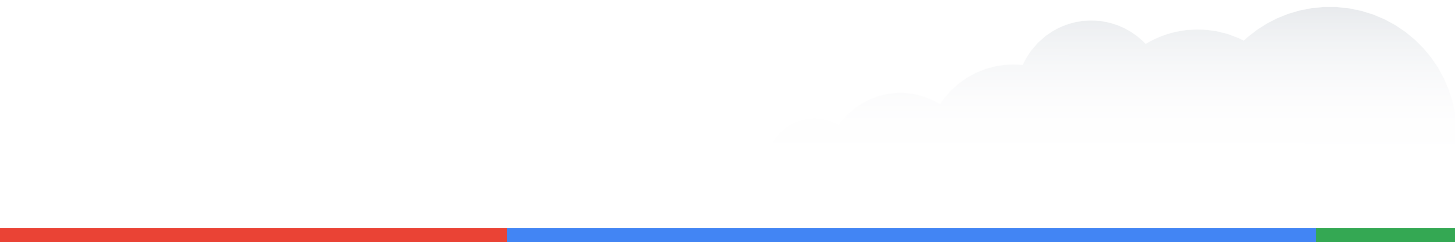


Staying ahead of the latest threats

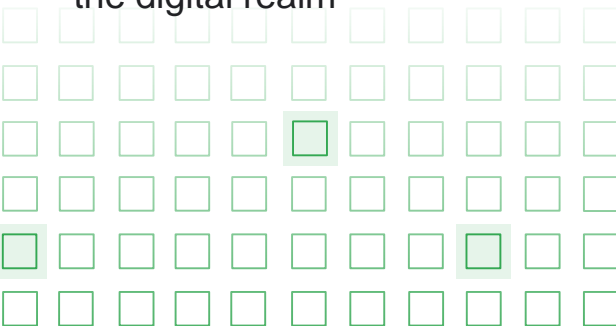
with **intelligence-driven** security operations



A decorative grid of 100 squares arranged in 10 rows and 10 columns. Most squares are light green with a thin green border. Three squares are highlighted with a darker green background and a thicker green border: one at row 2, column 9; one at row 3, column 5; and one at row 4, column 2.

Threat intelligence

A repository of evidence-based information about existing or potential threats and threat actors in the digital realm

A decorative grid of 100 squares arranged in 10 rows and 10 columns. Most squares are light green with a thin green border. Four squares are highlighted with a darker green background and a thicker green border: one at row 3, column 5; one at row 4, column 2; one at row 9, column 1; and one at row 9, column 9.

Threat actors



Tactics, Techniques
and Procedures (TTPs)

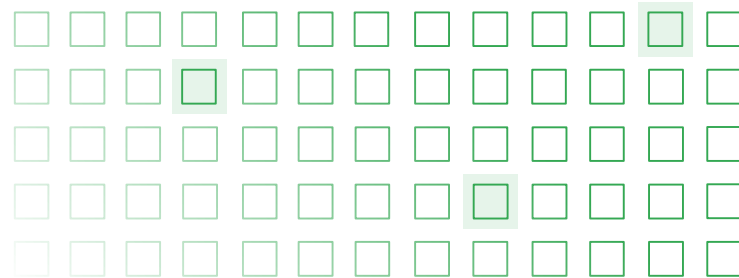


Indicators of Compromise (IOCs)



Vulnerabilities

Threat intelligence challenges



Data overload



Lack of context



Expertise gaps




Integration

A decorative grid of 100 squares arranged in 10 rows and 10 columns. Most squares are light blue, but four squares are highlighted with a darker blue border: one at row 2, column 4; one at row 3, column 1; one at row 4, column 9; and one at row 5, column 5.

SIEM

A centralized platform for security teams to collect, analyze, and respond to security-related data and events from various sources across an organization's IT infrastructure.

A decorative grid of 100 squares arranged in 10 rows and 10 columns. Most squares are light blue, but four squares are highlighted with a darker blue border: one at row 2, column 3; one at row 3, column 9; one at row 4, column 6; and one at row 5, column 2.

Log collection and aggregation



Correlation and analytics



Detection and alerting



Investigation



Response

SIEM challenges



**Unaware of
the threat
landscape**



**No outcomes
out of the box**



DIY



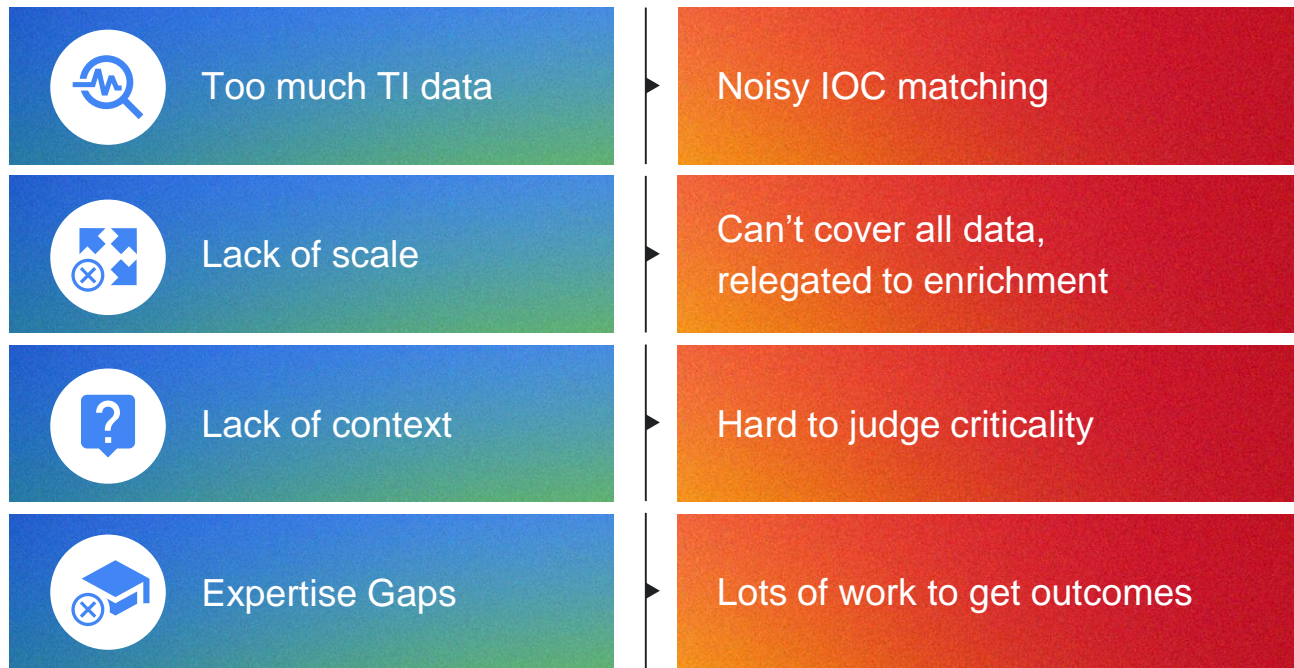
Scalability

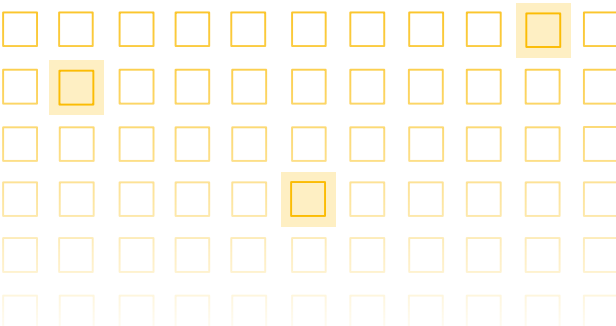


**Manual
processes**

Combining SIEM + TI

The worst of both worlds?





Applied threat intelligence



Extensive understanding of the threat landscape



Continuous analysis of all data against the latest frontline intelligence



“Post-processing” using advanced techniques for higher fidelity



New insights about threat actors are turned into behavioral detections and outcomes

Google provides unrivaled global threat visibility



50B+ files

Across thousands of file formats for
all operating systems

1.5B+

Sandbox
reports

2M

Analyses
per day



232

ISO COUNTRIES
submitting files



3M+

MONTHLY USERS
sourcing data

6B+ URLs

6M+ URL analyses
per day

5B+

Domains

170B+

pDNS
Resolutions

45/71

70+ Antivirus
90+ URL blocklists
20+ Sandboxes
30+ Crowdsourced
(YARA, SIGMA, IDS) repos
100K+ Crowdsourced rules

1000+

Total employees
supporting IR

300+

Incident response
consultants

1100+

Engagements per
year

400k

Incident investigation
hours per year

500+

Researchers &
analysts

30+

Languages spoken

300+

Tracked threat
groups

53+

Countries with incident
response engagements

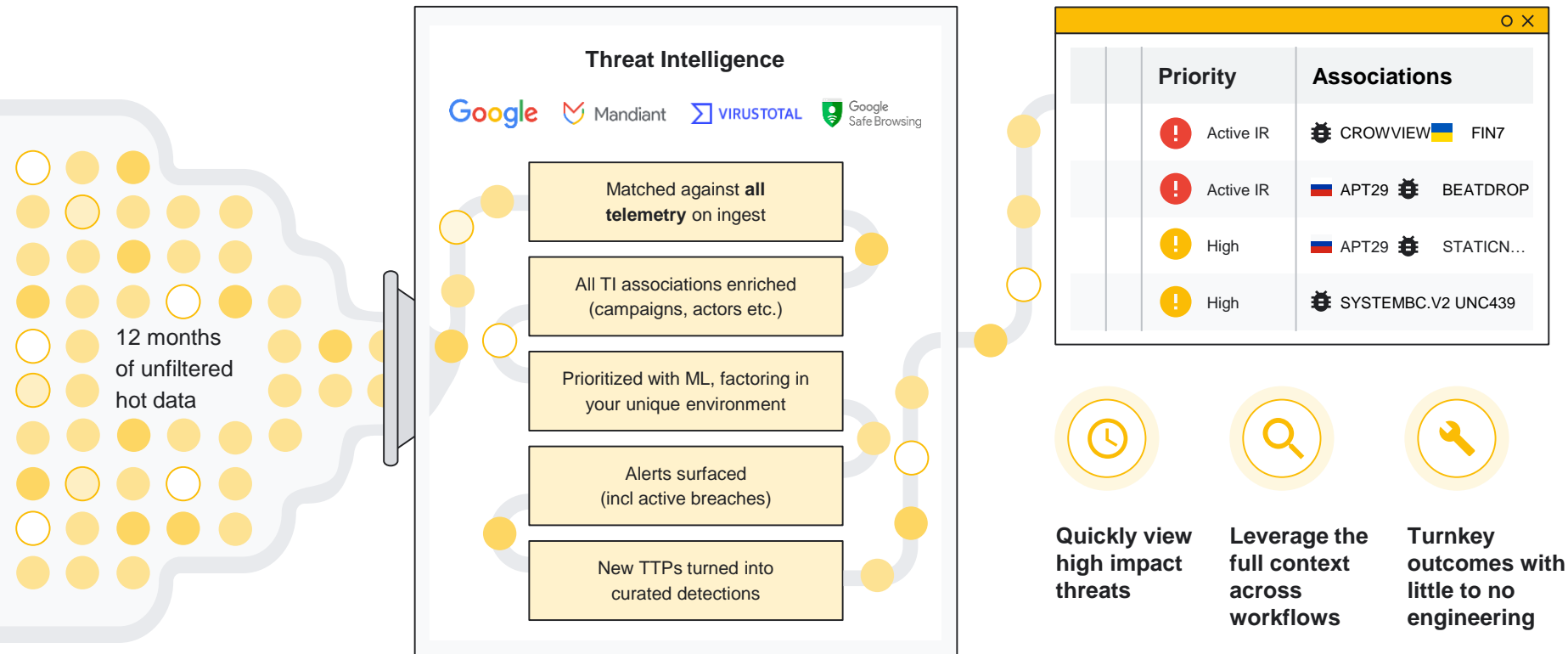
5 Billion

Google Safe Browsing user devices
protected each day from malware and
social engineering

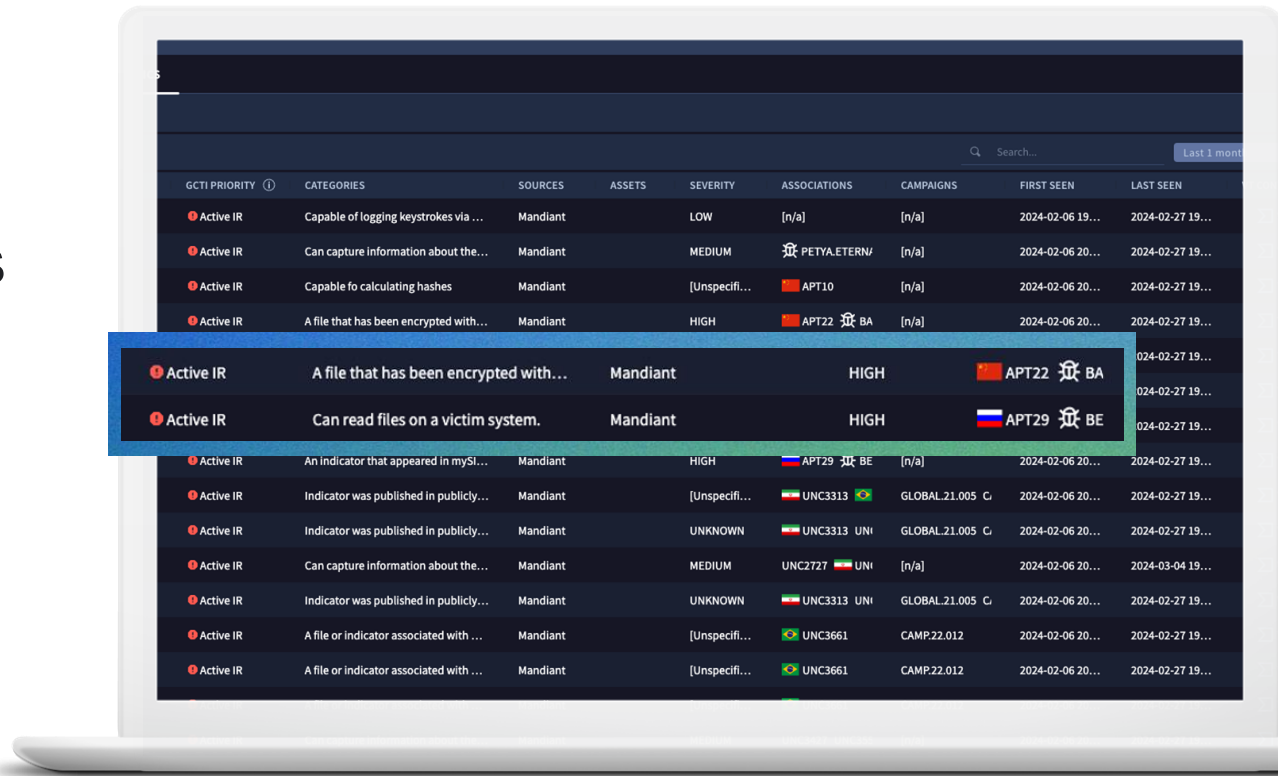
1.5 Billion

Active Gmail users protected against
phishing, malware, and spam through
embedded security monitoring

Applied threat intelligence: How it works



Surface indicators from the latest frontline incident response engagements



GCTI PRIORITY ⓘ	CATEGORIES	SOURCES	ASSETS	SEVERITY	ASSOCIATIONS	CAMPAGNS	FIRST SEEN	LAST SEEN
Active IR	Capable of logging keystrokes via ...	Mandiant		LOW	[n/a]	[n/a]	2024-02-06 19...	2024-02-27 19...
Active IR	Can capture information about the...	Mandiant		MEDIUM	PETYA.ETERN/	[n/a]	2024-02-06 20...	2024-02-27 19...
Active IR	Capable fo calculating hashes	Mandiant		[Unspecifi...	APT10	[n/a]	2024-02-06 20...	2024-02-27 19...
Active IR	A file that has been encrypted with...	Mandiant		HIGH	APT22	BA	2024-02-06 20...	2024-02-27 19...
Active IR	A file that has been encrypted with...	Mandiant		HIGH	APT22	BA	2024-02-06 20...	2024-02-27 19...
Active IR	Can read files on a victim system.	Mandiant		HIGH	APT29	BE	2024-02-06 20...	2024-02-27 19...
Active IR	An indicator that appeared in mySI...	Mandiant		HIGH	APT29	BE	2024-02-06 20...	2024-02-27 19...
Active IR	Indicator was published in publicly...	Mandiant		[Unspecifi...	UNC3313	GLOBAL.21.005 C	2024-02-06 20...	2024-02-27 19...
Active IR	Indicator was published in publicly...	Mandiant		UNKNOWN	UNC3313	GLOBAL.21.005 C	2024-02-06 20...	2024-02-27 19...
Active IR	Can capture information about the...	Mandiant		MEDIUM	UNC2727	GLOBAL.21.005 C	2024-02-06 20...	2024-03-04 19...
Active IR	Indicator was published in publicly...	Mandiant		UNKNOWN	UNC3313	GLOBAL.21.005 C	2024-02-06 20...	2024-02-27 19...
Active IR	A file or indicator associated with ...	Mandiant		[Unspecifi...	UNC3661	CAMP.22.012	2024-02-06 20...	2024-02-27 19...
Active IR	A file or indicator associated with ...	Mandiant		[Unspecifi...	UNC3661	CAMP.22.012	2024-02-06 20...	2024-02-27 19...

Understand threat actor associations related to the IOC

The screenshot displays a threat intelligence platform interface. At the top, a navigation bar includes a 'Back to Breach Analytics' link, a long alphanumeric hash (HASH_SHA256: 0084698bf5926c0673a745833521fc5d050cd30feb03eb6c0e0b92826245066), and a 'VT Context (42/70)' link. Below this, a status bar indicates 'Status: Match' and 'IR Status: This Indicator was in an Active IR 1 month ago'.

The main section is titled 'INDICATOR DETAILS' and contains a table with the following data:

Property	Value	Source	Discovery Info
GCTI Priority	Active IR	Mandiant	Mandiant Discovered
IC-Score	100 (Show Details)	Capable of executing constructing (ccpattine) a mutex	Mandiant Last Updated

Below the table, there are two tabs: 'EVENTS (16)' and 'ASSOCIATIONS (2)'. The 'ASSOCIATIONS (2)' tab is selected, showing two entries:

- THREAT ACTOR**
APT22
APT22 (BAE), APT22 (Palo Alto Networks), Barista Team, Bronze Olive (Dell SecureWorks), Calypso (Positive Technologies), Chamelgang (Positive Technologies), Eartheistries (Trend Micro), Famoussparrow (ESET), Ghostemperor group (Symantec), Wicked Panda (CrowdStrike)
Target Industries: Aerospace & Defense, Chemicals & Materials, Construction & Engineering, Education, Energy & Utilities, Governments, Healthcare, Hospitality, Legal & Professional Services, Manufacturing, Me...
APT22 is a Chinese cyber espionage group that frequently uses strategic web compromises to exploit targets of interest. APT22 actors have identified vulnerable public-facing web servers on victim networks and uploaded web gain access to target networks, but these instances appear to be less common.
- MALWARE**
BASELESS
Preshin
Target Industries: Aerospace & Defense, Automotive, Chemicals & Materials, Construction & Engineering, Healthcare, Manufacturing, Media & Entertainment, Retail, Technology, Transportation
BASELESS is an HTTP backdoor capable of file transfers, command execution, and file downloads. The malware retrieves its C2 information from a resource section created when a dropper installs the backdoor. The malware is retrieve information from protected storage such as proxy credentials and auto-complete passwords. The malware is proxy aware.

Leverage “Intel-driven” detections to prioritize

The screenshot displays a security dashboard interface. At the top, the 'Alerts & IOCs' section shows a breadcrumb trail: '← Back to Breach Analytics | HASH_SHA256 : 0084698bf5926c0673a745833521fc5d050cd30feb03eb6c00eb92826245066 | VT Context (42/70)'. Below this, the 'Indicator Details' section provides information about the indicator: 'GCTI Priority' is 'Active IR', 'Type' is 'HASH_SHA256', 'Source' is 'Mandiant', 'IC-Score' is '100 (Show Details)', and 'Category' is 'Capable of executing constructing (creating) a mutex.'.

The 'EVENTS (16)' and 'ASSOCIATIONS (2)' sections are visible. The 'EVENTS' section is expanded, showing a table of events:

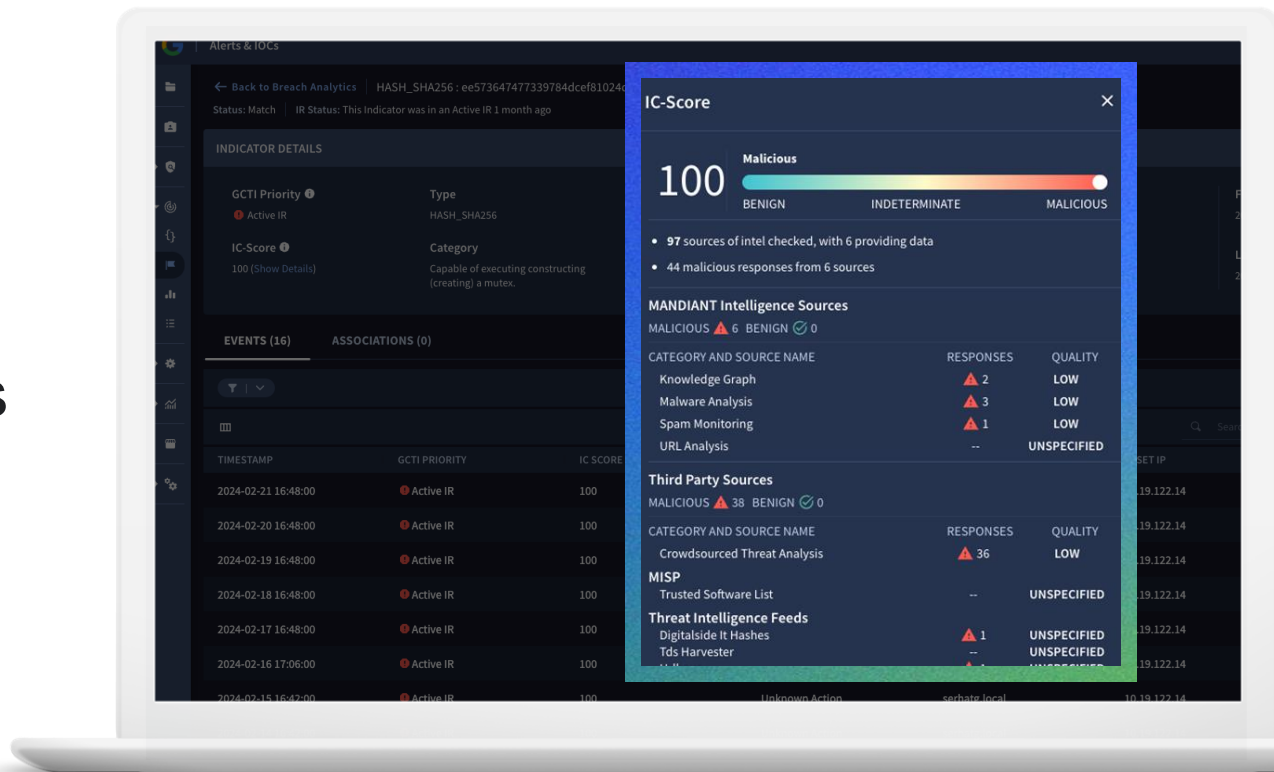
TIMESTAMP	GCTI PRIORITY	IC SCORE	DEVICE ACTION
2024-02-21 17:06...	Active IR	100	Unknown Action
2024-02-20 17:06...	Active IR	100	Unknown Action
2024-02-19 17:06...	Active IR	100	Unknown Action
2024-02-18 17:06...	Active IR	100	Unknown Action
2024-02-17 17:06...	Active IR	100	Unknown Action
2024-02-16 17:06...	Active IR	100	Unknown Action
2024-02-15 17:06...	Active IR	100	Unknown Action

An 'Event Viewer' overlay is shown on the right, displaying a timeline of observations leading to the prioritization of the indicator. The observations are:

- IC-Score is 100
- Indicator is not yet common knowledge in the security community
- Indicator is not commonly observed by Mandiant
- Indicator sourced from active IR
- Indicator is not a known internet scanner
- Network flow does not appear to be outbound
- Event indicates activity was successful

The 'Conclusion' section shows a red exclamation mark icon and the text 'Active IR'.

Full transparency
in how indicator
confidence scores
are calculated



Enable curated detections developed by Google experts to address the latest emerging threats

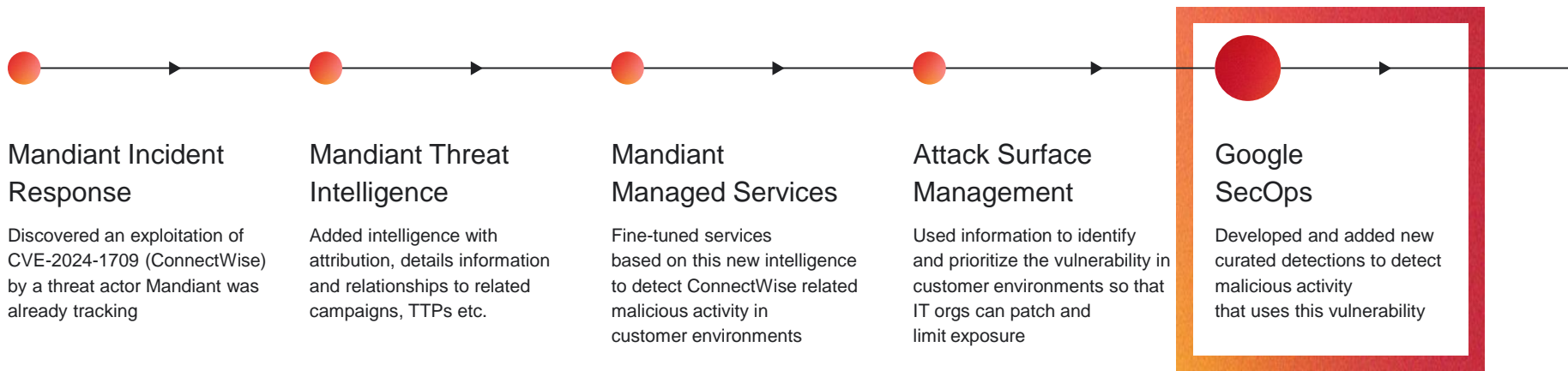
The screenshot displays the 'Rules & Detections' dashboard in Google Cloud. The top navigation bar includes 'RULES DASHBOARD', 'RULES EDITOR', 'CURATED DETECTIONS' (selected), and 'EXCLUSIONS'. The main content area is divided into three sections: '77/78 ENABLED RULE SETS' (As of today), 'MOST ACTIVE RULES' (Over last 7 days), and 'MOST ACTIVE RULE SETS' (Over last 7 days). Below these sections are tabs for 'RULE SETS' and 'DASHBOARD'. A table of curated detections is highlighted with a blue border, showing columns for NAME, LAST UPDATED, ENABLED RULES, ALERTING, CAPACITY, and MITIGATION. The table lists four rule sets: 'Applied Threat Intelligence - Curated Prioritization', 'Active Breach Priority Host Indicators', 'Active Breach Priority Network Indicators', and 'High Priority Host Indicators'. Below the table, there are links to 'Linux Threats', 'Managed Detection Testing', 'Risk Analytics for UEBA', and 'Windows Threats'.

NAME	LAST UPDATED	ENABLED RULES	ALERTING	CAPACITY	MITIGATION
Applied Threat Intelligence - Curated Prioritization • 4 Rule sets					
Active Breach Priority Host Indicators	2024-02-27	P B	P B	0	Non
Active Breach Priority Network Indicators	2024-02-27	P B	P B	0	Non
High Priority Host Indicators	2024-02-27	P B	P B	0	Non
High Priority Network Indicators	2024-02-27	P B	P B	0	Non

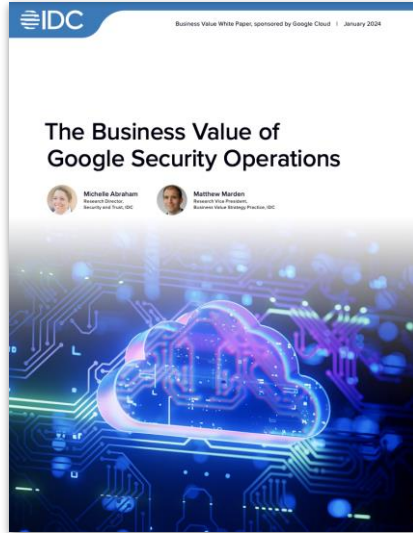
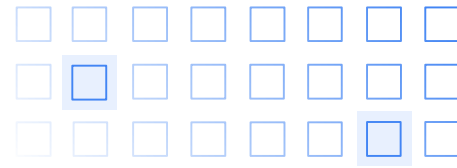
Leverage applied threat intelligence constructs in search and detection authoring

```
rule fusion_feed_example_principal_process_file_md5 {  
  meta:  
    rule_name = "File Hash - Applied Threat Intelligence"  
    description = "Matches file hashes against the Applied Threat Intelligence Fusion Feed."  
  
  events:  
    // Filter on Mandiant Fusion Intel from Chronicle Entity Context Graph  
    $context_graph.graph.metadata.product_name = "MANDIANT_FUSION_IOC"  
    $context_graph.graph.metadata.vendor_name = "MANDIANT_FUSION_IOC"  
    $context_graph.graph.metadata.entity_type = "FILE"  
    $context_graph.graph.metadata.source_type = "ENTITY_CONTEXT"  
  
    // Get context join  
    $ioc = $context_graph.graph.entity.file.md5  
    $ioc = $e1.principal.process.file.md5  
  
    // Group by IOC every 1 hour  
    match:  
      $ioc over 1h  
  
    outcome:  
      // Extract the Mandiant Automated Intel confidence score of maliciousness  
      $confidence_score = max(if($context_graph.graph.metadata.threat.verdict_info.source_provider = "Mandiant  
Automated Intel", $context_graph.graph.metadata.threat.verdict_info.confidence_score, 0))  
  
      // Extract the status of the indicator as seen in a breached environment  
      $breached = max(if($context_graph.graph.metadata.threat.verdict_info.pwn = true, 1, 0))  
  
      // Intermediary outcome variable to combine conditions of intelligence extracted in the previous outcome  
      $matched_conditions = if($confidence_score >= 80 AND $breached = 1, 1, 0)  
  
    condition:
```

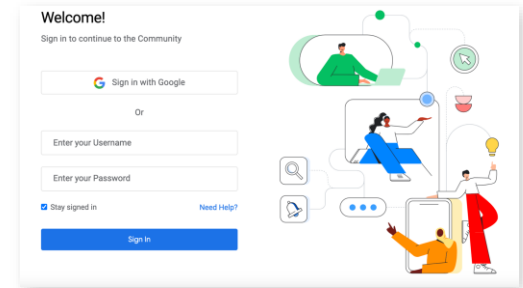
Applied threat intelligence in the real world - ConnectWise



Additional Resources



 Google Cloud Security



Visit
cloud.google.com/security/sec-ops



Visit
[BrightTalk Resource Section](#)



Visit
[googlecloudcommunity.com/gc/
Google-Cloud-Security](https://googlecloudcommunity.com/gc/Google-Cloud-Security)

Thank you

Google Cloud
Security

