RESEARCH

Tripwire State of Cyber Hygiene Report

August 2018

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

When a high-profile cyberattack grabs the headlines, your first instinct may be to funnel resources into purchasing a shiny new tool to defend your organization. But often, that's not what's really needed.

Real-world breaches and security incidents prove over and over again that many of the most widespread issues still stem from a lack of basic cyber hygiene. Therefore, organizations can't overlook the fundamentals such as addressing known vulnerabilities, ensuring secure configuration, and monitoring systems for change.

You can start to build up cyber hygiene by following established best practices such as the Critical Security Controls, a prioritized set of steps maintained by The Center for Internet Security (CIS). There are 20 CIS Controls, but implementing just the top six establishes what CIS calls "cyber hygiene."

This report illustrates how organizations are implementing these top six controls, if at all. To gather this data, Tripwire partnered with Dimensional Research, sending a survey to independent sources of IT security professionals. The survey was completed by 306 participants in July 2018, all of whom are responsible for IT security at companies with more than 100 employees.

Key survey findings:

» **Incomplete visibility is common**
Many organizations still struggle to maintain the adequate visibility into their environments needed to address potential issues quickly. Results showed that organizations need to improve visibility into the devices and software on their networks, logs from critical systems, and configuration changes.

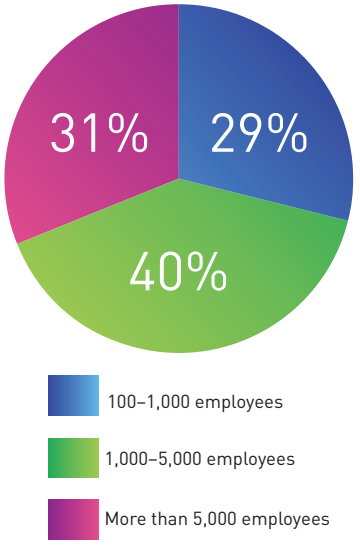
» **Vulnerability scans aren't as extensive as they should be**
Almost all participants use vulnerability scanning, but only half run comprehensive, authenticated scans. Only 59 percent are scanning weekly or more, as recommended by CIS.

» **Hardening benchmarks are a missed opportunity**
Sixty percent of participants are not using hardening benchmarks like CIS or DISA to establish a secure baseline. While many security teams implement good basic protections around administrative privileges, these low-hanging-fruit controls should be in place at more organizations.

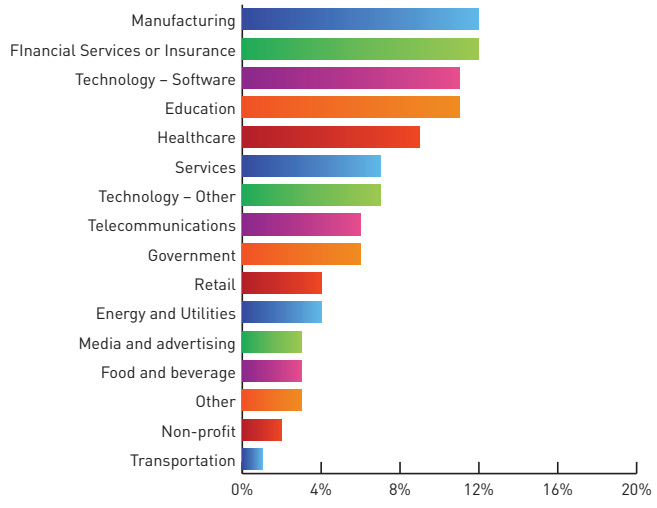
Demographics

A total of 306 qualified participants completed the survey. All participants had responsibility for IT security as a significant part of their job at organizations with more than 100 employees.

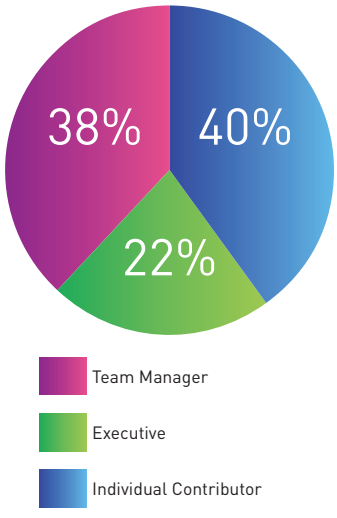
Company Size



Industry



Job Level



Control 1: Inventory and Control of Hardware Assets

CIS Control 1 advises organizations to keep an accurate network inventory. This provides visibility into devices that could pose security threats or that shouldn't be on your network at all.

Results:

» Few organizations can say they have inventory of all the devices on their network. Only 29 percent track more than 90 percent of devices, and a third track less than 70 percent. In large organizations, that leaves a significant amount of attack surface unaccounted for (Fig. 4).

» This year, more organizations say they're detecting new devices on their network within minutes (43 percent) than participants in a 2015 survey (32 percent). That still leaves a majority (57 percent) who take hours, weeks, months or longer. It should be every organization's goal to detect new devices within minutes, as that's all an attacker may need to inflict damage (Fig. 5).

» Teams are taking longer to address unauthorized devices than they did in 2015, evidenced by a decrease in "minutes" responses and an increase in "months" responses (Fig. 6).

You need to know your attack surface in order to protect your systems. While tracking each and every device is challenging in dynamic environments, a small percentage of untracked devices could be a significant chunk of the attack surface in a large organization. This control must be continually revisited as you mature your security operations.

Many of these requirements can be met with free tools and managed with simple spreadsheet software. But as your organization grows and implements more controls, these requirements become more complex and tightly integrated with the entire suite of CIS security controls.

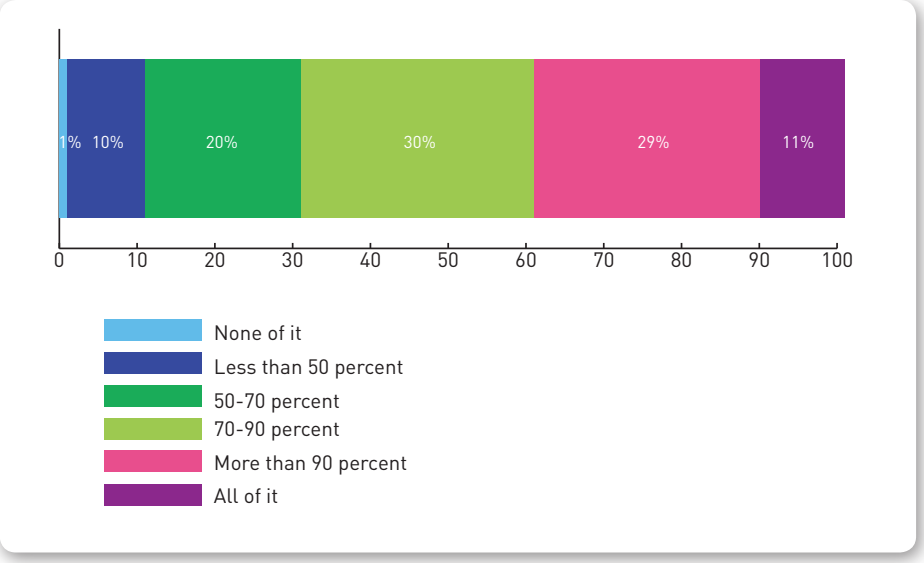


Fig. 4 Approximately how many of the devices connected to your organization's network do you have tracked in an asset inventory?

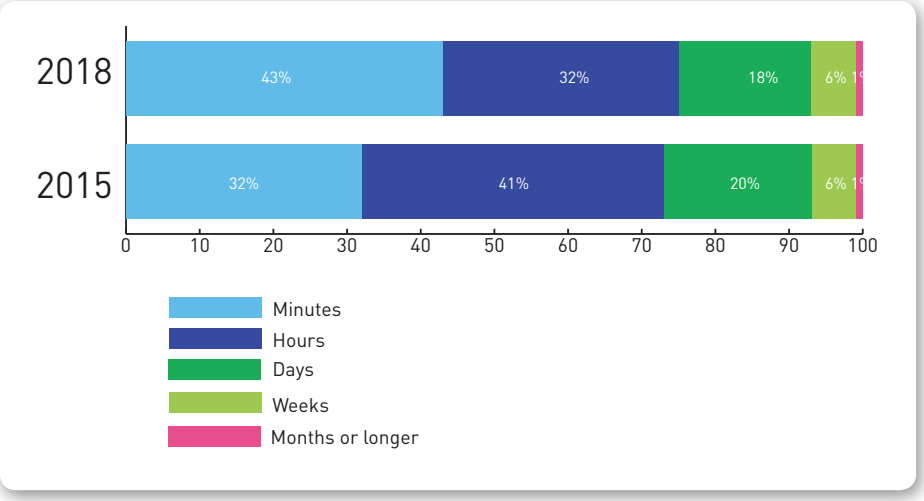


Fig. 5 How long does it take to detect new devices added to the organization's network?

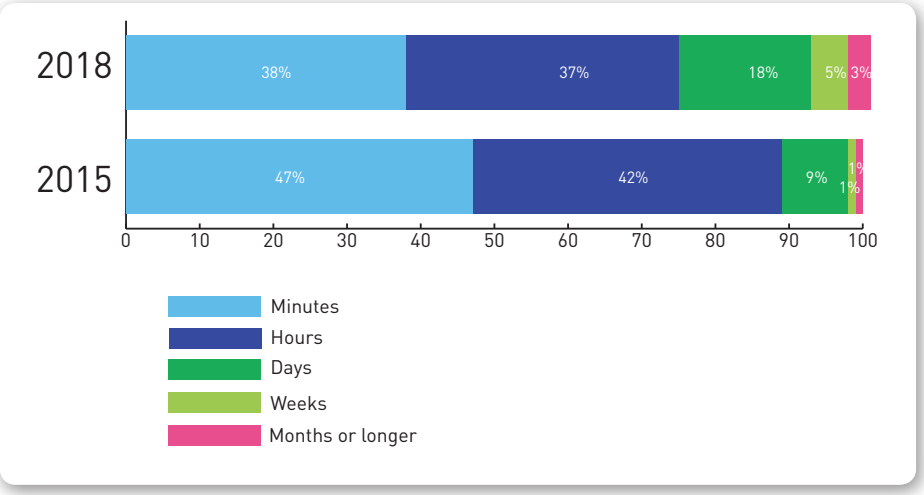


Fig. 6 How long does it take to isolate/remove an unauthorized device for your organization's network?

Control 2: Inventory and Control of Software Assets

In keeping with Control 1's hardware inventory, Control 2 focuses on inventorying software. By implementing this control, organizations can weed out malware and software that should not be running on their network.

Results:

» Organizations have an even harder time tracking software than hardware on their network. Only 21 percent track more 90 percent of their software, while 56 percent track less than 70 percent (Fig. 7).

» Along the same lines as hardware detection, organizations should aim to detect new software on the network within minutes. Less participants said they can detect unauthorized software within minutes this year (14 percent) than in 2015 (21 percent). More this year said it took weeks (12 percent) and months or longer (12 percent) (Fig. 8).

» Little more than a third (36%) are not using application whitelisting, leaving the door open for problematic software to be downloaded onto the network (Fig. 10).

Many of the tools organizations leverage to meet Control 1 also support Control 2. This being the case, there's no reason not to treat these two controls as one when you're developing your strategy to implement them.

Several of these requirements can be accomplished with open-source or built-in tools. That being said, as your organization grows, you will also outgrow the capabilities of these free tools. Software is much more dynamic than hardware and can therefore be harder to track.

Utilizing application whitelisting can be one of the most effective ways to satisfy these controls, but it can also be disruptive. Organizations interested in the benefits of whitelisting—without the disruption—should consider tools that do what's called "non-blocking" whitelisting.

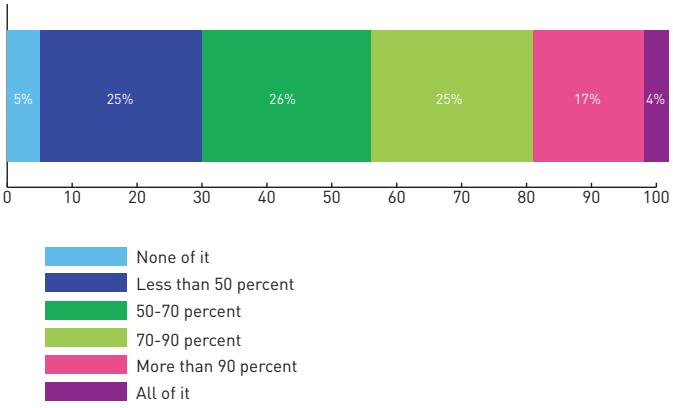


Fig. 7 Approximately how much of the software on your organization's network do you have tracked in an asset inventory?

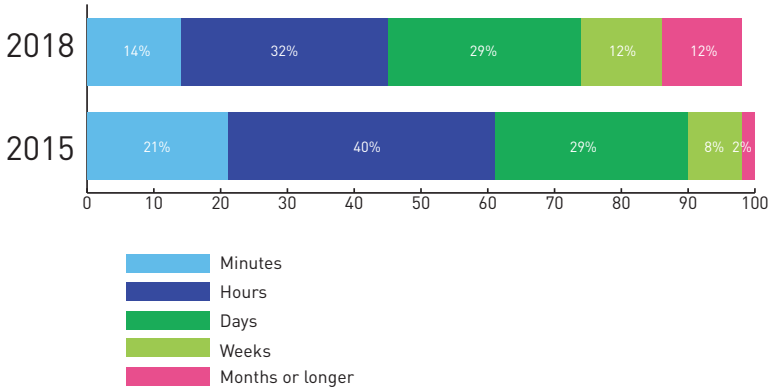


Fig. 8 How long does it take to detect unauthorized software added to the organization's network?

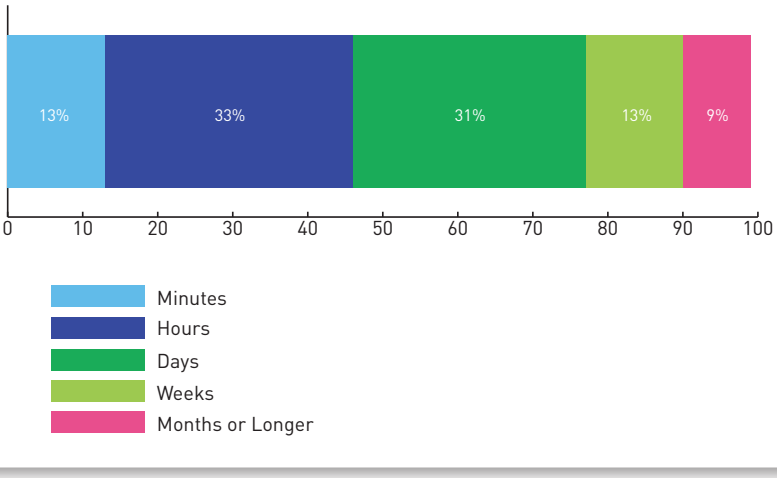


Fig. 9 How long does it take to address unauthorized software on your organization's network?

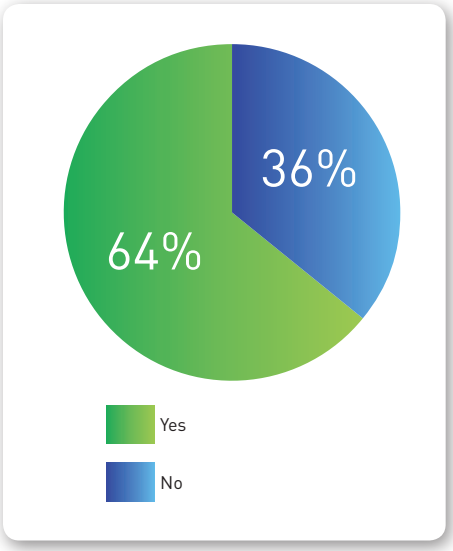


Fig. 10 Does your security program utilize application whitelisting?

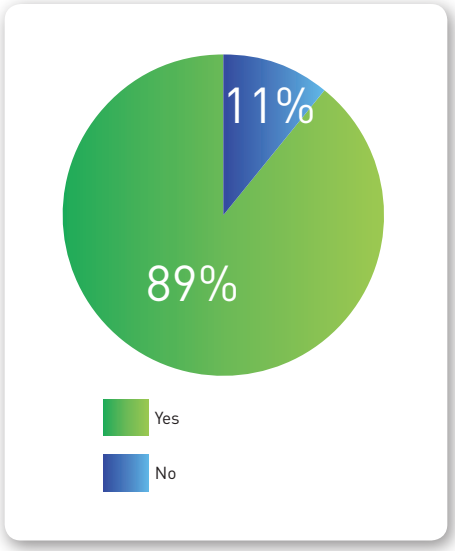


Fig. 11 Does your organization run vulnerability scans?

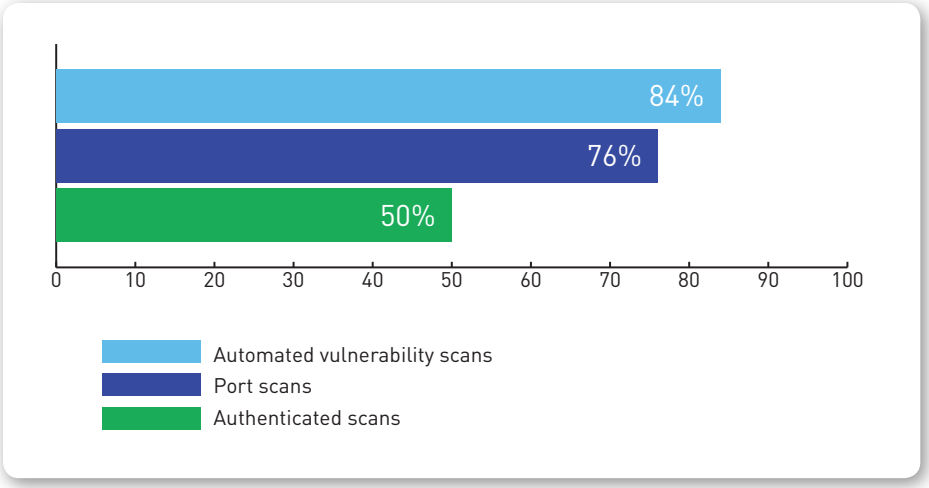


Fig. 12 What kind of vulnerability scanning do you do? Choose all that apply.

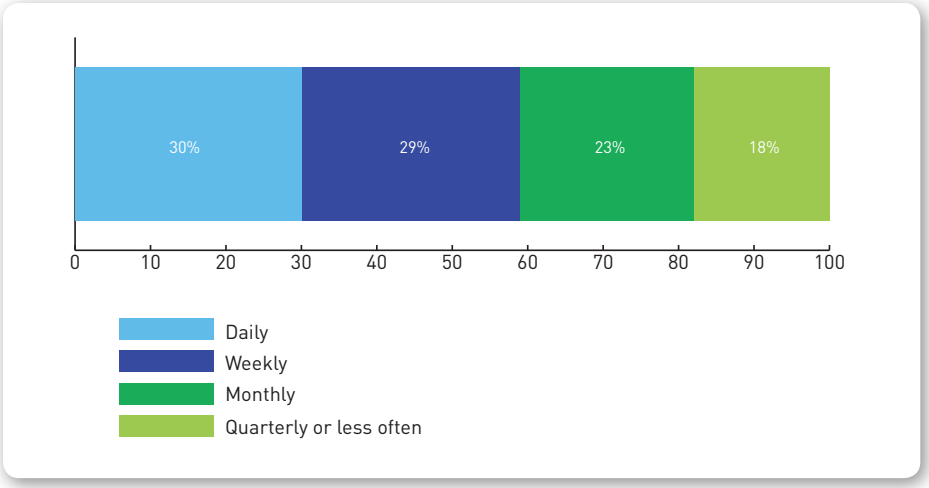


Fig. 13 How often do you run vulnerability scans?

Control 3: Continuous Vulnerability Management

High-impact security breaches often stem from known vulnerabilities. In this area of the report, we explore how organizations are assessing and addressing vulnerabilities in their environments.

» Almost all participants are running vulnerability scans. However, only 50 percent are running authenticated scans, which are the most comprehensive (Fig. 12).

» Forty-one percent of participants are running scans monthly, quarterly or less often—when weekly or more is recommended (Fig. 13).

» Most (56 percent) are able to deploy a patch within a week, but about a quarter are still taking about a month or longer (Fig. 14).

» Among organizations that have implemented DevOps, 46 percent aren't scanning for vulnerabilities throughout the continuous integration and deployment (CI/CD) pipeline (Fig. 15).

A robust, vulnerability management program powered by the correct tools will empower your organization to take control of its own security and manage risks presented by both internal and external threats. Utilizing remote and credentialed scans gives you a holistic view of your network that allows you to better understand threats before they become a problem. When you review and compare your results, you will quickly know what has changed and what risks those changes introduce. Vulnerability management programs, when properly implemented, expose a plethora of faults and flaws in even the most secure enterprises networks. Don't be alarmed; simply apply risk-ratings and break the work into smaller, more manageable portions.

Control 4: Controlled Use of Administrative Privileges

Attackers are going to go after administrative accounts. With admin access, there's no need to burn costly zero-days and create a bunch of noise in the environment. Know what the attackers are after so you can create appropriate controls and implement detection mechanisms. This section explores how well administrative privileges are managed and protected by organizations.

Results:

» Only 47 percent use dedicated workstations for administrative activities. It's recommended that tasks requiring administrative access be done on dedicated workstations that are segmented from the primary network and not to be allowed Internet access (Fig. 17).

» A third of organizations do not require changed default passwords, 41 percent still don't use multifactor authentication for accessing administrative accounts, and 43 percent do not require unique passwords for each system (Fig. 18).

Administrative credentials are as valuable than the data you're trying to protect. Organizations should provide the same level of care with them as with their most sensitive data.

Compliance frameworks and hardening benchmarks provide guidance on best practices for handling all employee credentials, not just those of administrators. Investigate how these best practices can be applied to your unique environment.

Make sure not to overlook common sense efforts like changing default passwords and using multi-factor authentication. If using passwords unique to each system, you may need a privileged identity management system.

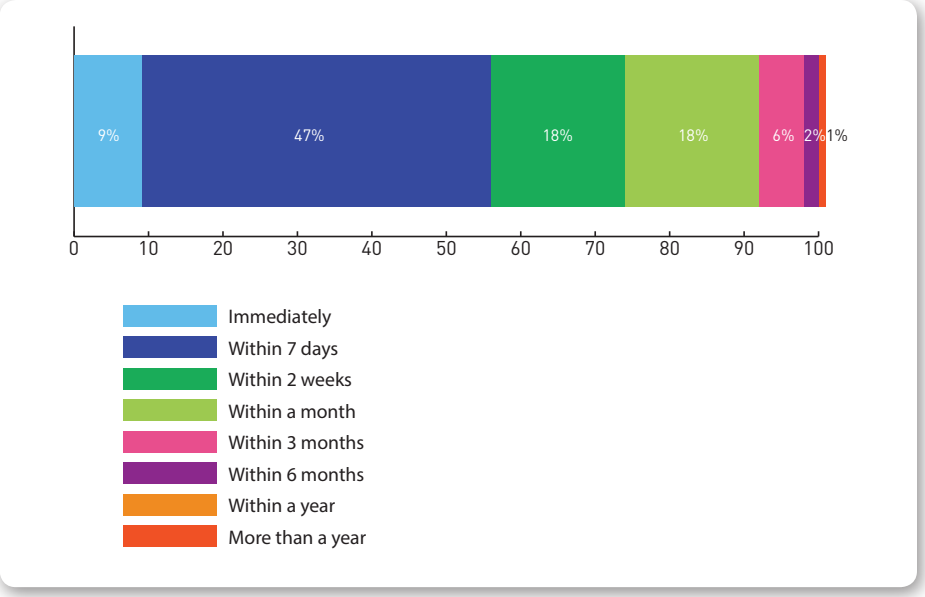


Fig. 14 In general, how long does it take to deploy a security patch in your environment?

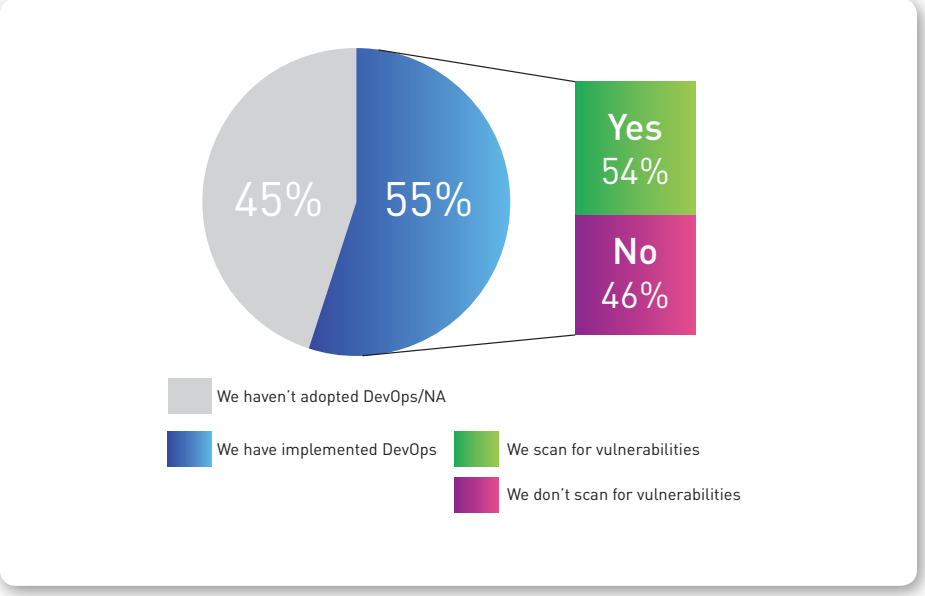


Fig. 15 If your organization has implemented DevOps, do you scan for vulnerabilities throughout the CI/CD (continuous integration/continuous deployment) pipeline?

Control 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Most software and operating systems are configured in an open and insecure state. Systems should be configured to a defined, ideal and secure state, following cybersecurity best practices and your organization's own policies.

Results:

» Only 40 percent have taken advantage of hardening benchmarks like CIS or DISA to establish a secure baseline (Fig. 19).

» More than a third (38 percent) still struggle to enforce configuration settings (Fig. 21).

» Only 18 percent are detecting configuration changes in minutes. Similar to the detection of new hardware and software on the network, detecting configuration changes ideally would not take hours or longer (Fig. 23).

Misconfigurations are the underlying reason for many successful breaches, and improper configuration changes can cause operational disruption. Just about every security framework and compliance regulation related to security calls for secure configuration management. Hardening benchmarks like CIS or DISA can be leveraged to establish secure configurations, and file integrity monitoring (FIM) tools can monitor configuration files and report on changes in real time.

Configuration management becomes increasingly difficult in complex technology environments consisting of numerous systems, asset owners and applications—all with differing configuration states and business requirements. Enterprises stand to benefit from technology that automates the assessment, monitoring, and management of configurations across all systems to ensure ongoing security and compliance.

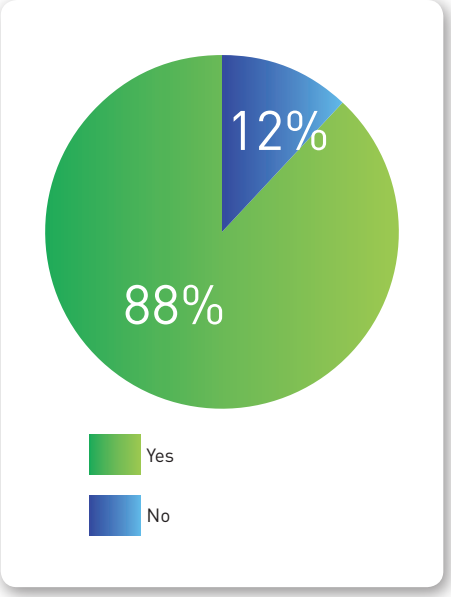


Fig. 16 Do you ensure use of dedicated administrative accounts for elevated activities?

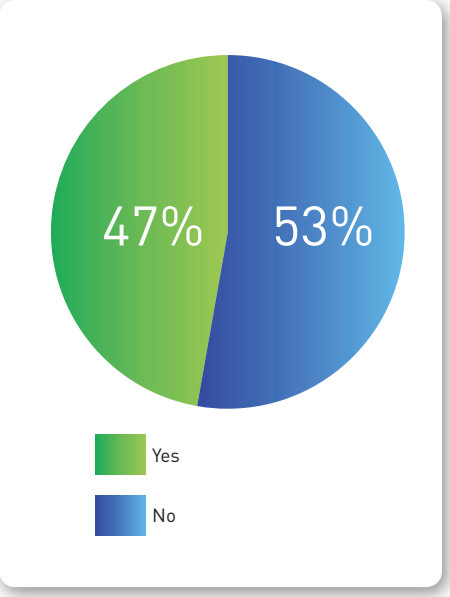


Fig. 17 Does your IT staff use dedicated workstations for all tasks requiring administrative access?

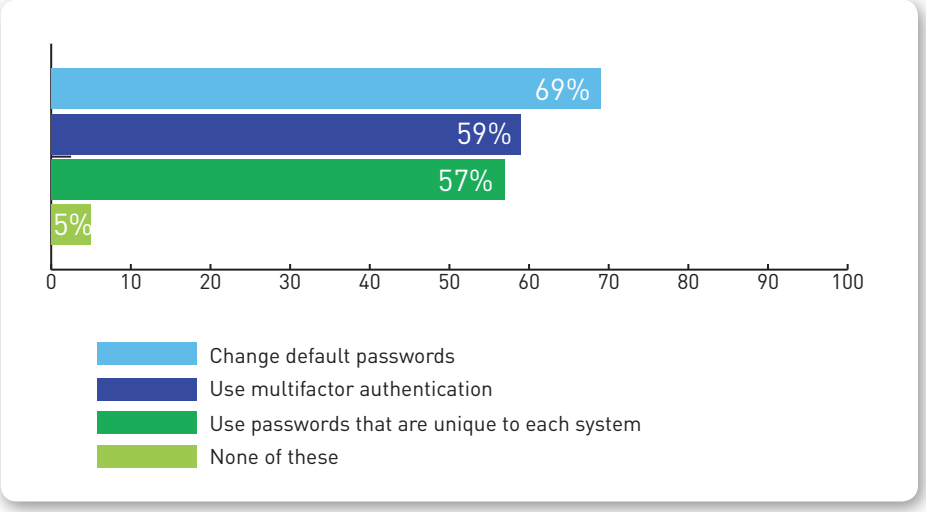


Fig. 18 Which of the following does your organization require in order to access administrative accounts? Choose all that apply.

CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs

Security logging and analysis can help IT teams determine the location of attackers, identify malicious software and track activities on victim machines.

Results:

» More than half (54 percent) of organizations are not collecting logs from critical systems into a central location. Centralized logging is conducive to effective event monitoring and analysis (Fig. 26).

» Logs should be used to identify abnormal activity on a daily basis, but 44 percent are only reviewing logs weekly, monthly, quarterly or less. Nine percent never review logs at all (Fig. 27).

» A quarter of participants said they are not efficient at all in log analysis, and 73 percent noted room for improvement (Fig. 28).

An attacker may create a ton of noise on an endpoint while leaving little trace on the network or vice-versa. You need to collect logs from as many systems as possible to get an accurate picture of what is going on. Both CIS and DISA hardening guides provide guidance on how to enable logging on endpoints as well as how to get it off to a centralized server. Ensure appropriate logs are being aggregated to a central log management system for analysis and review. This isn't necessarily every single log in your environment; you can use log aggregators to filter out the disinteresting events and only send "valuable" events up to a more expensive logging server or SIEM.

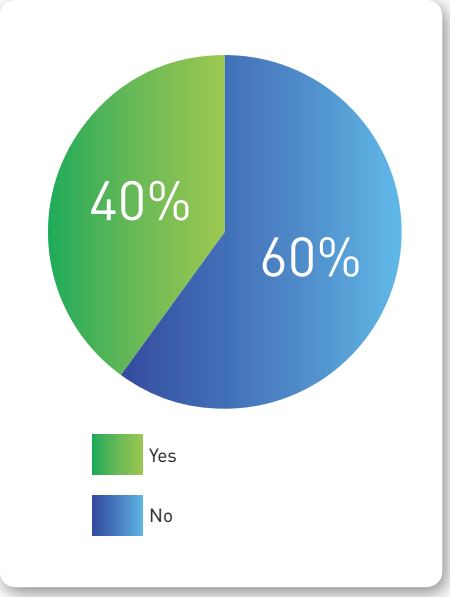


Fig. 19 Have you used hardening benchmarks (like CIS or DISA) to establish a secure baseline?

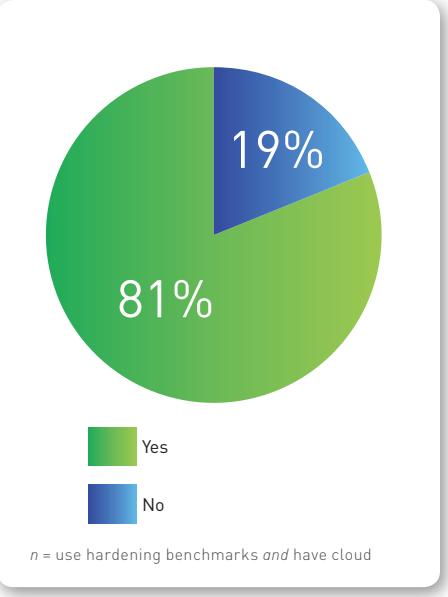


Fig. 20 Do you use hardening benchmarks (like CIS or DISA) in your cloud environments?

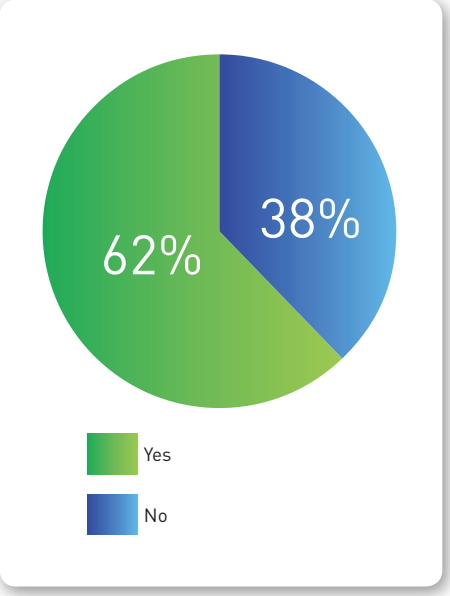


Fig. 21 Do you deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems?

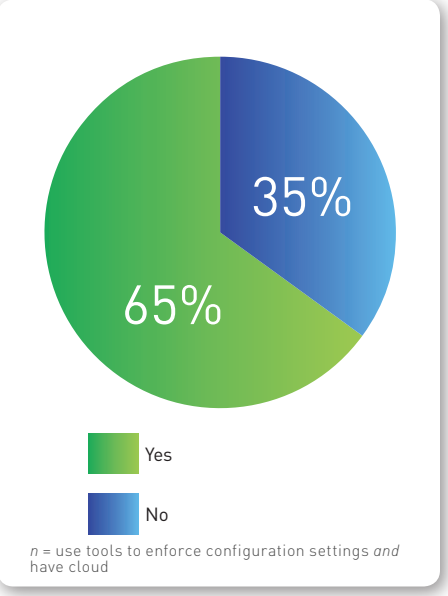


Fig. 22 Do you deploy tools that automatically enforce and redeploy configuration settings for your cloud environments?

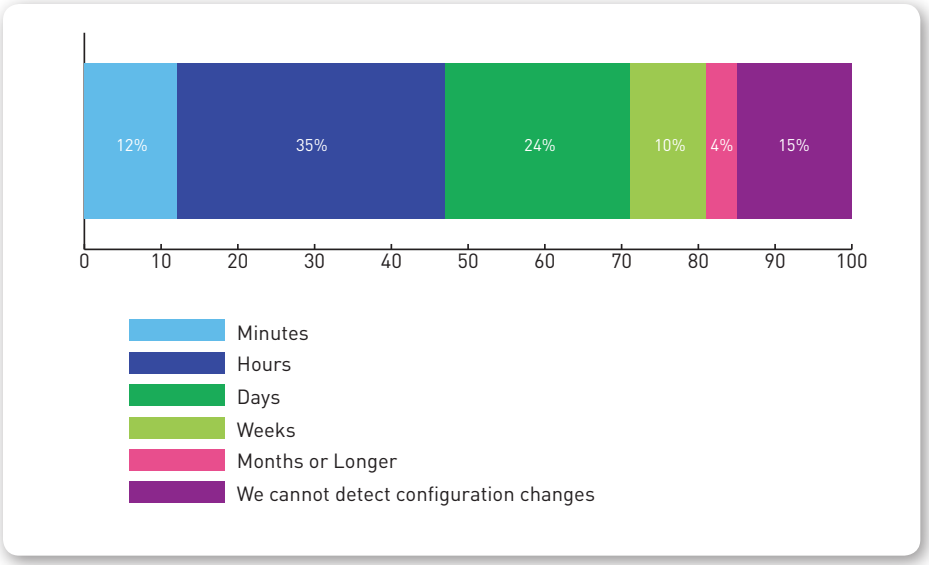


Fig. 23 About how long does it take to detect configuration changes to hardware and software on your organization's network? Choose the answer that most closely applies.

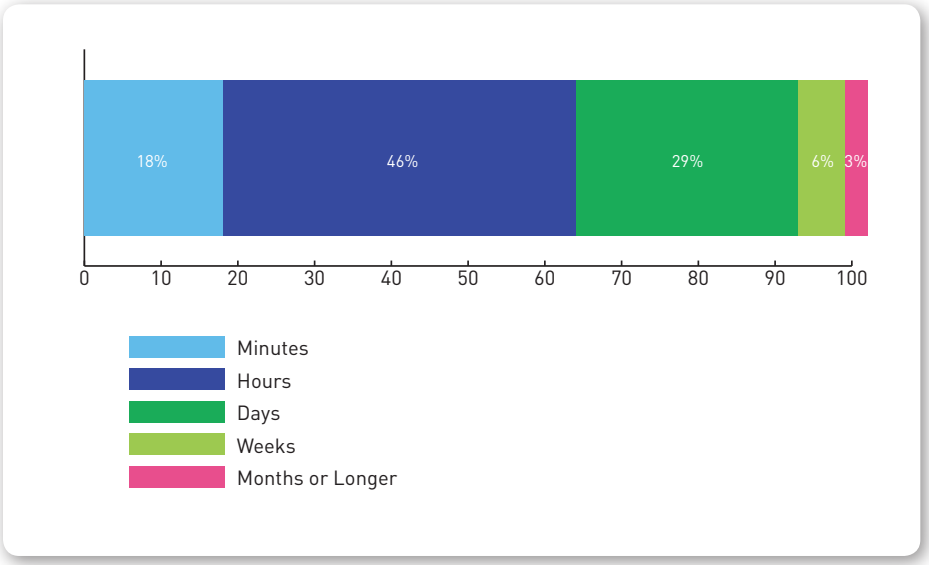


Fig. 24 How long does it take to remediate a configuration change?

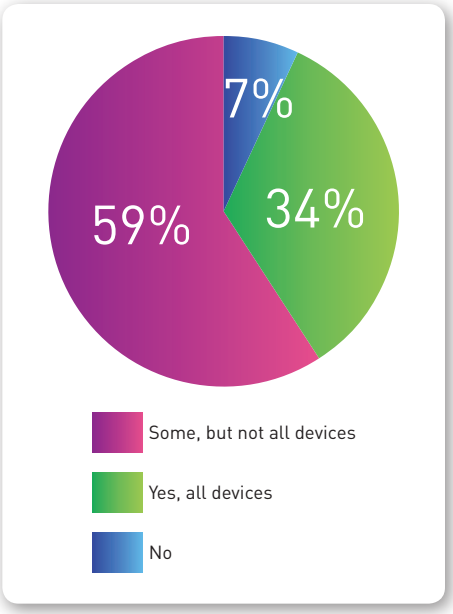


Fig. 25 Have you ensured that local logging has been enabled on all systems and networking devices?

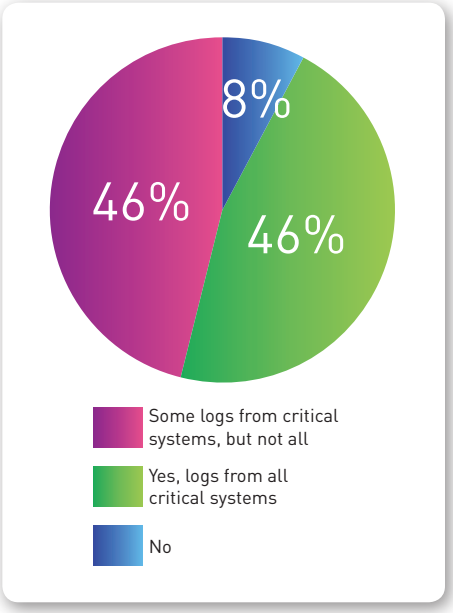


Fig. 26 Are you collecting logs from all critical systems into a central location?

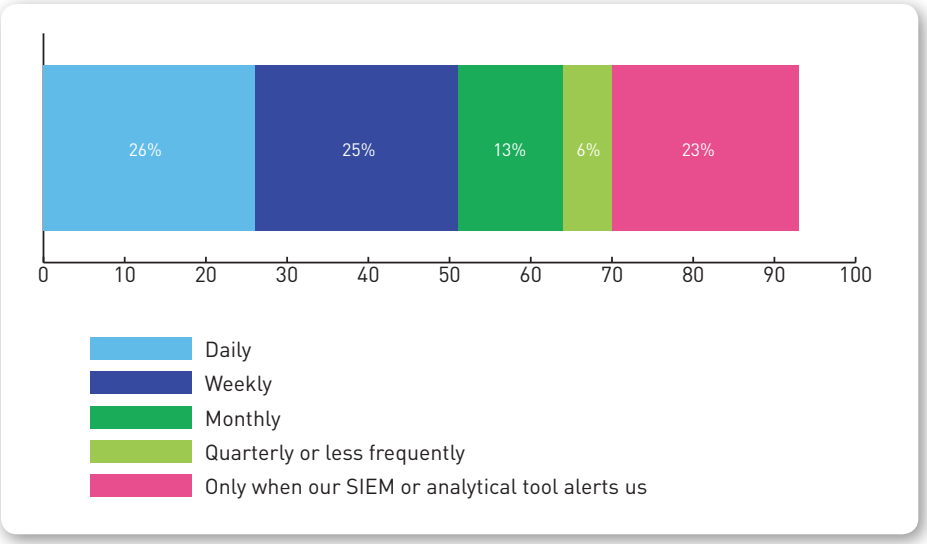


Fig. 27 How often do you review logs for anomalies or abnormal events?

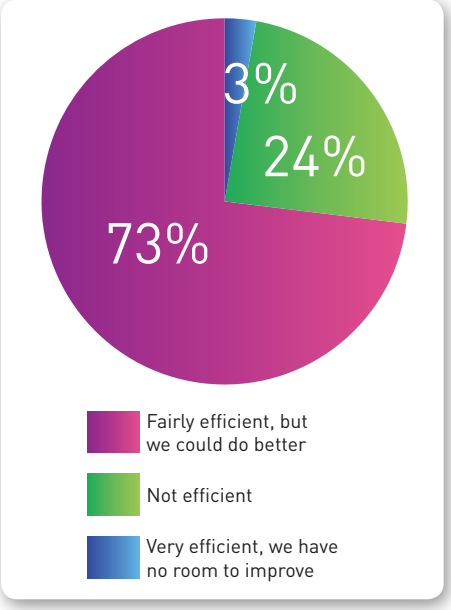


Fig. 28 How efficient is your organization at identifying actionable events and decreasing event noise?

Summary/Conclusion

There is no silver bullet in cybersecurity. A combination of security solutions is required to provide suitable threat prevention, detection and mitigation. Implementing cyber hygiene provides organizations with the foundational breadth necessary to manage risk in a changing landscape. Basic cyber hygiene helps you deepen your understanding of your organization's attack surface in order to minimize it as much as possible and monitor it for suspicious activity.

New tools and technologies enter the information security market all the time, but it's clear that many of them simply don't meet organization's actual needs. Focusing on the basics that produce demonstrable results may not make headlines. But the fundamentals of finding and patching vulnerabilities, ensuring systems are securely configured, and monitoring them for change go a long way in maintaining a strong security posture.

Learn more about implementing critical security controls at www.tripwire.com.

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at** tripwire.com

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » **Watch us at** youtube.com/TripwireInc

BRDMSCH1a 1808