Unit 42 Incident Simulation and Testing Services

What if you could see yourself as attackers see you? You'll know if your security controls are working, and if not, you can proactively adjust them to improve your security posture based on likely attack scenarios unique to your organization.

World-Renowned Security Experts, Always in Your Corner

As an industry-leading threat intelligence, incident response, and cyber risk management organization, it's our job to help you prepare for and respond to some of the most challenging threats so you can get back to business faster. As threats escalate and evolve, we act as your trusted partner to help you simulate threats and test your security controls to validate and strengthen your security program.

Pressure-Test Your Defenses

When an attack occurs, you want to take action immediately and with purpose. By partnering with Unit 42, you can measure your ability to respond to an attack before it happens. You'll do this by first working with our security consultants to evaluate your current defenses. You can then simulate your response to a cybersecurity incident with customized scenarios based on industry-specific threats that make use of real-world breaches we've already investigated and resolved. This knowledge and experience help us prioritize attack scenarios that represent a real risk to your organization.

Tabletop Exercises

How well will you react in the event of an attack? Evaluate your incident response plan with real-world attack scenarios that help you identify gaps and improve response capabilities. By partnering with us, you can gauge your response to a real-world cybersecurity incident using lessons learned from actual Unit 42 cases.

Using regional and industry-specific Unit 42 threat intelligence, you will work with our consultants to design customized scenarios that reflect real attacks you are most likely to see, creating technical and non-technical exercises to suit all audiences. By role-playing a customized, simulated incident that leverages our deep threat intelligence and experience, you will understand your organization's incident response strengths and opportunities for improvement, measuring yourself against best practices. Not only will you determine how your documented plan performs against various breach scenarios, you will also assess your organization's decision-making speed under pressure. As a result, you won't get blindsided when there is a real attack when you:

- Benchmark your preparedness.
- Test your incident response plan.
- Improve alignment and decision-making.

Table 1: Tabletop Exercises Features	
Custom Tabletop Exercise Our consulting team will leverage their deep threat intelligence and incident response experience to build a custom and relevant simulation for you using lessons learned from actual Unit 42 cases. We can design technical and non-technical exercises to suit all audiences.	**Enhancement Opportunities** Following the Tabletop Exercise, we will provide a list of prioritized recommendations for improving your incident response capabilities, processes, and tooling.
Know Your Strengths Unit 42 will identify and document your incident response strengths and weaknesses.	**Actionable Next Steps** You'll receive tactical, action-oriented remediation steps to address the weaknesses, gaps, and vulnerabilities discovered.

Penetration Testing

Test your defenses against an attacker's playbook with real-world attack simulation in your environment. It's critical to understand the specific strengths and weaknesses of your environment. With Unit 42, you will simulate real-world attack scenarios that are unique to your organization's needs. You accomplish this by pressure testing your organization's technical controls and network security—safely applying tactics, techniques, and procedures (TTPs) that real threat actors use to gain unauthorized access and maintain a foothold in compromised environments. By collaborating with our team of experts, you will see your defenses through the lens of a threat actor, leveraging known adversary TTPs in the process. With the resulting knowledge, you will understand exactly how a threat actor could tangibly impact your operations. The knowledge you gain will help you take proactive measures to close vulnerabilities in your environment before an incident occurs, including how to:

- Conceptualize threat actor impact.
- Pressure test security controls and capabilities.
- Enhance technical security posture.

Table 2: Penetration Testing Features	
Executive Summary You'll receive an executive summary that provides our high-level findings and recommendations resulting from the Penetration Test, with a focus on business outcomes.	**Detailed Technical Report** Unit 42 will provide an in-depth technical report describing the details of the engagement scope, methodology, testing TTPs, and specific findings.
Prioritized Recommendations Unit 42 will provide specific and prioritized recommendations based on the potential security impact and exploitability of vulnerabilities or weaknesses discovered across your environment.	**Remediation Steps** You'll receive tactical, action-oriented remediation steps to address the weaknesses, gaps, and vulnerabilities discovered during Penetration Testing exercises.
Custom Objective Reporting Unit 42's team of skilled offensive security experts can support your unique objectives, such as testing specific TTPs against critical assets specific to your organization.	

Purple Team Exercises

It's critical to know how attacks are likely to unfold so you can up-level your organization's ability to effectively detect and prevent cyberthreats. With Purple Team Exercises, your organization's security personnel (Blue Team) will collaborate with Unit 42's elite team of offensive security engineers (Red Team) to orchestrate drills that test your network monitoring and incident response processes. These drills will include initial phishing attacks as well as the use of manual and automated techniques by Unit 42 to further exploit systems, elevate credentials, and move deeper into the network. Through this exercise, you will immediately understand the impact of changes to alerting or detection mechanisms. What's more, you will participate in simulations that include customized scenarios that are the most likely to impact your organization. With reports at both the executive and technical levels that you receive at the end, you can develop the right remediation steps, adjusting capabilities to improve organizational awareness and your readiness to respond. In short, you can:

- Combine the power of Red and Blue Teaming.
- Tune defenses and get real-time feedback.
- Identify gaps in security control coverage.

Table 3: Purple Team Exercises Features	
Phishing Simulation Exercises Phishing is the number-one attack vector leveraged by threat actors to gain initial access to an organization's environment. Unit 42 will conduct multiple phishing campaigns to test your email security controls and attempt to gain access to your environment.	**Penetration Testing** After gaining initial access, Unit 42's team of offensive security experts will leverage both manual and automated techniques to further exploit systems, elevate credentials, and move deeper into the network. This includes both internal and external Penetration Tests.
Defense and Alerting Recommendations Through a collaboration between Unit 42 and your security team, you will establish the ideal tuning of defensive capabilities and alerting mechanisms.	**Custom Payload Deployment** At your request, Unit 42 may develop and deploy custom payloads to achieve specific objectives or test criteria.
Executive Summary You will be provided with an executive summary tailored to executives, C-suite, and boards of directors. This will contain our high-level findings and recommendations.	**Detailed Technical Reporting** Unit 42 will provide an in-depth technical report describing the details of the engagement, including methodology, testing techniques, tactics, findings, recommendations, and next steps.
Recommendations and Remediation Steps You will receive recommendations prioritized based on the impact and exploitability of vulnerabilities or weaknesses identified during the testing. You will also receive tactical, action-oriented remediation steps to address the weaknesses, gaps, and vulnerabilities discovered during the engagement.	

Unit 42 Retainer

The clock starts immediately when you've identified a potential breach. But if you can't determine the root cause and contain the breach right away, your adversary will be back in no time. With a Unit 42 Retainer in place, you eliminate the unnecessary delays of negotiating costs and terms or scrambling to find help when time is of the essence. Instead, you will engage with an assigned point of contact at Unit 42—someone with an intimate understanding of your infrastructure, existing playbooks, and team—who can quickly support you.

The Unit 42 Retainer allows you to purchase prepaid credits that fit your budget and cybersecurity needs. The Retainer lets you choose your response-time SLAs to align with your existing SecOps and IR capabilities and strategy. This means you can minimize the impact of an attack and get back to business sooner.

Our Retainers are structured to help you become more resilient through proactive services. You can allocate credits towards Unit 42 Cyber Risk Management Services, such as Tabletop Exercises, Penetration Testing, Purple Team Exercises, Compromise Assessments, Board Advisory Services, Breach Readiness Assessments, and more. And with a Unit 42 Retainer, our experts become an extension of your team—well-versed in your environment so we can respond quickly and accurately should an incident occur. Put us on speed dial, and we'll be ready to assist at a moment's notice.

About Unit 42

Palo Alto Networks Unit 42™ brings together world-renowned threat researchers, elite incident responders, and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time so that you get back to business faster.

Under Attack?

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team at start.paloaltonetworks.com/contact-unit42.html or call North America Toll-Free: 866.486.4842 (866.4.UNIT42), EMEA: +31.20.299.3130, UK: +44.20.3743.3660, APAC: +65.6983.8730, or Japan: +81.50.1790.0200.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com