2017 Threat Landscape Survey: Users on the Front Line

Lee Neely

2017 Threat Landscape Survey: Users on the Front Line

A SANS Survey

Written by Lee Neely

August 2017

Sponsored by
Cylance, FireEye, McAfee, and Qualys

Executive Summary

Endpoints—and the users behind them—are on the front lines of the battle: Together they represent the most significant entry points for attackers obtaining a toehold into the corporate network. Users are also the best detection tool organizations have against real threats, according to the 2017 SANS Threat Landscape survey. In it, 37% of respondents reported that calls to the help desk enabled them to discover their most impactful threats.

ENDPOINT

"An endpoint device is an Internet-capable computer on a TCP/IP network. The term can refer to desktop computers, laptops, smartphones, tablets, thin clients, printers or other specialized hardware such POS terminals and smart meters."[3] For our purposes, endpoints are the devices users interact with directly and regularly—their desktop, laptop, smartphone, tablet or printer.

In this survey, conducted during May and June 2017, phishing (which also includes spearphishing and whaling) and ransomware represented the top two most significant threats to hit organizations in the past year. Ransomware was also listed as their "most surprising threat" in a write-in question. (In that question, 16% cited ransomware, including WannaCry, as their most surprising threats.)

This year, DDoS replaced advanced persistent threats (APTs) as the third-most significant threat, when we consider the phishing components as one type of threat. The results mirror the 2016 Threat Landscape Survey results[1] and media reports of larger scale, more-difficult-to-prevent DDoS attacks, particularly through DNS reflection attacks.[2]

This year, we also tracked the introduction of malware-less threats that typically get around traditional malware defenses. These include credential compromise, scripting attacks, process exploits and malicious binaries.

Endpoints on the Front Line

- **74%** of respondents named clicking a link or opening an attachment in an email as the top ways threats enter the organization, and **48%** named web drive-by or download, both of which involve user intervention.
- **21%** identified awareness training for users as the top mitigation effort in which they intend to invest over the next 18 months.
- **81%** see endpoint security tools as the most helpful for threat detection.
- **81%** noted log management tools and services were helpful in determining threat scope.

While these threats had the most impact, respondents saw all manner of threats on their networks. In fact, 59% reported that the threats discovered on their networks did not have a major impact. This suggests that current defenses are more effectively detecting and removing threats at the endpoint. Endpoint security was selected by 81% respondents as the top most helpful tool or service in detecting threats before they take a foothold. For more specificity this year, we separated answer options for endpoint security from endpoint detection and response (EDR), and found that EDR was considered most helpful 59% of the time (making it sixth most helpful overall). IDS/IPS/UTM was second most helpful, followed by SIEM, network monitoring/DPI (deep packet inspection) and threat intelligence. The big change from 2016 is that SIEM moved from the fifth to the third most helpful tool, which indicates respondents may be better able to leverage this technology.

[1] "Exploits at the Endpoint: SANS 2016 Threat Landscape Survey," September 2016, www.sans.org/reading-room/whitepapers/analyst/exploits-endpoint-2016-threat-landscape-survey-37157

[2] www.darkreading.com/vulnerabilities-and-threats/2016-ddos-attack-trends-by-the-numbers/d/d-id/1326754?image_number=7

[3] Adapted from http://whatis.techtarget.com/definition/endpoint-device

Organizations are looking toward prevention focused on further educating users, improving operational security practices, increasing the skills of the response staff, and improving the implementation and effectiveness of tools they already use. As they plan their threat prevention and mitigation road maps, organizations should examine the path from the services to the endpoint, making sure relevant, current protections are in place that rely less on the user to detect an active attack and more on automation.

Key Findings

The top threats with significant impact entering the organizations:

- **40%** of respondents (the most) selected phishing, including spearphishing and whaling
- **20%** identified ransomware
- **11%** chose DDoS
- **11%** chose APT

The top malware-less threats having the most impact on organizations:

- **22%** (the most) chose credential compromise
- **19%** selected scripting attacks
- **14%** identified process exploits
- **14%** tagged malicious binaries

About Our Respondents

SANS created this survey to find out what threats are impacting our respondents, where they are focusing their efforts and what gaps they see in their practices, and 263 IT and security professionals stepped up to help us understand the current state of affairs. They represented a nearly equal mix of security-specific roles and more general IT roles: 42% had security-specific jobs, including analysts, architects and CISOs, and 39% held IT roles, including system administrators and IT managers. Some interesting titles also showed up under the "other" category, including threat analyst, data security expert and information security engineer.

Company sizes ranged from under 100 to over 100,000, with 45% representing organizations of 1,000 or less employees and contractors; 22% representing organizations of 1,001 to 5,000; 25% had 5,001 to 100,000; and 8% had more than 100,000 employees and contractors.

Mostly headquartered in the United States, the top five industries represented in this survey base are shown in Table 1. Other sectors, including healthcare, manufacturing, telecom and energy, among others, each contributed less than 7% of the total and accounted for the remaining respondents.

Table 1. Top Five Industries Represented

Industry	Percentage
Banking and finance	17.9%
Government	12.2%
Cyber security	11.4%
Technology	10.6%
Education	8.7%

The Threat Landscape

When describing the ecosystem of an attack, we need to start with definitions. The SANS Internet Storm Center has a nice glossary of industry standard definitions of the following terms:[4]

- A **threat** is a potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm.
- A **threat vector** is the method a threat uses to get to the target.
- An **incident** is an adverse network event in an information system or network, or the threat of the occurrence of such an event.

Other key definitions include the following:

- "A **data breach** is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property."[5]
- **Malware-less attacks** are a category of threats that use the built-in features of the operating system to turn it against itself without downloading recognizable files.

Top Threats

Phishing (72%), spyware (50%), ransomware (49%) and Trojans (47%) are the threats most seen by respondents' organizations, but not all of these have significant impact. When it comes to impact, phishing has the greatest impact, and DDoS and APT have a greater impact than either Trojans or spyware. See Figure 1 on the next page.

[4] https://isc.sans.edu/glossary.html

[5] http://searchsecurity.techtarget.com/definition/data-breach

Over the past 12 months, which of the following types of threats have you seen in your organization? Of those, please indicate which types of threats had the most significant impact on your organization. ***Select all that apply.***

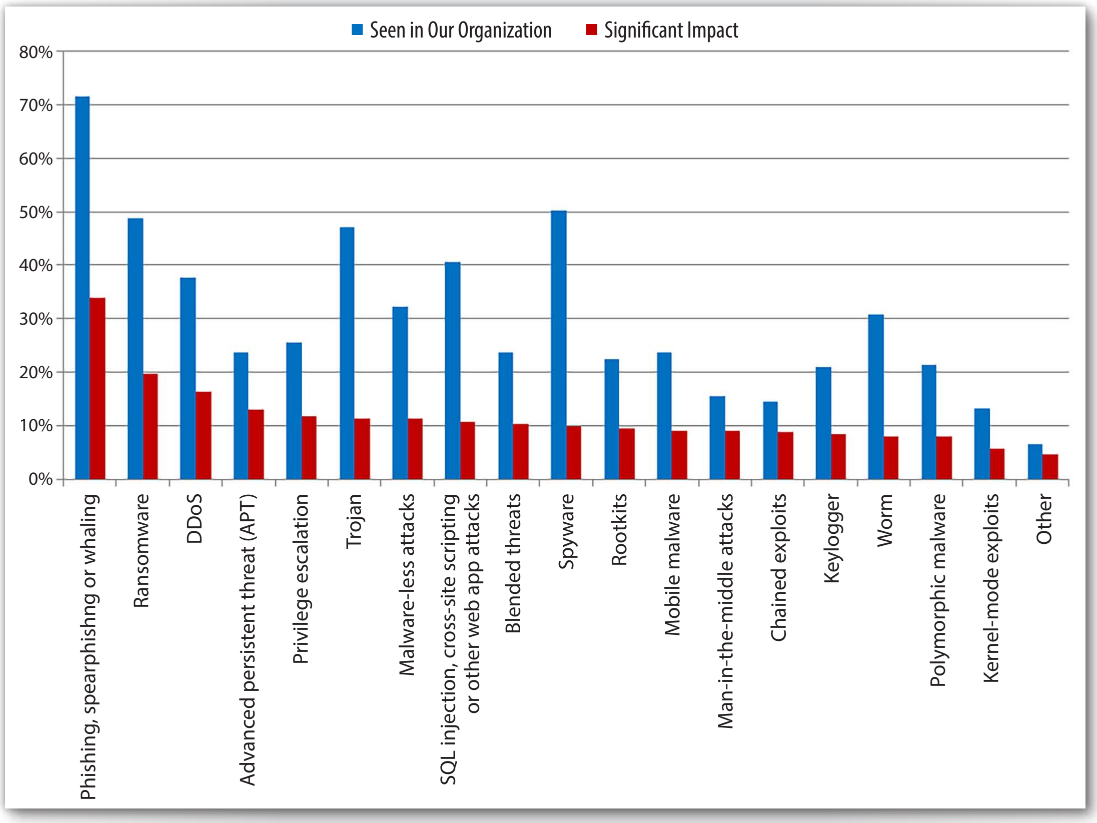

Figure 1. Threats Seen and Those Having the Greatest Impact

In addition to the traditional threats reported by respondents, we now have malware-less threats entering the organizations, impacting IT systems and adding to IT staff workload. These attacks are more difficult to find because they can't be detected by signature-based technologies. Given that this type of attack is on the rise and evading detection, organizations should be utilizing tools that detect and pre-empt patterns and movements of attacks rather than just signatures.

Of the 32% of organizations that reported seeing malware-less attacks and the 11% reporting serious impact from these attacks, scripting attacks were the most common, while credential compromise or privilege escalation caused the most impact, as illustrated in Figure 2.

What type of malware-less threats have you just seen in your organization or which you have seen and had the most significant impact?

If you have not encountered malware-less threats, please skip this question.

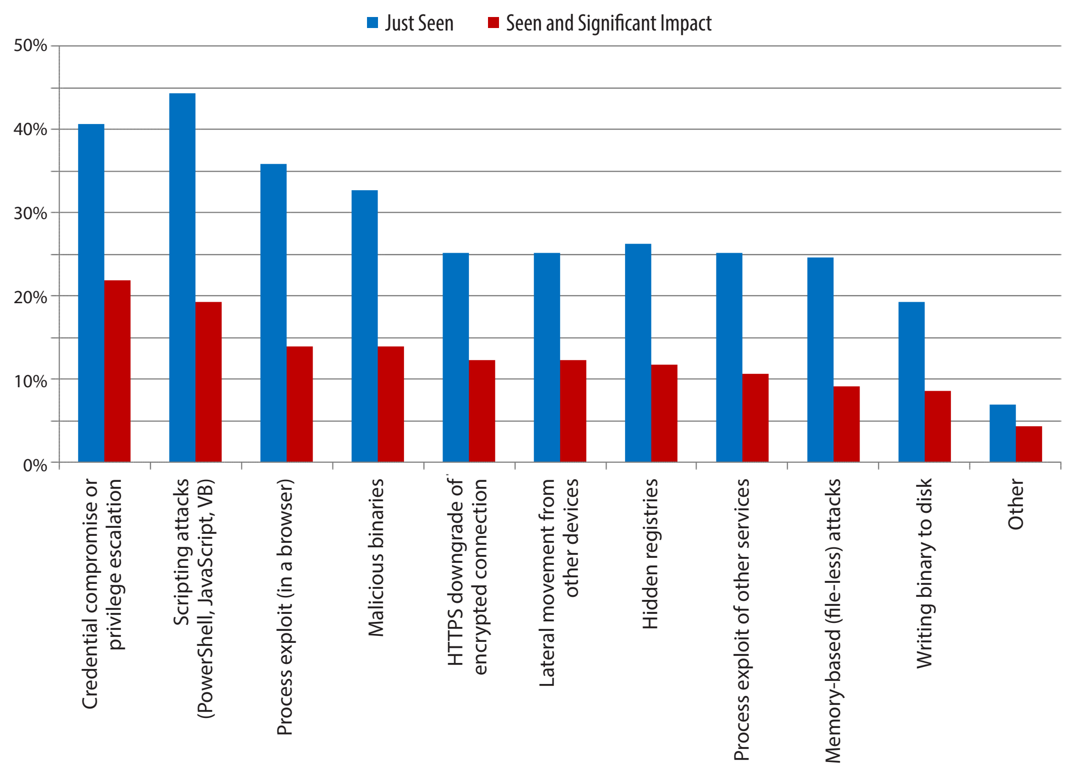

Figure 2. Occurrence and Impact of Malware-less Threats

Of the malware-less threats with significant impact, 22% cite credential compromises as being used in the attacks, and 19% reported the use of scripting attacks, including PowerShell, JavaScript and VB.

Because we are seeing more exploits, such as the link-hovering exploit for PowerPoint that executed PowerShell scripts that are designed to bypass Window's PowerShell security settings, and a seeming rise in Macro viruses, expect a rise in the occurrence and sophistication of malware-less threats.

The worrisome part is that malware-less threats don't rely on using files that can be captured by or trigger defenses, so much of the detection is based on humans rather than tools. Automation, pattern matching, artificial intelligence, threat hunting and machine learning will all play a role in helping identify such attacks in the future.

Most Surprising Threats

Similar to their most impactful threats, the most surprising threats seen and addressed in respondent enterprises that were most frequently listed include ransomware (including in a trusted binary and WannaCry), targeted attacks, DNS poisoning, malware installed on air-gapped laptops, persistent (difficult to remove) malware, accidental DDoS, single sign-on exploitation/privileged access, mobile attacks originating from inside the network and pointing outward, three vishing (voice phishing) attacks in a row, server-side vulnerabilities, targeted attacks, attacks on printers, double payload malware, very specific phishing attacks and attacks on apps.

Of the discovered significant threats, 42% report that none of these threats were unknown or zero-day, and 33% report fewer than 10% of the threats were unknown or zero day. Given the list of surprising threats seen, some of which started as zero day, there is a chance that organizations are not detecting all their zero-day/unknown threats, and/or are not dealing with them. It also means that organizations may not be patching their systems with security updates, leaving them vulnerable. In fact, in the 2016 SANS survey on continuous monitoring, the largest group of respondents (21%) were taking 2 weeks to a month to repair critical vulnerabilities, just over 20% were taking 1–12 months to repair and nearly 11% were unsure.[6]

Without proper visibility into unknown threats, it appears to respondents that mostly known threats are penetrating their borders. This makes organizations rely too heavily on the protections for threats the organizations know about, leaving their system ripe for serious zero-day attacks that could run rampant once introduced.

[6] "Reducing Attack Surface: SANS' Second Survey on Continuous Monitoring Programs," November 2016, www.sans.org/reading-room/whitepapers/analyst/reducing-attack-surface-sans%E2%80%99-second-survey-continuous-monitoring-programs-37417, Figure 9.

Top Vectors

In the survey, 74% of the threats entered as an email attachment or link, 48% entered the browser via web-based drive-by or download, and 30% through application vulnerabilities on user endpoints. See Figure 3.

TAKEAWAY

In the survey, removable media, endpoint misconfiguration, and web server/application vulnerabilities were tied as entry points. It's important to note that most of the top entry methods attempted influence of the end user or end user device, either by direct or unintended action. These top vectors are where organizations with limited resources should focus most of their attention.

What vector(s) did these threats take to enter your organization? ***Select those that most apply.***

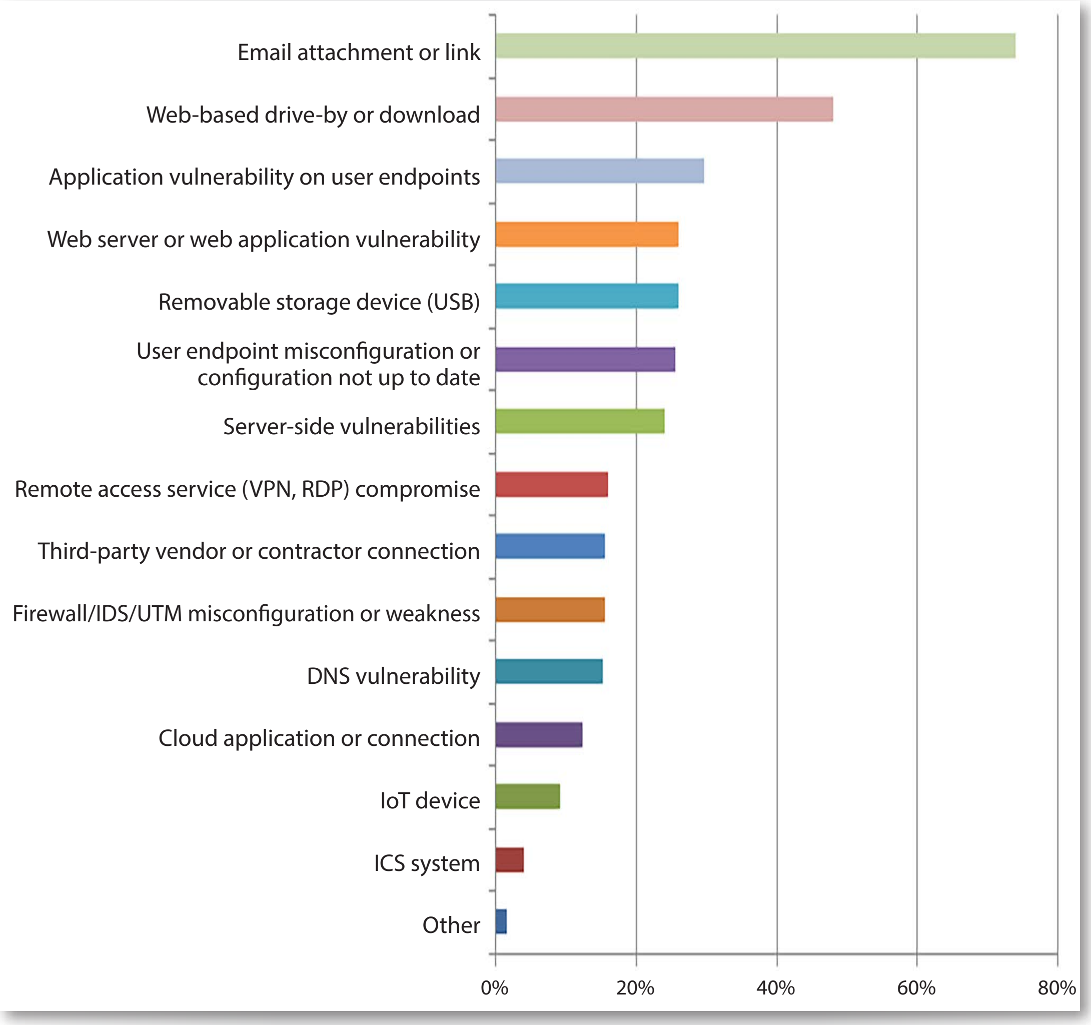

Figure 3. Vectors Threats Use to Enter Organizations

Web servers and web application vulnerabilities are tied for fourth position with removable storage devices at 26%. User endpoints are implicated in the removable storage devices category. Removable devices are utilized to overcome air-gap technologies.[7]

[7] www.techrepublic.com/article/6-ways- to-secure-air-gapped-computers-from-data-breaches

Impact

There is some confusion between what constitutes a data breach and a security incident. A data breach involves the release of (sensitive) information, while an incident is an event with a system impact, such as DDoS, website defacement or ransomware. Reporting requirements are very different for each, but in general, organizations are required to report data breaches and can use their discretion in reporting security incidents.

When it comes to damage, 59% of discovered threats were just nuisance events that had to be investigated but didn't cause damage. As far as damaging attacks, denial of service (27%) and system damage (26%) were nearly equal in being reported as damaging. As reported earlier, DDoS was the third most common impactful attack method used against respondent organizations, so this makes sense. In many cases, denial of service can cause damage to systems, and damaged systems can cause denial of service. Data destruction, including loss of data integrity, also occurred in 19% of instances. Write-in responses also included loss of services to customers due to outage. See Figure 4.

What damages resulted from discovered threats? ***Select all that apply.***

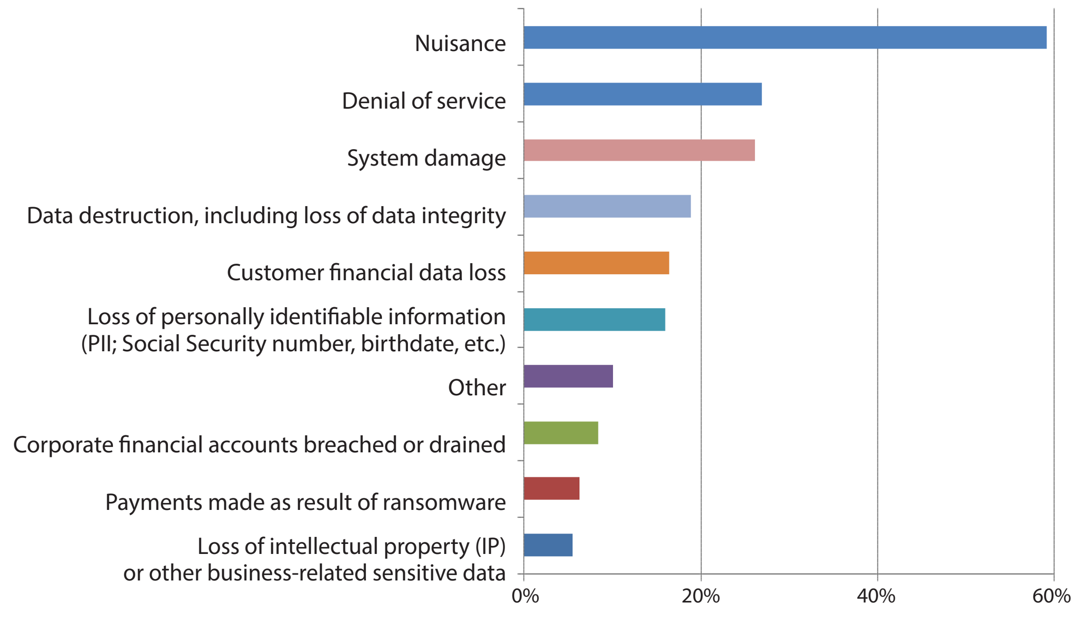

Figure 4. Damages from Discovered Threats

Recall that while organizations see many threats, not all of them are manifested in a significant impact. For example, while 50% of organizations reported seeing spyware, only 10% reported a significant impact from discovered spyware. This is a reflection on our ability to contain and eliminate threats before they get out of hand. Such results point back to users assisting in reducing the impact of attacks, with one write-in response to another question on impact saying, "None [no impact], users reported them, and we've stopped them all (as far as we know)." This point was further reinforced by organizations' abilities to respond and remediate quickly, which we cover in the next section.

Threat Response

Respondents indicate they have their highest level of confidence in their ability to respond to threats rather than detect or intercept them. That raises the question: If you can't detect the threat, how can you respond to it?

Overall, respondents ranked their confidence in meeting the following challenges:

- Respond to significant threats on the network and endpoints (90%)
- Detect significant threats occurring on your network and endpoints (82%)
- Intercept threats before they cause damage on your network and endpoints (74%)
- Remove all artifacts of significant threats on network and endpoints (73%)
- Detect zero days/unknown threats that could impact your organization (48%)

The majority of respondents (51%) are least confident in their ability to detect zero days, which points to earlier survey results showing APTs as one of the top four methods used in significant breaches. It also reiterates the need to prevent breaches through good hygiene of systems because zero days and APTs take advantage of known and unknown vulnerabilities in systems.

Discovery

When it comes to discovery of threats with significant impact, network monitoring and alerts from the perimeter defenses are the top means of discovery, according to results illustrated in Figure 5.

If you can't detect the threat, how can you respond to it?

How were the most impactful threats discovered? ***Select all that apply.***

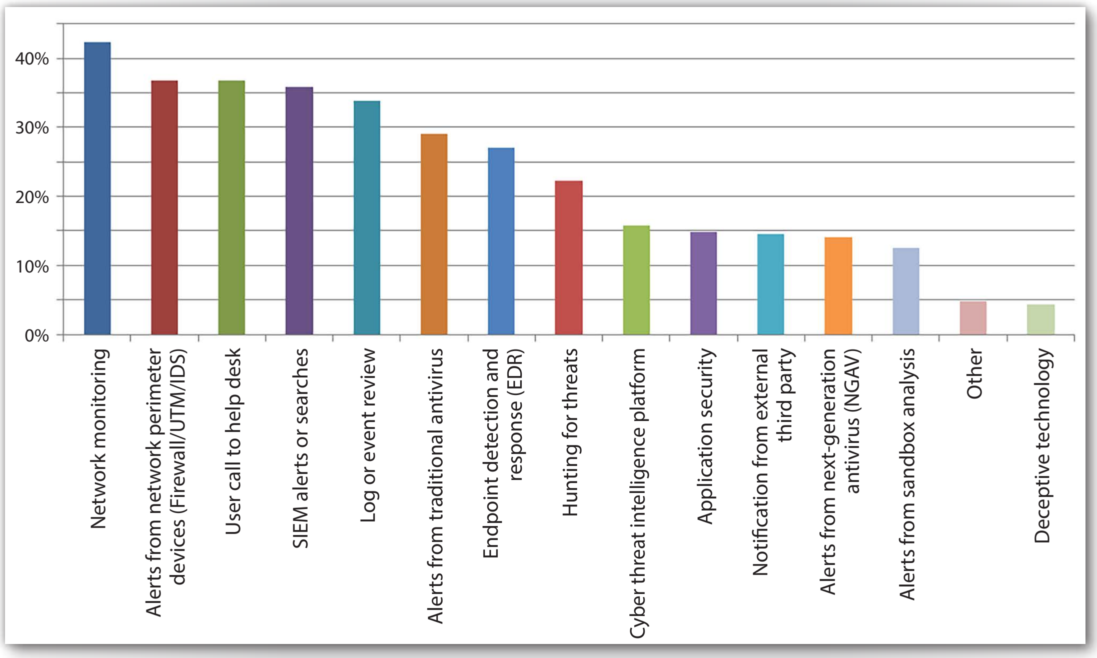

Figure 5. Discovery of Significant Threats

Somewhat disconcerting is that calls from users are tied with perimeter alerts and endpoint tools for effective discovery, while traditional antivirus or EDR, are in sixth and seventh place behind log or event review, which are often called *offline discovery tools* (meaning log review is not the means to real-time event discovery).

Even so, 56% of organizations are reporting fewer than 10 calls a week to the help desk that need to be investigated as threats. Of these calls, which are investigated as potential threats, 79% turn out to be actual threats, indicating that the end user remains a highly tuned detection mechanism. The question, however, is: Why is the end user so good at detecting potential threats? Is it because the user realizes he or she has done something wrong, or is it because the user notices unexpected behavior? User action, then, is the most common means of threat introduction and also a top means of identifying when "something's wrong" with the endpoints the users are operating. Despite the contributions end users make, overreliance on them to detect threats is a tenuous position to be in.

Many identified threats turn out to be false positives, as illustrated in Figure 6. We need to minimize false positives that take up valuable time and resources, but we mustn't lose sight of the fact that threats to get into the system and that nuisance false positives may mask or distract security personnel from responding to more insidious threats in our systems.

40%

of respondents reported that 11% or more of all identified threats they follow up on turned out to be false positives

How many threats that you followed up on could be considered "false positives" that don't apply to your organization?

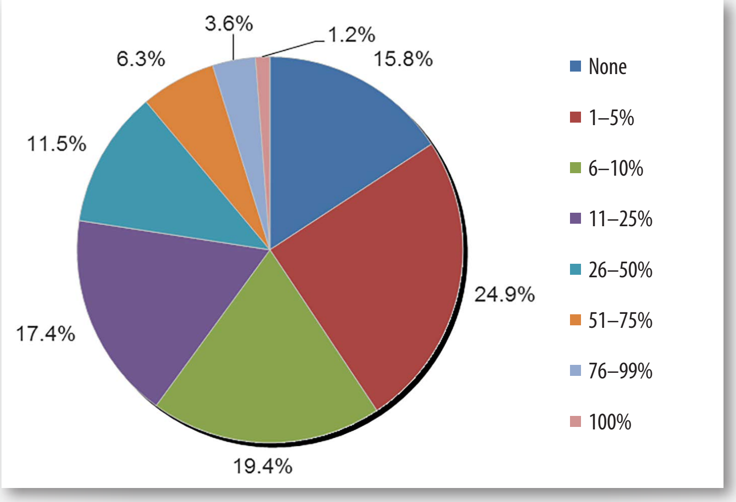

Figure 6. Threats and False Positives

Remediating Threats

Almost 72% of organizations discover threats within 24 hours of introduction, and 63% remediate within 24 hours of discovery. Frequency of remediation processes aid in reducing response times because staff are familiar with them. An additional 36% of respondents remediate weekly and 18% daily, as illustrated in Figure 7.

How often are you remediating impacted systems?

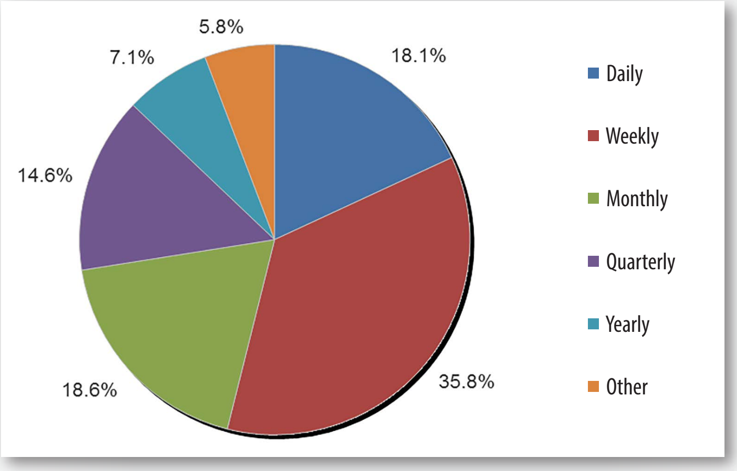

Figure 7. Frequency of Remediation

Without effective use of automation to not only better categorize threats, but also aid remediation, this may represent a continuous stream of work taking resources away from core business functions, especially if the threats turn out to be nuisances or false positives.

Determining Root Cause and Measuring Impact

Knowing how the threat happens is half the battle. And, although threats are getting in, 73% of respondents have been able to identify the root cause of the threats affecting their organizations. See Figure 8.

Were you able to determine the root cause of your incident(s)?

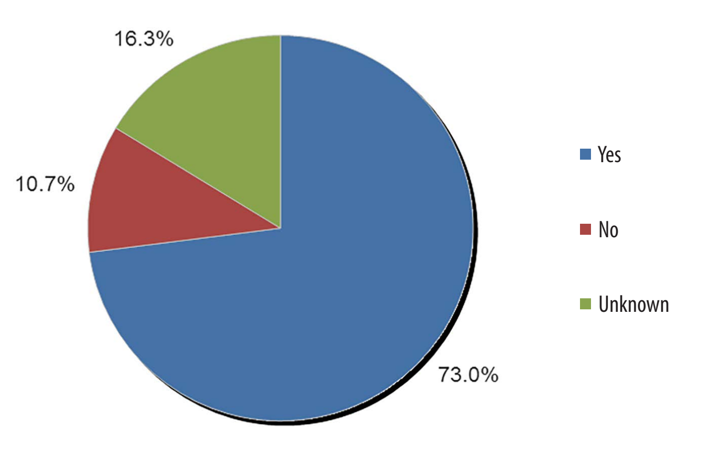

Figure 8. Ability to Determine Root Cause

For those threats that resulted in incidents, organizations measured the significance of the incidents based on their overall impact in terms of availability, cost to respond and recover, loss of sensitive data, and reputational damage, as shown in Figure 9 on the next page.

What were the top three reasons you consider this incident to be the most significant?
Please rank your top three reasons in order of impact, with "First" being the most significant.

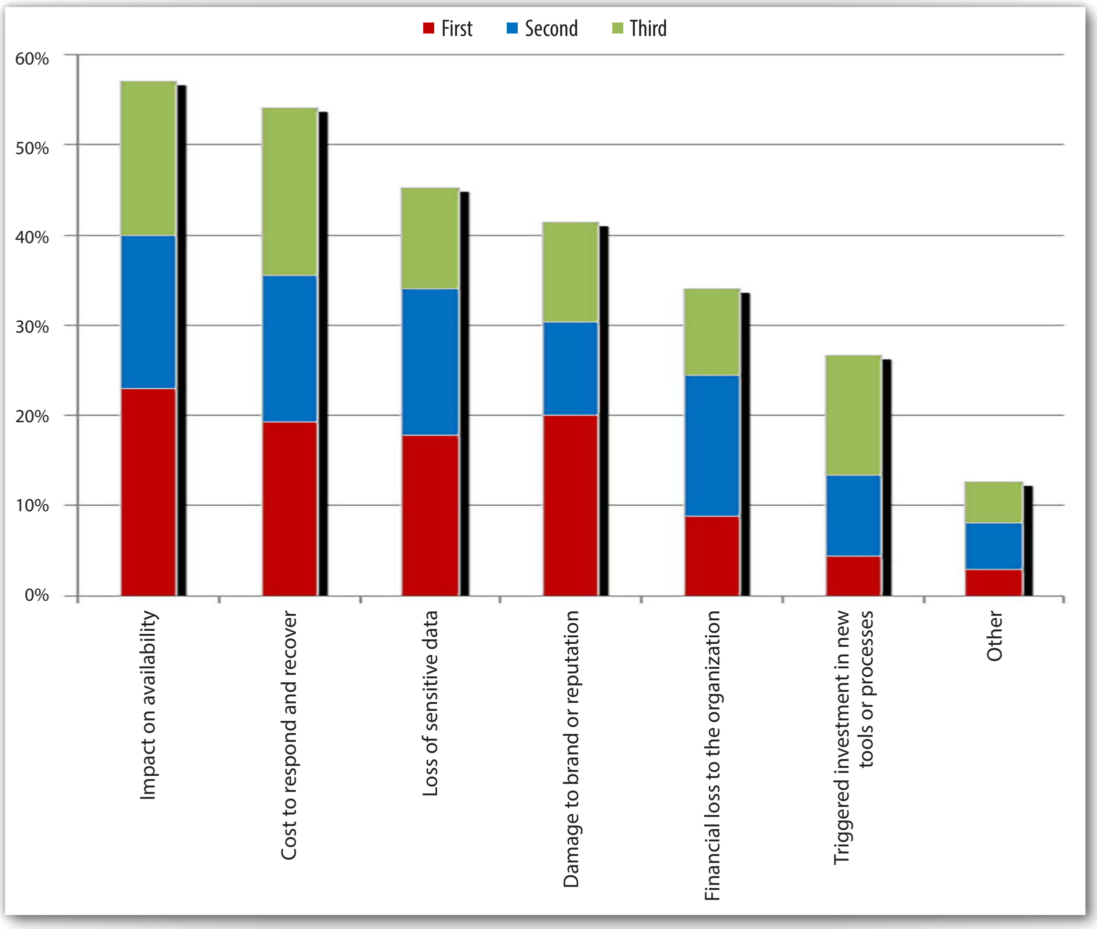

Figure 9. Reasons Incidents Are Considered Significant

The most significant reasons, represented by the red bar in Figure 9, indicate that availability and reputational damage are the top two factors that affect impact, followed by costs to recover and loss of sensitive data. Direct financial losses to the organization (for example, a direct ACH transfer) were rated as having a much lower measure of significance. Write-in responses in the "other" category pointed to lost time for workers/analysts/responders. One even pointed to patient safety as its measurement. Organizations should leverage the OWASP Risk Rating Methodology[8] or NIST Special Publication 800-30[9] to establish a method for measuring threat impact—which includes organization, mission, business and information system factors—to provide a more consistent measurement approach.

[8] www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[9] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Tools and Services to Scope Events

To determine the severity of their events, organizations are primarily scouring their logs, utilizing incident response and forensics tools, and relying on their SIEM systems. See Figure 10.

What tools or services do you find most helpful in accurately determining the scope of these events? ***Please select those that most apply.***

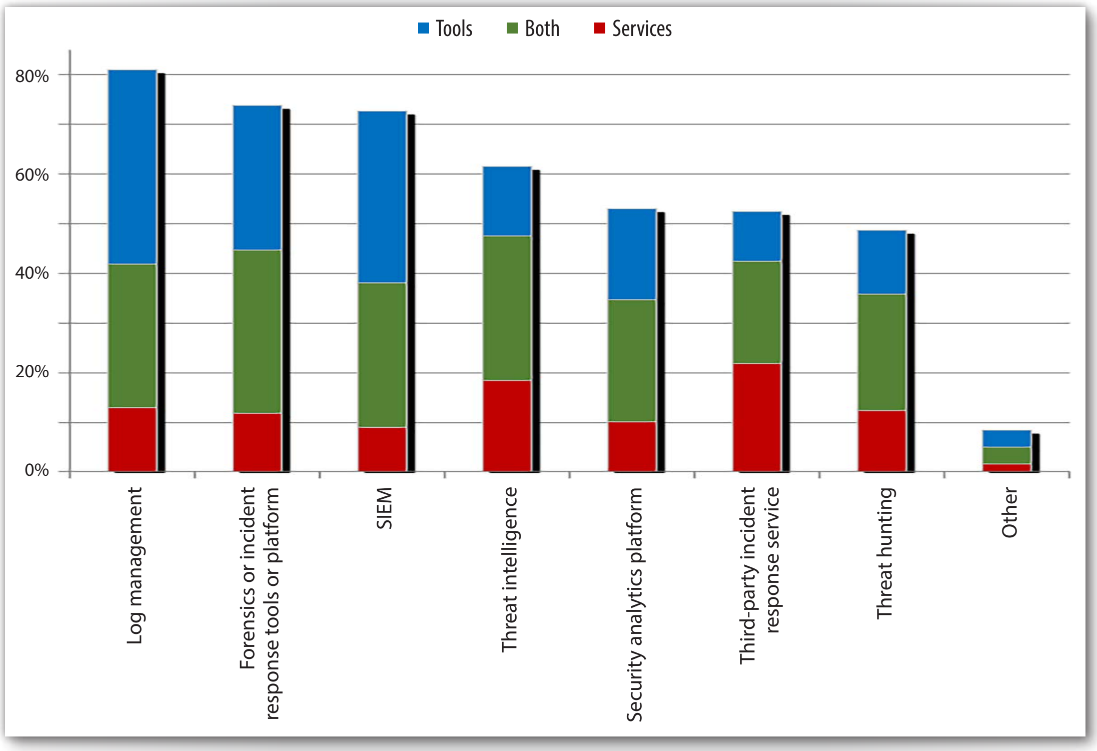

Figure 10. Tools and Services to Determine Scope of Events

Note that the near-equal mix of tools and services utilized for these capabilities. In fact, if we combine the red and blue bars, more organizations are using services than are utilizing just the tools to accomplish these tasks.

Tools for Detection

Services don't weigh as heavily in the detection arena, where the best threat detection tools start with endpoint security, followed by the IDS/IPS/UTM and the SIEM. Because the endpoint is the principal entry point, there is good alignment here. Support from network detection and monitoring tools gives staff visibility into actions that happen on the endpoint as well. See Figure 11.

What tools or services do you find most helpful in accurately detecting threats before they take a foothold in your enterprise? ***Please select those that most apply.***

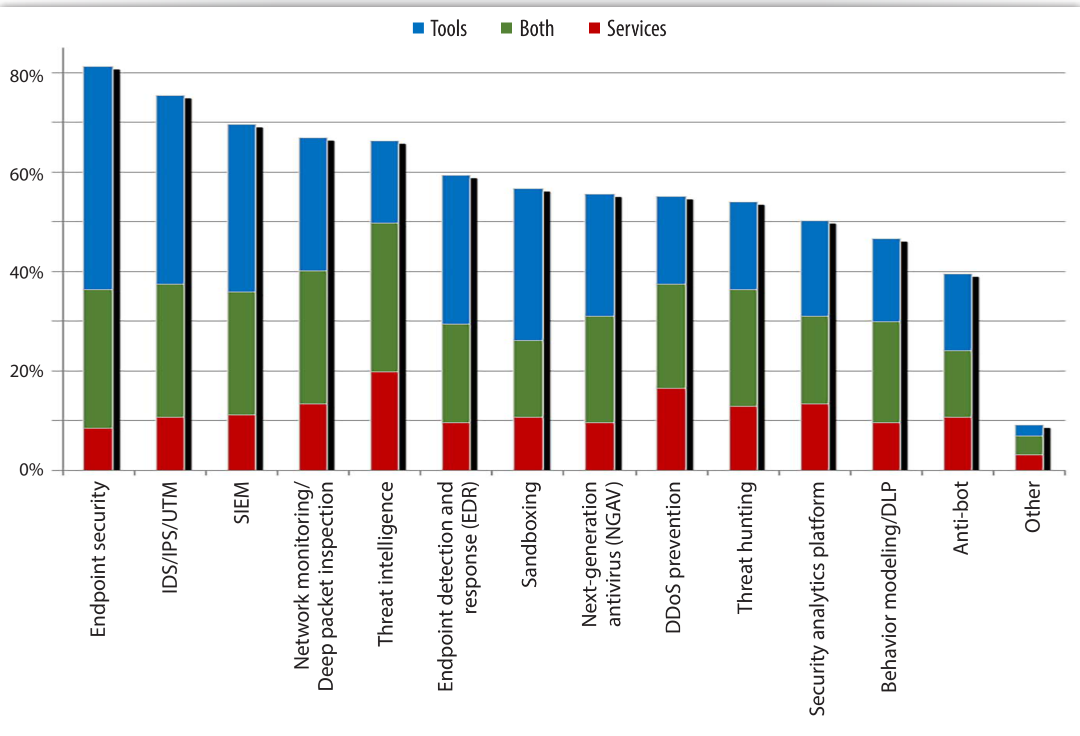

Figure 11. Tools and Services to Detect Threats

Respondents are utilizing these capabilities mostly in a near-equal mix of tools (blue bar) and layered tools and services (green bar), based on results of this question, where respondents were able to select all answers that apply. Services alone are used less frequently. Threat intelligence plays a lesser role in preventing impactful threats than it did in our 2016 survey, dropping from fourth to fifth, while behavior monitoring is taking a lesser role, moving from seventh to eleventh. The big change was the increased use of SIEM tools (from 60% in 2016 to 70% in 2017), supporting the need for automation over manual mechanisms of detection and response.

Remediation

For survey respondents, remediation of threats, in most cases, took a little longer than discovery. Yet, their remediation efforts are impressive: 63% of respondents were able to remediate within 24 hours. See Figure 12.

On average, how much time do you estimate it took to discover the threats that actually became incidents? How long was it from discovery until you considered remediation complete? ***Please check both columns as they apply.***

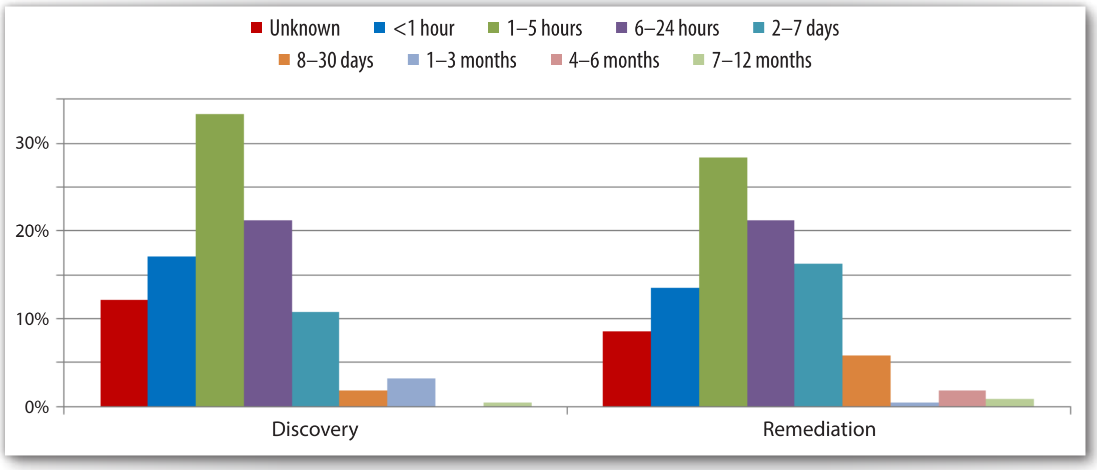

Figure 12. Time to Discovery and Remediation[10]

That is pretty amazing, so we asked how they were remediating.

Leveraging the most effective means for remediation is key to the short recovery time. The most effective methods are: Reimaging or restoring compromised machines from a gold baseline image, isolating infected machines from the network while remediation is performed, and shutting down the system and taking it offline. Table 2 (on the next page) provides a snapshot of responses.

[10] An additional 0.5% also took more than a year to remediate. It is not shown because the percentage is so small, and no respondents took more than a year to discover the threat.

TAKEAWAY

The most effective means to remediate affected devices are reimaging or restoring with a gold baseline image, isolating infected machines while they are remediated, and shutting down systems and taking them offline.

Table 2. Effective Means for Remediation

Answer Options	Very Effective	Effective	Sum of Both
Reimage/Restore compromised machines from gold baseline image	51.4%	26.1%	77.5%
Isolate infected machines from the network while remediation is performed	45.4%	33.0%	78.4%
Shut down system and take it offline	42.7%	26.1%	68.8%
Quarantine affected hosts	36.7%	32.1%	68.8%
Block command and control to malicious IP addresses	32.6%	33.0%	65.6%
Update policies and rules based on IOC findings and lessons learned	26.1%	31.7%	57.8%
Remove rogue files	25.2%	33.5%	58.7%
Identify similar systems that are affected	21.6%	36.2%	57.8%
Kill rogue processes	17.4%	32.6%	50.0%
Remove file and registry keys related to the compromise without rebuilding or reinstalling the entire machine	16.1%	27.1%	43.1%
Reboot system to recovery media	14.2%	24.3%	38.5%
Boot from removable media and repair system remotely	14.2%	22.0%	36.2%
Remotely deploy custom content or signatures from security vendor	12.8%	31.7%	44.5%
Other	5.5%	4.6%	10.1%

Organizations have figured out what works best and worst. Least effective mechanisms include removing files and registry keys without reinstall/reimage, booting from removable media and attempting a remote repair, killing rogue processes, and using recovery media. As attractive as a surgical fix is, too often a threat, once discovered, has changed enough that removing the known-bad elements is not sufficient to eradicate it, so reimaging is the most effective means. However, this can often be a manual, time-consuming process. So the best situation is to detect the malicious processes before they become embedded in the machine—or at least to prevent their spread to other machines to reduce the amount of reimaging (and the associated work downtime) required.

Where Next?

We know the challenges organizations face in identifying threats, responding to incidents and remediating systems. But knowing isn't enough. We need to take action.

Improvements Needed

When asked what could be done to prevent threats from entering the organization, the message that came through was a call for needed human and tool improvements, both for end users and IT staff. In the survey, 67% told us users need training to be more aware, and 42% called out the need to improve operational practices, including patching, as illustrated in Figure 13.

What could your organization have done better to prevent the threat?

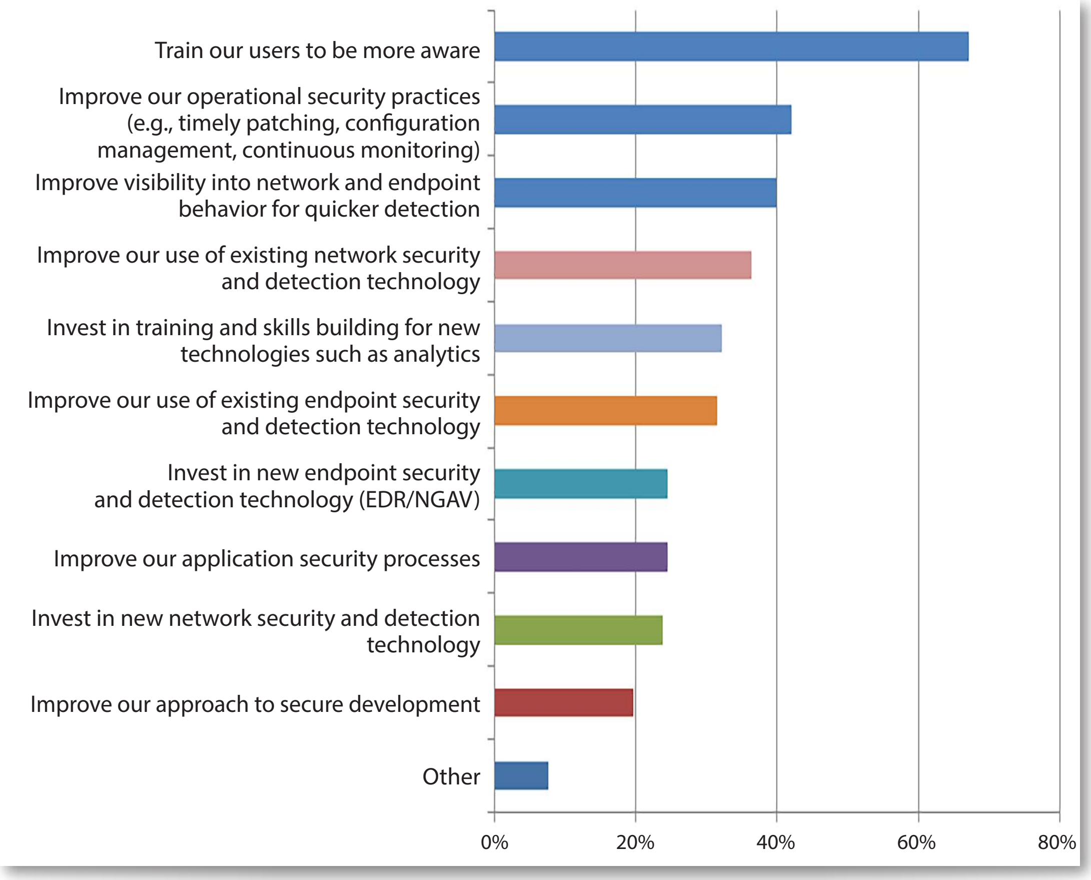

Figure 13. Improvements Needed

The need to improve visibility into endpoint behavior was also selected by 40% of respondents. This may be a call to look into new and improved EDR capabilities that, in response to a previous question, are not among the leading detection technologies in use. The more they get used, perhaps the more effective they will become. IT staff also needs skill and process enhancement, as well as new items in their toolkit to help make sense of all their threat data and to be ready for new technologies, which 32% selected.

Overcoming Obstacles

Lack of skilled resources holds back protection efforts to the point that the IT staff feel hamstrung by their tools. They report they still have trouble filtering out false positives, distinguishing real, high-impact threats they should respond to, and collecting the right threat data to act appropriately. Beneath all that was a strong need for either skills or budget to implement needed threat protection solutions. See Figure 14.

What challenges do you face in protecting against threats in your enterprise?
Select all that apply.

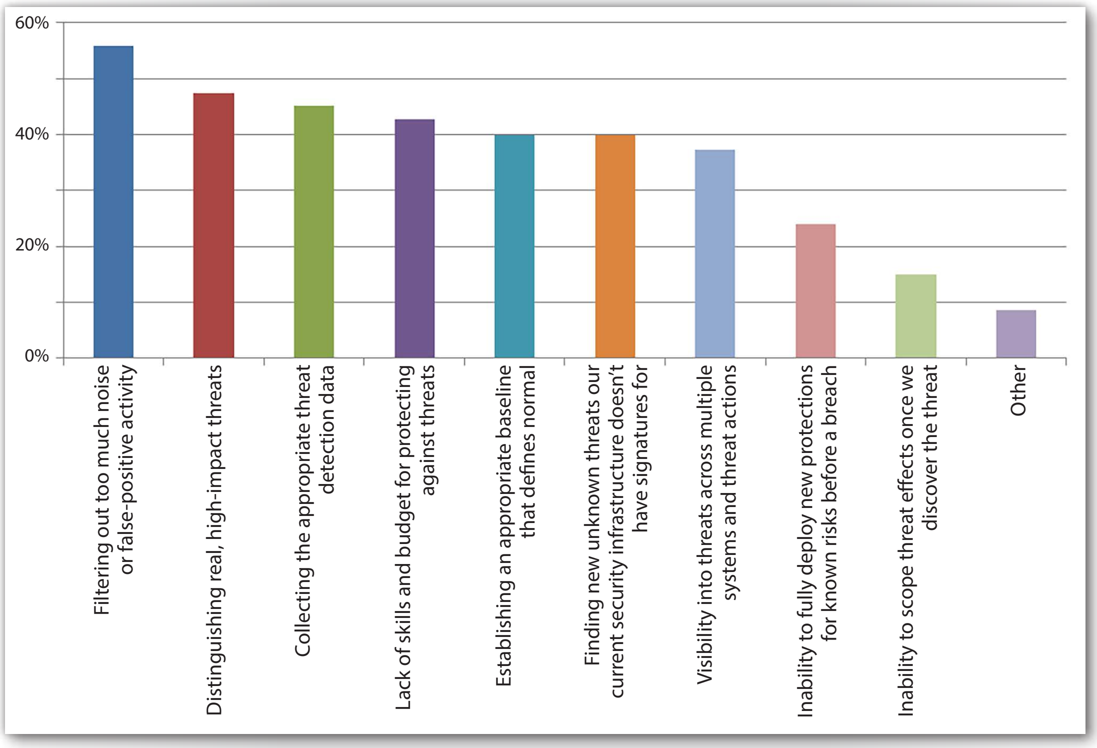

Figure 14. Challenges to Threat Protection

This result is somewhat different from 2016, where detecting unknown or zero-day threats and lack of skills and budget were the top challenges for the enterprise, at 60% and 56%, respectively. These areas appear to have improved somewhat, but the focus has shifted to data collection, filtering and correlation, which can help offset skills shortfalls.

Overcoming today's challenges will take a combination of approaches. Outsourcing is one avenue worth exploring, as managed detection and response services are gaining traction. These services can help extend security teams with the experience to overcome today's challenges and help protect network assets.

Leveraging the CIS Critical Security Controls[11] is also a solid approach to focus and prioritize these efforts to maximize the return, which is critical when skills and budget are challenges. Tools and automation are key to implementing these controls, as it is no longer practical to simply rely on staff in today's environment of rapidly changing threats. Start with a full hardware and software inventory (Controls 1 and 2), as well as verified secure configurations (Control 3), so staff can more easily identify and respond to introduced threats that may otherwise not be noticed.

Detecting changes and events requires continuous monitoring, vulnerability assessment and remediation (Control 4). Malware defenses (Control 8), as well as having system logs that are collected, analyzed and correlated (Control 6), can also be leveraged to change the skills/staffing mix needed for survival.

Organizations have identified activities intended to address many of these concerns. Improvements in operational security practices, training staff in new skills and improvements to network security all align with implementing the CIS Critical Controls. See Figure 15.

In the next 18 months, in what area do you intend to make a major investment to protect, detect and respond to threats in your environment?

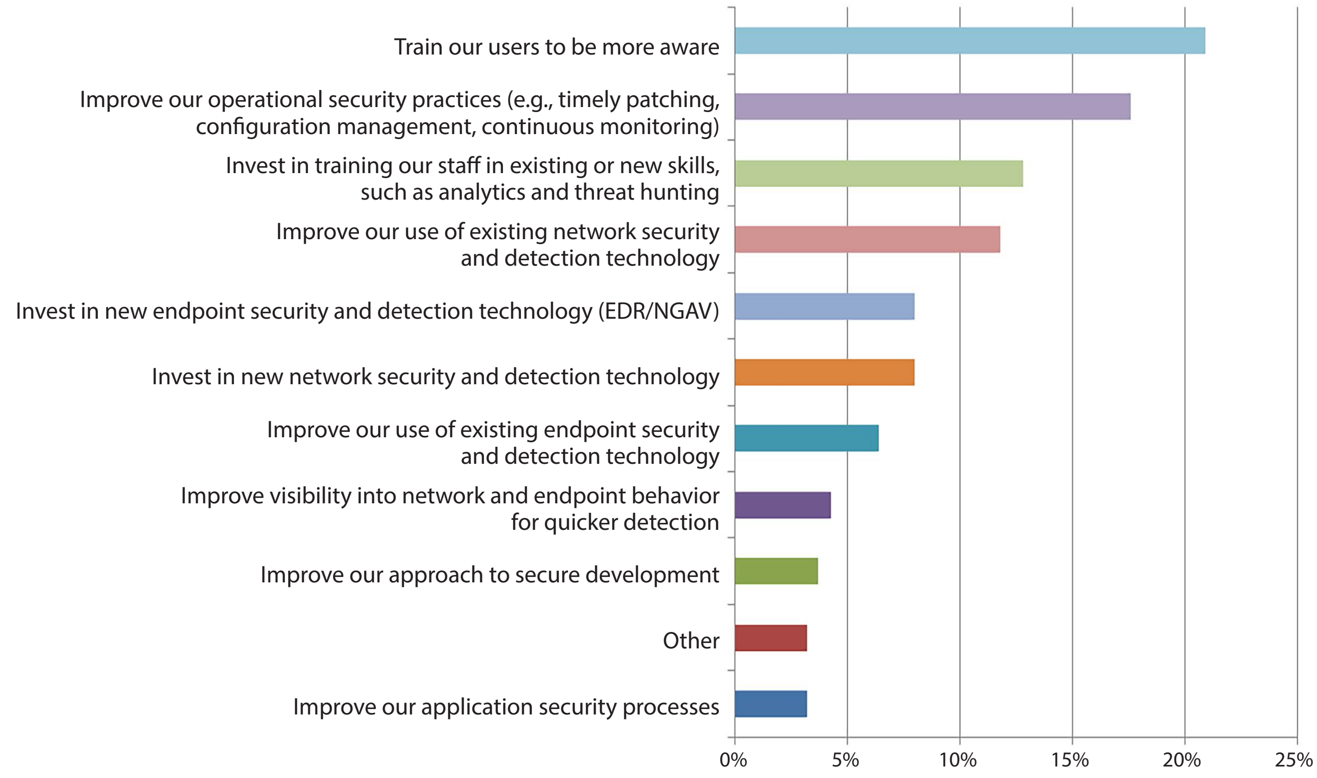

Figure 15. Future Investments

[11] www.cisecurity.org/controls

Try as we might to improve the technical capabilities, 21% of respondents state their organizations are focusing on user education as their primary investment to protect their environment. It is time to take user training to the next level. User training has to be commensurate with the threats our adversaries are throwing at us. Measure that training effectiveness with an eye to user success, not achievement of absolute success. Not only do we need to educate users, but as 42% of respondents indicate, we also need to invest in better operational security. Unfortunately, only 18% put their investments in this area. In addition to these areas, staff training on existing and new skills such as analytics and threat hunting, and improved leveraging of existing network security and detection mechanisms, targeted by 13% and 12%, respectively, for investment in the coming 18 months, are key to staying abreast of the changing threat landscape.

Conclusions

If you really want to stay awake at night, ponder whether the threats that affect organizations today are the finished product, or simply a trial balloon for the next wave of layered (and often malware-less) threats to come at your organization.

There are not a lot of zero-day threats leveraging new threat vectors. Zero-day exploits are still largely running parallel to the same vulnerabilities they've always exploited, while DDoS and ransomware attacks are becoming more damaging than ever. Therefore, threats continue to enter the system, and organizations are still falling victim. This should raise some questions: Does that mean there is an acceptable level of compromise? Or does this mean we're protecting the wrong things? Are we looking in the wrong direction? Because end user systems are the most targeted, reported organizational priorities suggest they are putting their efforts in the right places but are, perhaps, placing too much emphasis on user training when they should be demanding more automated tools, visibility into unknown threats and even into the threat posture of the devices at risk. Seek to bridge gaps in IT staff capabilities with training, tools and external expertise where appropriate.

While there is no such thing as perfect security, the end of Moore's law[12] does not signal a reduction in the pace of new potentially vulnerable information technology. Quite the contrary, Internet of Things demand is accelerating the number of vulnerable devices, not only in the home but also in the workplace,[13] meaning that the need to think outside the current protection framework is more important than ever.

[12] https://arstechnica.com/information-technology/2016/02/moores-law-really-is-dead-this-time/

[13] http://www.zdnet.com/article/internet-of-things-hyper-growth-so-many-things-so-little-time-to-protect-ourselves/

About the Author

Lee Neely, a SANS mentor instructor, teaches cyber security courses for SANS. He worked with the SANS SCORE (Security Consensus Operational Readiness Evaluation) project to develop the iOS Step-by-Step Configuration Guide, as well as the Mobile Device Configuration Checklist included in the SEC575 course. Lee holds the GMOB, GPEN, GWAPT, GAWN, CISSP, CISA, CISM and CRISC certifications. At the Lawrence Livermore National Laboratory (LLNL), Lee leads LLNL's cyber security new technology group, working to develop secure implementations of new technology, including developing the secure configurations, risk assessments and policy updates required for its corporate and bring-your-own-device mobile devices.

Sponsors

SANS would like to thank this survey's sponsors:

CYLANCE

FireEye®

McAfee™
Together is power.

Qualys®
Continuous Security

Last Updated: August 19th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Tampa-Clearwater 2019	**Clearwater, FLUS**	**Aug 25, 2019 - Aug 30, 2019**	**Live Event**
SANS Copenhagen August 2019	**Copenhagen, DK**	**Aug 26, 2019 - Aug 31, 2019**	**Live Event**
SANS Philippines 2019	**Manila, PH**	**Sep 02, 2019 - Sep 07, 2019**	**Live Event**
SANS Munich September 2019	**Munich, DE**	**Sep 02, 2019 - Sep 07, 2019**	**Live Event**
SANS Brussels September 2019	**Brussels, BE**	**Sep 02, 2019 - Sep 07, 2019**	**Live Event**
SANS Canberra Spring 2019	**Canberra, AU**	**Sep 02, 2019 - Sep 21, 2019**	**Live Event**
SANS Network Security 2019	**Las Vegas, NVUS**	**Sep 09, 2019 - Sep 16, 2019**	**Live Event**
SANS Oslo September 2019	**Oslo, NO**	**Sep 09, 2019 - Sep 14, 2019**	**Live Event**
SANS Dubai September 2019	**Dubai, AE**	**Sep 14, 2019 - Sep 19, 2019**	**Live Event**
SANS Paris September 2019	**Paris, FR**	**Sep 16, 2019 - Sep 21, 2019**	**Live Event**
Oil & Gas Cybersecurity Summit & Training 2019	**Houston, TXUS**	**Sep 16, 2019 - Sep 22, 2019**	**Live Event**
SANS Rome September 2019	**Rome, IT**	**Sep 16, 2019 - Sep 21, 2019**	**Live Event**
SANS Raleigh 2019	**Raleigh, NCUS**	**Sep 16, 2019 - Sep 21, 2019**	**Live Event**
SANS Bahrain September 2019	**Manama, BH**	**Sep 21, 2019 - Sep 26, 2019**	**Live Event**
SANS San Francisco Fall 2019	**San Francisco, CAUS**	**Sep 23, 2019 - Sep 28, 2019**	**Live Event**
SANS London September 2019	**London, GB**	**Sep 23, 2019 - Sep 28, 2019**	**Live Event**
SANS Dallas Fall 2019	**Dallas, TXUS**	**Sep 23, 2019 - Sep 28, 2019**	**Live Event**
SANS Kuwait September 2019	**Salmiya, KW**	**Sep 28, 2019 - Oct 03, 2019**	**Live Event**
SANS Northern VA Fall- Reston 2019	**Reston, VAUS**	**Sep 30, 2019 - Oct 05, 2019**	**Live Event**
SANS Cardiff September 2019	**Cardiff, GB**	**Sep 30, 2019 - Oct 05, 2019**	**Live Event**
SANS Tokyo Autumn 2019	**Tokyo, JP**	**Sep 30, 2019 - Oct 12, 2019**	**Live Event**
SANS DFIR Europe Summit & Training 2019 - Prague Edition	**Prague, CZ**	**Sep 30, 2019 - Oct 06, 2019**	**Live Event**
Threat Hunting & Incident Response Summit & Training 2019	**New Orleans, LAUS**	**Sep 30, 2019 - Oct 07, 2019**	**Live Event**
SANS Riyadh October 2019	**Riyadh, SA**	**Oct 05, 2019 - Oct 10, 2019**	**Live Event**
SIEM Summit & Training 2019	**Chicago, ILUS**	**Oct 07, 2019 - Oct 14, 2019**	**Live Event**
SANS October Singapore 2019	**Singapore, SG**	**Oct 07, 2019 - Oct 26, 2019**	**Live Event**
SANS Lisbon October 2019	**Lisbon, PT**	**Oct 07, 2019 - Oct 12, 2019**	**Live Event**
SANS San Diego 2019	**San Diego, CAUS**	**Oct 07, 2019 - Oct 12, 2019**	**Live Event**
SANS Baltimore Fall 2019	**Baltimore, MDUS**	**Oct 07, 2019 - Oct 12, 2019**	**Live Event**
SANS Doha October 2019	**Doha, QA**	**Oct 12, 2019 - Oct 17, 2019**	**Live Event**
SANS Denver 2019	**Denver, COUS**	**Oct 14, 2019 - Oct 19, 2019**	**Live Event**
SANS Seattle Fall 2019	**Seattle, WAUS**	**Oct 14, 2019 - Oct 19, 2019**	**Live Event**
SANS New York City 2019	**OnlineNYUS**	**Aug 25, 2019 - Aug 30, 2019**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**