data sheet

Ransomware Resilience Review (R^3)

Mandiant will assess your current technical and procedural controls to defend against and recover from a sophisticated ransomware attack and provide strategic improvement plans over a three-week engagement

BENEFITS

- Understand your exposure related to ransomware attacks
- Reduce the likelihood, and impact of incidents
- Build consensus for required mitigation and improvements
- Prioritize budget and resources

Mandiant has been at the forefront of cyber security and cyber threat intelligence since 2004. Our incident responders have been on the frontlines of the most complex breaches worldwide. Mandiant's Ransomware Resilience Review (R3) draws on this expertise to deliver tailored, actionable recommendations that will help assess the internal security controls that protect against large scale ransomware attacks, reduce risk, and minimize the likelihood, impact, and cost of a security incident caused by remote work enablement technology.

Overview

As the risk of devastating ransomware attacks grow ever higher, organizations across all industry verticals are facing a threat to their day-to-day operation from opportunistic cyber criminals and nation-state actors. Companies of all sizes have been affected, some escaping with short-term standstill of business functions and million-dollar ransom demands, others only regain full business capacity months later, if ever. The threat actors we track are using increasingly complex tools and techniques, with more targeted attacks, and no indication of slowing down in the current climate. The increased sophistication and impact of these attacks has changed the defensive requirements and considerations needed of enterprise networks.

A Mandiant Ransomware Resilience Review (R3) is designed to give organizations a view of their current resilience to a sophisticated ransomware attack based on the security controls and policies in place, as well as present a report on the impact an attack of this type would have on your business. This is carried out via a technical and strategic assessment of the current setup. Organizations can leverage this review to validate the security posture of their internal security controls, while also ensuring that security best practices are followed as they relate to the availability of the data that the company requires to conduct business.

WHAT YOU GET

- **Recommendations Report:** You will receive a single report, which combines the findings identified within the Strategic and the Proactive Phases of the assessment.

  The report will focus on detailing those high impact issues and recommendations that are needed to ensure critical risks do not exist within the organization, due to the remote access solutions.

Our Approach

The first element of the assessment, The Strategic Phase, is based upon documentation reviews and workshops with key stakeholders to collect information around infrastructure, practices and policies. Comparing these against Mandiant best practice, a report on this strategic element will then be produced providing a series of actionable recommendations.

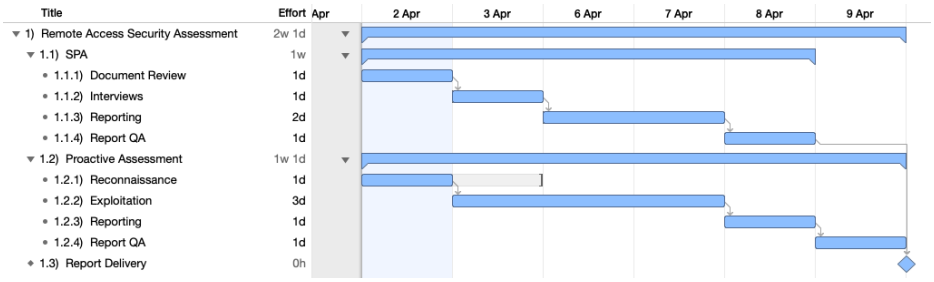
In the Proactive Phase, Mandiant Red Team consultants will work alongside the Strategic team to validate the findings that have been identified. This will involve conducting reconnaissance against the organization's Internet-facing systems using a list of remote access IP addresses and domains provided, others identified using open source intelligence (OSINT), and from Active Discovery. The discovery will focus on remote access solutions including VPN, remote desktop services, remote e-mail, collaboration tools (e.g. web conference, chat, and file sharing solutions) and virtual desktop infrastructure gateways, providing you with a list of all identified endpoints. After validation with the customer, Mandiant will perform manual targeted attacks against those systems with the aim of gaining access to your private networks, using techniques commonly employed by real threat actors and groups.

At the end of the assessment we will provide you with a single report that details the issues identified in both the Strategic and Proactive Phases, allowing you to prioritize remediation efforts.

The entire engagement can be conducted remotely, and meetings will be conducted using video conferencing.

Engagement Timeline

The current delivery time for these assessments is approximately 6 working days, if the Strategic and Proactive Phases are run in parallel. However, this timescale will shift if the reviews are run sequentially or a large number of remote access services are identified. The following is a sample timeline when the reviews are run in parallel:



Active vs Passive Reconnaissance

Passive reconnaissance involves activities that disclose information about the organisation without Mandiant making connections to your company's assets, instead we use third-party resources to harvest data (OSINT). Active reconnaissance will involve activities that require us to connect to your internet-facing assets in order to retrieve information. The following table provides some examples:

Activity	Passive	Active
DNS Reconnaissance	X	X
Subdomain Enumeration	X	
IP Space Discovery	X	
Host, Port and Service Enumeration	X	X
Directory Enumeration		X
Username Enumeration		X

FAQs

- **What this service is not?**
  It is not a vulnerability assessment of your complete Internet-facing infrastructure; it is specifically focused on existing and newly implemented remote access solutions on common ports that provide employees or third-parties access to your private networks.

- **We're worried that this assessment will impact our, already limited, VPN capacity.**
  Mandiant will carry out the strategic review alongside the reconnaissance phase of the proactive testing. This allows us to identify systems that may be under heightened stress and adjust our approach accordingly. We understand that availability of your resources is critical and so we will throttle any active scanning that we conduct and liaise with you to ensure that your remote access solutions are not 'red lining'.

- **What is considered out-of-scope**
  Mandiant will not:
  Conduct social engineering attacks (phishing, vishing, etc) against your staff
  Conduct comprehensive vulnerability scanning against your entire internet-facing infrastructure
  Target remote elements that are not access solutions such as websites, web service endpoints and similar exposed services
  Attempt to physically access your premises

How to Prepare for this Assessment

To support the Strategic Phase we will require access to documentation that describes and supports your remote access solutions, this could include:

- Remote Access Procedures, Processes, and Policies
- Access Management Policies and Procedures
- Password Policy
- Crisis Communications Plan
- Types of remote access logs in the SIEM
- Processes and Procedures for third party connectivity
- Remote access architecture diagrams (physical and logical)
- Any other relevant documents

We will also need to be able to interview members of the organisation that support the remote access solution. This could include representatives from:

- Information Security
- Networks
- Infrastructure
- Incident response (SOC/CIRT)
- Access Management
- Other suitable stakeholders

To assist with the Proactive red team Phase of the assessment we will need:

- A list of known internet-facing remote access services/solutions that you are aware of
- Written approval to conduct scanning and active attacks against those remote access solutions

To learn more, visit: **www.FireEye.com/services**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber-attacks.

FIREEYE™