Ransomware Readiness Assessment

Achieve a Target State of Ransomware Readiness

Ransomware attacks are holding organizations hostage, and with ransom demands averaging $5.3 million, 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 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 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 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 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 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 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 post-exploitation 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 integrates network, endpoint, cloud, and third-party data to stop sophisticated attacks. Cortex XDR has been designed from the ground up to help organizations like yours secure their digital assets and users while simplifying operations. Using behavioral analytics, it identifies unknown and highly evasive threats targeting your network. Machine learning and AI models uncover threats from any source, including managed and unmanaged devices.

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

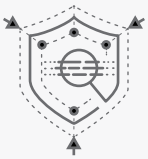
Purple Team Ransomware Campaign

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 & 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 BoD 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.

About Unit 42

Unit 42 brings together world-renowned threat researchers 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 offered 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. Unit 42 Security Consultants serve as a trusted partner with state-of-the-art cyber risk expertise and incident response capabilities, helping you focus on your business before, during, and after a breach.

Get in Touch

If you'd like to learn more about how Unit 42 can help your organization defend against and respond to severe cyberthreats, visit https://start.paloaltonetworks.com/contact-unit42.html to connect with a team member.

Under Attack?

If you think you may have been breached or have an urgent matter, please email unit42-investigations@paloaltonetworks.com or call US Toll-Free: 1.866.486.4842 (866.4.UNIT42), EMEA: +31.20.299.3130, APAC: +65.6983.8730, and Japan: +81.50.1790.0200.

paloalto NETWORKS

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_082521