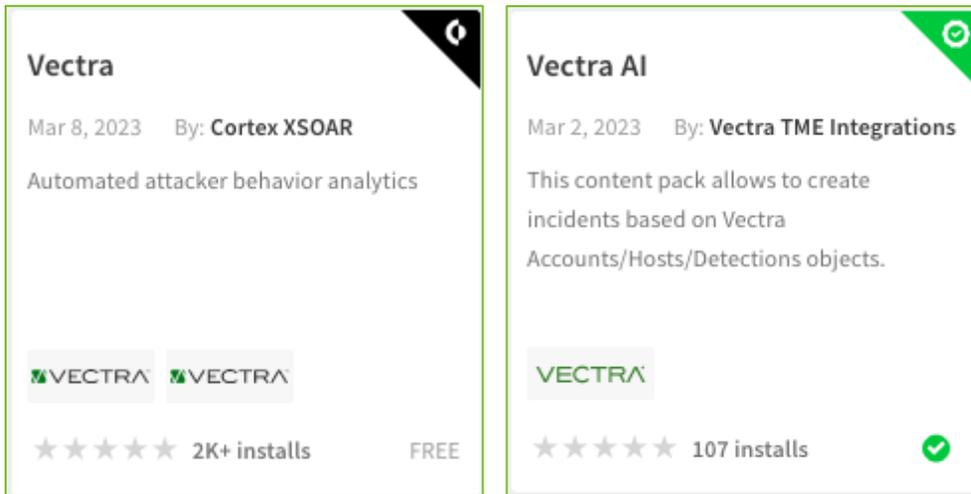# Vectra for XSOAR
Content Pack Deprecation Notice

April 2023

Deprecation Notice

The Vectra content pack provided by Cortex XSOAR (named Vectra) will be deprecated in April 2023. A new verion of the content pack (named Vectra AI) by Vectra TME Integrations is available in the marketplace and those using the Cortex XSOAR (Vectra) content pack are encouraged to migrate to the currently supported Vectra AI content pack. The previous content pack will continue to function but users will need to migrate to the new content pack should support be required.

Vectra

Mar 8, 2023   By: **Cortex XSOAR**

Automated attacker behavior analytics

★ ★ ★ ★ ★   2K+ installs   FREE

Deprecated Content Pack

Vectra AI

Mar 2, 2023   By: **Vectra TME Integrations**

This content pack allows to create incidents based on Vectra Accounts/Hosts/Detections objects.

★ ★ ★ ★ ★   107 installs

Active Content Pack

Replacement Commands

Vectra has developed a new XSOAR content pack to replace the legacy Cortex XSOAR content pack. This new content pack includes commands that replace and extend the functionality of existing commands. The following table outlines which commands should be used for updating existing integrations.

LEGACEY COMAND (Vectra Content Pack)	REPLACEMENT COMMAND (Vectra AI Content Pack)
vec-detections	vectra-search-detections
vectra-detections	vectra-search-detections
vectra-get-detections	vectra-search-detections
vectra-get-detection-by-id	vectra-detection-describe
vec-get-detetctions-by-id	vectra-search-detections
vec-hosts	vectra-search-hosts
vectra-hosts	vectra-search-hosts
vectra-get-hosts	vectra-search-hosts
vec-get-host-by-id	vectra-host-describe
vectra-get-host-by-id	vectra-host-describe

vectra-get-users	vectra-search-users
vectra-search	vectra-search-hosts, vectra-search-detections

New Commands

In addition to the replacement commands, new functionality is included with the current content pack. The following table outlines the new functionality provided.

NEW COMMAND	NEW COMMAND DESCRIPTION
vectra-search-accounts	Returns a list of Account objects
vectra-search-assignments	Return a list of assignments
vectra-search-outcomes	Returns a list of assignment outcomes
vectra-account-describe	Returns a single Account details
vectra-account-add-tags	Add tags to an Account
vectra-account-del-tags	Delete tags from an Account
vectra-host-add-tags	Add tags to an Host
vectra-host-del-tags	Delete tags from an Host
vectra-detection-get-pcap	Returns a Detection's PCAP file (if available)
vectra-detection-markasfixed	Marks/Unmarks a Detection as fixed by providing the Detection ID
vectra-detection-add-tags	Add tags to a Detection
vectra-detection-del-tags	Delete tags from a Detection
vectra-outcome-describe	Returns a single outcome details
vectra-outcome-create	Creates a new assignment outcome
vectra-assignment-describe	Returns a single assignment details
vectra-assignment-assign	Assigns an Account/Host entity to a Vectra User for investigation
vectra-assignment-resolve	Resolves an assignment by selecting resolution scheme

Deprecated Commands

Several commands from the initial content pack have been deprecated and not carried forward into the active content pack. These commands were deprecated because they didn't provide any security use cases used by security analysts. These obsoleted commands primarily pertained to system settings and not security monitoring context.

DEPRECATED COMMAND	STATUS	DEPRECATED COMMAND REASON
vec-settings	deprecated	No security use case
vectra-settings	deprecated	No security use case
vec-health	deprecated	No security use case
vectra-health	deprecated	No security use case

vec-triage	deprecated	Use mark as fixed, assignments, resolutions
vectra-triage	deprecated	Use mark as fixed, assignments, resolutions
vec-sensors	deprecated	No security use case
vectra-sensors	deprecated	No security use case
vectra-get-proxies	deprecated	No security use case
vectra-get-threatfeed	deprecated	No security use case – lists feed not IOCs

Recommended Action

Those using the legacy Vectra content pack should review their playbooks to determine the commands that require migration. The current content pack can support the legacy parameters for ingesting data to create incidents but it's most likely the user will want to expand the parameters to take advantage of the expanded support the new content pack brings.