Automated Cloud-based Threat Detection and Response

CORTEX XSOAR BY PALO ALTO NETWORKS | Chronicle

In today's ever-changing security landscape, incident response teams often miss out on potential threats that can impact their organization because they're time-strapped by manual processes and high alert volume. They're unable to take advantage of the breadth of external threat intelligence available and how these threats impact their organizations.

To meet these challenges, users can combine the real-time threat detection capability of Google Chronicle with the security orchestration and automation features of Cortex XSOAR to improve threat visibility and accelerate incident response.

Integration Features

Automate incident and indicator enrichment with Google Chronicle alert data such as domain/IP reputation, ingestion time and sighting details.

Access or query Google Chronicle for asset list and details associated with a domain/IP from within Cortex XSOAR

Leverage hundreds of Cortex XSOAR product integrations to coordinate and automate remediation across endpoints or affected assets.

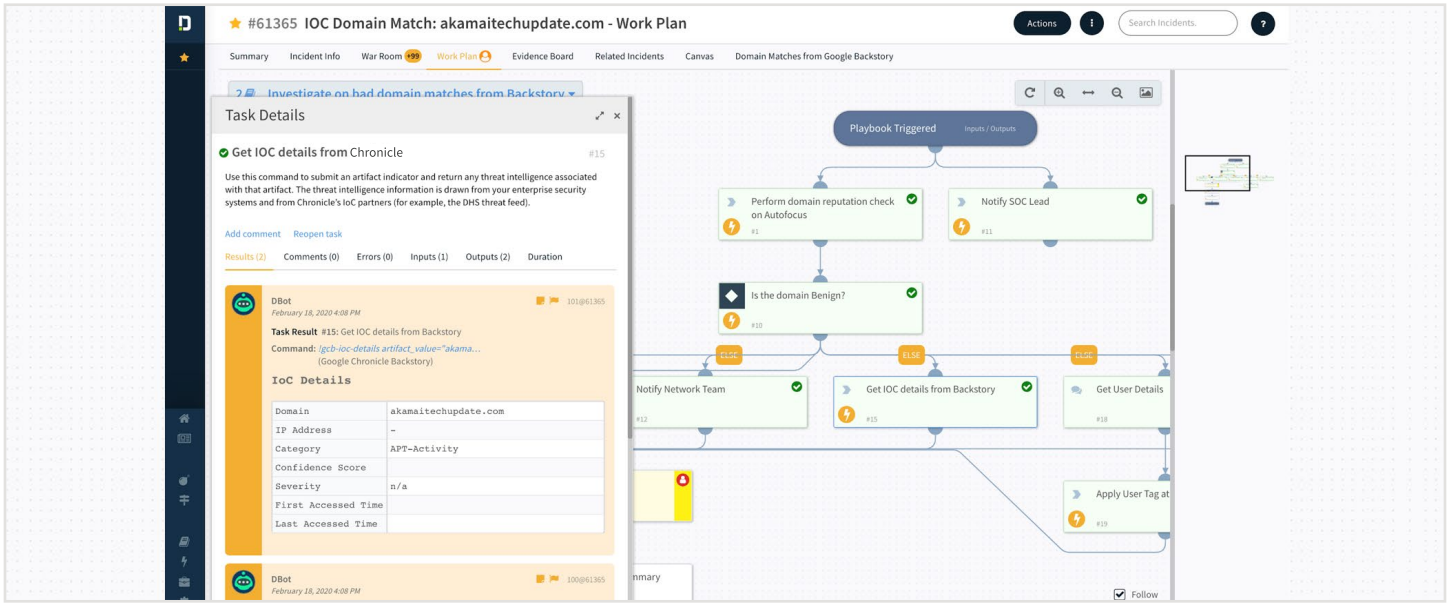
Use Case #1 Automated Incident Data Enrichment and Response

Challenge: The disparate nature of threat intelligence and incident response tools can make it tough for SOC teams to track the lifecycle of an incident. Security analysts have to collect context manually, resulting in screen-switching, duplication of work, and repetitive processes.

Solution: SOCs using Chronicle for threat intelligence and Cortex XSOAR for security orchestration and incident response respectively can automate indicator enrichment through Cortex XSOAR playbooks. These playbooks will harness Chronicle indicator intelligence and use that information to execute actions across the entire stack of products that a SOC uses. For example, analysts can leverage Chronicle to enrich domains and IPs as automatable playbook tasks.

Benefit: Cortex XSOAR playbooks coupled with Chronicle actions can standardize and speed up triage and resolution of security alerts. Analysts get a comprehensive view of assets impacted and the response workflow on a single screen. With the repeatable tasks now automated, analyst time is freed up for deeper investigation and strategic action.

paloalto NETWORKS



Use Case #2 Interactive Real-Time Investigation of Complex Threats

Challenge: Apart from running automated actions, attack investigations usually require additional real-time tasks such as pivoting from one suspicious indicator to another to gather critical evidence, drawing relations between incidents, and finalizing resolution. Running these commands traps analysts in a screen-switching cycle during investigation and a documentation-chasing cycle after investigations end.

Solution: After running enrichment playbooks, analysts can gain greater visibility and new actionable information about the attack by running Chronicle commands in the Cortex XSOAR War Room. For example, analysts can get additional context and user details from Chronicle in real time.

Analysts can also run commands from other security tools in real-time using the War Room, ensuring a single-console view for end-to-end investigation. The War Room will document all analyst actions and suggest the most effective analysts and command-sets with time.

Benefit: The War Room allows analysts to quickly pivot and run unique commands relevant to incidents in their environment from a common window. All participating analysts will have full task-level visibility of the process and be able to run and document commands from a unified console. They will also prevent the need for collating information from multiple sources for documentation.

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 Chronicle 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.