IronNet

SURVEY WHITE PAPER

Collective Offense Calls for Collective Defense:

A Reality Check for Cybersecurity Decision Makers

Executive Summary

To better understand the current challenges and strategies among senior cybersecurity executives, IronNet commissioned the independent research firm Vanson Bourne to interview 200 U.S. security IT decision makers from industries including technology, telecommunications, retail, financial services, government, media, utilities, and many other sectors.

The survey polled respondents—more than half of whom serve in C-level positions—on issues ranging from confidence and efficacy around their cybersecurity solutions and perceived vulnerabilities to Artificial Intelligence (AI) and Machine Learning (ML) investment decisions and attitudes on collective defense and threat sharing.

AMONG THE STUDY'S KEY FINDINGS:

85%

of respondents are most likely to **rate their organization's cybersecurity technology, systems, and tools as advanced.**

Nonetheless, respondents suffered an average of one cybersecurity incident every three months, with 80% saying severity was such that C-level/board meetings were required afterward.

94%

of respondents say that their organization **would be willing to increase the level of threat sharing** with their industry peers if it demonstrably improved their ability to detect threats.

92%

of respondents say that they **would increase their level of threat sharing** with government if it enabled the government to use political, economic, cyber, or other national-level capabilities to deter cyber attacks.

73%

(almost three-quarters) of respondents **state that their organization has invested in Artificial Intelligence or Machine Learning** in the past 12 months.

Budget and doubts on ROI were the top reasons for those not investing in AI/ML.

The survey results collectively show an industry of leaders struggling to balance high confidence in current systems and practices against the need to continually improve and mature those systems. The survey concludes that in the face of adversaries who are increasingly collaborating for a *collective offense,* organizations must mature their *collective defense* to meet these powerful and ever-changing threats.

Introduction

A cybersecurity executive's world is crowded with decisions to make and learning curves to master to combat a range of growing threats. It no longer takes a nation-state to mount a nation-state-grade cyber attack. Threat actors are increasingly sharing techniques and best (or worst) practices to make their attacks more profitable for themselves and more damaging to organizations. Collective offense is testing the integrity of cyber defenses everywhere.

The rise of collective offense is troubling on a number of fronts, not least of which is the level of reported coordination among threat actors in the 2016 US election, hacking with the help of third-party intermediaries. Collective offense collaboration can come at the behest of nation-state actors and/or between various independent "cyber mercenary" groups. To make matters worse, collaboration is happening not just before and during an attack, but also afterward, as cyber criminals share data from successful breaches and sell their exploit tools on the dark web.

With this backdrop and the IronNet survey by Vanson Bourne, one thing is clear: while business concerns often vary from one industry to the next, there's a surprising consensus when it comes to cybersecurity. Regardless of the industry, more than half of security IT decision makers reported concerns about data or IP theft (59%) and destructive attacks on their systems (58%). These are followed by fears of attacks that cause business disruption (40%), include financial theft (37%), incur a large cost for recovery (36%), or result in damage to the organization's reputation (28%).

How successfully executives manage to navigate these concerns seems closely linked with what the survey results suggest are some pivotal, industry-wide dynamics that collectively amount to a reality check for the sector.

Key Findings and Analysis

Taken together, the survey findings put into stark relief a few overarching trends that at once define the current challenges most companies face, and the road map for better cybersecurity in the future.

A Disconnect Between Confidence Levels and Actual Vulnerability and System Maturity

Despite most IT decision makers' reported confidence that their cybersecurity capabilities are advanced and in better shape than others in their industry (55%), they nonetheless experienced an average of four attacks on their organization over a 12 month period, with 20% of respondents being hit six or more times.

In fact, almost 8 in 10 respondents state their organization has had a cybersecurity incident so severe, it has required a subsequent C-level/Board meeting. Following these meetings, more than half of organizations (57%) changed their cybersecurity processes and protocols to prevent a similar attack in the future, and half (50%) increased investment in current cybersecurity technology, systems, and tools. Improvements like these are good, but they remain overly reactive to the extent they only happen in the wake of a C-level post-mortem.

This reactive dynamic may help explain the apparent disconnect between high levels of confidence despite ongoing high incidences of attacks. As a starting point, consider the example of the body's immune system in the face of the common cold: your signature-based antibodies are great at recognizing known threats and being ready to fight these threats off the next time they occur. There's a certain benefit from gaining an understanding about that known threat. Unfortunately, the reason this benefit is nearly useless against the common cold is that the cold virus is always mutating; the threat is ever changing.

In a similar sense, many of today's cybersecurity tools look at yesterday's threats. We perform digital forensics that give us insight into how the attack occurred. We gain a sense of confidence from having reverse-engineered the problem, and we're confident that won't happen again. But as with the common cold, malicious actors are not a static adversary—they're always changing their methods and modes of attack. And the quickening pace of collaboration among threat actors further amplifies the threat.

All this means that tools designed to understand what happened yesterday will continue to allow new threats to hit the organization today. To add to the challenge, recent headlines about the return of Triton malware illustrate that even attacks we're familiar with can come back again in newly-altered and dangerous forms as malicious actors continually refine their methods.

A Learning Curve of Collective Defense

The rise in collaboration between malicious actor groups and wider sharing of nation-state-level tools and techniques is happening concurrently with mounting struggles in organizations around budgets and talent acquisition. For all these reasons, companies can no longer afford to defend in isolation. In other words, to cope with an increasingly *collective offense*, organizations need the best possible *collective defense*.

The notion of collective defense is nothing new. The vast majority (94%) of respondents' organizations currently subscribe to or invest in some form of collective defense, including threat sharing of IPs, file hashes, domains, and other signature-based indicators. However, the continued high incidence of successful attacks lays bare the fact that most collective defense strategies in use today simply aren't achieving the cybersecurity objectives they were designed for.

Traditional collective defense measures typically focus on the sharing of indicators for extant threats and cannot detect variations of similar attacks or unknown attacks where no indicators exist. Moreover, the time frame from discovery to sharing tends to be measured in weeks, if not months, giving threat actors ample time to reuse the same tactics on numerous targets. But, as noted above, even the most responsive patch efforts can't change the fact that threat actors do not stand still and constantly refine their strategies, tactics, and targets. This means insights from after-the-fact forensics or patches are of limited use. They are essentially snapshots and bandages that cover yesterday's attacks but don't fully protect you from tomorrow's threats.

Thankfully, organizations are increasingly grasping the need for better threat information sharing. Half of decision makers surveyed noted that their threat sharing tool could be improved upon, and 46% identified a need for enhanced sharing of cyber attacker tools, tactics, and procedures (TTP) and faster sharing of raw intelligence at network speed. The lack of such protections magnified the damage from recent attacks like Hydro Norsk, NotPetya, and others that quickly spread from company to company and could have been mitigated by better collective defense.

AI and ML Investment is Robust, but Maturity is Key to ROI

The IronNet survey addressed the pivotal role of AI and ML in powering cyber solutions in real time at the scale of even a global enterprise. CIOs, SOC analysts, and data scientists across a range of industries are continually struggling to analyze network traffic patterns for insights as systems scale and the avalanche of content outpaces the human ability to monitor all data.

Not surprisingly, nearly three-quarters (73%) of respondents say their organization has begun exploring the use of AI or ML-based cyber defense capabilities in the past 12 months, of which almost 7 in 10 (69%) state that it has exceeded their expectations. Even with the investment in AI/ML solutions, the same organizations surveyed still experience on average one breach per quarter, indicating that there is still a level of maturation needed for these types of solutions.

Of the 27% of respondents who hadn't invested in AI or ML in the past 12 months, 35% said their reason was that they were simply unsure of the value. The source of that uncertainty and the persistence of successful breaches may reflect both market confusion and the fact that not all AI/ML solutions are suitable for cybersecurity. The efficacy of AI/ML applications in cybersecurity depends on how they were designed and what exactly they were designed to do.

For example, it's one thing to have AI to help manage big labeled data sets, like translating language, or use ML to learn and predict the fuel pump failure rate in a locomotive engine. But it's another thing altogether to use AI/ML in cybersecurity, where you're looking for patterns you've never seen before. As with the reckoning with collective defense, decision makers are beginning to realize that not all AI/ML tools are alike.

About the Survey

IronNet commissioned Vanson Bourne to interview 200 U.S. security IT decision makers in January and February 2019. Of those respondents, 107 served in C-level roles, and 67% reported working in organizations with 5,000 employees or more. The top three organizational sectors represented were IT, technology, and telecoms (30%); retail, distribution, and transport (29%); and financial services (28%). Other sectors included manufacturing, professional services, media and entertainment, energy utilities, construction, and the public sector. The full survey results appear in the Appendix to this white paper.

A RANGE OF INDUSTRY CONCERNS

Beyond the core themes of the survey, respondents' answers shed light on a wide range of industry concerns:

Organizations are still experimenting with a variety of cybersecurity approaches to meet their challenges — On average, organizations deploy at least four types of security solutions. The most common included SIEM or log management (55%), a Threat Intelligence Platform (TIP) (52%), Advanced Endpoint Detection and Response (EDR) tools (50%), and Network Traffic Analysis (NTA) tools (50%).

Organizations see numerous hurdles to implementation — Nearly a quarter of respondents identified that they are facing issues with each of the following: lack of real-time visibility across industrial control systems and IoT (27%), lack of timely threat intelligence information (25%), and too many cybersecurity tools and poor integration between them (24%).

The biggest perceived vulnerabilities are from "unknown" threats — Respondents were least confident in their organization's ability to detect an unknown threat such as an APT group or malicious human operator within the network, with nearly three-quarters (73%) of IT decision makers noting their business would potentially miss these attacks.

Cybersecurity challenges go beyond just the core technology — When asked about improvements, most respondents pointed to the maturity of their cybersecurity processes/protocols, stating they need improvement before they are able to make strides to adopt new cybersecurity tools (41%). Other concerns included difficulty in securing newly-deployed technologies (28%), inability to hire enough skilled security personnel (27%), and a lack of in-house expertise (26%).

Actionable Takeaways

A main priority for IronNet in this survey was to identify not just key dynamics and challenges across today's cybersecurity landscape, but to also provide actionable insights or takeaways that cybersecurity practitioners can use to guide their decisions and maximize ROI from cybersecurity investments. Here are five such takeaways:

- **C-SUITE AND BOARD-LEVEL VISIBILITY AND BUY-IN ARE KEY** — There is a silver lining to the statistic shared earlier that 8 in 10 respondents had a cybersecurity incident so severe, it required a C-level/ Board meeting afterward: some organizations were able to leverage that attention proactively, driving their organizations to redesign systems to better protect data, IP, and finances (44%); conduct internal cybersecurity training for employees (40%); and review policies or create new ones (40%). It's clear that attention from those at the top of the organizational chart—if leveraged for a forward-looking instead of a reactive focus—can make cybersecurity investments more proactive, prioritized, and strategic.

- **ORGANIZATIONAL TRANSPARENCY MUST IMPROVE** — C-level respondents were more likely to rate the aspects of their organization's cybersecurity as more advanced and mature than their non-C-level peers. One interpretation is that those higher up in the hierarchy are unaware of the full details of their organization's cybersecurity posture. That suggests companies must adapt to share threat and system information more fully and forthrightly, given a rise in regulations around breach disclosures, both within and outside of the organization.

- **PRACTICE DEFENSE IN BREADTH, NOT JUST DEFENSE IN DEPTH** — Given the frequency of attacks that successfully penetrate systems, it is not surprising to see that organizations deploy an average of at least four types of security solutions. However, these solutions must be orchestrated by a strategy that deploys the breadth of detection methods in the right places across your system. If you rely on the same type of defense throughout your network, then your defense in depth will be no more imposing to threat actors than a series of doors with the exact same lock.

- **ELEVATE ROI AS THE DRIVER OF COLLECTIVE DEFENSE DECISIONS** — The survey makes clear that the desire for collective defense among industry peers is high. Some 94% of respondents say their organization would be willing to increase what they currently share with other industry peers if it led to better detection of threats for all members. The more the entire sector heeds the caveat that value is the missing ingredient for crafting better collective defense, the more we will see improvement across the industry.

- **THE FORCING FUNCTION TO EMBRACE COLLECTIVE DEFENSE SHOULD BE PROACTIVE, NOT JUST REACTIVE** — In most major cyber attacks, once the problem has reached the mainstream awareness, the cyber security community quickly works together to share information and mitigation techniques. One example of this pattern of action occurred in the NotPetya attacks. Proactively sharing threat insights at machine speed and as anomalies are discovered with industry peers will help accelerate and scale up collective defenses for all members, limiting future outbreaks before they get out of hand.

Appendix

DEMOGRAPHICS: 200 U.S. SECURITY IT DECISION MAKERS INTERVIEWED IN JANUARY AND FEBRUARY 2019, SPLIT IN THE FOLLOWING WAYS...

Organization Size

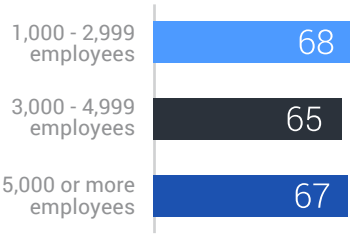

Figure 1: "How many employees does your organization have in the U.S.?" asked to all respondents (200).

Respondent Seniority

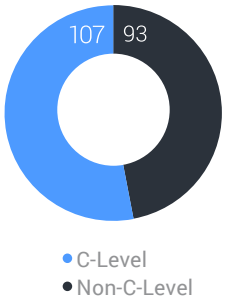

Figure 2: "Which of the following most accurately describes your job role in the organization?" asked to all respondents (200).

Organization Sector

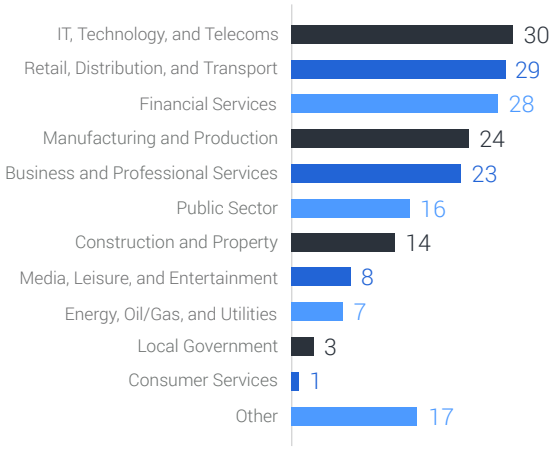

Figure 3: "Within which sector is your organization?" asked to all respondents (200).

ADVANCEMENT AND MATURITY BY SENIORITY

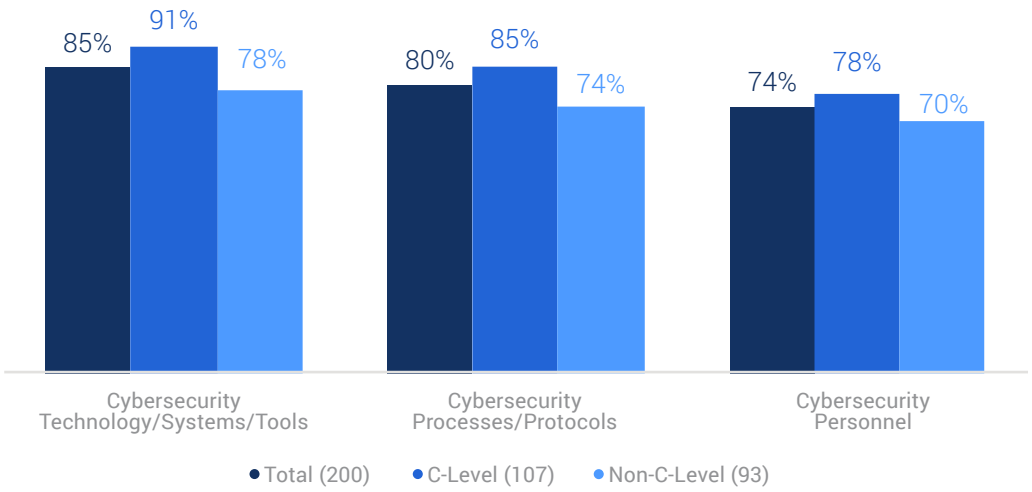

Figure 4: Analysis showing respondents' rating of aspects of their organization's cybersecurity, showing combination of "extremely advanced" and "advanced", showing results split by seniority (base numbers in chart).

Appendix

CYBERSECURITY INCIDENTS AND THEIR IMPACTS

Respondents' organizations have experienced an average of four cybersecurity incidents in the past 12 months, with the majority (81%) having experienced at least one. There is still a lot more that can be done to reduce this number.

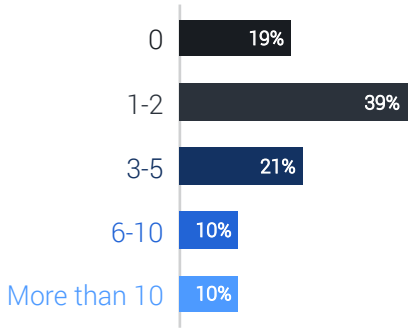

Figure 5: "Approximately how many cybersecurity incidents has your organization experienced in the past 12 months?" asked to all respondents. Data for "Don't know" (1.0%) is not shown.

INCREASING THREAT SHARING WITH INDUSTRY PEERS

94%

of respondents say their organization would be **willing to increase what they currently share** with other industry peers

Figure 6: Analysis showing the number of respondents whose organization would be willing to increase what they currently share with other industry peers if it demonstrably improved their ability to detect threats, asked to all respondents (200).

INCREASING THREAT SHARING WITH GOVERNMENT

92%

of respondents say their organization would be **willing to increase what they currently share** with government

Figure 7: Analysis showing the number of respondents whose organization would be willing to increase what they currently share with the government if it led to improved threat response at a national level (i.e., faster takedowns threats, economic sanctions, etc.), asked to all respondents (200).

Appendix

INVESTMENT IN ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

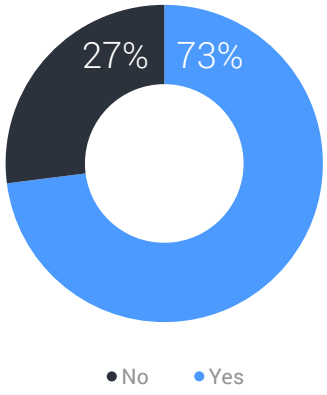

Figure 8: "Has your organization invested in Artificial Intelligence (AI) or Machine Learning (ML) based cyber defense capabilities in the past 12 months?" asked to all respondents (200).

CYBERSECURITY INCIDENTS AND THEIR IMPACTS

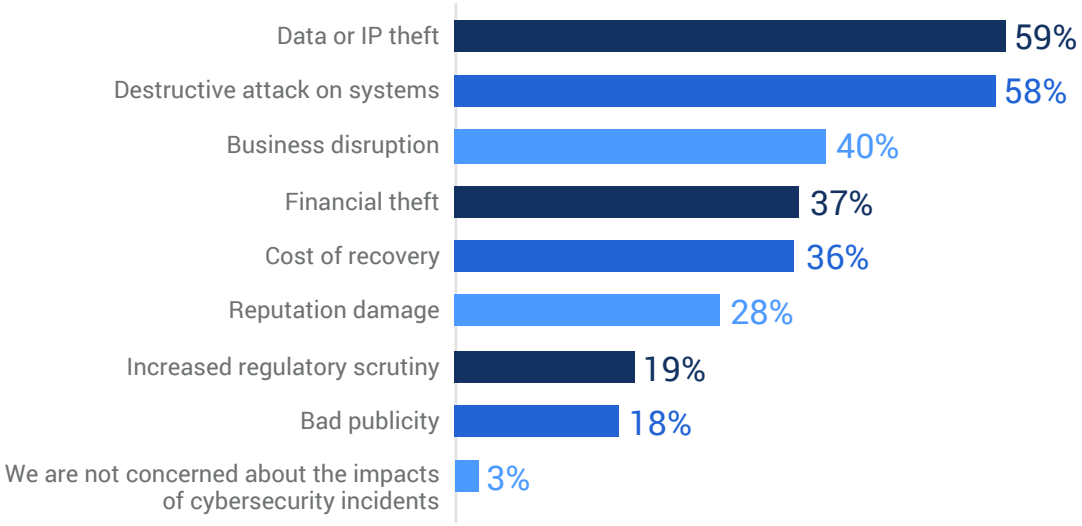

Figure 9: "Which of the following impacts of cybersecurity incidents is your organization most concerned about?" asked to all respondents (200). Showing the combination of responses ranked first, second, and third; data for "Don't know" (0.0%) is not shown.

Appendix

INVESTMENT IN ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

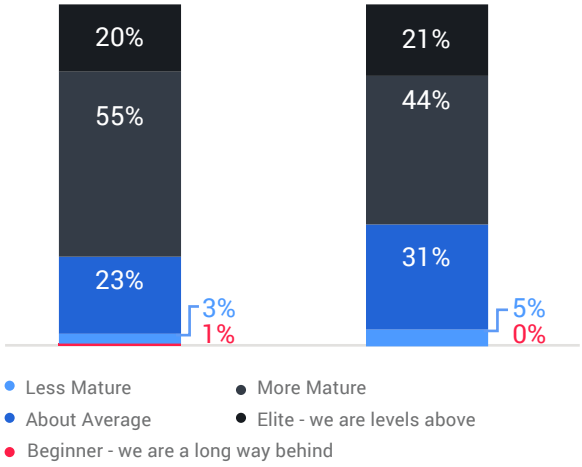

Figure 10: "How would you rate the maturity of your organization's overall cybersecurity compared to the following groups?" asked to all respondents (200). Data for "Don't know" (0.0% for both groups) is not shown.

PROVIDE MORE RELEVANT OR ACTIONABLE INFORMATION MEETINGS

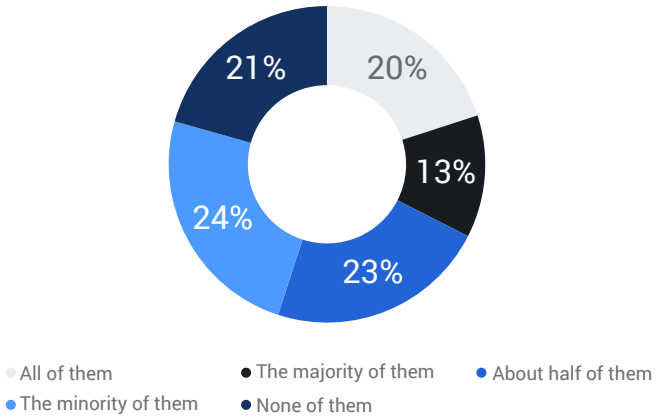

Figure 11: "How many of the cybersecurity incidents that your organization has experienced over the past 12 months have been so severe that they required C-level/Board meetings after the event?" asked to respondents from organizations that have experienced cybersecurity incidents in the past 12 months (160). Data for "Don't know" (0.0%) is not shown.

CYBERSECURITY INCIDENTS AND THEIR IMPACTS

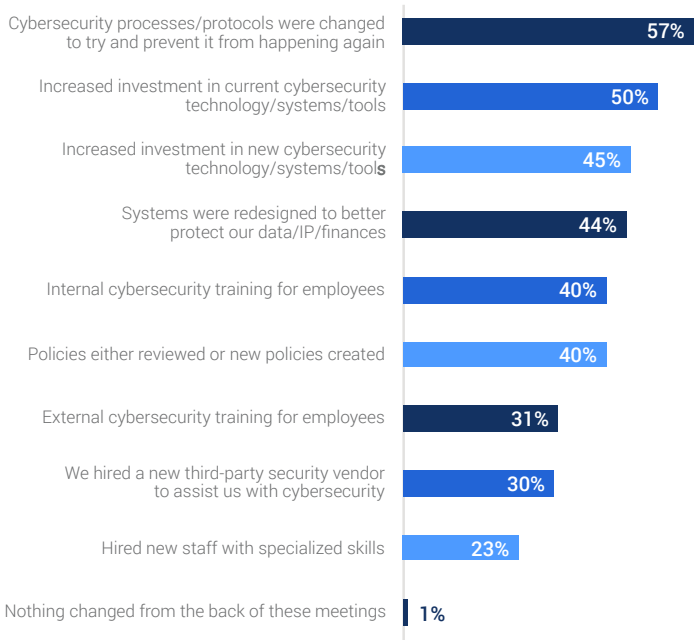

Figure 12: "What actions were taken from the back of the C-level/Board meeting that occurred as a result of a severe cybersecurity incident at your organization?" asked to respondents from organizations where a cybersecurity incident from the past 12 months was so severe that it required a C-level/Board meeting after the event (127). Data for "Other" (0.0%) and "Don't know" (0.0%) are not shown.

Appendix

IMPROVEMENTS TO THREAT SHARING AND INTELLIGENCE SOLUTIONS

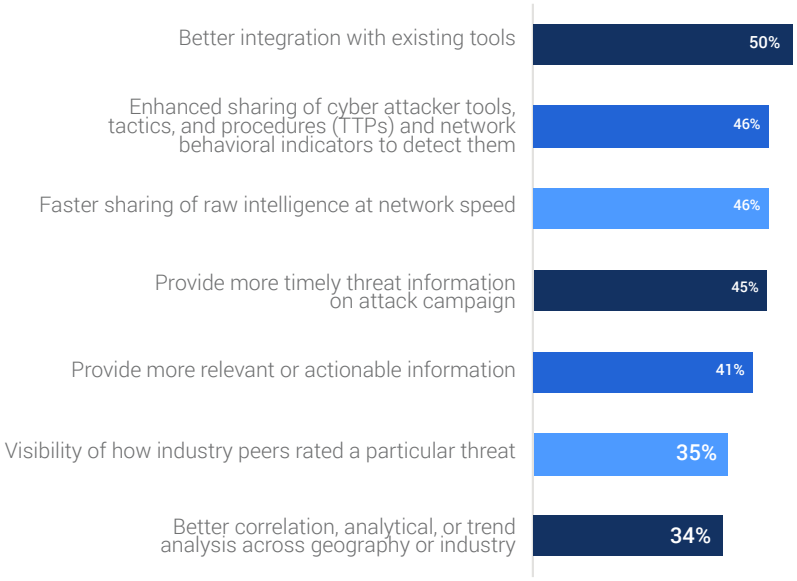

Figure 13: "How could the existing threat sharing or threat intelligence solutions that your organization currently leverages be improved?" asked to respondents from organizations that currently subscribe to or invest in threat sharing or threat intelligence solutions (188). Data for "Other" (0.0%) and "Don't know" (1.1%) are not shown.

INVESTMENT IN ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

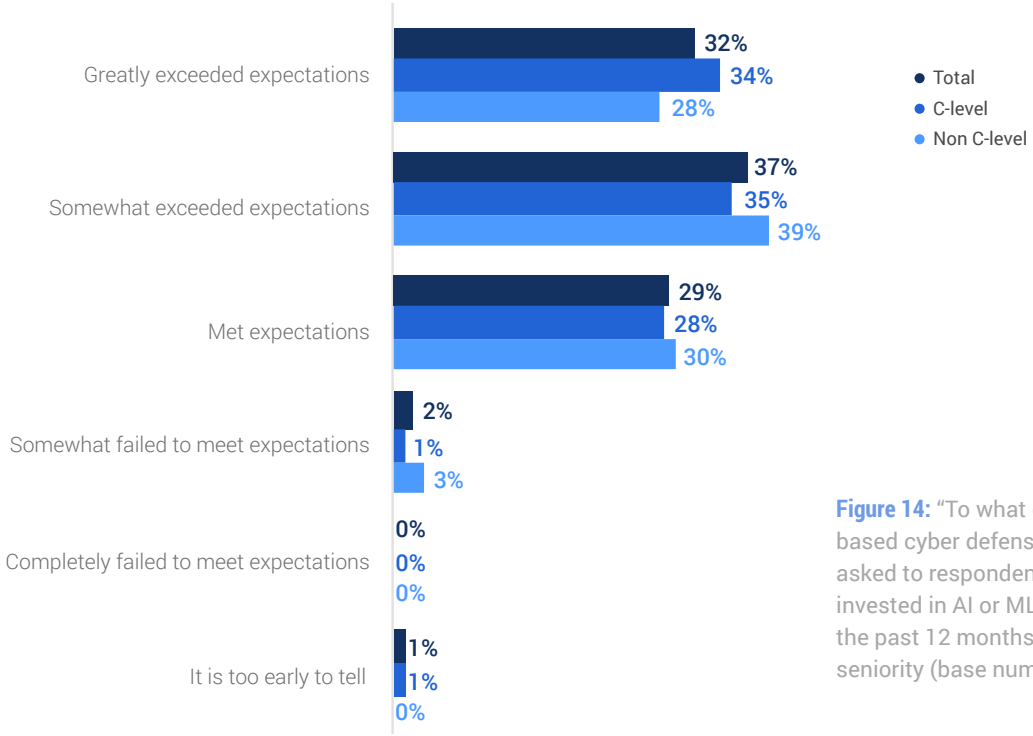

Figure 14: "To what extent has your organization's AI/ML based cyber defense investment met your expectations?" asked to respondents from organizations that have invested in AI or ML based cyber defense capabilities in the past 12 months showing data split by respondent seniority (base numbers in chart).

Appendix

CYBERSECURITY DEFENSES IN USE

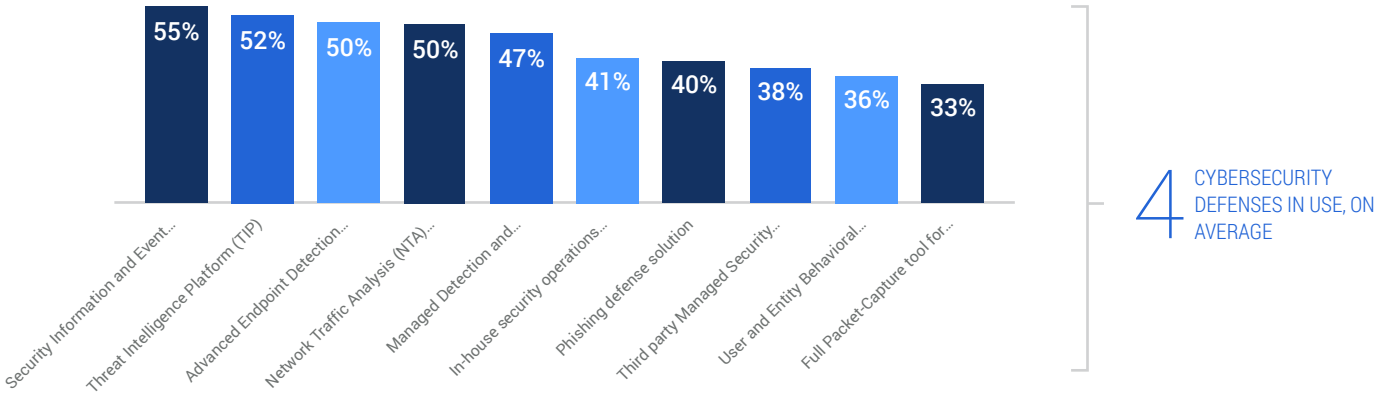

Figure 15: "What types of cybersecurity defenses does your organization use today?" asked to all respondents (200). Data for "Other" (0.0%) is not shown.

ISSUES WITH CYBERSECURITY DEFENSES

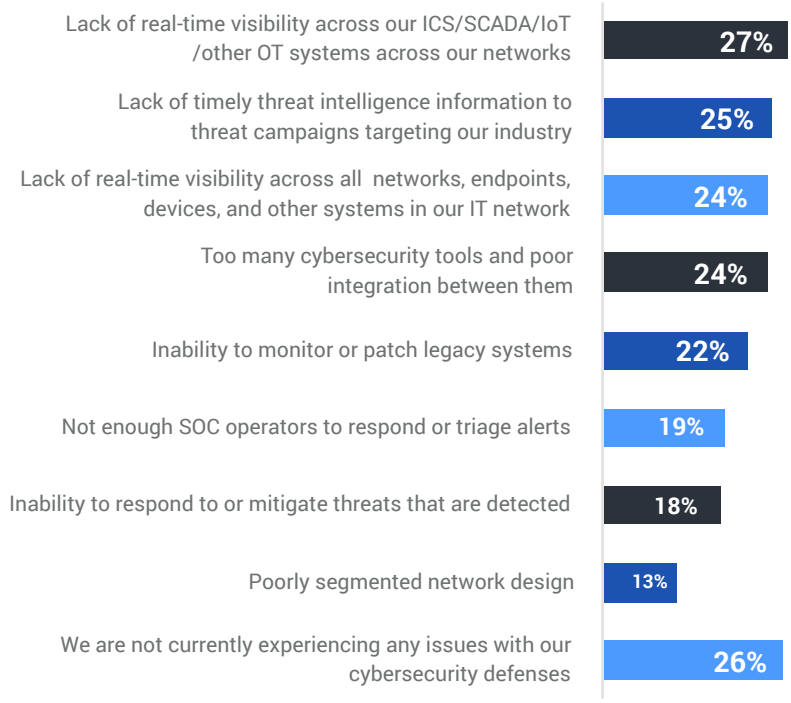

Figure 16: "Which of the following issues is your organization currently experiencing with its cybersecurity defenses?" asked to all respondents (200). Data for "Other" (0.0%) and "Don't know" (0.0%) are not shown.

Appendix

CONFIDENCE IN DETECTION

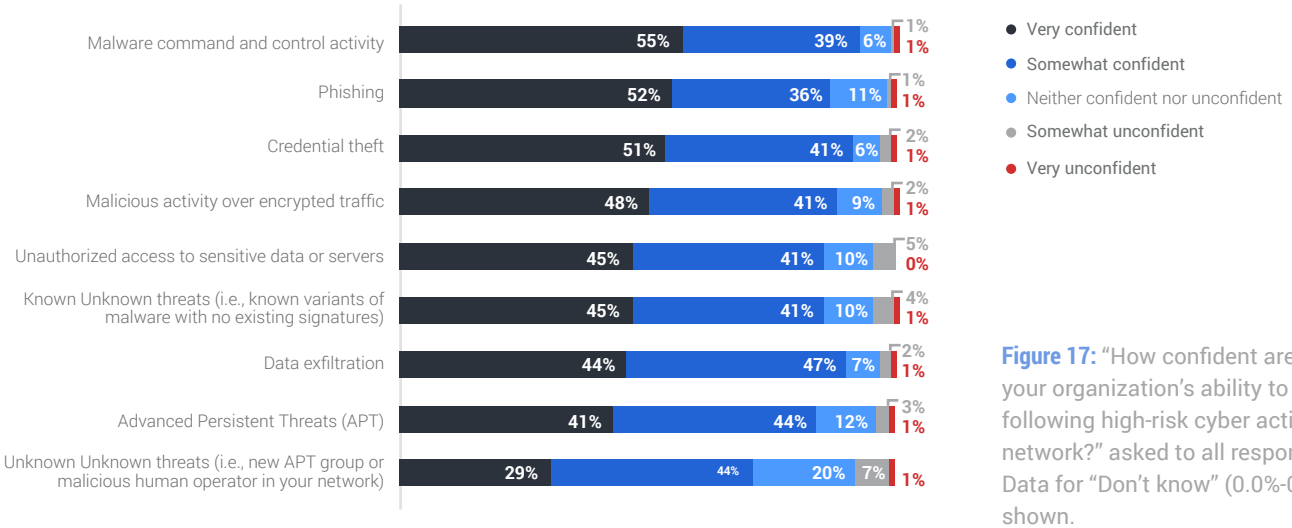

Figure 17: "How confident are you in your organization's ability to detect the following high-risk cyber activities on your network?" asked to all respondents (200). Data for "Don't know" (0.0%-0.5%) is not shown.

ISSUES WITH CYBERSECURITY DEFENSES

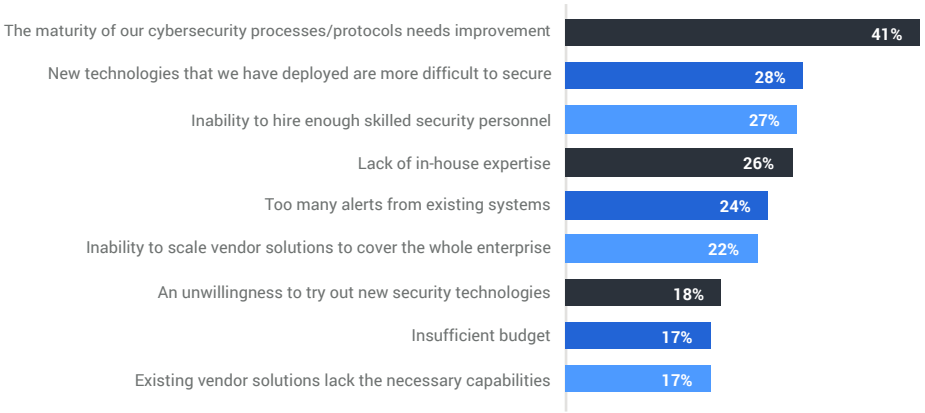

Figure 18: "Which of the following are reasons for the issues that your organization is currently experiencing with its cybersecurity defenses?" asked to respondents from organizations that are currently experiencing issues with their cybersecurity defenses (148). Data for "Other" (0.0%) and "Don't know" (0.0%) is not shown.

About IronNet

IronNet's mission is to deliver the power of collective cybersecurity to defend companies, sectors, and nations. The company was founded in 2014 by GEN (Ret.) Keith Alexander, the former Director of the National Security Agency and founding Commander of U.S. Cyber Command. Our team consists of expert offensive and defensive cybersecurity operators with unmatched experience defending commercial and government networks against advanced threats. IronNet is backed by blue-chip investors C5 Capital, ForgePoint Capital, and Kleiner Perkins.

