Google Chronicle and Palo Alto Cortex XSOAR

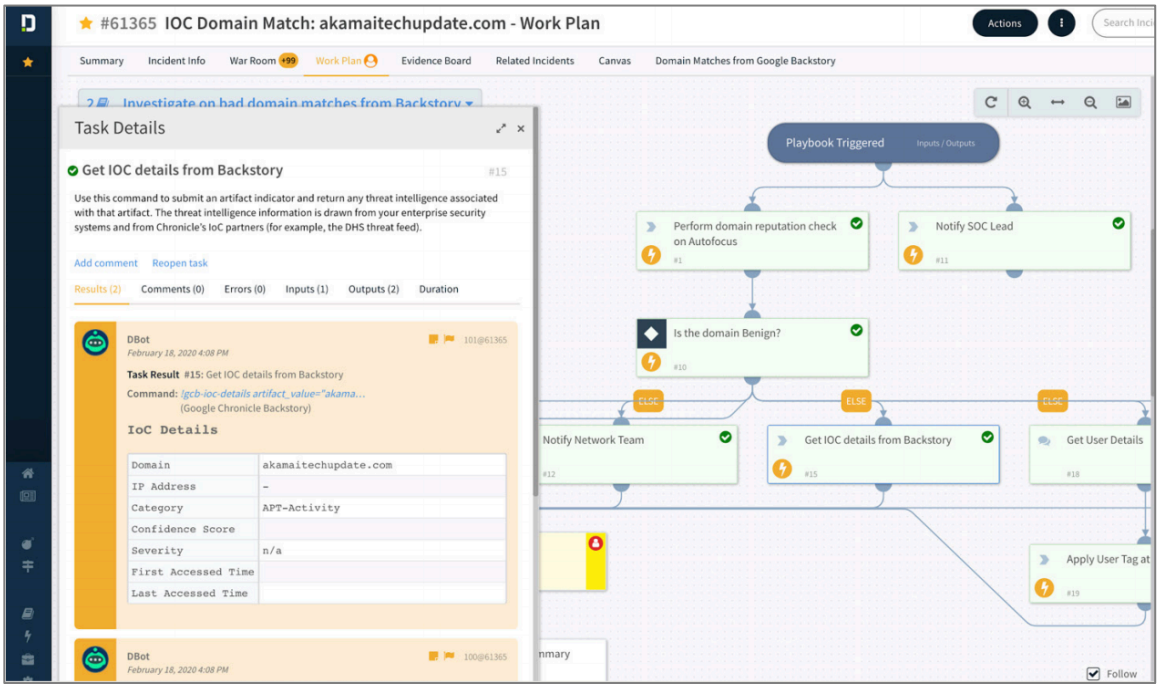
Automated Cloud-based Threat Detection and Response

Global scale threat investigation and detection with Chronicle

Google Chronicle is a petabyte scale security analytics platform for investigation and detection of modern threats. The Chronicle security analytics platform enables organizations to ingest all their security telemetry at a fixed, predictable cost into a private cloud container and retain it for a full year. Chronicle automatically and continuously enriches raw events with correlated information on users, assets and threats indicators. A web interface specifically designed for SOC analysts enables investigation and detection of threats with sub-second latency across all their security telemetry.

Chronicle and Cortex XSOAR integration

A purpose-built integration between Google Chronicle and Cortex XSOAR now enables customers to combine the real-time threat detection and investigation capabilities of Google Chronicle with the SOAR features of Cortex. Specifically, Chronicle instances, APIs and search parameters are all accessible directly within Cortex XSOAR for full automation of playbooks.



Leveraging Chronicle enrichment and speed in XSOAR playbooks

A threat hunter learns about malware infrastructure (IPs, domains, URLs, files) that is part of an advanced persistent threat (APT) from a security report. Uncovering the potentially infected assets that have reached out to any of the malware artifacts is an extremely tedious task that

involves executing numerous slow queries and manually stitching IPs to hostnames. When possible, it can take days or weeks of advanced analyst time. Often it is just impossible because the required telemetry (DNS, DHCP, proxy, EDR) has only been retained for a month due to cost constraints while the campaign is known to have been active for much longer.

Through this integration:

- A junior analyst can simply execute predefined Cortex XSOAR playbooks that instantly return every asset that has reached out to any of the known IoCs.
- The playbook can then automatically execute a reverse query for all returned assets to quickly learn if they have reached out to any other malicious IoCs.
- No data stitching was required as Chronicle had already enriched underlying events (through IP to host as well as host to IoC correlation).
- All these queries could be executed against a full year of security data with sub-second latency given Chronicle's default retention, speed and pricing model.
- The analyst can use the Chronicle interface for deeper investigation such as to understand the full attack chain timeline pattern for this threat.
- Remediation steps can be automated into playbooks by leveraging the hundreds of Cortex XSOAR product integrations.

Joint Solution Benefits

Intelligent Data Fusion Timelines and enriched data model for investigation and detection	**Continuous IoC Matching** Continuous, retrospective analysis of telemetry vs. threat intelligence	**Hunt at Google speed** Subsecond searches against petabytes of data
Native Integration Chronicle instances and APIs directly accessible in Cortex playbooks	**Remediation Library** Leverage 100s of Cortex XSOAR product integrations for playbook automation	**Drive Analyst Productivity** End to end automation enables analysts to focus on higher value tasks

About Google Chronicle

Chronicle, part of Google Cloud, is focused on enterprise cybersecurity solutions. We leverage massive data and compute resources to analyze and fight cyber threats. Our Backstory security analytics platform helps enterprise security teams investigate incidents and hunt for threats in their networks, at the speed of search.

About Cortex XSOAR

Palo Alto Networks Cortex XSOAR is a comprehensive security orchestration, automation, and response (SOAR) platform that combines security orchestration, case management and interactive investigation to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity.