

Mandiant + Cloudflare

Integrate third-party threat intel data from Mandiant with rich threat intelligence from Cloudflare One, all while improving your cyber risk posture

The modern threat landscape

More severe, increasingly sophisticated

IT and security teams are inundated with reports from threat intelligence and security vendors that do little to improve their actual security. Today's organizations are dealing with problems beyond threat severity, from risk identification and low cyber readiness to an overall lack of visibility.

Threat intelligence solves for these issues, with high quality telemetry and deep insights into the techniques and actors targeting an organization's industry — and even more, offering protection against threats with minimal to no involvement

Mandiant and Cloudflare's threat intel partnership enables organizations to understand and prepare for future risks, improve their response to attacks, and allocate security resources to protect high-business value assets.

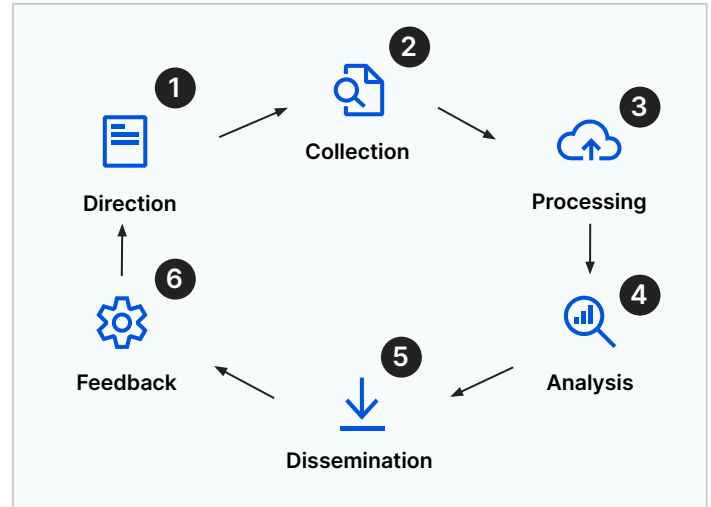


Figure 1: The threat intelligence lifecycle. 1. Define and refine the objectives. 2. Gather data from multiple sources, open and closed. 3. Evaluate reliability, collate from multiple sources. 4. Decide what this information means, assess its significance, and recommended an action. 5. Deliver the intelligence to the consumer. 6. Adjust as required.

Threat intelligence challenges



Risk identification

Leading indicators of risk to an organization are difficult to identify when thoughts, capabilities, and actions of adversaries are unknown.



Low cyber readiness

Organizations do not have the awareness and response tools required to prepare for attacks, affecting cyber readiness and response time.



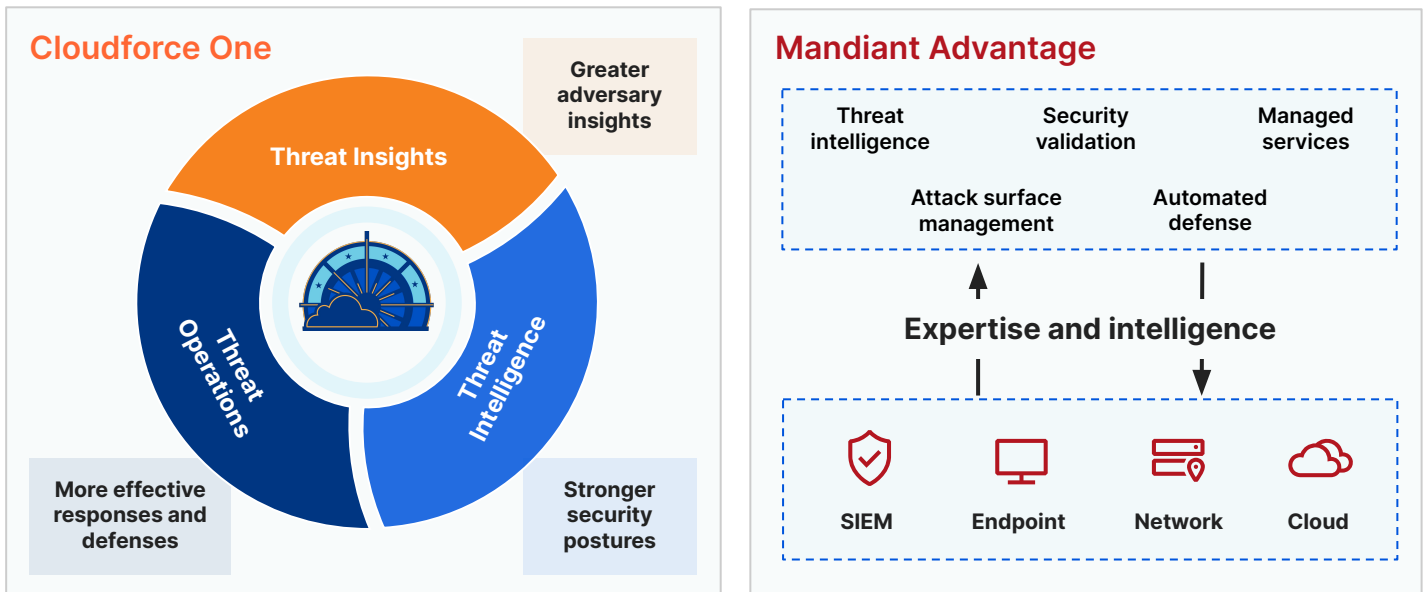
Lack of visibility

CISOs are not equipped with the right information to help them acquire or build technologies to support risk assessment and business use cases.

Integrate threat intelligence

Threat intelligence aims to provide specific information on threats and attackers. This includes the goals of a threat actor, conditions under which a specific threat is likely to exploit a vulnerability, organizational outcomes should a threat be successfully executed, and more.

Integrating Mandiant’s threat intel feeds with Cloudflare will make it easy for organizations to take advantage of active and relevant indicators of malicious activity from Mandiant’s extensive threat intelligence data. Cloudflare will take care of importing the data and refreshing it regularly to help protect organizations from the latest threats Mandiant sees on the frontlines.



Mandiant Advantage customers with a Threat Intelligence subscription can enter their API keys to leverage Mandiant’s most popular feeds like FQDN and IP address indicators of security threats and their related context throughout Cloudflare One products like our Secure Web Gateway (SWG), Magic Firewall, or our WAF.

“As cyber threats continue to rapidly evolve, organizations require up-to-date and relevant intelligence integrated with their preferred technology solutions to comprehensively protect their environments. Together, Mandiant and Cloudflare are enabling our mutual customers to better protect themselves from malicious actors that are active on the front lines right now.”¹

Robert Wallace, Senior Director, Strategy at **MANDIANT**



Focus on your core business with an improved cyber risk posture

Incident response partnership

As an incident response provider, Mandiant deals with active under attack situations daily, spending time and resources helping customers mitigate attacks and getting their network and web properties online. To increase the speed of selecting a security vendor, Mandiant has partnered with Cloudflare to enable rapid referral of organizations under attack.

Cloudflare and Mandiant's partnership enables businesses to focus on their core business by improving their cyber risk posture, powered by Cloudflare's network across 275+ cities, with 155 Tbps of network capacity and large suite of security solutions. To protect mutual customers from long-tail risks like ransomware or DDoS attacks, our cyber risk partnership with Mandiant meets organizations' expectations for rapid response, while providing businesses with industry-leading security and risk coverage.

Key takeaways for organizations with actionable threat intelligence

1

Stop common threats

Easily mitigate threats like DDoS or ransomware, which are rising in frequency, severity, and sophistication.

2

Mitigate attacks quickly

Obtain rapid referral to incident response providers when under attack to actively investigate and mitigate threats.

3

Improved security posture

Adopt security best practices and standards to proactively address potential vulnerabilities.

About Mandiant

Mandiant is recognized by enterprises, governments, and law enforcement agencies worldwide as the market leader in threat intelligence and expertise gained on the frontlines of cyber security. To make every organization confidently ready for cyber threats, Mandiant scales its intelligence and expertise through the Mandiant Advantage SaaS platform to deliver current intelligence, automation of alert investigation and prioritization and validation of security controls products from a variety of vendors.

About Cloudflare

Cloudflare, Inc. is on a mission to help build a better Internet. Cloudflare's platform protects and accelerates any Internet application online without adding hardware, installing software, or changing a line of code. Internet properties powered by Cloudflare have all web traffic routed through its intelligent global network, which gets smarter with every request. As a result, they see significant improvement in performance and a decrease in spam and other attacks.

1. <https://blog.cloudflare.com/bring-your-own-threat-feeds-with-cloudflare-one/>