silo
By Authentic8

SURVEY REPORT

Organizations Not Equipped to Meet Rising Tide of Financial Crime Threats

Results from Authentic8's 2020 Global Financial Crime Investigations Survey

Table of Contents

Key Findings 3

Results: Survey Says 4

- Most Organizations Tread Water to Keep Up With Caseload 4
- Typical Scope of Research Collection and Analysis Revealed 5
- Investigator Challenges Run Counter to Organizational Policy 7

Insights: Making the Right Investment in People, Process and Tools 10

Conclusion 12

2020 GLOBAL FINANCIAL CRIME INVESTIGATIONS

Executive Summary

Financial crime is on the rise with no slowdown in sight. Case in point, a 2020 PWC survey reported that between 2018 and 2020, 47 percent of companies suffered a financial crime event, representing a total of $42 billion in losses. The coronavirus crisis also increased the threat to banks and financial service institutions; just between February and March 2020, cyberattacks in the industry increased 38 percent. These trends are troubling, and financial service organizations struggle to stem the tide through improved preventative measures, investigations and response.

Industry news tends to focus on the next security technology breakthrough to solve all of financial service organizations' woes — artificial intelligence (AI), security orchestration, automation response (SOAR), blockchain forensics and so on. However, precious few headlines are allocated to the critical role of the "humans in the loop" interactions required for structured or ad-hoc online research into financial crimes. A human needs to research critical signals received from feeds and the security information and event management (SIEM) system to "follow the money" and provide qualitative assessment.

To better understand these types of interactions, Authentic8 in concert with the Association of Certified Financial Crime Specialists (ACFCS) conducted an in-depth survey of investigators from over 150 organizations. The respondents included individuals across the use case spectrum including financial crime (anti-money laundering, tax evasion, bribery), fraud (identity theft, credit card theft, account theft, phishing) and governance, risk and compliance (general GRC, know your customer, customer due diligence).

One clear finding: Analyst efficiency is stagnant or even declining. How can organizations change course? Some try to hire their way out of the problem — that is, add to the "people" element in "people, processes and tools." With rising crime and fraud activity, the scale of hiring required is an expensive proposition. Another approach is to improve the efficiency of each analyst's workflows — enable people by investing in processes and tools. Both approaches require an intimate understanding of the difficulties and inefficiencies of the online research function. The survey results that follow shine a light on the challenges of financial crime investigation teams and their productivity, so organizations can best target investment and reduce the variety of risks associated with financial crime.

Key Findings

Caseload Productivity is in Trouble

57 percent of survey respondents say productivity is the same or worse compared to 2019, and 90 percent indicate that more investment is needed in open source intelligence (OSINT) gathering capabilities to accelerate time-to-insight for investigations.

Anonymity is Critical

50 percent of respondents state that anonymity is critical while conducting investigations, recognizing that without managed attribution, targets could seek retribution and entire cases could be blown, further hampering productivity.

Dark Web Remains in the Dark

46 percent are not able to follow leads into the dark web, though they indicate that this capability would be valuable if done securely and in accordance with compliance and risk management requirements. Limiting investigator access to the dark web is hurting the efficiency and effectiveness of their investigations.

DIY Isolation Isn't Up to the Task

Nearly all (98 percent) of respondents agree they need to protect IT infrastructure while browsing unsafe sites. However, research analysts are sometimes left to their own devices to properly isolate their online research to reduce risk to their organizations, adding to caseload productivity issues. Clunky processes, such as requesting permissions, or other overhead management can also add time to investigations.

Keeping Up With Criminals and Technology is Biggest Challenge

Training to keep up with evolutions in criminal tactics, techniques and procedures, as well as changes in technology ranks as the top challenge for investigators (28 percent). They are struggling to get the specialized training they need to successfully perform investigations in the most efficient manner.

RESULTS:

Survey Says

Most Organizations Tread Water to Keep Up With Caseload

First the bad news: More than half (57 percent) of the investigators surveyed are not seeing an increase in their case output over last year (see figure 1). Further statistics in these survey findings will shed light on what's hampering productivity.

Stagnant or declining caseload productivity is not just a matter of investigator frustration; it can lead to increased organizational risks such as:

- Additional costs based on fraud or writedown of fraudulent transactions
- Further exposure as adversaries change their techniques before investigators catch up
- Falling out of compliance with regulatory or internal policy requirements
- Decreased brand trust due to inability to properly tackle financial crimes
- Profitability, if hiring is increased without addressing inefficient processes

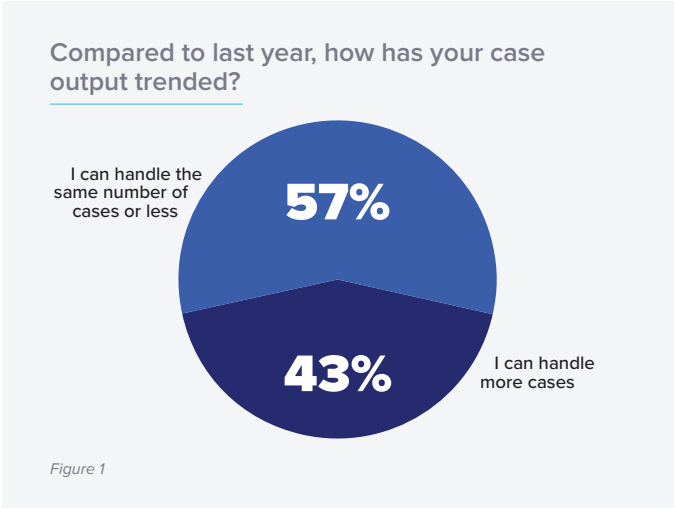

Figure 1

Additionally, the vast majority (believe 90 percent) their organizations should invest more to accelerate time-to-insight (see figure 2). Both this statistic and the reported decline in productivity have significant implications for management now and over time, as criminal activities continue to increase.

Consider identity theft for use in fraud: The period between 2018 and 2019 saw a 46-percent increase in reported thefts, making 2019 the worst year in history; credit card fraud specifically has been steadily increasing and surged 72 percent in 2019 over 2018 statistics. In order to keep pace with the rising threat, organizations need to better enable investigators.

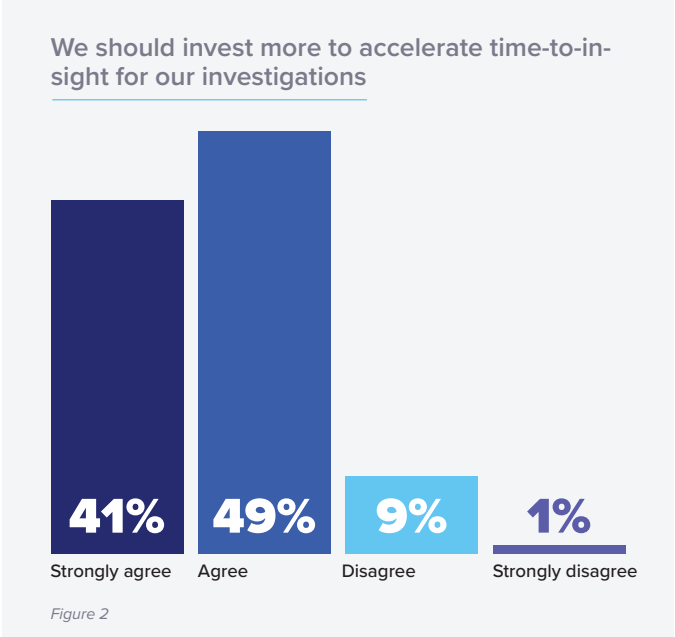

Figure 2

The good news: Enhancing financial crime investigations with OSINT techniques and tools reaps productivity benefits. More than 70 percent of respondents say their organization plans to or has already invested in OSINT gathering tools (see figure 3). Additionally, 86 percent of survey respondents who said they can handle more cases already invested in OSINT or will be investing in it (see figure 4). If you don't have a well-established online research program that utilizes OSINT techniques, it may be time to invest in one; these results show that effective OSINT gathering is a clear way to improve caseload productivity.

Has your organization invested in OSINT gathering tools and process to aid financial crime investigations?

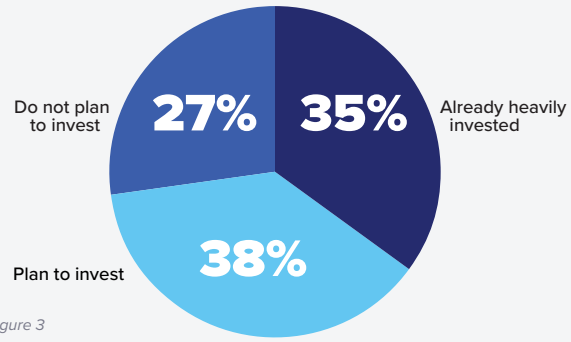

Figure 3

For those who can handle more cases, have you invested in OSINT gathering capabilities?

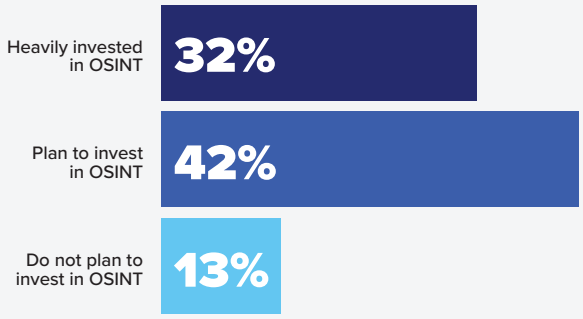

Figure 4

HOW CAN MY ORGANIZATION IMPROVE CASELOAD PRODUCTIVITY?
Jump to > Insights: Making the Right Investment in People, Process and Tools

Typical Scope of Research Collection and Analysis Revealed

Survey respondents provided interesting insight into the scope of their day-to-day activities. These types of "humans in the loop" investigations can't be automated or eliminated through preventive security technologies. So in the framework of people, processes and tools, it's important to have a good understanding of areas contributing to inefficiency and hampering productivity.

So what does a typical investigation look like?

International

58 percent of investigations involve multiple countries (see figure 5) regardless if an organization operates globally or not. International investigations create tradecraft requirements for processes and workflow tools. Challenges include in-geo IP addressing for site access and language barriers and local time zone considerations. Failing to look like a typical visitor to adversary sites in terms of location, time and language can be a tip-off and derail an investigation, contributing to caseload backup.

What is the geographic scope for your online investigative activities?

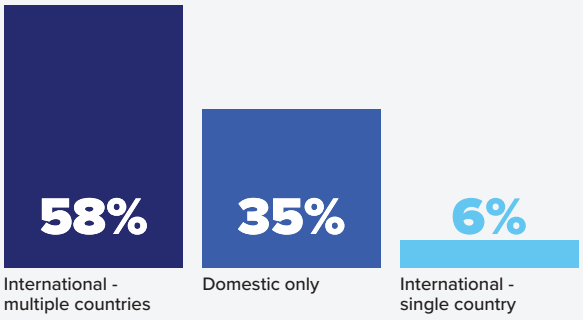

Figure 5

Collaborative

50 percent of cases involve two to four analysts; 14 percent include five or more (see figure 6). The number of analysts involved in the typical financial crimes investigation indicates they need to collaborate extensively. 52 percent of respondents strongly agreed that they need to collaborate safely and securely with their peers (see figure 7).

How many analysts work jointly on a typical online investigation?

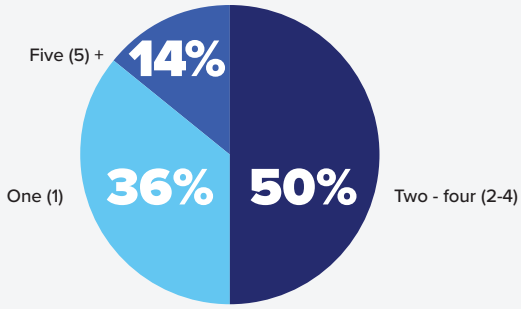

Figure 6

We need to safely and securely collaborate with peers in the analysis of collected research

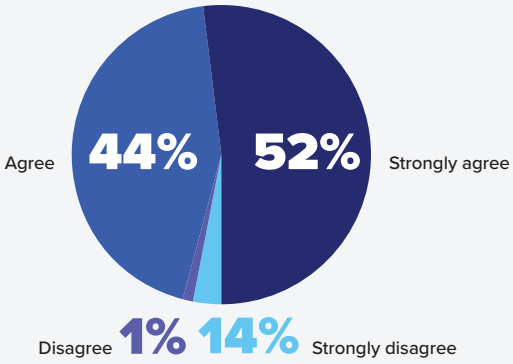

Figure 7

How, where and with whom investigators collaborate are important considerations. Research needs to be kept externally from the organization to limit risk but be properly accessible to all investigators involved in the case. Specifically with financial crimes, this off-network storage needs to maintain chain-of-custody and preserve non-repudiation of all the collected assets. Encrypted storage and audit trails must be a part of enabling your analysts to collaborate.

The inability to collaborate can have major implications on caseload productivity. If investigators lack the tools and processes to collaborate well, efforts may be unnecessarily duplicated and enlightening connections between points of research could go unnoticed, thus prolonging the time it takes to close out a case.

In-Depth

Effective collaboration requires collecting and sharing a large number of assets, files and documents. 59 percent strongly agreed that they needed integrated tools for evidence capture, analysis and storage (see figure 8). Integrated tools for these tasks greatly simplify workflows, decrease time spent on administrative-type tasks and enable investigators to work through evidence faster.

We need integrated tools for evidence capture, analysis and storage

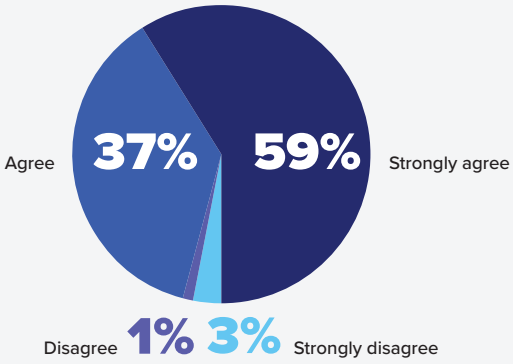

Figure 8

Additionally, 40 percent of cases require investigating six or more sites; of these, more than 40 percent require 10 or more (see figure 9). This statistic emphasizes the depth of typical investigations and the need to streamline collaboration.

Involved

42 percent of survey respondents spend between three and eight hours of investigation time per case; 26 percent spend nine or more hours (see figure 10). While productivity is an issue for the majority of respondents, these timeframes can be a good benchmark for your financial crime investigations team to understand productivity relative to their peers. Especially if you're in the quarter of investigators spending more than nine hours on investigations, you should look critically for inefficiencies in your workflows and see how you can bring research time down.

Investigator Challenges Run Counter to Organizational Policy

Enabling and supporting an ad-hoc online research team for financial crimes is a challenge for most IT teams. Investigator needs often fall outside of standard corporate policies — from the web resource access privileges, to the infrastructure requirements that protect IT and corporate assets, to compliance and risk management to oversee investigation activities. As a result, investigators are often not equipped to follow leads to all corners of the web, potentially adding to time spent on research.

Dark Web Access

Criminals have the open, deep and dark web at their disposal. This offers a lot of places to hide, and for investigators, a lot of ground to cover. 25 percent of respondents are leveraging the dark web for investigations. But a whopping 46 percent don't, though they indicate that it would be valuable to do so if it could be done securely and with an audit trail to satisfy compliance and risk management teams (see figure 11).

How many websites do you need to research for a typical investigation?

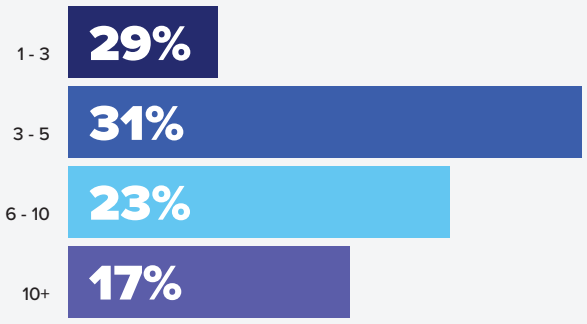

Figure 9

How much time cumulatively over days do you spend researching online for a typical investigation?

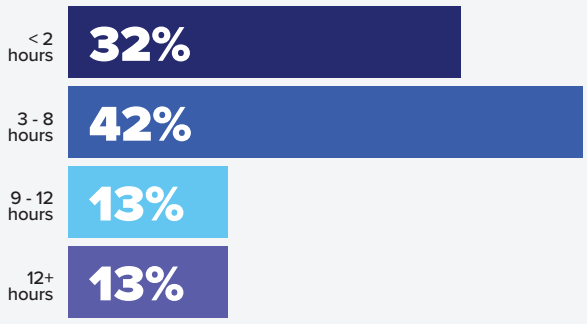

Figure 10

Are you/your team researching and collecting evidence from the dark web?

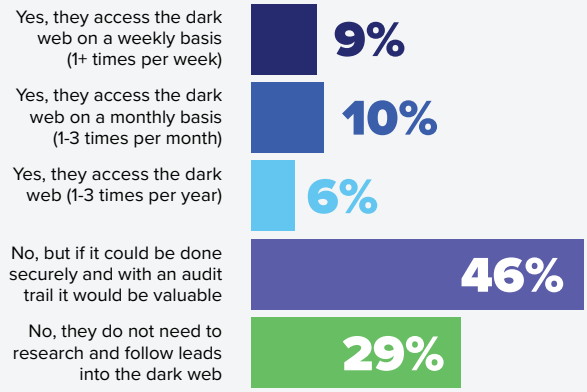

Figure 11

For investigators to keep up with their adversaries and improve time-to-insight and overall productivity, companies should train and equip them properly for dark web access. This requires maintaining detailed audit logs that capture and securely store all researcher activities; providing isolation from malicious files and sites; and offering rock-solid anonymity to prevent retribution against the company and/or exposing to a target that they are being investigated.

Isolation

Common financial crime investigations into money laundering, financial fraud, customer-targeted phishing, etc. require investigators to visit and collect assets from sites and forums with malicious intent outside the dark web. Nearly all (98 percent) of respondents agree they need to protect IT infrastructure while browsing unsafe sites (see figure 12).

The potential to infect corporate infrastructure is real and costly. Yet in many organizations investigators are expected to be experts in protecting themselves and the company — essentially, to have a level of IT expertise. While some investigators may be up to the challenge, remember that any effort expended by this team on protecting the company from their research activities takes away from caseload productivity. Placing the burden on IT is more logical, as long as the overhead imposed on investigators is within reason. The survey respondents indicate more investment is needed to enable this latter approach: 37 percent of respondents strongly agree, while 47 percent agree that their organization should invest more to reduce management overhead for IT related to investigations (see figure 13).

We need to protect IT infrastructure while browsing unsafe sites and/or malicious content

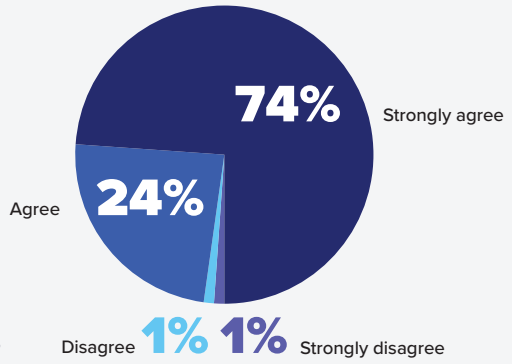

Figure 12

We should invest more to reduce management overhead for IT related to investigations

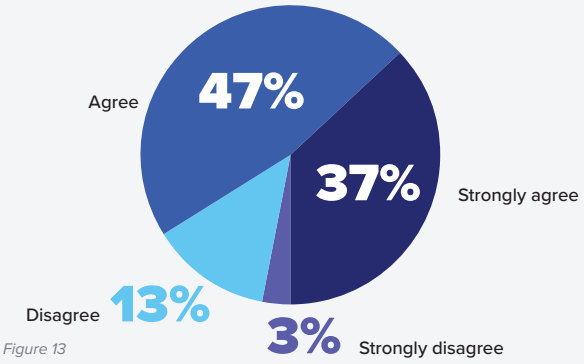

Figure 13

Anonymity

Anonymity during investigations is critical according to 50 percent of survey respondents; an additional 40 percent indicated it was desirable for both the investigator and their company (see figure 14).

This statistic is surprising in relation to a finding from a previous Authentic8-ACFCS survey conducted earlier in 2020. It found 58 percent of respondents conducted investigations without protection via a local browser on their PC. The contradiction of belief and practice shows a shortcoming in proper investigator enablement.

Is it critical to you/your organization that online research activities be conducted anonymously?

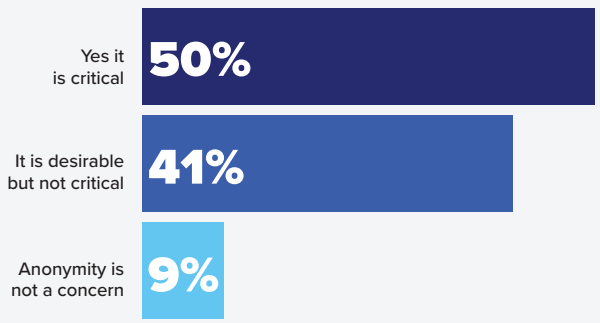

Figure 14

Investigators must operate under the assumption that research targets are paying attention, looking for signs that they are being watched. Managing the online fingerprint (i.e., managed attribution) is an important part of an investigator's tradecraft. Local browsers can reveal detailed information about the investigator, organization and corporate assets, even with incognito mode, VPN or privacy plugins in place. This attribution leakage can open companies and individuals to retribution from research targets as well as jeopardize investigations, putting the organization at a variety of risks and adding to the caseload productivity issue.

Training

Despite the disruption caused by COVID-19 in 2020, the shift to working from home did not rank among investigators' top challenges nor did hiring/retaining staff. Two of the biggest challenges include training: to keep up with evolving adversary techniques and evolving compliance and regulatory changes (see figure 15).

These types of training are not the typical employee training conducted by HR or compliance departments, so frequently this type of specialized training falls through the cracks. But online investigators need to be in continuous learning-mode to be efficient and effective in their day-to-day activities. Budgeting for and investing in this element of enabling analyst teams will produce strong returns in the quality and quantity of investigations they're able to conduct.

Figure 15

silo By Authentic8

INSIGHTS:
Making the Right Investment in People, Process and Tools

Organizations face a dilemma: How can they keep up with the increasing caseload demands, when a majority of their investigators say that caseload productivity is stagnant or declining? Do they go on a hiring spree, or do they invest in productivity enhancement? Most crime investigator managers would hope for the latter, but where can they start?

To overcome productivity issues, investment in OSINT gathering capabilities will accelerate time-to-insight for investigations. This may require a combination of investments including new hires, workflow enhancements and new technology. But before a dollar is spent, it's important to first understand the inefficiencies and gaps in your current investigation program.

STEP 1:
Understand the typical scope of online research collection and analysis

Financial crime investigations are global, require several research sources and involve multiple analysts that need to share findings and collaborate with peers.

To meet the needs of this typical scope — particularly its collaborative aspects — respondents strongly indicated they needed integration across research, evidence capture, analysis and storage. Investing in understanding this process and streamlining opportunities should be the first step in improving productivity, before bringing on new analysts and investing in new technology. To understand if new personnel investments are in fact needed, establish a baseline set of metrics to understand where resources are needed most. If technology investments are required, look for a solution that can enable your specific investigation use cases and also addresses as much of your analyst workflow as possible through a single pane of glass.

STEP 2:
Understand the unique challenges faced by investigators that typically run counter to organizational policy

Increasing productivity for analyst teams in your organization comes with unique requirements that are typically outside the boundaries of what an IT department is willing and able to support. As a result, teams are not equipped to follow leads to all corners of the web.

The survey responses highlight challenges including access to the dark web, full isolation from web-borne threats, the ability to maintain anonymity and continuous training to keep up with evolving threats.

Nearly half of survey respondents are not currently leveraging the dark web in investigations, but they recognize the value this capability would add. While web-borne risks are present in the open and deep web, they grow more severe the deeper you get, even potentially putting researchers and their organizations at risk of physical harm, not to mention risk to IT infrastructure. Investigators recognize this risk, but they are often left to their own devices to figure out how to overcome it. Even with the help of an IT resource, do-it-yourself approaches through "dirty" connections, VPNs, virtual or "burner" machines, etc. is time consuming, and time is money. Pausing investigations to wait for IT permissions also drives down productivity.

STEP 2 CONTINUED:

Additionally, allowing analysts to manage attribution through incognito mode or other cookie blocking is child's play to sophisticated adversaries. Investigators are frequently forced to use a general-purpose browser and traverse over the corporate network. There is valid concern these unsophisticated methods could result in attribution data leaks, exposing themselves and the company to exploitation. Respondents indicated that anonymity for the investigator and the company is not just important — it's critical. Blown investigations and retribution are real possibilities with potential for virtual or physical harm, not to mention wasted effort.

To keep pace with adversaries, respondents recognize the need for continuing training on evolving criminal tactics, techniques and procedures as well as changes in technology that could be harnessed by adversaries or the investigators themselves. Ongoing, specialized training for investigators can improve not only the effectiveness of the research, but also the efficiency by which they can move through cases.

STEP 3:

Assess practical options for addressing the unique needs and challenges

Compared to financial crime feeds or prevention technologies, the function of financial crime investigations includes a critical human element. Engaging investigators in an assessment of their productivity, typical case scope and unique day-to-day challenges in comparison to peers (as in this survey) is a worthwhile exercise — especially if you find yourself among the majority with caseload productivity challenges.

Based on the overall survey results, tools and tradecraft are two areas for improving productivity. Getting a grasp of any inefficiencies or gaps in these areas is a good starting point for many organizations. Below is a list of questions to get you started.

Tools

- Do investigators come across leads where leveraging the dark web would help an investigation?
- What does their workflow and tool set look like across collection, analysis and action?
- Are they cobbling together what they need on their own? If so, would efficiencies be realized with a standardized, purpose-built research platform across crime, fraud or compliance teams?

Tradecraft

- What's the team's maturity in terms of tradecraft?
- Do they need continuous training to keep up with the adversary?
- Are there junior analysts that need to be onboarded with the basics of conducting a proper online investigation?
- Are they properly isolating and protecting themselves and the company infrastructure from malicious threats? If they are, how much effort does it take them to get into this position (e.g., separate workstation, VM creation, persona management, VPN establishment, etc.)?
- Are they managing attribution during their research to get the most out of their efforts as well as protect the company from retribution?

Conclusion

A strong link exists between the caseload productivity of financial crime investigators and the bottom line of financial service institutions or the integrity of government and law enforcement agencies. If investigators aren't able to meet the demands of increased adversarial behavior, their organization risks monetary losses, compliance violations and increased exposure to further crimes.

Investigators participating in this survey are clear in their needs to overcome productivity challenges. OSINT enablement emerged as a distinct indicator of healthy caseload productivity; investing in the people, process and tools for OSINT yields returns in research efficiency. Also, enabling the typical global, collaborative, in-depth and involved scope of investigations equips analysts for continued success.

Additionally, understanding that financial crimes investigations have unique needs outside of standard organizational policy is key. The majority of respondents indicated dark web research is a part of their job function or would add value if important considerations of isolation, anonymity and compliance could be met. Lastly, ensure investigators have the proper training they need. Respondents cited training as their biggest organizational challenge; overcoming it with regular, specialized training will contribute to increased productivity and investigative effectiveness.

Understanding how your financial crime investigations team compares to its peers is crucial to guiding investments in its improvement. By scrutinizing why analysts aren't able to perform their job to its fullest, where process inefficiencies lie and where technology gaps need to be filled will build a formula for healthy, productive programs to thrive today and as the financial crime landscape evolves.