DEMISTO
A PALO ALTO NETWORKS® COMPANY | okta

Automated Identity-driven Incident Response

Benefits

- Orchestrated response actions enable identity to serve as security control point
- Contain and remediate threats quickly by automating identity-centric actions
- Enhance visibility on user activity and identity contex

Compatibility

- Products: Demisto Enterprise, Okta

Overview

Attackers are increasingly targeting people, rather than infrastructure, forcing security teams to consider security strategy around identity as a key control point. This can put additional burden on security teams that already manage a variety of disparate tools that often lack integration and automation capabilities. In addition, these teams are also strapped with limited resources, including time and talent, which makes it harder to manage and protect their environments.

Okta and Demisto integration features:

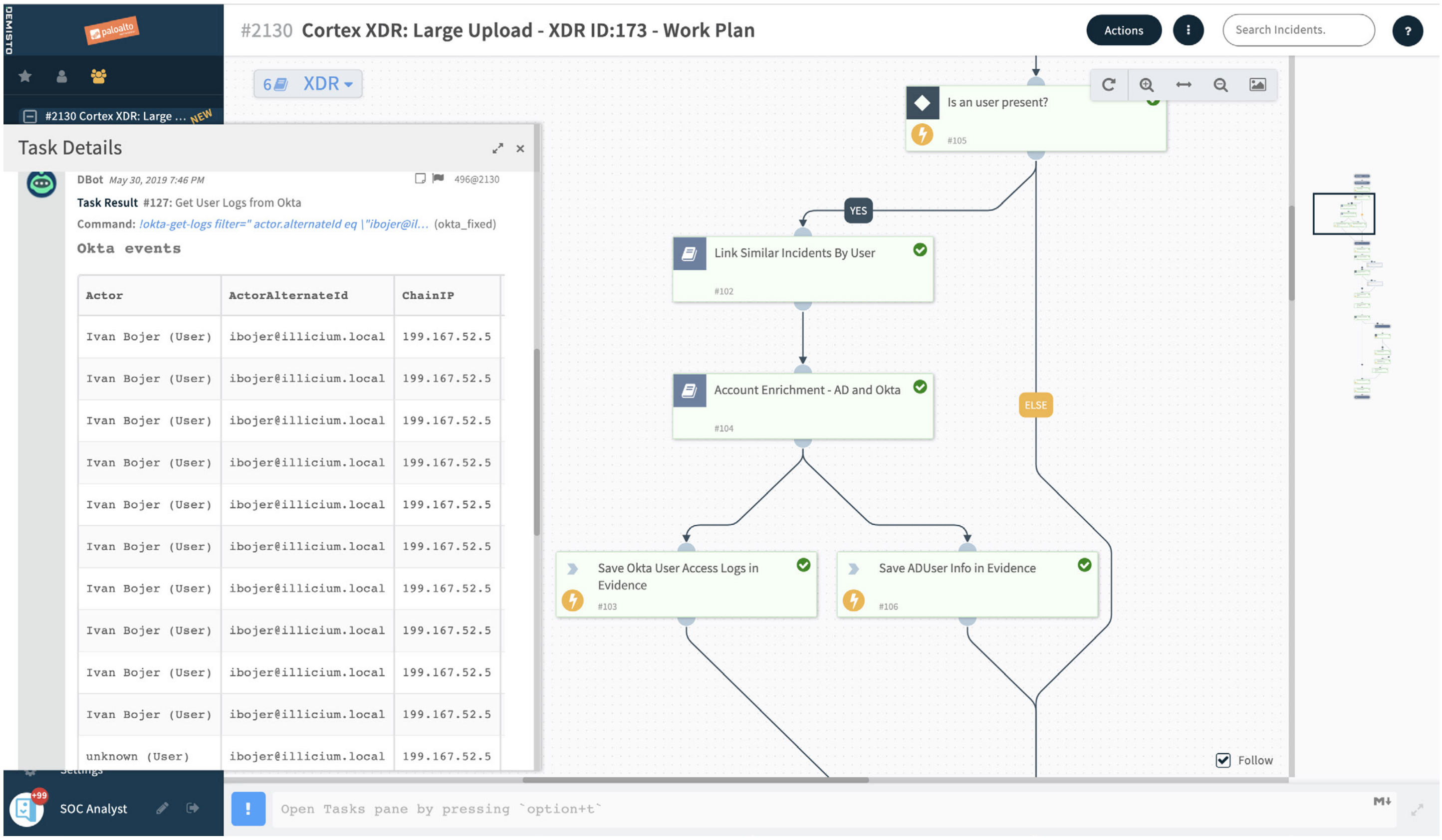
- Automate identity context and user activity enrichment of security alerts as they arise.
- Query user activity for risky events, like failed logins and new factor enrollments to get in front of threats as they emerge.
- Prioritize alerts and orchestrate automated remediation actions based on pre-defined workflows and policies.

USE CASE #1 BETTER VISIBILITY INTO IDENTITY-CENTRIC INCIDENTS

Challenge: Security teams manage complex environments, often with siloed information and manual processes. However, it may also not be practical for every team to have direct access to identity management systems to monitor access for specific, limited subsets of users.

Solution: Demisto playbooks ingest alerts and automate identity context and user activity enrichment, allowing security analysts to query user activity for risky events, like failed log-ins or factor enrollments, without having to leave the Demisto platform. Okta playbooks within Demisto also enable additional enrichment so security teams can instantly view a user's groups and roles, what apps and data they can access, and other contextual information to further enhance the investigation of threats.

Benefit: The Okta integration provides comprehensive visibility into user activity to streamline the investigation process in Demisto. Okta administrators can extend visibility to other security teams as needed, without having to provide direct access to the Okta platform.


DEMISTO
paloalto
#2130 Cortex XDR: Large … NEW
Settings
+99
SOC Analyst
6 XDR
Actions
Search Incidents.
?
Is an user present?
#105
YES
ELSE
Link Similar Incidents By User
#102
Account Enrichment - AD and Okta
#104
Save Okta User Access Logs in Evidence
#103
Save ADUser Info in Evidence
#106
Follow
M↓

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

Task Details

DBot *May 30, 2019 7:46 PM* 496@2130

Task Result #127: Get User Logs from Okta

Command: *!okta-get-logs filter=" actor.alternateId eq \"ibojer@il…* (okta_fixed)

Okta events

Actor	ActorAlternateId	ChainIP
Ivan Bojer (User)	ibojer@illicium.local	199.167.52.5
Ivan Bojer (User)	ibojer@illicium.local	199.167.52.5
Ivan Bojer (User)	ibojer@illicium.local	199.167.52.5
Ivan Bojer (User)	ibojer@illicium.local	199.167.52.5
Ivan Bojer (User)	ibojer@illicium.local	199.167.52.5
Ivan Bojer (User)	ibojer@illicium.local	199.167.52.5
Ivan Bojer (User)	ibojer@illicium.local	199.167.52.5
Ivan Bojer (User)	ibojer@illicium.local	199.167.52.5
Ivan Bojer (User)	ibojer@illicium.local	199.167.52.5
Ivan Bojer (User)	ibojer@illicium.local	199.167.52.5
unknown (User)	ibojer@illicium.local	199.167.52.5

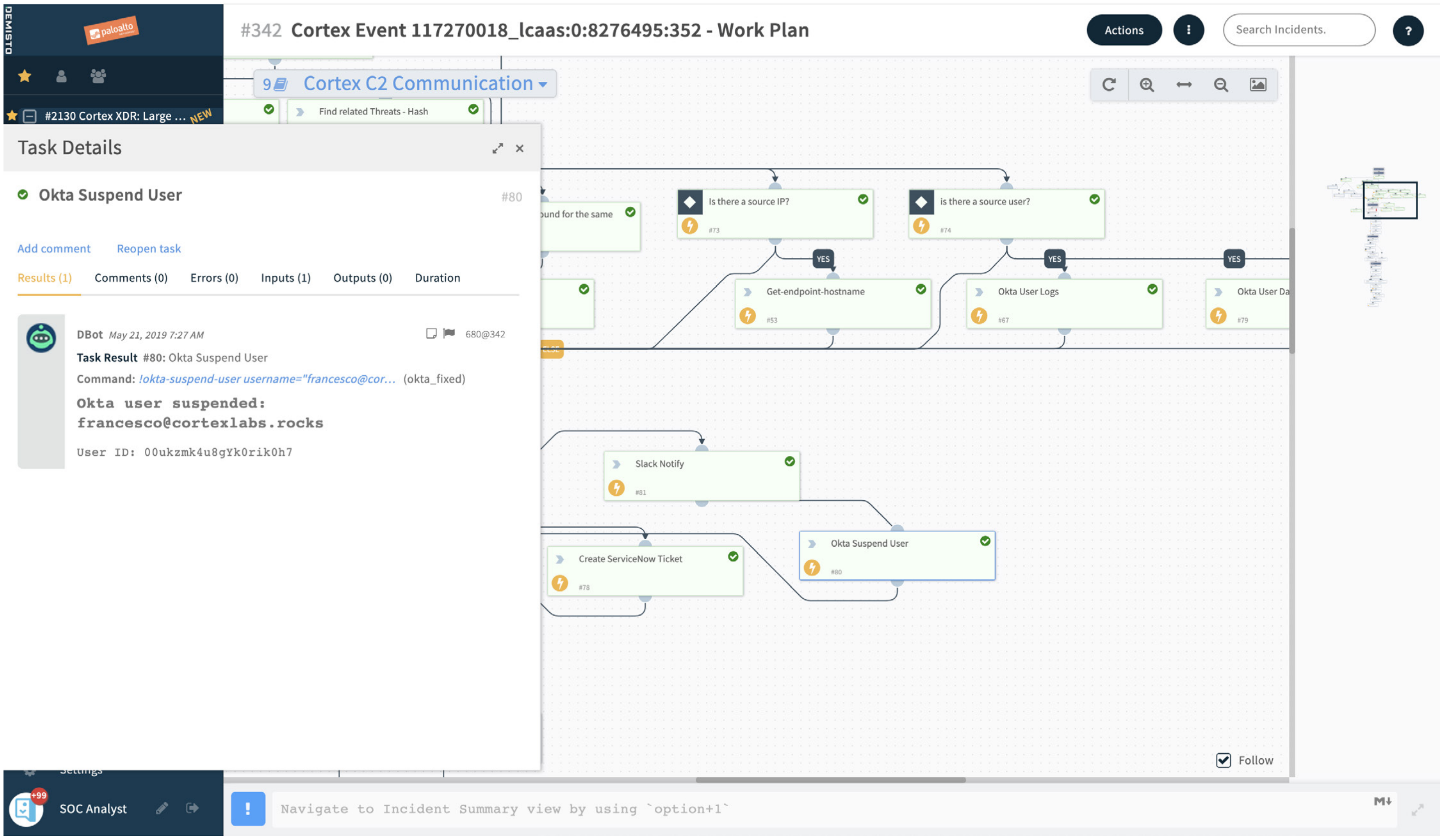
Open Tasks pane by pressing `option+t`

USE CASE #2 ORCHESTRATE AND AUTOMATE IDENTITY-CENTRIC SECURITY RESPONSE

Challenge: Security teams often have a variety of security tools at their disposal. Given that resources can often be limited, they need these tools to integrate better together to enable workflow automation across the entire incident management lifecycle.

Solution: In order to close the security loop, Okta and Demisto also integrate to enable identity-centric orchestrated response actions. Now security teams can better respond to suspicious account activity, like a log-in from a new device or location, by running playbooks to automatically restrict access to sensitive applications or prompt for step-up authentication. If, after further investigation, the user does appear to be compromised, playbooks can take additional remediation actions by suspending the compromised account and conducting a password reset. Together, Okta and Demisto enable automated actions to enforce identity as a security control point.

Benefit: Automated playbooks leveraging the Okta and Demisto integration speed up response to the threat of suspicious activity on a user account by adjusting the user group and associated security policies, without the need for analyst intervention. An analyst can be notified only if further investigation is required. This process frees up analyst time from repeatable, straight-forward incident response tasks to focus on the more complex cases.



#342 Cortex Event 117270018_lcaas:0:8276495:352 - Work Plan

Task Details

Okta Suspend User #80

DBot May 21, 2019 7:27 AM 680@342

Task Result #80: Okta Suspend User

Command: !okta-suspend-user username="francesco@cor… (okta_fixed)

```
Okta user suspended:
francesco@cortexlabs.rocks

User ID: 00ukzmk4u8gYk0rik0h7
```

Navigate to Incident Summary view by using `option+1`

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 6,500 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, visit https://www.okta.com/.

About Demisto

Demisto, a Palo Alto Networks company, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Demisto, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit www.demisto.com.