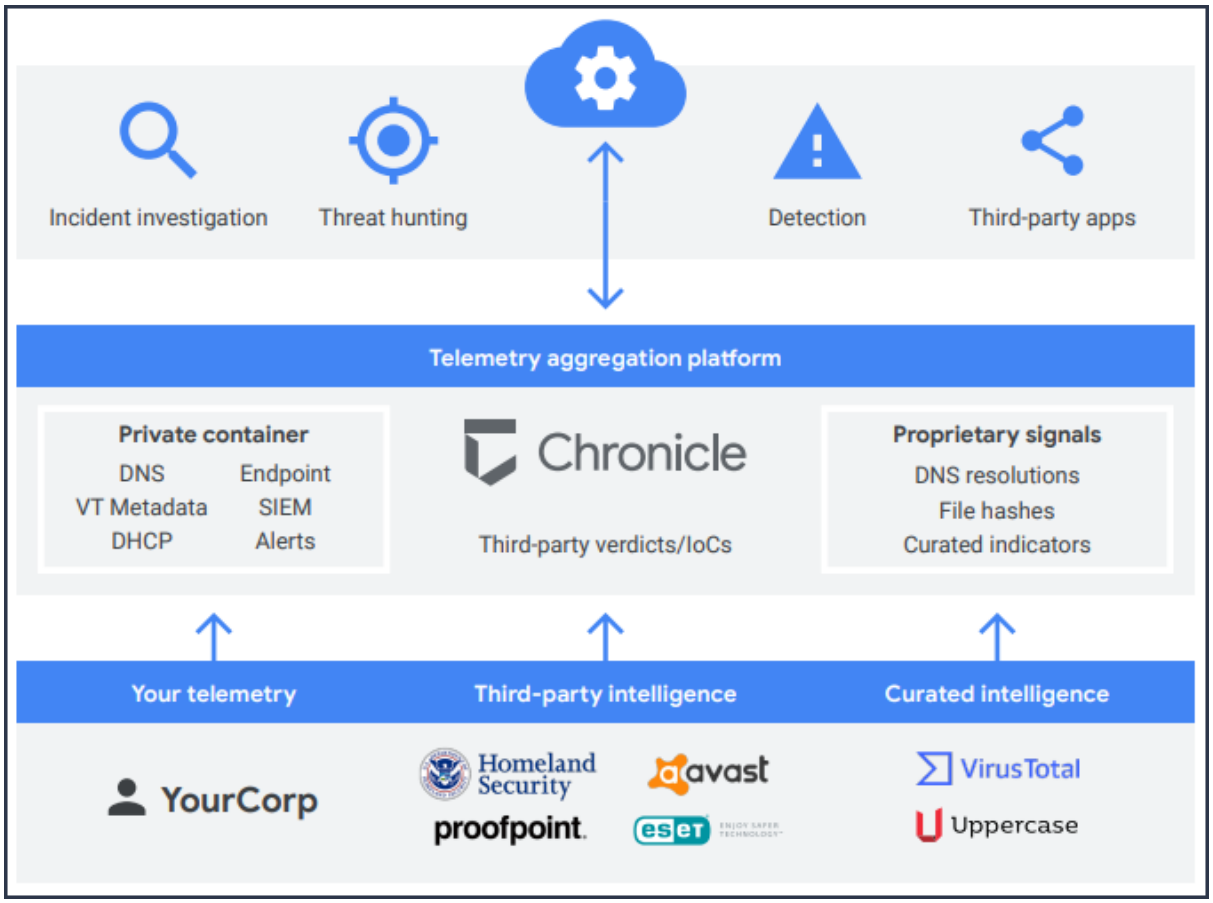
Chronicle overview

Chronicle is a cloud service, built as a specialized layer on top of core Google infrastructure, designed for enterprises to privately retain, analyze, and search the massive amounts of security and network telemetry they generate. Chronicle normalizes, indexes, correlates, and analyzes the data to provide instant analysis and context on risky activity.

Chronicle enables you to examine the aggregated security information for your enterprise going back for months or longer. Use Chronicle to search across all of the domains accessed within your enterprise. You can narrow your search to any specific asset, domain, or IP address to determine if any compromise has taken place.



Chronicle platform overview

Data collection

Chronicle can ingest numerous security telemetry types through a variety of methods, including:

- Forwarder: A lightweight software component, deployed in the customer's network, that supports syslog, packet capture, and existing log management or security information and event management (SIEM) data repositories.
- Ingestion APIs: APIs that enable logs to be sent directly to the Chronicle platform, eliminating the need for additional hardware or software in customer environments.
- Third-party integrations: Integration with third-party cloud APIs to facilitate ingestion of logs, including sources like Office 365 and Azure AD.

Data analysis

The analytical capabilities of Chronicle are delivered to security professionals as a simple, browser-based application. Many of these capabilities are also accessible programmatically through Read APIs. Chronicle gives analysts a way, when they see a potential threat, to determine what it is, what it's doing, whether it matters, and how best to respond.

Security and compliance

As a specialized, private layer built over core Google infrastructure, Chronicle inherits compute and storage capabilities as well as the security design and capabilities of that infrastructure.

Chronicle features

Search

- Raw Log Scan: Search your raw unparsed logs.
- Regular Expressions: Search your raw unparsed logs using regular expressions.

Investigative views

- Enterprise Insights: Displays the domains and assets most in need of investigation.
- Asset view: Investigate assets within your enterprise and whether or not they have interacted with suspicious domains.
- IP Address view: Investigate specific IP addresses within your enterprise and what impact they have on your assets.
- Hash view: Search for and investigate files based on their hash value.
- Domain view: Investigate specific domains within your enterprise and what impact they have on your assets.
- User view: Investigate users within your enterprise who may have been impacted by security events.

- Procedural filtering: Fine tune information about an asset, including by event type, log source, network connection status, and Top Level Domain (TLD).

Curated information

- Asset insight blocks: Highlights the domains and alerts that you might want to investigate further.
- Prevalence graph: Shows the number of domains an asset has connected to over a specified time period.
- Alerts from popular security products.

Detection Engine

You can use the Chronicle Detection Engine to automate the process of searching across your data for security issues. You can specify rules to search all of your incoming data and notify you when potential and known threats appear in your enterprise.

Additional tools

- VirusTotal: Launch VirusTotal from Chronicle to further investigate an asset, domain, or IP address by clicking VT Context.
- Chronicle extension for Chrome: Launch Chronicle from anywhere within the Chrome browser.