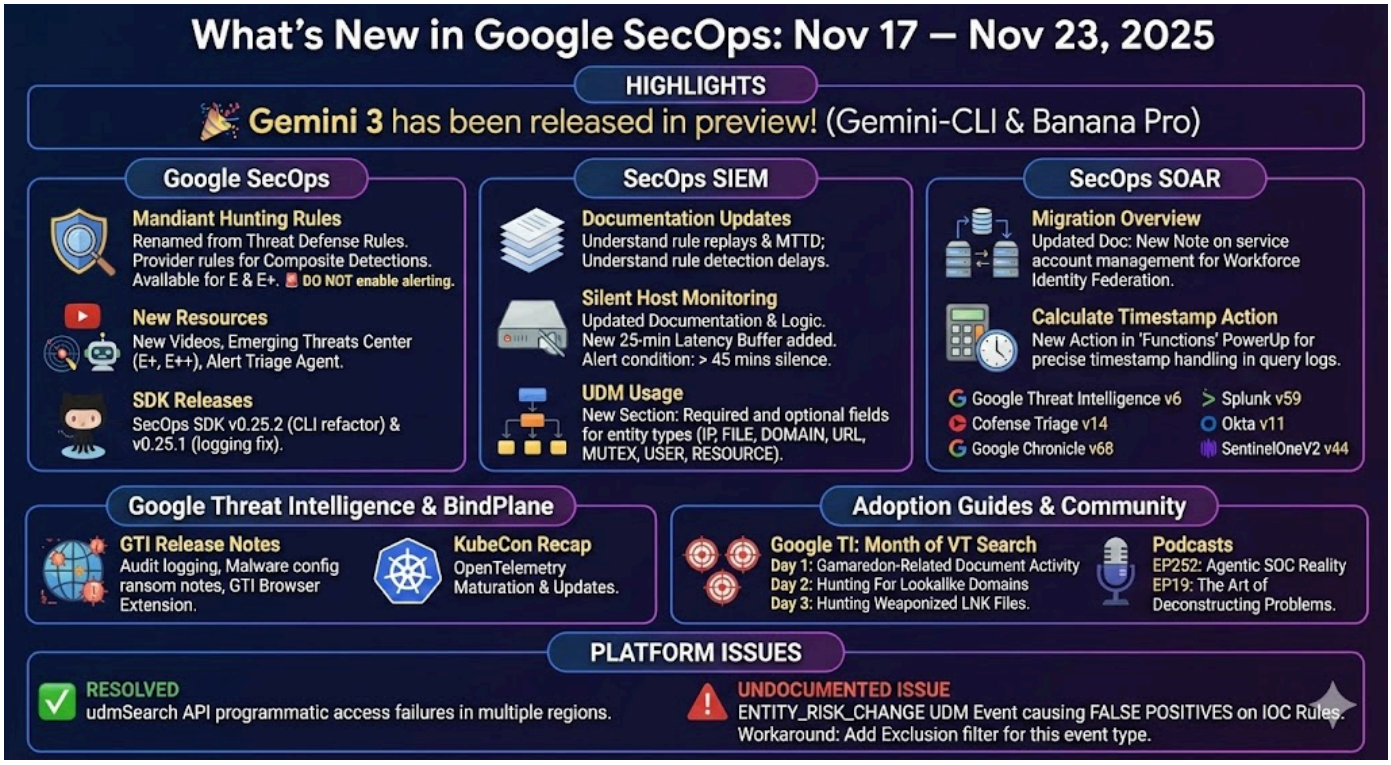
Google Chronicle

What is Google Chronicle?

- **Google Chronicle** is the former name of **Google Security Operations (Google SecOps)** — a **cloud-native cybersecurity platform** from Google Cloud.
- It provides **SIEM + SOAR + Threat Intelligence + AI-driven analytics** to help SOC teams **detect, investigate, and respond to cyber threats at massive scale**.



It's a Modern SIEM + SOAR

- **SIEM** = collects & searches all your security logs
- **SOAR** = automatically responds to attacks (like blocking an IP)

Key Features and Components

- **Runs 100% on Google Cloud** – no hardware, no servers to manage
- **Can store YEARS of data at very low cost** Old tools charge you for every GB you store → very expensive **Chronicle charges only when data enters**, not for keeping it → super cheap for big companies
- **Searches billions of events in seconds** You can ask in plain English: "Show me all failed logins from India in the last 6 months" → answer comes instantly!
- **Uses AI & Google's own threat intelligence** It knows about new viruses and hacking techniques even before you hear about them (thanks to VirusTotal, owned by Google)
- **Detects hidden attacks automatically** Finds weird behavior that normal tools miss (example: someone logging in at 3 AM from another country)
- **Helps you investigate like a movie** Click one alert → see the full story timeline of the attacker (like a video replay)
- **2024 Update: Now called "Google Security Operations" (Google SecOps)** Same product, new name, more AI features using Gemini (Google's AI)

How Chronicle (Google Security Operations) Works

- Google Chronicle is a **cloud-native SIEM** that collects logs from your environment, normalizes them into the **Unified Data Model (UDM)**.
- enriches them with **Threat Intelligence**, stores them cheaply for long periods, and allows **lightning-fast search + real-time alerting + automated response**.

Chronicle Working Flow

Below is the **official SOC workflow** in simple terms.

1. Log Ingestion Layer

Chronicle receives logs from many sources:

- Windows Event Logs
- Sysmon
- EDR tools (CrowdStrike, Defender ATP, SentinelOne)
- Firewalls (Palo Alto, Fortinet, Cisco)
- Proxy logs
- VPN logs
- Cloud logs (GCP, AWS, Azure)
- Email security
- DNS logs

Logs can be sent using:

- Google Ingestion API
- Forwarders
- Connectors
- Cloud-native integrations

Everything enters Chronicle in its raw format.

2.Normalization Layer (UDM Mapping)

Chronicle automatically converts all raw logs into the **Unified Data Model (UDM)**.

Examples:

Raw Field	UDM Field
Image	principal.process.file.name
ParentImage	principal.process.parent.file.name
CommandLine	principal.process.command_line
DstIP	network.dst.ip
SHA256	target.file.sha256

No parsers, regex, or manual parsing needed.

3. Enrichment Layer (TI + Context)

Chronicle enriches every event with:

✔️ VirusTotal

- Hash reputation
- Domain/IP analysis
- Global detection count

✔️ Mandiant Threat Intelligence

- APT group mapping
- Malware families
- MITRE ATT&CK context

✔️ Google Internal TI

- New phishing domains
- Zero-day indicators
- Rare global events

✔️ Additional Context

- Geo-IP location
- WHOIS info
- User/host context
- Prevalence score

This enrichment makes investigations **much faster**.

4. Storage Layer (Petabyte Scale Storage)

Chronicle stores all enriched UDM events in **Google Cloud's scalable backend**.

Benefits:

- Can store **months or years** of data
- No extra cost for storage
- Extremely fast lookup

Chronicle treats data like **Google Search** treats the internet.

5. Search & Analytics Layer

The SOC analyst uses:

✔️ UDM Search

```
principal.process.file.name = "powershell.exe"
```

✔️ Natural Language Search

"Find all failed logins from Russia last 90 days"

✔️ IOC Search

```
target.file.sha256 = "<hash>"
network.dst.ip = "<ip>"
```

✔️ **Entity View**

Click a domain/IP to see:

- History
- Alerts
- Affected hosts
- WHOIS
- VT context

Search returns results in **seconds**, no matter how large the dataset.

6.Detection Layer (YARA-L Rules)

Chronicle evaluates all logs with:

✔️ **Google-built detections**

✔️ **Mandiant-built detections**

✔️ **Custom YARA-L rules**

Example:

```
rule Suspicious_PS_Encoded {
  events:
    $e.principal.process.command_line = /-enc/
}
```

If a rule matches → **Alert generated**.

7.Alerting & Incident Layer

Alerts include:

- Severity
- MITRE mapping
- Full attack timeline
- Asset info
- Enrichment
- Related alerts

SOC analysts can:

- Investigate
- Assign severity
- Open cases
- Pivot deeper

This is where investigations begin.

8.Investigation Layer (Timeline + Graph)

Analysts use:

✔️ Timeline view

Shows:

- Processes
- Commands
- Connections
- Files
- User activity

✔️ Entity Graph

Visual mapping of attack flow:

- Domain → file → process → C2 → persistence

Helps reconstruct the entire attack chain.

9. SOAR Response Layer (Automation)

Chronicle SOAR (formerly Siemplify) automates responses:

- Block IP/domain
- Disable user
- Isolate host
- Quarantine file
- Create tickets
- Notify teams

Includes:

✔️ Playbooks

Automation workflows like:

1. Extract IOC
2. Check VirusTotal
3. Check Mandiant
4. Query SIEM
5. If malicious → isolate host

✔️ Case Management

Track the full investigation lifecycle.

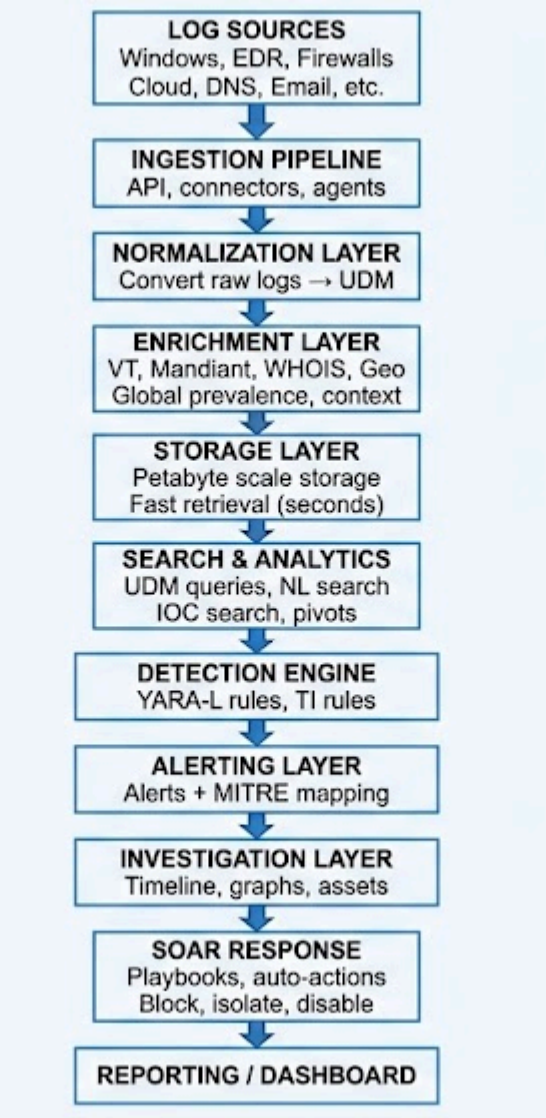
10.Reporting & Dashboards Layer

Chronicle provides dashboards for:

- MITRE ATT&CK coverage
- Detection trends
- Endpoint alerts
- Cloud security alerts
- SOC performance
- Risk scoring

FULL END-TO-END FLOW DIAGRAM

This is a complete flow model used in SOC training.



Integration & Enterprise Use Cases

Google SecOps integrates with:

- **AWS, Azure, GCP**
- Firewalls (Palo Alto, Fortinet, Cisco)
- EDR/XDR platforms (CrowdStrike, SentinelOne, Defender ATP)
- Identity providers (Okta, AD)
- Email security tools
- Network telemetry
- Containers & Kubernetes logs

Used by SOC teams for:

- Threat hunting
- Incident response
- Compliance monitoring
- Behavior analytics
- Attack surface visibility

Why Organizations Choose Google SecOps

- Unlimited scale
- Cost-effective log ingestion
- Powerful automation
- Built-in advanced threat intelligence
- AI-driven response and investigation
- Very fast search & correlation
- Cloud-native → zero maintenance overhead

Importance of Google Chronicle

1. Understanding UDM (Unified Data Model)

Chronicle **converts every log into a common format** called UDM.
This is the **#1 skill** for a SOC Analyst using Chronicle.

Why UDM matters?

- You learn **one search language** for all tools (Windows, Sysmon, EDR, Firewall, Cloud logs)
- Detections work on **all log sources**
- Threat hunting becomes predictable and easy

Artifact	UDM Field
Process Name	principal.process.file.name
Parent Process	principal.process.parent.file.name
Command Line	principal.process.command_line
Source IP	network.src.ip
Destination IP	network.dst.ip
File Hash	target.file.sha256

Example UDM Mappings: If you master these → **you can investigate ANY alert quickly**.

2. Core Chronicle Searches Every SOC Analyst Must Know

- **Process Execution**

```
metadata.event_type = "PROCESS_LAUNCH"
principal.process.file.name = "powershell.exe"
```

- **Suspicious Parent → Child (Phishing → Payload)**

```
principal.process.parent.file.name = "winword.exe"
principal.process.file.name = "powershell.exe"
```

- **Outbound C2 Traffic**

```
metadata.event_type = "NETWORK_CONNECTION"
network.dst.ip = "*"
network.bytes_sent < 500
```

- **File Creation**

```
metadata.event_type = "FILE_CREATION"
```

- target.file.path = "*\\AppData*"

- **Failed Logins from Unusual Country**

```
security_result.action = "FAILED_LOGIN"
principal.ip_geo.country != "India"
```

These will cover **80% of your SOC investigation use cases**.

3. Chronicle Auto-Enrichment — HUGE Power for SOC

Chronicle automatically enriches logs with:

- **VirusTotal Malware Score**

Auto-checks hashes → shows malicious/unknown verdict.

- **Mandiant Threat Intel**

Shows if an IP/domain is associated with:

- APT Groups
- Zero-day exploitation
- Malware campaigns

- **Geo-location + WHOIS**

Auto-enriched for all IPs.

- **Asset Context**

Shows device info, user context, past alerts.

SOC analyst doesn’t waste time manually checking external tools.

4. Why Chronicle Searches Are Faster for SOC Analysts

Legacy SIEM:

- Running a 90-day search = **2–10 minutes**
- Large queries sometimes fail

Chronicle:

- Searches **1–12 months of logs instantly**
- Built on the same architecture as Google Search / BigQuery

This dramatically improves:

- **Investigation speed**
- **Threat hunting productivity**
- **Incident response timing**

5. Chronicle Attack Timeline

When you open an alert, Chronicle shows a **visual timeline**:

- Process tree
- Network flows
- Files created
- Registry edits
- Related alerts
- Lateral movement
- C2 beacons
- Persistence techniques

This is like watching a **movie replay** of the attacker.

SOC analysts LOVE this because:

- No manual log correlation
- No combing through raw Windows logs
- You instantly see the whole attack path

6. Top 10 Chronicle Detections Used in Real SOCs

1. PowerShell Download Cradle

powershell.exe IEX (New-Object Net.WebClient).DownloadString

2. Cobalt Strike Beacon Behavior

Low bytes sent + low periodic beaconing.

3. Suspicious Parent Chain

word → powershell → rundll32 → network connection.

4. RDP Brute-force

Hundreds of failed logins from same IP.

5. Rare External Domains

Connections to never-seen-before domains.

6. DNS Tunneling

Excessive TXT queries or long subdomains.

7. LOLBAS Execution

Using built-in Windows binaries for attacks, e.g. mshta.exe, regsvr32.exe, wmic.exe.

8. Credential Access

lsass.exe access attempts by unusual processes.

9. Privilege Escalation

whoami /priv, secedit, token manipulation.

10. Persistence

Tasks created via schtasks /create.

These detections are applied over UDM → **low noise + accurate**.

7. YARA-L — Writing Detections Like a Professional SOC Analyst

YARA-L is Chronicle's detection language.

Example: Suspicious PowerShell

```
rule Suspicious_PowerShell_Execution
{
  events:
    $e.metadata.event_type = "PROCESS_LAUNCH"
    $e.principal.process.file.name = "powershell.exe"
    $e.principal.process.command_line =
/-enc|FromBase64String|IEX/
}
```

Example: Rare External Domain Contact

```
rule Rare_Domain_Connection
{
  events:
    $e.metadata.event_type = "NETWORK_CONNECTION"
    $e.network.domain.first_seen = true
}
```

SOC analysts who know YARA-L are considered **high-value**.

8. Use Cases for SOC Analysts (Exactly What You Need)

Threat Hunting

Find anomalies → Rare processes, rare domains, suspicious commands.

Incident Response

Build timeline, pivot across related artifacts, identify root cause.

Lateral Movement Tracking

Search for RDP, SMB, PsExec usage.

Malware Analysis

Check file hash → VirusTotal → see detection families.

Detection Engineering

Write YARA-L rules → deploy to detection pipeline.

Compliance & Reporting

Chronicle automatically keeps **years of logs**.

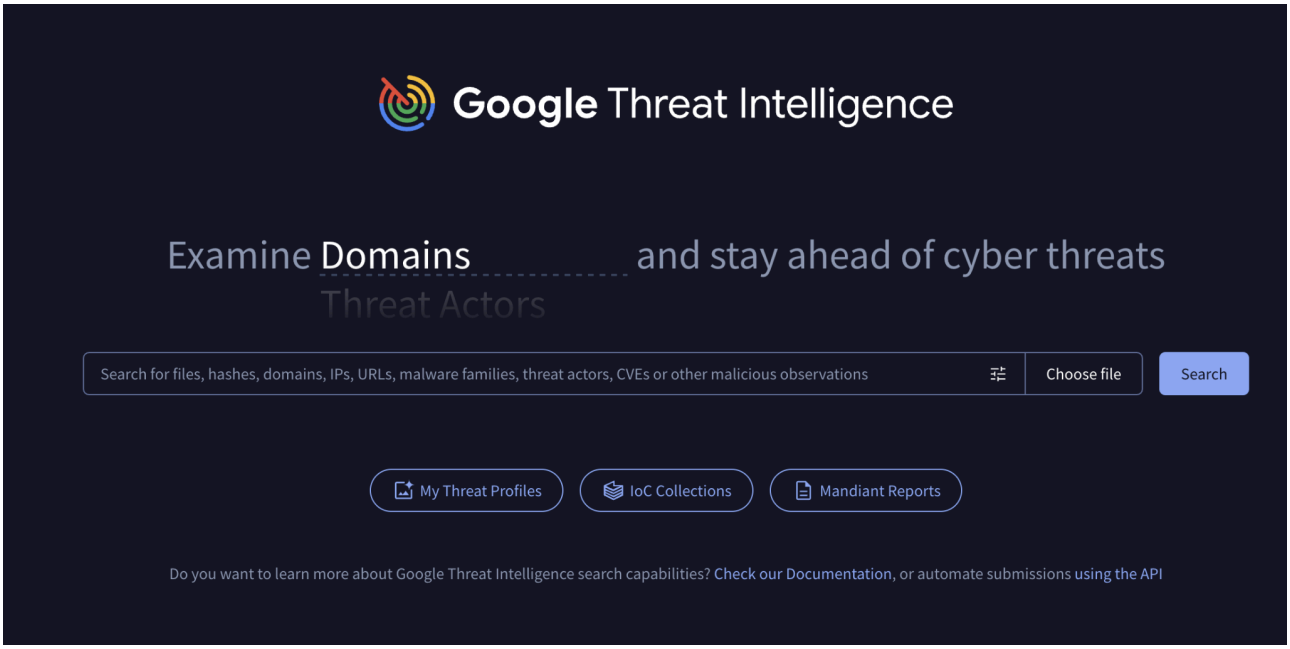
9. Why SOC Teams Prefer Chronicle Over Legacy SIEMs

Feature	Legacy SIEM	Chronicle
Storage Cost	Extremely high	Very low
Speed	Slow for large datasets	Instant search
Threat Intelligence	Often limited	Google + VT + Mandiant
Automation	Basic	Full SOAR + AI
Investigation	Manual correlation	Visual timeline
Scaling	Hardware required	Auto-scaled in cloud

10. 2024–2025 New Features SOC Analysts Must Know

- Chronicle is now **Google Security Operations (SecOps)**
- Integrated **Gemini AI for Security**
- AI-based **attack story summarization**
- Natural language threat hunting
- Stronger **SOAR automation**
- Built-in **response actions** (isolate host, block IOC, etc.)

THREAT INTELLIGENCE IN GOOGLE SECOPS

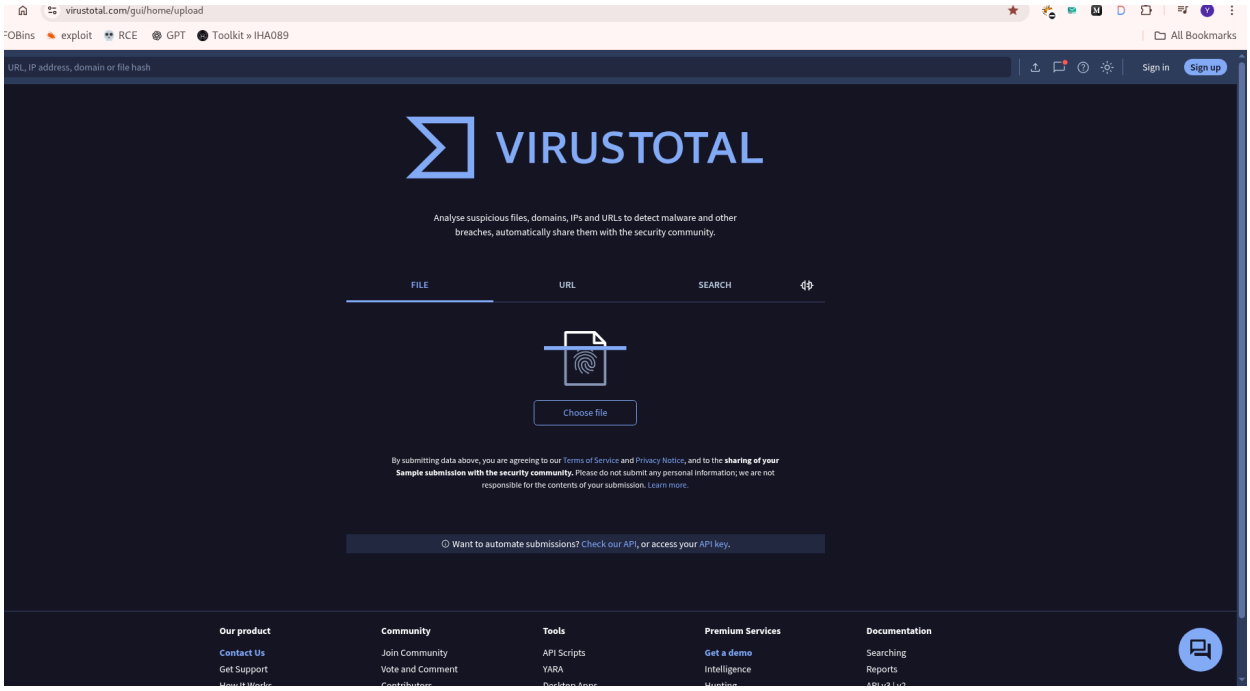


Google SecOps has **built-in TI** from:

- **VirusTotal**
- **Mandiant**
- **Google internal threat signals**

This is one of the strongest advantages for SOC teams.

A. VIRUSTOTAL ENRICHMENT



Chronicle automatically enriches with VT:

✔️ Hash Reputation

Shows if a file hash is malicious, suspicious, or unknown.

✔️ VT Detections

Shows antivirus engines that flagged it.

✔️ Behavior & Relation

- Domains contacted
- C2 infrastructure
- Related malware samples

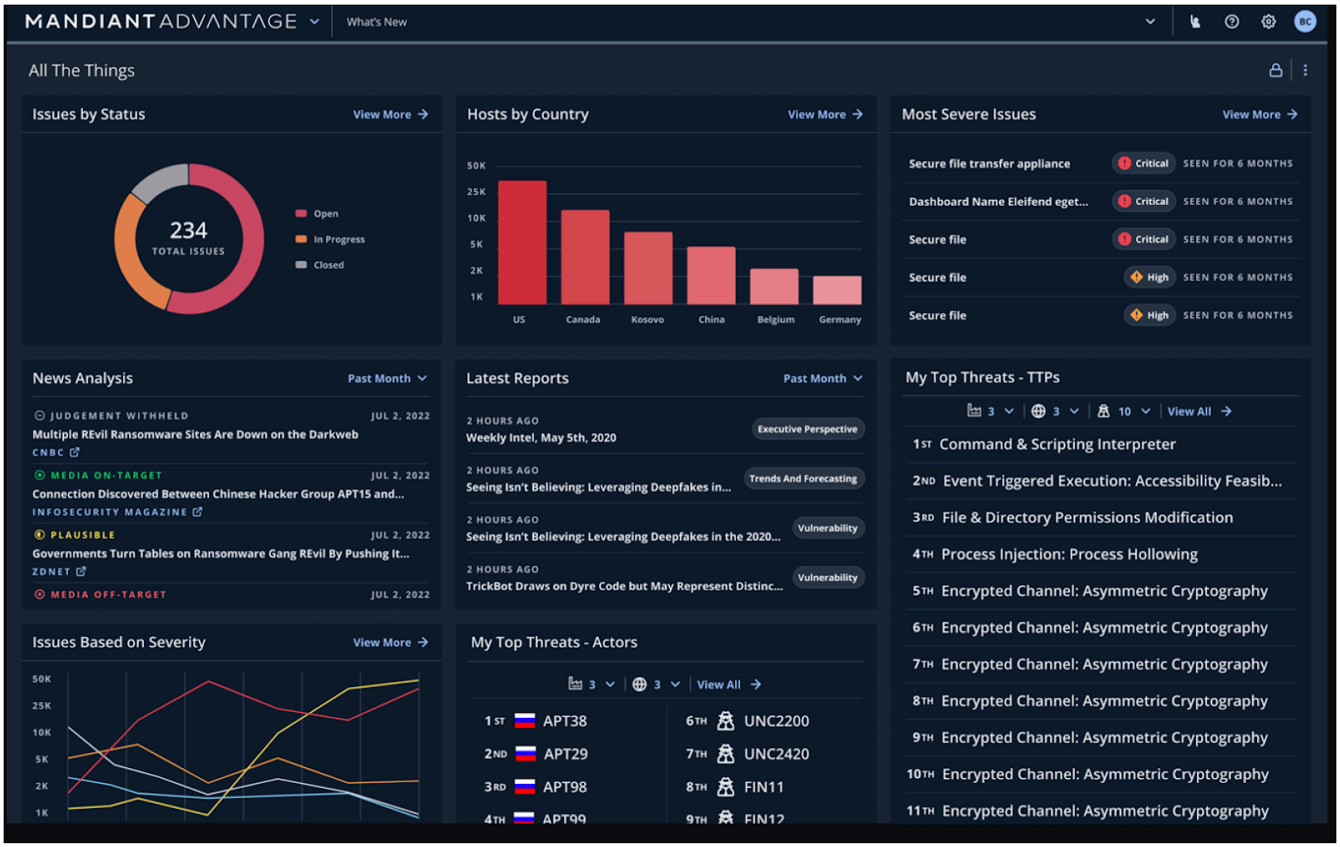
✔️ File Metadata

- Size
- Pack signatures
- Compilation timestamp
- PE sections

SOC Benefit:

Instant decision-making without leaving SIEM.

B. MANDIANT THREAT INTELLIGENCE



Mandiant TI is one of the world's **top cyber threat research sources**.

Chronicle integrates Mandiant intelligence to show:

✔️ APT & Threat Actor Association

- APT29
- FIN7
- UNC groups

✔️ Exploit Indicators

Zero-days, exploitation attempts.

✔️ Malware Family Mapping

- Cobalt Strike
- Rasberry Robin
- Emotet
- TrickBot
- QakBot

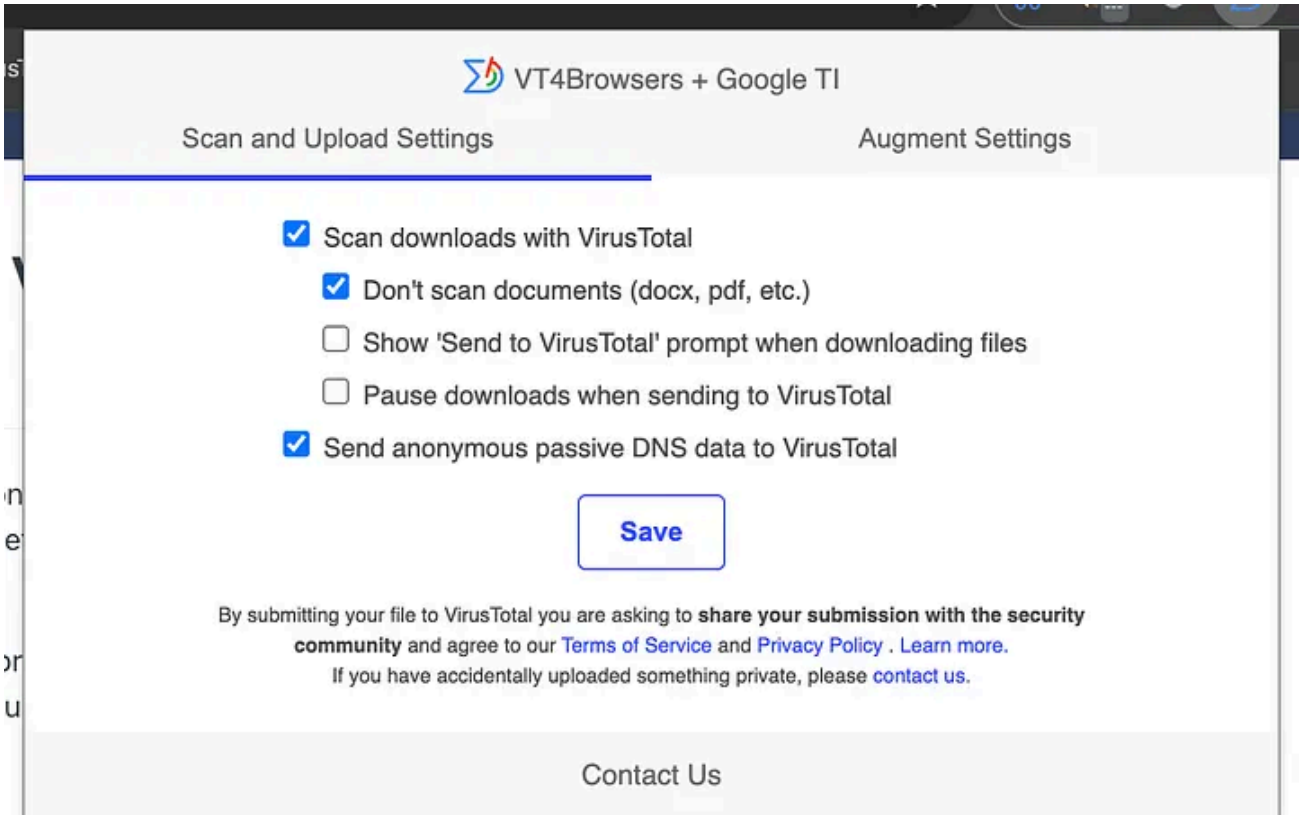
✔️ Attack Techniques

Mapped to MITRE ATT&CK.

SOC Benefit:

You immediately know **who** the threat actor might be and **how** they operate.

C. GOOGLE INTERNAL THREAT SIGNALS



Google collects global telemetry from:

- Gmail
- Google Search
- YouTube
- Android
- Google Cloud
- Chrome

This helps detect:

✔️ **Emerging malware**

✔️ **New phishing domains**

✔️ **Zero-day exploitation**

✔️ **Unusual C2 infrastructure**

SOC analysts get intelligence **before the rest of the world**.

D. HOW TI ENRICHMENT SHOWS UP IN CHRONICLE

When you click an alert, you automatically see:

✔️ **File hash reputation (VT)**

✔️ **Domain/IP reputation (Mandiant + VT)**

✔️ **Related malware families**

✔️ **Past sightings in your environment**

✔️ **Global prevalence (rare or common)**

✔️ **Recommended MITRE techniques**

No manual lookup required.

Components of chronicle

Component	Purpose	Why Important for SOC
UDM	Normalized log schema	Easy hunting & detections
Search	Query logs fast	Investigations in seconds
YARA-L	Custom detections	Build your own rules
Timeline	Attack replay	Faster incident analysis
Playbooks	Automation	Reduce analyst workload
Cases	Incident tracking	Organized investigations
VirusTotal	IOC enrichment	Faster verdicts
Mandiant TI	Threat actor insights	Understand attacker TTPs
AI (Gemini)	Automated reasoning	Faster, smarter analysis
Dashboards	Monitoring	High-level SOC visibility

Here are the **names only** of tools similar to Google Chronicle:

- **Microsoft Sentinel**
- **Splunk Enterprise Security (ES)**
- **Splunk SOAR (Phantom)**
- **Palo Alto Cortex XSIAM**
- **Sumo Logic Cloud SIEM**
- **Rapid7 InsightIDR**
- **Rapid7 InsightConnect (SOAR)**
- **Elastic Security (Elastic SIEM)**

✅ Advantages of Google Chronicle

- Extremely fast search (seconds even for months of data)
- Very low-cost long-term storage (no storage-based pricing)
- Automatic log normalization using UDM
- Built-in threat intelligence (VirusTotal + Mandiant + Google TI)
- Strong AI assistance (Gemini) for hunting & investigation
- Visual attack timeline simplifies investigations
- Cloud-native and highly scalable (no hardware needed)
- Integrated SOAR for automation & response
- Easy pivoting and IOC enrichment
- Suitable for large enterprises with massive data

❌ Disadvantages of Google Chronicle

- UDM query language requires learning
- Dashboards are limited compared to Splunk/Sentinel
- SOAR capabilities not as advanced as Palo Alto XSOAR
- Cloud-only (no on-premise option)
- Customization options are fewer than Splunk
- Some integrations may require tuning
- Visualization/pivoting not as deep as Elastic

Reference

https://cloud.google.com/blog/products/identity-security/introducing-chronicle-security-operations
https://docs.cloud.google.com/chronicle/docs/overview
https://en.wikipedia.org/wiki/Google_Security_Operations

-Yuvaraj.D