Google Cloud   **Chronicle**

Chronicle Integration Program

Develop an integration with Chronicle to enrich customers' SOC intelligence with your data

Google's Cloud-Native SIEM, Chronicle, is built to handle massive amounts of data and extract signals to find threats instantly. Our mutual customers benefit from having your data ingested, indexed and correlated within Chronicle to enrich their security insight and remove blind spots.

Become a Chronicle Technology Partner

As a Chronicle Technology Partner with a Chronicle integration, you can increase customer value by including your product's data in their Chronicle instance.

Develop an integration and normalize your data

Send your data to Chronicle pre-normalized in Chronicle's Unified Data Model (UDM) structure via the Ingestion API. This is the recommended approach as it allows our mutual customers to realize rapid value from your data within Chronicle.

Leverage development support

Google will provide signed Chronicle Technology Partners with a Not-for-resale (NFR) development license to build and maintain the integration with Chronicle. Technical support is also available via the Chronicle technology partner team.

Increase your brand awareness

Once your integration is complete, your logo will be added to the Chronicle Partners page. Upon Google approval, we can also support marketing efforts you lead such as: a solution brief about the integration, a blog post about the integration and other initiatives. Please note that no Chronicle or other Google branding such as logos can be utilized without Google approval.

Visit chronicle.security or contact GCS-Tech-Alliances@google.com to learn more.

Chronicle Highlights →

Customers benefit from Google Chronicle scale, speed and smarts to optimize action-able security intelligence.

- Built on the power and speed of Google search, delivers valuable data insight in seconds

- Infinite scalability, able to ingest 100s of petabytes of security telemetry data and securely store for an extended period of time

- Normalization, indexing, correlation and dashboarding makes data available for immediate and rich contextual analysis

- Automatically connects related activity data into a single data structure for each event for greater contextual understanding

- Presents the whole picture with an identity graph to best understand and respond to unusual activity.

- Integrated threat intelligence feeds such as from VirusTotal to streamline threat hunting in real-time and retroactively.