



# Tackling Attack Detection and Incident Response

---

## Research and Analysis by Intel Security and ESG

*By Jon Oltsik, Senior Principal Analyst*

April 2015

---

This ESG paper was commissioned by Intel Security and is distributed under license from ESG.

## Contents

Executive Summary .....	3
Always On .....	4
Cybersecurity Defense.....	7
The Bigger Truth .....	11

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

## Executive Summary

The Enterprise Strategy Group (ESG) recently worked with Intel Security to analyze the results of a research project based upon a survey of 700 IT and security professionals at mid-market (i.e., 500 to 999 employees) and enterprise (i.e., more than 1,000 employees) organizations located in Asia, North America, EMEA and South America. Survey respondents came from numerous industries with the largest respondent populations coming from information technology (19%), manufacturing and materials (13%), and financial services (9%). Respondents were asked a series of questions about their organizations' information security policies, processes, and technologies as well as their current security challenges and future strategies.

Based upon this research, ESG concludes:

- **Security professionals remain busy and challenged by targeted attacks.** On average, security respondents indicated that their organizations conducted 78 security investigations last year, and about 28% of these investigations focused on targeted attacks. Targeted attack investigations are especially cumbersome as they require experienced security analysts, a comprehensive view of IT assets, and security data analytics. These particular investigations can be extremely time consuming which may impede remediation actions and lead to data breaches in spite of the security team's best efforts. The Intel Security data points to the need to change from simply collecting volumes of data to finding value in the data—this is the path to address attacks more efficiently.
- **While targeted attacks abound, incident detection and response are fraught with one-way streets, roadblocks, and detours.** Cyber-attackers are using a combination of social engineering techniques, publicly-available social networking services, and stealthy malware to trick end-users, circumvent security controls, and compromise systems. While these offensive tactics are fairly straightforward, cybersecurity defenses remain haphazard at best. Security professionals often have limited knowledge about the latest hacking tactics, techniques, and procedures (TTPs). Incident detection and response are held back by a series of time consuming tasks, manual processes, and inefficiencies that elongate response time leading to damage control and cleanup. Security monitoring tools have limited visibility into users and technologies while security point tools lack the level of integration needed to coordinate and monitor security defenses across the network. Alarming, the Intel Security data portrays an unfair fight where cybersecurity offense often overwhelms cybersecurity defenses. Businesses need to change their security strategies to be able to deal with incidents within the most crucial timeframe after infection, before serious damage can be inflicted. Intel Security refers to this ideal incident detection/response window as the "golden hour."
- **Security professionals are asking for help in multiple areas.** The security professionals surveyed for this project have a multitude of suggestions to help them improve cybersecurity defenses and incident detection and response efficiencies. More than half point out the need for better security tools for incident detection and security analytics while around 40% recommend more training for cybersecurity professionals and the SOC team. And since 80% of organizations believe that their incident detection/response processes are hindered by a lack of security technology integration, many security professionals believe that their organizations would benefit from an end-to-end, tightly-integrated enterprise security architecture. In aggregate, cybersecurity advancements are needed across people, processes, and technology.

CISOs should use the data presented in this report in two ways:

1. **As a guideline for security assessment.** This report highlights a number of issues hindering incident detection processes and effectiveness. CISOs should assess whether these problems exist within their organizations and, if so, attempt to identify and measure the ramifications.
2. **As a blueprint for strategic planning.** The data points to the need for vastly improved security data analytics and an integrated enterprise security technology architecture. CISOs should investigate their plans in these and other areas identified herein.

## Always On

Most information security professionals would readily admit that there is a persistent cyber-war in progress where their organizations face a constant barrage of attacks. On average the IT and security professionals' surveyed claim that their organizations conducted 78 individual security investigations in 2014. Not surprisingly, security investigation frequency was closely correlated to an organization's size—the larger the organization, the more security investigations they conducted (see Table 1).

*Table 1. Average Number of Security Incidents in 2014*

	Total survey population (n= 700)	500 to 999 employees (n = 196)	1,000 to 4999 employees (n = 248)	More than 5,000 employees (n = 256)
Average number of security incidents in 2014	78	31	41	150

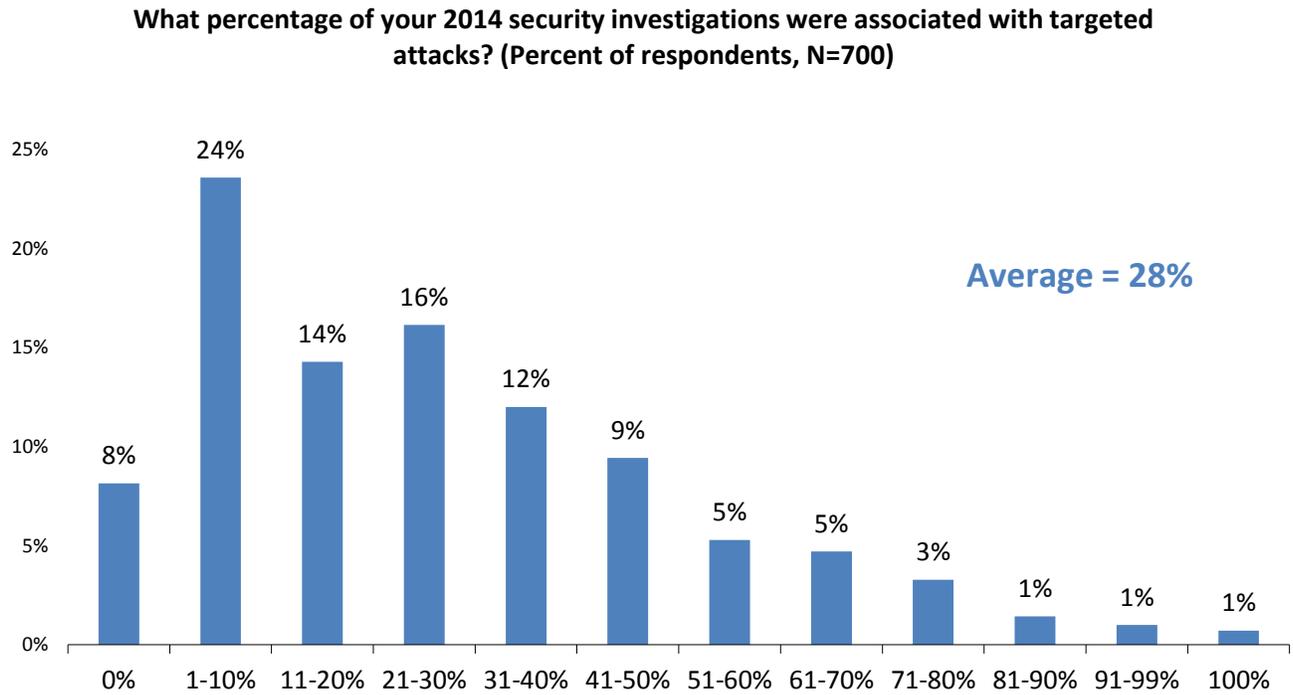
*Source: Intel Security, 2015.*

At almost half of the companies surveyed, the majority of these security investigations focus on routine security incidents where end-user PCs become infected with adware, spyware, and volumetric viruses commonly downloaded from an assortment of sources. However, the other half spend the majority of their time investigating more sophisticated and often inter-related problems: targeted attacks (by an external adversary targeting a particular individual, group, or type of site or service), data breaches, and malicious insider attacks. In fact, 28% of security investigations are associated directly with more dangerous and potentially damaging targeted attacks (see Figure 1).

This is an important distinction. With more than 1 in 4 security investigations linked to targeted attacks, many organizations:

- **Face targeted attacks on a regular basis.** While pedestrian malware continues to be a major pain point, the Intel Security data indicates that no one is immune to the dangers of today's targeted cyber-attacks. Small, medium, and large organizations consistently reported that 28% of their security investigations were focused on targeted attacks and organizations across all industries were impacted. Clearly, the advanced persistent threats (APTs) that were once the scourge of government agencies and the defense/intelligence industry are now widespread, presenting a real menace to all organizations.
- **Require new resources and skills to conduct targeted attack investigations.** In general, security professionals can get help with common malware from their AV and IDS/IPS vendors. Alternatively, investigating targeted malware that flies "under-the-radar" may require some combination of security analytics tools, threat intelligence feeds, and advanced cybersecurity skills. Based upon this, it is safe to assume that targeted attack investigations are more difficult and time consuming than more common ones and many organizations simply are not prepared with the right resources, skills, or analytics.
- **Have more at stake with targeted attack investigations.** Adware and spyware may disrupt employee productivity but targeted attacks can result in costly and damaging data breaches. This puts pressure on the security analyst team to isolate and remediate problems as soon as possible but best efforts alone won't prevent data breaches.

Figure 1. Percentage of Security Investigations Associated with Targeted Attacks

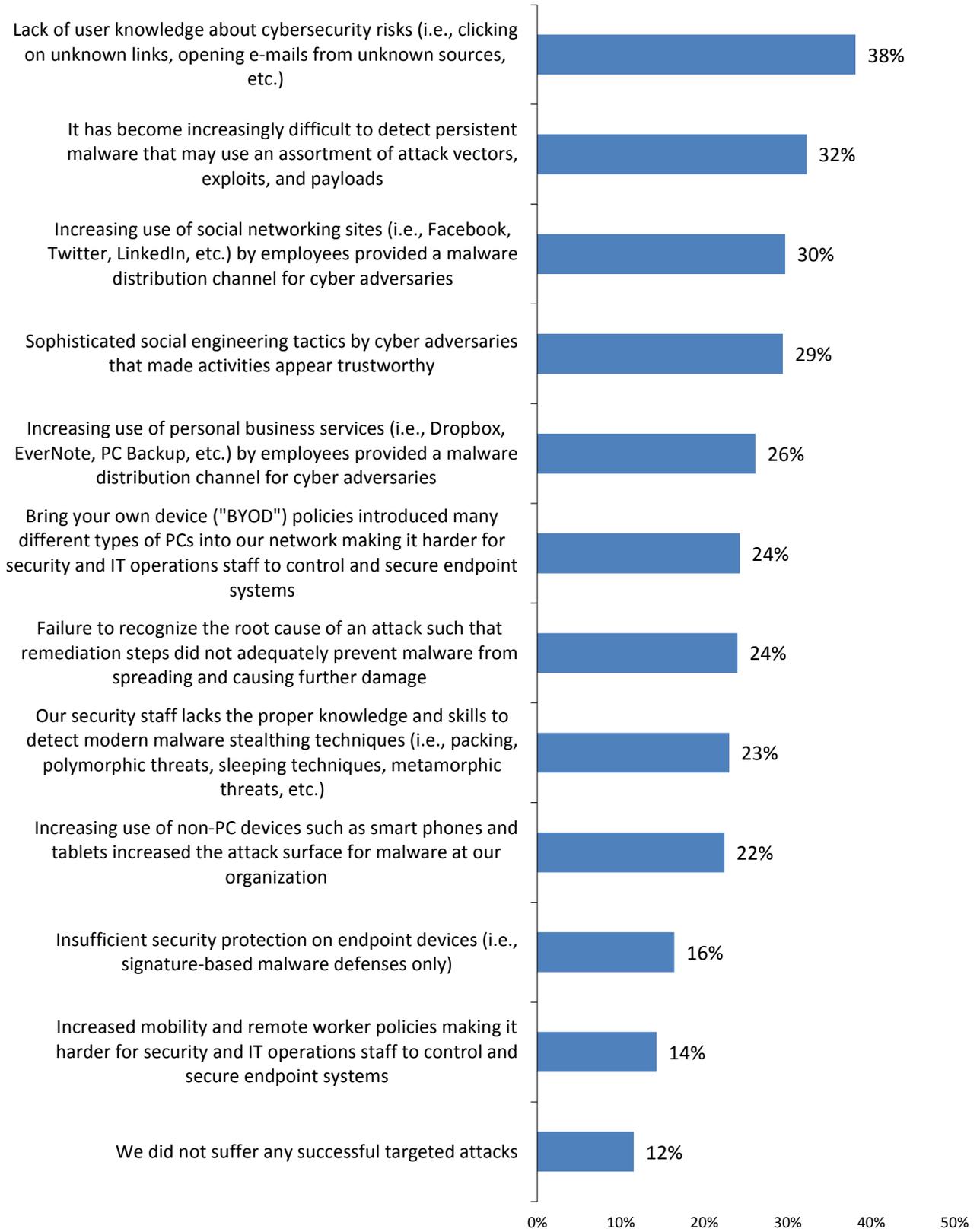


Source: Intel Security, 2015.

All of these security investigations raise an obvious question: Why are cyber-adversaries able to penetrate networks and compromise systems with targeted attacks? Unfortunately, security professionals point to an assortment of root causes—38% cite a lack of user knowledge about cybersecurity risks, 32% claim that it is increasingly difficult to detect persistent/modern malware, 30% blame an increase in the use of social networking, and 29% identify sophisticated social engineering tactics (see Figure 2).

Figure 2. Reasons Cited for Targeted Attack Success

**If your organization suffered one or more successful advanced, targeted attacks in 2014, which of the following things do you believe made these attacks successful? (Percent of respondents, N=700, multiple responses accepted)**



Source: Intel Security, 2015.

This list reflects a microcosm of today’s cybersecurity landscape. Smart, crafty, and creative cyber-adversaries use social engineering and stealthy malware to entice gullible end-users to click on a URL or open an e-mail attachment. In the meantime, nearly one-third (32%) of security professionals struggle to detect and respond to these attacks.

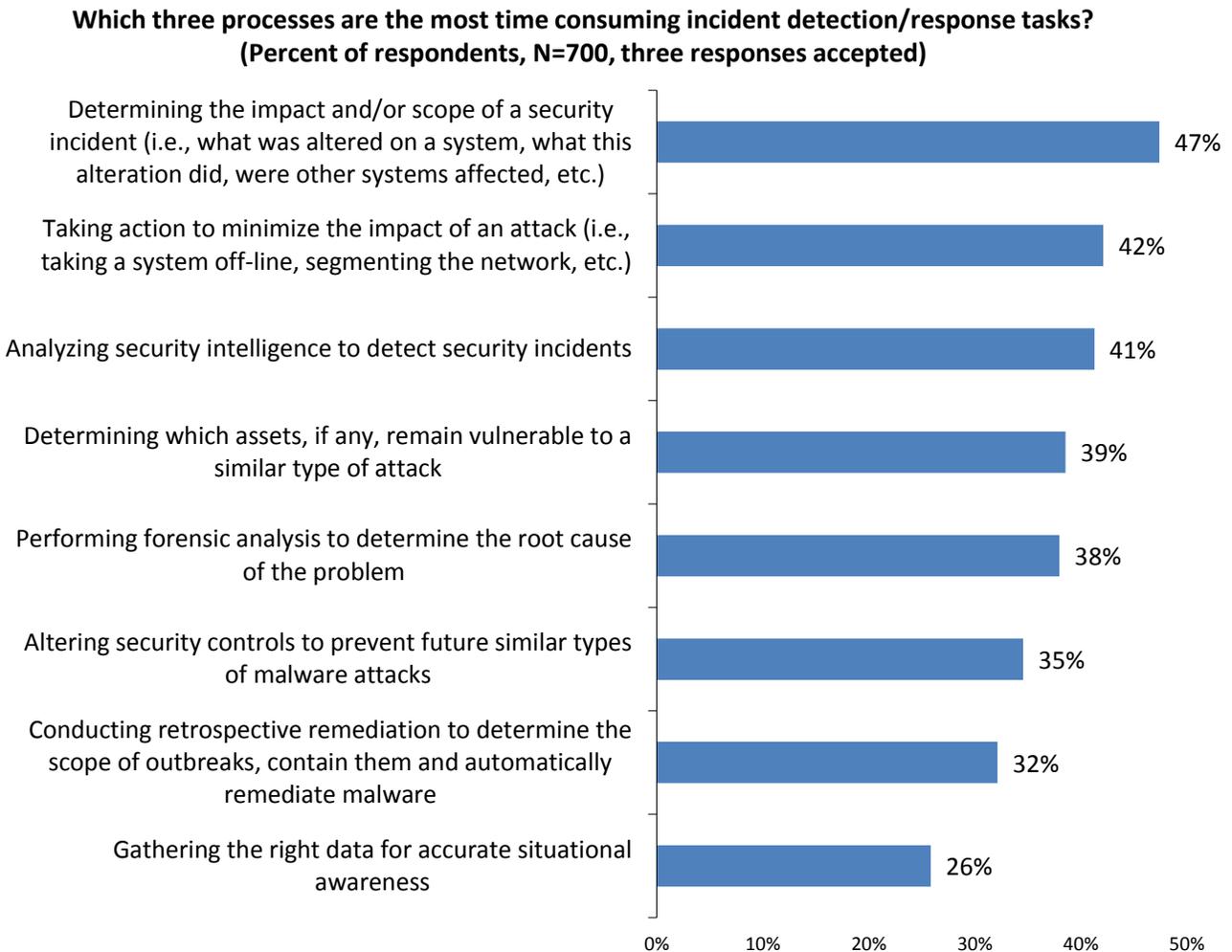
The research points to a clear mismatch between offensive cybersecurity threats and traditional cybersecurity defenses. This imbalance is cause for alarm and must be addressed by all organizations as soon as possible. It’s important that security professionals understand that the volume of data alone isn’t making them smarter—what’s needed is more analysis and action on seemingly unrelated events that add up to significant incidents.

## Cybersecurity Defense

The Intel Security research seems to indicate that it is relatively easy for cyber-adversaries to launch targeted attacks, evade security defenses, and compromise systems. Security professionals recognize this situation and remain diligent in their efforts to prevent, detect, and respond to targeted attacks but are often hamstrung by manual processes, isolated security controls, or limited security analytics.

For example, incident detection and response processes depend upon a number of time consuming tasks, including determining the impact/scope of a security incident (47% say this is a time-consuming task), taking action to minimize the impact of an attack (42%), and analyzing security intelligence to detect security incidents (41%) (see Figure 3). When these time consuming processes are added together, it is often days, weeks, or months before cyber-attacks are identified and remediated.

Figure 3. Time Consuming Tasks Associated with Incident Detection/Response



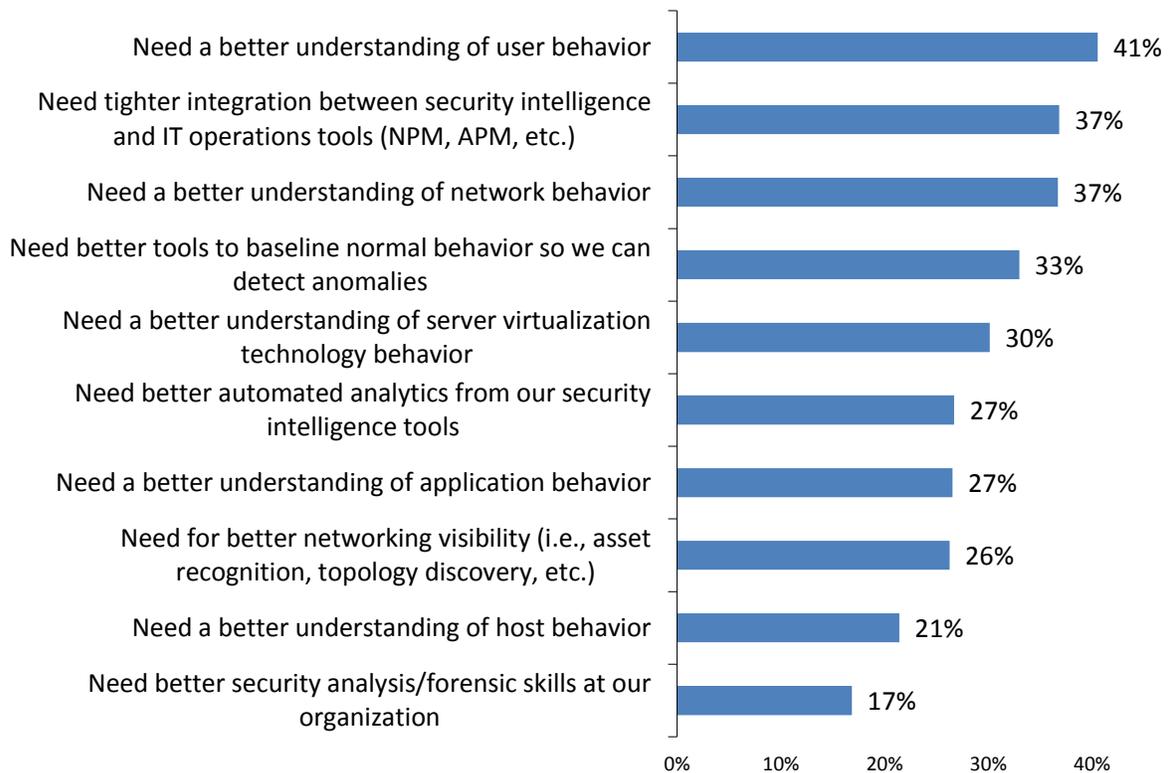
Source: Intel Security, 2015.

When it comes to incident detection and response, time has an ominous correlation to potential damage—the longer it takes an organization to identify, investigate, and respond to a cyber-attack, the more likely it is that their actions won't be enough to preclude a costly breach of sensitive data. To address this situation, many organizations are moving toward continuous monitoring of users, systems, applications, and sensitive data located on internal networks and external resources (i.e., SaaS, IaaS, PaaS, business partner systems, etc.). Effective continuous monitoring demands end-to-end collection, processing, and analysis of volumes of security data such as log files, network flows, endpoint/network forensic data, threat intelligence feeds, etc. Being able to identify and respond to an incident within the first hour (i.e., the Intel Security “golden hour”) can greatly minimize the impact of the breach.

While many organizations strive for continuous monitoring across IT, many continue to have limited visibility into one or more IT areas. When asked about the biggest inhibitors to having real-time and comprehensive security visibility, 41% of organizations said that they need a better understanding of user behavior, 37% claim that they need tighter integration between security intelligence and IT operations tools, 37% need a better understanding of network behavior, and one-third (33%) need better tools to baseline normal behavior so they can detect anomalies (see Figure 4).

*Figure 4. What's Needed for Real-time and Comprehensive Security Visibility*

**Of the following, which are the biggest inhibitors to having real-time and comprehensive security visibility at your organization? (Percent of respondents, N=700, multiple responses accepted)**



Source: Intel Security, 2015.

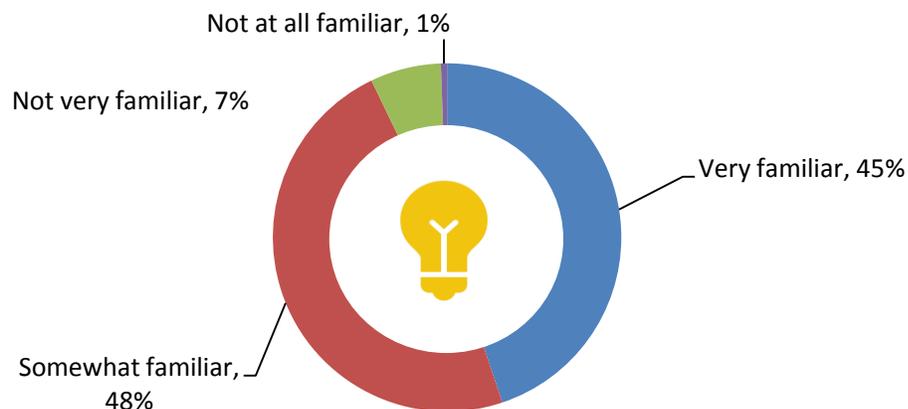
Addressing these visibility and comprehension deficiencies is critical. For example, a lack of knowledge about user behavior could give cyber-adversaries the opportunity to create rogue user accounts or suddenly download volumes of sensitive documents to a user's PC. Similarly, when security analysts are unsure about network activities, they are more likely to miss suspicious connections, egress traffic, or DNS behavior. CISOs must address these visibility gaps in order to arm security analysts with the data they need to pivot across applications, networks, and systems as they pursue targeted attack investigations.

End-to-end security visibility is vital but security data is meaningless by itself if security analysts can't understand the information or its ramifications. In fact, effective incident detection and response is really anchored by the experience, instincts, and skills of the security analyst team as they observe content, monitor behavior, analyze data, and meander from data point to data point as part of their investigations.

Given the need for a strong foundation of security knowledge, ESG found it somewhat troubling that only 45% of security professionals consider themselves very knowledgeable about malware obfuscation techniques while 8% are not very familiar or not at all familiar with malware obfuscation techniques (see Figure 5). With limited knowledge in this area, it is easy to see why over-burdened security analysts might disregard security alerts, minimize investigations efforts, or mistakenly classify a malicious file as benign. This is especially alarming as many organizations have visibility gaps AND skills deficiencies, limiting their ability to detect and respond to cyber-attacks.

*Figure 5. Security Professionals are Unfamiliar with Malware Obfuscation Techniques*

**Many of today's sophisticated malware attacks use tools to obfuscate or hide specific aspects of their exploits, payloads, communications, and other tactics and processes. Are you familiar with these types of techniques? (Percent of respondents, N=700)**



*Source: Intel Security, 2015.*

Enterprise security activities around incident prevention, detection, and response are often based upon an army of disparate point tools used for threat management, policy enforcement, access control, and security monitoring. In many cases, these tools were added to the network organically over time in response to new types of cyber-risks.

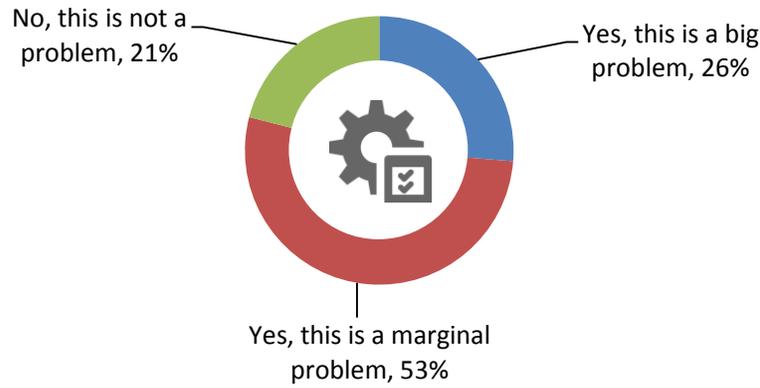
Each point tool is designed for a specific function and may be effective on its own but the infosec team is ultimately responsible for securing all IT assets regardless of their location or the types of threats they face. It is often difficult, if not impossible, to create/enforce security policies or monitor enterprise security status by piecing together reports generated from dozens of independent tools.

The complex and cross-vector nature of targeted attacks makes the point tool model even less acceptable. Multiple events detected by different sensors must be aggregated to correlate events into an attack sequence, permit an investigative workflow, or communicate appropriate containment and remediation out to relevant controls.

Is this lack of integration impeding efforts around incident detection and response? According to the research, the unfortunate answer is "yes"—26% of organizations say that the lack of integration and communications between security technologies/tools creates a big problem for incident detection and response while 53% state that the lack of integration and communications between security technologies/tools is still a marginal problem (see Figure 6).

Figure 6. *The Lack of Security Technology Integration Leads to Incident Detection/Response Problems*

**Does your organization have difficulty with incident detection and response due to lack of integration of and communications between its security technologies/tools?**  
**(Percent of respondents, N=700)**

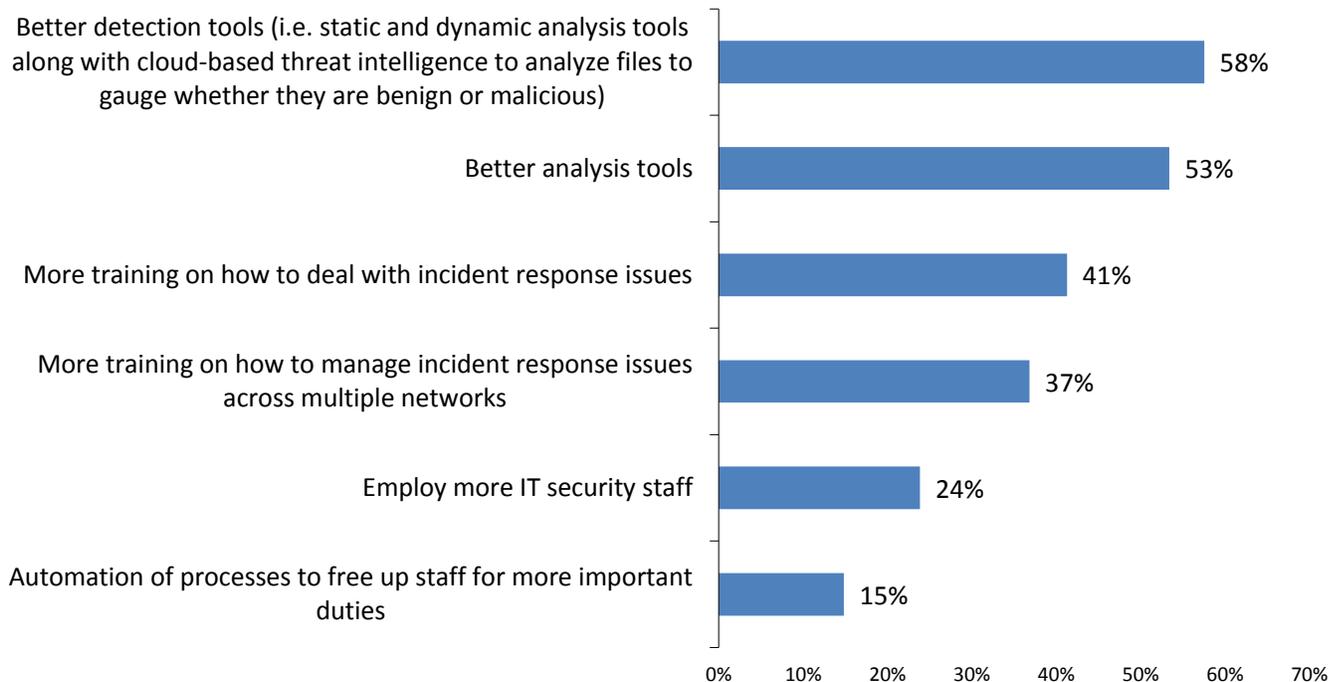


Source: Intel Security, 2015.

Security professionals were asked to give their own opinions about how their organizations could improve the efficiency and effectiveness of the information security staff itself. The research shows a real desire for more effective security analytics tools—58% of respondents want better detection tools while 53% say they need better analysis tools for turning security data into actionable intelligence. There is a yearning to improve the security organization’s skill set with more training on incident response and a general need to grow the infosec staff (see Figure 7). Taken together, this data demonstrates the need for improvement across people, process, and technology.

Figure 7. *What’s Needed to Improve the Efficiency and Effectiveness of the Information Security Staff*

**In your opinion, which of the following items would do the most to improve the efficiency and effectiveness of your staff? (Percent of respondents, N=700, multiple responses accepted)**



Source: Intel Security, 2015.

## The Bigger Truth

The Intel Security research exposes a few fundamental and pervasive cybersecurity weaknesses:

1. Organizations perform dozens of security investigations each year and around one-fourth of these investigations center on targeted attacks. These particular investigations tend to require advanced skills and security analytics tools as well as an integrated architecture.
2. Despite “silver bullet” products deployed in the last few years, targeted attacks are succeeding and demonstrate an imbalance between cyber-adversary offense and the corresponding defenses of large and small organizations. While cyber-adversaries conduct stealthy attack campaigns based upon social engineering tactics, enterprises find it difficult to prevent, detect, or respond to these attacks in a timely fashion.
3. Many organizations lack the type of comprehensive continuous monitoring they need to identify and respond to suspicious behavior during the critical timeframe after exploitation but still before serious damage occurs (i.e., the Intel Security “golden hour”).
4. The data also points to organizational and technology issues as well. Many organizations lack advanced cybersecurity skills while the security technologies they depend upon introduce overhead as they lack the right level of technical integration. As a result, incident detection and response processes are fraught with multiple time consuming tasks and operational overhead.
5. Security professionals believe that they need better security analytics technologies, integration, and additional training to improve the efficiency and effectiveness of their security teams.

CISOs should study this research and assess whether their organizations face similar cybersecurity challenges across all aspects of their infosec domain and strategy. Additionally, ESG believes that there is a hidden story within the Intel Security research that hints at best practices and lessons learned. This data strongly suggests that CISOs:

- **Commit to continuous cybersecurity education.** Like physicians, cybersecurity professionals must keep up with the latest research and development in their area of expertise. This includes advances in malware techniques, threat vectors, and new innovations in cyber defenses. Unfortunately, continuous education is often disregarded as the security team is often too busy keeping up with its workload or reacting to emergency alerts. This results in the situation described in this report where less than half of the security professionals surveyed were very familiar with malware obfuscation techniques. CISOs must seek to balance these diverse activities since cybersecurity professionals won't be effective if they don't know how to identify or remediate the latest types of cyber-threats. Some type of cyber-education should be required for the entire organization on an annual basis and supported by a continuous program led by the security team and HR. Cyber-education programs are most successful when executive management take a leadership role by stressing their importance and cheerleading the effort at all times.
- **Anchor their cybersecurity strategy with strong analytics moving from volume to value.** While threat prevention controls like the SANS top 20 are critical, CISOs must assume that targeted attacks will circumvent security defenses, penetrate networks, and compromise systems. To address this inevitability, cybersecurity strategy must be based upon strong security analytics. This means collecting, processing, and analyzing massive amounts of internal (i.e., logs, flows, packets, endpoint forensics, static/dynamic malware analysis, etc.), organizational intelligence (i.e., user behavior, business behavior, etc.) and external data (i.e., threat intelligence, vulnerability notifications, etc.). Security analytics must be based upon intelligent algorithms wherever possible that can detect anomalous behavior, pinpoint affected systems, and help analysts determine a root cause and scope as quickly and accurately as possible. CISOs should remember that collecting and processing data is a means toward action—improving threat detection and response effectiveness and efficiency.
- **Create a tightly-integrated enterprise security technology architecture.** Nearly 80% of organizations believe that the lack of integration between security tools creates a bottleneck and interferes with their ability to detect and respond to security threats. This should be perceived as a bright red flag. CISOs must alleviate this limitation by developing an enterprise security architecture that replaces security point tools with an integrated enterprise security architecture over the next three years. This security architecture

should encompass internal networks and cloud-based IT assets. The project plan should start with immediate pain points or fully-amortized security technologies and then introduce further integration points in phases over time. Each phase should include success metrics around security efficacy and operational efficiency. While it is beyond the scope of this paper to provide details about an integrated enterprise security architecture, the key characteristics include central command-and-control (i.e., policy management, configuration management, security analytics, etc.) and distributed enforcement up and down the technology stack.

- **Automate incident detection and response whenever possible.** While cyber-threats grow exponentially, existing security tools and personnel can only increase their capacity arithmetically. In other words, most organizations have no chance of keeping up with ever-changing malware or cyber-attack techniques. To level the playing field, CISOs must commit to more automation. For incident detection, this requires advanced malware analytics, intelligent algorithms, machine learning, and the consumption of threat intelligence to compare internal behavior with incidents of compromise (IoCs) and tactics, techniques, and procedures (TTPs) used by cyber-adversaries. Furthermore, security and IT operations teams should instrument IT infrastructure and automate tasks and workflows for continuous remediation to quarantine compromised systems or block newly-discovered malicious URL and IP addresses as quickly as possible. The short-term goal here should be reducing the low-risk security workload to free experienced SOC personnel and allow them to focus on high-priority tasks.



Enterprise Strategy Group | **Getting to the bigger truth.**