Unit 42
M&A Cyber Due Diligence

Highlight Cybersecurity Risks, Vulnerabilities, and Attack Surface Exposure That May Impact the Viability of Your Investment

Reduce Cyber Risk Associated with Mergers and Acquisitions

Enter into a Merger or Acquisition with Eyes Wide Open

Mergers and acquisitions can add to your attack surface, create new vulnerabilities, and increase cyber risk. Bringing organizations together and combining SOCs with different priorities and policies can create unexpected gaps in cybersecurity procedures and incident response plans.

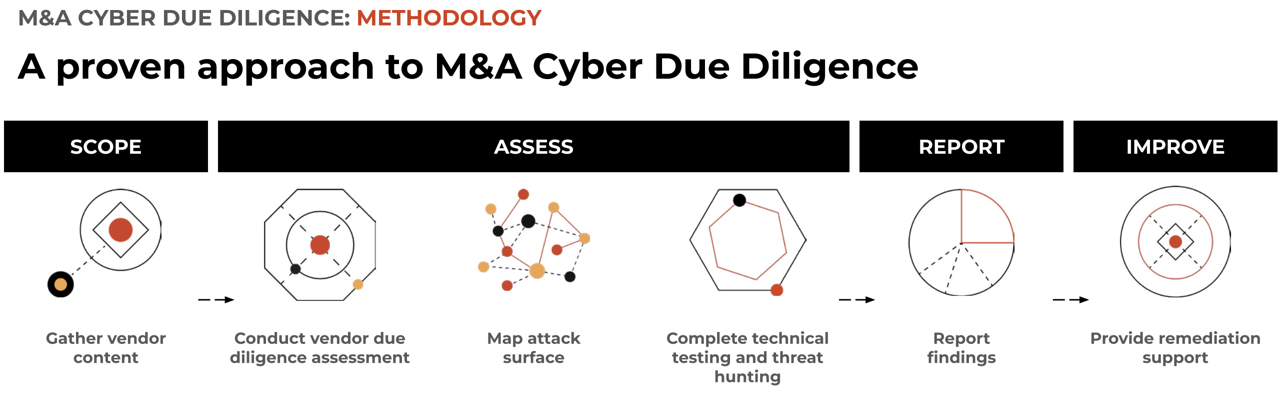
The Unit 42® M&A Cyber Due Diligence service identifies potential red flags and highlights cybersecurity risks in the context of a merger or acquisition. Leveraging Unit 42's proprietary M&A Cyber Due Diligence Framework, you will get a broad understanding of a potential target's cybersecurity posture and receive a report detailing findings, recommendations, and tactical remediation steps to reduce acquisition risk.

Unit 42 M&A Cyber Due Diligence Benefits

- **Reduce risk and meet your deadlines.** Unit 42 is built on speed. By leveraging our proprietary Cyber Due Diligence Framework and the power of Cortex XDR® and Cortex Xpanse®, you can adhere to strict timelines while providing an in-depth view of a target company's risk posture.
- **Identify red flags.** Highlight cybersecurity risks, vulnerabilities, information technology hygiene concerns, and attack surface exposure that may impact the viability of your investment.
- **Remediate smarter.** Obtain prioritized findings and recommendations that can be leveraged to strategically close gaps and guide remediation activities, making the most effective use of available resources.

Unit 42 M&A Cyber Due Diligence Methodology

Unit 42 offers a proprietary framework to identify and mitigate acquisition and merger security risks.



M&A CYBER DUE DILIGENCE: METHODOLOGY

A proven approach to M&A Cyber Due Diligence

SCOPE — ASSESS — REPORT — IMPROVE

Gather vendor content

Conduct vendor due diligence assessment

Map attack surface

Complete technical testing and threat hunting

Report findings

Provide remediation support

Figure 1: Unit 42 M&A Cyber Due Diligence methodology

- **Gather vendor content.** Unit 42 conducts a pre-engagement survey to understand the state of current processes, tools, and capabilities.
- **Conduct Vendor Due Diligence Assessment.** Using our Vendor Due Diligence Framework, we identify cyber acquisition risks across all aspects of the target organization.
- **Map attack surface.** We'll use Cortex Xpanse to create a detailed map of the target's asset inventory and attack surface.
- **Completed technical testing and threat hunting.** Our team will conduct technical testing and threat hunting to identify cybersecurity risks and exploitable weaknesses.
- **Report findings.** You'll receive a detailed report, including security risks with recommendations prioritized to guide your efforts.
- **Provide remediation support.** Unit 42 assists clients and supply chain vendors with remediation tasks and implementing recommendations to enhance security.

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