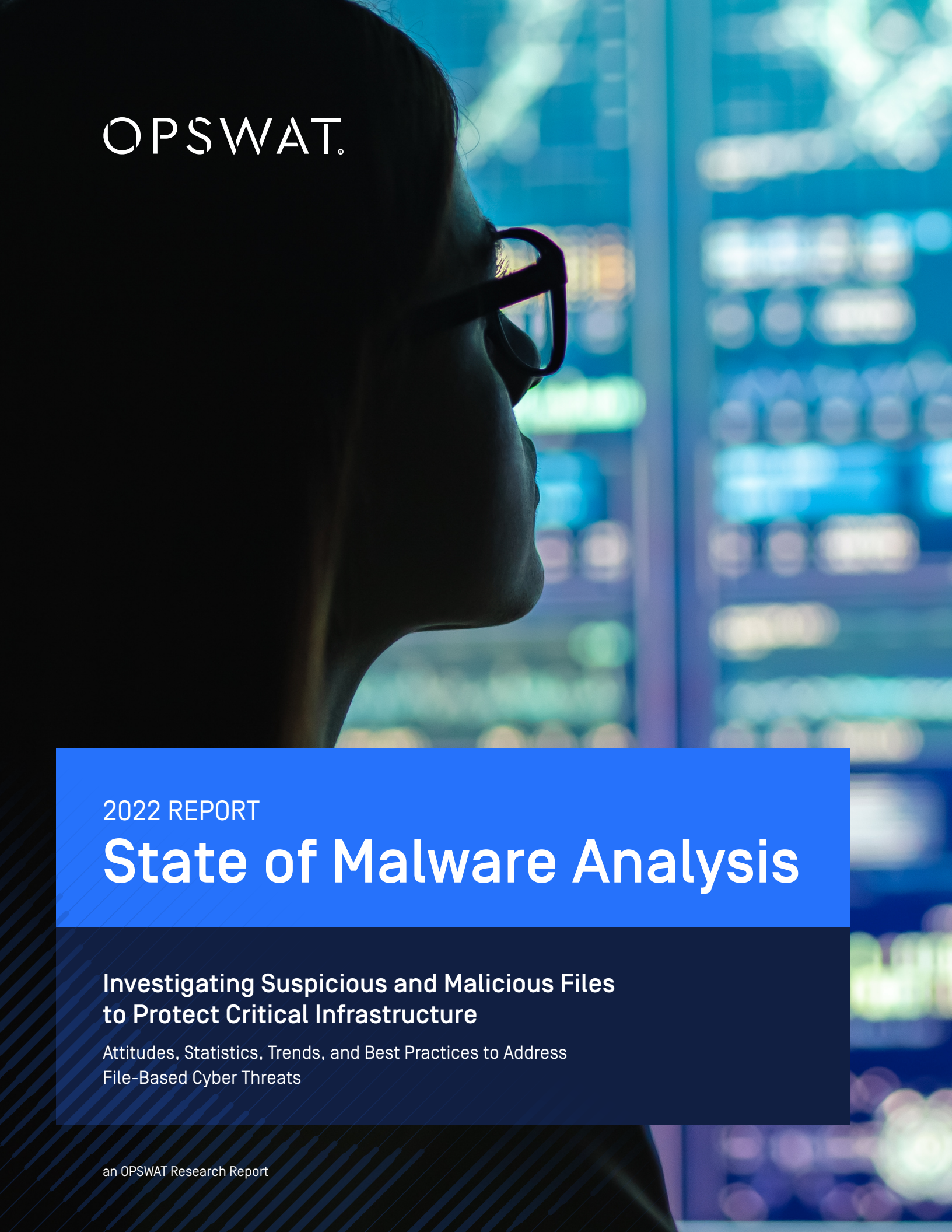


OPSWAT.

2022 REPORT

State of Malware Analysis

Investigating Suspicious and Malicious Files to Protect Critical Infrastructure

Attitudes, Statistics, Trends, and Best Practices to Address File-Based Cyber Threats

an OPSWAT Research Report

Contents

Key Findings

Malware Analysis Tools Lack Automation, Integration, and Accuracy

93%

of organizations with malware analysis capabilities **face challenges with their malware analysis toolset**.

99% stated they would benefit from additional capabilities for malware analysis.

58%

of organizations believe their greatest challenges are a **lack of automation** and 56% stated they struggle with **tools that are not integrated**.

Malware analysis can be a time-consuming manual process across multiple disparate tools and disconnected workflows.

52%

of organizations evaluating malware analysis tools identify **accuracy as the most important factor**.

Only 23%, less than one-quarter, are very confident in their ability to identify, investigate, and resolve malware threats.

Organizations Are Challenged to Find, Train, and Retain Malware Analysis Staff

94%

of organizations with malware analysis capabilities **face challenges finding malware analysis expertise**.

The top challenges are that candidates do not have the right skills and need to be trained (57%), or that there are not enough candidates (54%).

70%

of these organizations acknowledge their **malware analysis function is understaffed**.

Unfortunately, it may be getting worse; 89% struggled with staffing in their IT security organization during the past 12 months.

73%

of organizations **train their existing employees to acquire talent** for malware analysis, but 50% say **it is difficult to find training programs**.

Introduction

As organizations grapple with Advanced Persistent Threats (APTs), targeted attacks, and highly-motivated ransomware groups, malware analysis has become a critical business process to help respond to emerging threats. Mature organizations have moved beyond "check the box" compliance to adopt a security posture that not only "assumes breach" but also proactively consumes threat intelligence to better understand their adversaries and hunts for threats to stay ahead of attackers.

It is evident that malware analysis is maturing as a business process since 48% of surveyed organizations reported that they have a "dedicated" malware analysis function. Furthermore, the majority of surveyed organizations (58%) reported intermediate capabilities for malware analysis, such as sandbox tools for threat detection.

However, despite this growing sense of maturity, nearly every organization (93%) is challenged by malware analysis. These challenges are rooted in tedious manual processes – a lack of automation, integration, and accuracy.

Furthermore, even more organizations (94%) are challenged by the staffing requirements for malware analysis – finding, training and retaining experienced malware analysis talent. Even worse, struggles with burnout point toward a greater trend of employees leaving the workforce – the cybersecurity skills gap has never seemed more apparent.

Consequently, most organizations (66%) are turning to managed security service providers (MSSPs) and vendors to help shoulder the burden (at least partially). Even more so, 74% of organizations are training existing employees to acquire malware analysis expertise.

If malware analysis is to continue maturing as a business function, then organizations need to be aware of their current limitations. OPSWAT conducted this research to help organizations understand the greatest challenges facing malware analysis today so they can make better-informed decisions and improve their own programs.

What is Malware Analysis?

"Malware analysis" defines the set of activities supporting file-level investigations of suspicious files (potential spyware, ransomware, APTs, remote Trojans, key-loggers, etc.) to understand their behaviors and purpose. This is sometimes called file investigation or reverse engineering and serves several elements of the business including threat management, risk and compliance, incident response, threat hunting, digital forensics, and so forth.

The Technology:

Malware Analysis Lacks Automation, Integration, and Accuracy

Effective incident response, threat hunting, and other mature cybersecurity functions rely on quality threat intelligence that delivers insight into how malware behaves and the tactics adversaries implement. File-based malware analysis plays an important role in providing this visibility; however, it is also one of the greatest challenges to overcome. There are too many manual processes, too many tools, not enough integration, and ultimately poor data outcomes – it is an inefficient process that can create a bottleneck – and when responding to an attack, time is of the essence.

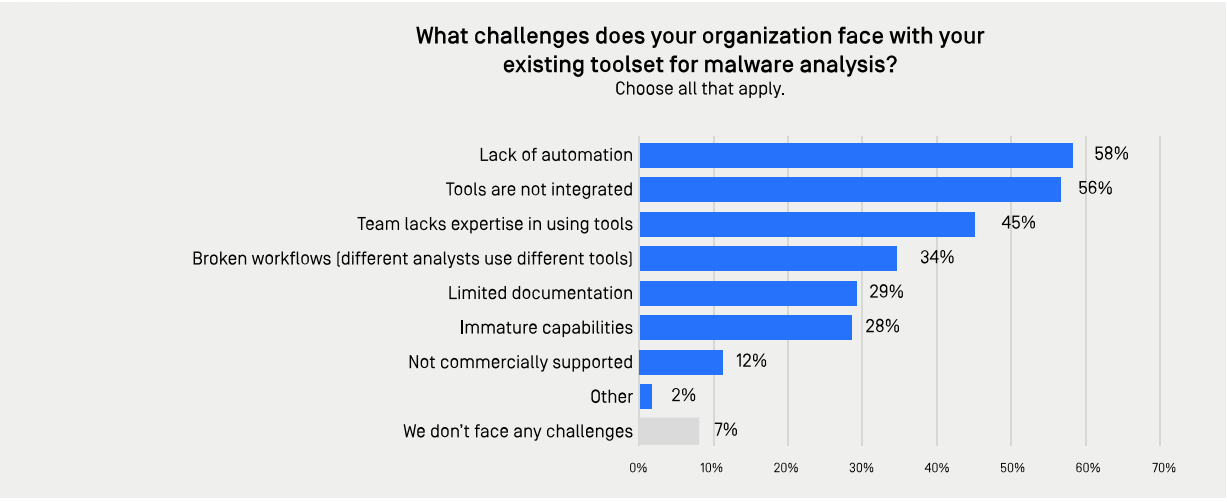


Fig 1: 93% face challenges with their malware analysis toolset; lack of automation / integration top list

Overwhelmingly, 93% of organizations with malware analysis capabilities face challenges with their malware analysis toolset. The majority of these organizations cite the lack of automation (58%) and tools that are not integrated (56%) as their top challenges – these are challenges that reveal malware analysis as a time-consuming manual process. Furthermore, nearly half of these organizations (45%) also noted that their team lacks expertise in using tools – we will explore this human element later.

58% **of organizations with malware analysis capabilities lack automation, followed by a lack of integration.**

The lack of integration between malware analysis tools can become a sore spot for organizations that use multiple tools – and most of them do. Nearly three-quarters (72%) of organizations with malware analysis capabilities are using three or more different types of malware analysis tools: 86% are using anti-malware tools, 58% are using forensic tools, and 53% are using dynamic analysis or sandbox tools.

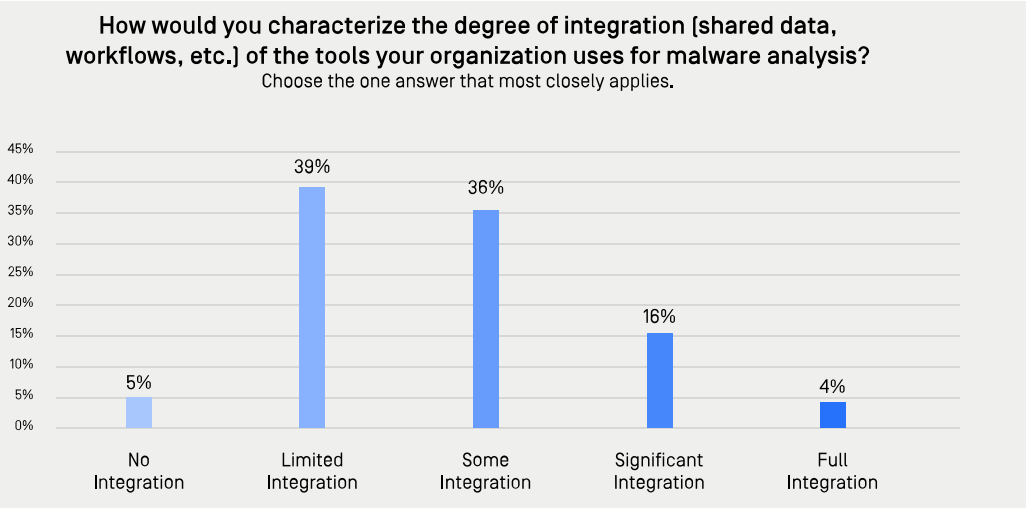


Fig 2: Malware analysis tools typically have a low level of integration

Overwhelmingly, 87% of these organizations are purchasing commercial tools from security vendors; furthermore, more than one-third (38%) are using tools from the open source community, and more than one-quarter (28%) are using custom, homegrown, or in-house tools. However, only 20% of the survey participants reported any significant integration among malware analysis tools. It is clear that this lack of integration is a challenge, which adds additional complexity to these time-consuming manual processes. More complexity stalls productivity and introduces the potential for error.

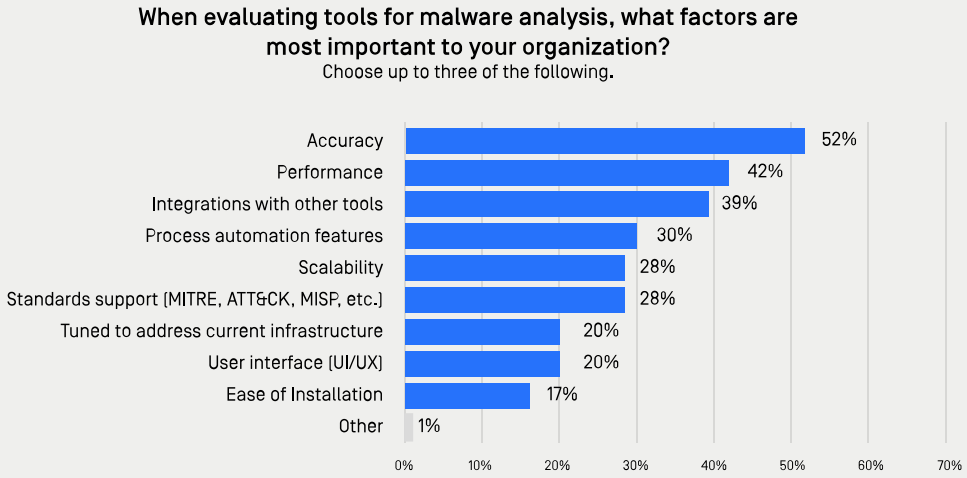


Fig 3: Accuracy is the top factor when evaluating tools for malware analysis

When it comes to evaluating tools for malware analysis, integration with other tools is one of the top three factors, but accuracy and performance are the most important. In fact, accuracy is the only factor that a majority of survey participants (52%) believed was the most important. One interpretation could be that accuracy is the most important because these organizations know how much they already struggle with poor data and a general lack of actionable intelligence. False positives are another issue that demands better accuracy, as critical time could be wasted clearing erroneous alerts instead of focusing on real threats.

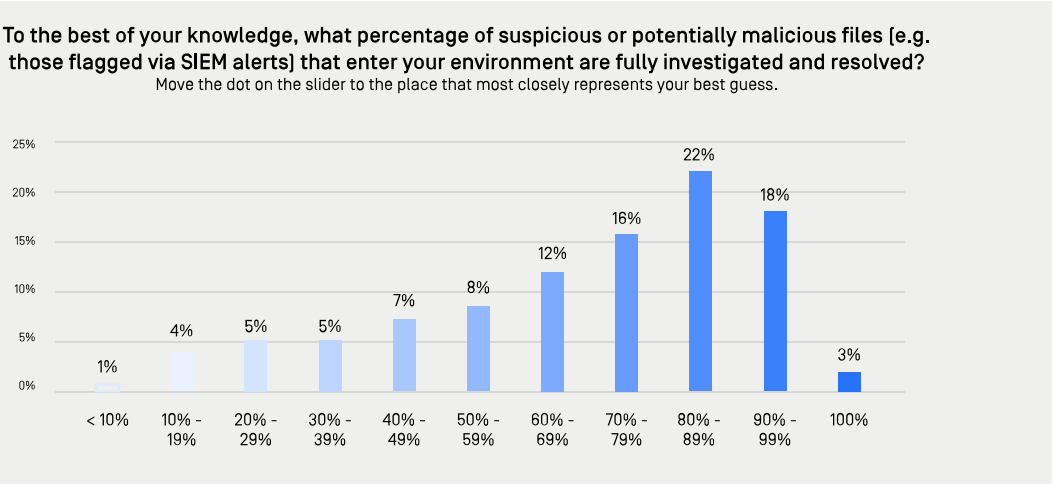


Fig 4: Only 21% report that they resolve more than 90% of malicious files

Only 3% of organizations are able to fully investigate and resolve malicious files through malware analysis. Less than one-quarter (23%) are very confident in their ability to identify, investigate, and resolve malware threats. In fact, 80% of these organizations resolve less than 90% of their malicious files – and one in five (22%) resolves less than half!

The sheer volume of cybersecurity alerts, compounded by the vast majority being false positives requiring further disposition, simply overwhelms the capacity of existing staff. And this gap perpetuates day after day increasing the risk of a breach. It seems clear that malware analysis could be improved with better accuracy and performance, perhaps leveraging automation across multiple tools, thereby improving analyst productivity and the organizations' ability to keep up.

One interesting observation is that executives and managers were more than twice as likely as their front line staff to think they resolve 90% or more of their suspicious files – perhaps because upper management is more removed from these time-consuming and error-prone manual processes. Ultimately, neither group (only 23%) was very confident in their abilities to resolve 90% or more of their suspicious files. There is a lot of room for improvement.

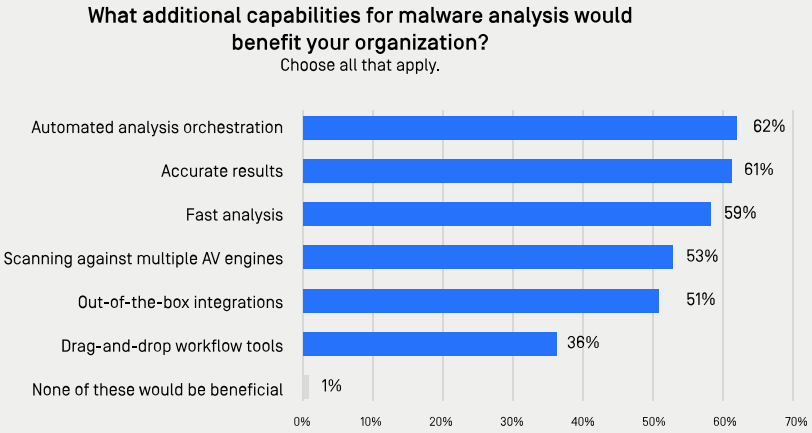


Fig 5: 99% would benefit from additional capabilities for malware analysis

When organizations face so many challenges with malware analysis, it is easy to understand why they need additional capabilities. Remarkably, the majority of these organizations would benefit from automated analysis orchestration (62%), accurate results (61%), fast analysis (59%), scanning with multiple AV engines (53%), and out-of-the-box integrations (51%). Of course, all of these capabilities could help reduce manual actions and improve response times, which brings us to our next point: the human element.

The Human Element:

The Cybersecurity Skills Gap Hits Malware Analysis

The cybersecurity skills gap has been an issue for more than a decade (Evans and Reeder published A Human Capital Crisis in Cybersecurity in 2010). This skills gap is even more pervasive with malware analysis. According to these survey participants, 66% believe their incident response function is understaffed and even more (70%) believe that their malware analysis function is understaffed.

More than half of these organizations (53%) hire new employees to acquire talent for malware analysis, but even more (73%) train their existing talent; however, both of these approaches have their own challenges.

70% of organizations believe that their malware analysis function is understaffed.

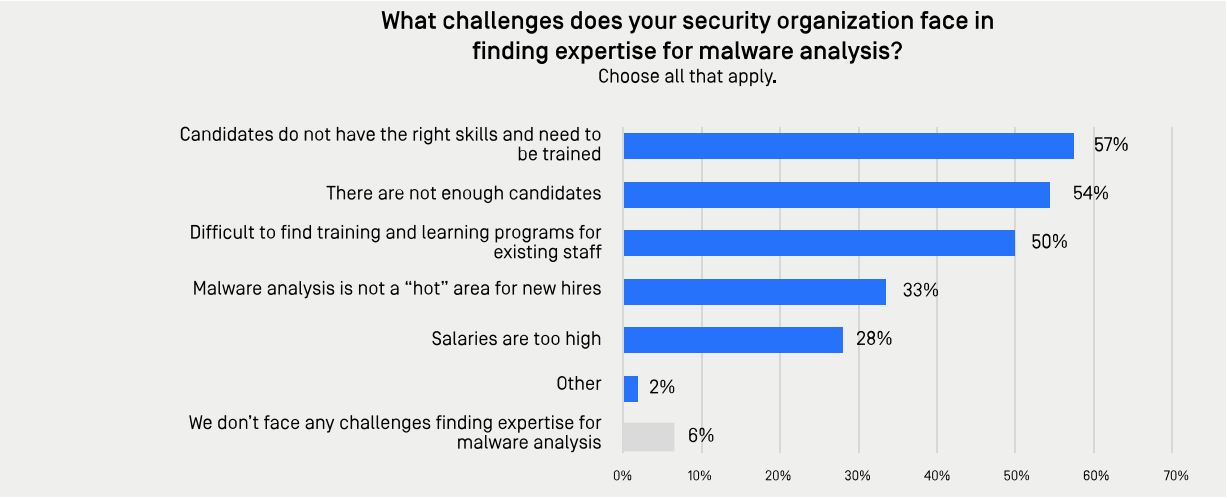


Fig 6: 94% report specific challenges finding malware analysis expertise

Overwhelmingly, 94% of organizations with malware analysis capabilities face challenges in finding experienced malware analysts. The majority of these organizations believe that candidates do not have the right skills and need to be trained (57%), or that there simply are not enough candidates (54%). Furthermore, half of these organizations believe that it is difficult to find training programs for existing staff (50%). This challenge seems to be double-edged, i.e. there is a lack of talent in the job market and it is difficult to train existing talent.

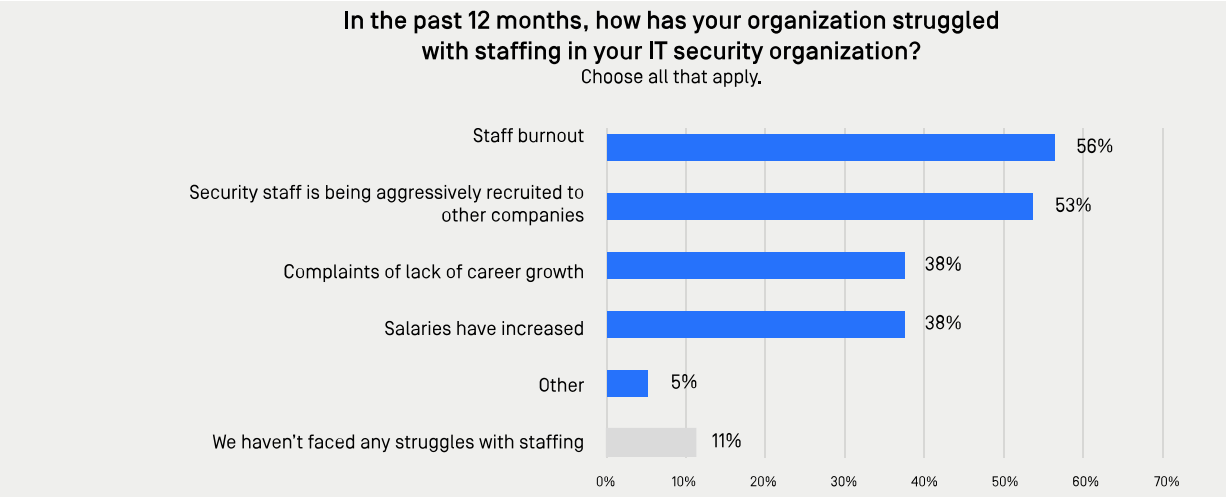


Fig 7: 89% report their IT security team has faced staffing challenges

This skills gap is even more pronounced in the midst of the great resignation. According to the U.S. Department of Labor Statistics, 4.5 million workers quit (across all industries) in November 2021, including 2% of information industry workers. Among organizations with malware analysis capabilities, 89% struggled with staffing in their IT security organization during the past 12 months. The majority of these organizations have experienced staff burnout (56%), or their security staff are being aggressively recruited to other companies (53%) - and with well over one-third of these organizations (38%) concerned with increasing cybersecurity salaries or a lack of career growth plans, staff have chosen to leave. Extrapolating these findings, it seems just as likely that staff burnout could be caused by tedious processes and a sense of constantly being backlogged, or that they left to work for a company with better tools and mature processes.

Furthermore, there is a management disconnect that suggests potential inertia from leadership in improving front-line support. There was an interesting trend across several questions that revealed an inflated perception from senior management regarding the ability to investigate and resolve alerts related to suspicious or malicious files.

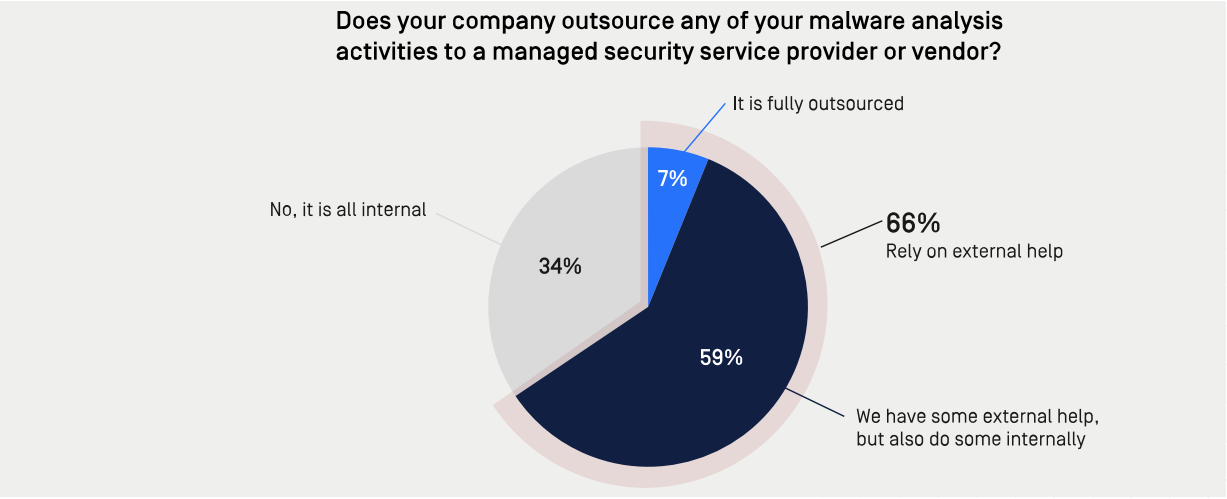


Fig 8: Two-thirds (66%) rely on external help for malware analysis

With so many challenges finding, training, and retaining malware analysis experts, it should come as no surprise that two-thirds (66%) of these organizations outsource some of their malware analysis activities to a managed security service provider (MSSP) or third-party vendor. Ultimately, it seems like organizations would prefer to train their own employees to perform malware analysis, they have just been challenged to find an effective training program.

Additional Findings

Beyond the technical limitations of malware analysis tools and the staffing challenges of malware analysis experts, there were a few additional survey questions that yielded interesting results that didn't quite fit elsewhere.

Organizational Responsibility

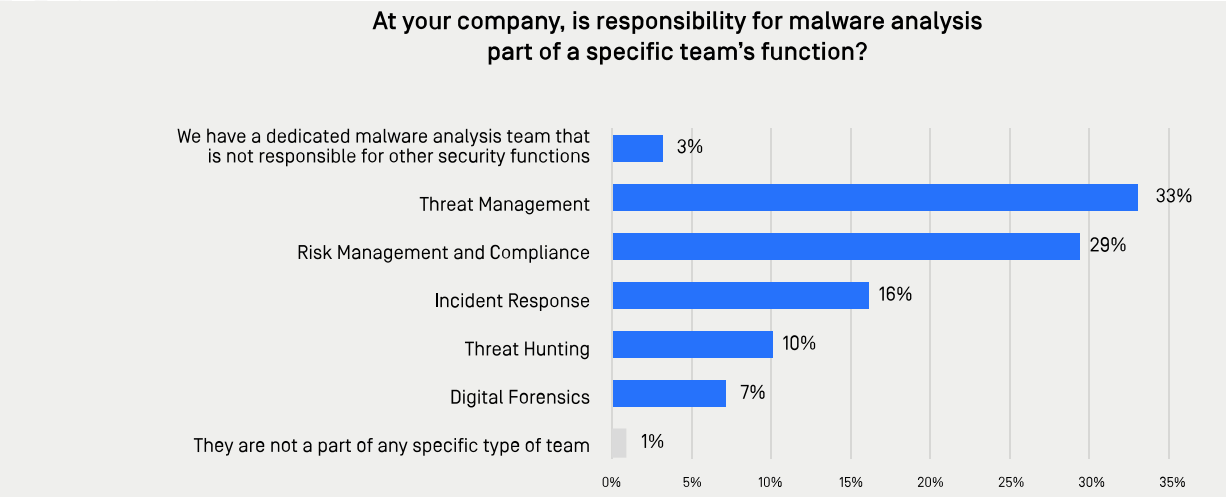


Fig 9: Malware analysis is typically owned by threat management or risk management/compliance

The responsibility for malware analysis shows a surprisingly broad range of functional owners, with threat management (33%) representing the largest organizational group. Two-thirds (64%) reported that malware analysis ownership resides in the general IT security or InfoSec organization which typically manages the security controls.

Attack Vectors

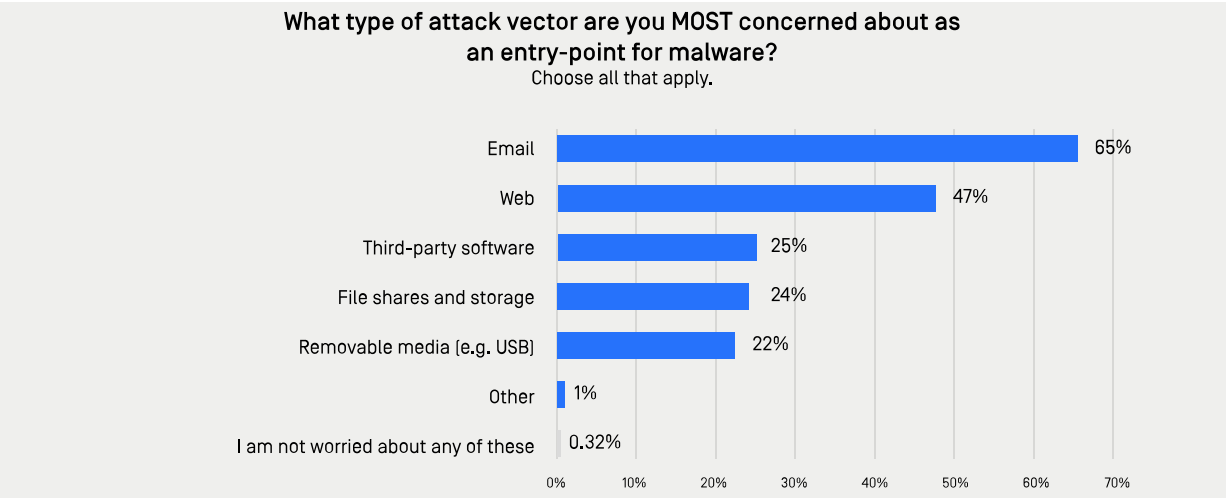


Fig 10: Email is the most concerning potential entry-point for malware reported

It may not be a surprise that email (65%) and web (47%) are the top two attack vectors that concern these organizations; after all, these are the most obvious choices. However, what is interesting is that a quarter (25%) of survey participants eschewed these more obvious choices in favor of third-party software – it seems that third-party software risk, perhaps made more visible from recent SolarWinds and Log4J events, is becoming an elevated concern within the industry.

Cloud

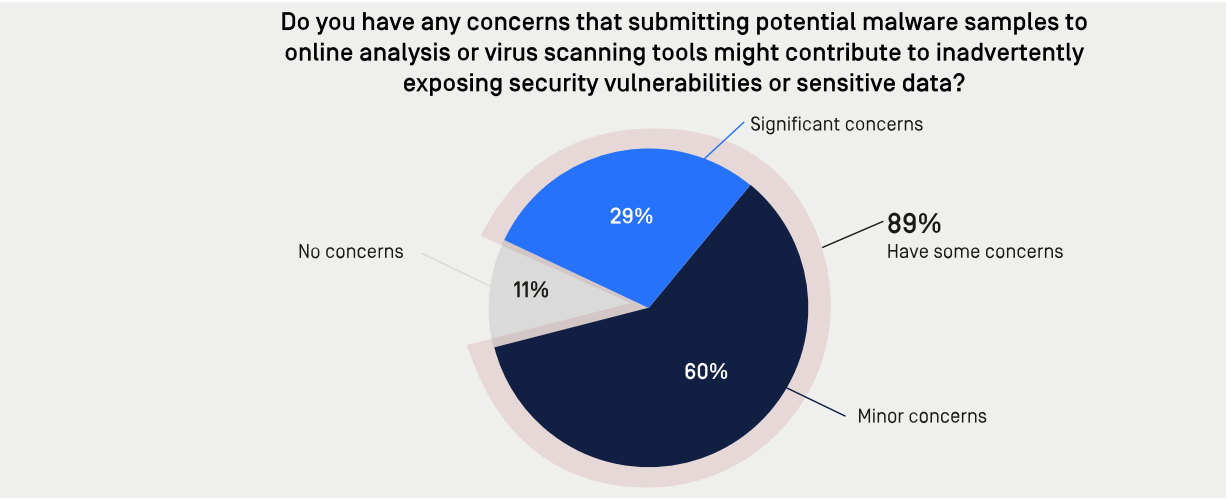


Fig 11: 9 in 10 (89%) have concerns about using online tools for malware analysis

Beyond the threats of email, web, and third-party software is another third-party risk: cloud-based malware analysis platforms. Overwhelmingly, 89% of survey participants shared some concerns that submitting malware samples to online analysis and virus scanning tools might inadvertently expose security vulnerabilities or sensitive data. Once again, it is interesting to note that executives are less concerned with this risk than team managers or individual contributors, who often are hyper-sensitive to security risks and run a bit contradictory to the broader acceptance of cloud migration trends for business applications.

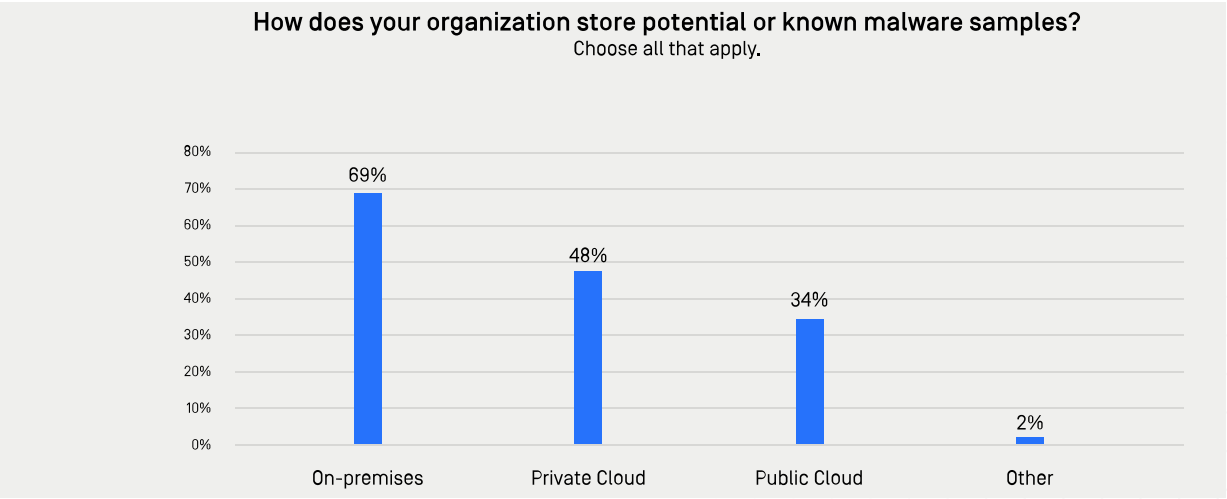


Fig 12: Only a third (34%) store malware samples in the public cloud

This concern with third-party risk can also be seen in how organizations store their malware samples. Only one-third (34%) of these organizations store their malware samples on the public cloud, while more than two-thirds (69%) of these organizations store their malware samples on-premises.

Conclusions, Recommendations, Methodology

The technical limitations of malware analysis and the struggle to find experienced malware analysts are two sides of the same coin. The demand for more automated, integrated, and accurate solutions becomes even more pronounced when organizations are understaffed, and their employees lack the training they need to work effectively.

Malware analysis is a time-consuming manual process, made all the more complex by tools that are not integrated. Such monotonous workflows can become the source of employee burnout, or introduce human error into the process – the demand for high-performance and accurate solutions is at a premium. Security can be enhanced through less complexity.

The fact that **20% of surveyed organizations resolve less than 50%** of their malware analysis queue is indicative of how these challenges can spiral out of control for so many.

Recommendations

Business leaders should realize that investing in more automated, integrated, and accurate solutions is a win-win situation because it enables their employees to work more efficiently, more effectively, and less tediously – resulting in happier staff. That spells higher performance and lower costs in the long run, and a more secure posture going forward.

Finally, the decade-long cybersecurity skills gap has never seemed more apparent – organizations need to realize that there is a shortage of experienced malware analysis talent. Partnering with MSSPs and training programs can help bridge this skills gap. Streamlined solutions can help lower this technical barrier to malware analysis with enhanced automation, integration, and accurate results.

Methodology

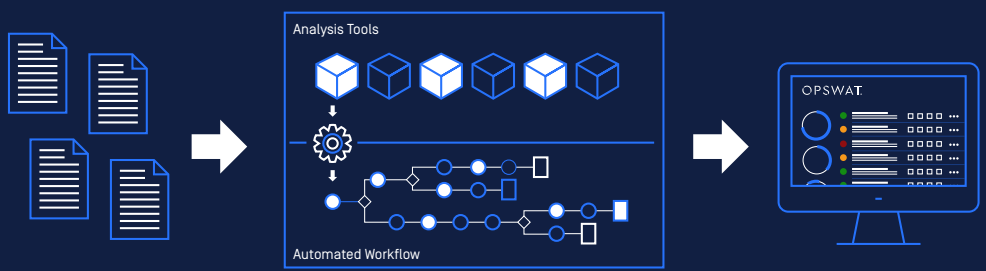
Dimensional Research, an independent research firm specializing in enterprise technology, invited independent sources of IT security professionals to participate in an online survey. A variety of questions were asked on topics related to general security and malware analysis. Responses were captured between December 8 and December 21, 2021.

A total of 309 qualified participants completed the survey, comprising 17+ industries where 54% included Industrial Control Systems (ICS) as well as IT within their critical infrastructure. All had decision-making responsibility for security of online applications at a company that had at least 500 employees and a malware analysis security function. Participants whose company did not have malware analysis capabilities were filtered out of the survey. That was a small minority (3.7%).

OPSWAT.

MetaDefender Malware Analyzer

OPSWAT MetaDefender Malware Analyzer and OPSWAT Sandbox bring a new level of "smart" to the process of malware analysis. From introducing faster and more accurate analysis technologies, to repositioning malware analysis as a business-enabling process versus one of drudgery, IT service teams benefit from more actionable intelligence, timely responses, service uptime, and risk-adaptive operations. OPSWAT provides a complete integration, orchestration, automation and reporting framework to support your malware analysis needs. By leveraging all your existing best-of-breed tools, removing repetitive manual activities through automation, and unifying outcomes from multiple analyses, your business will benefit from more accurate and timely analysis outcomes.



Files – In | Automated File Analysis | Local Threat Intelligence – Out

Contact OPSWAT →

OPSWAT.

Trust no file. Trust no device.