider Evaluation Criteria

To help S&R professionals understand the CTI provider landscape, it's important to provide additional detail on how these providers collect, analyze, and generate intelligence in support of the intelligence cycle. The intelligence cycle consists of five phases: 1) planning and direction; 2) collection; 3) processing; 4) analysis and production; and 5) dissemination. This intelligence cycle is popular with most intelligence agencies.[3]

Collection: What Are The Provider's Sources And Methods?

The Department of Defense's JP 2-01 defines collection operations as "operations to acquire information about the adversary and other relevant aspects of the operational environment and provide that information to intelligence processing and exploitation elements."[4] Collection is the process through which the CTI provider attempts to answer its intelligence requirements. A vendor's intelligence requirements should be aligned to your organization, and vendors should be able to discuss their intelligence requirements with you. Intelligence requirement definition occurs in the planning phase of the intelligence cycle.[5] CTI providers use a number of techniques for collection including open source, technical, and human (see Figure 2):

FIGURE 2 Collection Techniques And Capabilities

Open source collection	
BitTorrent monitoring	Provider monitors BitTorrent sites for information leakage as well as threats against clients.
Code-sharing-site monitoring	Provider integrates with APIs of common code-sharing repositories such as GitHub to identify leaked code.
Dark web monitoring	Provider monitors dark web content that uses protocols like Tor, I2P, and Freenet.
Deep web monitoring	Provider monitors sites that aren't indexed by search engines for threats against clients.
Open source intelligence feeds	Provider uses open source intelligence feeds such as SANS DSHIELD and Spamhaus
Paste site monitoring	Provider monitors sites like Pastebin for dumps that include client information.
Public IRC monitoring	Provider collects public Internet relay channel communications.
Social media monitoring	Provider monitors social media for threats against clients.
Surface web monitoring	Provider uses crawlers to search the publicly accessible web: websites, blogs, open forums, open boards.
Technical collection	
Commercial intelligence feeds	Provider purchases threat intelligence feed from other threat intelligence providers.
Consumer device monitoring	Provider monitors consumer devices such as home NAS drives and routers for corporate data leakage.
DNS sinkholes	Provider redirects malicious traffic so communications can be captured and analyzed.
DNS traffic	Provider has access to DNS traffic which is incorporated into intelligence analysis.
Exploit and vulnerability monitoring	Provider monitors exploit and vulnerability activity that is relevant to clients.
Honey networks	Vendor operates honeypot networks to collect against adversaries.
Incident response	Provider gathers intelligence from incident response service engagements.
Human collection	
Asset recruitment	Provider has regional assets (e.g., Eastern Europe) that actively recruit and maintain sources.
Cybercollection	Provider develops and maintains sock puppets/personas/legends to gain and retain access to closed forums and boards.
Regional assets	Provider has regional assets (e.g., Eastern Europe) operating out of specific regions that interact with the local community (threat actors, law enforcement).

Analysis: What Is The Provider's Ability To Support Automated Analysis?

Raw collection provides less value until the intelligence has been analyzed. Some organizations perform their own analysis and treat all vendor products as raw intelligence. Most organizations rely on vendors to provide them finished intelligence that has been analyzed. A CTI provider's analytical capabilities are a critical component for evaluating vendors. From an analysis perspective, CTI providers use the following approaches:

- **Automated analysis with limited human analyst support.** All CTI providers are using automation to drive their collection, processing, and analysis efforts. For analysis, vendors leverage statistical and pattern analysis of both structured and unstructured data. Examples where CTI providers perform automated analysis include malware, attacker infrastructure, and open source website in foreign languages.
- **Automated analysis with significant human analyst support.** A benefit of carbon-based analysis is that people understand context and can provide a deeper understanding of critical issues. In this scenario, automation is used to enable the analyst since human analysts cannot scale. Some vendors have robust language coverage with native speakers from the regions that threat actors operate out of. In some cases, vendors make their internal analysts' tools available to customers. Verisign iDefense's IntelGraph is one example.[6]

Production: How Does The Provider Help Generate The Three Levels Of CTI?

CTI isn't just about collection capabilities; they are a simply a means to an end. Intelligence products are the result of collection and analysis, and they are the deliverables that S&R pros need. There are three levels of CTI: tactical, operational, and strategic. For most security teams, especially when starting out, it's important that you don't hyperfocus on the three tiers. In fact, most teams naturally start out with tactical CTI. In 2013, the Intelligence and National Security Alliance (INSA) produced a document titled "Operational Levels of Cyber Intelligence" that expands on traditional tiers of intelligence and extends them to the cyberdomain.[7] When you evaluate CTI providers, ask them how they demonstrate support for the three levels of intelligence (see Figure 3):

- **Tactical cyberthreat intelligence.** Tactical CTI is focused on now and the immediate future. According to INSA, the "tactical level of the cyberdomain is where the on-the-network actions take place. This is where malicious actors and network defenders maneuver against each other."[8] Tactical CTI is commonly technical in nature and could be as simple as using threat indicators to proactively hunt for and defend against adversaries. Tactical intelligence can also be referred to as technical intelligence.
- **Operational cyberthreat intelligence.** Operational threat intelligence focuses on the motivations, intent, and capabilities of adversaries.[9] Operational threat intelligence is concerned with how adversaries plan, conduct, and sustain campaigns and major operations. Adversary tactics,

techniques, and procedures (TTPs) are a key component of operational threat intelligence. Operational CTI is focused on the near term. Operational intelligence can also be referred to as adversary intelligence.[10]

› **Strategic cyberthreat intelligence.** Strategic intelligence ideally informs business decisions regarding the risks and implications associated with threats. According to INSA, strategic "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."[11] S&R pros can use strategic intelligence to direct cybersecurity investment.

FIGURE 3 Examples Of Tactical, Operational, And Strategic Intelligence Products

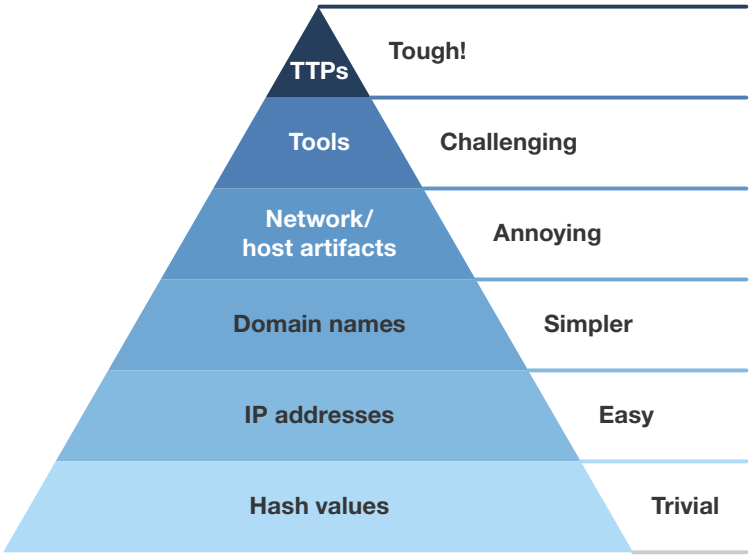
Tactical intelligence products
Daily media highlight analysis
Flash/Tipper reports for rapid dissemination
Malware analysis reports
Raw information reports
Real-time attack maps of your infrastructure and your business partner's infrastructure. All other attack maps are a distraction.
Threat intelligence feeds (IP, domain, URL)
Operational intelligence products
Adversary assessments that profile specific threat actors
In-depth technical reports that include technical analysis, and, course of, action with appropriate signatures
Vulnerability analysis reports
Weekly, monthly, quarterly intelligence summaries
Strategic intelligence products
Strategic assessment for specific verticals with a 1- to 5-year forecast
Annual intelligence summary
Comparison of internal risk profile across different industries
Geopolitical analysis
Simulations that allow exploration of potential risk when contemplating entering new geographies and business sectors and when adopting new technologies
Threat activity correlated to internal security controls/maturity

CTI On Adversary Tactics, Techniques, And Procedures Is A Challenge

David Bianco's Pyramid of Pain "shows the relationship between the types of indicators you might use to detect an adversary's activities and how much pain it will cause them when you are able to deny those indicators to them."[12] The lower a threat indicator is on the Pyramid of Pain the easier it is for an adversary to adapt to your deployment of a countermeasure against it. For example, if you add adversary IP addresses to your block lists, it is trivial for adversaries to switch IP addresses. However, if you are able to identify and put in place countermeasures against adversary TTPs, it will be much more challenging for the adversary to respond.

The Pyramid of Pain also applies to CTI providers: The higher up the pyramid, the more difficult it is to provide that level of CTI (see Figure 4). Malicious IP addresses, domain names, and URLs are the most common output from CTI feeds, while CTI providers that are able to provide specific adversary TTPs are far less common. The collection and analytical expense for delivering TTP-level CTI are much higher than what can be collected from sinkholes, honeypots, and web crawlers. Asking a threat intelligence provider to provide a TTP from an adversary relevant to your threat model is a good litmus test of their capabilities and cost.

FIGURE 4 The Pyramid Of Pain Is Painful For CTI Providers, Too



Source: David Bianco, "The Pyramid of Pain," Enterprise Detection & Response, January 17, 2014 (detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html)

CTI Provider Vendor Landscape

Forrester has included 20 vendors in our analysis of the CTI provider landscape. The vendors that were included have mindshare with Forrester clients; they came up in customer inquiries and conversations. With the exception of one vendor, all CTI can be purchased as stand-alone offerings without being an existing customer. (We will evaluate managed security service provider CTI in future research.) The CTI provider landscape consists of the following vendors (see Figure 5):[13]

- **Bitsight Technologies AnubisNetworks.** Founded in 2006, AnubisNetworks provides Cyberfeed, a subscription-based service offering tactical CTI feeds. There are DNS malware, malware analysis, website analysis, and social web feeds. AnubisNetworks provides a JSON API as well as SIEM plug-ins for CEF and LEEF and TAXII formats to integrate CTI. The Cyberfeed Live Dashboard provides real-time visibility into the service. On October 21, 2014, Bitsight Technologies acquired AnubisNetworks.[14] Bitsight Technologies followed up the AnubisNetworks acquisition with a $23 million Series B financing round on June 25, 2015.[15] AnubisNetworks is a key component of Bitsight Technologies' vendor risk management and security performance benchmarking offerings.
- **CrowdStrike.** Founded in 2011, CrowdStrike provides tactical, operational, and strategic CTI products focused on adversaries. CrowdStrike tracks nation-state, criminal, hacktivist, and activist adversaries. CrowdStrike provides tactical intelligence reports ranging from in-depth technical analysis to tipper reports providing timely and concise details on threats. CrowdStrike also provides strategic reporting covering geopolitical and historical adversary activity. All new clients receive dedicated intelligence support to ensure they fully understand how to leverage the CTI offerings. Clients can submit requests for information (RFIs) through a portal for tailored intelligence support.[16] CrowdStrike provides an API for CTI integration. On July 13, 2015, CrowdStrike closed a $100 million Series C financing round.[17]
- **Cyjax.** Founded in 2012, Cyjax is a United-Kingdom-based CTI provider, originally known as Welund Horizon. The firm relaunched as Cyjax on September 7, 2015. Cyjax provides a broad range of intelligence offerings through a web-based portal and an API with basic functionality. Cyjax monitors both the deep web and dark web and mirrors underground marketplaces. Cyjax monitors a client's brand, looking for leaked information and compromised hosts. Cyjax also provides blacklists for CTI integration, weekly executive summaries, and intelligence-management-as-a-service, allowing clients to submit RFIs. Cyjax is focused on cybercriminals and hacktivists.
- **Cytegic.** Founded in 2012, Cytegic is an Israeli-based startup focused on the strategic side of the threat intelligence paradigm. The Dynamic Trend Analysis (DyTA) solution is designed to forecast cyberthreat activity for geopolitical regions and business sectors by correlating trend and pattern analysis. DyTA does this by analyzing structured and unstructured data from open sources including blogs, forums, and social media as well as technical CTI. DyTA's cyberthreat forecast can then be exported to Cytegic's Cyber Decision Support System (CDSS), which compares

threat activity against defensive posture to help S&R leaders better manage risk and investment is cybersecurity. CDSS includes a simulation engine to allow organizations to run scenarios to test readiness against threats.

- **Cyveillance.** Founded in 1997 and acquired by QinetiQ in 2009, Cyveillance provides OSINT.[18] Cyveillance traditionally offered finished intelligence reporting, but in September 2014, it launched Cyber Threat Center (CTC), a cloud-based OSINT analysis platform that enables analysts to search and monitor OSINT relevant to their organization.[19] The CTC also includes an analyst workspace and access to global intelligence reports. Cyveillance's Special Investigations Unit and Watch Desk provides OSINT analysts on-demand on a time-and-materials basis. Cyveillance provides phishing and malicious URL feeds and is currently beta testing a REST API for CTI Integration. In addition to OSINT CTI, Cyveillance provides brand intelligence, brand protection, and corporate and executive security.
- **Digital Shadows.** Founded in 2011, Digital Shadows is a London- and San Francisco-based OSINT provider. Digital Shadows provides finished OSINT reporting as well as SearchLight, an OSINT analysis platform that provides a macro view of an organization's digital footprint as well as attacker profiles. A SearchLight subscription also includes 8 hours of monthly analyst time. Digital Shadows has been deeply involved in the Bank of England's CBEST framework and meets the threat intelligence provider standards for CBEST and STAR.[20] In addition to the SearchLight portal, Digital Shadows offers a well-documented API for CTI integration. Beyond cyberthreats, Digital Shadows also delivers broader situational awareness into intellectual property theft loss as well as brand and reputation damage.
- **Emerging Threats.** Emerging Threats (ET) was founded as an open source community in 2003, incorporated in 2011, and acquired by Proofpoint on March 2, 2015.[21] ET provides tactical CTI on malware. Proofpoint ET runs a distributed global malware analysis platform that generates CTI. ET provides three CTI products. The ET Pro rule set includes SNORT and Suricata signatures to detect and block malicious activity. The IQRisk Rep List provides IP and domain reputation lists in a text-based format. The IQRisk Query is a threat intelligence enrichment that offers analysts web-based portal and API access to three years of ET's threat data. ET still maintains the ETOpen Ruleset, an open source IDS/IPS ruleset.
- **FireEye/Mandiant.** FireEye's premiere offering is Advanced Threat Intelligence Plus (ATI+). FireEye threat intelligence analysts take threat data gathered from FireEye's global sensor footprint and fuse it with data gathered from Mandiant incident response engagement to generate intelligence products. FireEye provides tactical, operational, and strategic products. ATI+ provides adversary intelligence including threat actor profiles, monthly industry snapshots, and quarterly trend reports. There is no formalized RFI process; customer inquiries are handled on ad hoc basis. FireEye is the only participant in this report that requires organizations to be an existing customer to use FireEye threat intelligence. Unfortunately, FireEye threat intelligence cannot be automatically integrated into non-FireEye products.

- **Flashpoint.** Founded in 2010, Flashpoint is focused on criminal threat actors operating in the deep web and dark web. Flashpoint maintains access to malware, fraud, and cybercrime forums and creates searchable copies of forum content that analysts can interact with. Flashpoint also has offerings around threat actor monitoring within BitTorrent as well as IRC. Additionally, Flashpoint creates finished intelligence reports for clients. Flashpoint has a formalized RFI process that provides analysts on-demand to customers. Flashpoint has a RESTful API as well as integrations with Threat Intelligence Platforms.[22] Flashpoint secured a $5 million round of Series A funding on April 17, 2015.[23]
- **Intel 471.** Intel 471 was founded in 2014 and publicly launched its first offering on June 1, 2015. Intel 471 provides raw intelligence collection against cybercriminals. Rather than providing finished intelligence products, Intel 471 provides information reports with original sourcing on threat actor activity. Intel 471 uses a combination of open source, technical, and human collection. Intel 471 provides an outsourced collection capability and then S&R pros incorporate this raw collection into their broader threat intelligence analysis processes. That way, clients avoid paying a premium for external analysis, as this need is taken on internally. Intel 471 reporting can be accessed via either a web portal or API.
- **IID.** Founded in 1997, Internet Identity (IID) provides tactical CTI in the form of malicious IPs, URLs, hostnames, and domain feeds via the SaaS-based ActiveTrust offering. ActiveTrust can be accessed through a searchable web portal or a REST API that includes a software development kit (SDK). ActiveTrust also exports CTI in CEF format for SIEM integration. Analyst on-demand capability is billed on a time-and-material basis. Many commercial CTI providers including Proofpoint Emerging Threats and Flashpoint also contribute to the ActiveTrust exchange, which seeks to be a clearinghouse for open source, proprietary IID, and commercial CTI feeds.
- **iSight Partners.** Founded in 2006, iSight Partners is one of the longest-standing adversary intelligence providers. iSight Partners operates in 16 countries and supports 24 languages. iSight's ThreatScape subscriptions include cybercrime, cyberespionage, hacktivism, critical infrastructure, vulnerability, and exploitation offerings. iSight provides a wide range of intelligence reporting ranging from tactical to strategic products. iSight enables integration with the ThreatScape API and SDK. iSight has a formalized RFI process to request analyst support in each subscription. Bessemer Venture Partners invested $30 million in a Series C funding round in January 2015. According to reports, iSight Partners is also looking to raise another $100 million ahead of a potential 2016 IPO.[24]
- **Norse Corporation.** Founded in 2010, Norse is a tactical intelligence provider that garnered headlines during the 2014 Sony Pictures breach.[25] In April 2015, Norse launched a new threat intelligence offering and shifted from its IPViking feed to the Norse Intelligence Service (NIS). The NIS takes technical data gathered from its global collection network of sensors, agents, honeypots, and crawlers and overlays it against client and client business partner networks to provide

continuous monitoring against threats. Norse analysts are available to support clients in detection and response activities. Norse also offers the Norse Appliance, which integrates Norse tactical intelligence to block malicious network activity.

- **Recorded Future.** Founded in 2009 with notable investments from Google Ventures and In-Q-Tel, Recorded Future provides a SaaS-based open source analysis platform. Recorded Future doesn't provide finished intelligence; it instead automates open source collection and prepares the results for your own internal analysts. Recorded Future enables analysis with powerful visualization and querying tools. Recorded Future's OSINT capabilities allow clients to extend beyond cyberdomain to geopolitical, business, regulatory, and legal realms. Recorded Future harvests open source data in English, Spanish, French, Russian, Chinese, Arabic, and Farsi.
- **SurfWatch Labs.** Founded in 2014, SurfWatch Labs (SW), originally known as HackSurfer, seeks to apply the business intelligence lens to cybersecurity by mapping cyberthreats to business risk. SW provides strategic intelligence using OSINT collection to gather relevant risk data. SW Analytics is the data warehouse for collected cyberthreat intelligence and the analytics engine that serves as the foundation for all SW solutions and products. The SW Threat Intelligence Suite encompasses four products: SW C-Suite, SW Cyber Risk Cloud, SW Risk Monitor, and SW News & Analysis. SW also provides a REST API that can be integrated with a customer's SIEM or other cybersecurity tools.
- **Symantec.** The DeepSight Intelligence business unit was formed in 2003 and until recently has focused on tactical CTI. DeepSight provides feeds focused on security risk, vulnerabilities, and IP/URL/domain reputation. Symantec's newly added DeepSight Adversary and Threat Intelligence focuses on cybercrime, hacktivism, and cyberespionage threats. Symantec provides both a portal and API to access CTI. Another new capability within the DeepSight offering is a Directed Threat Research Service that allows customers to submit RFIs and also augment their staff with Symantec's analysts. A combination of open source, technical, and human collection is used to derive tactical and operational intelligence products.
- **Verisign iDefense.** iDefense has more than 40 dedicated TI analysts proficient in 20 languages. iDefense provides adversary intelligence for espionage, cybercrime, and hacktivism threat actors. iDefense also has vulnerability intelligence offerings. iDefense provides 14 different types of threat intelligence reporting. In August 2015, iDefense launched its IntelGraph, a platform that allows users to search, manipulate, and visualize relationships within iDefense's knowledge base. iDefense has a formalized RFI process. iDefense was founded in 1999 and acquired by Verisign for $40 million in 2005. iDefense helps to ensure the availability of .com and .NET infrastructure and can incorporate DNS resolution data into its CTI.
- **Wapack Labs.** Wapack Labs is a self-funded operation, originally founded as RedSky Alliance in 2012 but spun off into a separate entity in April 2013. Wapack Labs provides adversary intelligence focused on espionage and criminal threat actors. Wapack Labs produces intelligence products ranging from tactical to strategic. CTI products include adversary TTPs as well as recommended

courses of action. A combination of open source, technical, and human collection is used to derive intelligence products. Wapack Labs provides subscription offerings that include both raw information and finished intelligence reporting. The Threat Recon API is available to clients in a free, query-based pricing model.

- **Webroot.** Webroot was founded in 1997 and has a wide portfolio of security offerings including endpoint and network security. Webroot provides tactical CTI for both security vendor and enterprise customers. The BrightCloud Threat Intelligence offering is built upon Webroot's consumer, SMB, and enterprise client product footprint as well as Webroot's global collection network. BrightCloud threat intelligence provides vendor clients antiphishing, file, IP, mobile app, and web reputation feeds. For enterprise clients, BrightCloud IP reputation can be integrated directly into Palo Alto Networks firewalls as well as into LogRhythm and Splunk. Webroot provides a REST API for security vendor integrations.
- **ZeroFox.** Founded in 2013, ZeroFox is a SaaS-based social risk management vendor that provides OSINT insight into phishing and malware attacks delivered via social media. The ZeroFox threat feed includes URL, IP, DNS, geolocation, and malware threat data as well as social media context. The threat feed's REST API enables integrations into network security devices including proxies and firewalls as well as SIEMs. ZeroFox has partnership integrations with Checkpoint, Intel Security, OpenDNS, and Splunk. ZeroFox has use cases beyond social media threats as they also monitor their client's brand and reputation and enable the safe use of social media accounts.

FIGURE 5 Matrix Of CTI Providers

CTI provider	Intelligence products	FTEs dedicated to analysis	Provide TTPs	API	Formal RFI process	Custom/ tailored intelligence	Portal access
Bitsight Technologies AnubisNetworks	Tactical	~ 10		✓			✓
CrowdStrike	Tactical, operational, strategic	~ 20	✓	✓	✓	✓	✓
Cyjax	Tactical, strategic	~ 5	✓	✓		✓	✓
Cytegic	Strategic	~ 5					✓
Cyveillance	Tactical, operational, strategic	~ 75	✓			✓	✓
Digital Shadows	Tactical, operational, strategic	~ 20	✓	✓	✓	✓	✓
Emerging Threats	Tactical	~ 5		✓			✓
FireEye/ Mandiant	Tactical, operational, strategic	~ 50	✓			✓	✓
Flashpoint	Tactical, operational	~ 10	✓	✓	✓	✓	✓
Intel 471	Raw collection	N/A	✓	✓		N/A	✓
IID	Tactical	~ 5		✓		✓	✓
iSight Partners	Tactical, operational, strategic	~ 120	✓	✓	✓	✓	✓
Norse	Tactical	~ 15				✓	✓
Recorded Future	Raw collection	N/A	✓	✓		N/A	✓
SurfWatch Labs	Strategic	~ 10		✓		✓	✓
Symantec	Tactical, operational	~ 50	✓	✓	✓	✓	✓
Verisign iDefense	Tactical, operational, strategic	~ 30	✓	✓	✓	✓	✓
Wapack Labs	Tactical, operational, strategic	~ 15	✓	✓	✓	✓	✓
Webroot	Tactical	~ 10		✓			
ZeroFox	Tactical	~ 5		✓		✓	✓

Recommendations

Only You Can Set Yourself Up For Success In CTI

Investing in externally provided CTI can be an expensive endeavor, with prices ranging from the tens of thousands to millions. If you're able to make this level of investment, you must be prepared to quantify its benefits when renewal comes up. In the classic movie Office Space, a pair of external consultants, referred to as "the Bobs," are brought in to evaluate the workers and their performance. Prepare for the Bobs: You need to be able to demonstrate the return on your investment in CTI. Measure your intrusion and breach volume before and after implementation. Measure changes in time-to-detection or dwell-time. Tie protection and detection metrics to specific business initiatives. When selecting vendors, it's important that you:

- **Disregard vendors who try to distract you with the size of their threat intelligence.** When it comes to collection, size isn't the most critical input. Don't be distracted by vendors who claim to have the "largest global threat intelligence network on the planet." Claims of "5 million endpoints" or "hundreds of thousands of networks sensors" should go in one ear and out the other. If a vendor's collection capabilities don't produce threat intelligence that is relevant to your organization and threat model, then it's nothing more than window dressing. When it comes to actionable intelligence, relevancy matters.
- **Insist on more transparency into sources and methods.** Be wary of providers that won't provide any details on their collection capabilities. One hundred percent transparency isn't realistic; providers naturally want to protect their sources and methods, but they must find a compromise that informs prospects and demonstrates differentiation. In a crowded market, providers who keep everything about sources and methods private will be hard-pressed to make customer shortlists where they will be given the opportunity to validate their nebulous claims. Challenge vendors that provide little detail and suggest nondisclosure agreements; as a last resort, eliminate them from consideration.
- **Understand how the providers derive their intelligence.** Make sure you understand the analytical process used by the CTI provider to develop intelligence. This is where you find out how the vendor leverages the processing and analysis stages of the intelligence cycle. Some providers are more focused on rules-based engines or predictive analytics while others add an additional layer of human analysis capabilities. Clarify the ratio of technical-to-human analysis, and keep in mind that the more human analysis, the more expensive the CTI offering. For human analysis, does the provider have formalized analytic tradecraft using something like the Diamond Model for Intrusion Analysis?[26]
- **Select a provider that will stand by you after the sale.** Your relationship with the CTI provider should continue past the pre-sales process. Vendors should dedicate ongoing time and resources to make sure that you are able to maximize your significant investment. Time should be allocated for

onboarding that should include discussions on how to submit RFIs and how to integrate CTI into your technology stack. It should also include periodic intelligence requirement discussions to ensure that their collection and intelligence production are aligned to your current and future needs.[27]

› **Focus on vendors with robust CTI integration capabilities.** CTI isn't actionable unless it's integrated; tactical intelligence should be integrated into security controls, and operational and strategic intelligence should be integrated into your decision-making processes. Look for vendors who provide both portals and APIs.

Supplemental Material

Companies Interviewed For This Report

Bitsight Technologies AnubisNetworks
CrowdStrike
Cyjax
Cytegic
Cyveillance
Digital Shadows
Emerging Threats
FireEye/Mandiant
Flashpoint
IID
Intel 471
iSight Partners
Norse
Recorded Future
SurfWatch Labs
Symantec
Verisign iDefense
Wapack Labs
Webroot
ZeroFox

Endnotes

[1] For more information about the biggest breaches from 2015, see the upcoming "Lessons Learned From The World's Biggest Customer Data Breaches And Privacy Incidents, 2015" Forrester report.

[2] You may be familiar with Russell Lincoln Ackoff's DIKW Pyramid, which presents a hierarchy in which data becomes information that becomes knowledge and then ultimately becomes wisdom. You may also have heard a version of this adapted for threat intelligence. Data becomes information that then becomes threat intelligence. The point is often made that a human is required for data to become actual intelligence. Source: Gene Bellinger, Durval Castro, and Anthony Mills, "Data, Information, Knowledge, and Wisdom," Systems-Thinking, 2004 (http://www.systems-thinking.org/dikw/dikw.htm).

[3] Against today's mutating threat landscape and sophisticated cybercriminals, security and risk (S&R) professionals are outgunned and outmatched. The traditional strategy of waiting for an alert and then responding to a compromise is futile against 21st century threat actors. Delayed responses when cybercriminals have already begun exfiltrating intellectual property aren't acceptable. Something must change, and S&R professionals must proactively defend their networks and data. For more information, see the "Five Steps To Build An Effective Threat Intelligence Capability" Forrester report.

Source: "What is Intelligence?" Central Intelligence Agency, June 20, 2008 (https://www.cia.gov/news-information/featured-story-archive/2007-featured-story-archive/what-is-intelligence.html).

[4] Source: "Intelligence, Series 2-0 Publications, PDFs," Joint Electronic Library (http://www.dtic.mil/doctrine/new_pubs/jointpub_intelligence.htm).

[5] Threat intelligence is one of the most over-hyped capabilities within information security today. Ask five different security vendors what actionable threat intelligence means and you will undoubtedly receive five different responses. With every security vendor marketing and espousing the virtues of their approach to actionable intelligence, security

and risk (S&R) leaders need a way to differentiate and dedicate their limited resources to the most beneficial intelligence sources. For more information, see the "Use Actionable Threat Intelligence To Protect Your Digital Business" Forrester report.

[6] Source: Josh Ray, "Announcing Verisign IntelGraph: Unprecedented Context for Cybersecurity Intelligence," Verisign, July 30, 2015 (http://blogs.verisign.com/blog/entry/cyber_threats_in_context_use?).

[7] Source: "Operational Levels of Cyber Intelligence," Intelligence And National Security Alliance, September 2013 (http://www.insaonline.org/i/d/a/b/CyberIntel_embed.aspx).

[8] Source: "Operational Levels of Cyber Intelligence," Intelligence And National Security Alliance, September 2013 (http://www.insaonline.org/i/d/a/b/CyberIntel_embed.aspx).

[9] Attributing security incidents such as corporate espionage, customer data theft, and denial of service attacks to specific adversaries was once a rare practice, but it's now becoming more and more common even for private sector enterprises, not just security experts and government agencies. It allows security and risk (S&R) pros to put a name and a face to a once nebulous attacker operating from somewhere in cyberspace. When you know what group is targeting you as well as their motivations and capabilities, you can transition your cybersecurity strategy from a largely ineffective, haphazard defensive approach to one that is proactive and targeted. For more information, see the "Know Your Adversary" Forrester report.

[10] Attributing security incidents such as corporate espionage, customer data theft, and denial of service attacks to specific adversaries was once a rare practice, but it's now becoming more and more common even for private sector enterprises, not just security experts and government agencies. It allows security and risk (S&R) pros to put a name and a face to a once nebulous attacker operating from somewhere in cyberspace. When you know what group is targeting you as well as their motivations and capabilities, you can transition your cybersecurity strategy from a largely ineffective, haphazard defensive approach to one that is proactive and targeted. For more information, see the "Know Your Adversary" Forrester report.

[11] Source: "Operational Levels of Cyber Intelligence," Intelligence And National Security Alliance, September 2013 (http://www.insaonline.org/i/d/a/b/CyberIntel_embed.aspx).

[12] Source: "The Pyramid of Pain," Enterprise Detection & Response, January 17, 2014 (http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html).

[13] CTI provider matrix capabilities are based on vendor feedback, Forrester client feedback, and analyst perspective from extensive research, knowledge, and experience in the industry.

[14] Source: "Bitsight Acquires Security Intelligence Company AnubisNetworks," Bitsight Technologies press release, October 21, 2014 (http://www.bitsighttech.com/press-releases/news/bitsight-acquires-innovative-security-intelligence-company-anubisnetworks).

[15] Source: "Bitsight Announces $23 Million In Series B Funding To Accelerate Worldwide Adoption Of Security Ratings," Bitsight Technologies press release, June 25, 2015 (http://www.bitsighttech.com/press-releases/bitsight-announces-series-b-funding-to-accelerate-adoption-of-security-ratings).

[16] A RFI is a specific time-sensitive ad hoc requirement for information or intelligence products, distinct from standing requirements or scheduled intelligence production. An RFI leads to a production requirement, if the request can be answered with information on hand, or a collection requirement, if the request requires collection of new information. Source: "Intelligence, Series 2-0 Publications, PDFs," Joint Electronic Library (http://www.dtic.mil/doctrine/new_pubs/jointpub_intelligence.htm).

[17] Source: "CrowdStrike Closes $100 Million Financing Round Led by Google Capital," CrowdStrike news release, July 13, 2015 (http://www.crowdstrike.com/crowdstrike-closes-100-million-financing-round-led-by-google-capital/).

[18] Source: Jeff Clabaugh, "Cyveillance acquired by QinetiQ," Washington Business Journal, May 6, 2009 (http://www.bizjournals.com/washington/stories/2009/05/04/daily43.html).

[19] Source: "Cyveillance Launches Cyber Threat Center for Security, Risk Pros," Cyveillance press release, September 15, 2014 (https://www.cyveillance.com/home/company/press-releases/cyveillance-launches-cyber-threat-center-security-cyber-risk-professionals/).

[20] Source: "About CREST," CREST (http://www.crest-approved.org/why-use-crest/index.html) and "CBEST Vulnerability Testing Framework Launch," Bank of England (http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx).

[21] Source: "Company History," Emerging Threats (http://www.emergingthreats.net/about-us/company).

[22] Source: BrightPoint Security (https://www.brightpointsecurity.com/); ThreatConnect (http://www.threatconnect.com/); and Threatstream (https://www.threatstream.com/).

[23] Source: "Flashpoint Leading Deep and Dark Web Intelligence Provider, Raises $5 Million in Financing Round," Flashpoint press release, April 17, 2015 (http://flashpoint-intel.com/news/flashpoint-leading-deep-and-dark-web-intelligence-provider-raises-5-million-in-financing-round/).

[24] Source: Jim Finkle, "Cyber intel firm iSight plans funding round ahead of 2016 IPO," Reuters, August 19, 2015 (http://www.reuters.com/article/2015/08/19/isight-ipo-idUSL1N10U28X20150819).

[25] Norse cast doubts on the FBI's assertion that North Korea was behind the breach and instead pointed to Sony insiders. Source: Security Dispatch, "Norse Investigation Focusing on a Small Group, Including Sony Ex-Employees," Darkmatters, December 29, 2014 (http://darkmatters.norsecorp.com/2014/12/29/ex-employee-five-others-fingered-in-sony-hack/).

[26] Source: Defense Technical Information Center (http://www.dtic.mil/docs/citations/ADA586960).

[27] Develop intelligence requirements aligned with what matters most to the business. For more information and guidance, see the "Use Actionable Threat Intelligence To Protect Your Digital Business" Forrester report.

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.