DEMISTO
A PALO ALTO NETWORKS® COMPANY

CORTEX XDR™
BY PALO ALTO NETWORKS

Automated Data Visibility, Detection, and Response

Benefits

- Achieve unparalleled visibility over your network, endpoint, and cloud data with Cortex XDR's stitching and behavioral analytics.
- Execute end-to-end incident response by ingesting Cortex XDR incidents into Demisto for playbook-driven orchestration across security products.
- Reduce incident resolution times by using one integrated solution for alert detection, investigation, and response.
- Shorten the decision-making cycle by automating key tasks with analyst review.

Compatibility

- Products: Demisto Enterprise, Palo Alto Networks® Cortex™ XDR

Security teams face a massive number of security alerts every day as attackers rely on brute force, automation, and varied attack vectors to compromise target systems. It is virtually impossible for humans to scan through these alerts manually, resulting in overworked teams, increased error rates, and dangerous alerts slipping through the cracks.

Teams also struggle with disjointed data and processes during investigation and response. This challenge is caused by siloed data and products that, while valuable in an isolated sense, rarely interconnect to form a bigger attack picture. Security analysts must collect context manually, resulting in screen-switching, duplication of work, and repetitive processes.

Demisto integrates with Cortex XDR to provide teams with a continuous security platform, enabling them to unify data across sources, prevent and detect attacks, accelerate investigations, and automate repeatable tasks to reduce response times.

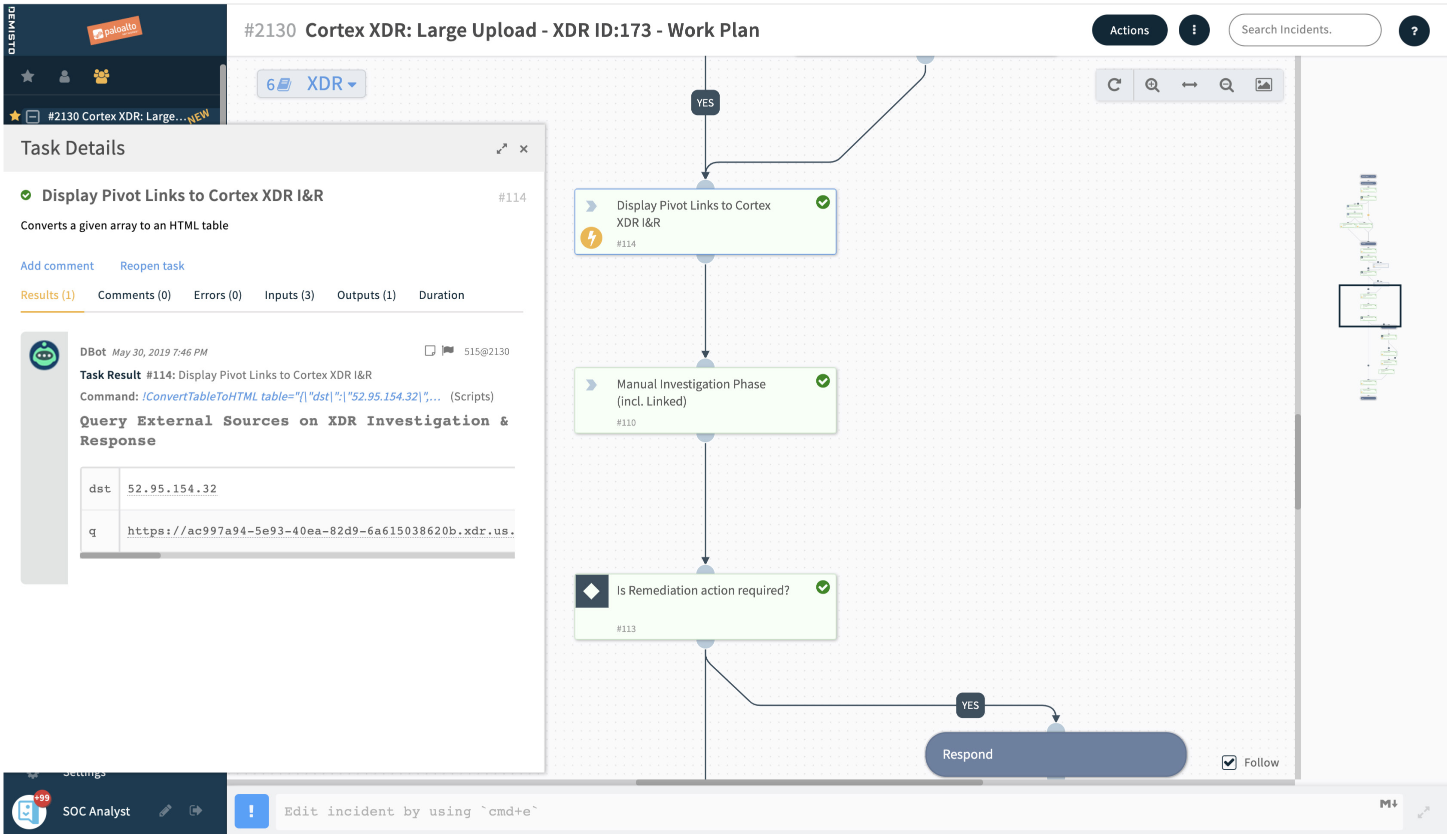
Integration Features

- Ingest Cortex XDR incidents within Demisto for playbook-driven enrichment and response.
- Update incident information in Cortex XDR based off insight gathered from playbooks and investigation within Demisto.
- Get custom cross-sections of Cortex XDR incident information (such as related alerts, file artifacts, network artifacts) within Demisto, either as automated playbook tasks or in real-time within the War Room.
- Leverage hundreds of Demisto third-party product integrations to execute response processes for Cortex XDR incidents that span across security products and functions.
- Run thousands of commands across third-party products interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.

USE CASE #1 AUTOMATED INCIDENT INGESTION, ENRICHMENT, AND RESPONSE

Challenge: Organizations today deal with an expanded threat surface. Security attacks can leave footprints across network, endpoint, or cloud environments, but teams struggle to continuously monitor these environments, correlate data across sources to get the bigger picture, and then drive that data to response in a scalable manner.

Solution: Cortex XDR collects rich, detailed data across network, endpoint, and cloud environments before applying behavioral analytics and AI to stitch the data together and display incidents in a sequenced manner. Demisto can ingest these incidents from Cortex XDR and trigger playbooks that coordinate across users' security product stack for further enrichment and response. These playbooks can be automated, manual, or a mixture of both, depending on user requirements.



#2130 Cortex XDR: Large Upload - XDR ID:173 - Work Plan

Task Details

Display Pivot Links to Cortex XDR I&R #114

Converts a given array to an HTML table

DBot May 30, 2019 7:46 PM 515@2130

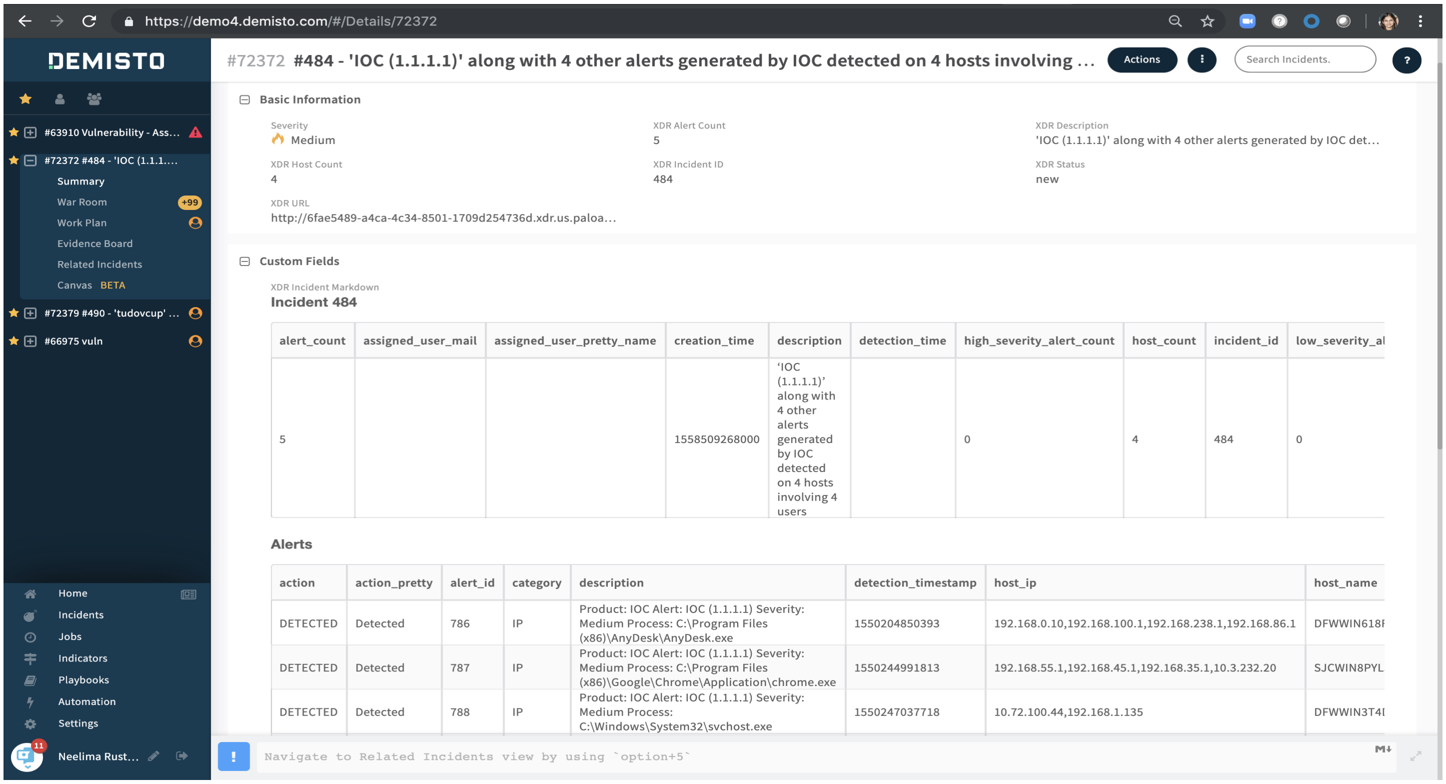
Task Result #114: Display Pivot Links to Cortex XDR I&R

Command: *!ConvertTableToHTML table="{\"dst\":\"52.95.154.32\",...* (Scripts)

Query External Sources on XDR Investigation & Response

dst	52.95.154.32
q	https://ac997a94-5e93-40ea-82d9-6a615038620b.xdr.us.

Figure 1: Screenshot of Demisto playbook triggered off a Cortex XDR incident



#72372 #484 - 'IOC (1.1.1.1)' along with 4 other alerts generated by IOC detected on 4 hosts involving …

Basic Information

Severity
Medium

XDR Alert Count
5

XDR Description
'IOC (1.1.1.1)' along with 4 other alerts generated by IOC det…

XDR Host Count
4

XDR Incident ID
484

XDR Status
new

XDR URL
http://6fae5489-a4ca-4c34-8501-1709d254736d.xdr.us.paloa…

Custom Fields

XDR Incident Markdown

Incident 484

alert_count	assigned_user_mail	assigned_user_pretty_name	creation_time	description	detection_time	high_severity_alert_count	host_count	incident_id	low_severity_al
5			1558509268000	'IOC (1.1.1.1)' along with 4 other alerts generated by IOC detected on 4 hosts involving 4 users		0	4	484	0

Alerts

action	action_pretty	alert_id	category	description	detection_timestamp	host_ip	host_name
DETECTED	Detected	786	IP	Product: IOC Alert: IOC (1.1.1.1) Severity: Medium Process: C:\Program Files (x86)\AnyDesk\AnyDesk.exe	1550204850393	192.168.0.10,192.168.100.1,192.168.238.1,192.168.86.1	DFWWIN618F
DETECTED	Detected	787	IP	Product: IOC Alert: IOC (1.1.1.1) Severity: Medium Process: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	1550244991813	192.168.55.1,192.168.45.1,192.168.35.1,10.3.232.20	SJCWIN8PYL
DETECTED	Detected	788	IP	Product: IOC Alert: IOC (1.1.1.1) Severity: Medium Process: C:\Windows\System32\svchost.exe	1550247037718	10.72.100.44,192.168.1.135	DFWWIN3T4I

Navigate to Related Incidents view by using `option+5`

Figure 2: View of Cortex XDR incident within Demisto

Benefit: Leveraging Cortex XDR's threat detection capabilities along with Demisto's security orchestration and automation helps teams unify response processes across their product stack. Demisto playbooks triggered off Cortex XDR data help minimize screen switching, manual reconciliation of data, and repetitive work for security teams.

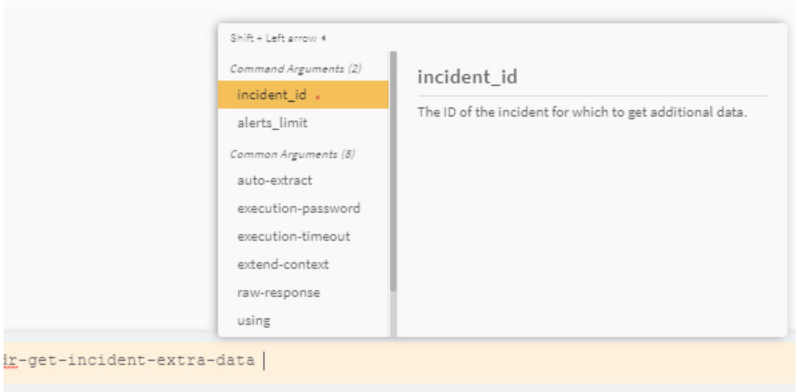
USE CASE #2 REAL-TIME INVESTIGATION FOR COMPLEX THREATS

Challenge: Standardized processes are not enough for responding to every security alert. Attack investigations usually require additional tasks such as pivoting from one suspicious indicator to another to gather critical evidence, drawing relations between incidents, and finalizing resolution. Running these commands across different security products traps teams in a screen-switching and information-collecting cycle that wastes valuable time.

Solution: Cortex XDR stitches data from disparate sources together to provide security teams with sequenced incidents that prevent the need for analysts to manually correlate information and hunt for context. Analysts can also access incident root cause with one click, enabling them to visualize how the attack took place.

Within Demisto, real-time investigation is facilitated through the War Room, a shared space where analysts can collaborate, remotely execute actions across integrated products, and have all their actions documented at one source. Demisto also provides machine learning insights to suggest the most effective analysts and command-sets with time.

Analysts can execute Cortex XDR commands from the Demisto War Room to get high-fidelity incident information. For example, analysts can run the xdr-get-incident-extra-data command along with the appropriate parameters to access information such as related alerts, file artifacts, and network artifacts.



The ID of the incident for which to get additional data.

```
ir-get-incident-extra-data
```

Figure: View of Cortex XDR commands in Demisto War Room

Benefit: Automated and real-time investigation capabilities from Cortex XDR and Demisto help analysts maintain incident oversight across the lifecycle, even when standardized processes aren't enough to enforce end-to-end response.

Cortex XDR's data stitching and causality views help carve a story out of the rows and columns of data that would otherwise be laborious to navigate. Demisto's War Room allows analysts to quickly pivot and run unique commands relevant to incidents in their network 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 the same window. They will also prevent the need for collating information from multiple sources for documentation.

USE CASE #3 PROACTIVE SECURITY FOR CONTINUOUS IMPROVEMENT

Challenge: Even when organizations successfully respond to an incident, it's a challenge to capture the learnings from that incident – what happened, how it happened, and how it can be stopped in the future – and feed them into your security products to prevent those incidents from affecting your organization in the future. Security teams are usually so busy dealing with the incidents of the present that they don't have time to think about preventing the incidents of the future.

Solution: Teams can use both Cortex XDR and Demisto to run threat hunting operations and lend a proactive bent to their security operations. On Cortex XDR, rapid IOC searching, custom rules, and Behavioral Indicators of Compromise (BIOCs) ensure that new information gained is fed back into the system. This new information can be used both to thwart upcoming attacks as well as to retroactively study data and capture previously hidden threats.

Updated incident information can be pulled from Demisto into Cortex XDR to form the basis for the creation of new custom rules.

In Demisto, threat hunting playbooks can be run in real-time or as scheduled exercises. These playbooks can integrate with users' threat intelligence platforms and rapidly search for malicious IOCs before automating enforcement actions.

Benefit: Custom rules and threat hunting enable teams to continue deriving value from their Cortex XDR and Demisto deployments, resulting in a security product stack that learns with time and runs new operations on old data rather than employ a 'no news is good news' approach.