Unit 42 Cyber Risk Assessment

Measure Your Defenses Against Evolving Threats and Apply Customized Recommendations to Improve Your Security Program

Protect Against the Biggest Risks to Your Organization

Evaluate Your Current State of Readiness with a Unit 42 Cyber Risk Assessment

To stay ahead of threat actors, it's more critical than ever to understand your organization's security maturity and prioritize risk effectively with a framework-based or regulatory-focused risk assessment.

The Unit 42® Cyber Risk Assessment helps you compare the current versus target state of security controls, identify risks and gaps, and develop a plan to improve. This assessment outlines the strengths, weaknesses, and opportunities of your current cybersecurity program to help your stakeholders understand the threat landscape and how to reduce the risks to your business.

Unit 42 Cyber Risk Assessment Benefits

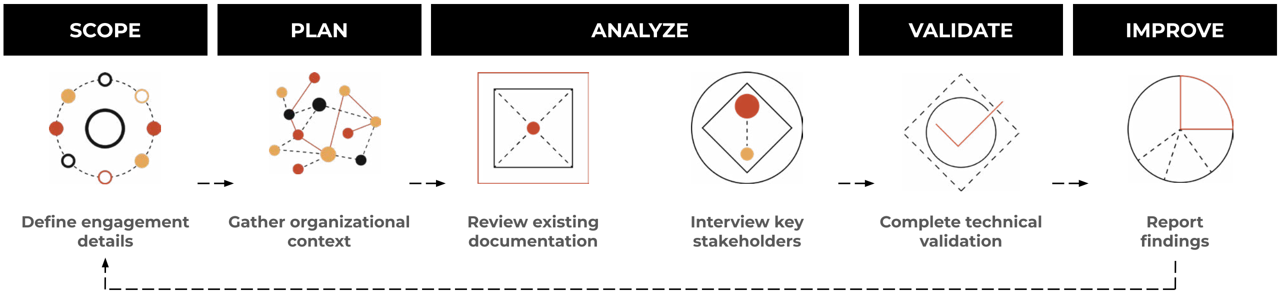
- **Evaluate your current state of readiness.** Work with our experts to assess your current security posture. Identify and prioritize the most critical improvements on which to focus. From full program build-outs to strategic guidance, we help you establish world-class cybersecurity.
- **Lay a strong foundation.** Develop the foundations for strong cybersecurity, including policies, procedures, standards, workflows, staffing charts, and strategic roadmaps to position your security program for success.
- **Focus on what matters.** Discover and prioritize security risks across your organization to build a 1–, 3–, or 5–year strategic roadmap that guides your security program so you can focus on your business.

Unit 42 Cyber Risk Assessment Methodology

With a Unit 42 Cyber Risk Assessment, you'll gain a better understanding of the threat landscape and how to reduce the risks to your business.

CYBER RISK ASSESSMENT: METHODOLOGY

Best practices to strengthen your security program



SCOPE | PLAN | ANALYZE | VALIDATE | IMPROVE

Define engagement details → Gather organizational context → Review existing documentation → Interview key stakeholders → Complete technical validation → Report findings

Figure 1: Unit 42 Cyber Risk Assessment methodology

- **Define engagement details.** Unit 42 collaborates with you to identify the appropriate assessment depth, framework, and outputs.
- **Gather organizational context.** We'll provide a pre-engagement questionnaire to gain an understanding of organizational processes, tools, and capabilities.
- **Review existing documentation.** Our team will review your existing documentation to identify gaps in security control design.
- **Interview key stakeholders.** Unit 42 will interview your people to gain additional insight regarding security control deployment and technical capabilities.
- **Complete technical validation.** We conduct focused technical testing to verify information collected during documentation review and stakeholder interviews.
- **Report findings.** You'll receive a detailed report including security risks with recommendations prioritized to guide your efforts.

About Unit 42

Unit 42® brings together our world-renowned threat researchers and hunters with an elite team of security consultants to create an intelligence-driven, response-ready organization. The Unit 42 Threat Intelligence team provides threat research that enables security teams to understand adversary intent and attribution while enhancing protections ofafered by our products and services to stop advanced attacks. As threats escalate, Unit 42 is available to advise customers on the latest risks, assess their readiness, and help them recover when the worst occurs. For the latest threat intel and research, please visit https://unit42.paloaltonetworks.com/.

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