Top Five Areas Where Intelligence Bolsters Your Security

Recorded Future® | CYBERSECURITY DIVE | Custom content for Recorded Future by studioID

Defending enterprises against modern cybercriminals — who are plentiful, well-resourced, persistent and endlessly inventive — has never been an easy task. But 2020's events, including the global coronavirus pandemic, the sudden and unexpected shift to remote work and a dramatic acceleration in the growth of the digital economy, have multiplied the challenges that security programs face.

In today's world, cybercrime is big business: Damages inflicted by cybercriminals are predicted to cost victims $6 trillion globally in 2021, according to Cybersecurity Ventures. Losses from cybercrime are exponentially larger than the costs associated with natural disasters, and they are said to be more profitable on a worldwide scale than the entirety of the illegal drug trade.

This continues to be the case even though defenders have access to more tools, technologies and data than they've ever had in the past. Network telemetry and monitoring infrastructures are more comprehensive, automated solutions are more sophisticated, threat intelligence feeds are more plentiful, and security operations (SecOps) teams are collecting and aggregating more log data.

But these technological advances haven't turned the tide in the war against cybercrime. In fact, maintaining an effective enterprise security program is more challenging than ever. According to research conducted by the Ponemon Institute, past a certain point, organizations with more tools are actually less able to detect and respond to attacks than those running fewer solutions. The average enterprise now maintains 45 distinct security technologies. Organizations with 50 or more tools rank 8% lower in their ability to detect an attack and 7% lower in their ability to respond to an attack than organizations with fewer than 50 tools.

What factors account for this diminishing return on investments in cybersecurity? In large part, it's due to information overload. Having more tools means that cybersecurity practitioners confront more data, alerts and events, many of which are false positives. They won't necessarily have a better view of the environment. They won't have a more accurate understanding of the threat landscape in which the business operates, or a firmer grasp on how to prioritize their time and attention.

Contemporary security programs are invariably resource-constrained, particularly when it comes to the time and attention of experienced professionals. With more than 3.1 million cybersecurity positions unfilled worldwide, according to (ICS)2, it's vital that lean teams understand how to direct their efforts where they'll have the biggest impact. To do so, they'll need to recognize which information is most worthy of their attention —what is signal and what is noise.

Statistician and election forecaster Nate Silver has written, "In less than a second, we humans are producing the equivalent of the amount of data that the Library of Congress has in its entire print collection. But most of it is [useless]. Distinguishing the signal from the noise requires both scientific knowledge and self-knowledge."

In cybersecurity, intelligence solves exactly this problem. It enables a deeper and more scientific understanding of the external and internal threat landscape that lets professionals prioritize what matters the most.

Intelligence Is the Answer

In purpose and content, intelligence goes far beyond the traditional threat intel feed. It's part of an outcomes-centric approach to reducing risk that fuses internal and external threat, security and business insights that are relevant across the enterprise. It's contextualized and actionable. This intelligence doesn't complicate the decision-making process. Rather, it enriches knowledge. It's designed with a purpose: to enable fast, informed decision-making and effective action.

Historically, threat intelligence was operational. Intel feeds were composed of technical details such as malware file hashes or IP addresses that are associated with malicious activity. This is useful information, to be sure, but needs to be cleaned and curated before it becomes usable within a security program. All too often, raw threat intelligence feeds are full of irrelevant, inaccurate, redundant or out-of-date information, none of which should guide real-world decisions.

"Threat intelligence originated from a need and a promise," says John Wetzel, director of intelligence solutions at Recorded Future. "The promise was that if we defenders all shared all of the indicators that we all had amongst ourselves, we could make the world a better and safer place. The challenge was: How do we actually do this?"

"When people started collecting data, two things happened that they weren't expecting," he adds. "The first is that they got more data than they could handle. No one anticipated the current volumes of external threat data. And the second is that there was a lack of context around that data. But context was desperately needed. Without context, you can't drive insight that leads to right action. Instead, all you've created is overwhelming noise."

Today's most useful intelligence is different. It's a strategic asset that can guide both high-level executive decisions and operational choices made by security, IT and risk management teams. Its sources are internal and external, technical and human, and global as well as local. The goal is to crystalize value from large volumes of information for the benefit of the business and the security community as a whole.

Intelligence needs to be...

- Embedded within collaborative processes and frameworks
- Able to provide full, 360-degree visibility
- Automated and extensively integrated with other security technologies, such as security information and event management (SIEM) and security orchestration, automation and response (SOAR)
- Wholly aligned with the organization and its security team's most important use cases

While traditional threat intelligence feeds were primarily consumed by SecOps teams and threat hunters, intelligence is far more broadly applicable. Its beneficiaries are SecOps teams, risk managers, vulnerability management teams and IT operations teams, of course. But because it casts light on business risk, it's useful anywhere that business decisions are made.

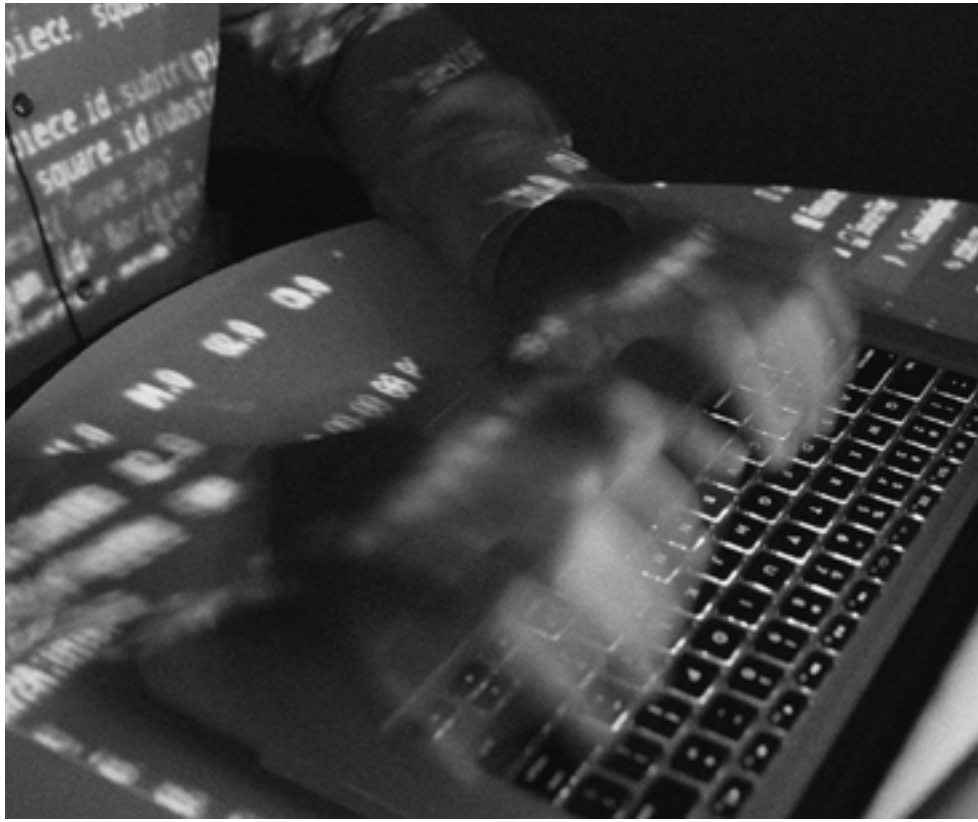
Here are five key places where you can and should incorporate intelligence into your enterprise security program:

1.

Security Operations: Infusing Intelligence Enhances Efficiency and Effectiveness

Security operations centers (SOCs) are chronically understaffed, and security analysts have fast-paced, stressful and often thankless jobs. According to research from Exabeam, 39% of security analysts report that the SOC in which they work is short of essential personnel, with 50% of these saying that their team needs six or more additional employees. As a result, individual security analysts chronically confront high volumes of events and alerts. It's simply impossible to investigate each one in the limited time they have.

Inevitably, security analysts must make careful, prioritized choices about how they're spending their time and attention. A recent study conducted by Cisco reveals that the average SecOps team investigates only 48% of the alerts it receives; among these, only 26% are found to have any value or legitimacy. In these circumstances, security analysts are always at risk of making mistakes—it's all too easy to ignore a true positive or spend too much time on what turns out to be a red herring.



The primary decisions that must be made when triaging and investigating alerts are about relevance and context. With accurate intelligence close at hand, it's possible to tell almost at a glance whether or not a particular event is likely to be malicious. This sort of contextual information enables analysts to correlate events with activity patterns both inside and outside of their environment. It makes it possible to answer questions like: Does this pattern resemble tactics or techniques that attackers are known to use? Does this chain of events seem like reconnaissance, lateral movement or another typical attack stage?

"Intelligence gives you a window into the adversaries' thinking," says Wetzel. "It gives analysts an understanding of what they're likely to target within an environment before they actually get there. This kind of critical context makes it possible for security operations teams to move much faster. It's really a force multiplier, because in SecOps, speed is everything."

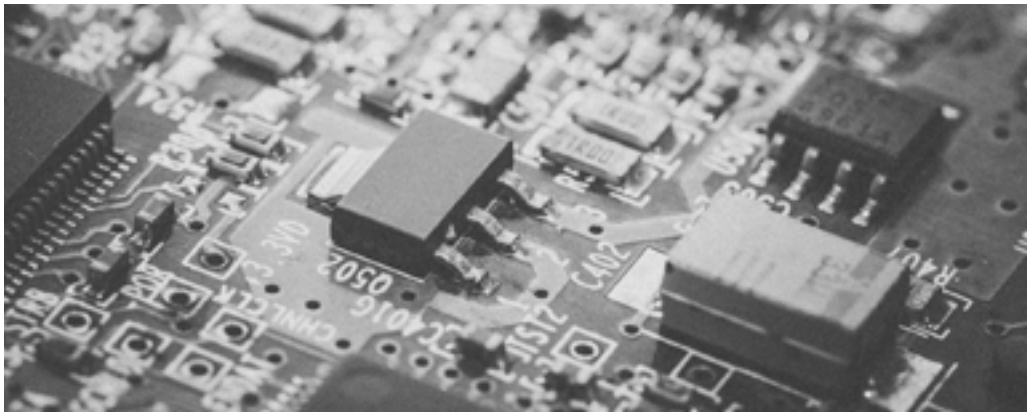
Not only can actionable and accurate intelligence enable security analysts to make better decisions faster, but it can also substantially reduce false positive rates when properly integrated with security platforms. This doesn't just mean ingesting more threat feeds into your SIEM, though. It means choosing the most pertinent and best-curated information sources. Feeds that don't include relevant context will simply increase your false positive rates.

Integrating intelligence into analyst workflows in SIEM and SOAR tools makes it possible for security professionals to work smarter instead of harder. They'll see fewer false positives and improved efficiency. In addition, incident responders can prepare playbooks in advance—on the basis of intelligence they're confident is accurate—for responding to threats that are most likely to impact their organization. This can dramatically increase the speed at which teams can operate.

2. Vulnerability Management: Smarter Patching Better Addresses Real-World Risks

Today's IT and security professionals are increasingly challenged to patch software vulnerabilities in a timely fashion, even though it's well known that vulnerabilities for which a patch had long been available are exploited in a significant percentage of breaches. 77% of the respondents to a Ponemon Institute survey said that their organization simply didn't have enough resources to keep up with the volume of patches that need to be applied. This represents a 5% increase from what enterprise security teams reported just two years ago. And it's occurring despite the fact that enterprise teams now spend an average of 206 hours per week patching applications and systems at an average weekly labor cost of $12,875.

It requires gargantuan effort to keep up with the torrent of vulnerabilities that are assigned Common Vulnerabilities and Exploitations (CVE) scores each year. Roughly 18,000 such vulnerabilities were reported in 2020, and nearly 60% of these were considered "high" or "critical" priority. Despite the sense of urgency this situation creates, a mere 5.5% of these are known to have actually been exploited by threat actors. And many of these weren't even assigned the highest CVE scores. This small subset of vulnerabilities does, however, tend to be used over and over again in attacks.



This means that if vulnerability management teams could identify in advance the few vulnerabilities that attackers will target most often, they could save themselves massive amounts of time and effort—reducing more risk with fewer patches.

With intelligence, your team can figure out which vulnerabilities are actually being weaponized and exploited, and which ones adversaries are ignoring. In addition, tailoring intelligence to your own technology stack allows you to discover newly disclosed vulnerabilities long before they're added to the National Vulnerability Database. This allows your organization to stay in front of new, high risk vulnerabilities.

3. Threat Intelligence: Knowing Your Enemy Enhances Risk Analysis

Threat intelligence is the traditional foundation of intelligence. This is where several of the core concepts in intelligence originated—including tracking local, regional and global attack trends, attempting to understand how cybercriminals think and operate, and making efforts to infuse this information into defensive strategies.

Understanding, for example, that 55% of breaches can be attributed to organized criminal groups—as the Verizon Data Breach Investigations Report tells us—reveals a need for greater insight into which tactics, techniques and procedures (TTP) these attackers are most likely to employ and which companies, in which verticals, they're most likely to target. Such situational awareness can then be used to inform threat hunting as well as risk analytics. It's also obviously useful for SecOps programs.

Most traditional threat intelligence comes in a form that isn't easy to consume, though. This usually comes from two sets of sources: threat feeds, which comprise long lists of IP addresses to block and indicators of compromise (IOCs) to watch out for, and long-form reports that detail the activities of a particular advanced persistent threat (APT) group or actor.

"Traditional threat intelligence is quite flawed" says Trevor Lyness, product marketing manager at Recorded Future. "Threat feeds lack context and evidence, making it difficult to trust the information you're getting. Often, they just pass along a list of 'bad things' without showing why something is malicious or how it's relevant to your organization. Threat reports, on the other hand, lack timeliness. In other words, they often become outdated the moment they're published. They're also written by human analysts, making them subject to analytical error or bias. Finally, most threat reports are informative, but not actionable or easily understood by executives."

"Threat information only becomes useful as intelligence when it's enriched with context and backed by evidence—and when it's crystal clear how to act upon it. That might not enable an individual team member to single-handedly stop attacks, but it does amplify the security team's overall effectiveness."

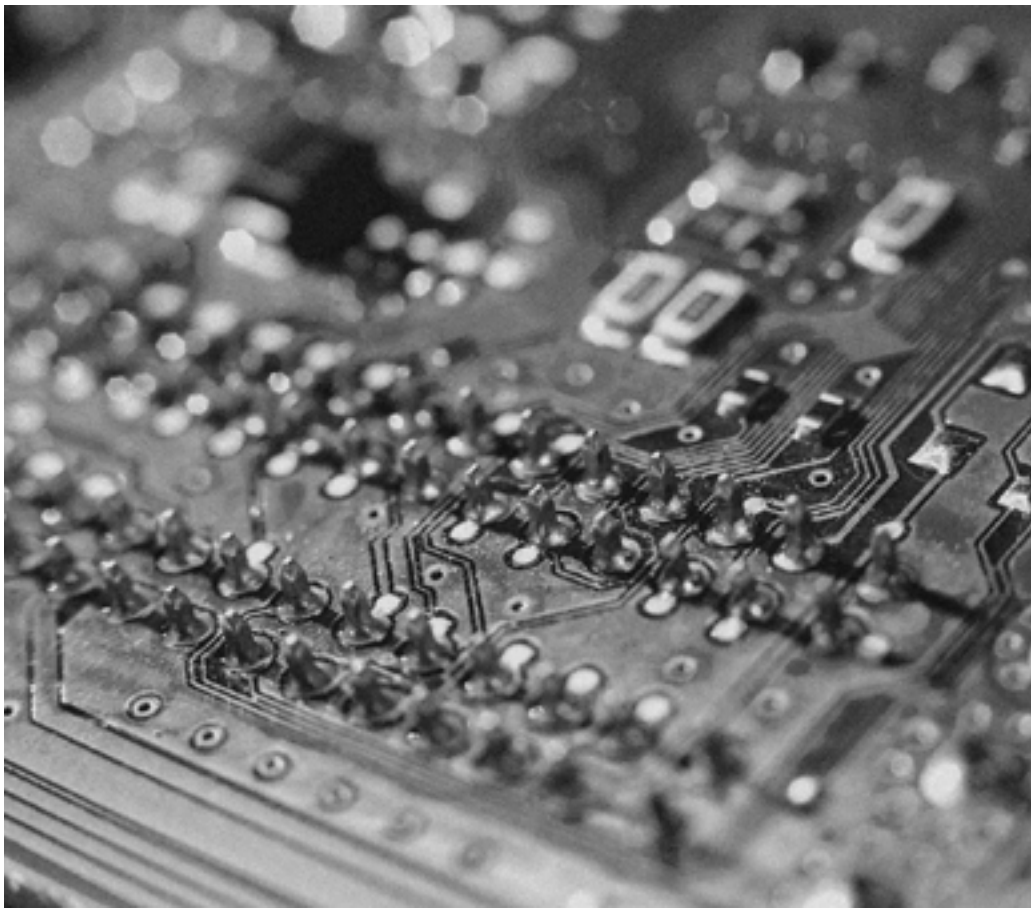
Finding external and internal threat information that's current and accurate has long been considered part of the threat hunting function. But threat hunters haven't always had access to the best sources. Such sources can save time and labor because there are no mistakes, duplicate entries or irrelevant inclusions, and they provide ample context for every data point they include.

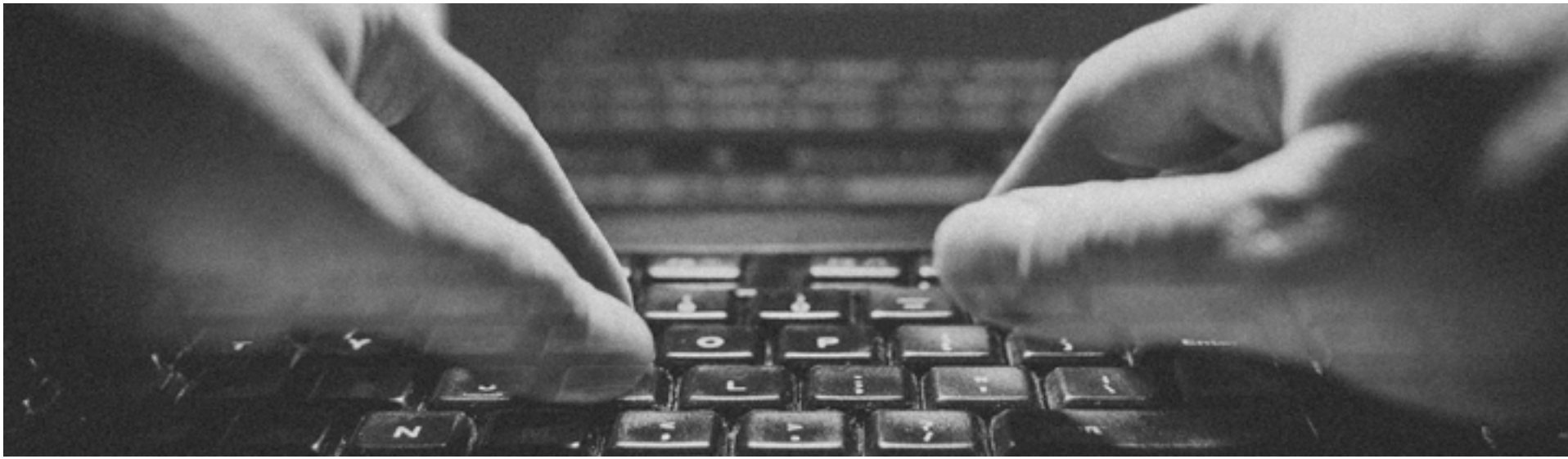
4. Managing Third-Party Risk: Protecting the Enterprise Is Vital in an Interconnected World

As recent events—including the devastating SolarWinds breach and the far-reaching Kaseya ransomware attack—have amply demonstrated, third-party risk is omnipresent. It's also nearly impossible to eliminate and is challenging even to measure, let alone mitigate. Every enterprise today relies on vendors and partners, and IT ecosystems are increasingly interconnected, extending far beyond what were once the defined boundaries of the corporate network.

Although third-party risks are unquestionably real and significant, few organizations have tools and processes that are adequate to manage them. According to a Ponemon Institute study, 58% of organizations don't have a formal third-party risk management program at all. And 53% report that their methods for managing third-party risk are either "only somewhat effective" or are entirely ineffective.

Traditional risk assessments, which usually take the form of questionnaires, are static and rely on self-reported information. This falls far short of what's needed. Too many organizations don't understand their own vulnerabilities and risks well enough to be able to disclose them, even if they were willing to do so.





"It's hard enough managing your own security posture," Lyness says. "Imagine trying to control someone else's. The best you can do is try to assess and make recommendations, or maybe enforce contractual obligations. But someone might think they have a great vulnerability management program when in fact they have a bunch of systems that are discoverable and unpatched and have been for a long time. External third-party intelligence can give you a much more objective lens through which you can see what the third party is doing."

With externally sourced intelligence, you'll have much deeper insights into your current risks as well as those that your vendors and partners face but might not be aware of. By curating information that's available to the public, as well as what's disclosed on the Dark Web, alongside technical sources, you'll quickly gain a picture of a third-party's security posture. Intelligence provides forewarning if a breach does occur, or if new risks arise after a contract is signed.

In this arena, too, timeliness is key: If a vendor or partner is breached, you need to learn about it as quickly as possible so you can rapidly assess its impact (if any) on your organization. This intelligence can potentially mitigate legal and financial risks in a crisis—and it bolsters your ability to protect sensitive data and other valuable information.

5.

Brand Protection: Safeguarding the Value of Your Good Name Has Long-Term Benefits

The value of an online brand has never been more critical for success—or more important to protect—than it is in the modern digital business era. It can take years of painstaking effort—and careful marketing strategies—to build a reputation for trustworthiness, reliability and product quality. But a single phishing campaign employing a counterfeit version of your website and logo can do immeasurable damage to the brand reputation you've so carefully cultivated. So can brand impersonations on social media, where criminals pretend to be part of your organization so they can steal customer information or directly cause reputational damage.

But figuring out that these kinds of activities are taking place is far from easy because brand attacks live outside your organization's network. Cybercriminals can rely on fraudulent domains to take advantage of your customers without needing to hack, trick your employees or gain any kind of access to your systems. Stolen or counterfeit intellectual property can circulate for years before you become aware of the issue, if you find out at all. In fact, many organizations suffer data breaches without ever becoming aware that their digital assets have been stolen.

Hunting for evidence that your brand has been impersonated online is a time-consuming process that requires extensive

expertise and familiarity with the cybercriminal underground. Plus, it needs to be ongoing: You can't conduct a single search for information and conclude that your brand is safe simply because nothing appeared at that time.

Brand intelligence automatically searches the deepest corners of the open web, Dark Web, and technical sources to detect when your company, products, executives, or customers are attacked. It can even comb through underground criminal forums for chatter indicating that threat actors have set their sights on your enterprise. What's more, a brand intelligence solution may be able to alert you that a data breach is in progress, limiting your exposure and reducing damage to your brand.

Conclusion

Today's enterprise security programs face formidable challenges. As technologies evolve and increase in complexity, the attack surface continues to grow while headcounts remain stagnant. It's no easier to find, hire and retain talented cybersecurity professionals than it was a few years ago. This means that security leaders must find ways to accomplish more with the same number of people.

The only way to achieve this aim consistently is to work smarter and not harder. Security programs must rely on intelligence that can guide them in applying their efforts where they'll have the biggest impact. With access to the right intelligence sources—timely, relevant, in context and presented in a manner that makes them easy to understand and use to drive action—it will finally be possible for security teams to gain the upper hand over attackers.

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

LEARN MORE

studio / ID

BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

LEARN MORE