Cisco Cloud Security APIs and Splunk

Best Practices In Practice

Yaron Caspy
Product Manager

DEVNET-2125

Cisco Webex App

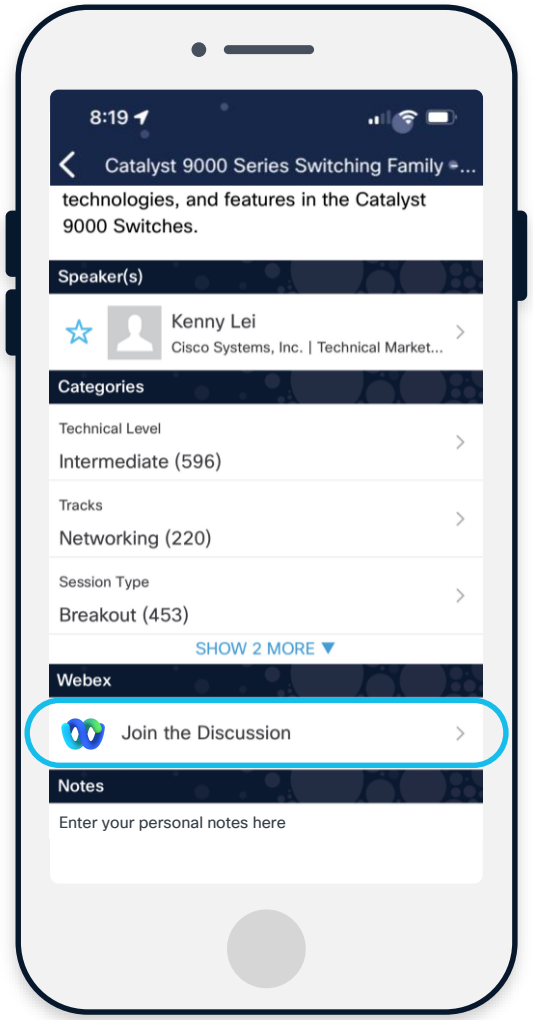
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 13, 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#DEVNET-2125**

Agenda

01 Introduction

02 Evolving Best Practices

03 Interactive Dashboards

04 Balancing Enrichment

05 What's Next

06 Resources

Introduction

Introduction

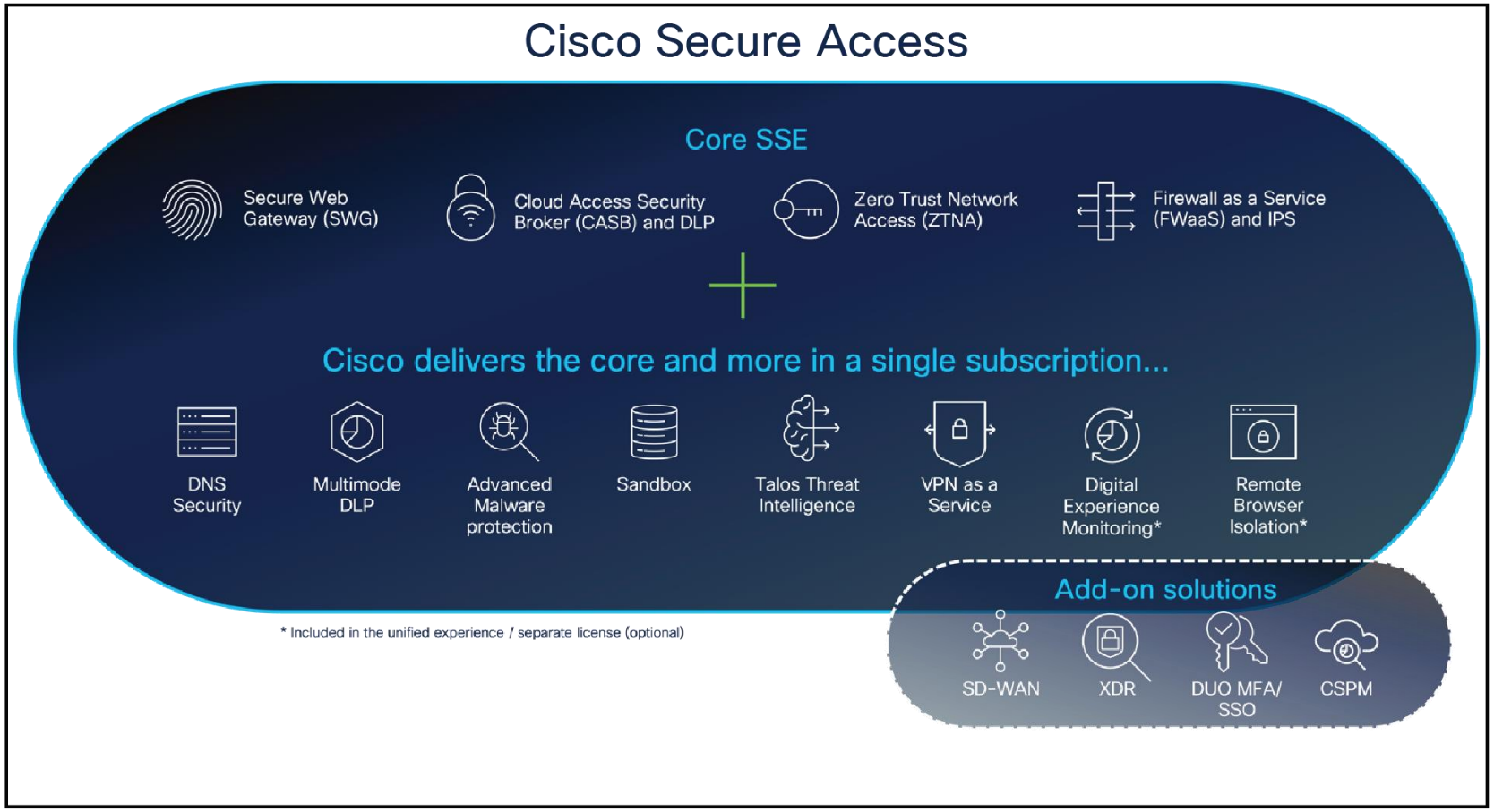
Cisco Umbrella

SWG

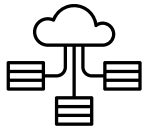
CASB

DNS security

CDFW

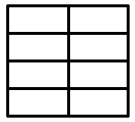


Splunk Development

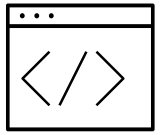


GET

Present



Store

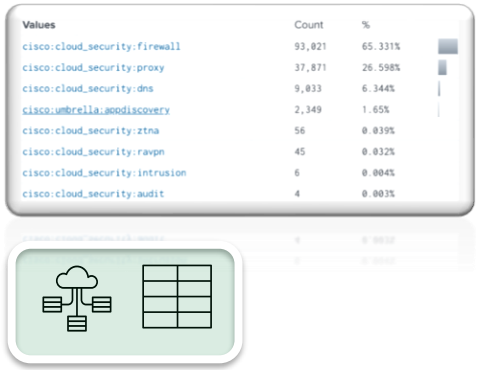


Invoke

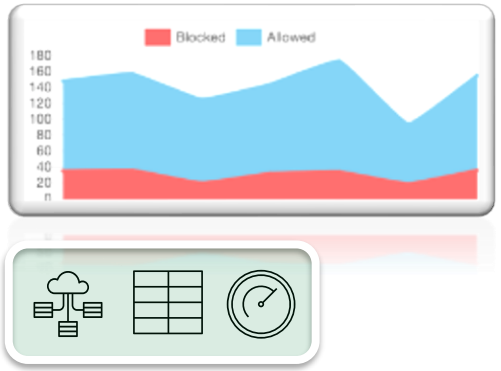
SOC/NOC Use Cases

and Common Practices

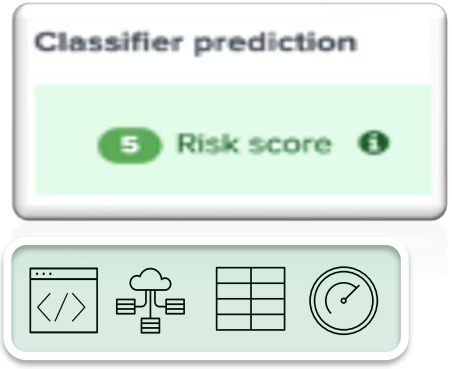
Query



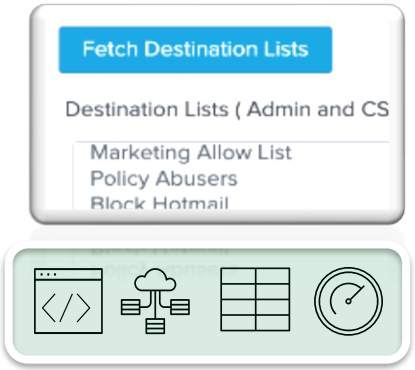
Monitor



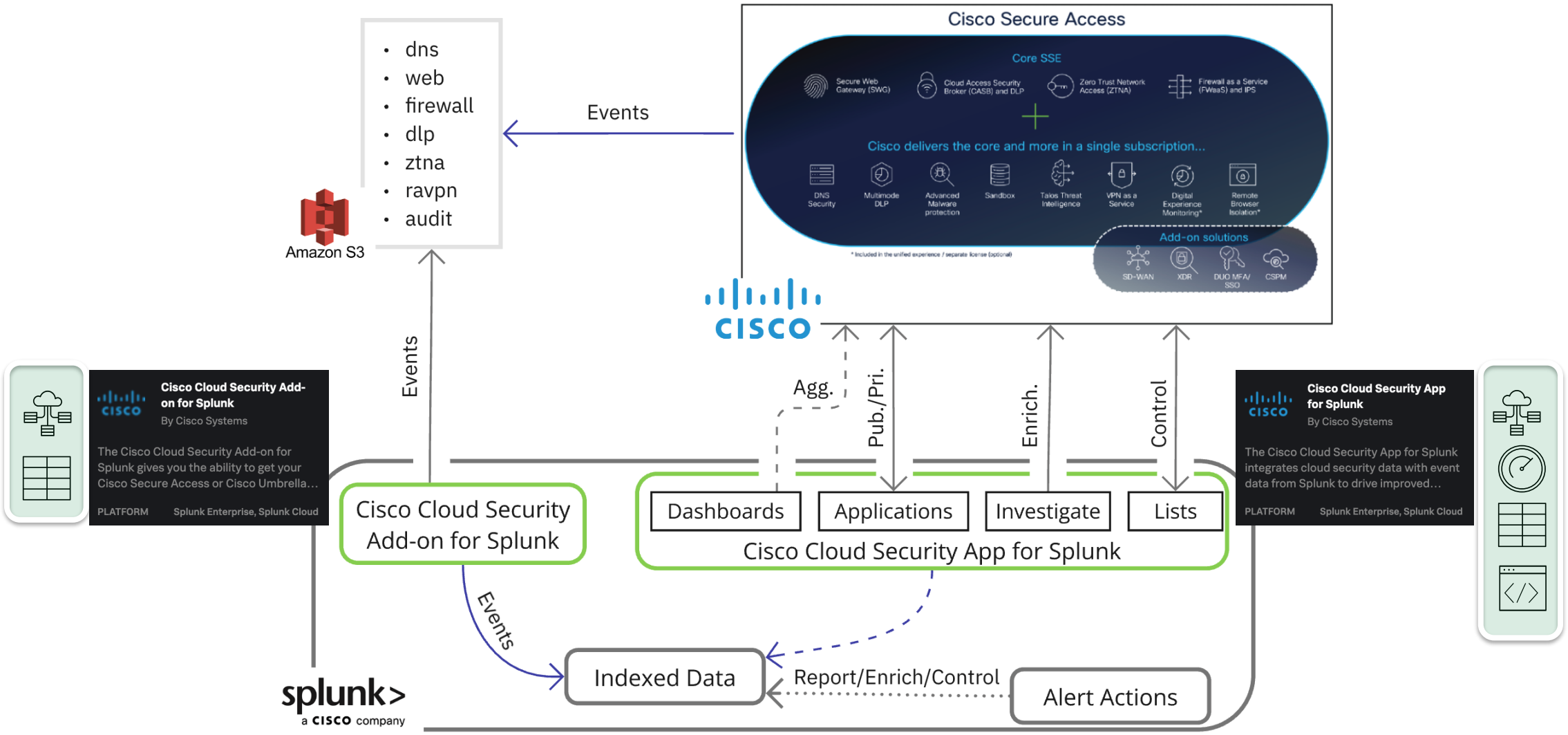
Analyze/Investigate



Act



In Practice



Evolving Best Practices

Act 1: The Straightforward Approach

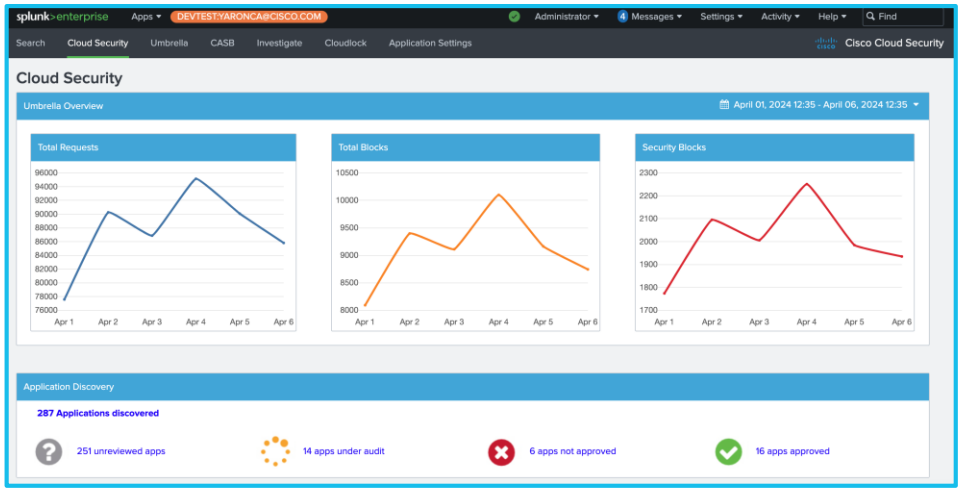
Cisco Cloud Security Add-on for Splunk

1 Query

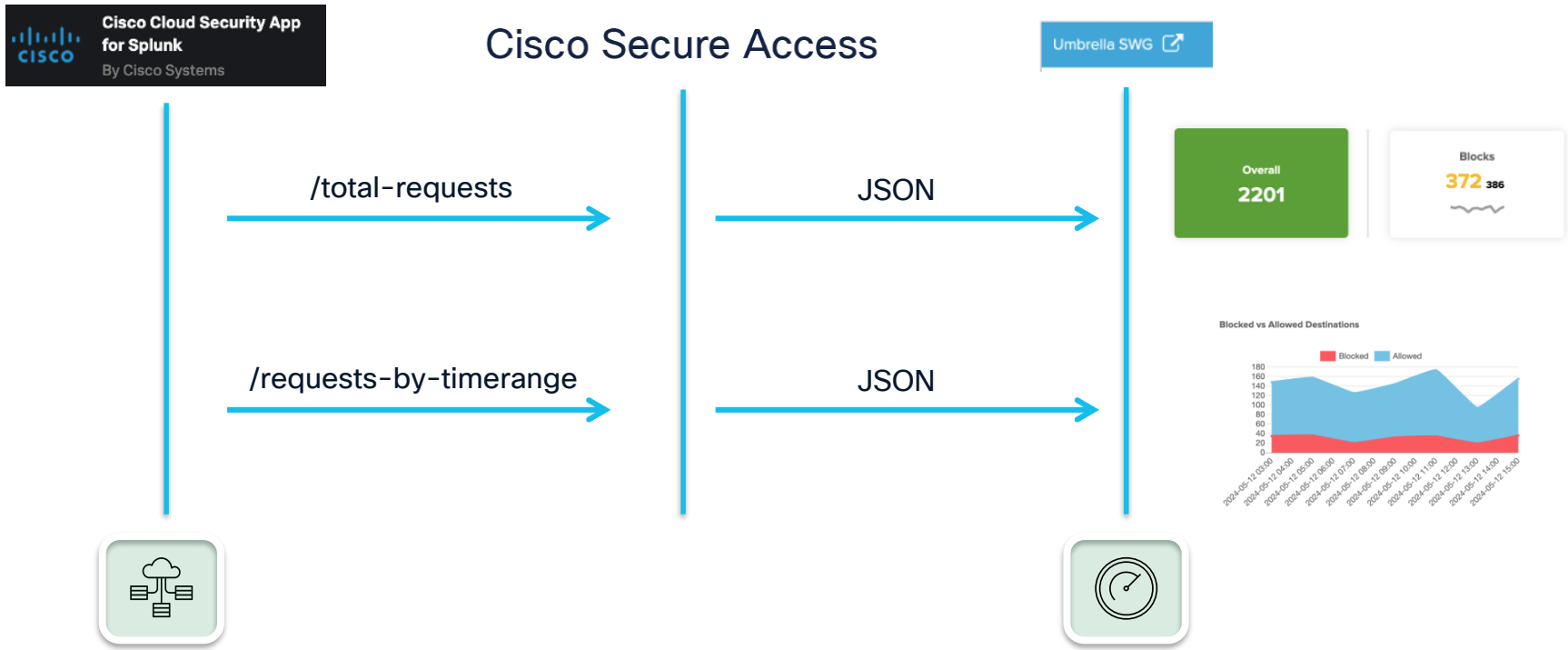
Values	Count	%
cisco:cloud_security:firewall	93,021	65.331%
cisco:cloud_security:proxy	37,871	26.598%
cisco:cloud_security:dns	9,033	6.344%
cisco:umbrella:appdiscovery	2,349	1.65%
cisco:cloud_security:ztna	56	0.039%
cisco:cloud_security:ravpn	45	0.032%
cisco:cloud_security:intrusion	6	0.004%
cisco:cloud_security:audit	4	0.003%

Cisco Cloud Security App for Splunk

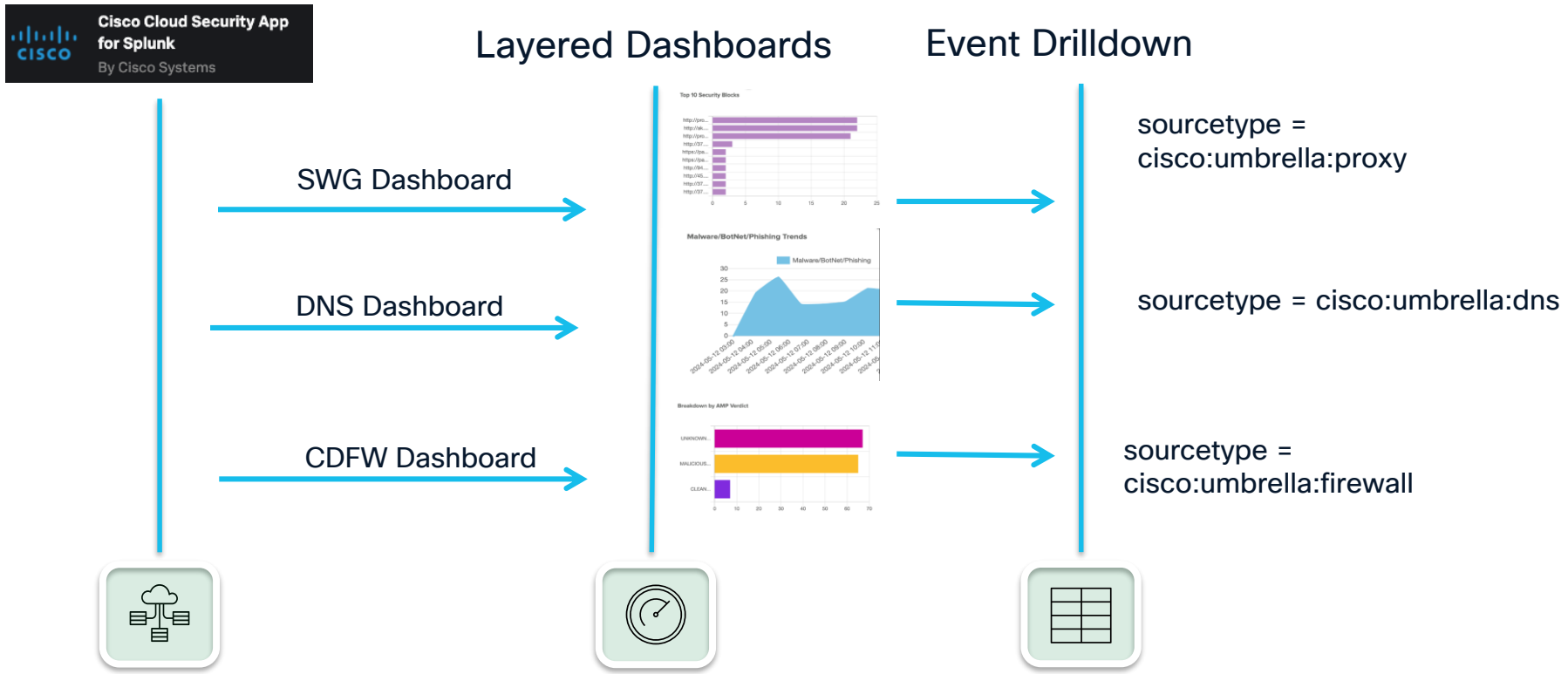
2 Monitor



Act 2: The Need for Speed



Act 3: What about that Granularity?



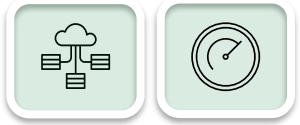
Interactive Dashboards

Implement API Best Practices

Enum

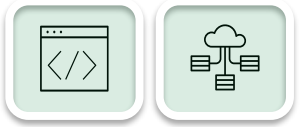
App Discovery

Application Name	Category	Weighted Risk	Label
OpenAI ChatGPT	Generative AI	High	Unreviewed Update
Snapchat	Collaboration	High	Not Approved Update
OpenAI API	Generative AI	High	Unreviewed Update
Skype	Collaboration	Medium	Unreviewed Update
Sentry	IT Service Management	Medium	Unreviewed Update
ZARC	Hosting Services	Medium	Unreviewed Update



Paginate

First Prev 1 2 3 4 5 Next Last



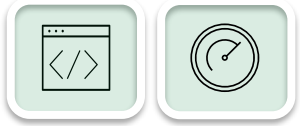
Detail

Application Name : OpenAI ChatGPT

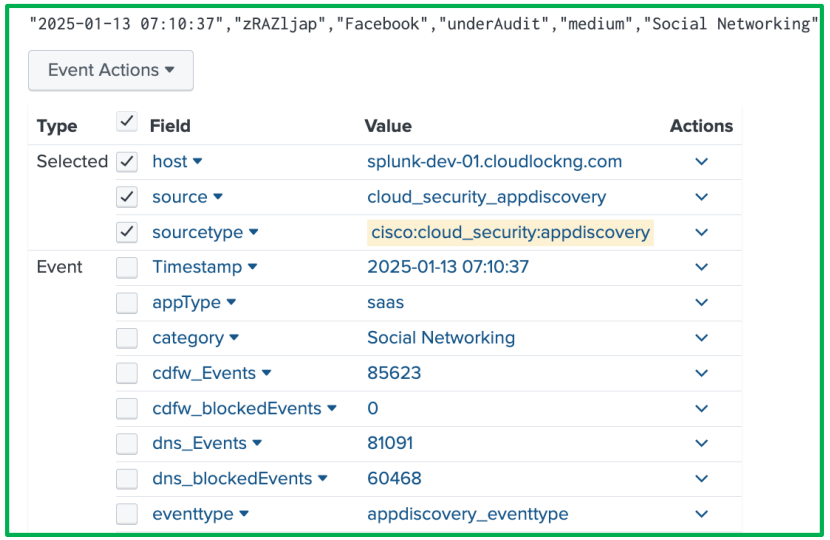
ID :	I9GLZOWa
Description :	Provides a chat based search platform
Risk score :	High
Label :	Unreviewed
Category :	Generative AI
URL :	https://chat.openai.com/chat
Vendor :	OpenAI
First detected :	2024-10-14T00:00:00
Last detected :	2025-01-11T00:00:00

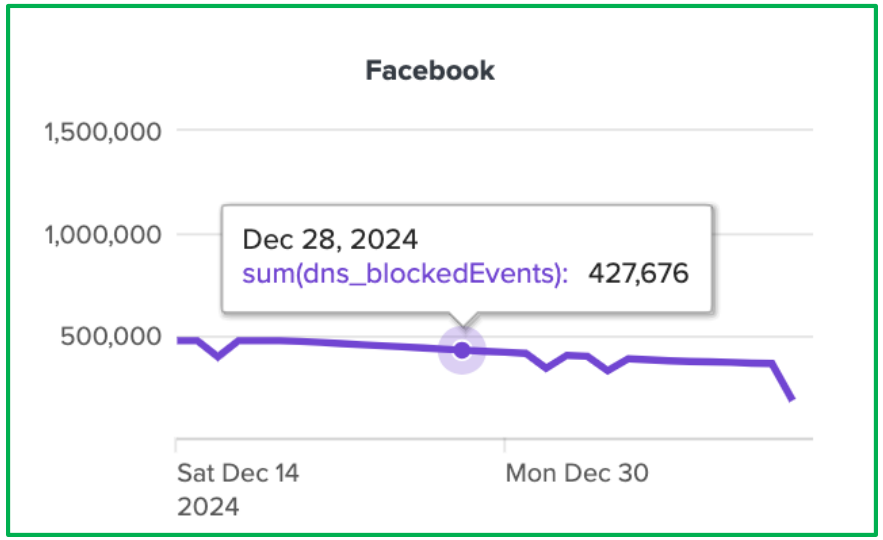
List of identities

Identities Name	DNS Requests	Blocked DNS Requests	Web Traffic
George Orwell (gorwell@tmelabs.com)	126	126	0
Peter Parker (pparker@tmelabs.com)	101	101	0
Robert Banner (rbanner@tmelabs.com)	104	104	0
Steven Rogers (srogers@tmelabs.com)	133	133	0
Tony Stark (tstark@tmelabs.com)	144	144	0



There are exceptions

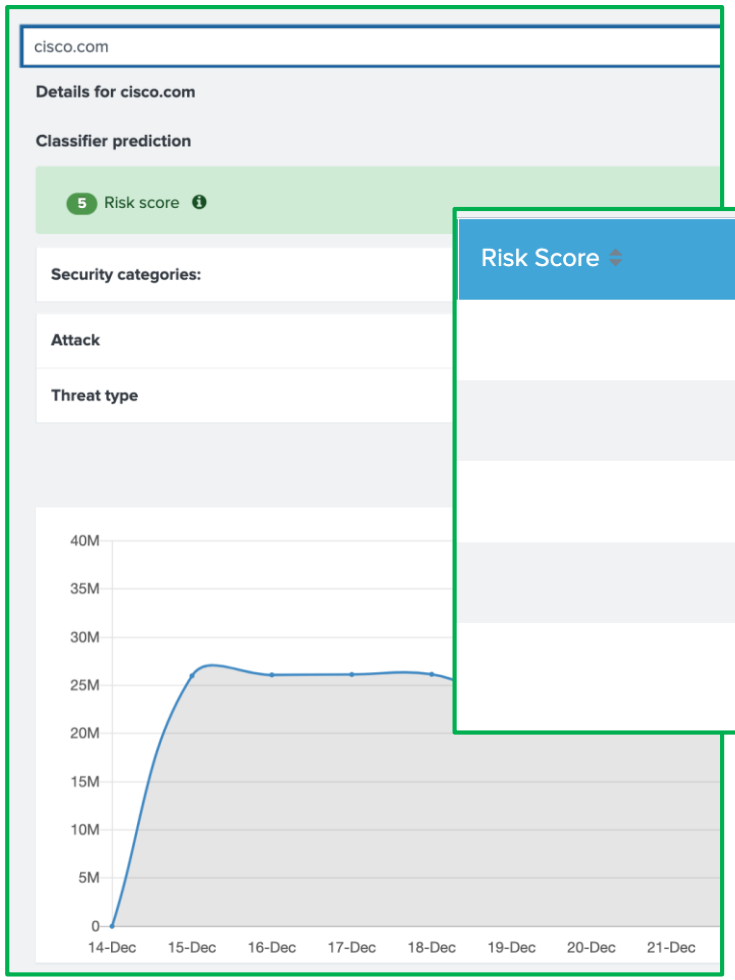




Balancing Enrichment

A Threat Hunter, an Analyst and a CISO walk into a SIEM

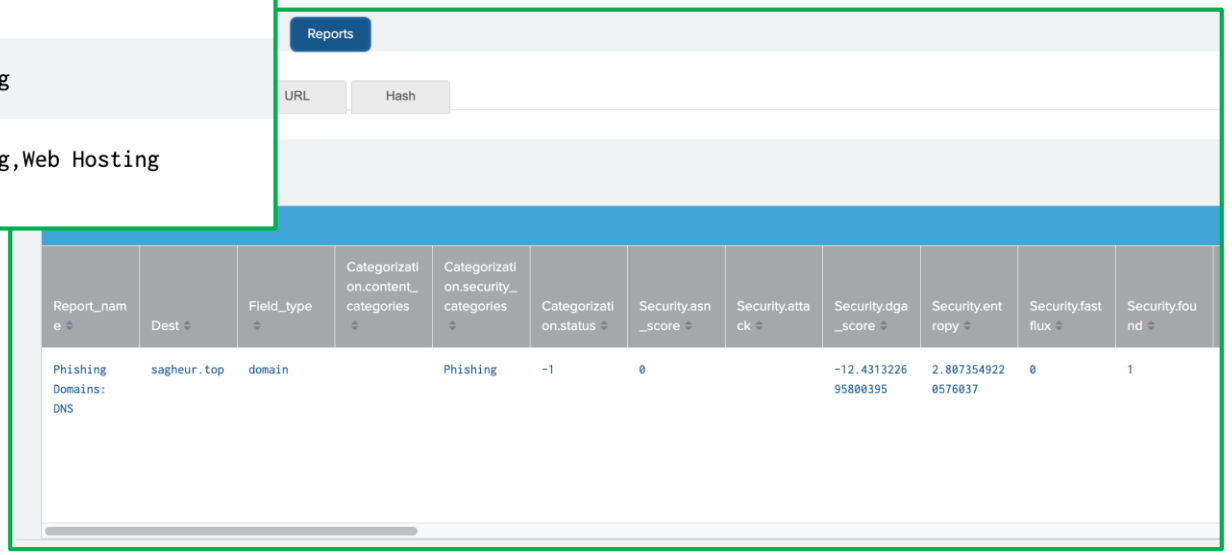
Investigate



Triggered Investigations

Risk Score	Category
100	Malware,Phishing
100	Malware,Phishing
100	Phishing
100	Malware,Phishing
100	Malware,Phishing,Web Hosting

Reports

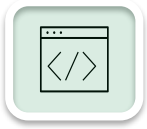


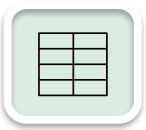
Making Interfaces - Actionable

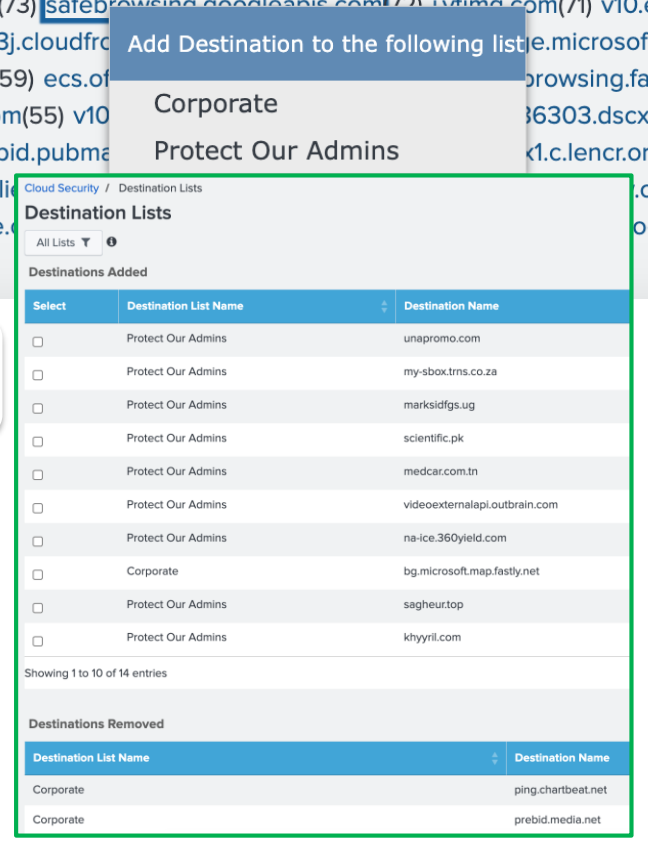
Investigate

Related Domains

google.com(3787) yahoo.com(1494) foxnews.com(1429) get.s-onetag.com(813) btloader.com(480) tr.outbrain.com(425) postrelease.com(362) lb.eu-1-id5-sync.com(233) i.jsrdn.com(213) licensing.bitmovin.c
ping.chartbeat.net(160) www.googletagmanager.com(156) match.sharethrough.com(147) prebid.media.net(147) dsp-cookie.adfarm1.adition.com(129) play.google.com(117) www.yelp.com(104) self.events.data
presence.services.sfb.trafficmanager.net(74) img-s-msn-com.akamaized.net(74) settings-win.data.microsoft.com(74) bg.microsoft.map.fastly.net(73) safebrowsing.googleapis.com(72) i.ytimg.com(71) v10.eve
www.facebook.com(69) id.sv.rkdms.com(68) ad.360yield.com(66) ogads-pa.clients6.google.com(66) login.mso.msidentity.com(66) dt2usiyxy6j3j.cloudfro e.microsoft.c
browser.events.data.microsoft.com(61) clientservices.googleapis.com(61) teams.events.data.microsoft.com(60) s3-w.us-east-1.amazonaws.com(59) ecs.of rowsing.fastly
ocsp2.globalsign.com(56) mobile.events.data.microsoft.com(56) rub-winners-us-east-1-rtb.adroll.com(56) connect-metrics-collector.s-onetag.com(55) v10 36303.dscx.ak
widgets.outbrain.com(53) officewhatsnew.z13.web.core.windows.net(52) aax-eu.amazon-adsystem.com(52) teams.cloud.microsoft(52) hbopenbid.pubma k1.c.lencr.org(4
dc.services.visualstudio.com(49) gsp-ssl.ls-apple.com.akadns.net(49) ak.privatelink.msidentity.com(49) outlook.office365.com(49) signaler-pa.cli .c10
d1ekdn256kz7p5.cloudfront.net(46) prod.roaming1.live.com.akadns.net(46) lh5.googleusercontent.com(45) cdnjs.cloudflare.com(45) chat-e2ee. ogle
videoexternalapi.outbrain.com(41) optimizationguide-pa.googleapis.com(40) turnip.cdn.turner.com(40)







What's Next?

“If you build it”…

1

Cisco Cloud Security Add-on for Splunk

By Cisco Systems

The Cisco Cloud Security Add-on for Splunk gives you the ability to get your Cisco Secure Access or Cisco Umbrella…

PLATFORM Splunk Enterprise, Splunk Cloud

Logs from Secure Access/ Umbrella [via S3]

2

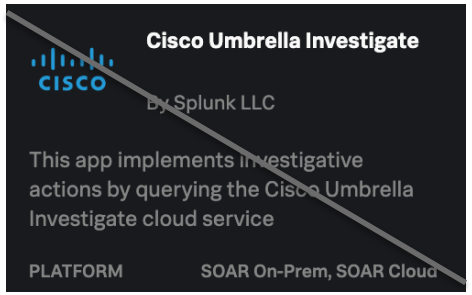
Cisco Cloud Security App for Splunk

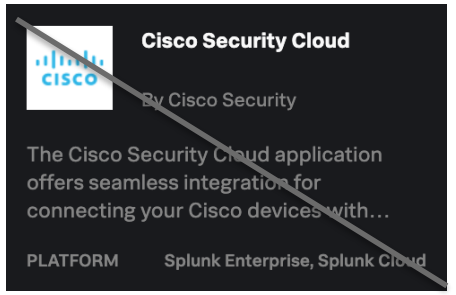
By Cisco Systems

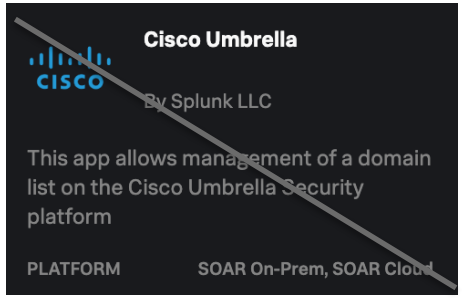
The Cisco Cloud Security App for Splunk integrates cloud security data with event data from Splunk to drive improved…

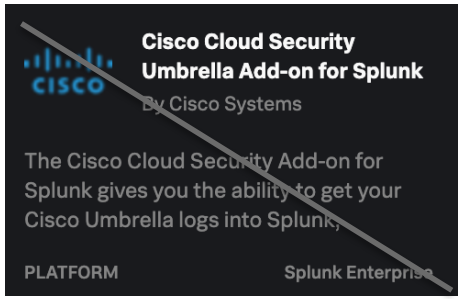
PLATFORM Splunk Enterprise, Splunk Cloud

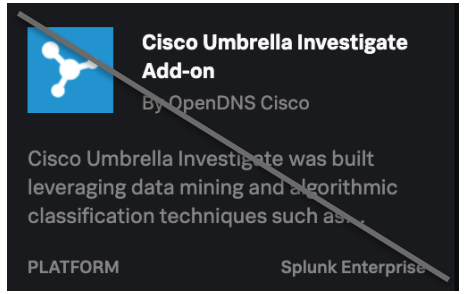
- Secure Access/Umbrella Dashboards [via API]
- Investigate
- Cloudlock

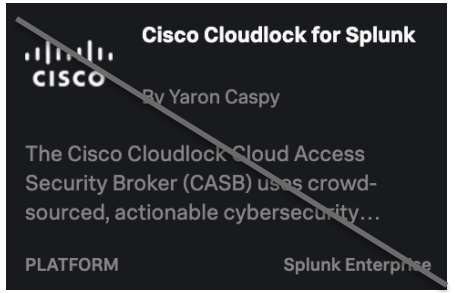












Resources

What Next?

- API Documentation
- Cisco Cloud Security Add-on for Splunk Guide
- Cisco Cloud Security App for Splunk Guide
- DevNet Sandbox for SIG
- Self-paced course on the Umbrella Learning Hub
- Cisco Developer Learning Labs Center

Complete your session evaluations

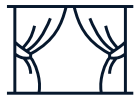
Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: through Webex App

Thank you

cisco Live !


CISCO