Google Cloud

Defend against novel attacks in real-time with Applied Threat Intelligence

The Challenge

Understanding the threat landscape and what it means for your organization is a cornerstone of modern threat detection, investigation, and response (TDIR). Security operations platforms typically include limited, or no threat intelligence that is integrated out-of-the-box to deliver **actionable outcomes** for security teams. As a result, many security teams struggle to understand which threats constitute real concern for their organizations, and what steps they need to take to **respond more effectively to the ever-changing threat landscape**.

Applied Threat Intelligence in Google Security Operations

Applied Threat Intelligence goes beyond a basic repository of indicators of compromise and adversary behaviors. It leverages Google's market-leading understanding of the threat landscape, including Mandiant's latest emerging threat intelligence, and **seamlessly applies them to each customer's unique environment**, The result? Prioritized and actionable outcomes that helps you piece together the story between events, alerts and your assets and users to stay ahead of the latest threats.

Without Applied Threat Intel	With Applied Threat Intel
Can't scale to enrich every event.	Use Google's hyper-scale infrastructure to ensure **every event is matched with the latest threat intelligence**.
Can't dedupe or automate data aggregation	See all of your matches **automatically aggregated**, in one **single pane of glass**.
Prioritize using only a static risk score	Leverage machine learning to prioritize threats **to your unique environment.**
Access a limited repository of open-source intelligence	Bring your own intelligence *and* get **market- leading intel** from Mandiant, VirusTotal and Google.
Painstakingly write all of your own rules	Use 3,500 single event and 200 multi-event **pre defined rules** that are **mapped to MITRE ATT&CK**.
Lack confidence in defense against advanced attackers	Defend against emerging threats with access to the latest **intelligence seen in active Mandiant IR**.

Google Cloud

With Applied Threat Intelligence, you can:

Understand threats

See every event, asset, and alert enriched with intelligence context.

Prioritize by risk

Leverage AI and ML to prioritize risks based on threat insights combined with how they apply to your unique environment.

Uncover novel threats early

Detect novel threats leveraging indicators from Google's intelligence and emerging threats from Mandiant incident response.

Automate response

Apply out-of-the-box playbooks to automate and speed response.

Improve defenses

Get deep insights into actors, motivations and behaviors targeting your organization so you can enhance your security.

Put Google's Market Leading Threat Intelligence to Work

Google Security Operations with Mandiant Threat Intelligence and VirusTotal tells you more about your adversaries than anyone else.

MANDIANT
NOW PART OF Google Cloud

- **Adversary Intelligence** curated by more than 500 **Mandiant** intelligence analysts tracking over 350 threat groups.
- **Emerging threat intelligence** collected from over 200,000 hours of **Mandiant** incident response each year.

VIRUSTOTAL

- **Crowdsourced intel** from over 3M users across 232 countries.
- The world's **largest observatory** with more than 50 billion files and 6 billion URLs.

Google Cloud

- Intelligence collected from the over 5B devices, over 3B email inboxes and scans over 60B URLs each day by **Google**.
- Phishing and malware protection with data from **Safe Browsing** resulting in 35% fewer victims.

30min From Mandiant frontlines to your data

20x More real-time detections

10x Faster investigations

The Google Security Operations platform offers a modern approach to threat detection, investigation and response (TDIR) with the speed, scale and intelligence of Google.

Ready to start your journey?
https://cloud.google.com/security/products/security-operations