



SANS Institute

Information Security Reading Room

What Security Practitioners Really Do When It Comes to Security Testing

Matt Bromiley

Copyright SANS Institute 2020. Author Retains Full Rights.

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

What Security Practitioners Really Do When It Comes to Security Testing

(Part 2 of Are Your Security Controls Yesterday's News?)

Written by **Matt Bromiley**

October 2019

Sponsored by:
Cymulate

Introduction

Take a moment to consider your current security control testing procedure(s). Do you perform scheduled, scope-limited penetration tests because you're required to? Do you simply let the vulnerability scanner do its thing and hope the attackers don't do the same? Or are you unsure about how you're testing your controls?

In the first of this duo of spotlight papers,¹ we discussed why security controls testing should not be constrained by scope-limited penetration tests or tests using attacks that do not mimic true threat actor activities. In conjunction with that paper (which we will call Part One), SANS ran a poll asking respondents to provide data about their current security control testing procedures. We explore that data in this paper.

Across our 366 poll respondents from the security community, approximately 75% indicated they do in fact test the effectiveness of their security controls, as illustrated in Figure 1. The rest of this paper will discuss additional details provided by this majority, but that still leaves us with approximately 25% who either do not test or are unsure if they do.

Do you test the effectiveness of your security controls?

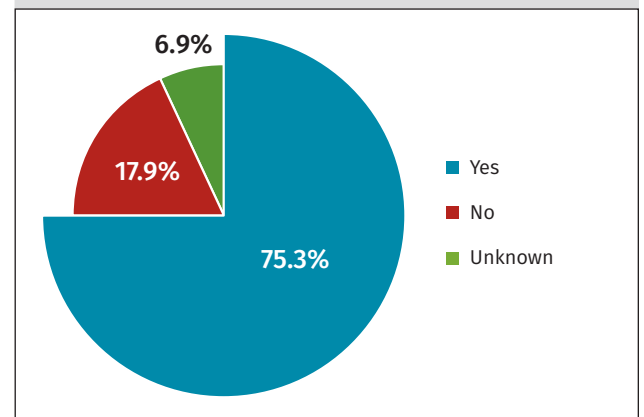


Figure 1. Poll Responses to Question About Effectiveness of Security Controls

Whether you're testing your security controls or not, one truth remains: Attackers don't care about scope.

¹ "Are Your Security Controls Yesterday's News?"

www.sans.org/reading-room/whitepapers/analyst/security-controls-yesterday's-news-39065. Registration required.

Although it's the theme of this spotlight series, it bears repeating: You should be testing your controls! If you are not testing your security controls, there's a chance someone else is. And they don't produce a pretty report at the end.

Getting It Right

Effective security control testing doesn't occur overnight; organizations will typically align their testing with various security frameworks that provide a useful scope of reference. In this survey, approximately 39% of our respondents indicated that they use NIST's Risk Management Framework,² with MITRE's ever-popular ATT&CK™ Framework coming in at just under 15%.

As seen in Figure 2, organizations also utilize internally developed frameworks, CVSS and others. Choosing the right framework for security control testing contributes significantly to the success of the testing. Typically, security teams and/or organizations may gravitate to compliance-type frameworks, ones with checkboxes that can represent a false sense of security and defense. Threat actors have shown repeatedly that they do not care about compliance standards or hypothetical defenses.

Instead, we recommend aligning with a framework that provides the foundation to identify and test against "real-world" threats, whether they are employed by a particular threat actor or something that is commonly exploited. MITRE's ATT&CK™ Matrix can start your security team thinking about the many methods by which a threat actor may escalate privileges, for example. By being able to test and verify against those techniques, you can start to limit what a "real" threat actor could do if they breached the environment.

This type of scenario-based testing may not necessarily be threat-actor based, but you will find yourself mitigating a lot of commonly used techniques by attackers of all skill levels. On the topic of relevant scenarios, we also asked our respondents to rank scenarios in terms of criticality with respect to their organization. The top-ranked critical scenario, as shown in Figure 3 on the next page (where the lower the score, the higher the criticality) was an attack on consumer-facing applications. A close second and third place were the ability to detect file-less and signature-less attacks and spear-phishing, respectively.

If you are not testing your security controls, there's a chance someone else is. And they don't produce a pretty report at the end.

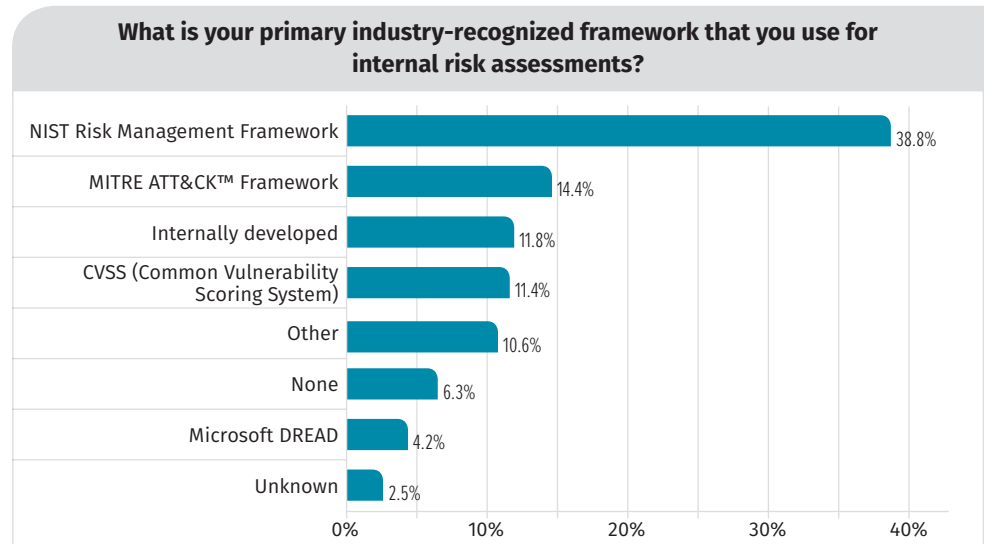


Figure 2. Poll Responses to Question About Which Primary Framework Respondents Use for Internal Risk Assessments

² "Risk Management," [https://csrc.nist.gov/projects/risk-management/risk-management-framework-\(RMF\)-Overview](https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview)

Rounding out our ranked threat actor scenarios were concerns such as exfiltration of data, unsafe browsing habits, ransomware and compromise of critical assets. Given the recent wave of highly targeted and coordinated ransomware attacks, we've seen that these attacks can potentially cause more technical and financial damage than other types of attacks.

However, organizations that utilize technique-based frameworks for their security control testing can rest easier; many of our top-concerning scenarios employ multiple techniques. For example, advanced malware may utilize an application vulnerability to deploy signatureless attacks. This blending of multiple critical techniques into one scenario highlights the need to tune security controls based on a combination of techniques, not a simple scenario.

These results brought to the surface other concerns for us: Are organizations testing their security controls in line with the highest concerns—or greatest fears? Are they limiting the success of security control testing via scope definitions or environment segmentation? In the next section, we examine just how testing is being performed.

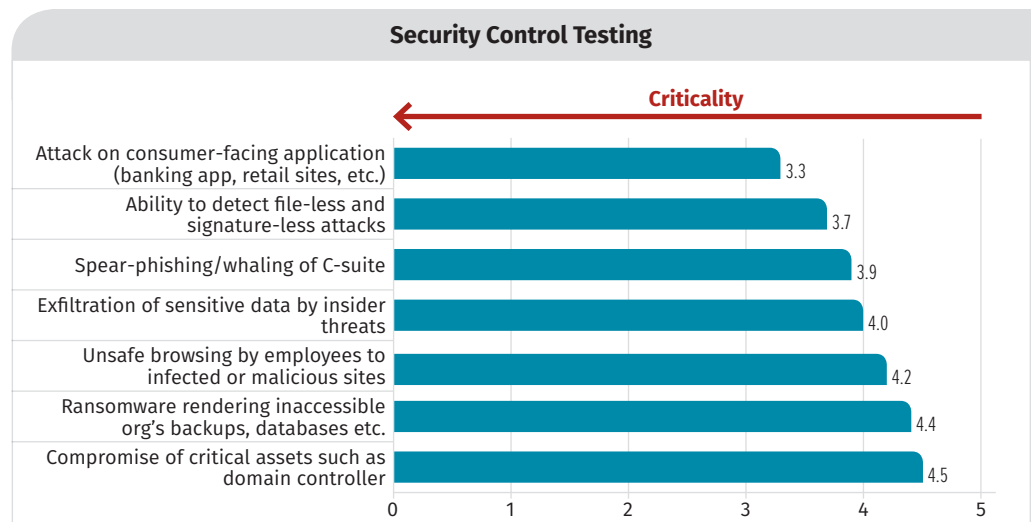


Figure 3. Ranking of Scenarios According to Perceived Criticality

TAKEAWAY

Security control testing can ensure that you have some controls or detections in place for some of the more advanced threat actor techniques, but these will often cover some of the basic techniques as well. Utilize a framework that focuses on *attacker techniques*. After all, they're the ones you need to defend against!

Getting It Done

It's likely that your security controls are being tested. Hopefully, the party doing the testing is one you're aware of! To the 76% of our full respondent base that perform testing, we inquired about the methods used to test the effectiveness of their security controls (see Figure 4). Leading the pack was penetration testing, at a whopping 84%. Vulnerability scanning came in second, nearly 20% behind. As shown in Figure 4, Red/Blue/Purple teaming activities³ were in fourth place, at approximately 44%.

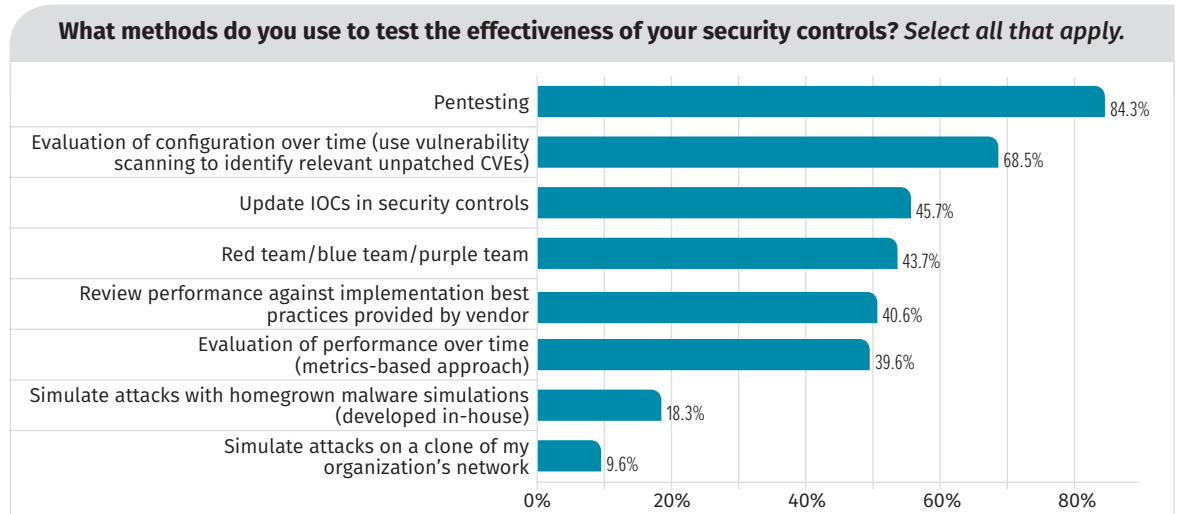


Figure 4. Poll Results About Methods Used to Test Security Controls Effectiveness

³ While we did not expand on the concept of blue/red/purple teaming within this survey, we'll classify that as activities performed in unison by a blue and red team, who are trying to defend and attack, respectively.

We hypothesized in Part One of this spotlight series that penetration tests and vulnerability scans were the primary security control effectiveness test, and unfortunately, they possess inherent weaknesses. Penetration tests, while useful for identifying pathways into an environment, are often dependent on the skill level of the penetration tester. Furthermore, penetration tests may do little to replicate the toolsets that a “real” threat actor may employ, thus providing a false sense of security. Lastly, and perhaps most importantly, penetration testing may be limited in scope and/or performed on a periodic, well-known schedule. This does little to take into account all the moving pieces of a complex organization—ones that an attacker may jump on and take advantage of.

To follow up on the notion of effectiveness, we also asked our respondents what technology they employ in testing their security controls. As shown in Figure 5, approximately 70% utilize vendor-provided testing tools. The top three responses were rounded out with automated penetration testing tools and home-grown tools/scripts, respectively.

In addition to the tools present, we also wanted to get an idea of how frequently security control testing happens. According to approximately 68% of our respondents, security control testing occurs at best case monthly and worst case annually. As shown in Figure 6, nearly 16% of our respondents indicated that testing occurred occasionally—yet another dangerous precedent.

Security control testing should be *ongoing*. It should be performed in response to events and done continuously. How do you do that? We’ll discuss that next.

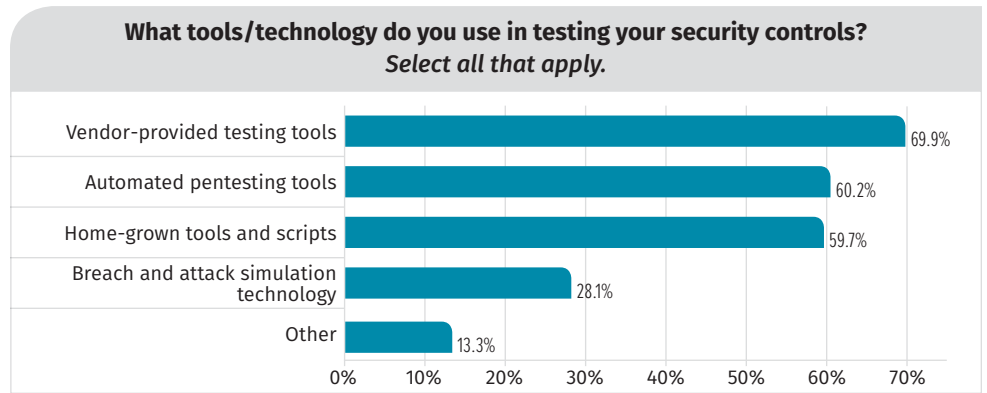


Figure 5. Poll Results in Response to Question About What Technology Respondents Employ in Testing Their Security Controls

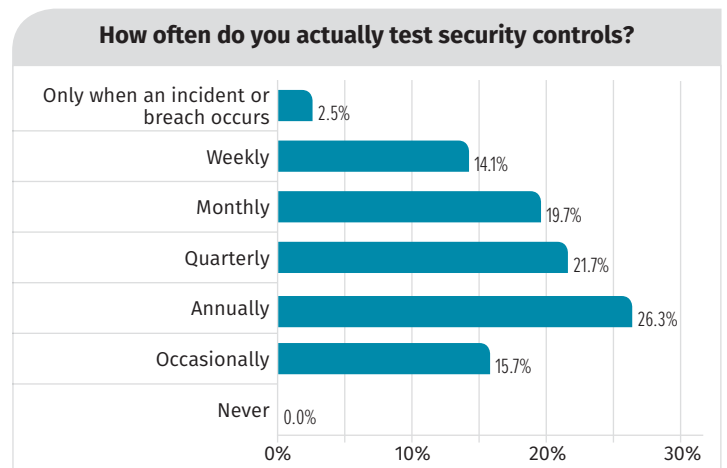


Figure 6. Poll Results in Response to Question About How Frequently Respondents Test Security Controls

Making It Better

Lastly, we asked our respondents how they are utilizing security control testing in their day-to-day activities. In short, is testing making their organization better or worse? As shown in Figure 7, approximately 75% of our respondents indicated that security control testing has a primary objective of identifying gaps that require remediation, with misconfiguration and poor policies a close second at 63%.



Figure 7. Poll Results in Response to Question About Objectives for Testing Controls

These statistics are encouraging. When security controls are used to identify and make immediate improvements in the environment, they are truly serving their unique purpose. Another area to give particular attention to is our fourth-place objective: testing defensibility against the very latest threats. We hope this objective means your organization is analyzing, documenting and testing against true threat actor activities.

Even with the best-laid plans, organizations still run into issues that may prevent them from achieving the level of success that they seek. In a near four-way tie, as shown in Figure 8, our respondents indicated that limitations and a lack of approach, knowledge and visibility in the use of automation are their top barriers.

Limitations in the use of automation in testing are one area where we expect organizations to grow the most in the coming months. Thanks to solid foundational frameworks and integrated environments, automation can be the key that replaces periodic testing with increased, continuous, almost real-time security control testing with environment-wide scope.

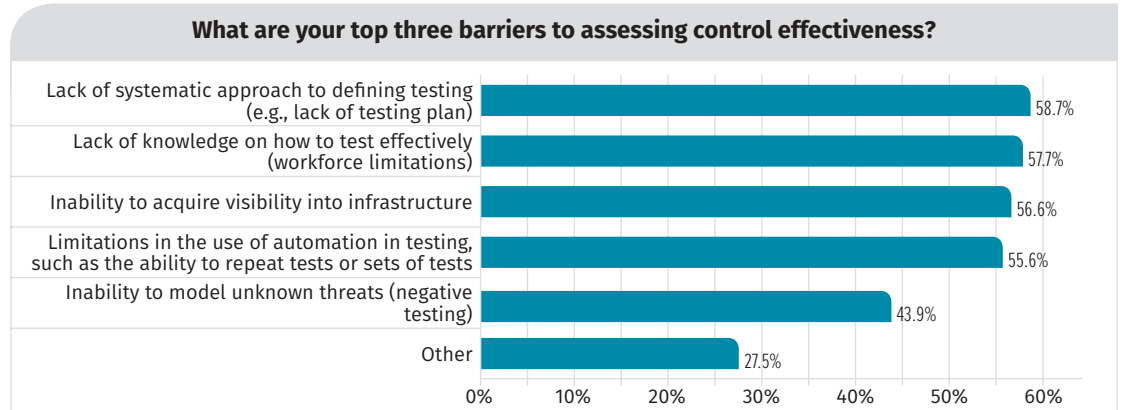


Figure 8. Poll Responses to Question About Top Three Barriers to Assessing Control Effectiveness

Closing Thoughts

Many organizations rely very heavily on their security controls to protect their environments. A lot of security work is typically done behind the scenes, and users simply go about their day, oftentimes without knowledge of the complexities going on in the background. For the information security team, it's an ongoing task to not only implement security controls, but also test their effectiveness. Without testing controls, we can never be sure they are working properly to defend the organization.

In this two-part SANS spotlight series,⁴ we discussed why security control testing is so crucial. Furthermore, we also discussed how oftentimes, penetration tests and simple vulnerability scans do not effectively test your implemented security controls. Threat actors who have your organization in their crosshairs will employ *whatever technique necessary* to achieve their objective. It's tough for your penetration testing team to emulate all the possibilities. Thus, we *must have a better way to test our security controls*.

Focus your security control testing on techniques and paths that can be exploited by multiple types of threat actors. By utilizing technique-based frameworks, your organization can effectively test and neutralize multiple types of attacks simultaneously, providing a sense of security that defends against real-world threats, not the limited scope of a penetration test. It's time to make your security controls do their job—defend the organization against realistic rather than hypothetical threats.

Without testing controls, we can never be sure they are working properly to defend the organization.

⁴ Part One: "Are Your Security Controls Yesterday's News?" www.sans.org/reading-room/whitepapers/analyst/security-controls-yesterday's-news-39065. Registration required.

About the Author

Matt Bromiley is a SANS Digital Forensics and Incident Response instructor, teaching Advanced Digital Forensics, Incident Response, and Threat Hunting (FOR508) and Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response (FOR572), and a GIAC Advisory Board member. He is also a principal incident response consultant at a major incident response and forensic analysis company, combining experience in digital forensics, incident response/triage and log analytics. His skills include disk, database, memory and network forensics, as well as network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:





Upcoming SANS Training

[Click here to view a list of all SANS Courses](#)

SANS Cairo February 2020	Cairo, EG	Feb 15, 2020 - Feb 20, 2020	Live Event
SANS Brussels February 2020	Brussels, BE	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS Scottsdale 2020	Scottsdale, AZUS	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS San Diego 2020	San Diego, CAUS	Feb 17, 2020 - Feb 22, 2020	Live Event
Open-Source Intelligence Summit & Training 2020	Alexandria, VAUS	Feb 18, 2020 - Feb 24, 2020	Live Event
SANS Training at RSA Conference 2020	San Francisco, CAUS	Feb 23, 2020 - Feb 24, 2020	Live Event
SANS Zurich February 2020	Zurich, CH	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Secure India 2020	Bangalore, IN	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Manchester February 2020	Manchester, GB	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Jacksonville 2020	Jacksonville, FLUS	Feb 24, 2020 - Feb 29, 2020	Live Event
ICS Security Summit & Training 2020	Orlando, FLUS	Mar 02, 2020 - Mar 09, 2020	Live Event
SANS Secure Japan 2020	Tokyo, JP	Mar 02, 2020 - Mar 14, 2020	Live Event
Blue Team Summit & Training 2020	Louisville, KYUS	Mar 02, 2020 - Mar 09, 2020	Live Event
SANS Northern VA - Reston Spring 2020	Reston, VAUS	Mar 02, 2020 - Mar 07, 2020	Live Event
SANS Munich March 2020	Munich, DE	Mar 02, 2020 - Mar 07, 2020	Live Event
SANS Jeddah March 2020	Jeddah, SA	Mar 07, 2020 - Mar 12, 2020	Live Event
SANS St. Louis 2020	St. Louis, MOUS	Mar 08, 2020 - Mar 13, 2020	Live Event
SANS Paris March 2020	Paris, FR	Mar 09, 2020 - Mar 14, 2020	Live Event
SANS Prague March 2020	Prague, CZ	Mar 09, 2020 - Mar 14, 2020	Live Event
SANS Dallas 2020	Dallas, TXUS	Mar 09, 2020 - Mar 14, 2020	Live Event
Wild West Hackin Fest 2020	San Diego, CAUS	Mar 10, 2020 - Mar 11, 2020	Live Event
SANS Doha March 2020	Doha, QA	Mar 14, 2020 - Mar 19, 2020	Live Event
SANS San Francisco Spring 2020	San Francisco, CAUS	Mar 16, 2020 - Mar 27, 2020	Live Event
SANS Norfolk 2020	Norfolk, VAUS	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS SEC504 Nantes March 2020 (in French)	Nantes, FR	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS London March 2020	London, GB	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS Secure Singapore 2020	Singapore, SG	Mar 16, 2020 - Mar 28, 2020	Live Event
SANS Kuwait March 2020	Salmiya, KW	Mar 21, 2020 - Mar 26, 2020	Live Event
SANS Seattle Spring 2020	Seattle, WAUS	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS SEC560 Lyon March 2020 (In French)	Lyon, FR	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Oslo March 2020	Oslo, NO	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Madrid March 2020	Madrid, ES	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Dubai February 2020	OnlineAE	Feb 15, 2020 - Feb 20, 2020	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced