DOMAINTOOLS

2017 CYBERSECURITY REPORT CARD

SECURITY PROFESSIONALS RATE THEIR MATURITY AND SHARE BEST PRACTICES

Conducted By: Byron Acohido & DomainTools Research Team

SUMMARY

Today's global enterprises are inundated daily with malicious activity, leaving security analysts and IT executives scrambling to find the ideal combination of manpower, resources, techniques, and advanced cybersecurity solutions to help defend against network threats coming from sophisticated hackers.

This report summarizes the findings of a survey comprised of more than 550 security professionals and IT executives, who are in the trenches implementing security solutions. The goal was to determine the current state of cybersecurity within the enterprise including what initiatives are proving most effective and where the gaps remain in threat detection and prevention.

KEY FINDINGS

NOBODY'S PERFECT

Networks are inundated by cyberattacks and security teams admit they can't detect or prevent them all. More than one in four organizations have been breached in the past 12 months, while shockingly 23 percent aren't sure if they have been breached or not.

MAKING THE GRADE

Automation and training, and threat intelligence make for a top rating, Of the 15 percent of companies that gave themselves an "A" grade, the vast majority boast a formalized training program for security staff, virtually all utilize some degree of automation within their security programs, and 78 percent use threat intelligence to follow up on forensic clues of an attack to protect the company.

TOP OF THE CLASS

The survey found a strong correlation between "A" grade companies experiencing the lowest number of breaches within the past year. When asked if they have experienced a network breach in the past 12 months, only 15 percent of "A" companies have, compared to 27 percent of "C" companies, 38 percent of "D" companies, and 63 percent of "F" companies.

EXTRA CREDIT

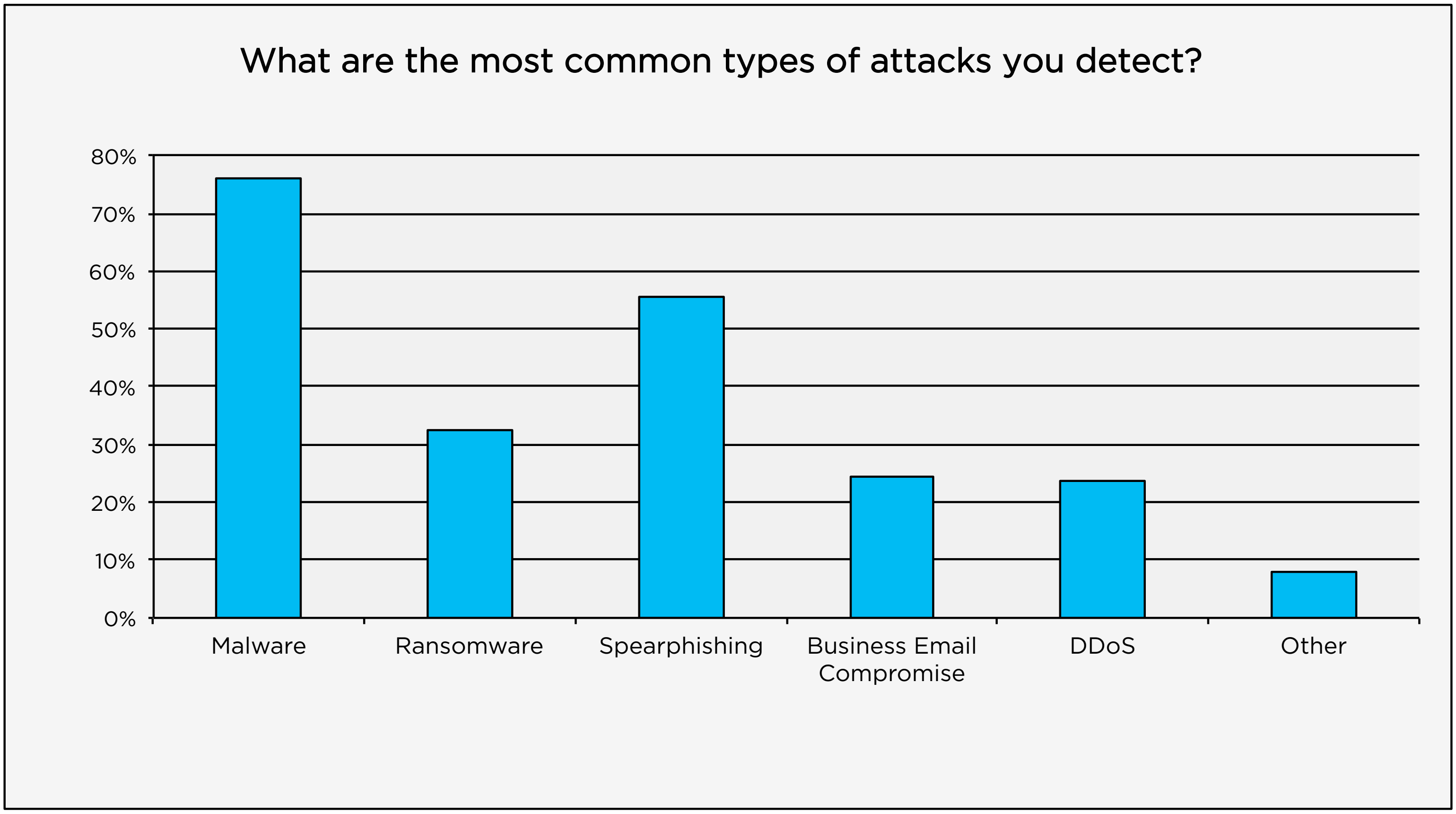
Amongst the disparate tools and strategies, threat hunting emerges as a top tactic. The majority of respondents find value in hunting – specifically drilling down on forensic clues from phishing emails, such as domain name, IP address, or email address, and disclose that it leads to information that makes the organization more secure.

NOBODY'S PERFECT

More than one in four organizations have been breached in the past 12 months, while shockingly 23 percent aren't sure if they have been breached or not. What's more, one-third of security pros are savvy enough to detect daily attacks, but the looming majority (66 percent) are unaware of the daily onslaught of malicious activity. While malware (76 percent) and spearphishing (56 percent) are the most common types of threat vectors, business email compromise (25 percent) and DDoS attacks (24 percent) are on the rise. Nearly one-third of respondents were the recipients of attempted cyberextortion, also known as ransomware, which cost businesses more than $1 billion in 2016.

While companies are experiencing regular network attacks, the good news is that the majority (53 percent) of security execs detected a recent attack the same day it occurred, nearly a third (28 percent) detected a recent attack between a day and a week, and roughly 20 percent detected a recent attack between a week and a month after it occurred. However, one of the four companies who have been breached in the past 12 months aren't sure if the attack was targeted or not and nearly 20 percent of companies believe the attack wasn't customized to their organization.

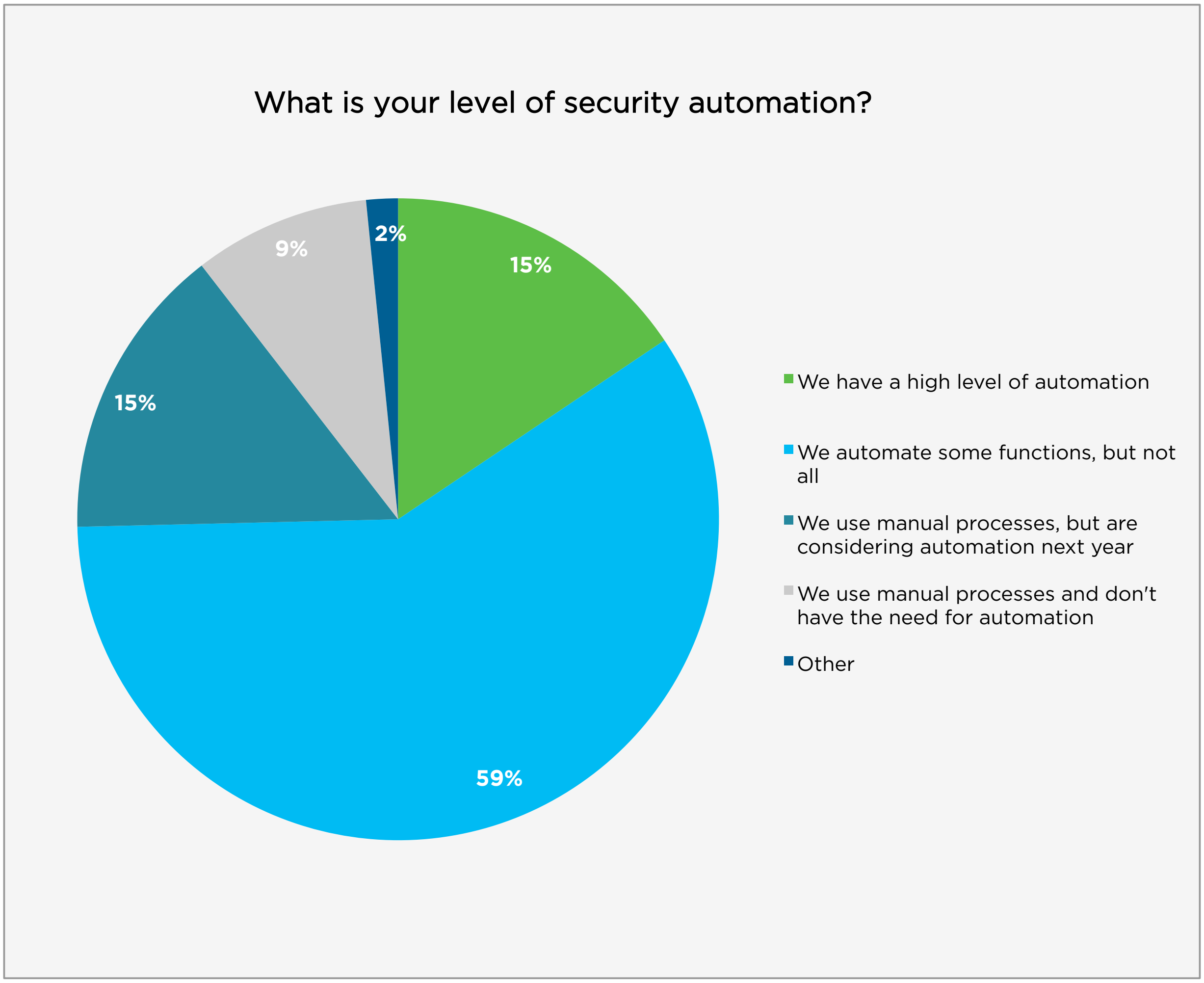
Figure 1: The most common types of attacks that security professionals are regularly detecting on their network include malware, spearfishing, ransomware, business email compromise and DDoS.



MAKING THE GRADE

Automation, training, and threat intelligence make for an "A" grade enterprise
While the bulk (41 percent) of organizations report having a full SOC in-house and over a quarter (26 percent) have analysts performing SOC-like function, there is a not a one-size fits all approach to carrying out security operations within the enterprise. This is further evidenced by the fact that the majority (56 percent) of companies have an in-house malware analyst yet nearly one-third (29 percent) use or consult external resources to learn more about malware. Of the 15 percent of companies that gave themselves an "A" grade, the vast majority (82 percent) boast a formalized training program for security staff, virtually all (99 percent) utilize some degree or a high level of automation within their security programs, and 78 percent use threat intelligence to follow up on forensic clues of an attack to protect the company. These attributes compare starkly to lower-graded companies. For example, only 37 percent of the "C" companies and none of the "F" companies have a formalized training program, 63 percent of "D" companies use manual processes and are more likely to think they do not need automated processes.

Figure 2: Current level of security automation within an enterprise.

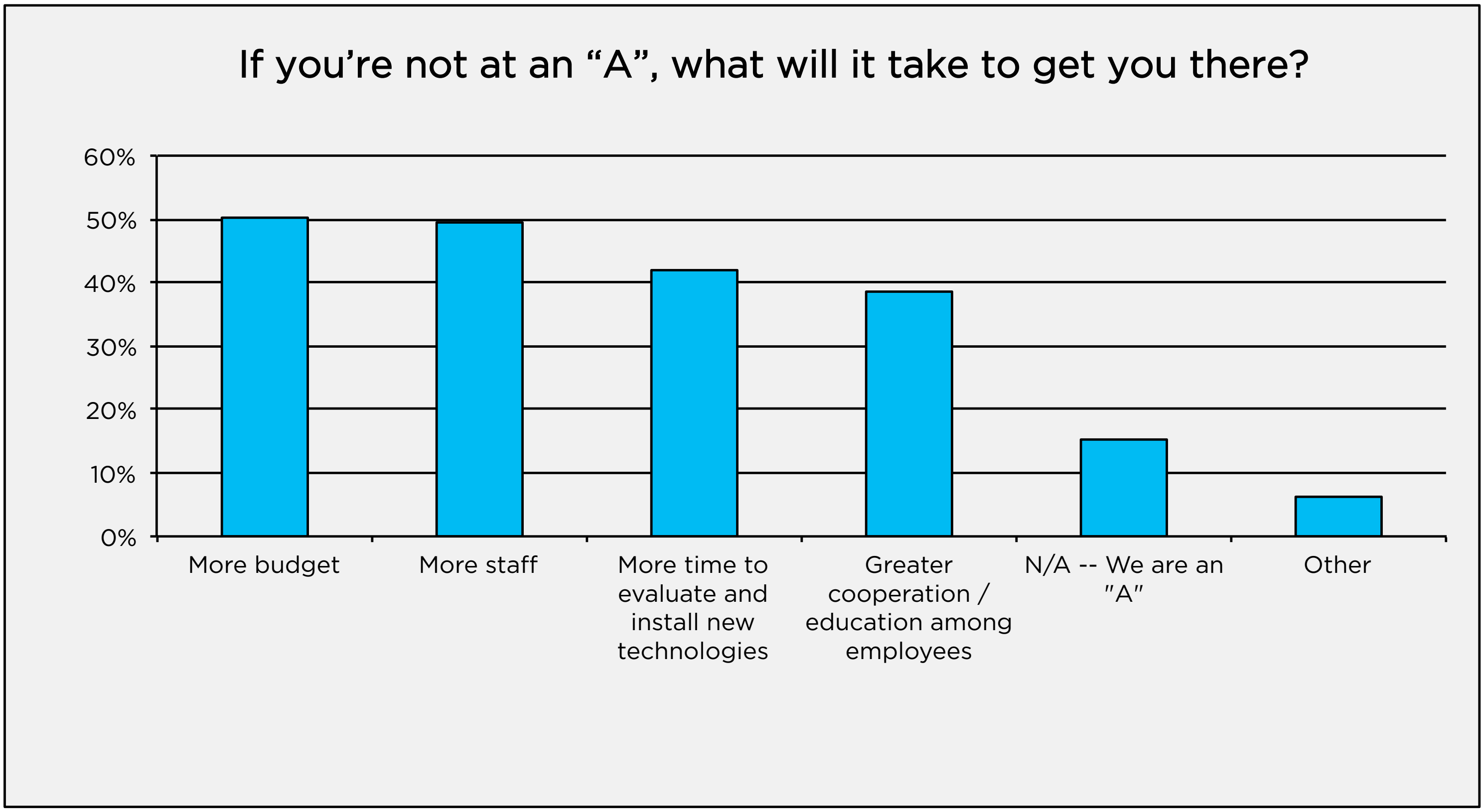


TOP OF THE CLASS

When asked if they have experienced a network breach in the past 12 months, only 15 percent of "A" companies have, compared to 27 percent of "C" companies, 38 percent of "D" companies, and 63 percent of "F" companies. In addition to more budget (50 percent) and more staff (49 percent), more time to evaluate and install technologies (42 percent), 39 percent of companies that did not grade themselves an "A" said that they need greater cooperation and education among employees in order to be successful.

> *"With devious hackers leveraging various tactics and threat vectors, it's clear there is no one-size-fits-all approach to protecting the network. What's interesting about our new global survey data is to see the actual connection between hunting threats and secure networks, as the 'A' companies that are more likely to drill down on forensic clues were less likely to be breached compared to the other companies."*
>
> Tim Helming
> Director of Product Management
> DomainTools

Figure 3: If a security professional didn't give their organization an "A", budget, staff, more time to evaluation solutions top the list of what it will take to bump up their grade.

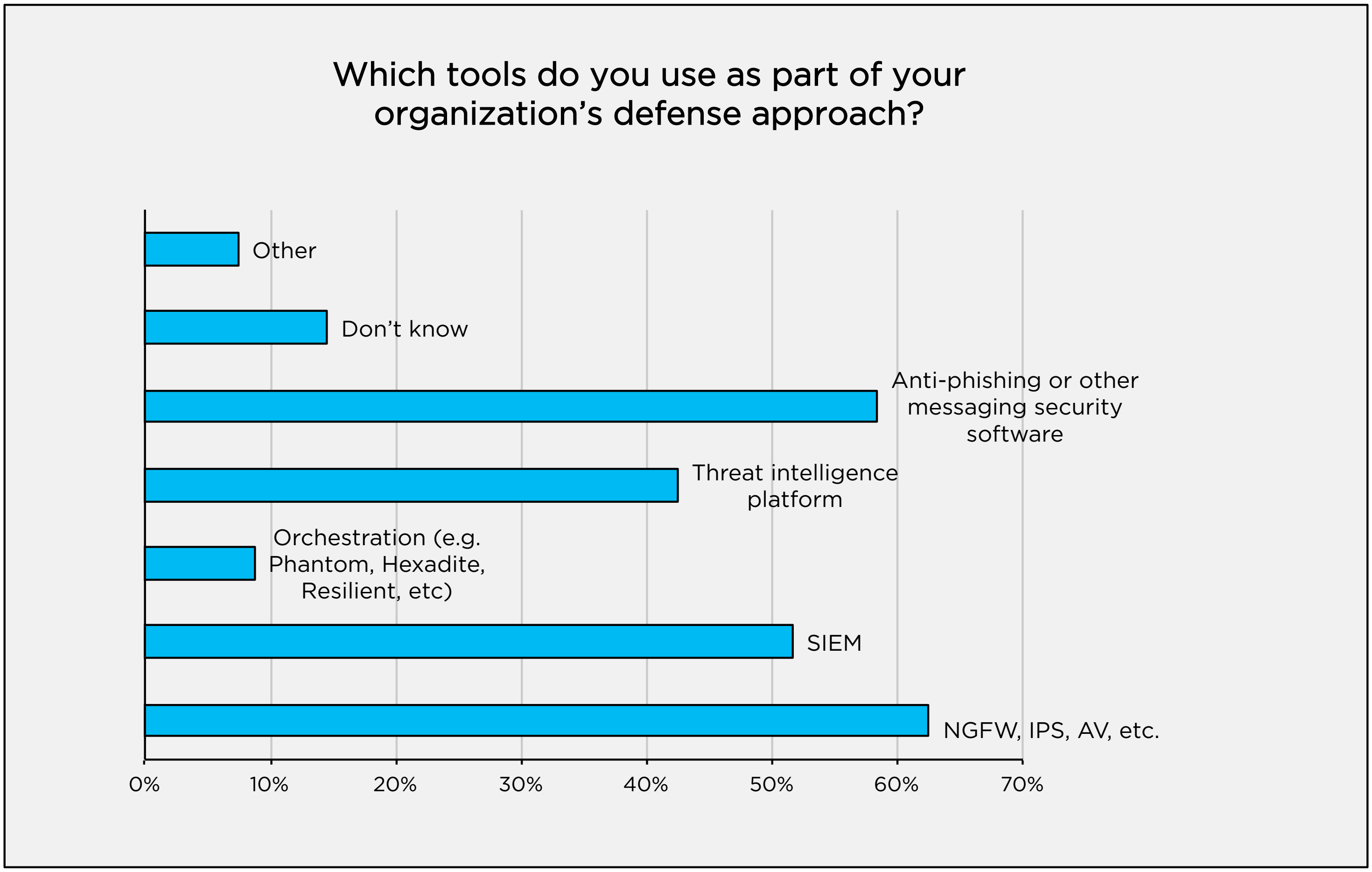


EXTRA CREDIT

The overwhelming number of ways to attack a network naturally begets the need for a variety of protections. Almost all companies use more than one cybersecurity system, including firewalls (63 percent), anti-phishing or other messaging security software (57 percent), Security Information and Event Management (SIEM) systems (52 percent), and threat intelligence platforms (42 percent). More than one quarter (26 percent) spend 26 hours or more per week hunting threats in the network, and the vast majority (78 percent) find value in threat hunting – specifically in drilling down on forensic clues from phishing emails, such as domain name, IP address, or email address, and disclose that it leads to information that makes the organization more secure.

Interestingly, "A" and "B" companies were more likely to follow up on clues and evidence compared to "D" and "F" companies. Also, the top three kinds of data that security pros log for later review include web and email filter traffic (69 percent), firewall/IPS denied traffic (65 percent) and DNS traffic (54 percent). Unfortunately, the majority (68 percent) of organizations do not have a current capability/methodology for mapping threat infrastructure or utilize a variety of systems to manually develop a larger threat map.

Figure 4: The most commonly used tools used by security professionals as part of their organization's defense approach include NGFW, IPS, AV, etc., anti-phishing or other messaging security software and threat intelligence platforms.



METHODOLOGY AND RESPONDENTS

The survey was conducted by DomainTools in conjunction with Byron Acohido in December 2016 and polled 552 global security professionals and executives working in finance, government, healthcare, retail, and technology 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 (Figures 5, 6 and 7).

Figure 5: Titles (C-level 7.79%, VP or SVP 5.07%, IT Manager 18.12%, Security Research or Analyst 37.5%, Threat Hunter 3.70%, other 27.72%)

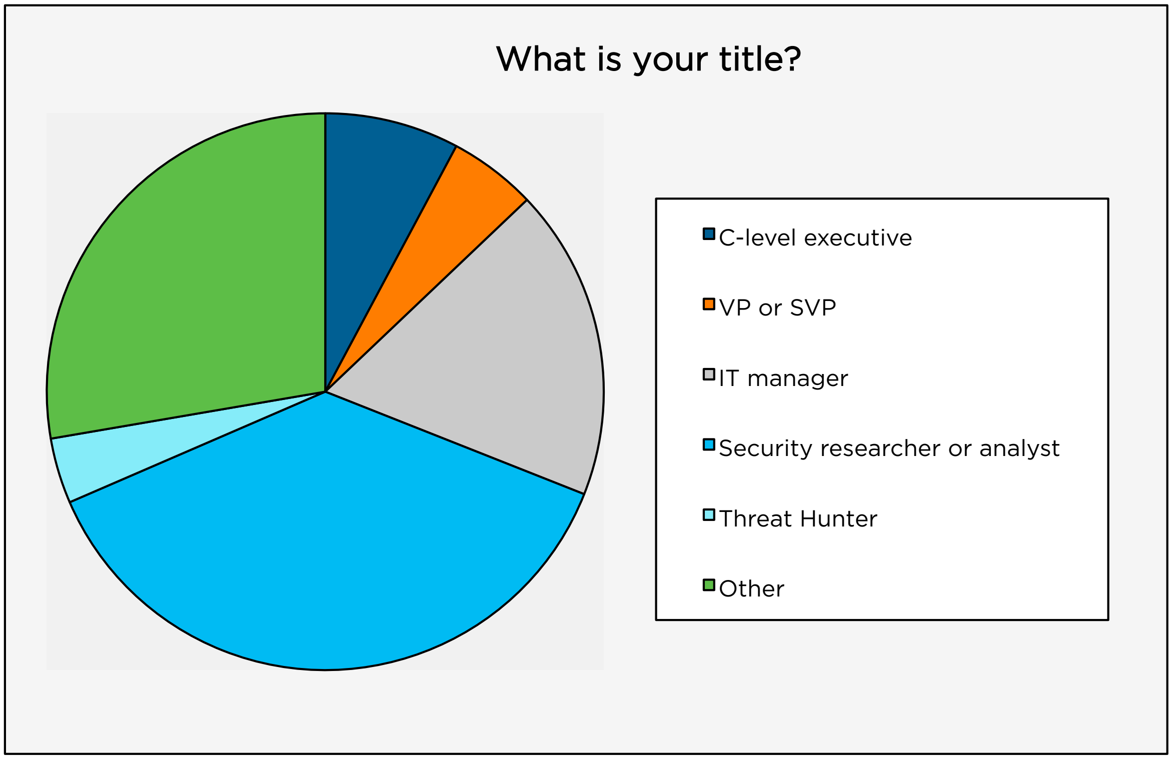


Figure 6: Industry (Finance 11.23%, Government 14.67%, Healthcare 4.35%, Retail 2.9%, Technology 44.75%, other 22.1%)

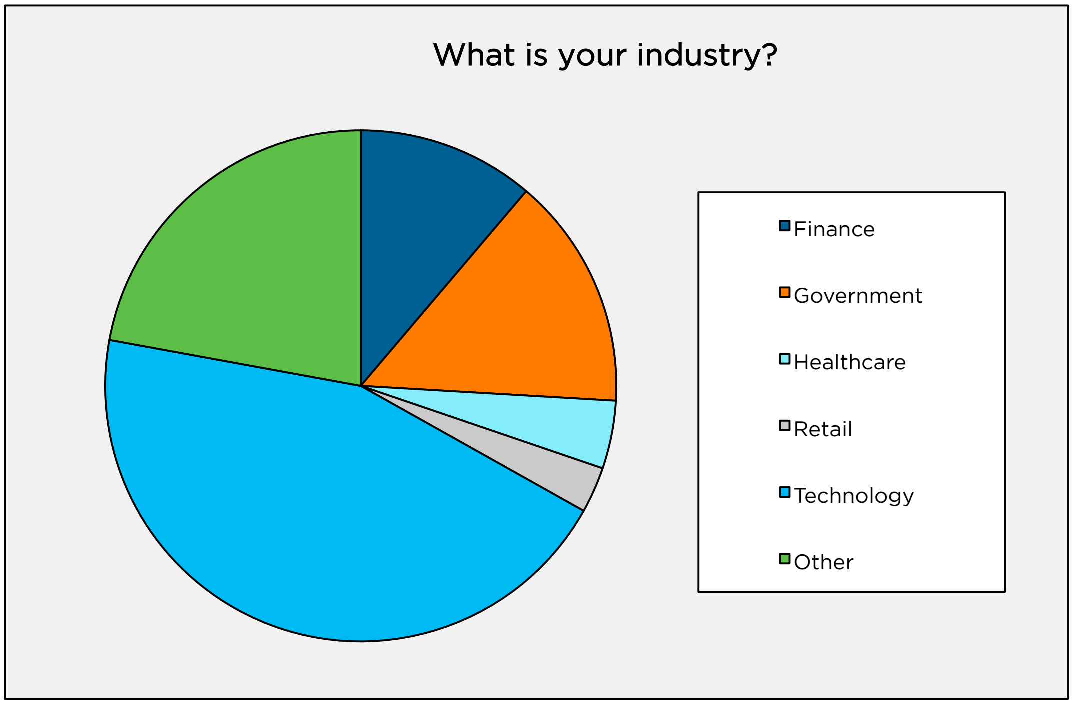
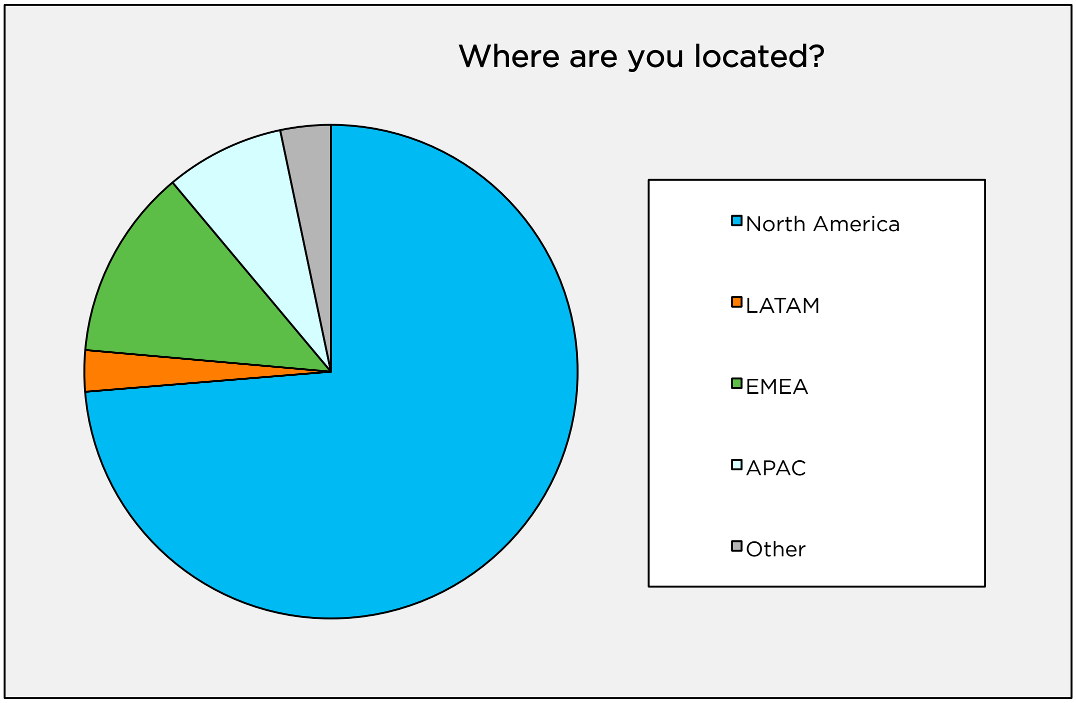


Figure 7: Location (North America 73.73%, LATAM 2.72%, EMEA 12.50%, APAC 7.79%, other 3.26%)



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.

Our goal is to stop security threats to your organization before they happen, using domain/DNS data, predictive analysis, and monitoring of trends on the Internet. We collect and retain Open Source Intelligence (OSINT) data from many sources and we index and analyze the data based on various connection algorithms to deliver actionable intelligence, including domain scoring and forensic mapping.

For more information about DomainTools' data and products, please visit our website at **www.domaintools.com**.

WORLD'S LARGEST DNS FORENSICS DATABASE

>> **10 Billion+** current and historical Whois records

>> **4.5 Billion+** IP address change events

>> **1.8 Billion+** Registrar change events

>> **3 billion+** name server change events

>> **580 million+** screenshots