DOMAINTOOLS®

2018 CYBERSECURITY REPORT CARD:

ORGANIZATIONS RATE THEIR SECURITY POSTURE AND SHARE BEST PRACTICES

Like it or not, good grades matter. And as organizations become increasingly focused on benchmarking internal groups for their ability to run efficiently and add business value, cybersecurity teams must be positioned to measure the effectiveness and sophistication of their programs against industry standards.

This paper outlines the results of the DomainTools second annual Cybersecurity Report Card Survey. More than 500 security professionals from companies ranging in size, industry and geography were surveyed about their security posture and asked to grade the overall health of their programs. Their responses, particularly when compared to the results of the **2017 Report Card**, shed light on how cybersecurity practices are evolving, and what the most successful organizations are doing to ensure they stay ahead of the ever-growing and changing threat landscape.

Overall, the incidence of security breaches decreased slightly. 20 percent of respondents indicated a breach had occurred in the past 12 months, versus more than 25 percent in 2017. Still, one-third of organizations detect malicious activity – predominantly from malware, spear-phishing, ransomware and business email compromise (BEC) – several times every day. Among organizations that did report a breach, in 2018, fewer indicated they 'did not know' whether they were targeted or not than in 2017, suggesting an improving awareness about the nature and origination of attacks.

KEY FINDINGS

GPAs ARE RISING

Overall, report card grades improved in 2018, with 21 percent of respondents giving their programs an "A," and 42 percent rating their work at a "B." Use of automation, improvements in employee security training and a 10 percent increase in the use of threat intelligence tools contributed to the boost in confidence.

Also, the number of people that responded "I don't know" to "which tools do you use as part of your organization's defense approach?" decreased by about five percent, demonstrating a gradual improvement in program development.

EASY A

Strategic use of automation technology plays a significant role among highly-rated programs. So much so that 92 percent of "A" companies said they use automation to simplify time-consuming processes. Conversely, "D" and "F" companies said their processes are highly manual. When compared to last year, there was an eight percent decrease in the number of teams using manual processes and an increase among groups considering automated solutions.

KEY FINDINGS (CONT.)

HIGHER EDUCATION

One surprising finding was the decrease in malware analysis when investigating attacks. Malware analysis declined by 12 percent from 2017, and forensic analysis of compromised machines was scaled back by six percent.

> *"Manual disk forensics and malware analysis are time consuming and it is difficult for security professionals to quantify the time it takes to complete their analysis. The only effective way to scale out malware analysis across a large organization, or an organization with a large volume of security incidents, is through security automation, such as malware analysis sandboxes. There are multiple malware analysis sandbox services available, and each have their own unique configurations."*
>
> *- Tarik Saleh, Senior Security Engineer, DomainTools*

ROOM FOR IMPROVEMENT

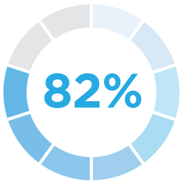
Even with top marks, there is always room for growth. The survey revealed threat infrastructure as one key opportunity for teams to hone in on and strengthen their posture. Thirty-five percent of respondents admitted they don't have the capability to expand from one indicator to a larger map of threat infrastructure, and one-third said they spend less than five hours per week hunting for threats in the network.

GPAs ARE RISING

Along with more organizations awarding their cybersecurity programs with an "A," the percentage of respondents that said their organization should be graded as a "C" or worse also declined. There was little change in how security operations are carried out, with a fairly even split between teams comprised of exclusively in-house experts, or a combination of in-house experts with outside analyst support. Despite the consistency in team structure from year to year, and the fact that the threat landscape hasn't changed much since 2017, security pros feel more confident now than in previous years. The survey uncovered a variety of reasons why security GPAs are rising amidst a steady flow of active or suspected cyber attacks.

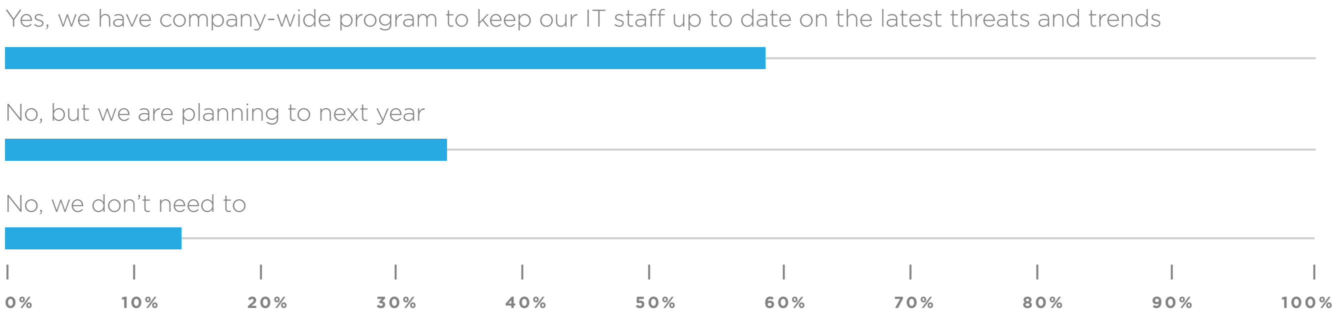
One of these is an increased interest in providing company-wide training to keep IT staff and the broader staff up-to-date on the latest threats. Five percent more organizations plan to step up training in the coming year than did last year, and the number of those that intend to skip training initiatives decreased by half from 2017.

In addition to better attitudes toward the importance of training, more organizations are relying on threat intelligence tools and advanced methods for thwarting attacks. The survey also found that when investigating or stopping a customized attack, the vast majority (82 percent) of security professionals find value in drilling down on IP addresses or domain names to make organization more secure and are more likely to agree the higher grade they give themselves as an organization (e.g. 60 percent of "A" companies vs. 37 percent of "F" companies).



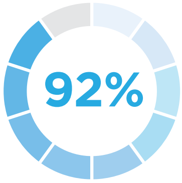
The vast majority of security professionals find value in drilling down on IP addresses or domain names.

Q: Do you have a formalized training program for your security staff?



EASY A

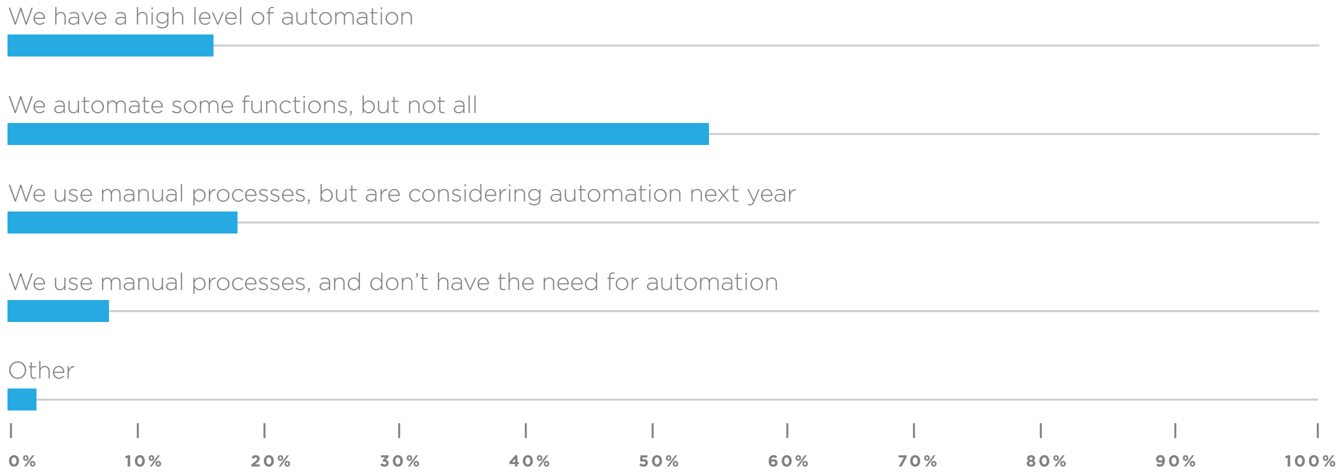
As worldwide cyber threats and threat actors grow in numbers, motivation and capability, organizations must rely on a strategic combination of advanced technology and highly skilled staff to effectively combat them. Automation is supporting security teams in strengthening their security postures, and 92 percent of organizations that graded themselves with an "A" in 2018 have some level of automation. Use of automation tools increased slightly in this year's survey, and the number of professionals considering automating elements of their security processes also increased. A separate joint **report from DomainTools and Ponemon Institute** earlier this year found that 60 percent of security and IT professionals believe automation will improve their staff's ability to do their jobs because it will enable them to focus on more serious vulnerabilities and overall network security. Still, 63 percent say that human involvement in security is important in the age of automation. The key is that while automation will help streamline manual, low-skill tasks, its use must be applied in a strategic way that allows for work on more advanced threats to be carried out by highly-skilled security professionals.



Percentage of organizations that graded themselves with an "A" in 2018 have some level of automation.

Percentage of security and IT professionals that believe automation will improve performance.

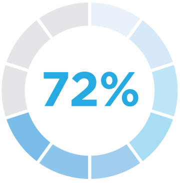
Q: What is your level of security automation?



HIGHER EDUCATION

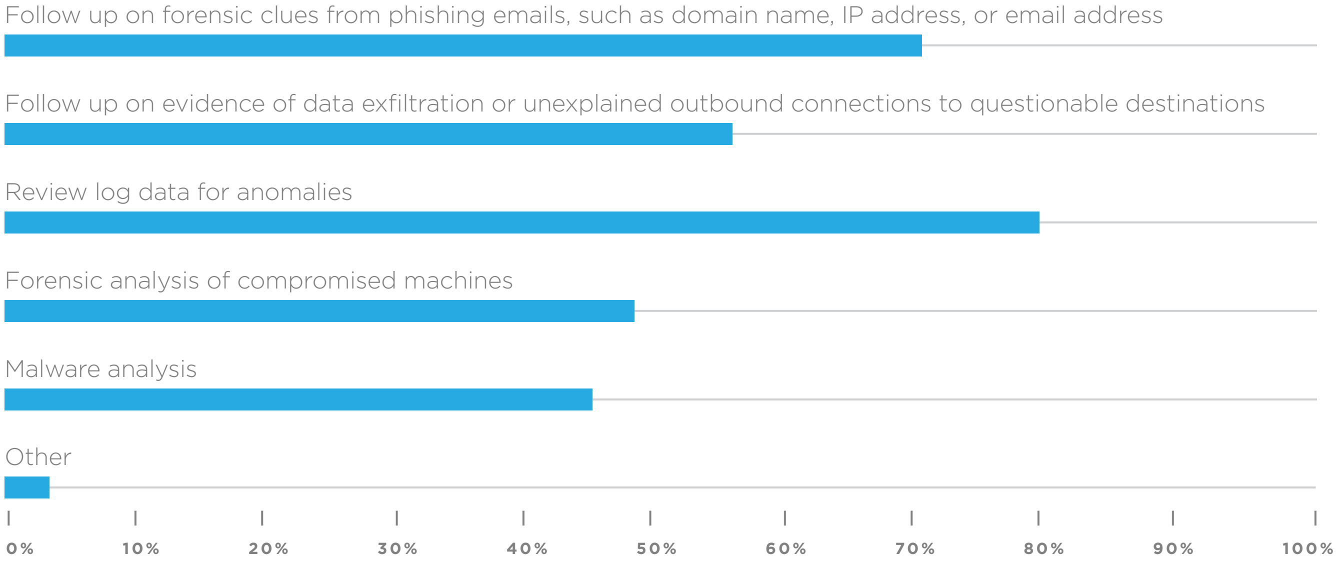
Malware and ransomware continue to be the most common attacks detected by security experts surveyed. However, in 2018, when investigating attacks, malware analysis decreased by 12 percent from the previous year. Forensic analysis of compromised machines also decreased. One potential reason for this is that malware analysis tends to be a manual and time-intensive process. Because teams are increasingly pressured to be more time-efficient and operate on lean budgets and resources, manual activities, even if they are high-value, may take a hit.

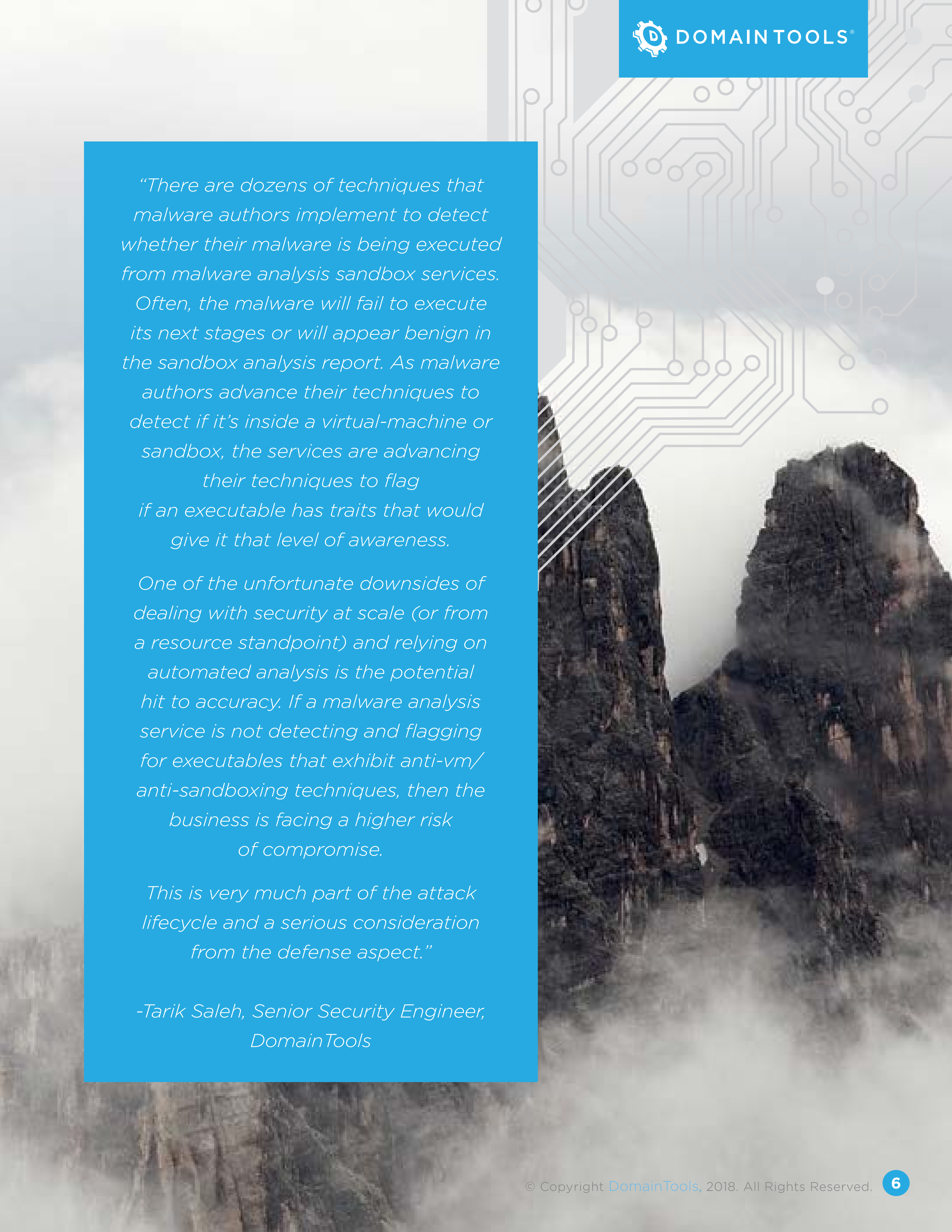
It is critical for skilled analysts to be given the necessary time to conduct in-depth analysis of threat indicators and active threats from malware or other methods. Teams should rely on a combination of tools that can help streamline certain tasks, while still giving their experts ample time to do the critical research. This is validated in the survey, as "A" and "B" organizations were much more likely to follow up on clues and evidence and conduct forensic analysis of compromised machines compared to "D" and "F" teams (e.g. 72 percent of "A" organizations review log data compared to 37 percent of "F" organizations).



Percentage of "A" organizations that review log data compared to 37 percent of "F" organizations.

Q: When investigating attacks, do you do the following?





"There are dozens of techniques that malware authors implement to detect whether their malware is being executed from malware analysis sandbox services. Often, the malware will fail to execute its next stages or will appear benign in the sandbox analysis report. As malware authors advance their techniques to detect if it's inside a virtual-machine or sandbox, the services are advancing their techniques to flag if an executable has traits that would give it that level of awareness.

One of the unfortunate downsides of dealing with security at scale (or from a resource standpoint) and relying on automated analysis is the potential hit to accuracy. If a malware analysis service is not detecting and flagging for executables that exhibit anti-vm/anti-sandboxing techniques, then the business is facing a higher risk of compromise.

This is very much part of the attack lifecycle and a serious consideration from the defense aspect."

-Tarik Saleh, Senior Security Engineer, DomainTools

ROOM FOR IMPROVEMENT

In 2018, while 71 percent of "A" organizations said they have the capability to expand from one indicator to a larger map of threat infrastructure, **35 percent** of overall organizations are lacking in this area. Among those that do have threat infrastructure in place, 31 percent use a variety of systems to manually develop a larger threat map, and 19 percent rely on one product to view the broader picture.

When looking at threat hunting as part of the overall infrastructure, sophistication varies widely. As mentioned earlier, one-third of survey respondents spend less than five hours per week hunting threats; another third spends anywhere from six to 25 hours, and 11 percent spends more than 60 hours per week on this task. Nine percent of respondents said they do not threat hunt at all.

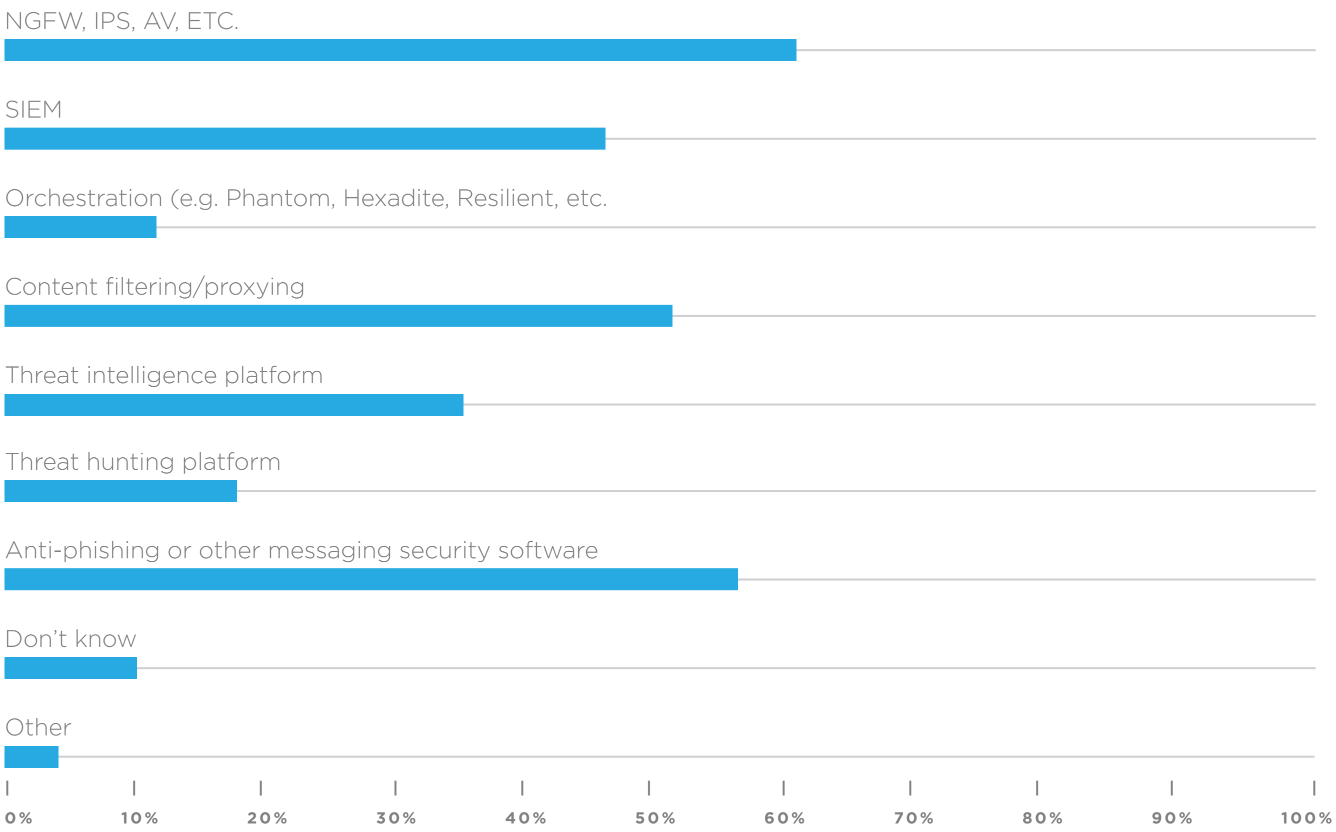
Developing and refining threat infrastructure is a clear area for improvement for many organizations, and those that graded themselves with a "D" or "F" pointed fairly equally to the need for more budget, staff, company-wide education and time to deploy technology in order to reach top marks.

"Unfortunately, a large skills gap still exists in this field, and until we find a better way as an industry to educate people on the many variants of security, adoption of proactive programs like threat hunting will lag. It is our deep idealism that hopes for more organizations to prioritize threat hunting, but in reality, it will be a gradual progression."

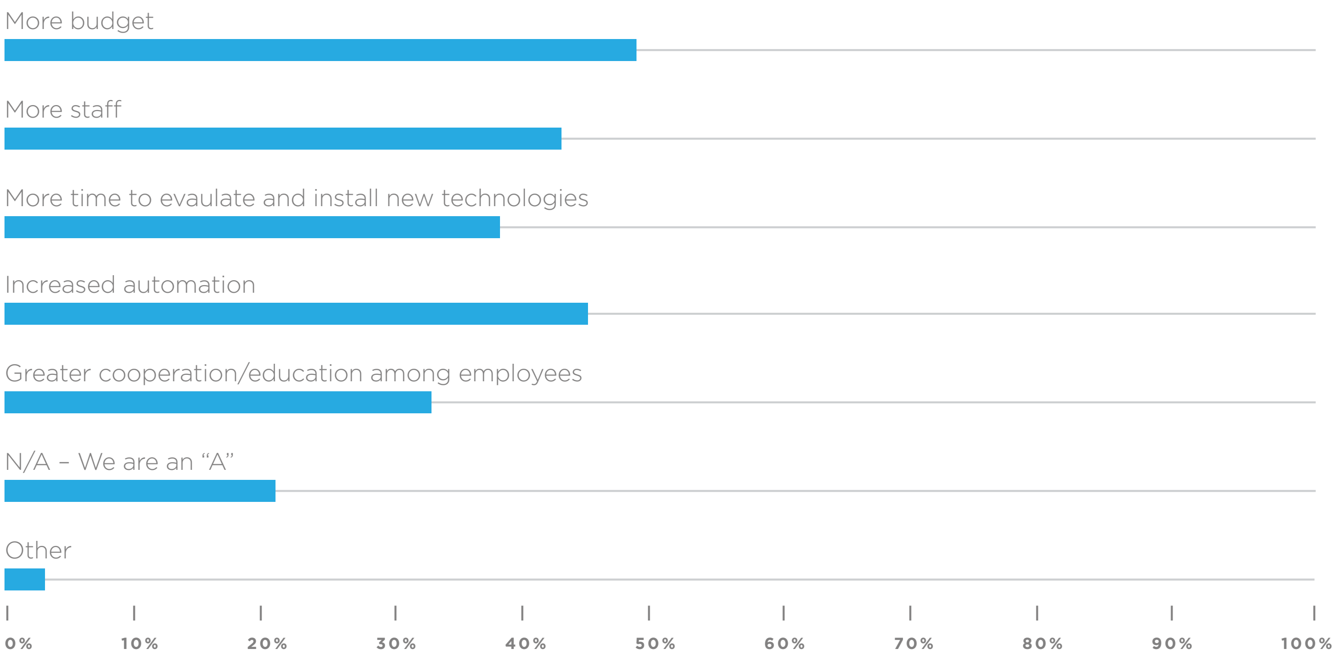
-Corin Imai, Senior Product Marketing Manager, DomainTools

ROOM FOR IMPROVEMENT (CONT.)

Q: Which tools do you use as a part of your organizations defense approach?



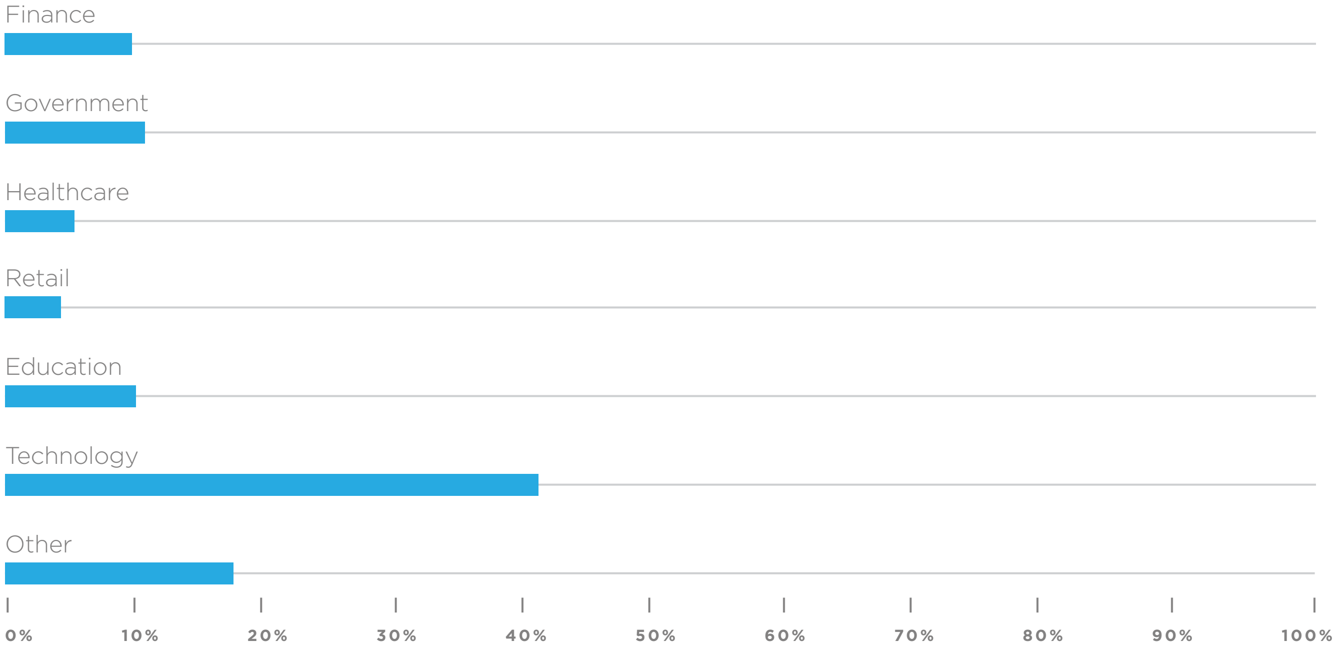
Q: If you’re not an “A”, what will it take to get you there?



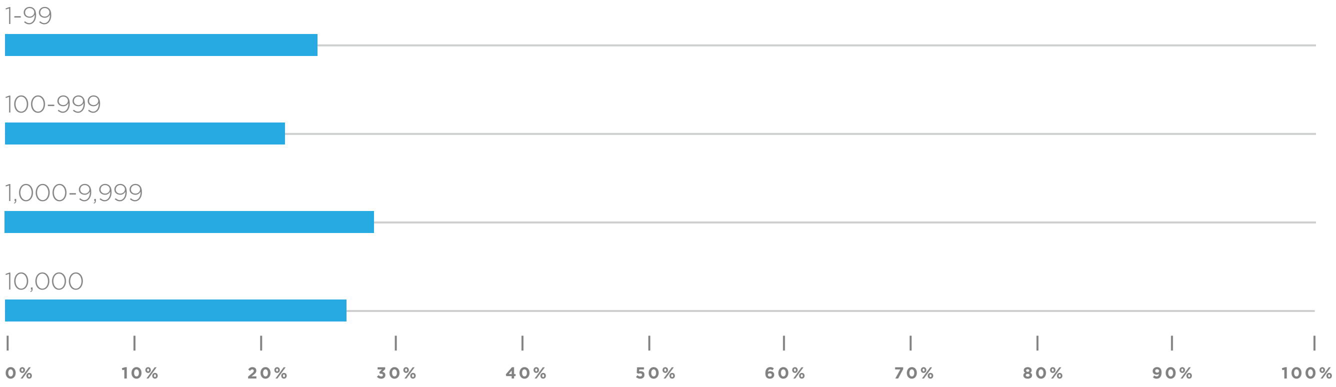
METHODOLOGY

The survey was conducted by DomainTools in July 2018, and polled 525 global security professionals and executives working in finance, government, healthcare, retail, technology and other industries in organizations of up to 10,000+ employees. Regions include North America, EMEA, APAC and LATAM. A breakdown of the respondents' titles, roles and industries are provided below.

Q: What is your industry?

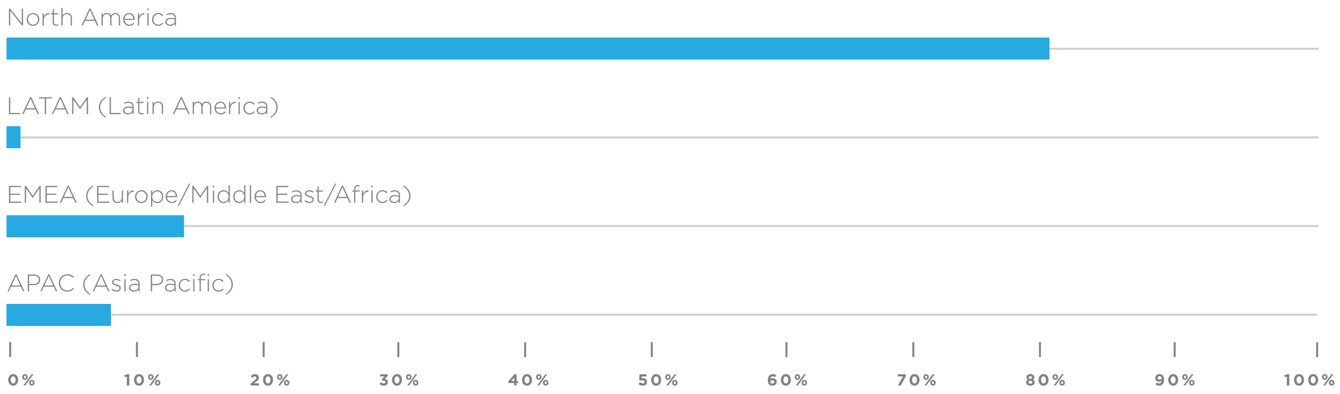


Q: How large is your organization?

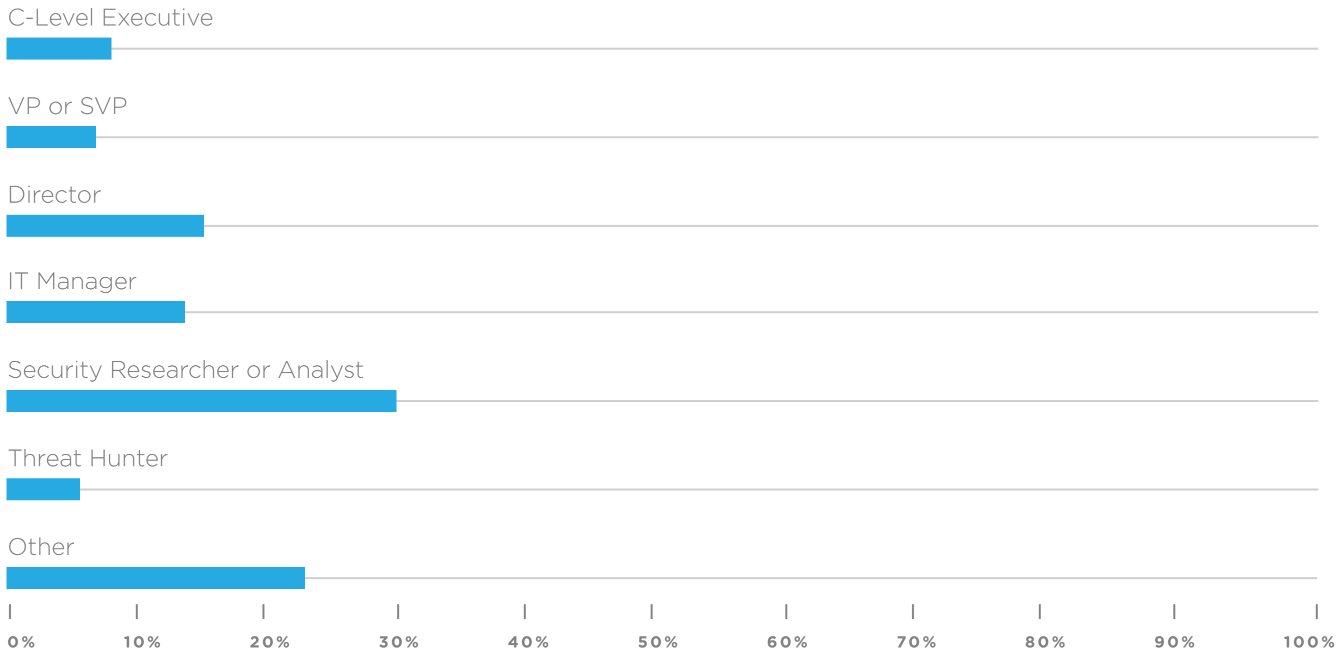


METHODOLOGY (CONT.)

Q: Where are you located?



Q: What is your title?



ABOUT DOMAINTOOLS

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work. Learn more about how to connect the dots on malicious activity at **http://www.domaintools.com** or follow us on **Twitter: @domaintools.**