Vulnerability Assessments

Mandiant offers a full range of application and infrastructure vulnerability assessments designed to identify and evaluate security vulnerabilities and recommend risk mitigation strategies.

Overview

An enterprise must maintain a robust and attack-resilient infrastructure in order to successfully defend against cyber attacks. Mandiant offers a complete portfolio of vulnerability assessment services that allow organizations to identify critical security vulnerabilities that attackers could exploit. These services help organizations improve their existing security posture while reducing the risk of a successful attack.

Mandiant’s approach

Mandiant’s methodology and tools are adapted to suit each client’s environment and objectives. Depending on the scope of the engagement, each application and infrastructure assessment can draw on a range of techniques that assess people, process, and technology:

People: Mandiant has utilized social engineering techniques including phone-based, USB drops and email phishing attacks to collect sensitive information such as user credentials, network information and passwords. Sometimes these activities involve spoofed web sites, help desk impersonations and implanting benign “malcode” that phones home.

Process: Mandiant has used a range of activities to identify policy and procedure deficiencies. This has included conducting compliance gap assessments against standards such as BS7799, ISO 27002 and HIPAA. Mandiant has also conducted PCI audits and software development lifecycle assessments.

Technology: Mandiant has conducted penetration tests and performed assessments across all major platforms including mobile devices, virtualized environments, SCADA environments, cloud deployments and traditional enterprise applications.

Actionable recommendations

Mandiant provides clients with actionable recommendations. All findings are rated based upon their risk, the probability of exploitation and the potential business impact. This allows clients to focus their efforts on addressing issues that matter the most.
Assessment services
Mandiant has led hundreds of complex computer intrusion investigations and has amassed a wealth of information on how attackers breach organizations, what type of data they seek, and how they steal this data. Armed with this knowledge, Mandiant helps organizations of all sizes and across all industries improve their security posture and reduce the risk of a security incident.

Infrastructure security
Mandiant has performed hundreds of external and internal infrastructure security assessments and identified thousands of critical vulnerabilities which exposed enterprises to external and internal attacks. Mandiant’s services include:

- External network vulnerability assessments and penetration tests
- Internal network vulnerability assessments
- Network architecture reviews
- Device configuration reviews (host and network)
- Wireless security assessments
- VoIP security assessments
- Active directory reviews
- Social engineering and physical penetration tests
- Insider threat assessments
- Custom services as requested

Application security
Testing applications at regular intervals, especially after important changes have been made to an application, is critical in order to maintain an attacker-resilient web presence. Mandiant has developed an extensive portfolio of application security assessments including:

- Web and client-server application security assessments
- Mobile application assessments
- Source code reviews for common programing languages
- Software development lifecycle (SDLC) reviews
- Application architecture assessments
- Custom services as requested

UNIQUE EXPERIENCE
Mandiant’s specialized skills and experience have enabled it to identify and assess security vulnerabilities in some of the most complicated and mission critical environments:

- Mobile device assessments
  Mandiant has performed mobile device assessments for some of the largest telecommunication carriers in the world. This work has included handset reviews, mobile device web site assessments and data center compliance assessments for the infrastructure that supports third party applications running on carrier networks.

- Web applications
  Mandiant has conducted reviews of large and complex custom web applications that consist of hundreds of dynamic pages and custom authentication mechanisms in highly fault tolerant configurations.

- Social engineering
  Mandiant has performed social engineering engagements that sent phishing emails to hundreds of client employees. Recipients were encouraged to click links or install attachments which then reported back to Mandiant servers. Mandiant summarized results for management so they could determine where to focus their future security awareness education.

- Security policies
  In one case, Mandiant evaluated the incident response capabilities of a European country. This involved working with the National Police, Ministry of Justice, the National Forensics Bureau and the European Union to understand current capabilities, identify their needs and develop a plan for instituting more rigorous and modern tools, processes and practices.