No.67
May 2nd 2023

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN-SPONSORED**

HardenStance's RSAC Survey Report:

▪ *Barriers to effective use of threat intelligence*

HardenStance conducted a survey of cyber security leaders during RSAC 2023 in San Francisco last week. Here's what the survey tells us about the gap between how we could be using cyber threat intelligence today – and how we are actually using it.

- Shortcomings in people and processes are holding back effective use of cyber threat intelligence a lot more than any shortcomings in technology. Whereas every single respondent to the HardenStance survey pointed to failings in people and processes, less than one in three identified technology shortcomings as being in the mix.
- The three most frequently identified barriers to more effective use of threat intelligence are lack of awareness, understanding and skills; lack of trust and confidence in the end-to-end process from sourcing threat intel to applying it; and organizational barriers and departmental silos impeding the efficacy with which threat intel can be applied to manage an organization's security posture.
- Users need guidance from vendors and partners on how to embed best practice use of threat intelligence throughout their organization's cyber security operations.

Survey Methodology

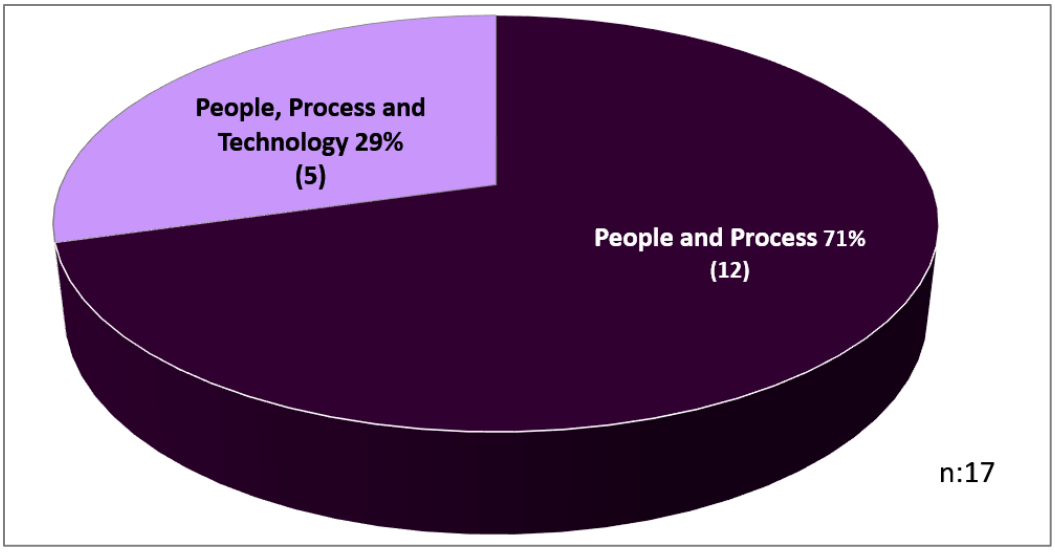
During meetings at RSAC 2023 last week, HardenStance asked 17 leaders from leading cyber security vendors the following survey question: *"What is the biggest barrier to infosec professionals identifying the most relevant cyber threats to their organizations and taking rapid and effective action to adjust their security posture accordingly?"*

The individuals who responded to the survey – together with their job title and type of company – are shown in **Figure 1.** Respondents were not given a menu of response options or asked to tick a box. The question was entirely open. Respondents answered freestyle with whatever popped into their heads. The survey results and supporting data follow on the next page.

Figure 1: Job Titles of the 17 Survey Respondents

Profiles of the 17 Director, VP & C-Level cyber security leaders in the survey sample	
VP Strategy, IoT PaaS Provider	Director, Product Marketing, Cloud Security Vendor
Head of Security Solutions, Networking vendor	CMO, Threat Intel vendor
VP, Business Development, Chip vendor	Director of Marketing, Threat Intel vendor
VP, Product Management, Threat Intel Vendor	Director, Product Management, EDR Vendor
CMO, Breach and Attack Simulation Vendor	Portfolio Director, Application Security Vendor
VP, Product Management, CAASM Vendor	VP, Product Management, DDoS Protection Vendor
VP, Public Policy, ICS Security Vendor	Head of Threat Intelligence, Network Security Vendor
CMO, Attack Surface Management Vendor	CTO, Network Security Vendor
Director, Marketing, Network Security Vendor	

Figure 2: The Biggest Barrier to Using Threat Intelligence More Effectively



Source: HardenStance

71% of respondents believe that people and process shortcomings represent the biggest barrier. Only 29% pointed to technology shortcomings also being in the mix.

Results of the HardenStance Survey

The break down in survey responses is shown in **Figure 2** above (the individual anonymized statements are shown on pages 4 - 5). Although they each emphasized different aspects of the problem, respondents were unanimous in agreeing that human and organizational shortcomings – issues with people and processes – are the key factors holding back better use of threat intelligence in cyber security.

71% of respondents believe that these people and process shortcomings represent the biggest barrier. Only 29% pointed to technology shortcomings also being in the mix. Not one of the individuals surveyed identified issues regarding any specific technology alone as the main barrier to better use of cyber threat intelligence.

A lot of IT and infosec professionals don't understand threat intel

Several respondents pointed to widespread shortfalls in the ability of many IT security professionals to understand, interpret and apply threat intelligence data in their environment. Respondents cited lack of awareness, knowledge and skillsets. One pointed to the industry's failure to simplify threat intel nomenclature to make it more easily understandable to non-specialists. They gave the simple example of the same threat group being called different things – for example Cozy Bear, Nobelium and APT29. Another said that the ability to intelligently consume, understand and act on threat intel is "the most valuable thing" a vendor can provide to an information security team.

Lack of trust and confidence in the process is also getting in the way

One of the two largest clusters of answers centred on how levels of trust and confidence in the process of curating, sharing and applying threat intelligence are holding users back from yielding the most benefit. The examples cited were as follows:

- One respondent pointed to people lacking confidence that if they share threat intel, the sharing process will be handled securely. Or they lack confidence that they will get back at least as much value from sharing as they put in.
- Two respondents pointed to what they both considered is a common distrust of some threat intel due to inadequate source attribution or data validation. One said that some vendors of threat feeds and other vendors in the threat intel ecosystem materially overstate how rigorously they validate their sources. Another said that while key government departments stress how important it is for them to validate their threat data, a lot of them still don't.

- Lack of confidence extends to what two respondents considered to be common cases where there is plenty of knowledge and competence to allow optimal actions in security operations to be driven by threat intelligence. However, these infosec practitioners are too fearful of implementing them for fear of annoying their users (hence they implicitly lack support from upper management).

At a basic level, one respondent cited the importance of an organization understanding what its 'crown jewels' are in terms of its data. This is foundational for tailoring threat intelligence to its cyber security posture. This respondent noted that many organizations still don't do this well. For example, they don't review the status of what constitutes their crown jewels and how best to defend them on a sufficiently regular basis.

Internal organizational barriers create an inhospitable terrain

The second of the two large clusters of responses cited information silos and other organizational barriers. Respondents expressed this challenge in different ways:

The second of the two large clusters of responses cited information silos and other organizational barriers.

- Different teams addressing different problems using different platforms. Security and fraud teams not communicating, especially in older, larger organizations.
- Information silos and domains that interrupt the flow of threat intelligence and delay the timeliest implementation of responses end-to-end.
- The need for data from various disparate sources to be consolidated and normalized. This is to enable connecting of the dots across that data to be done as a pre-requisite for getting maximum efficacy from using threat intelligence.
- Limitations in the ability of security policy to respond to threat intelligence quickly with in-flight or in-progress responses to minimize windows of exposure to threats.
- Not enough threat information sharing within an organization, between different departments. Threat intelligence-led thinking, isn't sufficiently institutionalized.

Technology shortcomings are not at the heart of the problem

As stated, only one third of respondents even mentioned a shortfall in technology when explaining the primary barriers as they saw it, whereas every one of them identified shortfalls in people and processes. Everyone surveyed therefore implicitly recognized that vendor solutions are heavily dependent for their efficacy on people and processes being aligned to leverage threat intelligence effectively.

In the case of a subset of advanced users, the efficacy of how they use threat intel can certainly be held back by the absence of a product or set of features. Hence it can also be turbo-charged by investment in those capabilities. But for the much broader business community, which survey respondents all appeared to speak to, basic human and organizational enablers need to be fixed first.

Of the 17 respondents, only 5 (29%) pointed to issues that could be interpreted as indicating a shortcoming in technology. Those five cited the absence of digitally signed JSON certificates by threat intel analysts; inadequate data validation; inadequate consolidation and normalization of data sources; inadequate visibility into vulnerabilities; and security policy that can't responding rapidly to threat intelligence inputs. Even some of these, however, can be attributable to shortcomings in skills and processes rather than purely to shortcomings in available technologies themselves.

The core finding from this year's survey – fixes for people and processes will yield more than technology fixes – echoes the findings of last year's RSA survey which concluded that "the most common belief is that the single most important thing we can do to improve our resilience is drive better cyber security awareness, education and training."

** HardenStance's Principal Analyst, Patrick Donegan, is a Cyber Threat Alliance 'Champion'. There's a lot of excellent information about cyber threat intelligence best practice available from www.cyberthreatalliance.org*

What they said – Here's how the 17 respondents answered

"Threat intelligence needs to be actionable. But that requires a very specific skillset that's capable of understanding and applying threat intelligence to arrive at a threat-intelligence driven security posture. A lot of folks just don't have that knowledge, that skillset in threat intel."
Director, Product Marketing, cloud security vendor

"Lack of knowledge and awareness arising from people trying to keep on top of things largely by themselves, without participating in trusted threat intelligence sharing groups and communities."
CMO, Cyber Threat Intelligence Vendor

"We could really do with normalizing some of the nomenclature to make threat intelligence more accessible to folks who aren't steeped in it 24/7. Someone talks about the Cozy Bear threat group. Someone else talks about APT29. But actually they're the same group."
Director of Marketing, Threat Intel Vendor

"Having clarity on what your crown jewels are, and regularly reviewing that, is foundational. That allows you to differentiate acceptable from unacceptable risk and focus on the subset of threats that matter most."
Director of Product Management, Threat Intel Vendor

"Especially in some large organizations, there's not enough threat information sharing within the organization, between different departments. The requirement, the way of thinking, understanding what represents a potential threat or vulnerability, the dynamic interaction between your attack surface and the threat landscape, that still isn't embedded or institutionalized in a lot of organizations"
Director of Product Management, EDR Vendor

"We often see that the willingness to learn from and share threat intel with others is there. People do get that. The barrier that has to be broken down is trust – trust that the process will be managed securely, trust that they will get back as much as they put in."
VP, Public Policy, ICS Security Vendor

"Defenders have to act on what they see – you can't just let potentially bad stuff through and hope."
Head of Threat Intelligence, Network Security Vendor

"People need to be willing to take a more assertive stance – even if that's at the expense of annoying a few users from time to time."
Director, Marketing, Network Security Vendor

"The most valuable thing you can give defenders is the ability to intelligently consume, understand and act on what the threat intelligence data is telling you."
VP, Product Management, DDoS Protection Vendor

"Threat Intel needs to be focused and actionable. You really need to be able to get to a short memo with maybe half a dozen bullets on it in a spirit of 'if you do nothing else today, make sure you do these five or six things'."
Director, Marketing, Network Security Vendor

"Getting rid of information silos within organizations would yield a big improvement. You have different teams addressing different problems, different platforms and platform owners. Security guys not talking to fraud guys. You especially see it in larger, older organizations like telcos."
Portfolio Director, Application Security Vendor

What they said – here's how the 17 respondents answered

"We need to find a way to build an end-to-end process, because at the moment we don't have that. We still have silos and domains that interrupt the flow of threat intelligence and delay the timeliest implementation of responses end-to-end."
Head of Security Solutions, Networking Vendor

"Better attribution of threat intelligence sources – for example the ability to be able to digitally sign JSON certificates. Threat feed providers will tell you their analysts have already crawled over everything to validate what they forward on to you. Actually, a lot of the time, they haven't."
VP, Strategy, IoT PaaS provider

"We still need much better data validation. We need to know where traffic originates from, what the size of the links are, whether it's sampled or unsampled. Organizations – even some government organizations will tell you how critical data validation is all day long. But a lot of them still aren't actually doing it."
CTO, Network Security Vendor

"It boils down to consolidating, normalizing all the data you can pull from the various disparate sources – your Attack Surface Management data, your controls validation data, vulnerability data, your threat intelligence – and then connecting those dots to demonstrate that you understand your risk and prove over time that your cyber risk posture is improving."
VP, Product Management, Cyber Asset Attack Surface Management (CAASM) Vendor

"There's too much emphasis on being able to detect threats after the fact. There's not enough on obtaining visibility into vulnerabilities and correlating that with the rest of your environment so that threats don't go turning into incidents."
CMO, Breach and Attack Simulation (BAS) vendor

"Improvements in in-flight or in-progress responses. Policy needs to be able to evaluate and respond quickly to reduce the amount of time an organization remains exposed from the time a threat is first identified to when a response is implemented."
VP, Business Development, Semiconductor Vendor

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, ETSI and TM Forum.

HardenStance Disclaimer

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.