# 8 Experts on Offensive Security

Mighty Guides

Sponsored by

Trustwave®

# Table of Contents

# Meet Our Experts

A comprehensive offensive security program extends an organization's internal capability to find weaknesses not discoverable by automated scanners and validates defensive posture. Competing priorities and limited in-house resources make it difficult for many organizations to operate an offensive security program internally to truly assess the effectiveness of their security from modern cyberattacks. We interviewed eight experts on what they look for when choosing a trusted partner to provide expert offensive security services that integrate and complement an existing internal security team.

We hope you enjoy their insights!


**David Rogelberg**
Publisher,
Mighty Guides Inc.
david@mightyguides.com
(516) 234 2969


Mighty Guides

**Shane Anglin**
Executive Vice President, CISO, Ameris Bank

**Damian Archer**
Vice President of AMS Consulting and Professional Services, Trustwave

**Jarrett Black**
Enterprise Account Executive, Trustwave

**Taraiz Khan**
Assistant Director, Information Security Assurance, Ernst & Young

**Izhar Mujaddidi**
Senior Director, Cybersecurity, Elevance Health

**Christopher Pope**
Manager, DevSecOps, Corporate IT, ExxonMobil

**Shashanko Roy**
Director of Cyber Security Services, KPMG US

**Nicole Tatrow**
Enterprise Account Executive, Trustwave

# Introduction

Cyberattacks continue to increase in sophistication and ubiquity. Each week, companies, governments, and organizations suffer security breaches that result in data loss, service outages, and other damages, costing millions of dollars in revenue and recovery, not to mention diminished customer trust.

To compound the challenge, organizations today manage services across a broad technology stack with engineering teams around the world. The increasing capacity and complexity of on-premises, cloud based, and hybrid services and the continued shift between office and remote workers have changed the threat landscape.

Traditional information-security defenses remain critical, but an offensive security program is essential for assessing security against modern cyberattackers, who are often well funded, organized and patient. Unfortunately, competing priorities and limited resources make it difficult for many organizations to maintain such a program. As a result, organizations are increasingly turning to third-party security providers to complement their existing in-house programs.

A comprehensive offensive security program extends your internal capabilities to find weaknesses not discoverable by automated scanners and validates your defensive posture. Penetration Testing-as-a-Service (PTaaS) using an interactive platform enables you to self-schedule assessments thereby easing integration of offensive security services into your own program.

Regardless of your organization's size or security program maturity, offensive security providers can tailor a program suited for your organization and the threats it faces. This Mighty Guide provides the information and guidance you need to choose the most capable provider.



Mighty Guides

**Mighty Guides make you stronger.**

**Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.**

**Reading a Mighty Guide is kind of like having your own team of experts. These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you.**

# Foreword

By **Ed Williams**, Vice President of EMEA Consulting and Professional Services, Trustwave

In a landscape where cyber threats evolve overnight, defensive measures alone are no longer sufficient. Cybersecurity demands a more proactive stance to stay ahead of adversaries who constantly refine their attack methodologies. Offensive security—which includes penetration testing, ethical hacking, and Red Teaming—is critical in identifying and mitigating vulnerabilities before malicious actors can exploit them.

This eBook—a collaborative effort between leading cybersecurity professionals and offensive security experts—provides deep insights into the necessity and implementation of proactive security measures. Recent challenges have underscored the importance of staying ahead, capable of and not only reacting to threats but also anticipating and neutralizing them. Offensive security is about understanding the mindset of attackers and using that knowledge to fortify defenses and uncover hidden vulnerabilities to refine their security postures.

The eBook delves into various offensive security strategies and the critical roles they play in a modern cybersecurity framework. Through extensive research and expert interviews, we explore how these proactive measures can transform an organization's security posture. We encourage you to leverage the insights within these pages to move beyond compliance or defensive measures and truly embrace proactivity to elevate your security strategies for a more resilient future.

Trustwave®

# It's Not Offensive or Defensive Security. It's Both.

The ever-shifting threat landscape demands a mix of offensive security tactics and frequent testing to go beyond compliance and truly manage your exposure.

**Get Proactive**

Chapter 1

# SCOPING THE RIGHT OFFENSIVE SECURITY PROGRAM

A robust offensive security program aims to find vulnerabilities before attackers do, allowing time to mount a proper defense. Offensive security experts work as trusted partners to find and exploit vulnerabilities in the system and then educate on the best approach to fix these flaws. This is accomplished by identifying vulnerabilities in an organization's code and infrastructure through penetration tests and vulnerability assessments.

These assessments follow the tactics, techniques, and procedures (TTPs) attackers use. While patching applications and training employees can thwart many indiscriminate attacks that scan the Internet for vulnerable software or unsuspecting people, taking a critical eye to assess defenses more deeply is



***"In the industry, it could be four to six weeks to kick off a pen test, and going into the PTaaS testing using our Fusion portal, I've seen that time decrease to 10 days, dramatically increasing the speed to value."***

**Jarrett Black**

Enterprise Account Executive, Trustwave

> ***Even many large organizations struggle to maintain every skill set on their internal security teams. Supplementing their capabilities with external resources enables security teams to leverage the competencies necessary to conduct thorough and deep security assessments."***

**Christopher Pope**

Manager, DevSecOps, Corporate IT, ExxonMobil

often necessary to prevent intentional, advanced attacks targeting the most valuable resources.

Implementing an offensive security approach is necessary because even though automated vulnerability scanners are crucial for finding common vulnerabilities in services and infrastructure, the most susceptible vulnerabilities can originate from architectural issues or logic flaws undetectable by even the best scanners. Finding these problems often requires human expertise in the underlying technologies and the mindset of an attacker to successfully exploit a series of vulnerabilities to achieve a specific goal. Managed offensive security providers supply the security experts and arm them with the best tools and training to find and assess vulnerabilities using techniques ranging from technical exploits to social engineering.

Jarrett Black, Enterprise Account Executive at Trustwave stresses the importance of using "all manual, human-led penetration tests" and emphasizes that humans with expertise in offensive security perform these self-scheduled tests. Trustwave's Penetration Testing-as-a-Service (PTaaS) gives clients "the ability to schedule them at their convenience."

## Choosing a Partner with Services that Best Fit Your Needs

Organizations have many options to consider when choosing a partner for an offensive security program, and it's essential to find one that fits the organization's architecture, risk profile, budget, and program maturity. The keystone of an offensive security program is the penetration test, and it's crucial to ask a prospective provider how they recommend tailoring their offerings to specific short- and long-term needs. For example, circumstances might call for a "white box" or "black box" test, which

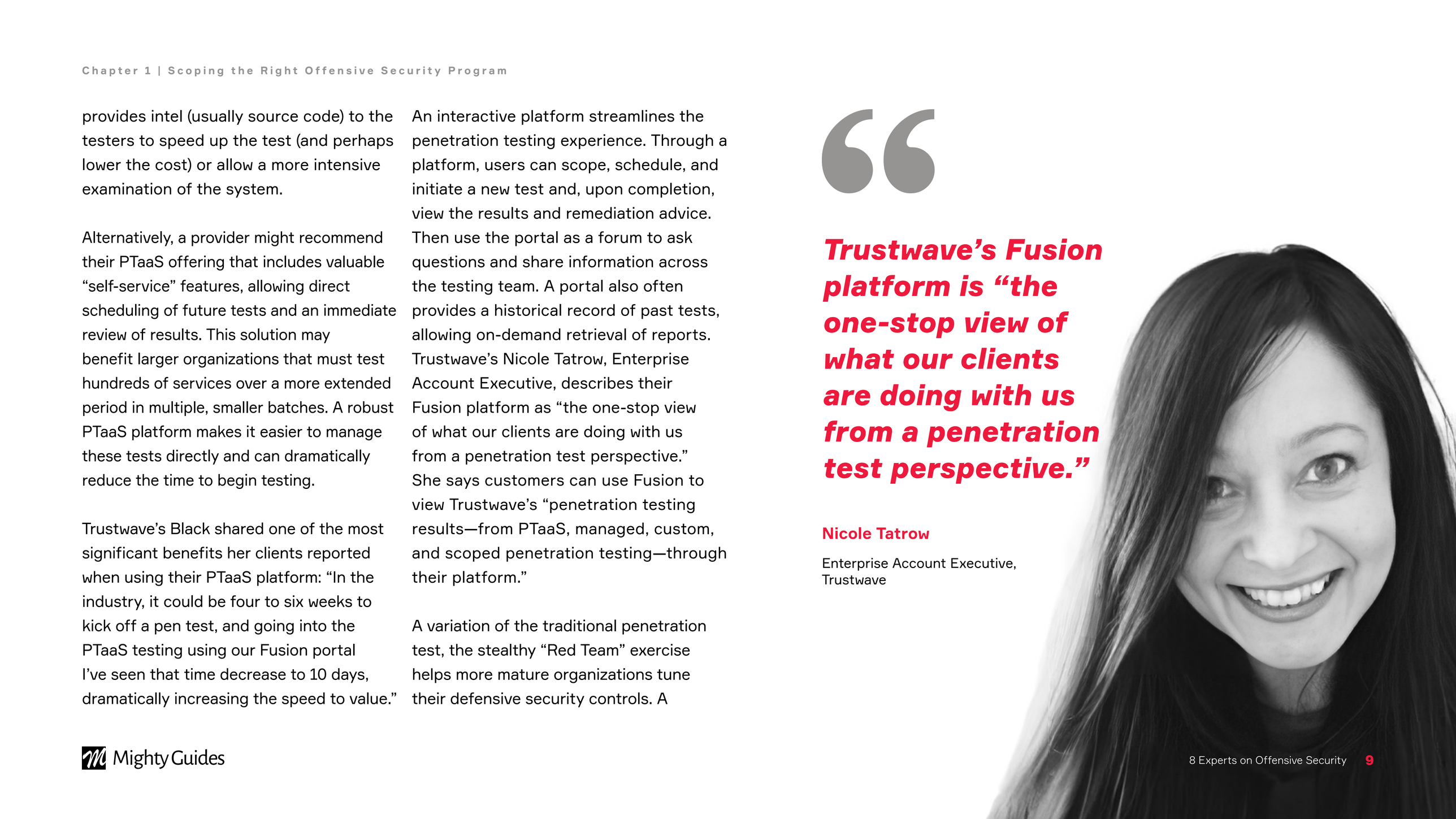
provides intel (usually source code) to the testers to speed up the test (and perhaps lower the cost) or allow a more intensive examination of the system.

Alternatively, a provider might recommend their PTaaS offering that includes valuable "self-service" features, allowing direct scheduling of future tests and an immediate review of results. This solution may benefit larger organizations that must test hundreds of services over a more extended period in multiple, smaller batches. A robust PTaaS platform makes it easier to manage these tests directly and can dramatically reduce the time to begin testing.

Trustwave's Black shared one of the most significant benefits her clients reported when using their PTaaS platform: "In the industry, it could be four to six weeks to kick off a pen test, and going into the PTaaS testing using our Fusion portal I've seen that time decrease to 10 days, dramatically increasing the speed to value."

An interactive platform streamlines the penetration testing experience. Through a platform, users can scope, schedule, and initiate a new test and, upon completion, view the results and remediation advice. Then use the portal as a forum to ask questions and share information across the testing team. A portal also often provides a historical record of past tests, allowing on-demand retrieval of reports. Trustwave's Nicole Tatrow, Enterprise Account Executive, describes their Fusion platform as "the one-stop view of what our clients are doing with us from a penetration test perspective." She says customers can use Fusion to view Trustwave's "penetration testing results—from PTaaS, managed, custom, and scoped penetration testing—through their platform."

A variation of the traditional penetration test, the stealthy "Red Team" exercise helps more mature organizations tune their defensive security controls. A



***Trustwave's Fusion platform is "the one-stop view of what our clients are doing with us from a penetration test perspective."***

**Nicole Tatrow**

Enterprise Account Executive, Trustwave

***Threat intelligence, vulnerability management, penetration testing, and ethical hacking exercises are all essential to provide insights into threats and attacker tactics, as well as prompt identification, assessment, and remediation of discovered vulnerabilities."***

**Taraiz Khan**

Assistant Director, Information Security Assurance, Ernst & Young

Red Team exercise looks for vulnerabilities to exploit and attempts to gain a foothold in the system without detection. Less mature programs may need the systems and teams in place to benefit from a Red Team exercise, so it's essential to choose advanced offerings like these wisely to ensure they align with capabilities, goals, and objectives.

An offensive security provider may also offer threat hunting and threat intelligence offerings. *Threat hunting* is a component of a defensive security program that leverages offensive security skills and looks for indicators of compromise and attack to discover whether attackers have successfully infiltrated systems. *Threat intelligence* provides refined and specific data about threats applicable to the technology and services used, helping to tailor defenses to repel the most likely attacks.

Beyond choosing the components of an offensive security program, it's important to stay mindful of common implementation challenges, such as selecting skilled testers suited to the environment and ensuring resource availability from engineering and product teams across the organization to participate as required. It's also crucial to have experience (or help) deciphering and triaging test results before planning and remediating the findings. Remember to leave time in the schedule to conduct a re-test that validates the remediation of found vulnerabilities. More complex environments require careful planning to skillfully move from one test to another to ensure the inclusion of all important systems.

A solid partnership with a qualified offensive security program provider offsets these challenges and helps build and operate an offensive security program tailored to specific needs. An ongoing partnership ensures expert availability when needed—whether for penetration testing, ongoing vulnerability scanning, merger and acquisition assessments, risk assessments, prioritizing and tracking remediation work, or forensics and incident response if necessary.

# Key Points

- Be sure to adequately understand your threat landscape and coverage of your existing information security controls to determine your offensive security needs.
- While automated scanners can find common vulnerabilities, finding the most critical vulnerabilities requires expertise in the technologies you use and the ability to think like an attacker.
- Offensive security providers offer a broad service catalog, which may include penetration tests, Red Team exercises, threat hunting, and threat intelligence services. Choose services that meet your testing needs and complement your in-house expertise.

Chapter 2

# TAILORING YOUR TEAM AND ASSESSING SKILLS AND EXPERIENCE

Most security programs include a mix of professionals focused on security operations, engineering, architecture, and governance, risk, and compliance (GRC). Those with more advanced capabilities may include Red Teaming, threat hunting, and penetration testing expertise, but these skills can be hard to find and expensive to maintain. Even organizations with robust in-house offensive security programs often supplement their capabilities with domain experts offered by a trusted partner. Before choosing a partner that's a good fit, it's essential to understand the requirements, which begins with a thorough understanding of the environment. Here are some questions to guide the way:

- **What technologies do your service and platform use?** On-premises servers and networking gear differ from virtualized cloud infrastructure, which may be orchestrated and abstracted through software layers. While conceptually similar, nuances between the major cloud service providers require expertise in the platforms used.
- **Is your organization subject to specific requirements of a niche vertical?** For example, suppose electronically protected health

> ***"Supplementing internal teams with external resources strengthens an organization's offensive security by bringing in a fresh perspective, specialized expertise, and increased capacity. These external resources provide objective assessments and help organizations stay current with the latest threats."***

**Taraiz Khan**

Assistant Director, Information Security Assurance, Ernst & Young

> ***Automating mundane and repeatable operational security tasks enables staff analysts and engineers to engage in more creative critical thinking activities and increases operational resilience, speed, efficiency, and security effectiveness of the overall security program.”***

**Shane Anglin**

Executive Vice President, CISO, Ameris Bank

information is processed in the United States. In that case, the organization may be subject to Health Insurance Portability and Accountability Act (HIPAA) regulations that require tight data and asset management. Working with government organizations may involve prescriptive testing requirements defined by government standards bodies such as the National Institute of Standards and Technologies (NIST) or laws such as the Federal Risk and Authorization Management Program (FedRAMP). These regulations and standards define specific controls influencing penetration testing scoping and requirements.

- **What is your architecture and code base?** Ensure a clear and thorough understanding of the product and service architecture. For example, testing a more extensive monolithic application differs from testing many interdependent microservices. Understand the code base and the repositories relied upon, including internally written code, code imported from third-party vendors, and any open-source code used.
- **How do your users and attackers see your services?** Threat model systems help to understand where critical assets and data reside, the boundaries between trusted and untrusted systems, what services provide input and output functions, and how users (and attackers) will interface with services.
- **Will cross-discipline teams be available to participate in the penetration test?** While an offensive security program may begin in the security team, the results will likely impact product and engineering. Partnering with these teams early on helps create the best test scope and allows them to plan for remediation activities.

Once this level of understanding is achieved regarding the environment and in-house security capabilities, a client is prepared to select a trusted partner that best aligns with its specific needs. This knowledge also enables the provider to recommend the best service offering. For example, a full-service offering (aka “white glove” treatment) might include a single point of contact for project and program management activities to help define scope, set testing parameters and rules of engagement, facilitate interactions with the testers, and marshal help to review and understand the testing results. This hands-on approach ensures successful engagement regardless of any environmental nuances or complexities.

In contrast, a PTaaS self-service model is more hands-off and allows the client to directly define and schedule a test through an interactive platform. This streamlines the setup and significantly reduces the time to begin a test from when it’s first requested.

Look for a provider with solid customer support that is flexible, adaptable to specific needs, and expert in the technologies used. A good provider will continually invest in their team and ensure their consultants have the time, budget, and support to train and keep pace with technological evolution.

***“Partnering with reputable external resources enhances an organization’s security credibility, demonstrating a commitment to security best practices and improves their security posture, compliance, and protection against evolving threats.”***

**Taraiz Khan**

Assistant Director, Information Security Assurance, Ernst & Young

# Key Points

- **Even organizations that have built up their own offensive security program benefit from offensive security domain experts to complement gaps in their capabilities.**
- **Know your environment, which informs your offensive security needs, including the technologies you use, the code base and repositories you rely on, and whether your industry vertical imposes additional requirements.**
- **Threat-model your systems before you choose your offensive security provider, so you know your trust boundaries and where your most critical assets reside, which will guide your security testing.**
- **Map your requirements and capabilities against a provider's service offerings to find a provider that aligns with your system complexity, budget, in-house resources and expertise, and program maturity.**

Chapter 3

# GETTING VALUE FAST

After choosing a testing provider, share goals, objectives, and environment details to structure and successfully scope the engagement with them. Work together to clearly define the testing activity's scope and parameters, including setting test objectives, identifying in-scope assets, and identifying the right people to help facilitate the testing and remediation. Discuss possible threat scenarios to the infrastructure that will shape the nature and approach of the test. For example, decide whether one or several tests work best, how to configure test or production environments, and how to provision necessary user access accounts to support the engagement.

Ask the provider how best to integrate their offerings with the organization's testing team. Damian Archer, Vice President of AMS Consulting and Professional Services at Trustwave, explains the value of the Trustwave PTaaS platform: "A client can log into the platform, schedule an assessment, and kick that assessment off within days without any interaction from the Trustwave team, given that the environment is understood. The platform speeds up the entire process."

A platform like this helps eliminate unnecessary hoops and decreases the ramp-up time to testing. Effective portals reduce the need to email reports

> ***Before and during a test, remember to effectively communicate with all stakeholders and implement comprehensive safeguards during testing to prevent scope creep and any significant disruptions."***

**Izhar Mujaddidi**

Senior Director, Cybersecurity, Elevance Health

> ***A client can log into the platform, schedule an assessment, and kick that assessment off within days without any interaction from the Trustwave team, given that the environment is understood. The platform speeds up the entire process."***

**Damian Archer**

Vice President of AMS Consulting and Professional Services, Trustwave

and questions back and forth, and once set up in their system, users can schedule scans at their convenience. Lean on the partner for concise explanations of their reported findings, including remediation options appropriate to the environment.

A good partner will also help triage their findings and offer remediation tips that enable operators and engineers to close the discovered vulnerabilities quickly. Archer says, "We provide what the finding is, what the associated risk is, and what the remediation would be. We can also provide video evidence of a finding demonstrating the exploitation and provide a debrief or readout if it's a critical finding. We can do that midway through the assessment with the developers to talk through the associated risk and impact of the finding."

Before kicking off a penetration test, ensure the vulnerability management program works well. Scan infrastructure and code for common vulnerabilities, exploits, and misconfigurations and remediate these before scheduling the penetration test. Properly configured, these scans help identify orphaned or misclassified assets, configuration drift from baseline,

insecure code, and possible misconfigurations in cloud or on-premises infrastructure. Identifying and patching common vulnerabilities ahead of a penetration test will increase its value because it reduces the number of (likely prominent) findings and allows the testers to focus on challenging and sophisticated vulnerabilities. In other words, it reduces the noise and focuses the penetration test on the unknown items.

***When involving multiple disciplines at different technical levels in a testing engagement, it's critical to leverage the specialization of each team member through collaborative and clear communication from the team leads."***

**Shashanko Roy**

Director of Cyber Security Services, KPMG US

# Key Points

- **Work with your offensive security provider to clearly define the scope and parameters of the testing activity, which includes setting test objectives, identifying the assets to be tested, and choosing the right people to facilitate smooth testing and successful remediation.**
- **Ask how the provider integrates with your security team and how they eliminate unnecessary hoops to jump through and decrease the ramp-up time.**
- **A good partner will help triage test findings and offer remediation tips that enable your operators and engineers to close the discovered vulnerabilities in a practical and efficient manner.**
- **Ensure your vulnerability management program works well before starting a penetration test. Scan your infrastructure and code and remediate for common vulnerabilities, exploits, and misconfigurations before the test to focus the provider on vulnerabilities you may not be able to discover yourself.**

Chapter 4

# TESTING BEYOND COMPLIANCE

Governance, risk, and compliance (GRC) programs assess an organization's risks, define and measure the effectiveness of controls to manage these risks, and validate the overall security program's effectiveness through external audits. Completing an annual penetration test is a specific requirement of many information security standards and frameworks. However, meeting compliance obligations is just the beginning.

Trustwave's Archer firmly believes that "compliance isn't an end state. It's a milestone in the journey of proving security. Penetration testing will go above and beyond the compliance minimums and identify issues, vulnerabilities, and other areas of concern outside of compliance standards. It will give you a more holistic and complete picture of an environment or target through an attacker's lens."

## Offensive Security Strengthens Dependent Controls

What is now considered table stakes is a penetration test required by most security standards as a core validation that vulnerabilities are identified and addressed. Beyond simply identifying vulnerabilities, however, offensive security testing can be used to look for systemic issues or flaws in other controls.

The International Organization for Standardization ISO/IEC 27001 describes the requirements of an effective

> ***Regulatory compliance often represents, at best, the basic minimum for security practices. Limiting your security assessments to what is legally required will leave out many exposures and realistic avenues of attack."***

**Christopher Pope**

Manager, DevSecOps, Corporate IT, ExxonMobil

***Testing beyond the minimums necessary for compliance helps organizations detect and prepare for vulnerabilities and unexpected threat scenarios that could result in financial, privacy, regulatory, and reputational impact for the business.”***

**Shashanko Roy**

Director of Cyber Security Services, KPMG US



information security management system (ISMS). This standard takes a risk-based approach to determining the system and controls appropriate to any organization and allows for implementation flexibility. Tailor your offensive security program to bolster and evidence various controls that matter to you. Trustwave’s Archer finds that customers understand many of the “OWASP Top 10 remediation mechanisms for common vulnerability classifications. Things like logic flaws or underlying architectural issues are more difficult to remediate.” Use the findings in a penetration test to identify training opportunities to improve the system development life cycle, detection and response processes, architectural design, and threat modeling.

A penetration test can also help determine the effectiveness of some other security controls. For example, use the test to:

- Assess detection and response capabilities.
- Validate threat models against actual exploitation tactics, techniques, procedures.

- Ensure that asset inventories and external endpoints are up to date.
- Review asset classification processes to include the most critical assets for testing.
- Test and validate vulnerability scanning controls.
- Test and validate cloud security posture management (CSPM) configurations.
- Look for systemic issues behind findings that bolster existing risks or identify new risks.

Extract as much value as possible from an offensive security program by aligning and scoping penetration tests with these other program elements. A continuous testing program reduces the drift of any of these dependent controls and prevents the buildup of technology debt.

***Identifying and remediating gaps beyond compliance requirements provides additional opportunity to minimize attack surfaces and creates opportunities for innovations, continuous monitoring, and competitive advantage.”***

**Izhar Mujaddidi**

Senior Director, Cybersecurity, Elevance Health

*Compliance isn't an end state. It's a milestone in the journey of improving security. Penetration testing will go above and beyond the compliance minimums and identify issues, vulnerabilities, and other areas of concern outside of compliance standards. It will give you a more holistic and complete picture of an environment or target through an attacker's lens."*

**Damian Archer**

Vice President of AMS Consulting and Professional Services, Trustwave

# Key Points

- **Penetration testing goes above and beyond compliance minimums and will identify issues, vulnerabilities, and other areas of concern outside of compliance standards.**
- **Tailor your offensive security program to bolster and evidence a wide variety of controls beyond the penetration test, for example, tailor it to ensure effective detection and response.**
- **Use the findings in a penetration test to identify training opportunities to improve your system development lifecycle, detection and response processes, architectural design, and threat modeling.**
- **Operating a program of continuous testing identifies regular maintenance opportunities, which prevents the buildup of technology debt.**

Chapter 5

# COMBINING OFFENSE AND DEFENSE

A Red Team exercise is a stealthy, goal-oriented version of a penetration test. Only a few key executives are aware of the engagement. The intention is to simulate an attack to test technical and human defenses. An information security operations team focused on detection and response is often called a Blue Team. Combining a Red Team offense and Blue Team defense in a joint engagement is known as a Purple Team exercise and not only helps identify and reduce vulnerabilities but improves detection and response capabilities.

Holding an honest opinion of a security program's capability maturity is essential when designing an appropriate offensive security program.

Trustwave's Archer has cautioned: "If they [clients] don't have any defensive capability, then there's no point in engaging a Red Team because you're testing defensive efficacy." He emphasized that, "you [Trustwave security experts] need to make sure the client at least has the basics in play before you start trying to do the advanced things. Otherwise, you end up with a report that's just torn you to pieces, and it's challenging to play catch up based upon the remediations in that report. Ensuring that client maturity aligns to

> ***"Proactively and progressively sharing the Red Team security testing actions directly with the defensive Blue Team enables the Blue Team to more effectively tune the security controls and processes in preparation for malicious and anomalous security events."***

**Shane Anglin**

Executive Vice President, CISO, Ameris Bank

[the] service offering is vitally important for the success of any assessment."

Purple Team engagements can work well if offensive and defensive capabilities are in-house or outsourced to a managed security service provider. The ability to outsource components to a managed security provider enables smaller or less mature security programs to benefit from more advanced and sophisticated Purple Team engagements.

Purple Team exercises are an excellent way to validate if a managed detection and response program is working properly.

Trustwave's Archer describes the synergies of using linked managed services: "We have a significant defensive security catalog of services and products. So, our expertise in defense is learned and borrowed from everything we do. Suppose you have Trustwave for both defensive and offensive security services. In that case, all those offensive security services almost become Purple Teams very naturally because we're able to create the right level of bridge between the defensive and offensive side of our service offerings."

***"Establishing communication channels and feedback between offensive and defensive security teams allows them to examine their effectiveness from the opposite perspective and helps them reach their maximum effectiveness. Without this, many crucial insights that can contribute to the overall enterprise security posture will be lost."***

**Christopher Pope**

Manager, DevSecOps, Corporate IT, ExxonMobil

***Connecting offensive and defensive security teams during testing fosters a collaborative approach to security, allowing organizations to reduce vulnerabilities and improve detection and response capabilities. By simulating real-world attacks, offensive teams help defensive teams practice responding to realistic threats, enhancing their detection and response strategies."***

**Taraiz Khan**

Assistant Director, Information Security Assurance, Ernst & Young

Purple Team exercises increase defensive posture by testing controls and exercising under-utilized tooling. The exercises hone and provide an end-to-end test of detection and response protocols. These engagements develop and test a team's threat-hunting skills by providing opportunities to look for indicators of compromise and indicators of attack (IoC/IoA) in a safe and controlled engagement. Purple Team exercises are popular for "gamification" to enroll subject matter experts from different teams in an organization in constructive (often fun) exercises.

## Offensive Security for any Organization

Offensive Security programs offer more than annual penetration testing. Partnering with a qualified provider will help identify any gaps in a client's security program and provide expert resources to find the vulnerabilities attackers use. With ever-increasing technological complexity and dependencies, choosing a trusted partner to help plan and deliver the right testing program for the organization is more critical than ever.

# Key Points

- A Red Team exercise simulates an attack to realistically test your technical and human defenses.
- A Purple Team exercise not only helps identify and reduce vulnerabilities but also improves your team's detection and response capabilities.
- A managed provider can offer more advanced capabilities such as Red, Blue, and Purple team services to smaller or less mature security programs.

# Learn More About Our Experts

**Shane Anglin**

**Executive Vice President, CISO, Ameris Bank**

Shane Anglin is an accomplished leader serving as the Executive Vice President and CISO at Ameris Bank, overseeing a comprehensive portfolio including Cyber Security, Information Security, Physical Security, and Identity Security. With a robust background in IT and IS security strategy, risk assessment, and technology innovation, he ensures optimal operations and secure assets. Shane's expertise extends from cloud-enabled enterprises to strategic security risk assessment, driving impactful change and fostering collaborative environments.

**Damian Archer**

**Vice President of AMS Consulting and Professional Services, Trustwave**

Damian Archer is the Regional Vice President of the AMS Consulting and Professional Services team at Trustwave. Damian has been in the security industry for over 20 years, having delivered, led, and managed offensive security assessments and programs for both public and private sectors. Damian continues to work closely with clients to ensure that their offensive, and wider, security needs are met and managed in line with the right security outcomes.

**Jarrett Black**

**Enterprise Account Executive, Trustwave**

With over two decades of experience in cybersecurity, Jarrett has a distinguished career specializing in offensive security. For the past 15 years, she has dedicated her expertise to Managed Security Services and Penetration Testing, partnering with top global companies to create and execute robust security strategies that meet client objectives.

**Taraiz Khan**

**Assistant Director, Information Security Assurance, Ernst & Young**

Taraiz is a seasoned information security professional, boasting a diverse career trajectory across esteemed organizations like EY, Wesley Mission Queensland, and Tabcorp. With over a decade of experience, he has honed his expertise in digital risk management, cybersecurity governance, and technology assurance. Taraiz holds a master's degree in Information Technology, Management Information Systems and Services from Macquarie University in Sydney, Australia.

# Learn More About Our Experts

## Izhar Mujaddidi

**Senior Director, Cybersecurity, Elevance Health**

Izhar Mujaddidi is an accomplished cybersecurity expert with over 20 years of experience, currently serving as Senior Director of Cybersecurity at Carelon Behavioral Health, an Elevance Health Company. Over the course of his career, Izhar has demonstrated excellence, securing significant contracts and maintaining compliance for both government agencies and Fortune 500 clients. Notably, he has spearheaded ISO and HITRUST certifications, pioneered innovative security solutions, and implemented advanced risk management frameworks.

## Christopher Pope

**Manager, DevSecOps, Corporate IT, ExxonMobil**

Christopher Pope is an accomplished IT manager and security leader at ExxonMobil, specializing in DevOps and enterprise security. In his role, Christopher implemented a DevSecOps program affecting 9 programs of work, 70 teams, and 300+ products. Christopher is known for his strong technical background, effective communication skills, and leadership abilities, making him a sought-after conference speaker and trusted professional in the field.

## Shashanko Roy

**Director of Cyber Security Services, KPMG US**

Shashanko Roy, Director of Cyber Security Services at KPMG US, is a seasoned cybersecurity, risk, and compliance leader. With a master's degree from the Indian Institute of Management, Bangalore, and significant roles at Mashreq Bank and KPMG, Shashanko's expertise has made a substantial impact in the field. He stays at the forefront of cybersecurity with ongoing learning and development and is especially knowledgeable in GRC application development, information governance, and IT audits.

## Nicole Tatrow

**Enterprise Account Executive, Trustwave**

Nicole is a seasoned industry professional with over 20 years of experience in cybersecurity. She has strategized with leading global companies to develop and implement effective offensive security programs, aligning talent and expertise with client needs. Additionally, Nicole has dedicated 17 years to organizing the DEFCON Hacking Conference.

Trustwave®

# Unlock the Full Potential of Your Microsoft Security Investment.

Accelerators for Microsoft Defender, Sentinel & Copilot
MDXR & Co-Managed SOC for Microsoft Security
Penetration Testing
MailMarshal & DbProtect

**Optimize Your Security**

Microsoft