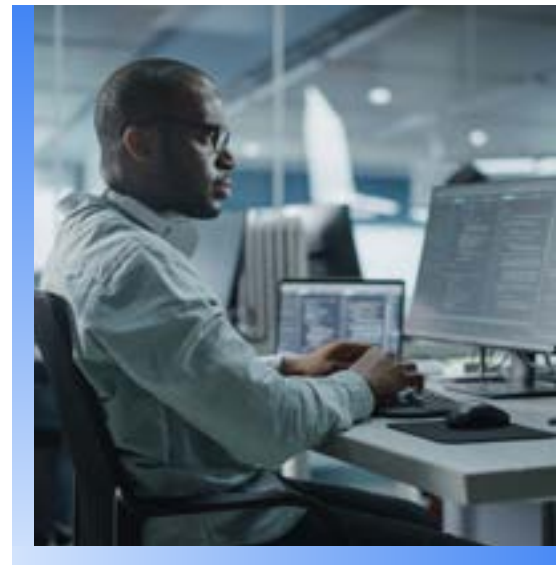


Chronicle OEM Program



Program Overview

Accelerate your business and focus your engineering on unique security use cases by building on Chronicle. Purpose-built on core Google infrastructure, Chronicle can ingest petabytes of data, normalize, index, and correlate it, hunt for threats in real-time and retroactively and retrieve data for analysis in seconds. Chronicle can also help your product automate workflows and manage incidents to streamline threat response processes. By becoming a Chronicle OEM, you can take advantage of Google speed, scale and smarts to have your product address use cases such as the following.



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 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 much faster than traditional SOC tools
- ✓ Automatically prioritize and score alerts based on correlated business and security context baked into each security event.
- ✓ Capitalize on security orchestration and automated response (SOAR) capabilities to power your product's ability to automate workflows and manage cases.

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.
-  **Unlimited data sources**


Ingest as many data sources as desired to maximize your solution value and customers' security intelligence.
-  **Hundreds of pre-built 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 detection Rule Engine**

Leverage Chronicle's powerful rule engine and curated rules to detect advanced threats in real-time and retroactively to optimize your customers' security.
-  **Continuous IoC matching**

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

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.
-  **BigQuery**

Included with a Chronicle OEM license, you can export Chronicle data into a BigQuery instance for each of your customers. This enables you to build custom, complex analytics, SQL searches and machine learning. Chronicle essentially provides a pre-built data model to BigQuery so you can continue to grow your offering's capabilities. BigQuery is Google Cloud's serverless, highly scalable data warehouse offering.
-  **Optional Add-ons**
 - Looker for Customized Analytics** - Build customized dashboards, analytics and even a user interface with Google Looker.
 - Security Orchestration Automation and Response (SOAR)** - Add automated security workflow and case management capabilities to your product too.



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

©2023 Google LLC. All rights reserved. Chronicle was acquired by Google and operates under Google Cloud.