4 Must-Have Security Assessments for Modern SecOps

Assessments dialed into your needs.

As a CISO, you've made security assessments an essential part of your strategy. But you can't benefit from assessments that tell you what you already know or issue blanket recommendations that aren't relevant to your business.

It's time to stop defending against every potential threat out there and focus on the ones most likely to impact your environment. When you work with Unit 42®, you get deep insights that go beyond surface-level checks and custom recommendations tailored to your situation and your environment.

This guide introduces you to four of the most critical assessments we provide:

1 **AI SECURITY ASSESSMENT**

Unlock AI potential with expert security insights.

2 **SOC ASSESSMENT**

Modernize your SOC with AI and automation.

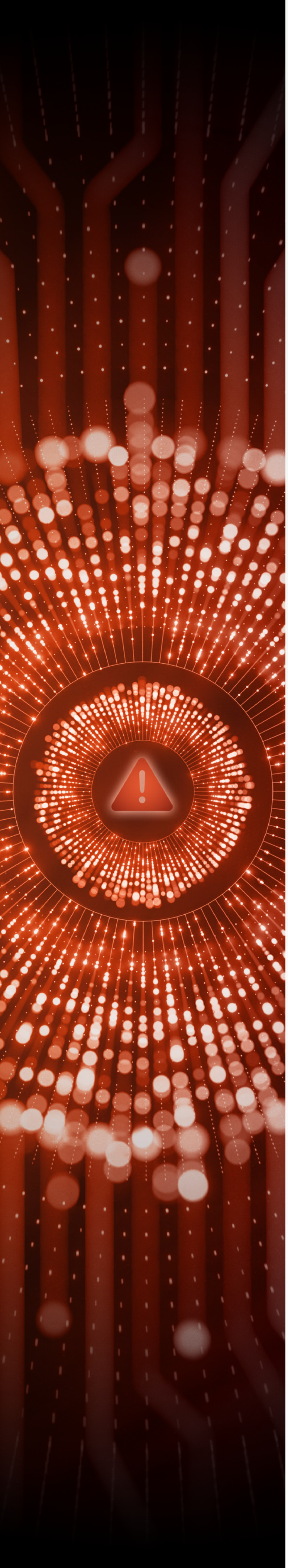
3 **CLOUD SECURITY ASSESSMENT**

Implement security purpose-built for the cloud.

4 **ZERO TRUST ADVISORY**

Design a cohesive and effective zero trust plan.

▶▶▶ **Find out how each service drives real-world improvements in your security posture—and gives you the insights needed to make informed decisions.**



1 AI Security Assessment

Empower safe AI use and development with visibility and security strategies.

Do you know how AI is being used—in both sanctioned and unsanctioned ways—by developers and employees across your organization? Unit 42 identifies your AI-related risks with industry-leading threat intelligence and AI expertise. You get tailored best practices to mitigate risks specific to your AI footprint, empowering your organization to adopt and innovate confidently with AI.

WHAT'S INCLUDED?

- ☑ A report of AI usage patterns and scenarios
- ☑ Threat-led, data-driven analysis of AI application architecture and workshops to assess your exposure, focused on your business use cases
- ☑ A tailored, prioritized roadmap of actionable recommendations and best practices for AI innovation

WHY DO YOU NEED IT?

Your teams are already running fast with AI, and it's important to make sure they don't trip. The scale of AI use and the speed of the models mean that one mistake could have a massive impact. The AI Security Assessment enables you to maximize AI innovation without compromising security.

WHEN DO YOU NEED IT?

- You're struggling to report on your AI security posture.
- AI use by employees and developers is moving fast and outside of InfoSec policies and controls.
- You're evaluating the potential for AI use or growth (a good time to identify and mitigate risks).
- Executives aren't aligned on the AI security investment.

WHAT WILL IT DO FOR YOU?

Reduce your AI adoption risk.
You are more prepared to manage potential threats and reduce overall risk when you understand AI tools use and development across the organization.

Secure AI use.
You can give your employees appropriate guardrails so they can work smarter—and innovate—without leaking sensitive data.

Fortify AI development.
We tune best practices to your key use cases so you can stay ahead of competitors without exposing yourself to avoidable risks.

Accelerate AI security.
Whether you're starting from scratch and need core governance or you want to improve your SOC with AI, we know what it takes to get you to the next level.

How the AI Security Assessment Works →

2 SOC Assessment

Modernize your SOC with AI and automation.

The SOC Assessment combines Unit 42 threat intelligence and frontline SOC expertise—including lessons learned from the Palo Alto Networks SOC—to uncover exposures in your attack surface and prepare you for threats based on geography, industry, and more. With your unique threat profile in hand, our experts deliver a roadmap to strengthen detection and response with AI and automation.

WHAT'S INCLUDED?

- ☑ Recommendations for SOC improvement, including proposed workflows, automations, and templates
- ☑ Best practices from the Palo Alto Networks world-class SOC
- ☑ Threat intelligence to help you defend against the threats most likely to impact you
- ☑ An executive report to gain alignment with your management team, board, and stakeholders

WHY DO YOU NEED IT?

The threat landscape never stops evolving, and neither should your SOC. This assessment is about leveling up your SOC to strengthen your security posture and stay ahead of whatever's coming at you. It empowers your team to become more efficient and effective in detecting and responding to threats with the latest and greatest technology, tools, and processes.

WHEN DO YOU NEED IT?

- You've had an attack, breach, or near miss.
- You're struggling to find the right balance of people, processes, and technology.
- You're experiencing high SecOps churn—or facing hiring and upskilling challenges.
- You're under pressure from stakeholders or the board to justify the investments you need.
- It's time—as in, it's been a year or more since your last SOC assessment.

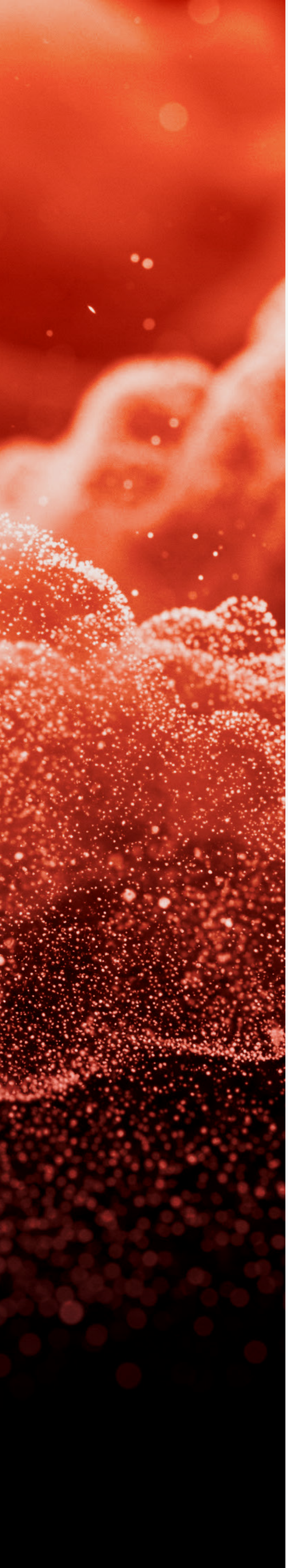
WHAT WILL IT DO FOR YOU?

Focus on key elements of your attack surface.
Your attack surface is constantly changing. With a SOC Assessment, you get a clearer picture of your dynamic environment—including forgotten assets, gaps in visibility, vulnerabilities, paths for lateral movement, potential attack paths, and more.

Prioritize and address cybersecurity gaps effectively.
Your SOC analysts are already busy enough. We help prioritize how to improve detection and response by working smarter. We also identify ways to help your team transition from being primarily reactive to taking a more proactive approach to threats.

Enhance the speed, precision, and impact of your SOC.
As cybercriminals use AI to launch faster, more sophisticated attacks, defenders must leverage AI and automation to stay ahead—detecting and responding to threats faster than attackers can act. We identify opportunities to improve your people, technologies, and processes—with streamlined workflows to advance the maturity of your SOC.

How the SOC Assessment Works →



3 Cloud Security Assessment

Turn cloud complexity into actionable security insights.

With proven code-to-cloud security strategies shaped by decades of real-world experience, the Unit 42 Cloud Security Assessment helps align your security program to the dynamic and distributed nature of modern cloud environments, ensuring protection is effective from development through deployment.

WHAT'S INCLUDED?

- ☑ Analysis of cloud threat trends and adversaries related to your business and technology
- ☑ Collaborative exploration and benchmarking of your cloud posture against best practices
- ☑ Prioritized, actionable guidance to remediate cloud misconfigurations and immediately improve your cloud security posture
- ☑ A custom transformation roadmap for future-proofing your cloud security program

WHY DO YOU NEED IT?

Cloud computing is inherently different from traditional on-prem computing. As a result, any existing security programs have to be adapted for the cloud to provide the necessary protection. This assessment enables you to do exactly that—and, as a result, to move fast in the cloud without compromising security.

WHEN DO YOU NEED IT?

- You're validating cloud security coverage, and your team needs help understanding the shared responsibility model, particularly when using multiple cloud providers.
- You're expanding your cloud environment—especially if you're moving critical workloads to the cloud.
- You struggle with fragmented security products that create operational overhead, obscure visibility, and delay detection and response to cloud-based threats.

WHAT WILL IT DO FOR YOU?

Unlock your cloud potential.
Deploy and scale in the cloud, knowing you have the right controls to proactively reduce risk.

Reduce cloud exposure risk.
Threat-driven prioritization aligned with business context will ensure that cloud security architecture and SecOps teams spend time mitigating the most impactful risks to your business.

Enhance collaboration for unified cloud security.
Build a cloud security program that closes gaps from fragmented responsibilities and optimizes resources. Align executives and teams to gain buy-in and justify what's needed to move securely in the cloud.

Secure the development pipeline.
Reduce friction and empower developers to build secure cloud applications from the start, leading to faster and safer innovation.

How the Cloud Security Assessment Works →

4 Zero Trust Advisory

Navigate the complexities of zero trust implementation.

The Zero Trust Advisory helps you adopt a modern cybersecurity approach that eliminates implicit trust and continuously validates digital interactions. No matter where you start, our experts guide you through the entire journey, from building a common understanding to creating an implementation roadmap and designing effective policies. We bring together cross-functional stakeholders to strengthen alignment for smooth implementation that won't disrupt business operations.

WHAT'S INCLUDED?

- ☑ Benchmarking of your infrastructure and security practices against best practices
- ☑ A zero trust vision, strategy, and implementation plan aligned to your business goals
- ☑ Target-state architecture design and supporting policies

WHY DO YOU NEED IT?

Translating zero trust principles into security policies that don't negatively impact your business is a complex task. When you're ready to implement, zero trust requires multi-team coordination across business, technology, and security teams. It's extremely helpful to have an expert guide.

WHEN DO YOU NEED IT?

- You are unclear how to start translating zero trust from a concept into a clear, actionable strategy tailored to your environment.
- Your zero trust initiative has lost momentum due to unclear priorities, a lack of internal alignment, or competing demands.
- You need data and expert insights to align security, IT, and business teams, build executive support, and maintain momentum for zero trust implementation.

WHAT WILL IT DO FOR YOU?

Turn strategy into action.
Unit 42 helps translate zero trust from a broad concept into a tailored, step-by-step roadmap based on your environment, risk profile, and business goals.

Refocus and accelerate progress.
We assess where your initiative stands, clarify priorities, and provide a clear path forward, reviving momentum and eliminating roadblocks.

Build alignment with credible insights.
Backed by threat intelligence and deep expertise, we deliver the data and perspective needed to unify teams, secure executive buy-in, and drive lasting progress.

How the Zero Trust Advisory Works →

Your Trusted Partner for Strengthening and Modernizing Security

When you work with Unit 42, you gain instant access to one of the world's largest and most experienced threat intelligence teams—with 300+ threat hunters, malware reverse engineers, and threat modeling experts. That's in addition to all the other ways you benefit:

- **Take advantage** of our comprehensive tools—and the insights we've gained from working with 80,000+ customers using Palo Alto Networks best-of-breed solutions.
- **Get support** from Unit 42 proactive services, managed services, and incident response experts ready to jump in when your team needs additional resources or specialized skills.
- **Feel supported and understood,** without judgment and with prioritized recommendations so you can transform at your own pace.

Stronger security begins with structure and clarity.

▶▶▶ **Go deeper on these assessments:**

AI Security Assessment

SOC Assessment

Cloud Security Assessment

Zero Trust Advisory

If you're under attack or want to engage with an expert to find the right assessment for you:

▶▶▶ Contact us now

paloalto NETWORKS | UNIT 42

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/unit42