DARKReading RESEARCH

FEBRUARY 2021

STATE OF THREAT INTELLIGENCE

Making the Case for Agile Threat Intelligence

cybersixgill

Executive Summary

The digital world is growing at an alarming rate — and the cybercrime world is no different. Threat actors and various groups keep getting better — faster. Consequently, cybersecurity teams are battling on an overwhelming number of digital fronts. Whether it's a financial institution trying to cope with constantly increasing volumes of leaked credit cards, a hospital looking to patch its critical vulnerabilities, or an enterprise hoping to prevent the next data breach, the current approach to threat intelligence struggles to keep up with the realities of the cybercrime threat landscape.

Data from Dark Reading's *The State of Threat Intelligence 2021* survey indicates that while threat intelligence is maturing and prevalent at organizations, many struggle with data quality issues, the context around threats, and making intelligence data actionable within their security operations center (SOC) and other security functions.

And while the area of deep and dark threat intelligence is gaining traction across the cybersecurity industry, many are struggling with a large knowledge gap regarding Deep and Dark Web intelligence collection, the importance of intel freshness, and the speed and rate of collections — and their overall impact on an organization's cybersecurity programs and posture.

Key Findings

This study, conducted among 106 cybersecurity and IT professionals at global enterprises, found:

Threat intelligence is table stakes for enterprise cybersecurity.

- 77% of organizations have at least one dedicated threat intelligence analyst, and 54% have more than five.
- 48% of organizations struggle with inaccurate data and 46% with stale data.
- The top three use cases for threat intelligence are threat detection and protection, vulnerability management, and threat investigations/incident response.

Enterprises are drowning in threat intel data and intelligence-alerted incidents.

- Nearly half of organizations process 50 or more incidents in their SOC each month.
- 35% of organizations use seven or more threat feeds at a time.
- 95% of organizations waste anywhere from one hour to five days per week per analyst on false positives.
- Nearly one in five organizations say half or more of their threat reports are irrelevant to their business.

Many enterprises report lacking threat intelligence visibility into the Deep and Dark Web.

- 32% of organizations say their threat intelligence feeds commonly miss Deep Web source areas and 30% say they commonly miss Dark Web source areas.
- 40% say their threat intelligence sources do not cover instant messaging apps.
- 51% say their intel sources commonly miss closed forums, and 50% say their intel sources commonly miss foreign language forums.

Enterprises struggle to operationalize their threat intelligence.

- 40% of organizations cite lack of context as the biggest source of dissatisfaction in threat intelligence.
- 56% of organizations say their team spends at least 12 hours per week researching and synthesizing threat intelligence reports.
- 35% of organizations say it takes 12 hours or more to supplement new threat intelligence data with enough research to begin escalating and remediating incidents.

The Growing Role of Threat Intelligence in Enterprise Cybersecurity

The field of threat intelligence has quickly matured over recent years, and in 2021, it appears that threat intel occupies a crucial role within most enterprise security programs. The data from this survey shows undoubtedly that threat intelligence teams provide a baseline function and information lifeline for most security organizations today.

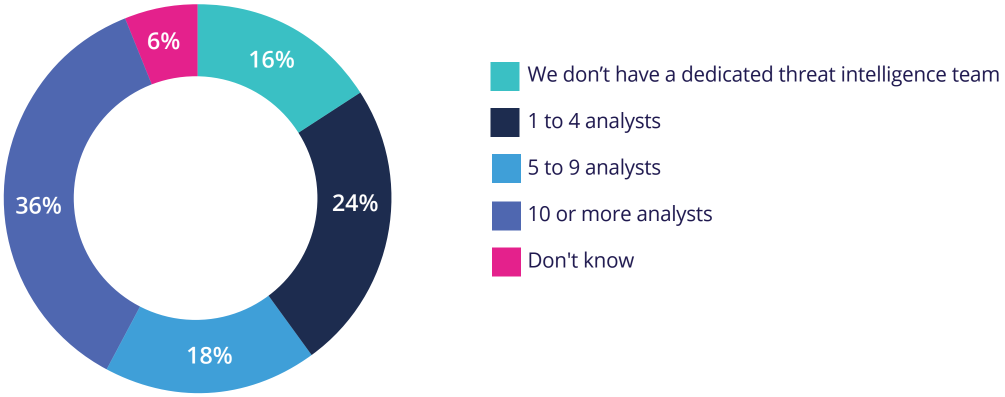
In querying large organizations, the study found that the majority of them — 78% — have at least one dedicated threat intelligence analyst on their team. Many have far more than that (Figure 1). More than half of organizations have five or more analysts dedicated to threat intel, and one in three organizations operate threat intel teams with 10 or more analysts.

These analysts support a range of important use cases within the enterprise. Unsurprisingly, the top named use case was threat detection and protection, which was far and away the most cited, with 64% of respondents naming this in their top three (Figure 2). The other two most commonly supported uses for threat intelligence were vulnerability management, named by 53% of organizations, and threat investigations and incident response, named by 44%. Clearly, threat intelligence serves a lot of purposes for security teams, as there were statistically significant findings for other important use cases, including prevention of leaked credentials, aiding automated threat blocking efforts, and informing strategic planning for cybersecurity roadmaps.

Figure 1

Threat Intelligence Analysts

How many threat intelligence analysts does your company employ?

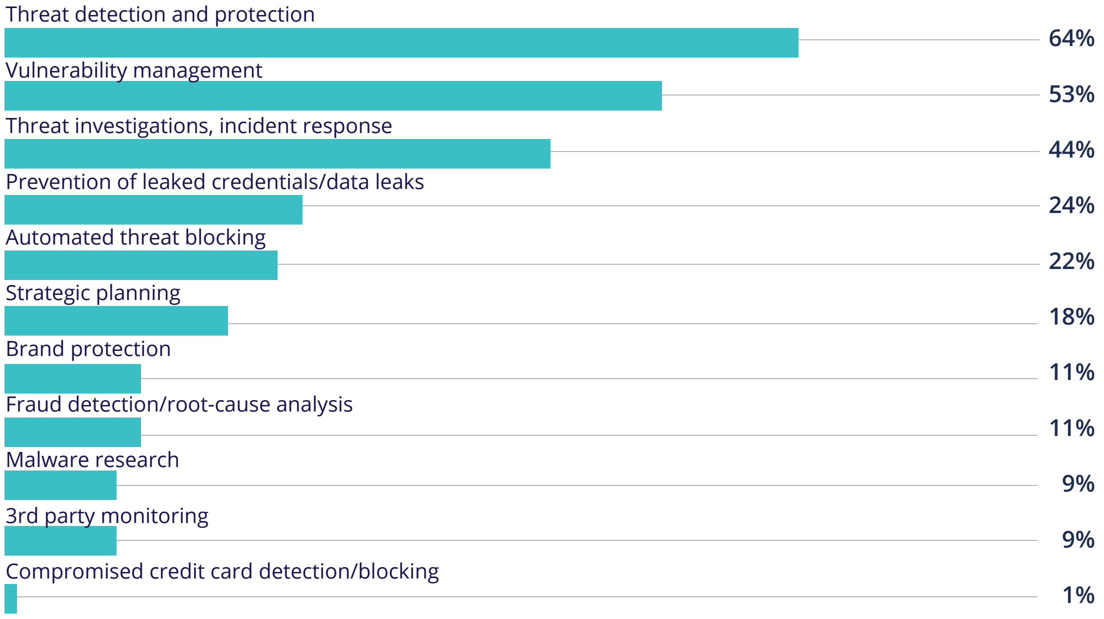


Data: Dark Reading survey of 106 cybersecurity and IT professionals at companies with 1,000 or more employees, November 2020

Figure 2

Primary Use Cases for Threat Intelligence

What are the primary use cases for threat intelligence in your organization?



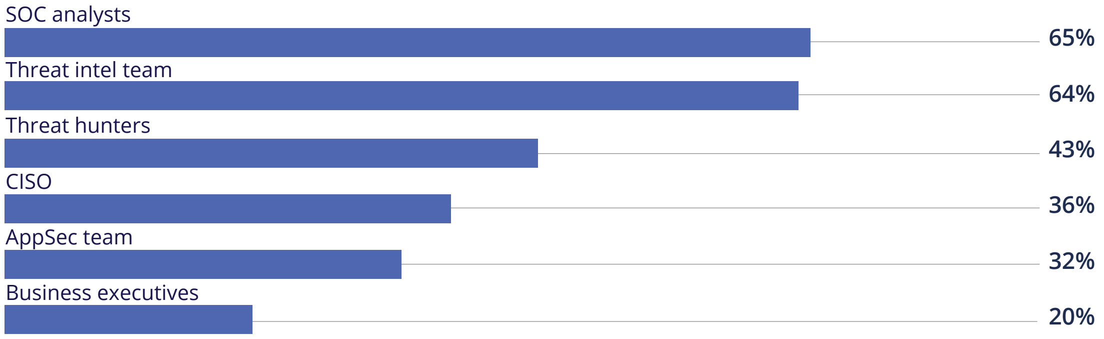
Note: Maximum of three responses allowed
Data: Dark Reading survey of 106 cybersecurity and IT professionals at companies with 1,000 or more employees, November 2020

With threat intelligence touching so many different aspects of the modern information security program, it should come as no surprise that there's a lot of different sets of eyes turned toward threat feeds today. A number of different enterprise stakeholders consume information in threat intelligence reports, with the two most cited audiences being SOC analysts (65%) and threat intelligence team members (64%) (Figure 3). Typically, the information flow doesn't stop at these specialists, as the survey shows other important audiences include the chief information security officer (CISO), business executives, and the application

Figure 3

Threat Intelligence Reports

Who consumes your threat intelligence reports?



Note: Multiple responses allowed
Data: Dark Reading survey of 106 cybersecurity and IT professionals at companies with 1,000 or more employees, November 2020

security (AppSec) team — all of whom likely consume curated intel after the intelligence team digests it.

Clearly, most organizations are putting at least some level of commitment and investment toward threat intelligence in 2021. The question is, how effective are they in squeezing benefits out of their threat intelligence data sources?

The State of Threat Intelligence 2021 survey shows some conflicting data that indicates many organizations understand the value and necessity of threat intelligence capabilities but may lack the maturity or visibility to fully understand where their threat intel deficiencies currently lie.

Data from this survey and other industry studies suggest problems with threat intelligence sources that people may not even realize they have. One of the biggest signs that there's still room for improvement is that, when the rubber meets the road, some 66% of organizations report that they've had at least one major security incident or data breach in the last year, with 13% admitting they've had more than 10 major incidents or breaches (Figure 4). Perhaps the most troubling red flag is that another 13% admit they don't know how many or even whether they've had a major breach in the past year. With this type of lackluster performance as it pertains to threat detection and protection — the No. 1 use case for threat intelligence — it's only rational to surmise that satisfaction levels may well be decoupled from the actual efficacy of their threat intel.

This makes sense considering that just last year SANS Institute found that a scant 4.2% of organizations measure the effectiveness of their threat intelligence sources and processes. More than likely, a significant knowledge gap still exists between what's available from leading threat intelligence sources today and what leading practices really look like.

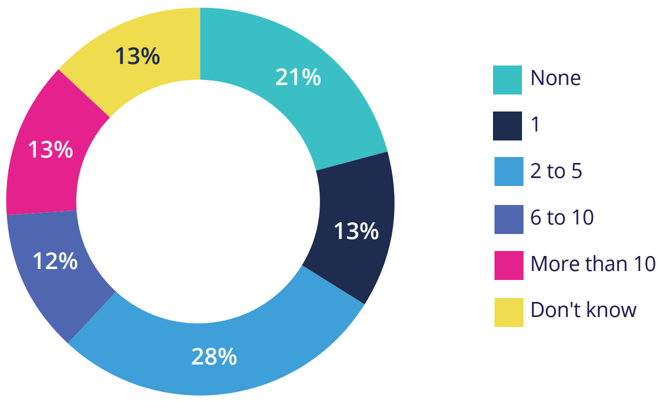
Common Threat Feed Challenges

Organizations are processing vast amounts of threat information, alerts, and security incidents alerted by threat intel

Figure 4

Major Security Incidents or Breaches

How many major security incidents or breaches has your organization experienced in the last 12 months?



Data: Dark Reading survey of 106 cybersecurity and IT professionals at companies with 1,000 or more employees, November 2020

sources. According to *The State of Threat Intelligence 2021* survey respondents, 60% of organizations are processing at least 25 SOC incidents per month. Almost one in three deal with 100 incidents per month, and some 16% process 500 or more unique security incidents per month.

As organizations are alerted to and work these incidents, they're dealing with a firehose of threat intel data streaming in from various fronts. A solid 81% of organizations subscribe to and ingest more than one threat feed, with 35% utilizing more than seven at a time.

Unfortunately, all of that threat data is often full of irrelevant and faulty data. The amount of time that threat intelligence analysts are spending sifting the good from the bad, running down false positives, trying to contextualize sparse details with further research, and generally spinning their wheels on unvetted and faulty sources of intelligence is adding up.

According to the survey, 95% of organizations waste at least an hour per week per analyst on false positives (Figure 5). Forty-three percent say that every analyst spends 12 hours or more per week chasing down false positives, and of that, 15% say each analyst wastes at least two full days a week on them.

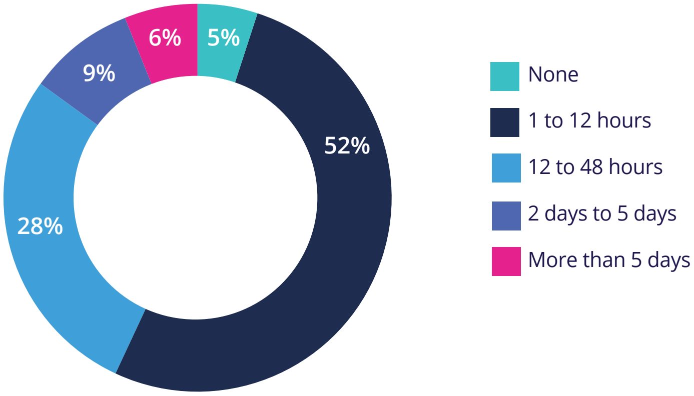
False positives, false negatives, and other time-wasting elements of threat intelligence are driven by a number of root-cause quality problems. The most commonly cited quality problem with threat intelligence sources is inaccurate data, but there is a fairly even spread of other cited problems. Other common issues in order of respondents' perceived severity is irrelevance to the technical environment, stale data, a lack of contextual information, and irrelevant business or industry context.

Frequently, teams also waste time on highly irrelevant threat reports. The survey shows that over three in four organizations admit at least 10% of their threat reports are irrelevant to their business. More troubling, nearly one in five organizations say half or more of their threat reports are irrelevant to them.

Figure 5

Time Wasted by False Positives

How much time do false positives waste at your organization (per week, per analyst)?

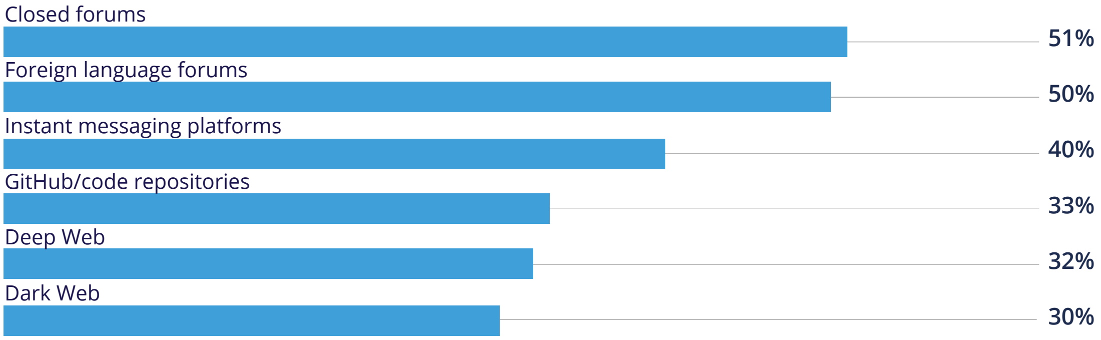


Data: Dark Reading survey of 106 cybersecurity and IT professionals at companies with 1,000 or more employees, November 2020

Figure 6

Most Commonly Missed Threat Intel Data Sources

Which threat intelligence data source areas do your feeds most commonly miss in their coverage?



Note: Multiple responses allowed
Data: Dark Reading survey of 106 cybersecurity and IT professionals at companies with 1,000 or more employees, November 2020

Threat intel can be irrelevant to a business on numerous fronts. The reported threat could be operating in a different business context or environment than the organization operates in. It could be operating within technical environments and platforms that the organization doesn't use. Or it could be targeting systems that the organization uses but with configurations that aren't relevant to them.

When there's a high volume of irrelevant reports within an intelligence source and not enough context or other mechanisms to easily filter them out, that's when organizations start to lose value from their threat intelligence function.

Clear Web vs. Deep and Dark Web Divide

The paradox of threat intelligence today is that while organizations are often drowning in threat information, many threat intel reports still commonly miss critical pieces of data.

Today's typical threat intel sources do a good job of covering areas like the Clear Web or sources gathered via open-source intelligence (OSINT) methodologies. This makes sense as the Clear Web is the obvious "low-hanging fruit" for security researchers to harvest with minimal time, effort, and expertise.

But this leaves areas like the Deep and Dark Web (DDW) less explored by many threat intelligence feeds. Thirty percent of organizations admit that their threat intel sources do not cover the Dark Web, and 32% report that their threat intelligence feeds most commonly miss Deep Web sources in their coverage (Figure 6).

This is extremely problematic, as cybercriminals tend to prefer to do much of their work under the cloak of the DDW. Whether it is buying and selling hacking tools on hidden marketplaces, sharing criminal tips on obscure forums, or otherwise setting up underground backchannels for communication, the DDW is where signs of new tactics, techniques, and procedures (TTP) and newly extant threat groups tend to surface first. In fact, in a different analysis conducted by Cybersixgill researchers, as the cybercriminal world geared up to leverage the chaos of the COVID-19 crisis in 2020, there was a corresponding 44% surge in Dark Web forum activity.

This cybercrime pattern puts most organizations in a precarious spot when it comes to threat intelligence. *The State of Threat Intelligence 2021* survey showed that the top two intelligence data sources commonly missed in threat intelligence source coverage are closed forums and foreign language forums used by cybercriminals and black hat hackers — which happen to be two of the favored channels for threat actors today.

Many organizations are cognizant of this DDW gap in threat intelligence and currently have a long wish list of sources they'd like to be covered soon. Topping the list are the Deep Web and Dark Web, cited by 65% and 62% of respondents respectively. Other commonly cited sources on those wish lists include more coverage thorough OSINT, the Clear Web, and instant messaging.

Making Threat Intelligence Relevant and Actionable

According to the SANS Institute, there are a number of key obstacles that prevent organizations from getting the most out of their threat intelligence sources, including a lack of trained staff, a lack of time, a lack of funding, and a lack of automation. *The State of Threat Intelligence 2021* survey indicates that large organizations are actively looking for better ways to overcome these obstacles, with varying degrees of success.

Survey responses show that organizations are constantly seeking technology and methods to better operationalize threat intelligence. Key to that is finding ways to make intel more relevant and actionable.

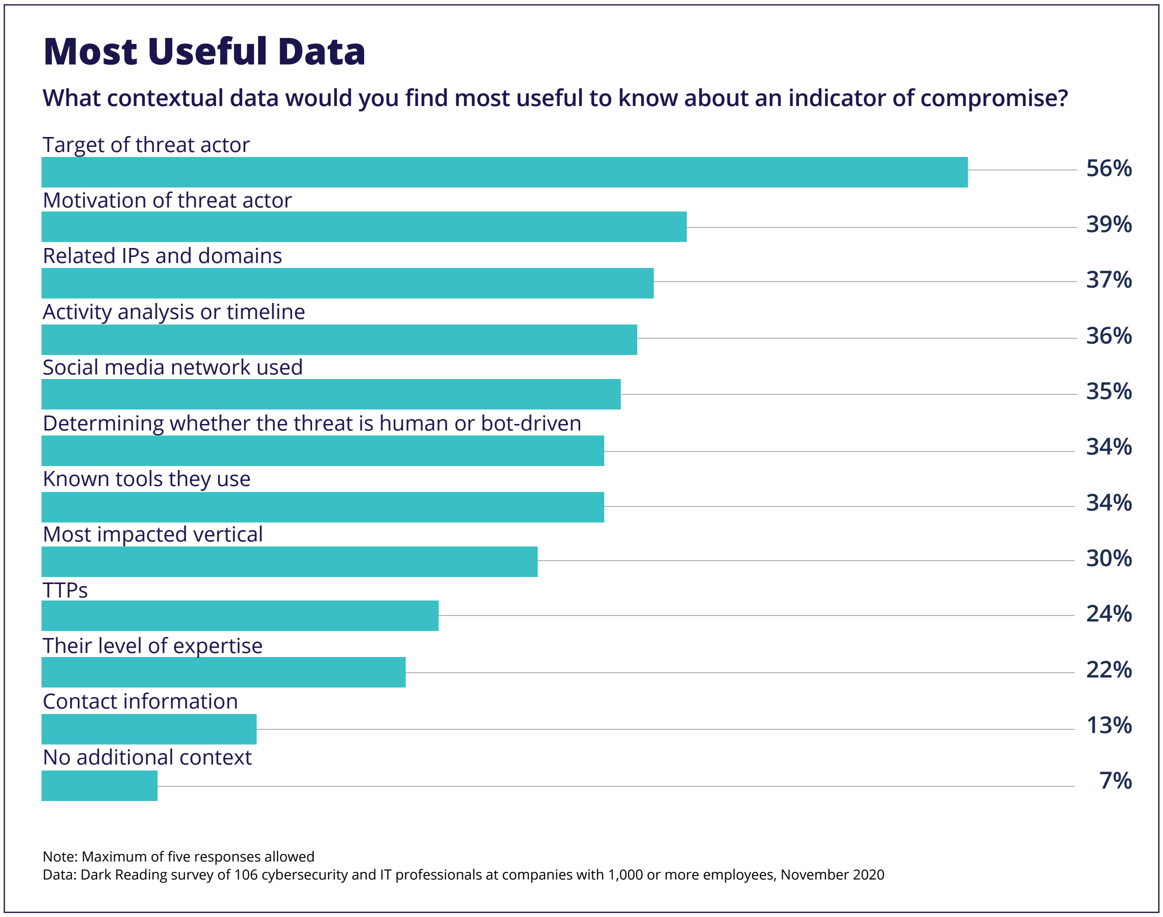
With so many organizations utilizing multiple threat feeds, overlapping threat information is inevitable. Currently, 46% of organizations report that they're using technology to automate that process — this explains the surge in security orchestration and response (SOAR) platforms that the market has seen in the last year. However, there's still a lot of work to be done, as 35% of organizations say they spend a moderate to significant amount of manual effort deduplicating overlapping threat information.

As previously mentioned, a lack of context around threat intelligence data is one of the big sticking points for threat intel teams today. Some 40% of all organizations cite this as the biggest source of dissatisfaction in threat intelligence reports. Conducting additional research to supplement reports with added threat context and synthesizing threat intelligence data take many threat intel teams significant amounts of person-hours each week. Approximately 56% of organizations say that their team spends at least 12 hours per week doing this kind of digesting and contextualization.

The most time-consuming activities in this process include confirming the accuracy of data, making it actionable, and enriching data with further research. All of these activities add a significant lag between when most organizations receive new intel and when they've processed it enough to actually act on it. Today, few security teams can act swiftly on threat intel data.

Approximately 35% of organizations say it takes 12 hours or more to supplement new threat intelligence data with enough research for the team to begin escalating and remediating an

Figure 7



Note: Maximum of five responses allowed
Data: Dark Reading survey of 106 cybersecurity and IT professionals at companies with 1,000 or more employees, November 2020

incident. And one in ten admit that it takes two or more days to do so.

Security teams want more context for indicators of compromise provided in threat reports (Figure 7). The top five pieces of contextual data they want included are:

- Target of threat actor
- Motivation of threat actor
- Related Internet protocol addresses (IPs) and domains
- Activity analysis or timeline
- Social media network used

At the same time, though, enterprises grappling with operationalizing threat intel thirst for more digestible reports.

With so much data, not enough context, and tons of irrelevant reports to cull from their feeds, it becomes a heavy lift for organizations to pull out the most important insights their teams need to know to proactively defend against and respond to the latest threats.

This is no doubt why 59% of organizations prefer the convenience of curated and digested threat reports, despite compromising on the robustness and broadness of data that would be offered by a continuous flow of raw threat intel data. Nevertheless, most organizations still aspire to have the full package — a feed of raw data full of context that could be provided in a curated manner.

Recommendations

The only way for today's security teams to effectively process the huge amount of threat intelligence data they need to digest is by implementing a modern threat intelligence methodology that is continuous, fast, iterative, and smart. This means automating collection, analysis, research, and response to minimize the amount of manual labor it takes to truly operationalize threat intelligence.

The optimal methodology should be:

Real-time and Complete

Data should be collected in real time and include sources in the DDW.

Contextual

Intelligence data points should be processed, structured, and correlated with other data sets to connect the dots and establish a bigger picture about the threats.

Operationally Integrated

All intelligence feeds should be integrated within a broader security platform so that every meaningful data point triggers an action to mitigate the threat.

Iterative and Continuous

Threat intelligence capabilities should be built so that teams can constantly and proactively respond to the most updated threat intelligence picture.

About Cybersixgill

Cybersixgill's fully automated threat intelligence solutions help organizations fight cyber crime, detect phishing, data leaks, fraud and vulnerabilities as well as amplify incident response – in real-time. The Cybersixgill Investigative Portal empowers security teams with contextual and actionable insights as well as the ability to conduct real-time investigations. Rich data feeds such as Darkfeed™ and DVE Score™ harness Cybersixgill's unmatched intelligence collection capabilities and deliver real-time intel into organizations' existing security systems. Most recently, Cybersixgill introduced agility to threat intel with their CI/CP methodology (Continuous Investigation/Continuous Protection). Current customers include enterprises, financial services, MSSPs, governments and law enforcement entities.

Learn more at **cybersixgill.com**

Survey Methodology

Dark Reading conducted an online survey on behalf of Cybersixgill in November 2020 to explore organizations' responses to cybersecurity incidences and trends in threat intelligence.

The final data set is comprised of 106 individuals with IT and cybersecurity job titles such as CIO/CTO, IT director/manager, CSO/CISO, cybersecurity director/manager, threat intelligence personnel, and chief privacy officer. All respondents in the dataset used for this report work at companies with 1,000 or more employees and are located predominantly at North American organizations. Respondents represent more than 16 industries including banking and financial services, healthcare, government, education, communications, and non-IT manufacturing.

Informa Tech research was responsible for all aspects of survey administration, data collection, and data analysis. Informa is the parent company of Dark Reading. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.