Chronicle

Chronicle Detect

Automatically find threats in real-time and at scale using Google-native infrastructure, detection techniques, and signals.

Overview

Chronicle Detect is a threat detection solution built on Google infrastructure to help you identify threats at unparalleled speed and scale. It includes a rules engine that operates at the speed of search, a rules language based on one of the most-used detection languages in the world, and an applied threat intelligence service that surfaces highly actionable threats in Chronicle environments.

Benefits

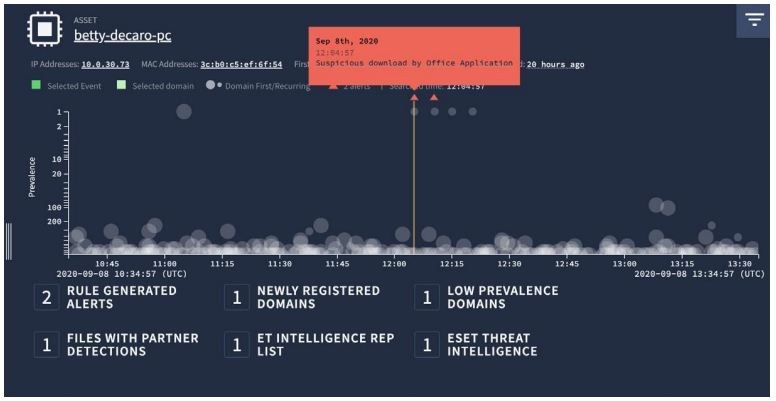
- Threat detection at Google speed and scale
- Built for security analysts, by security analysts
- Detections backed by elite threat researchers

Detections based on high value security data

Using our Google-scale platform, security teams can send their security telemetry to Chronicle at a fixed cost so that diverse, high value security data - such as EDR or XDR - can be taken into account for detections. We automatically make that security data useful by mapping it to a common data model across machines, users, and threat indicators, so that you can quickly apply powerful detection rules to a unified set of data.

Identify advanced threats with out-of-the-box rules

The Chronicle Detect rules engine includes predefined rules mapped to specific threats, suspicious activity, and security frameworks like MITRE ATT&CK. The rules engine syntax is built using the widely adopted YARA detection language, so you can easily adjust or extend rules to meet your enterprise's specific needs. Powered by Google infrastructure, Chronicle Detect allows you to interrogate all of your security telemetry in one place so that you can accurately identify threats and reach decisions faster than ever. The solution includes 500+ YARA-L based SOC Prime rules and a Sigma to YARA-L converter so that you can easily port or migrate existing rules from legacy systems to Chronicle.

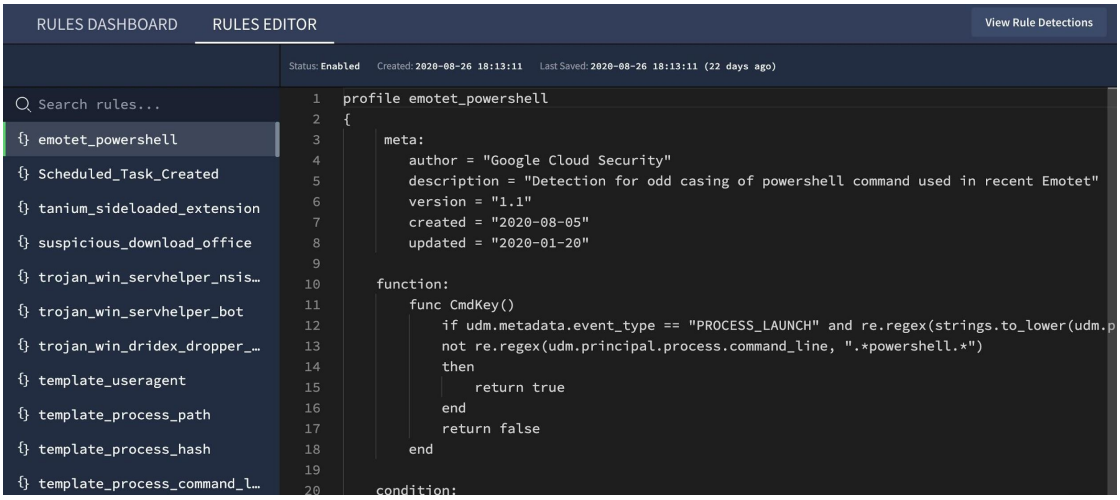


The Chronicle Detect rules engine helps you identify and understand multi-event attacks.

Chronicle

Powerful, flexible rules syntax

Chronicle Detect allows security teams to leverage YARA-L, the rule language designed for modern threat detection. While other complex security-related languages focus on querying data, YARA-L is used to define real-time and historical detection rules and perform threat hunting-style searches in your environment. Using YARA-L, you can edit pre-defined Chronicle Detect rules, write custom detections for TTPs specific to your enterprise, and build detections based on security frameworks like ATT&CK.



Using the YARA-L syntax, it's easy to edit and build detection rules in the Chronicle interface.

High fidelity threat indicators, validated hands-on by threat researchers

Select Chronicle customers can also take advantage of Google Cloud Threat Intelligence for Chronicle, an applied threat intelligence service that surfaces highly actionable threats in Chronicle environments. With this service, intelligence on attack patterns is gathered across Google's vast array of networks and services, coupled with operational research for deconfliction, context and enrichment, and then applied to customer telemetry. Threat Intel for Chronicle generates high fidelity alerts that help security teams focus on real threats in the environment and accelerate incident response time.

Respond to threats with SOC playbook and orchestration-ready APIs and integrations

Purpose-built integrations between Chronicle and leading SOAR vendors, such as D3 Security, IBM, Palo Alto Networks, ServiceNow, Siemplify, Splunk, and Swimlane, allow you to combine the real-time threat detection and investigation capabilities of Chronicle with your SOAR playbooks. Chronicle instances, APIs, and search parameters are accessible directly within SOAR platforms.