Mandiant

Datasheet

Threat Diagnostic

Benefits

- Uncover the threats targeting your organization and how to defend against them
- Validate the effectiveness of your security controls against threat capabilities
- Elevate and inform your security and risk management activities including: Red Teams, Vulnerability Management, Incident Response, Threat Hunting

Why Mandiant?

- Over the last decade, hundreds of organizations have worked with Mandiant as trusted advisors to build best practices for the consumption, analysis, and practical application of cyber threat intelligence (CTI)
- Organizations worldwide use our services to improve their security posture , gain a deeper understanding of threat activity and assess their defenses against real threats

Reveal your threats, secure your future

We understand the constraints most organizations are under when dealing with cyber threats. There are endless risks, and limited time to deal with all of them. That's why threat intelligence and effective threat prioritization is at the heart of a successful security program. But how do you get there?

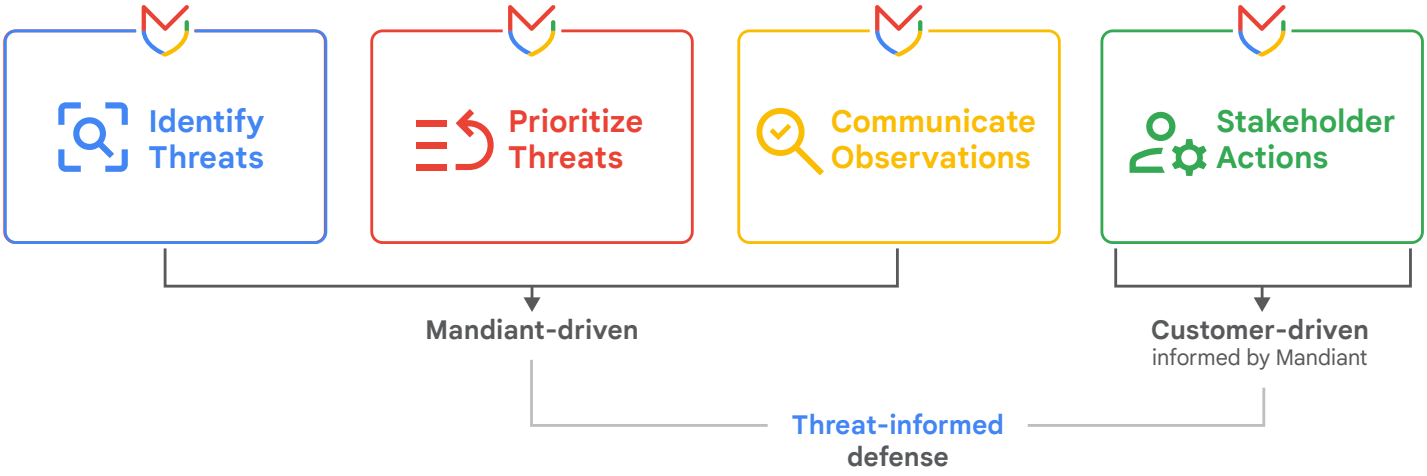
Effective threat prioritization requires a data-driven approach. Intelligence works well when it can be applied in the right place at the right time but how are you making these decisions today? If you are only using an external view as your deciding factor, you may be missing the most relevant information, which is organizational context. Context comes from a comprehensive understanding of the threat landscape. External and internal context is required to make better business decisions. So, how does Mandiant do this?

Threat Diagnostic is an intelligence-driven defense service that reveals the cyber threats targeting your enterprise, whether successful or unsuccessful. Through our proprietary methodology, Mandiant experts analyze your internal security telemetry against the external threat landscape and our global threat knowledge base. Observed threats are ranked based on their potential impact as well as your security posture. Findings are communicated to key stakeholders to ensure that defense gaps and vulnerabilities are identified, prioritized and addressed, improving organizational resilience.

By understanding how attackers operate, you can anticipate future attacks, and proactively implement targeted defenses. Threat Diagnostic enables you to connect seemingly disparate events, revealing your organization's true threat exposure.

Backed by Mandiant's proven methodology and extensive real-world expertise, you gain the targeted intelligence and informed insights necessary to build a proactive, and resilient defense strategy that is tailored to your organization's specific threat landscape.

Below is an overview of our methodology.



Successful Threat Diagnostic engagements are partnerships formed between our customers and Mandiant. We provide proactive identification, prioritization, and guidance for action across your security stakeholders. Engagements provide unparalleled threat context to empower your business to make informed security investments, communicate risk effectively, and optimize your security controls.

Delivery options are flexible with no technology deployment necessary and can be undertaken at the frequency that provides the most business value to your organization (annual, semi-annual or quarterly).

Annual or One Time

Enterprise Snapshot to Prioritize Threats

Semi-Annual (2x)

Understand Shifts in Threat Targeting

Quarterly (4x)

Highly Targeted Environments

Unlock deeper threat analysis and insights by combining Threat Diagnostic with your Google SecOps platform and Mandiant expertise for a stronger security posture.

At Mandiant, we understand every customer's security needs are unique, that's why our consultants tailor solutions to your specific requirements. Schedule a free consultation today to understand how we can help you reach your program goals.