THE STATE OF THREAT DETECTION REPORT 2019

KNOW YOUR TERRAIN, DEFEND YOUR TERRAIN

Fidelis Cybersecurity

INTRODUCTION

AS CYBER TERRAIN & SECURITY STACKS GROW, SO DO CYBER WOES

Cybersecurity hasn't gotten any easier. That should hardly be a revelation to professionals in the field, who every year are seeing their cyber terrain grow larger and larger. Every day, organizations are adding more cloud applications and endpoints; dealing with higher and higher levels of network traffic; and dealing with more connected devices than ever. All of this while trying to evolve their cyber defenses to stay one step ahead of adversaries that are accelerating their tactics, techniques and procedures (TTPs) at breakneck speeds. If that sounds hard to manage, it's because it is.

As cyber terrains continue to grow, the likelihood of unidentified blind spots grows too. Organizations are under immense pressure to close these visibility gaps in their systems, especially in the direct aftermath of a security incident. This leads many organizations to execute their cybersecurity strategy in a much more reactive manner than they would like. They continue to add point solutions to their security stack to immediately address specific security concerns. Yet they do so without a detailed analysis and understanding of if these point solutions are capable of interacting with the rest of the security stack, or if those solutions are redundant to solutions already in the stack.

As a result, organizations unintentionally introduce even more security gaps into their enterprise. Additionally, this makes it even harder to achieve visibility across cyber tools, much less the network at large. Short term fixes become part of the larger problem. This is hardest felt by organizations who are struggling to contend with a widespread cyber skills gap and do not have automated capabilities to mitigate. These problems are further compounded in organizations that do not currently have tailored threat intelligence, or the ability to execute advanced threat hunting methodologies.

Attackers are leveraging these cumulative vulnerabilities to penetrate traditional cyber defenses and lurk undetected in terrain blind spots, sometimes for weeks or months. So, how can organizations who recognize these vulnerabilities act to remedy them in a proactive and holistic manner?

To find out cybersecurity's biggest concerns, challenges and current state, Fidelis Cybersecurity surveyed roughly 300 cybersecurity professionals. The following pages include our findings.

SURVEY PARTICIPANTS

REGION

- USA: 43%
- Europe: 40%
- Asia: 7%
- Other: 10%

JOB TITLE

- CISO/CITO/CTO: 9%
- VP/Director/Manager: 32%
- Architect/Engineer: 30%
- Analyst: 14%
- Other: 15%

COMPANY SIZE

- Large Enterprise (5001+ employees): 33%
- Medium Enterprise (1001-5000 employees): 19%
- Medium Business (250-1000 employees): 16%
- Small Business (1-250 employees): 33%

MAJOR PAIN POINTS – VISIBILITY AND AUTOMATION

Survey respondents were asked to rank how heavily some of the top security issues were impacting their organization on a scale of 1 to 5 (5 being the highest impact). Of the issues presented, the lack of automation and visibility were the most pressing areas identified by respondents. This has not changed since last year's State of Detection and Response Survey. This means that even though visibility and a lack of resources are known to be the leading issues for security professionals, organizations are still struggling to address these crucial issues.

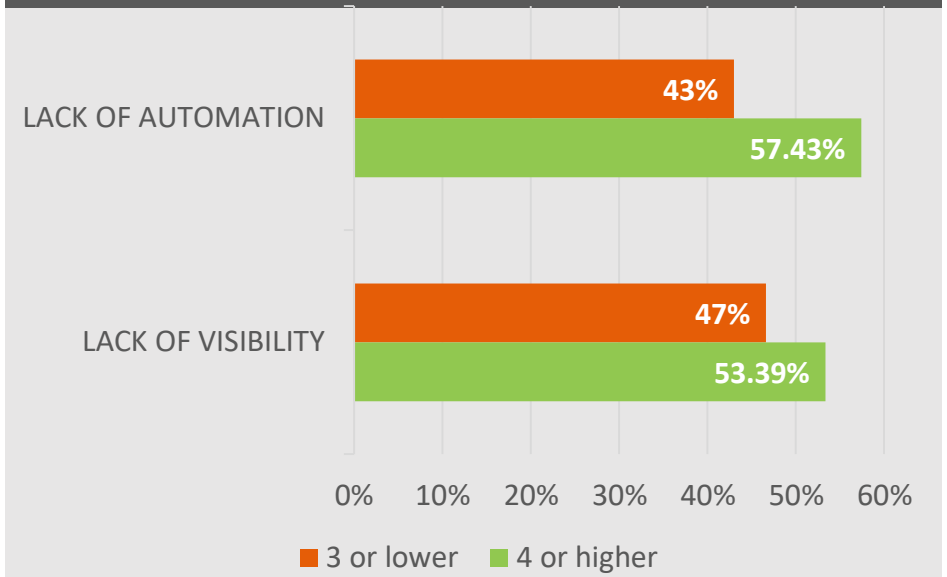
In this year's survey, 57.43% of respondents scored their lack of automation as a 4 or higher, making implementing automation the most pressing issue for organizations. Overall, the lack of automation scored a weighted average of 3.59.

The second most pressing issue for respondents was a lack of visibility, with 53.39% of respondents weighing this issue as a 4 or higher. Overall, the lack of visibility scored a weighted average of 3.52.

Other pressing issues for respondents include:

- A lack of integrated solutions (weighted avg. 3.30)
- Too many alerts across tools (weighted avg. 3.25)
- A lack of access to actionable threat intelligence (weighted avg. 3.12)
- A lack of qualified analysts (weighted avg. 3.07)

How heavily are some of the top security issues impacting your organization?



VARYING PERSPECTIVES ON ISSUES FACING SECURITY TEAMS

CISO/CIO/CTO Perspective
C-suite information and technology leaders' leading pain points this year were a lack of automation (weighted average of 4.09, with 78.26% of C-suite executives rating it a 4 or higher); too many alerts across tools (weighted average of 3.71, with 66.67% rating it a 4 or higher); and a lack of integrated solutions (weighted average of 3.62, with 57.14% rating it a 4 or higher).

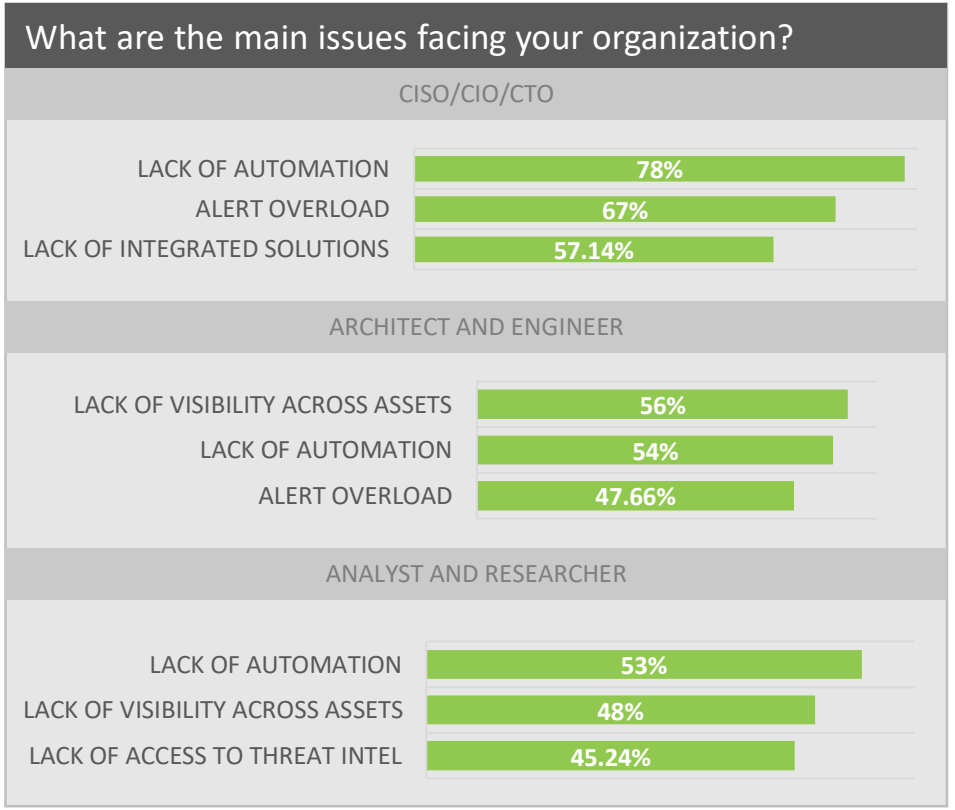
Last year: Insufficient security resources, lack of automation and alert overload were the leading issues.

Architect and Engineer Perspective
Architects' and engineers' leading pain points this year were a lack of visibility across all assets (weighted average of 3.63, with 55.71% rating it a 4 or higher); a lack of automation (weighted average of 3.51, with 53.52% rating it a 4 or higher); and too many alerts across tools (weighted average of 3.35, with 47.66% rating it a 4 or higher).

Last year: too many disparate tools, insufficient security resources, and a lack of automation were the leading issues.

Analyst and Researcher Perspective
Analysts' and researchers' leading pain points this year were a lack of automation (weighted average of 3.44, with 53.48% rating it a 4 or higher); a lack of visibility across all assets (weighted average of 3.27, with 47.73% rating it a 4 or higher); and a lack of access to actionable threat intelligence (weighted average of 3.14, with 45.24% rating it a 4 or higher).

Last year: lack of automation, alert overload, and insufficient security resources were the leading issues.



SECURITY STACK

As organizations continue to see their cyber terrain expand – 69% of respondents in our survey said their terrain is expanding – it will only get harder to maintain visibility and mitigate threats in a proactive manner through automation, threat intelligence and threat hunting. As a crutch, many will adopt point solutions, adding additional tools and capabilities onto their existing security stack to address specific issues or risks. Far too often though, these tools and capabilities are not implemented with proper planning, leading to redundancies and inefficiencies within the security stack.

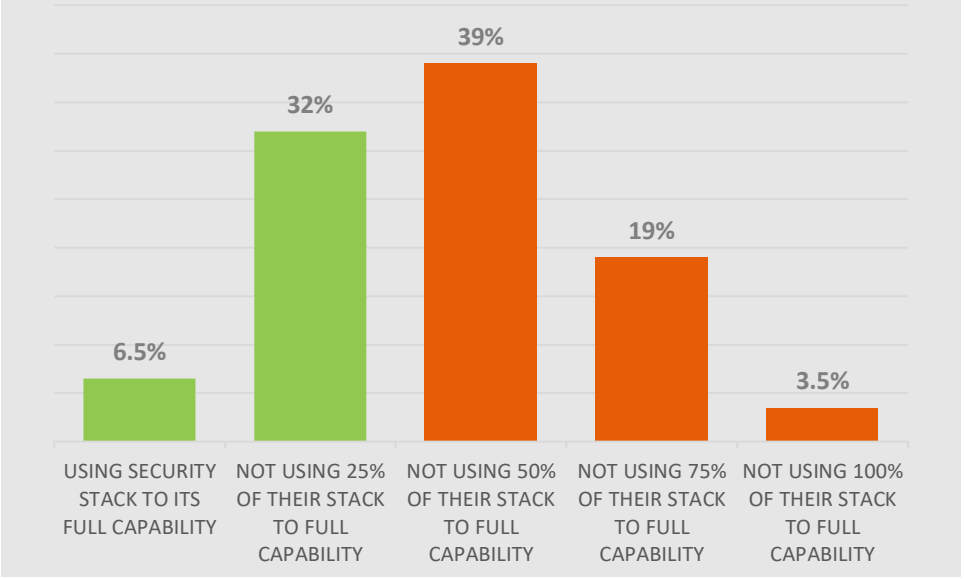
When we asked security professionals if they were using their full security stack to its full capability, the answer was a resounding no. Only 6.54% of all organizations surveyed believe they are using their full security stack to its full capability. We found:

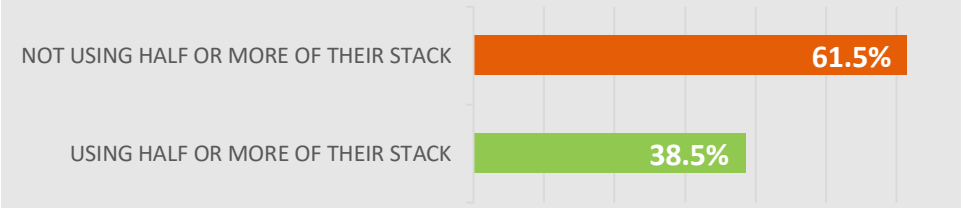
- 32% are not using a quarter (25%) of their stack to full capability
- 39% are not using half (50%) of their stack to full capability
- 19% are not using three-quarters (75%) of their stack to full capability
- 3.5% are not using their entire stack (100%) to full capability

This means that 61.5% of survey respondents are not using half or more of their stack to its full capability. This is even worse for the financial industry, where 73.17% of respondents stated that they are not using half or more of their stack to its full capability.

With a growing security stack, comes a growing list of patches to consider, ultimately creating a host of diversions that keep organization's attention diverted from the true threat. The good news is that most organizations realize that this is a problem, with 78% of respondents replying that they have, or are planning to consolidate their security stack. This rate is higher for the public sector and financial sector, with 81.82% and 85% respectively indicating that they have a strategy for consolidating or are planning to consolidate. Healthcare trails, with only 64.28% indicating they are planning to consolidate.

Are you using your full security stack to its full capability?





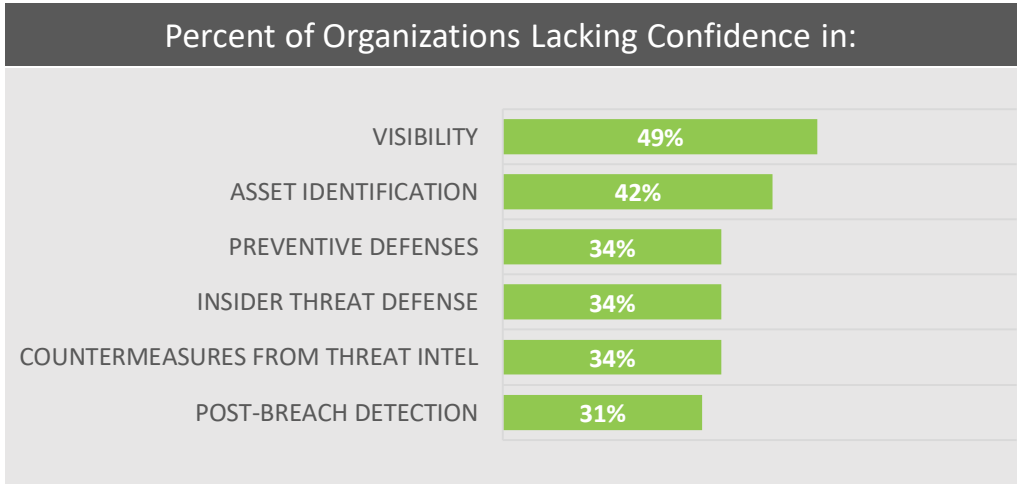
CONFIDENCE IN DEFENSES

The noted automation, visibility, and consolidation challenges have a ripple effect throughout organizations, negatively effecting their ability to prevent threats to their cyber terrain. Nearly half of respondents (49.02%) either did not have visibility of their entire cyber terrain or did not know the level of visibility of their terrain. A little less than half (42.29%) of respondents were not confident in their ability to identify vulnerable assets on their network. And over half of respondents (55.03%) did not have strategically placed sensors to prevent blind spots or did not know if their sensors were strategically placed. This means that roughly half of respondents could easily have malicious actors (insider or external) hiding in the blind spots of the cyber terrain.

When asked if they believed their preventive defenses were effective against targeted attacks, 34.32% of respondents did not believe them to be effective or did not know. This is significantly higher for healthcare respondents, 53.33% of whom lack confidence in their preventive defenses.

When asked if they were confident in their organization's ability to identify insider threats and stop resultant data exfiltration attempts, a little over a third (34.02%) of all respondents answered that they were "not so confident" (29.90%) or "not at all confident" (4.12%). This was more or less consistent among security professionals across industries, with 33.34% of healthcare professionals, 30.95% of financial professionals, and 30.77% of public sector professionals lacking adequate confidence. However, only 11.90% of the financial industry, 11.54% of the public sector, and no respondents from healthcare were "highly confident" in their ability.

Organizations' ability to react post-breach looks similar, with 30.88% of organizations replying that their post-breach capabilities were not very effective, or they did not know if they were effective. This is once again hardest felt by the healthcare industry, where 46.67% of organizations lack confidence in their post-breach abilities.



55% of respondents did not have strategically placed sensors to prevent blind spots

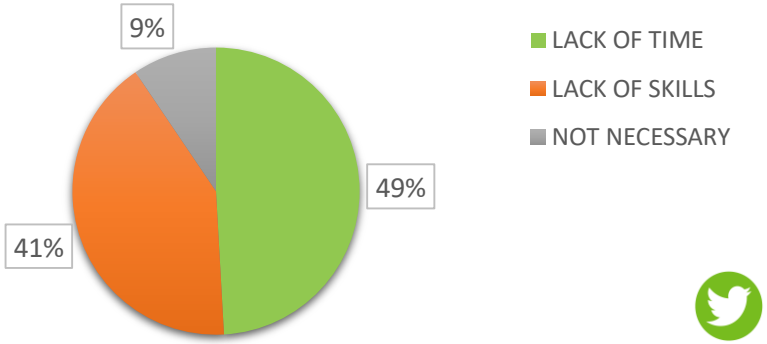
THREAT HUNTING

A lack of adequate preventive defenses makes threat intelligence and threat hunting all the more imperative for organizations. However, only 45.83% of organizations surveyed are currently engaged in threat hunting, with an additional 24.31% planning to engage in threat hunting in the future. When we asked organizations not engaged in threat hunting why they did not currently have threat hunting capabilities, most pointed to either a lack of time (49.11%) or a skills gap (41.42%) – mirroring the same two limitations as last year. Only 9.47% of organizations believed threat hunting was not necessary, down from 12.40% last year.

This helps to explain why a lack of automation is the leading pain points for surveyed organizations. Automated workflows speed up detection and response processes and facilitate threat hunting capabilities. Automation is also essential for data collection, providing analysts with critical context that allows them to determine an initial threat or indicator to hunt for and how malicious activity is impacting the environment. As such, automation should be a key consideration for the organizations that do not currently have threat hunting capabilities but are planning to implement them within the next year.

Does your security team currently engage in threat hunting?

Barriers to Threat Hunting:



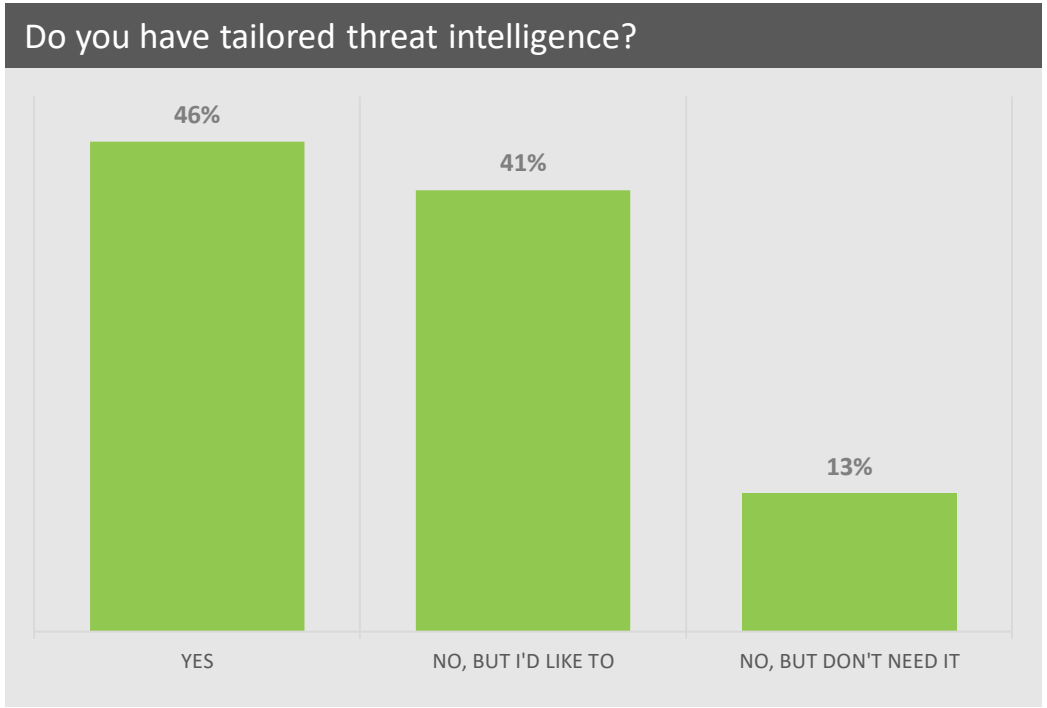
THREAT INTELLIGENCE

While many organizations have threat intelligence feeds and platforms of some kind, they often lack threat intelligence that is specifically tailored to their environment.

Of the organizations surveyed, only 45.80% reported that they had threat intelligence tailored to their organization. This is lower for respondents in the federal government (40.00%) and healthcare (20.00%), but higher for the financial industry (59.52%).

41% of respondents said they do not have threat intelligence capabilities but would like them. This is most prevalent among healthcare professionals, where 66.67% of organizations do not have threat intelligence tailored to their organization but would like to.

The lack of individually tailored threat intelligence is a major barrier to any organization, limiting the effectiveness of results that are returned from threat intelligence activities. This is evidenced by roughly one-third of respondents (33.90%), who indicated that they were “not so confident” or “not at all confident” in the countermeasures created from their threat intelligence.



CONCLUSIONS

- **ORGANIZATIONS LACK CRITICALLY NEEDED VISIBILITY**, DRIVEN BY AN EVER-EXPANDING CYBER TERRAIN AND OVERLY BURDENED SECURITY STACKS.
- **THE OVERWHELMING MAJORITY OF ORGANIZATIONS ARE NOT USING THEIR SECURITY STACK ANYWHERE CLOSE TO ITS FULL CAPABILITY**, SHOWING THE NEED FOR CONSOLIDATION, INTEROPERABILITY AND UNIFIED PLATFORMS.
- **VISIBILITY AND CONSOLIDATION ISSUES ARE NEGATIVELY IMPACTING THE RISK CONFIDENCE OF ORGANIZATIONS** AND INCREASING THE LIKELIHOOD AND ATTACKER WILL BE ABLE TO EVADE PREVENTIVE AND POST-BREACH DEFENSES.
- **A LACK OF AUTOMATION AND A GROWING SKILLS GAP IS PUTTING MORE AND MORE WORK ONTO SECURITY TEAMS** AND CAUSING ORGANIZATIONS TO FORGO IMPORTANT CAPABILITIES THAT COULD HELP TO PREVENT AND RESPOND, SUCH AS THREAT INTELLIGENCE AND THREAT HUNTING.

THE STATE OF THREAT DETECTION LIVE WEBINAR

August 27, 2019, 11:00 am ET / 8:00 am PT / 3:00 pm GMT

You can't defend what you can't see. Knowing your terrain is the first step in standing up an effective defensive posture. Register for our State of Threat Detection Live Webinar to hear a detailed analysis of survey findings straight from the experts and how findings can be applied to the modern enterprise.

REGISTER NOW

Fidelis Cybersecurity