Essential Intelligence Access

Benefits

- **Expertise:** Augment your team with access to world-class Mandiant intelligence analysts
- **Visibility:** Improve threat awareness with intelligence support tailored to your needs
- **Insight:** Accelerate security decisions with timely, expert-driven threat analysis
- **Prioritization:** Focus security efforts and mitigate risk through expert threat context and analysis

Why Mandiant?

- **For over a decade**, Mandiant has served as a trusted advisor to hundreds of organizations, helping them develop best practices for consuming, analyzing, and applying 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

Targeted Intelligence Expertise

Organizations of all sizes face the growing challenge of modern cyber attackers who are increasingly sophisticated, unpredictable, and persistent. Given the impact of these attacks, which exploit a range of vulnerabilities and attack vectors, organizations need to urgently and accurately understand adversary motivations, tactics, and objectives to effectively respond.

To address this challenge, Mandiant created Essential Intelligence Access (EIA). EIA connects organizations with our world-class intelligence experts, who deliver **targeted, actionable intelligence and personalized reporting** to enhance your security posture and build stronger resilience.

EIA **enhances your threat visibility**, allowing you to address the most relevant threats, and maximize operational efficiency.

Many organizations find it challenging to operationalize threat intelligence and synthesize it to fit their needs. Mandiant can help you transform **cyber threat intelligence (CTI)** into actionable insights that align with your specific organizational goals.


CTI Process Lifecycle
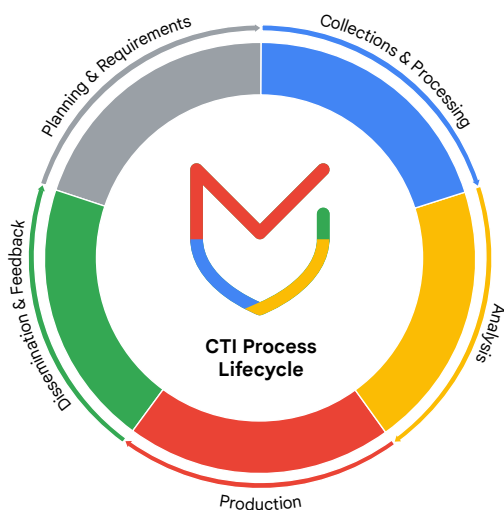
Good CTI should provide:

- **Context:** Understand the threat landscape
- **Foresight:** Anticipate future attacks
- **Actionability:** Enable informed and timely responses

Essential Intelligence Access Summary

Benefits	Description
Strategic Alignment	**Annual** planning session with Mandiant to align on CTI goals and use cases.
Intelligence Briefings	**Joint, multi-client** briefings covering the latest threat trends, malware and vulnerability analysis.
Proprietary Content	Access to exclusive Mandiant research, reports, and analysis, supplementing your existing threat intelligence feeds.
Takedown Requests	Targeted actions by Mandiant to neutralize external threats based on client requests (e.g., trademark infringement, social media impersonation, etc.)
Credential Monitoring	Alerts for potentially compromised credentials associated with your validated domain.
Streamlined Insights	Timely, analyst-compiled responses derived solely from Mandiant's curated intelligence holdings (not requiring new research or analysis).
Deep Dive Insights	In-depth, custom research, analysis, and expanded threat monitoring, tailored to address your organization's unique security challenges.

The true value of CTI lies in its ability to translate complex threat data into strategic advantage. This allows organizations to confidently navigate the ever-evolving cyber threat landscape. Unlock the full potential of threat intelligence by pairing EIA with **Google Threat Intelligence**.

Intelligence Operations
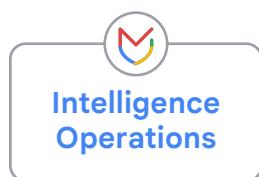
Essential Intelligence Access is part of Mandiant's Intelligence Operations group of subscriptions, offering personalized reporting and part-time expertise. For organizations requiring more comprehensive and dedicated support, we recommend exploring our **Advanced Intelligence Access (AIA)** service. AIA offers greater flexibility, agility and deeper intelligence integration to meet your specific mission needs. **Learn more** here.

At Mandiant, we understand that each organization has unique security needs, and we're ready to support you, wherever you are in your journey. Schedule a free consultation to discuss how we can help you achieve your program goals. **Contact us** today.