MANDIANT

DATASHEET

RANSOMWARE DEFENSE ASSESSMENT

BENEFITS

- Identify assets at higher risk of being affected by ransomware
- Identify security weaknesses targeted by ransomware
- Identify relaxed access controls on file shares
- Recognize operational deficiencies in the management of ransomware tasks
- Receive highly actionable recommendations and guidance to mitigate ransomware attacks

Why Mandiant

Mandiant has been at the forefront of cyber security and cyber threat intelligence since 2004. Our incident responders are on the frontlines of the most complex breaches worldwide. We have a deep understanding of threat actors and their rapidly changing tactics, techniques and procedures (TTPs) by leveraging our combined adversary, machine and victim intelligence sources.

The Ransomware Defense Assessment was developed based on extensive experience responding to and remediating ransomware incidents and gathering threat intelligence on emerging and evolving ransomware.

Overview

The Mandiant Ransomware Defense Assessment evaluates the effectiveness of an organization's ability to prevent, detect, contain and remediate a ransomware attack. Mandiant experts assess technical and non-technical elements of your security program to determine how your team will respond to a ransomware attack.

Mandiant experts evaluate the technical impact a ransomware attack could have on your internal network, discover what data could be jeopardized or lost and test the strengths and weaknesses of your security controls' ability to detect and respond to a ransomware attack.

Methodology

The Ransomware Defense Assessment includes documentation review, logging configuration analysis, deep-dive workshops, and real-world ransomware attack behavior simulations.

The Ransomware Defense Assessment focuses on four core ransomware competencies:

- **Security architecture.** The security technologies, controls and networks required to defend against a ransomware attack and continue business operations.
- **Response.** The capacities of an organization to quickly respond to and contain a ransomware attack.
- **Communications.** Internal and external communications processes used to deliver corporate messages to key stakeholders. Includes coordination with cyber insurance and legal counsel.
- **Recovery.** The processes and approach to remediate or recover from a ransomware attack.

Our simulations of real-world ransomware attack behavior:

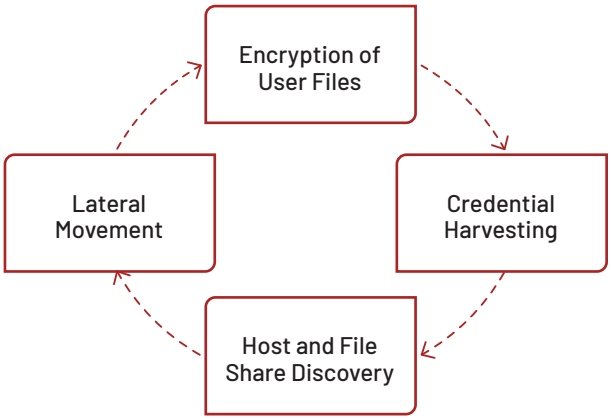
- Scan for Windows vulnerabilities exploited by ransomware
- Scan for accessible file shares which could be accessed by ransomware
- Simulate lateral movement of ransomware by attempting to exploit discovered vulnerabilities or re-use harvested credentials
- Test segmentation between networks to determine if ransomware can spread to other environments, such as:
  - Manufacturing and plant networks
  - Backup infrastructure networks
  - Retail networks
  - Other secure networks
- Simulate ransomware encryption behavior by using a custom, non-destructive ransomware emulation tool to mimic mass file encryption
- Perform techniques used by threat actors to deploy ransomware

Duration and deliverables

The Ransomware Defense Assessment typically takes one week. It can be delivered on-premise or remotely.

After the engagement, Mandiant provides a report that includes:

- Executive summary with strengths and areas for improvement
- Technical information about the testing process
- Detailed findings, categorized by severity
- Executive briefing



Learn more at **www.mandiant.com/consulting**

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.

MANDIANT