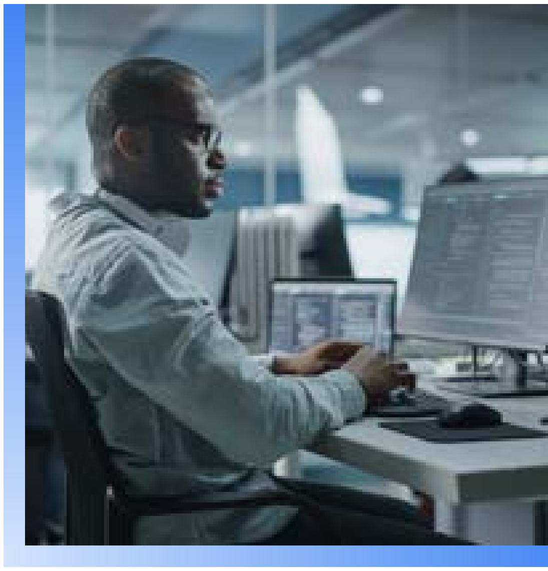
Chronicle OEM Program

Program Overview

Purpose-built and run on core Google infrastructure, Chronicle can ingest massive amounts of telemetry data, normalize, index, correlate it to known threats, and make it available for analysis in seconds. The Google Cloud Security OEM Program allows partners to take advantage of the speed, scalability and analytics of the Chronicle platform when building an XDR platform, storing and analyzing large amounts of data or meeting the need to normalize multiple types of log data.



Primary Use Cases

Power your XDR solution with Google Chronicle

- Easily ingest, normalize and maintain security telemetry
- Provide search, detection, and hunt capabilities across major classes of threats across all environments
- Power rapid investigation by correlating all relevant events and context for each threat
- Enable turn-key remediation with deep integrations into 3rd party tools and Google Cloud Platform and products

Scale up security operations with a data lake and log management

- Ingest everything from on-prem devices to multiple clouds – even the voluminous datasets (e.g. EDR, NDR, Cloud). This enables security data to exist in one place, and more importantly, aliased and correlated into a timeline of events.
- Rapidly normalize data with hundreds of parsers into a rich, extensible Unified Data Model spanning asset, user and indicators of compromise (IoC) dimensions and attributes
- Build and streamline customized user workflows and integrations with the API-first, open platform

Accelerate threat hunting, prioritization and incident response

- Automatically correlate IoCs against one full year of security telemetry
- Search at Google speed to hunt for threats faster than traditional SOC tools, including across all your customers' data for added, proactive customer value
- Prioritize alerts with supporting information from authoritative sources (such as CMDB, IAM, and DLP) baked into the security event. Chronicle alerting only escalates important threats, with scoring based on contextual vulnerability and business risk.

Google Cloud

Business Benefits

Sales

- Fast-path to Google Cloud Marketplace listing
  - Visibility with more than 10,000 Google Cloud sellers
  - Visibility with millions of Marketplace buyers
- Co-selling with Google Cloud Security Sales Specialists who are highly incented to work with you

Marketing

- Market elevation with Google Cloud branding
  - The power to leverage “Developed with Google Cloud” branding
  - Options to co-brand your campaigns with Google Cloud Security
  - Logo publication on Chronicle website
- Assistance with your collateral and campaigns
- Support for your events and invitations to participate in Google Cloud Security events

Engineering

- Engineering resource relief by using Google Chronicle
- Assigned partner engineering contact
- Access to customer success and support resources

Included with Chronicle OEM Licensing

Unlimited Chronicle instances

Grow your customer base without scalability or licensing concerns.

Master Chronicle account

Centrally manage your customers' Chronicle instances. Proactively hunt for a new threat discovered in one customers' Chronicle instance across all your customers instances to improve your offering.

Numerous data sources

Ingest as many data sources as desired to maximize your solution value and customers' security intelligence.

Hundreds of prebuilt parsers

Automatically ingest, analyze and normalize numerous data sources such as from CrowdStrike, Microsoft, Palo Alto Networks, VMware, Zscaler and hundreds of others.

One year data retention

Automatically retain all ingested data for a year to provide deep investigations over time and streamline compliance reporting.

Unified Data Model (UDM)

Analyze with ease via UDM, Chronicle's comprehensive and extensible schema for any security relevant telemetry. Data sent to Chronicle's UDM is enriched with context (asset, user, application, threat intelligence, and vulnerabilities) and correlation (IP to host for example)

Threat detections

Detect advanced threats and secure your customers

API's

Customize to best suit your customers' needs via the many APIs included, such as the Search API for programmatic access to your data, a Detection API to create, manage and run detection rules, the RBAC API and Threat Intelligence API for getting alerts on matched data with Threat Intelligence.

Raw Log scan

Search and analyze raw data too. Data types that are not normalized by parsers or UDM will still be ingested, stored and able to be searched, either through the Chronicle UI or the Raw Log Scan API.

Continuous IoC matching

At global scale, automatically and continuously surface all your customers' IoC matches and enrich with unique contextual data.

Looker visualization

Leverage out-of-the-box and customizable dashboarding with Looker for all data ingested into Chronicle.

BigQuery

Included with a Chronicle OEM license, you can also export petabytes of telemetry data from Chronicle into a BigQuery instance for your organization and/or for each of your customers. BigQuery is Google Cloud's serverless, highly scalable data warehouse offering. This enables your solution to easily apply highly complex and customized analysis against massive volumes of security data, such as for statistical and multi-year trend analysis, and displays the results within your UI.

Visit goo.gle/cloud-security-oem or contact GCS-OEM@google.com to learn more.