State of Enterprise DFIR

2023 REPORT

MAGNET FORENSICS®

Contents

EXECUTIVE SUMMARY 1

SURVEY DEMOGRAPHICS & METHODOLOGY 3

FINDING #1: DIGITAL FORENSICS IS INCREASINGLY ABOUT INCIDENT RESPONSE 4

- Root cause identification requires improvement 6
- Data exfiltration / IP theft and business email compromise (BEC) scams are the most common incidents 8
- Ransomware and data exfiltration / IP theft have the highest impact to the victim organization 9
- Evolving cyberattack techniques are the biggest challenge facing corporate DFIR professionals 11

FINDING #2 AUTOMATION ISN'T A LUXURY — IT'S A NECESSITY 12

- The soaring volume of investigations and data are real problems 14
- DFIR personnel are feeling burnt out — and reinforcements aren't coming any time soon 15
- Organizations need to improve collection, processing, and analysis 16

FINDING #3: DFIR LEADERSHIP HAS NEVER BEEN MORE IMPORTANT 17

- Improving the state of DFIR starts at the top 18
- Organizations are potentially exposing themselves to regulatory risk 20
- Third parties are valuable extensions of internal capabilities 21

CONCLUSION & RECOMMENDATIONS 22

CONTRIBUTORS 24

ABOUT MAGNET FORENSICS 26

Executive Summary

Digital forensics is a rapidly growing and continually evolving branch of forensic science that focuses on acquiring, analyzing, and reporting on evidence from digital systems. While it has long been embraced by law enforcement agencies as an important component of criminal activity investigation, including white-collar and cybercrime, digital forensics is also applied within corporate environments.

Initially, digital forensics in the enterprise context mainly applied to resolving human resources issues, assessing policy violations, and investigating malicious insiders. However, in recent years, the tools and techniques of digital forensics have been applied to a wider range of use cases and incident types.

This report, our third in an annual series, draws upon a comprehensive survey of corporate digital forensics & incident response (DFIR) professionals in North America (NA) and Europe, the Middle East, and Africa (EMEA), and aims to provide intelligence—with analysis, interpretation, and insights, rather than just data—tailored to the needs of enterprise decision-makers, particularly those involved with IT, cybersecurity, and governance.

Taking a broad perspective on the nearly 500 survey responses reveals three key findings:

1. **Digital forensics is increasingly about incident response**
2. **Automation is needed**
3. **DFIR leaders have a real opportunity now to shape the future of their labs**

First, digital forensics in the corporate world is increasingly about incident response (IR), within the broader context of enterprise cybersecurity programs. 60% of survey respondents are part of the Security Operations (SecOps) organization, where their expertise is applied to investigate ransomware attacks, data exfiltration / IP theft, and business email compromise (BEC) scams.

Unfortunately, investigating such incidents is becoming more challenging: 42% of survey respondents report that evolving cyberattack techniques are either a large or extreme problem for their investigations, as adversaries continue to invest in more tactics, techniques, and procedures (TTPs). One very real consequence is that it's taking too long to identify the root cause of attacks. This can lead to costlier and more drawn-out consequences for organizations while also making it more difficult to learn from these attacks and prepare for future incidents.

60%

of survey respondents are part of the Security Operations (SecOps) organization.

Second, in addition to investing in modern tooling that can help DFIR practitioners investigate incidents more deeply, enterprises need to embrace automation in the specific context of digital forensics.

54% of respondents are feeling burnt out, and nearly two-thirds report that recruiting, hiring, and onboarding qualified professionals is a major challenge. A leading contributor to burnout is a lack of automation. While security automation (e.g., SOAR) is in place in many organizations, this is distinct from forensic automation, which executes a data transformation pipeline (e.g., collecting and processing evidence) by orchestrating, automating, performing, and monitoring forensic workflows. Without solutions like these, DFIR practitioners are often forced to switch between different tools and manually execute time-consuming and repetitive tasks—wasting valuable expertise and unnecessarily drawing out investigation timelines.

Third, DFIR leadership has never been more valuable. 37% of practitioners point to a lack of a cohesive IR strategy and 36% cite a lack of standardized processes as major contributors to waste. Respondents also indicate that they are struggling to interpret and adapt to the array of ever-changing regulatory requirements impacting their roles. It falls upon leaders to secure budget for the right mix of in-house capability and access to specialized third parties (e.g., forensic service providers, or FSPs), to ensure DFIR practitioners are equipped with actionable legal opinions, and to set a clear strategy.

Survey Demographics & Methodology

The web-based survey of digital forensic and incident response (DFIR) professionals was conducted from October 4, 2022, to November 1, 2022. The survey targeted North America (NA) and Europe, the Middle East, and Africa (EMEA); these regions account for 94% of the survey's 492 respondents.

Approximately two-thirds of respondents are from organizations with 500 or more employees, and the respondents represent a broad distribution of 30 different industries and sectors, including:

- Security service providers: IR providers, forensic service providers (FSPs) Managed Security Service Providers (MSSPs), Managed Detection and Response (MDR) providers, etc.
- Technology companies: hardware, software, software as a service (SaaS), etc.
- Government organizations
- Engineering
- Manufacturing
- Insurance and financial services
- Telecommunications
- Education
- Healthcare
- Utilities

The presence of DFIR professionals within such a wide range of organizations is likely a byproduct of the evolving threat landscape, in which every organization—no matter size or industry—is a potential target of cyberattacks.

The respondents occupy a variety of roles within their respective organizations, with the most common having clear association with information technology (IT), security, and governance:

- DFIR / Forensics
- IT leadership
- Governance / Regulation / Compliance (GRC)
- IT security
- Infrastructure / Operations

RESPONDENTS: BY SENIORITY

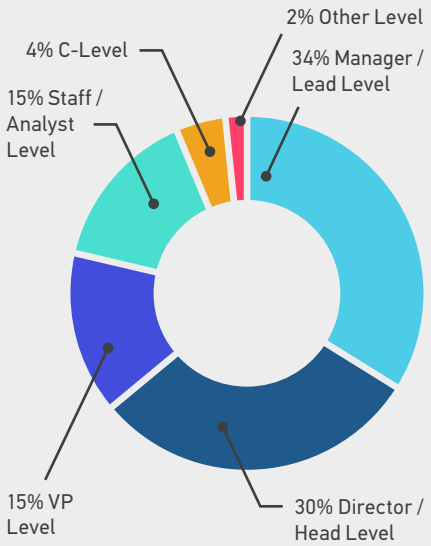


Figure 1: Distribution of respondents, by seniority

KEY INSIGHTS

FINDING #1: Digital Forensics is Increasingly About Incident Response

- Today's DFIR professionals are more likely than not to be considered part of the organization's broader security operations (SecOps) function, which speaks to the shifting nature of where their expertise is applied.
- Nearly one third of respondents indicated that identifying the root cause of incidents—which is crucial for containing the threat and strengthening security postures—requires either a complete overhaul (10%) or at least major improvements (23%).
- 42% of DFIR professionals report that evolving cyberattack techniques are either a large or extreme problem for investigations, illustrating that it's essential that DFIR teams are equipped to keep pace with adversaries' expansive and growing arsenal of TTPs.

For many years, digital forensics within a corporate setting applied primarily to resolving human resources issues (e.g., personnel disputes, harassment complaints), assessing policy violations (e.g., misuse of corporate assets), fulfilling legal obligations (e.g., eDiscovery), and investigating malicious insiders (e.g., fraud, data exfiltration, and intellectual property theft). For such use cases, dead box forensics was typically used to investigate specific endpoints or malicious insiders.

However, as the digital transformation opened up new attack vectors and made it easier for threat actors — particularly external adversaries — to conduct their operations, **investigations became more complex, and forensics became more important.** One result of this trend is that the tools and techniques of digital forensics are increasingly being integrated into formalized incident response (IR), the processes and activities that allow organizations to:

- Identify, contain, resolve, and recover from cyberattacks;
- Prepare evidence that can be used to support insurance claims, pursue legal avenues, and demonstrate duty of care to regulators; and
- Inform strategies and tactics to harden defenses against future attacks.

Recent high-profile breaches and relentless innovation in cyberattacks have led to a shift in how organizations perceive risk, with many recognizing that the important question is not if a breach will occur but when. This "assume breach" mentality forces organizations to make sure they're prepared to handle a security incident, and is a driving force behind the Zero Trust (ZT) cybersecurity paradigm.

A related outcome is that organizations have increased their investment in technologies, **including deep-dive analysis capabilities, that support a more robust incident response**. These technologies help ensure that organizations are prepared when a breach actually does occur. This has necessitated a migration from dead box forensics (which can be slow and logistically challenging) to a more dynamic approach that enables deep analysis without needing a full forensic acquisition.

The growing emphasis on digital forensics as a crucial component of cybersecurity overall, and incident response in particular, is changing how organizations are structured. In general, today's corporate DFIR professionals are considered part of the organization's security operations (SecOps) team, within the security operations center (SOC).

> "The increasing sophistication of attacker TTPs requires an increasingly sophisticated response. As organizational defenders, incident responders and forensic investigators are working together to uncover the root cause of incidents in order to harden their environments and improve their security controls."
>
> – Dean Turner, Vice President, Product Management, Private Sector

For smaller organizations, there's a 50% chance that personnel fulfilling DFIR functions are within the SOC, but the likelihood increases as the organization becomes larger, peaking with 77% for professionals within companies that have 2,500 to 4,999 employees. At 10,000 employees or more, DFIR professionals are more likely than not to be part of a dedicated DFIR group.

Root Cause Identification Requires Improvement

Cyberattackers employ **a lot of different techniques to gain initial access** into IT environments, and while identifying the root cause of an incident isn't easy (51% of respondents regard doing so as at least moderately challenging), few DFIR activities are as worthwhile. That's because containing an event, recovering from it (where applicable), and learning lessons all require, or at least strongly benefit from, accurately determining the incident's root cause.

Crucially, these **learnings contribute to a feedback loop that guides organizations as they implement new safeguards and processes**, such as updating response plans and identifying missing or required control points as part of their standard IR plan, that reduce the likelihood of future incidents. Additionally, digital forensics is critical to identifying the scope of a breach. For example, pinpointing a few hosts that exhibited lateral movement or data exfiltration isn't enough to determine if the preliminary breach or toolset remains elsewhere in the environment. Digital forensics can help root out attacker infrastructure and help to shut down a repeat incident.

The longer it takes to identify the root cause of a cybersecurity incident, the greater the threat to business continuity. While 17% of respondents reported that it takes less than 24 hours, on average, to determine the root cause (Figure 2), more than a third (36%) said that doing so takes between one day and one week. More worryingly, 22% indicated that it takes between one week and one month, and 21% reported that finding the root cause takes even longer than that.

These findings should concern security leaders, as delays open up opportunities for further attacks and disruption—after all, if you don't know how an adversary got in, then how will you keep them out in the future? For their part, DFIR professionals already recognize the need for improvements. When asked to what extent their organization needs to improve upon several DFIR functions, 10% of

> "The ability to get to root cause depends heavily on the resources of the team responsible. If the analysts are spending most of their time on whack-a-mole malware activities, there isn't proper time for root cause analysis."
>
> – Doug Metz, Professional Services Consultant, Magnet Forensics

respondents indicated that identifying the root cause of incidents required a complete overhaul, and a further 23% suggested that major improvements were necessary.

Put another way, 33% of corporate DFIR experts—one out of every three—are reporting that a critical ability requires considerable investments (and if the 10% figure doesn't seem 'big enough,' we'll note that **no other function received such support for an overhaul**).

> When you can identify and close the gaps discovered through root cause analysis, threat actors can no longer exploit the same vulnerability again, so teams can work towards a gradual reduction in breaches in addition to reducing the overall attack surface."
>
> – Doug Metz, Professional Services Consultant, Magnet Forensics

ROOT CAUSE: TIME TO DETERMINE

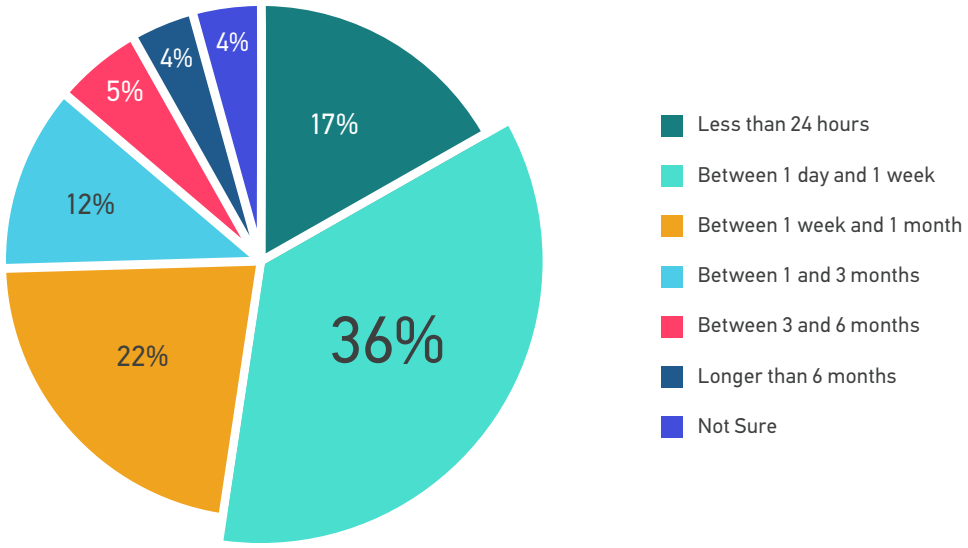


Figure 2: On average, how long does it take for a root cause to be determined?

Data Exfiltration / IP Theft and BEC Scams Are the Most Common Incidents

The evolution of DFIR shows up in the incidents that organizations most frequently encounter (Figure 3), as adversary-driven security events top the list. Data exfiltration or IP theft takes the number one spot, with 35% of respondents indicating that their organization encounters this type of security incident at least somewhat to very frequently.

While data exfiltration or IP theft are the most frequent events encountered, the three most common ways an organization can become a victim of such a data breach are double-extortion ransomware, business email compromise (BEC) scams, or a malicious insider—with ransomware being the most likely culprit.

We'll examine ransomware and data exfiltration or IP theft more in a moment, but first we'll look at BEC. These scams, in which a cybercriminal pretends to be a trusted contact and attempts to trick the recipient into transferring funds or information can be especially damaging (the FBI reported in May 2022 that **exposed losses from such scams added to $43 billion**, globally). Once funds have been transferred, they can be very difficult to recover, as scammers use bank transfers and cryptocurrency tumblers to immediately move the proceeds of their crimes elsewhere. Likewise, if intellectual property, trade secrets, personally identifiable information (PII), or any other digital data is sent to a fraudster, the victim organization cannot control or prevent it from spreading further.

FREQUENCY OF INCIDENTS (MOST TO LEAST)

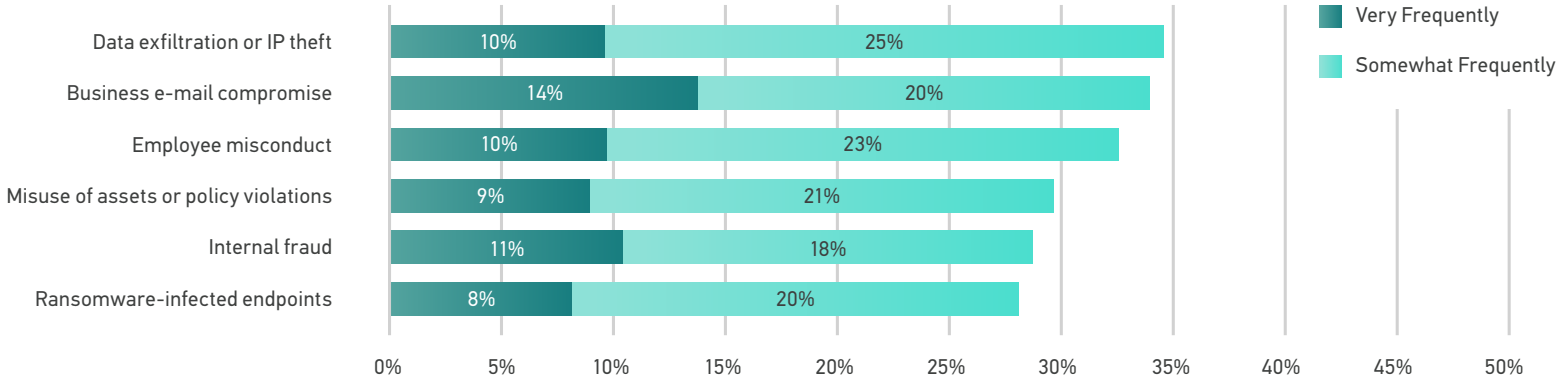


Figure 3: Please indicate how frequently your company/organization (or clients) encounters the following types of security events. [Very Frequently, Somewhat Frequently, Neither Rarely Nor Frequently, Somewhat Rarely, Very Rarely, Don't Know]

Unfortunately, large amounts of publicly available information (e.g., about partners, vendors, etc.) is available to help threat actors develop highly convincing lures. Add in the small likelihood of prosecution, and a range of techniques to execute these attacks (e.g., spoofing, spearphishing, malware), and **conditions are ripe for widespread attacks**. In fact, 14% of survey respondents indicated that their organization encounters BEC scams very frequently.

BEC scams rely heavily upon social engineering tactics to create a feeling of trust, allowing attackers to trick users. Especially sophisticated BEC scams may employ malware like Emotet or Qakbot (which themselves are often introduced via social engineering) that can hijack existing email threads, making the scammer's actions seem even more credible. Consequently, one of the most important defenses against these types of attacks is to invest in an effective phishing and security awareness training (PSAT) program to help increase awareness of such threats and build the organization's cyber resilience.

In addition to having preventative measures in place (e.g., PSAT, a vulnerability management program, endpoint defenses, detection and response capabilities etc.), organizations should keep detailed logs that can be incorporated into forensic investigations.

Moreover, having a simple way for employees to report suspicious emails—along with an amnesty policy—can encourage a culture of vigilance.

Ransomware and Data Exfiltration / IP Theft Have the Highest Impact to the Victim Organization

Security incidents can have significant impacts to organizations and the impacts are not limited to direct costs (e.g., ransoms paid) or for the duration of the attack. For example, IBM's much-cited **Cost of a Data Breach** report incorporates four process-related activities into its expenses:

- **Detection and escalation:** Activities that enable a company to reasonably detect the breach, including forensic and investigative activities, assessment and audit services, crisis management, and communications to executives and boards
- **Notification:** Activities that enable the company to notify data subjects, data protection regulators and other third parties, including: emails, letters, outbound calls or general notice to data subjects; determination of regulatory requirements; communication with regulators; and engagement of outside experts
- **Post-incident response:** Activities to help victims of a breach communicate with the company and redress activities to victims and regulators, including: help desk and inbound communications; credit monitoring and identity protection services; issuing new accounts or credit cards; legal expenditures; product discounts; and regulatory fines
- **Lost business:** Business disruption and revenue losses, including: business disruption and revenue losses from system downtime; cost of losing customers and acquiring new customers; and reputation losses and diminished goodwill

With such costs and consequences in mind, the survey respondents indicated that ransomware-infected endpoints have the highest impact to their respective organizations or clients (Figure 4).

IMPACT OF INCIDENTS (HIGHEST TO LOWEST)

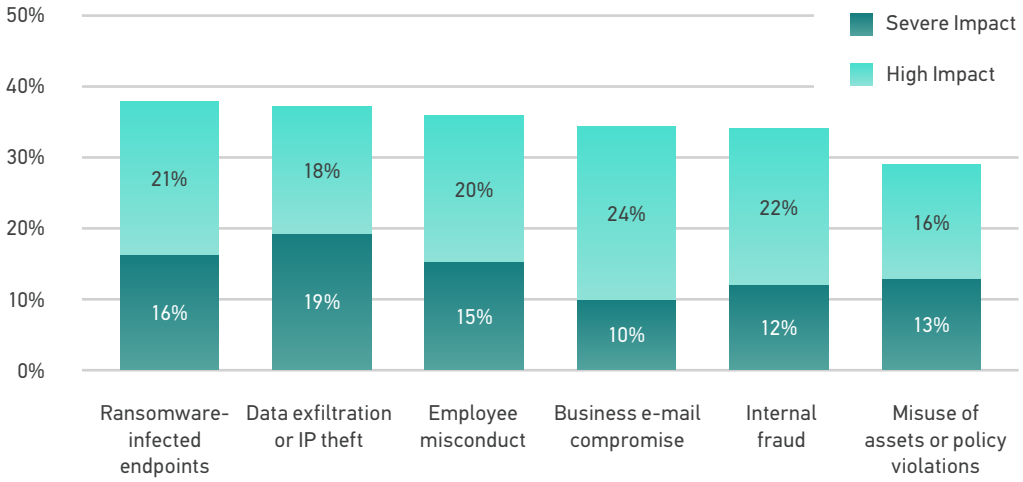


Figure 4: Please indicate the relative impact to your company/organization or clients of the following types of security events. [Severe Impact, High Impact, Moderate Impact, Low Impact, Neligible Impact, Don't Know]

Unfortunately, a mature ransomware ecosystem has flourished and attackers (e.g., LockBit, Alphv and Black Basta to name a few) are good at applying pressure to extract payments. In this new threat landscape, cybercrime perpetrators called initial access brokers (IABs) operate broad campaigns to enter dozens, hundreds, or even thousands of IT environments. Next, they perform some reconnaissance activities to identify the network owner (i.e., the organization), establish some degree of persistence, and gather additional intelligence. Then, they post the details of the compromised network (e.g., scale of compromise/infiltration, victim's industry, victim's annual revenue, etc.) on a cybercrime marketplace.

From there, a ransomware gang (or an affiliate) simply purchases the access and executes the ransomware attack, which typically combines the disruption of making systems and data unavailable with exfiltration of sensitive data and the very real threat of publicly releasing it.

In addition to causing potential embarrassment and personal friction (e.g., through the publication of HR files, personnel details, correspondence from executives, salary data, etc.) and harming competitive positions in the marketplace (e.g., by posting trade secrets and other IP), threat actors know that publishing private data can lead to costly regulatory fines for the victim (e.g., when it includes PII).

This is likely why the survey respondents rated **data exfiltration or IP theft as having the second-highest impact overall**. However, it received the most responses (19%) for the highest severity rating than ransomware (16%) (Figure 4). A plausible interpretation is that the short-term disruption directly associated with the ransomware (e.g., system and data unavailability) is regarded as less severe than the long-term consequences of the data breach component. Clearly, adversaries have found a very real pain point they can use to apply pressure for ransom payments.

Both to contain damage and to make sure the cycle of hardening defenses is helpful, it's **critical that DFIR professionals be equipped to rapidly investigate ransomware and data breach incidents**. However, cybercriminals are hard at work to make such investigations as difficult as possible.

Evolving Cyberattack Techniques Are the Biggest Challenge Facing Corporate DFIR Professionals

In recent years, **the vulnerability of the software supply chain** has been driven home repeatedly. The **full-service cybercrime economy** has virtually eliminated barriers to entry and **zero-day exploits** have impacted tens of thousands of organizations (e.g., ProxyLogon).

Complicating matters further, threat actors have discovered TTPs that make it especially hard to detect, contain, and investigate their intrusions. For example, **the use of stolen credentials has soared**, as have **attacks that target or leverage identity systems**, both of which can make it even harder to separate intruders from insiders. In parallel, the increased use of built-in system commands (living-off-the-land binaries, or "LOLBins") has made it much more difficult to detect intrusion actions against the backdrop of legitimate activity.

Unfortunately, the continued innovation of threat actors reaps them great rewards. Cybercrime proceeds have soared in recent years (although **there are signs that more organizations are choosing not to pay ransoms**), and 42% of corporate DFIR professionals indicated that evolving cyberattack techniques pose either an extreme or large problem for their investigations. This result placed evolving cyberattack techniques ahead of all other factors listed by the survey and, worryingly represents a 50% increase over last year's figure of 28%.

42%

of DFIR professionals indicate that evolving cyberattack techniques present either an extreme or large problem for their investigations.

For what it's worth, in the first edition of this report (published in 2021), DFIR professionals identified evolving cyberattack techniques as the most-concerning trend. They've been sounding the alarm for at least a few years, and organizations would do well to listen.

KEEPING UP WITH CHANGING TTPS

Many cybercrime gangs operate like Fortune 500 companies—complete with R&D specialists focused on equipping the organization with new and ever-evolving TTPs. Staying up to date is a real challenge, but here are a few tips:

- Follow the social media profiles/channels (e.g., Twitter, LinkedIn) of cybersecurity researchers and companies, as they'll often post their own research or share/promote the research of industry peers
- Faced with the uncertain future of Twitter, the infosec.exchange Mastodon instance has gained new prominence
- Government and industry organizations (e.g., MITRE, CISA), and cybersecurity-specific news media are also great sources of intelligence
- Search engine alerts, security mailing lists, and topic-specific social networking groups can also keep you apprised of the latest developments

By leveraging a cross-section of sources, you can increase the chances that important topics land in your inbox or alert stream!

KEY INSIGHTS

FINDING #2: Automation Isn't a Luxury—It's a Necessity

- **More is becoming too much**: nearly 45% of DFIR professionals report that the soaring number of investigations and volume of data they must consider together represent either an extreme (13%) or large (32%) problem.
- DFIR professionals are feeling burnt out, and reinforcements aren't on the way. More than half (54%) of respondents agreed with the statement, "**I am feeling burnt out in my job**," and an even larger proportion (64%) agreed that alert/investigation fatigue is a contributor. At the same time, recruiting, hiring, and onboarding DFIR professionals is a major challenge, so replacing burnt-out team members or expanding the team to share the load isn't a simple proposition.
- Automation already exists within most IT environments, including within SOCs, but digital forensics is a specialized field, with specialized functions. Free up human expertise and accelerate investigations by automating DFIR tasks that are today executed manually.

Automation has enormous potential to help increase the scale and efficiency of forensic investigations, both of which are needed to keep pace with rising demands.

It's worth emphasizing that the greatest promise of automation comes from helping DFIR personnel, not replacing them. By automating time-consuming and repetitive tasks that extend investigation timelines and contribute to burnout, automation will **allow DFIR practitioners to concentrate on higher-level thinking that only they can do well**—like getting to root cause, refining how incidents are detected, and identifying gaps in evidence. Additionally, this time gained back can help positively impact the signal-to-noise ratio as DFIR personnel can help to differentiate between low-severity and malicious activity.

50%+

of DFIR professionals indicate that investments in automation would be highly or extremely valuable for a range of DFIR functions.

Automation is already in place in many SOCs, but those solutions (e.g., security orchestration, automation and response, or SOAR) orchestrate and automate cybersecurity runbooks by taking telemetry, enforcing actions (e.g., on endpoints, on network controllers, etc.) and using other tools. While important for threat containment and remediation, these runbook-related activities are distinct from those performed by digital forensics automation solutions, which execute a data transformation pipeline (e.g., collecting and processing evidence) by orchestrating, automating, performing, and monitoring forensic workflows.

Indeed, despite the widespread adoption of SOAR platforms and similar cybersecurity solutions, the survey reveals that there remains much opportunity for digital forensic-specific automation investments to enable valuable improvements in DFIR outcomes.

> "It's essential for organizations to find solutions that work with their current tools and custom scripts versus scrapping their toolbox to start over. Automation platforms should be adaptable to maximize compatibility with orchestrating the alerting and response workflows organizations already have in place."
>
> – Trey Amick, Director, Forensic Consultants, Magnet Forensics

The Soaring Volume of Investigations and Data Are Real Problems

Today's corporate DFIR professionals are under enormous pressure to conduct fast and thorough investigations. Unfortunately, three developments are contributing to a landscape that can be characterized by one word: **more**. As in **more** investigation types, **more** investigations overall, and **more** data involved with each investigation.

And practitioners are recognizing the risk that comes with these demands (Figure 5). **45% of respondents regard the growing volume of investigations and data as either an extreme (13%) or large (32%) problem**. Every indication is that data volumes will continue to grow and that DFIR experts will be pulled into more investigations, so organizations need to invest in tooling—like automation—that can help experts keep pace.

Crucially, when investing in DFIR automation, it's **important that the solutions work with the existing toolset**, otherwise they could further an existing problem (37% of respondents indicated that a lack of tool integration is at least a large problem). Automation should address problems, not create new ones!

CHALLENGES: BY IMPACT TO INVESTIGATIONS (LARGEST PROBLEM TO SMALLEST PROBLEM)

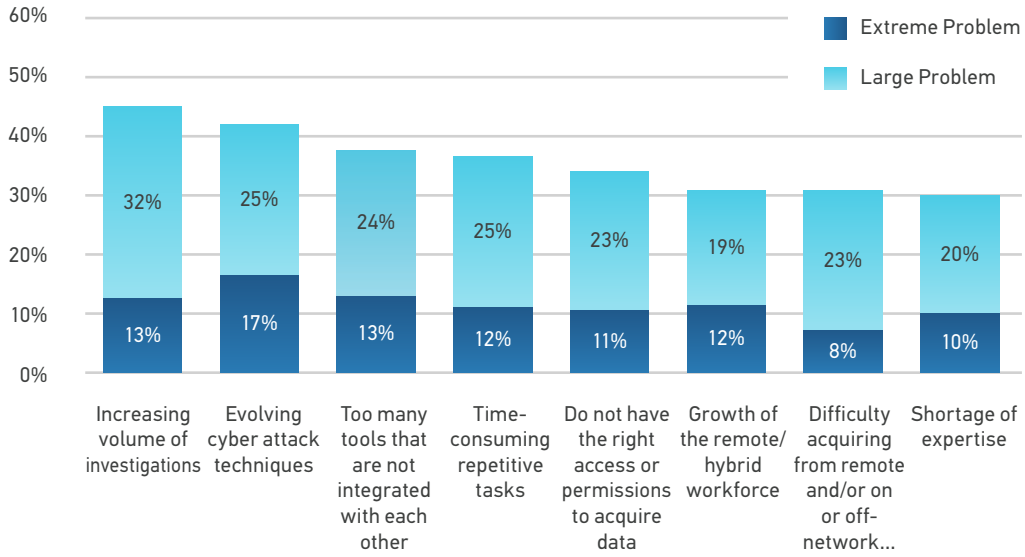


Figure 5: Please indicate to what degree the following potential challenges are problematic for your investigations, overall. [Extreme Problem, Large Problem, Moderate Problem, Small Problem, Not a Problem, Don't Know]

DFIR Personnel Are Feeling Burnt Out—And Reinforcements Aren't Coming Any Time Soon

Corporate DFIR practitioners are already feeling the impact of the soaring volume of investigations and data, plus other demands of the job (Figure 6). Nearly 30% strongly agreed that alert/investigation fatigue is a real issue, and more than 20% strongly agreed with the statement that "**I am feeling burnt out in my job**."

Leaders need to take these warning signs seriously. There's no quick fix when a fifth of the team leaves for less stressful pastures. More than 30% of respondents strongly agreed that recruiting and hiring DFIR professionals is a major challenge, and 27% strongly agreed that onboarding new hires is also challenging.

Globally, there's a **well-documented shortage of cybersecurity professionals**, and it will be many years (if ever) before the gap is filled by new graduates from specialized post-secondary training programs. Today, automation can help to address some of these personnel challenges by freeing up the in-house expertise that an organization already has. As well, organizations should invest in tools that extend some DFIR functions to other security personnel and in solutions that enable faster analysis by presenting data in an intuitive and easy-to-understand way.

SENTIMENTS RELATING TO BURNOUT AND RECRUITMENT

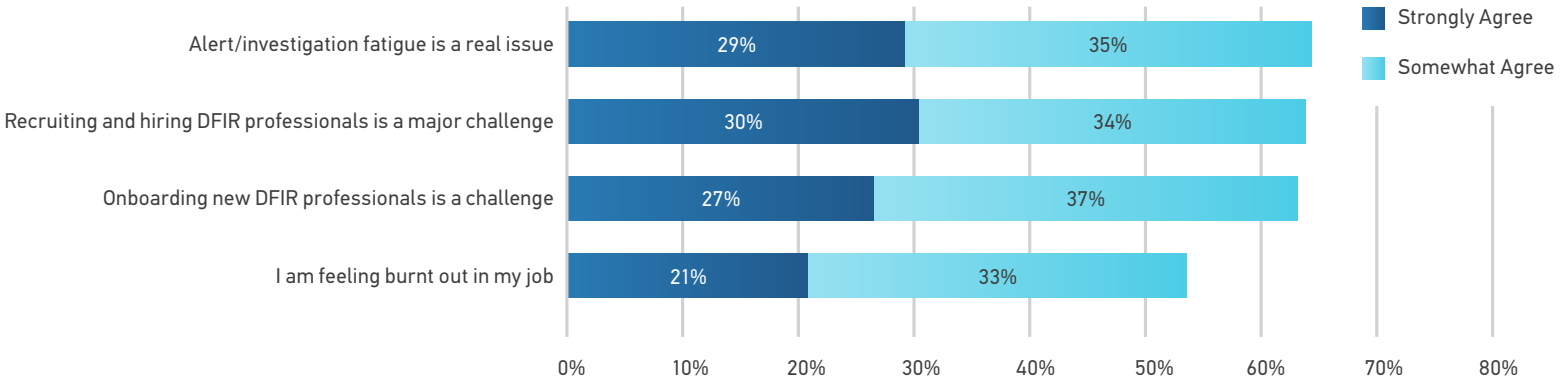


Figure 6: Please indicate the extent to which you agree or disagree with the following statements. [Strongly Agree, Somewhat Agree, Neutral, Somewhat Disagree, Strongly Disagree, Prefer Not to Answer]

Organizations Need to Improve Collection, Processing, and Analysis

As the ongoing digital transformation has caused data volumes to soar, it has become **more difficult for DFIR practitioners to access, collect, process, and analyze the range of artifacts** needed to obtain a complete view of an incident.

At the same time, the set of potential data sources has rapidly expanded to now include computers, mobile devices, software-as-a-service (SaaS) applications, cloud-based storage, IoT devices, and practically anything with telemetry (e.g., automobiles).

Unfortunately, today's workflows still **rely too much upon the manual execution of many tedious and repetitive tasks**, consuming expertise and slowing down investigations. For example, when evidence is needed from several endpoints, it often falls on the investigator to proceed in a one-by-one sequence until all the data is collected and processed. Only then can they examine the evidence and prepare a report.

These tasks don't require applied brainpower yet still consume an expert's time and, while necessary, they are already a known issue: 37% of respondents characterized time-consuming repetitive tasks as either a large or extreme problem in the context of investigations (Figure 5).

Additionally, the lack of integration and interoperation noted above often forces DFIR professionals to constantly switch from one forensic tool to another. Over time, and across the growing number and complexity of investigations, all this switching adds up—slowing down investigations and wasting the time of experts who are already in short supply.

Again, DFIR professionals are pointing the way forward (Figure 7). **More than half of respondents indicated that investments in automation would be either extremely or highly valuable** for a slew of DFIR tasks, led by remote acquisition of endpoints (56%).

VALUE OF FUTURE AUTOMATION INVESTMENTS (MOST VALUABLE TO LEAST VALUABLE)

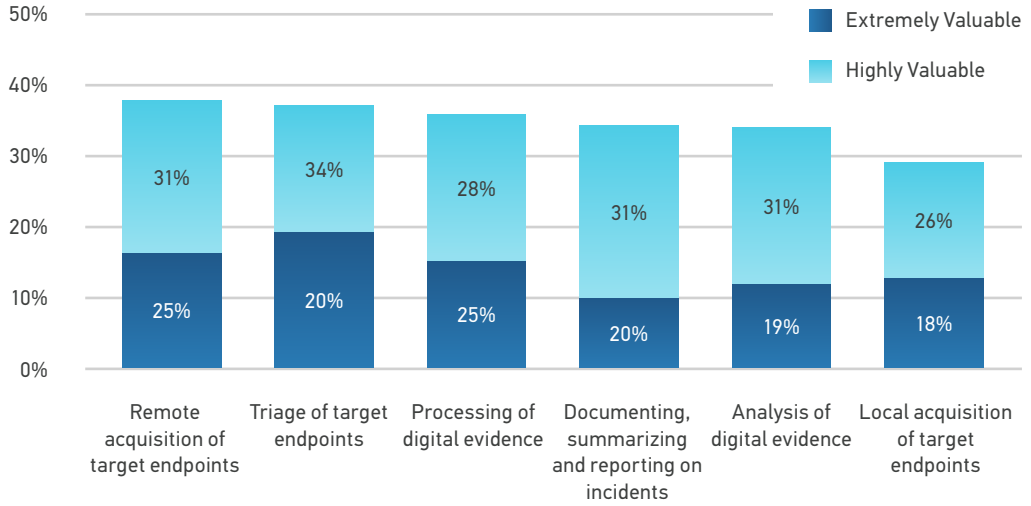


Figure 7: Where do you think investments in automation would be most valuable? [Extremely Valuable, Highly Valuable, Moderately Valuable, Slightly Valuable, Not Valuable, Not Sure]

KEY INSIGHTS

FINDING #3: DFIR Leadership Has Never Been More Important

- Organizations need effective incident response plans that specify the role of digital forensics. At the same time, leaders need to ensure DFIR practitioners are equipped with the resources and privileges they need to perform their roles.
- Regulatory obligations are constantly evolving, but DFIR professionals are struggling to keep up. To manage regulatory risk, leaders must ensure DFIR teams either have the necessary time to interpret regulations or have access to expert interpretations (e.g., from legal counsel).
- Third-party forensic service providers (FSPs) can meet many needs, such as extending an organization's capabilities and providing impartial reviews. The right 'mix' of resourcing almost certainly involves some use of FSPs—leaders must strike a balance by addressing short-term needs while still investing in internal capabilities for the long term.

The field of corporate digital forensics is undergoing rapid evolution and is under the spotlight like never before as practitioners contribute to incident response and as the function itself comes to be regarded as essential within broader cybersecurity initiatives.

In such circumstances, informed and decisive leadership plays a critical role in determining whether an organization can reach its goals and fulfill its obligations.

Improving the State of DFIR Starts at the Top

A crucial function of leadership is to set the strategy by which an organization can meet its mission effectively and efficiently. In a world of finite resources, any waste that exists ultimately makes the organization less secure, whether by directing resources to the wrong place (like the saying goes, "the wrong controls in the wrong place are often worse than having no controls at all") or by neglecting crucial areas until it's too late.

In the context of corporate DFIR, it appears that there is considerable room for improvement (Figure 8). 37% of respondents indicated that a lack of a cohesive IR strategy is either an extreme (10%) or large (27%) contributor to wasted resources.

Respondents also pointed to a lack of standardized processes as a major cause of waste, with nearly 36% reporting that this gap is either an extreme (7%) or large (29%) contributor.

When the pressure is on and the stakes are high—exactly the scenario that plays out during and following cyberattacks—it's important that DFIR practitioners can reference clear plans, rather than trying to figure things out 'on the fly.'

> Many organizations have adopted various types of cybersecurity frameworks, with the two more common ones being the ISO-27000 family of standards and the other being the NIST Cybersecurity Framework. The NIST framework utilizes a maturity rating which helps organizations evaluate their current activities and whether they are sufficient based on their environment. An organization's DFIR plans fall within the Respond / Response function of the NIST framework and within the ISO-27035 standard for incident management."
>
> – Trey Amick, Director, Forensic Consultants, Magnet Forensics

A well-developed IR plan includes, among many other things, what actions need to be performed, what decisions need to be made (and by whom), and—most importantly—in what order. In the context of digital forensics, **the plan should outline what forensics are required** (if required at all) for each incident type; and it should also ensure that well-meaning IT teams don't inadvertently destroy potential evidence in the race to recover (e.g., by re-imaging endpoints).

But beyond simply having a plan in place, the **DFIR practitioners must be empowered to access the data sources they need** (more than a third of respondents indicated that an inability to do so is at least a large contributor to waste) and must be equipped with the tools (or other resources) needed to perform their duties effectively. Leaders wield enormous influence in both areas.

CONTRIBUTORS TO WASTE (LARGEST TO SMALLEST CONTRIBUTOR)

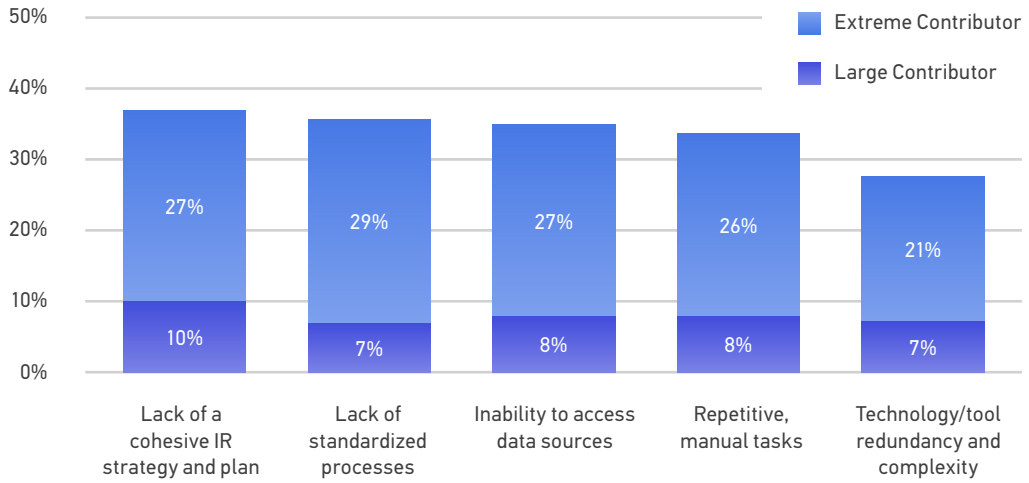


Figure 8: Currently, what do you believe to be the largest contributor to wasted resources? [Extreme Contributor, Large Contributor, Moderate Contributor, Small Contributor, Not a Contributor, Don't Know]

Organizations Are Potentially Exposing Themselves to Regulatory Risk

In response to data breaches and the evolving threat landscape, regulators are imposing new requirements around duty of care and disclosure. Unfortunately, there are signs that many DFIR functions are struggling to keep up, potentially exposing the larger organization to significant regulatory risk.

The large majority (65%) of survey participants are involved in the process of investigating and reporting cyber incidents or breaches to government regulators, with more senior respondents more likely to be involved. Of that proportion, fully two thirds (67%) indicated that their role has been impacted by new reporting regulations.

67%

of DFIR professionals indicate that their role has been impacted by new reporting regulations.

The most frequently cited impact is **increased pressure to produce investigative results faster** (67% of impacted DFIR professionals); of course, this pressure is in addition to the increasing caseloads, more difficult investigations, and other factors already discussed in this report. This trajectory is unsustainable, and leaders must prioritize equipping their teams with the resources (e.g., tooling, personnel) needed to keep pace.

Moreover, 46% of respondents reported that they simply don't have enough time to fully understand the new and changing legislation. Many DFIR professionals have backgrounds in law enforcement, cybersecurity, and IT, and comparatively few will have the training or qualifications to interpret complex regulations that often span hundreds of pages of dense legalese. Compounding matters further, many organizations are subject to multiple sets of regulations and obligations (e.g., economic zone, national, state/provincial, sector- or certification-specific, etc.).

Whether the most effective approach is empowering DFIR teams with the time to study regulations, or turning to legal experts for opinions and direction, or some hybrid, meeting regulatory obligations starts with understanding them—and that is led by leadership.

> The recent rise in cyber-attacks has garnered enough coverage to incite change–to begin with the passing of two new cyber-security laws in the U.S. in 2022. This is just the first step in a million-mile journey. Technology is always evolving and so, too, are regulations. DFIR professionals should be aware of what sector their organization falls into and whether new federal, state, and/or industrial rules and regulations relate to them.
>
> – Lynita Hinsch, Manager, Solutions Consultant, Magnet Forensics

Third Parties Are Valuable Extensions of Internal Capabilities

Leaders are responsible for ensuring the DFIR professionals are equipped and empowered to succeed, and access to third-party forensic service providers (FSPs) is a valuable resource.

Today, the majority of organizations represented in the survey outsource at least some DFIR investigations. Respondents from companies with fewer than 100 employees were the least likely to report that their organization outsources investigations (57%), while every other employee size cohort exceeded 73%, led by the 500-to-999 employee range (85%).

There are many reasons why an organization would bring in a third party to perform some aspect of investigations. The top reason—cited by 47% of respondents, and quite consistent across all organization sizes—is a lack of expertise or skillset internally. This result aligns with the earlier observations pertaining to challenges with recruiting, hiring, and onboarding qualified DFIR professionals, as well as the evolving complexity of today's investigations.

Additionally, this aligns with why business email compromise attacks are the most likely to require third-party resources to assist with the investigation, according to 50% of respondents.

47%

of respondents cited a lack of expertise or skillset internally as the top reason for using a service provider for some aspect of their investigation.

Not having the required toolset was the second-most cited reason overall (38%), and also speaks to investigation complexity, as different devices and data stores may need specialized tooling. In particular, FSPs are often able to provide big data analysis (e.g., to examine hundreds of servers concurrently) and direct experience dealing with specific threats (e.g., ransomware gangs or strains).

While some factors are consistent across organization sizes, others vary considerably. For example, organizations with fewer than 100 employees are more likely than others to use a third party as a result of the volume of investigations; they are also more likely to find third parties to be a cost-effective solution and far less likely to have a corporate policy in place requiring the use of third parties.

At the other end of the size spectrum, **the largest enterprises are considerably more likely than others to require an impartial third-party review**. In fact, this was the top reason why organizations with 10,000 or more employees call in outside assistance. While a major contributor to the need for third-party review is undoubtedly cyber insurance policy requirements, the largest enterprises likely also have more contractual and regulatory obligations than do the comparatively smaller organizations.

There is no doubt that FSPs are a very valuable resource that can extend the capabilities of the internal organization. At the same time, using FSPs to fill short-term gaps **in perpetuity** is not a viable long-term strategy. Leaders should listen to their teams about what value FSPs can bring, perhaps as part of a formal gap analysis exercise, but must balance short-term needs with long-term investments in the organization's own capabilities.

Conclusion & Recommendations

DFIR isn't easy, but it's never been more important—especially in today's threat landscape. Motivated, skilled, and well-financed cybercrime groups are constantly innovating. At the same time, the explosion in the volume of data and range of devices included in today's investigations is already straining DFIR personnel.

To manage cyber risk and meet growing and ever-tighter obligations, it is important that every organization has timely access to modern DFIR capabilities.

Here are several insights that you can takeaway to strengthen your DFIR approach:

INVEST IN DFIR SOLUTIONS THAT PRIORITIZE SPEED, ACCURACY, AND COMPLETENESS

Time is of the essence when a potential compromise is discovered. Delays in uncovering root cause of a cybersecurity incident potentially opens the organization up to more risk and impact to business continuity. As attacks become more and more sophisticated, invest in a forensic solution that allows you to get the details you need in a way that is simple yet thorough and accurate, so that you can unravel the incident quickly.

INTRODUCE FORENSIC AUTOMATION TO REDUCE BURNOUT

While automation is not a new solution in the cybersecurity space (many organizations utilize SOAR solutions), oftentimes the forensic investigation process still requires practitioners to wait for progress bars to complete to click next and move to the next step.

Introducing a forensic automation solution to streamline the collection and processing aspects of the workflow can help security leaders retain DFIR professionals as it has the potential to reduce burnout as well as eliminate the delays and burden of manual touchpoints that extend investigation timelines.

EMPOWER FORENSIC PRACTITIONERS TO ENACT IR PLAYBOOKS IN RESPONSE TO ACTIVE EVENTS

Putting an IR plan in place ahead of time helps to ensure a faster, smoother response to active events. Within the IR plan, clarify the role and responsibilities of the forensic investigator and how forensics contributes to the Respond/Response function of the NIST Cybersecurity framework. Additionally, our survey found that accessing data is a real issue and contributes to investigative delays. DFIR teams should work with various stakeholders from across the organization

to ensure when time is of the essence, investigators can access the data they need to perform their duties. Investing ahead of time for the right tooling to enable quick and targeted collections of data is critical in responding to active events. Lastly, cyber exercises, including both SOC and DFIR Teams with support of all the stakeholders should routinely be conducted, allowing for updates and adjustments to be made to the IR response plan.

ENSURE DFIR TEAMS UNDERSTAND THE ORGANIZATION'S REGULATORY (AND OTHER) OBLIGATIONS

New and changing cybersecurity regulations are putting pressure on DFIR teams in many ways. Staying on top of changes can be difficult when they are already thinly spread. Ideally, regulations should be read and interpreted by legal professionals who can 'translate' them into clear and actionable information for DFIR practitioners. If obtaining official legal interpretation is not possible, provide them with the resources they need—especially time—to read and digest the information, and supplement with limited access to legal counsel for especially confusing requirements. As well, requirements also come from insurance providers, customers, and vendors. Most importantly, understanding these details in advance of an incident ensures that DFIR teams can meet requirements with accuracy and speed.

LEAN ON SERVICE PROVIDERS, BUT HAVE A PLAN FOR THE FUTURE

Whether small or large, almost every organization leans on an FSP for at least some aspect of their DFIR investigations. Service providers help to augment the capabilities of the organization–this could be through providing specialized tooling or supporting internal teams challenged with talent gaps. In the long-term, security leaders should work with their internal teams to perform a formal gap analysis and balance their short-term needs with the long-term strategic needs of the security organization.

Contributors

This year's State of Enterprise DFIR Report featured contributions from an experienced team of Magnet Forensics DFIR experts. Magnet Forensics is proud to count a larger number of former digital forensic examiners and DFIR professionals, from both the public safety and enterprise sectors, as members of the team—providing a wealth of valuable knowledge and insights and shaping all that we do.

Trey Amick
Director, Forensic Consultants

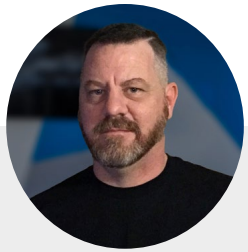
Trey Amick is a forensics investigator with a background in both law enforcement and corporate investigations. As a detective with the Rock Hill Police Department in South Carolina, Trey was sworn as a Special Deputy United States Marshal and supported the US Secret Service Electronic Crimes Task Force. Previously, he served in roles in both Patrol and Professional Standards. Most recently, as a corporate investigator, Trey managed the Enterprise Cyber Education and Awareness Team at Capital One, where he also served as part of the Cyber Technical Investigations Team.

Dean Turner
Vice President, Product Management, Private Sector

Dean Turner is Magnet Forensics' Vice President – Enterprise Strategy and is responsible for their AXIOM Cyber, IGNITE, AUTOMATE Enterprise and Platform strategies. Prior to joining Magnet, he was part of Cisco's Advanced Threat Group as Director of Product Management responsible for Cisco Threat Grid and Malware Analytics. Prior to joining Cisco, Dean worked with PayPal and Symantec where he was responsible for helping build out commercial threat intelligence programs. He was a co-founder of one of the first online information security resources - SecurityFocus - and brings with him over 20 years of experience in management, security operations, threat analysis and threat intelligence.

Lynita Hinsch
Manager, Solutions Consultant

Lynita Hinsch is a certified and experienced computer forensics professional who joined the Magnet Forensics team as a Solution Consultant in 2020. She began her training as an enlisted Computer and Communications Specialist in the U.S. Air Force with the Air Force Pentagon Communications Agency (AFPCA) in Washington, DC. After enlistment Lyn continued her career in both the Federal and Local Law Enforcement space working for such agencies as the U.S. Department of State, Defense Intelligence Agency, and Maricopa County Sheriff's Office before joining the corporate information security sector in the Fortune 100 space. She is a Champlain College alum with an undergraduate degree in Computer and Digital Forensics and more than a decade of experience.



Doug Metz
Professional Services Consultant

Doug Metz is a Professional Services Consultant with Magnet Forensics. Doug's work in information security has supported government, private sector and academic institutions for over a decade and a half and includes substantial experience in DFIR. In addition to his experience in the field, Doug holds several industry certifications including: MCFE, MCME, MCCE, GCIH, GCFE, GCFA, GCTI, GREM, CISSP, NW3C CCE.

Prior to joining Magnet Forensics, Doug served as Global Incident Response Manager for a Fortune 200 company, managing a global team of analysts and the Security Operations Center. Doug is also a member of the High Tech Crime Investigators Association (HTCIA), is a volunteer for The Auxtera Project and blogs at BakerStreetForensics.com.

Founded in 2010, Magnet Forensics is a developer of digital investigation software that acquires, analyzes, reports on, and manages evidence from digital sources, including computers, mobile devices, IoT devices and cloud services. Magnet Forensics' software is used by more than 4,000 public and private sector customers in over 100 countries and helps investigators fight crime, protect assets and guard national security.

LEARN MORE

MAGNET AXIOM CYBER

Organizations of all sizes fall victim to cybersecurity threats every day. With an artifacts-first approach and built-in remote acquisition, Magnet AXIOM Cyber helps you quickly understand security incidents so you can safeguard your business in the future. Use AXIOM Cyber for root cause analysis for Incident Response as well as HR, and Insider Threat investigations.

MAGNET IGNITE

When every minute counts, you need to know whether or not to spend the time and resources on doing a deep dive forensic analysis of an endpoint. Magnet IGNITE is a cloud-based compromise assessment tool that performs fast, remote scans and initial analysis of endpoints.

MAGNET AUTOMATE ENTERPRISE

Magnet AUTOMATE Enterprise is an automation solution purpose-built for enterprises to concurrently collect and process evidence from multiple targets and data sources so businesses can respond to security events faster. Integrate tools from across your tech stack to streamline workflows and reduce the number of manual touchpoints to get to the evidence you need faster.