

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 a regular stream of new rules and indicators, built by our elite research team.

Benefits

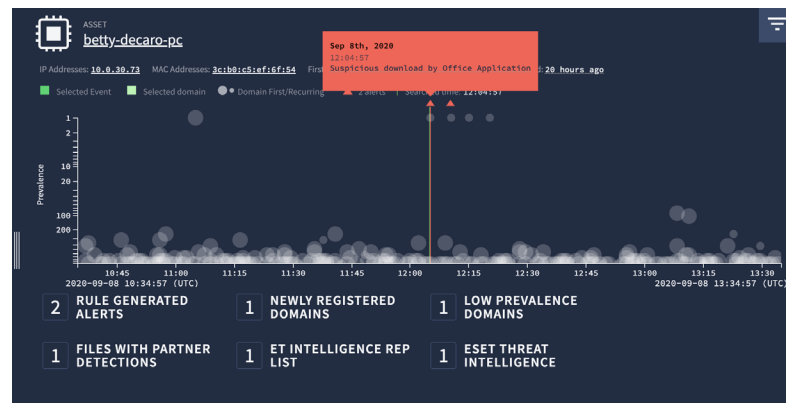
- Threat detection at Google speed and scale
- Built for security analysts, by security analysts
- Detections backed by elite threat researchers

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

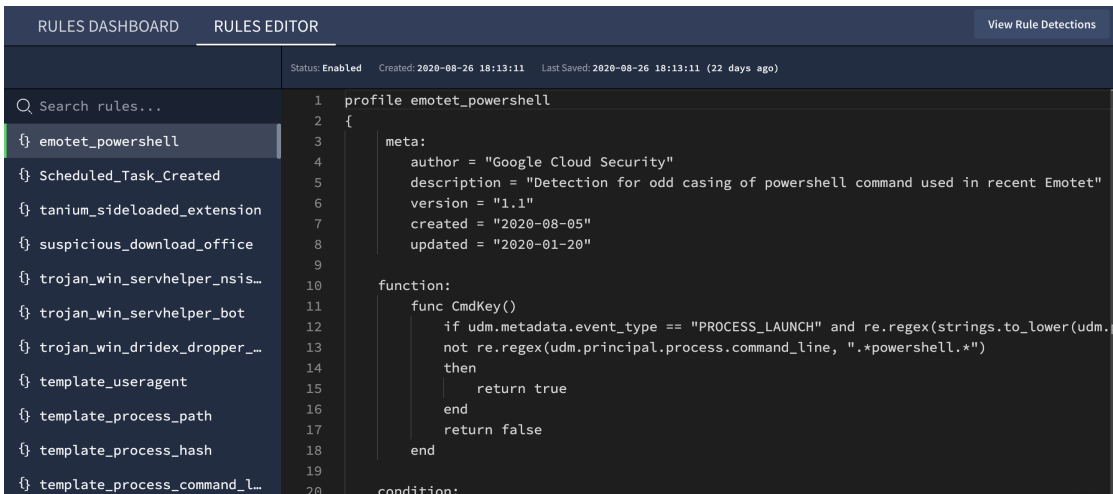
The Chronicle Detect rules engine includes pre-defined rules mapped to specific threats, suspicious activity, and security frameworks like MITRE ATT&CK. The rules engine syntax is built using the widely adopted YARA detection language, so you can easily adjust or extend rules to meet your enterprise's 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 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.

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.



```
1 profile emotet_powershell
2 {
3   meta:
4     author = "Google Cloud Security"
5     description = "Detection for odd casing of powershell command used in recent Emotet"
6     version = "1.1"
7     created = "2020-08-05"
8     updated = "2020-01-20"
9
10  function:
11    func CmdKey()
12      if udm.metadata.event_type == "PROCESS_LAUNCH" and re.regex(strings.to_lower(udm.p
13        not re.regex(udm.principal.process.command_line, ".*powershell.*")
14      then
15        return true
16      end
17      return false
18    end
19
20  condition:
```

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

Real-time threat indicators and automatic rules from Uppercase

Chronicle Detect features a stream of high-risk attack campaign indicators and rules from Uppercase, Chronicle's elite threat research team. Uppercase researchers leverage a variety of novel tools and techniques to provide Chronicle customers with indicators spanning the latest crimeware, APTs, and unwanted malicious programs. The Uppercase-provided IOC match feed is analyzed against all security telemetry in your Chronicle system, and lets you know right away when high-risk threat indicators are present in your environment.

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

Purpose-built integrations between Chronicle and leading SOAR vendors, such as Palo Alto Networks Cortex XSOAR, Splunk Phantom, and D3 SOAR, 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.