Ransomware Readiness Assessment

Achieve a Target State of Ransomware Readiness

Ransomware attacks are holding organizations hostage, and with ransom demands as high as $50 million,[1] your organization 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 Unit 42 on speed dial with SLA-driven response times.

With Unit 42, you will harness the power of Cortex XDR to conduct a Compromise Assessment of your environment, focusing on the early stages of ransomware by analyzing endpoint telemetry and hunting for indicators of compromise associated with sophisticated ransomware groups. You can engage in purple team exercises to safely target your environment with a simulated ransomware campaign that includes the advanced tactics used in real-world attacks we've investigated. Next, you can work with us on tabletop exercises to validate your response strategy. Through this process, you develop a comprehensive understanding of your ability to prevent and respond to these threats, along with recommended control enhancements.

After completing assessments, analyses, and exercises, you can work with the Unit 42 team to prepare and deliver a full report and set of recommendations, benchmarked against industry standards, to reduce the likelihood and impact of ransomware. This will enable your C-suite and board of directors to understand the organizational risk of the ransomware threat and empower you to drive better security outcomes.

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.

[1] *2023 Unit 42 Ransomware and Extortion Report*, Unit 42, March 21, 2023.

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

The Unit 42 Ransomware Readiness Assessment is available in three different tiers, designed to match your organization's needs.

Tier 1: Ransomware 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 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.

Unit 42 Retainer with 250 Credits for Incident Response

- **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 credits are valid for one year and can be used for IR services or proactive cyber risk management services as needed. Each Retainer service request is subtracted from your total allotted credits.
- **Deliverables:** What we provide will vary depending on the service request.

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

Tier 2: Ransomware Analysis (Includes everything in Tier 1)

Compromise Assessment with Cortex XDR

The Unit 42 Compromise Assessment is designed to identify evidence of historical or indicators of ongoing compromise. Unit 42 IR experts will analyze endpoint forensic artifacts and telemetry to search for the 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 postexploitation frameworks, and precursor malware that often leads to the installation of ransomware:

- **Outcomes:** Detailed analysis of client's networks and endpoint behaviors to determine whether there is evidence of unauthorized access or activity.
- **Services:** Our IR experts will perform a detailed analysis of forensic artifacts and endpoint telemetry to determine whether there is evidence of malicious activity caused by ransomware threat groups, such as:
  - Unauthorized access to the environment
  - Malicious software and malware persistence
  - Lateral movement and remote execution
  - Credential theft
  - Data exfiltration or sabotage
- **Deliverables:** 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 Cortex XDR

Cortex XDR® is the industry's first extended detection and response platform that spans all data to stop modern attacks. With Cortex XDR, you can harness the power of AI, analytics, and rich data to detect stealthy threats. Your SOC team can cut through the noise and focus on what matters most with intelligent alert grouping and SmartScore incident scoring. Delivering best-in-class endpoint threat prevention and an enterprise-ready console for investigations, Cortex XDR offers the visibility and protection you need to secure what's next.

Tier 3: Ransomware Resilience (Includes Everything in Tiers 1 & 2)

Purple Team Ransomware Campaign

External and internal penetration testing where Palo Alto Networks will attempt to identify and exploit system and network vulnerabilities from the perspective of an attacker and will attempt to gain entry to the customer's commercial network:

- **Outcomes:** Improve your organization's ability to quickly and effectively respond to a ransomware attack. Control and mitigate attacks through collaboration with Unit 42 offensive security experts to fine-tune defenses or add new controls.
- **Services:** The Unit 42 Offensive Security team targets your environment following predefined rules of engagement with a custom-designed campaign of advanced TTPs used in real-world ransomware attacks.
- **Deliverables:** Receive reports of the results of each simulated attack and training and control enhancement recommendations.

Executive and Board Advisory

Following the completion of assessments, analyses, and exercises, the Unit 42 team will prepare and deliver a full assessment of your organization's readiness as well as recommendations to reduce the likelihood and operational impact of ransomware-related cyber incidents:

- **Outcomes:** Empower your C-suite and board of directors to understand organizational risk related to the ransomware threat and drive better security outcomes.
- **Services:** We perform a data-driven appraisal of security capabilities covering safeguards and redundancies, people and business partners, and process and governance.
- **Deliverables:** Information security program recommendations benchmarked against industry standards, correlated with empirical incident response, red team, and threat intelligence data, and aligned with your organization's strategic objectives.

Approved by Cybersecurity Insurance Plans

Unit 42 is on the approved vendor panel of more than 70 major cybersecurity insurance carriers. If you need to use Unit 42 services in connection with a cyber insurance claim, Unit 42 can honor any applicable preferred panel rate in place with the insurance carrier. For the panel rate to apply, just inform Unit 42 at the time of the request for service.

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:

- Fill out the form at start.paloaltonetworks.com/contact-unit42.html.
- 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.
- Email **unit42-investigations@paloaltonetworks.com**.

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. Visit paloaltonetworks.com/unit42.

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_ds_ransomware-readiness-assessment_080423