IronNet™

CYBERSECURITY MARKET INSIGHTS:

What is **attack intelligence** and why do you need it?

IronNet.com | info@IronNet.com | (443) 300-6761

Executive Summary

In Spring 2021, IronNet commissioned the independent research firm Sapio to survey 473 IT security decision makers in the technology, public services, financial, and utilities sectors across the United States, United Kingdom, and Singapore. This 2021 Cybersecurity Impact Report revealed an interesting paradox. While most survey respondents (90%) indicated that the security posture of their company had improved in the past two years, 86% reported a cybersecurity incident so severe in the past year that it required a C-level or Board meeting.

Why is there a false sense of security? More important, what is the disconnect between a reportedly high level of confidence in existing controls and the fact that attacks continue to pummel companies of all sizes?

One reason for this paradox, in my opinion, is the lack of what I am calling "attack intelligence," or collective threat intelligence. What do I mean? This type of heightened threat intelligence is the combination of threat detection based on behavioral analytics, which can identify anomalies in network traffic, and Collective Defense based on visibility and real-time collaboration.

In short, attack intelligence delivers threat information that is three things **at once:**

- **Timely:** you need speed when it comes to both detection and triage
- **Relevant:** you need meaningful threats to emerge from information overload
- **Actionable:** you need situational context around detected anomalies

How is actionable attack intelligence different from traditional threat intelligence?

It's simple: threat intelligence, while still a very valuable element of cybersecurity, is "what could happen to me." Attack intelligence, on the other hand, describes "what is happening to me, or is happening to someone that looks like me, or is happening in my supply chain."

Threat intelligence basically tells security analysts that there are a lot of adversaries out there who can do a lot of bad things if they get in your network. It is not specific enough, and it is not normally timely enough, to allow them to focus limited cyber resources on the threats most likely to impact your specific business.

It is my hope that focusing threat intelligence on timely, relevant, and actionable threat information can mature every enterprise's security posture. The promise of actionable attack intelligence is far-reaching. In fact, "IT security professionals think that better detection technology (44%) and better infrastructure for information sharing (41%) would have helped companies in the context of the SolarWinds attack" (2021 Cybersecurity Impact Report). Actionable attack intelligence fills that void by giving you real-time and dynamic visibility over the entire attack surface that is relevant to you.

This market insights report covers the following topics to assist you in discovering the value of attack intelligence and the tools you need to implement it to improve and strengthen the cybersecurity posture of your enterprise or organization:

- **What is attack intelligence?**
- **What are the four characteristics that make attack intelligence actionable?**
- **What are the operational benefits of attack intelligence?**
- **How is attack intelligence different from threat intelligence?**
- **How do you gain actionable attack intelligence?**
- **What is the difference between attack intelligence through Collective Defense and threat intelligence from threat-sharing groups?**

Major General (Retired) Brett T. Williams is a co-founder of IronNet, Inc. IronNet delivers the power of collective cybersecurity to defend companies, sectors and Nations. He served nearly 33 years in the U.S. Air Force, and his last assignment was Director of Operations, U.S. Cyber Command. In that position, he was responsible for the operations and defense of Department of Defense networks as well as the planning and execution of offensive actions in support of national security objectives. General Williams is a highly experienced fighter pilot with more than100 combat missions in the F-15C. In addition, he held several large operational commands to include Commander of the Air Force's largest combat wing located in Okinawa Japan.

Can cyber threat intelligence **keep up?**

By Gartner's industry definition, threat intelligence is "evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets. CISOs should plan for current threats, as well as those that could emerge in the long term (e.g., in three years)."

Although it is a long-standing and valuable resource, traditional cyber threat intelligence often is not effective enough to keep up with the volume and speed of today's threats. There are three criteria needed *at once* to allow analysts to better capture and communicate knowledge of unknown threats in time to thwart network attacks in the early stages of intrusion:

- **Timely:** you need speed when it comes to both detection and triage
- **Relevant:** you need meaningful threats to emerge from information overload
- **Actionable:** you need situational context around detected anomalies

What is **attack intelligence?**

In short, actionable attack intelligence reveals what is happening in your network vs. what could happen.

By combining threat detection based on behavioral analytics and Collective Defense based on real-time visibility and crowdsourced collaboration among organizations, actionable attack intelligence closes the air gap of traditional threat intelligence platforms, tools, and feeds.

Being able to access attack intelligence at network speed is key for gaining the ability to take meaningful, proactive action. In fact,

How can threat information become timely, relevant, and actionable? The answer is attack intelligence. It allows analysts to see and respond to threats well before adversaries achieve their endgame: ransom, exfiltration, system exploitation, and/or successful social engineering campaigns.

The need for attack intelligence is urgent. A Ponemon Institute study, for instance, revealed that, "Timeliness of threat intelligence is critical but not achieved. Only 11 percent of respondents say threat intelligence is provided real time and only 13 percent of respondents say threat intelligence is provided hourly" (The Ponemon Fourth Annual Study on Exchanging Cyber Threat Intelligence, March 2021).

Only 11%

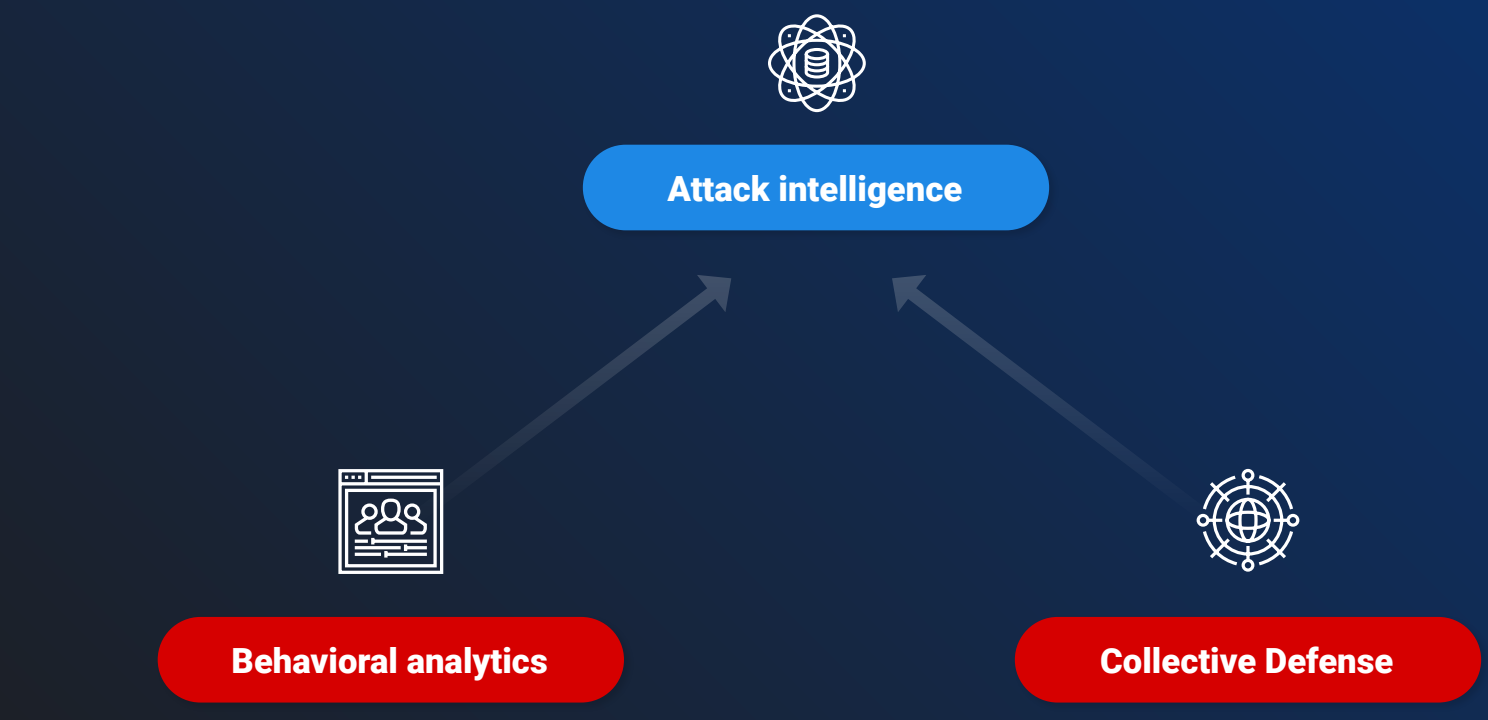
of security practitioners get threat intelligence in real time

— PONEMON INSTITUTE

77% of IT security practitioners "say threat intelligence becomes stale within minutes (54 percent) or within seconds (23 percent)"

— PONEMON INSTITUTE

Timely, relevant, and actionable attack intelligence comes from having visibility over the entire attack surface that affects your enterprise. That visibility must go beyond a single enterprise. A dynamic view of attacks as they are occurring at similar companies, within a sector, across a geographic area, across your supply chain, and/or across sectors is the only way to yield actionable attack intelligence with concrete, situational context.



What makes attack intelligence actionable?

There are four characteristics that make attack intelligence actionable:

1. **It is specific.** It is relevant to your enterprise or organization. It is based on a real threat to your company, sector, or supply chain. It is specific because you can see the attacks occur across the relevant attack surface at network speed, allowing you to know when the same or similar activity is happening to multiple companies at once. In other words, a campaign is in progress.

2. **It is timely.** That means the threat is happening now. It is not a signature that was detected an hour ago, a day ago, or a week ago, uploaded to a cloud and then batch downloaded to your security stack. You can see what is happening in real time.

3. **It has relevant metadata.** You can see all the characteristics of the attacker. How was it detected? What behavior did it display? What part of the kill chain was it in? Where did it fit in the MITRE ATT&CK® matrix?

4. **It is anonymized.** The only information shared is information about the attacker. No information is shared about the company that detected the event. No PII. No proprietary data. No competitive information. No internal network information. No information on whether the attack was successful or not. When the data about the attack is anonymized, then companies are more willing to share that data to empower analysts from different companies to collaborate over the same metadata, allowing companies to surge their collective resources and capabilities against a common threat.

What are the **benefits** of attack intelligence?

Attack intelligence enables you to move from a reactive security posture to a proactive one given that you can see relevant attack campaigns in progress. Knowing whether they are heading your way, with actionable threat information at your fingertips, allows for faster mitigation and response.

Not only is attack intelligence specific to your organization and timely, it also provides access to the relevant metadata for visibility of all the characteristics of the attacker. What's more, it is anonymized for crowdsourced threat-sharing and collaboration in real time. Through the lens of actionable attack intelligence, you can determine whether a network anomaly traditionally seen in isolation is of significance.

If you can see a once low-level detection across other environments, you know immediately to prioritize that threat, in turn helping you weed out the noise of threat intelligence feeds that do not provide relevant, specific context for your own environment. Actionable attack intelligence empowers you to make strategic, tactical, technical, and operational assessments at once.

With automated attack intelligence at hand, enriched by crowdsourced insights, you can access commentary, comparative information, context, and situational awareness about attacks either happening in your environment or most likely heading your way in the case of sector-targeted or supply chain attacks.

How is attack intelligence different from threat intelligence?

As collected and validated by cybersecurity analysts, threat intelligence involves the gathering and analysis of evidence-based threat information about known threats, including indicators of compromise (IoCs), implications, and advice for taking action. Threat intelligence feeds and platforms, as well as information-sharing ecosystems such as ISACs, publish threat information as weighed and vetted by analysts using open source information tools and their own tradecraft knowledge and expertise to gauge the validity and risk of cyber threats.

Traditional threat intelligence, however, often provides too much information, which is challenging to sort through to determine what is really important to your organization at any given time. As a Ponemon Institute survey revealed, "56 percent of respondents say a problem with threat feeds is that the threat data is often too voluminous and/or complex to provide timely and actionable intelligence" (The State of Threat Feed Effectiveness in the United States and United Kingdom Ponemon Institute Research Report Sponsored by Neustar).

So while a company or organization can consult threat intelligence information to gain a better understanding of possible threats in their ecosystem, the challenge is that threat intelligence often is not specific or timely enough to allow a security analyst to determine what is actually happening to their organization (or to similar organizations across their sector and/or supply chain) at any given time. To make matters worse, adversaries are constantly changing their tactics, techniques, and procedures (TTPs), creating an urgent need for a way to detect and prioritize unknown threats that do not yet have signatures or known indicators of compromise associated with them.

Delayed intelligence related to unknown threats has a direct impact on whether you can stop an attack. According to a March 2021 Ponemon Institute study, more than a third (38%) of cyberattacks "were not stopped because of the lack of timely and actionable data from [U.S. and U.K. survey respondents'] data feeds" (Ponemon, "State of Threat Feed Effectiveness" report). Attack intelligence closes the time gap between early detection of network threats and incident response.

At-a-glance **comparison**

TRADITIONAL THREAT INTELLIGENCE	ACTIONABLE ATTACK INTELLIGENCE
Threat intelligence is what could happen to your organization.	Attack intelligence describes what is happening to your network, or is happening to someone that looks like you, or is happening in your supply chain.
Threat intelligence basically tells you there are a lot of cyber adversaries who can do a lot of bad things.	Focused and specific, attack intelligence comes from detecting subtle anomalous use of trusted software, credentials, services and protocols.
It is not specific enough and it is not normally timely enough to allow you to focus your limited cyber resources on the threats most likely to impact your business.	Only through anomaly detection and alert correlation in real time will you be able to detect advanced attacks in the early stage.
Threat intelligence is typically not timely enough to allow you to take action during the early stages of network intrusion before an attacker moves laterally across your network or reaches the exfiltration or exploitation stage.	Attack intelligence reveals threats, with situation context, in time for you to take action before the threat has a significant impact on your business.

How do you gain **actionable attack intelligence?**

IronNet delivers actionable attack intelligence using an approach based on three lines of effort:

1. **Behavioral analytics**: A network detection and response (NDR) engine that is based on analyzing network traffic and identifying anomalies in that traffic that are most likely to be malicious. Identifying behavioral characteristics of the event is fundamental to detecting advanced, unknown threats. Traditional signature-based detection is not sufficient to detect even moderate level threats today.

2. **Visibility:** Being able to see the full attack surface relevant to your company through a Collective Defense system is essential for gaining truly actionable attack intelligence. Seeing just your enterprise is not sufficient. You need to see what is happening to other companies that look like you or companies in your supply chain that help you deliver value.

3. **Collaboration:** When you can see detections across multiple companies, you can detect campaigns in progress, in turn bringing to bear the power of the collaborating members to focus on defeating the attack together through Collective Defense.

What is the difference between **threat intelligence from threat-sharing groups** and **attack intelligence through Collective Defense?**

Traditional threat-sharing groups provide great value in facilitating collaboration and threat sharing within sectors. Among other differences noted below, however, attack intelligence raises the bar on threat-sharing by enabling real-time sharing of unknown threats based on automated and correlated detections of malicious network behaviors.

THREAT INTELLIGENCE VIA TRADITIONAL THREAT-SHARING GROUPS	ATTACK INTELLIGENCE THROUGH COLLECTIVE DEFENSE
A prolonged standard timeframe: incident happened, time-consuming research conducted, sanitization, sharing via more manual methods.	The ability to answer the question "What is happening now?" in real time via Collective Defense, which also provides the ability to collaborate (via rating/comments).
A reactive posture limited by seeing only what already has happened.	Visibility into what is currently happening via more coverage and more resources with less effort.
Access to only signature-based threat information.	Access to underlying (anonymized) threat detection data using Collective Defense across all community participants.
Non-specific alerts from threat intelligence feeds without context.	Vetted alerts on attack intelligence related to threats that are actually affecting your organization.
Relevant context and situational awareness that is fundamental to new attack/campaign discovery for detections humans have not seen.	The ability to understand clearly what analysts across the Collective Defense community are actually investigating in order to drive collaboration before, during, and after an attack.
Receiving less specific data around detections of unknown threats.	Relevant context and situational awareness that is fundamental to new attack/campaign discovery for detections humans have not seen.
Threat visibility limited to your own organization.	A real-time threat picture based on correlated alerts related to campaigns against their industry, supply chain, etc.
Responding on an organization by organization basis.	A way to empower SOCs to understand how triaging a specific alert has broader impact than their organization alone.

Summary

The concept of threat intelligence is not new as companies look to easy and valuable ways to share information to strengthen their cybersecurity posture. In fact, at IronNet we use threat intelligence as an input to derive relevant attack intelligence. Intelligence feeds such as AlienVault®, for example, are ingested to add context to events and alerts, reduce false positives, and detect previously discovered commodity attacks. What is novel, however, is the concept of actionable attack intelligence. Think of it as collective threat intelligence. This approach delivers a way to share behavior-based threat intelligence that automates some tedious investigation steps and integrates human insights that allow SOC analysts to accelerate response based on risk — all at network speed.

Actionable attack intelligence, as enabled by IronNet's Collective Defense platform, provides both big-picture threat context and tailored, sector-specific intelligence that is actionable immediately. In contrast to traditional threat intelligence platforms, which provide only hierarchical sharing capabilities, actionable attack intelligence enables dynamic, one-to-many communication. As multiple participants generate new attack intelligence around correlated threats across their environments, they can be part of the solution, not just spectators.

Connect with us to learn more about

actionable attack intelligence enabled by Collective Defense.

Contact IronNet

IronNet.com | info@IronNet.com | (443) 300-6761