Ransomware Readiness Assessment

Achieve a Target State of Ransomware Readiness

Ransomware attacks are holding organizations hostage, and with ransom demands averaging $847,000, you can't afford to be unprepared. The first step in defending against today's sophisticated ransomware attacks is assessing your ability to prevent and respond to them.

The Unit 42 Ransomware Readiness Assessment focuses on preparing your people, processes, and technology to mitigate the threat of ransomware. We work with you to develop control enhancements, remediation recommendations, and a playbook based on the latest best practices and threat intelligence to achieve a target state of ransomware readiness, helping you to:

- Avoid attacks with ransomware safeguards
- Recover faster with a best practice response playbook
- Test your readiness with a ransomware tabletop exercise
- Put our team on speed dial with SLA-driven response times

Benefits of the Assessment

- Better prevent attacks with control recommendations
- Detect hidden ransomware threats
- Test your readiness with a simulated attack
- Put the Unit 42 IR team on speed dial

Defending against today's sophisticated ransomware attacks starts with an assessment of your ability to prevent and respond

The Unit 42 Ransomware Readiness Assessment comes in two varieties, designed to match your organization's needs.

Option 1: Ransomware Readiness Assessment

Readiness Assessment

- **Outcomes:** Improve your organization's ability to quickly and effectively respond to a ransomware attack.
- **Services:** Unit 42 experts with extensive experience in cybersecurity and incident response (IR) will review your IR plan, capabilities, and technologies. Our consultants will highlight gaps and identify areas for improvement to help bolster your readiness and strengthen your overall cyber defense capabilities.
- **Deliverables:** We'll provide a report of findings and recommendations for your organization to achieve a target state of ransomware readiness.

Ransomware Threat Briefing

- **Outcomes:** Keep your security team and key stakeholders better informed of the current state of ransomware threats and actionable steps your organization can take to prevent attacks.
- **Services:** Our world-renowned Unit 42 threat intelligence team will update and educate your team on the latest ransomware threats, including attack vectors, TTPs, ransom demands, and top safeguards to prevent attacks.
- **Deliverables:** We'll host a verbal update and Q&A session with a Unit 42 threat intelligence analyst.

Ransomware Tabletop Exercise

- **Outcomes:** Improve your organization's ability to quickly and effectively respond to a ransomware attack.
- **Services:** We'll design and facilitate a ransomware attack tabletop IR exercise, based on the thousands of investigations our IR team has performed, to test your readiness with a simulated attack as well as help you practice IR processes and workflows. We evaluate effectiveness in real-world scenarios.
- **Deliverables:** We'll provide an after-action report with recommendations for improvement.

50 Hours Reserved for IR

- **Outcomes:** Extend your IR team's capabilities by putting the world-class Unit 42 IR team on speed dial with SLA-driven response times. Improve recovery times and the efficacy of IR.
- **Services:** Your retainer hours are valid for one year and can be used for IR services or proactive cybersecurity advisory services as needed. Each retainer service request is subtracted from your total allotted hours.
- **Deliverables:** What we provide will vary depending on the service request.

Complete ransomware readiness includes a hunt for indicators of compromise associated with early stages of the ransomware lifecycle

Threat actors can dwell in networks for months before encrypting files. The Complete Ransomware Analysis addresses this challenge with a ransomware-focused compromise assessment. We'll work with you to scan endpoints in your environment, review forensic artifacts, and collect endpoint telemetry to uncover evidence of malicious activity often associated with early stages of the ransomware lifecycle.

Option 2: Compromise Assessment (Includes Everything in Option 1)

Compromise Assessment with Cortex XDR

The Unit 42 Compromise Assessment is designed to identify evidence of historical or ongoing compromise. Unit 42 IR experts will analyze endpoint forensic artifacts and telemetry to search for early stages of the ransomware lifecycle. We hunt for indicators of compromise (IOCs) related to sophisticated ransomware threat actors, including unauthorized access, use of PowerShell post-exploitation frameworks, and precursor malware that often leads to the installation of ransomware.

1. **Deploy:** We'll deploy Cortex XDR to gain visibility into endpoint artifacts and telemetry.
2. **Analyze:** Our IR experts will analyze endpoint data to identify IOCs and potential gaps.
3. **Deliver:** You'll get a report with findings and strategic recommendations for control enhancements based on empirical observations, configuration settings, and opportunities to reduce your attack surface.

About Unit 42

Unit 42 brings together an elite group of cyber researchers and incident responders to protect our digital way of life. With a deeply rooted reputation for delivering industry-leading threat intelligence, Unit 42 has expanded its scope to provide state-of-the-art IR and cyber risk management services. Our consultants serve as trusted partners to rapidly respond to and contain threats so you can focus on your business.

About Cortex XDR

Cortex® XDR™ is the industry's first extended detection and response platform that integrates data from across your organization to stop modern attacks. Cortex XDR has been designed from the ground up to deliver enterprise-wide protection while simplifying security operations by breaking down security silos. Using behavioral analytics and AI, Cortex XDR identifies unknown and highly evasive threats. Your analysts can quickly investigate threats by getting a complete picture of each incident, and then respond across enforcement points to eliminate threats.

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