

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Cisco Cloud Security APIs and Splunk

Best Practices In Practice

Yaron Caspy, Product Manager
DEVNET-2125



#CiscoLiveAPJC

Cisco Webex App

Questions?

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

How

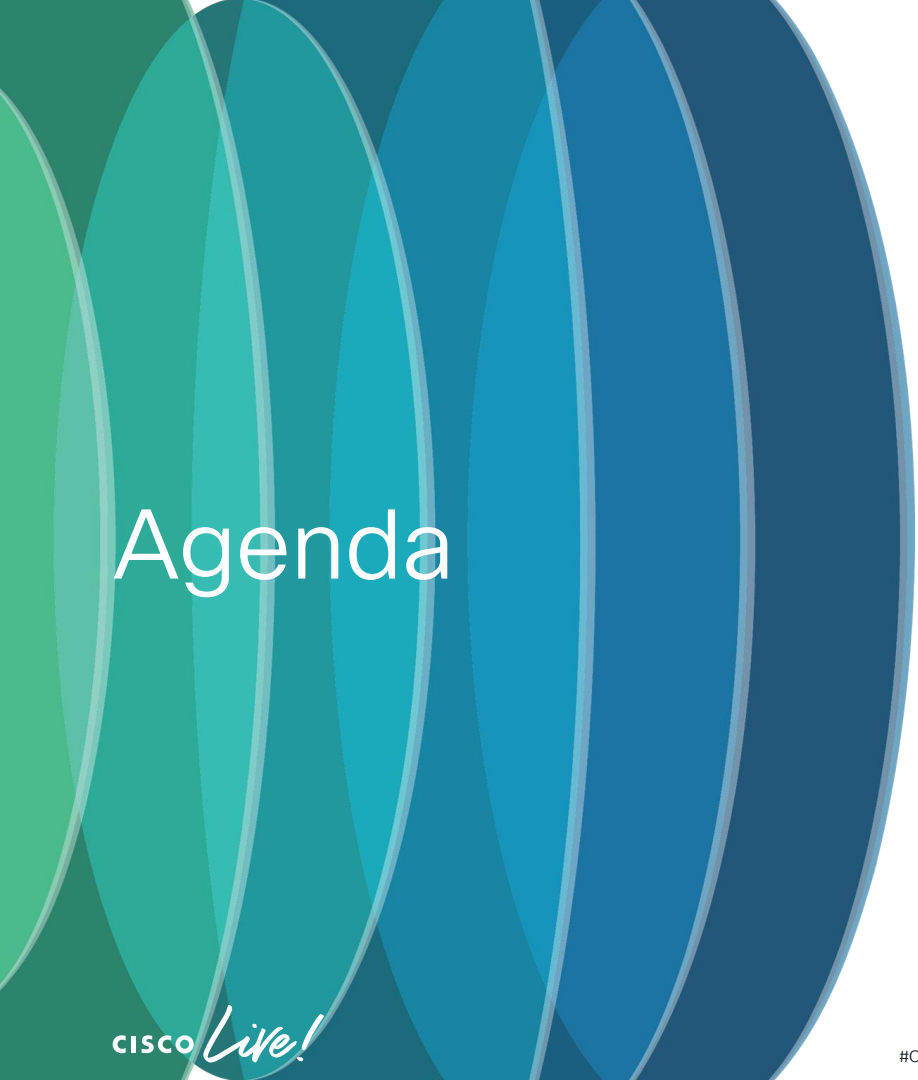
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



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

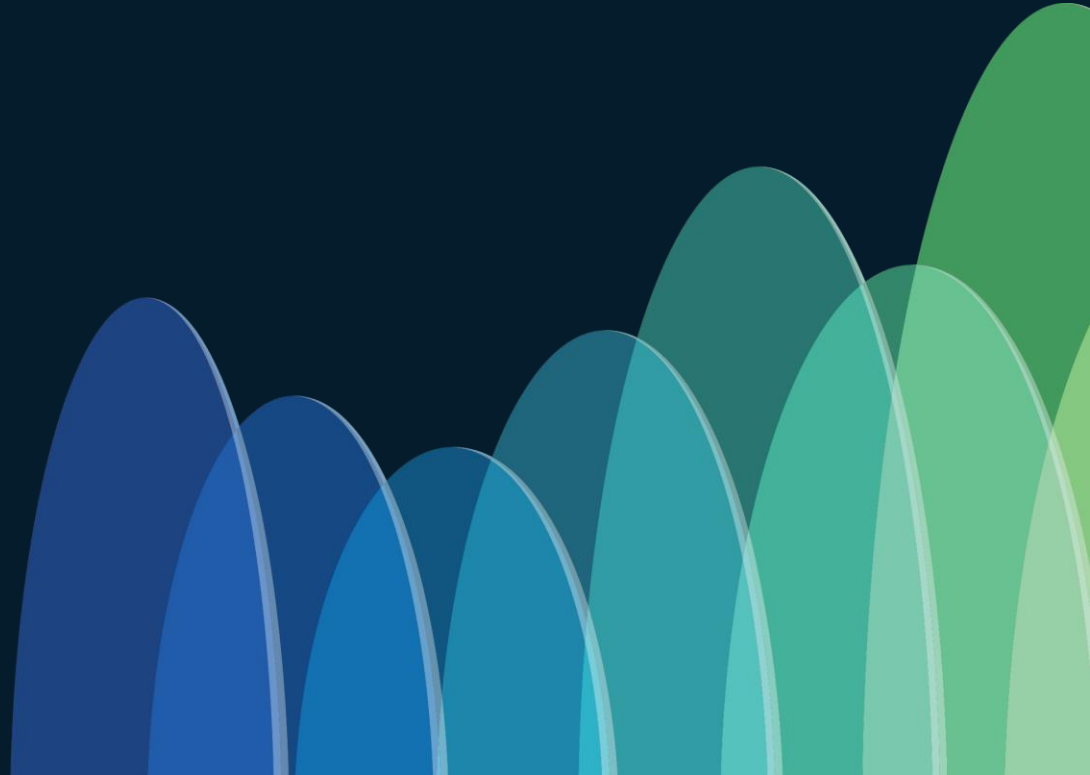




Agenda

- Introduction
- SOC Use Cases and Common Practices
- Migrating to Best Practices
- Granularity AND Speed
- Transparency
- Resources

Introduction



Introduction

Umbrella -> SIG -> SSE -> SASE



Cisco Umbrella

Secure Web
Gateway
(SWG)

Cloud Access
Security Broker
(CASB)

DNS security

Firewall as a
Service
(FWaaS)

Cisco Secure Access

Core SSE



Secure Web
Gateway (SWG)



Cloud Access Security
Broker (CASB) and DLP



Zero Trust Network
Access (ZTNA)



Firewall as a Service
(FWaaS) and IPS



Cisco delivers the core and more in a single subscription...



DNS
Security



Multimode
DLP



Advanced
Malware
protection



Sandbox



Talos Threat
Intelligence



VPN as a
Service



Digital
Experience
Monitoring*



Remote
Browser
Isolation*

* Included in the unified experience / separate license (optional)

Add-on solutions



SD-WAN



XDR



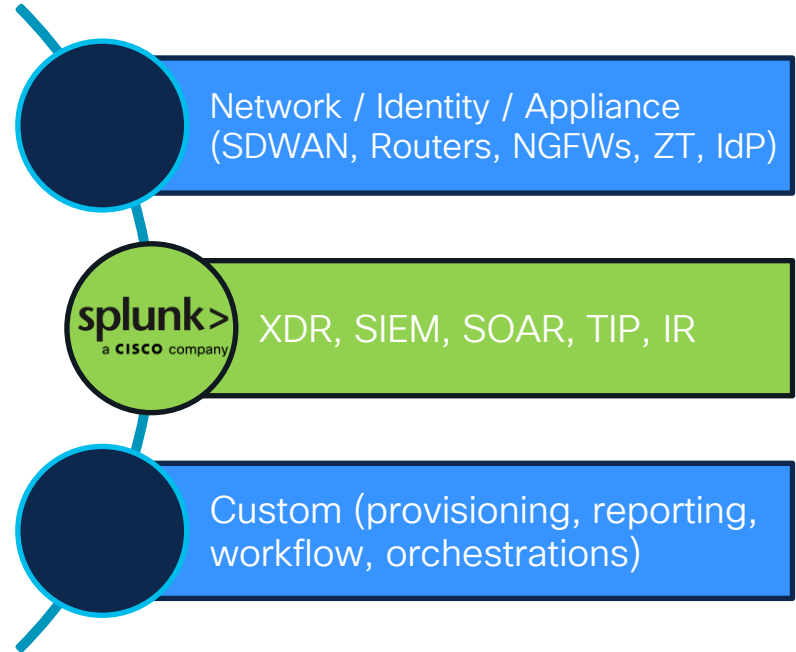
DUO MFA/
SSO



CSPM

cisco *Live!*

Integration Points



Cisco Cloud Security for Splunk

1



Cisco Cloud Security Add-on for Splunk

[Open App](#)

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

Category: [Security, Fraud & Compliance, SIEM](#) | Author: [Cisco Systems](#) | Downloads: 83 |

Released: 23 days ago | Last Updated: 22 days ago | [View on Splunkbase](#)

2



Cisco Cloud Security App for Splunk

[Open App](#)

The Cisco Cloud Security App for Splunk integrates cloud security data with event data from Splunk to drive improved network visibility, faster threat detection, and mitigation response.

This App:

1. Provides visualizations using Cloud Security APIs.
2. Gives SOC's/Threat Hunting teams the ability to learn more about destinations using the Investi... [More](#)

Category: [IT Operations, Security, Fraud & Compliance](#) | Author: [Cisco Systems](#) | Downloads: 1814 |

Released: 4 months ago | Last Updated: 4 months ago | [View on Splunkbase](#)



Cisco Cloud Security Umbrella Add-on for Splunk

[Open App](#)

The Cisco Cloud Security Add-on for Splunk gives you the ability to get your Cisco Umbrella logs into Splunk,

Category: [IT Operations, Security, Fraud & Compliance](#) | Author: [Cisco Systems](#) | Downloads: 3436 |

Released: 6 months ago | Last Updated: 5 months ago | [View on Splunkbase](#)

SOC Use Cases and Common Practices



SOC Use Cases and Common Practices

Take 1

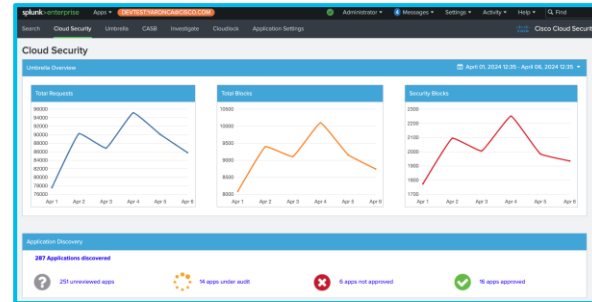
Cisco Cloud Security Add-on for Splunk

1 Ingest

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

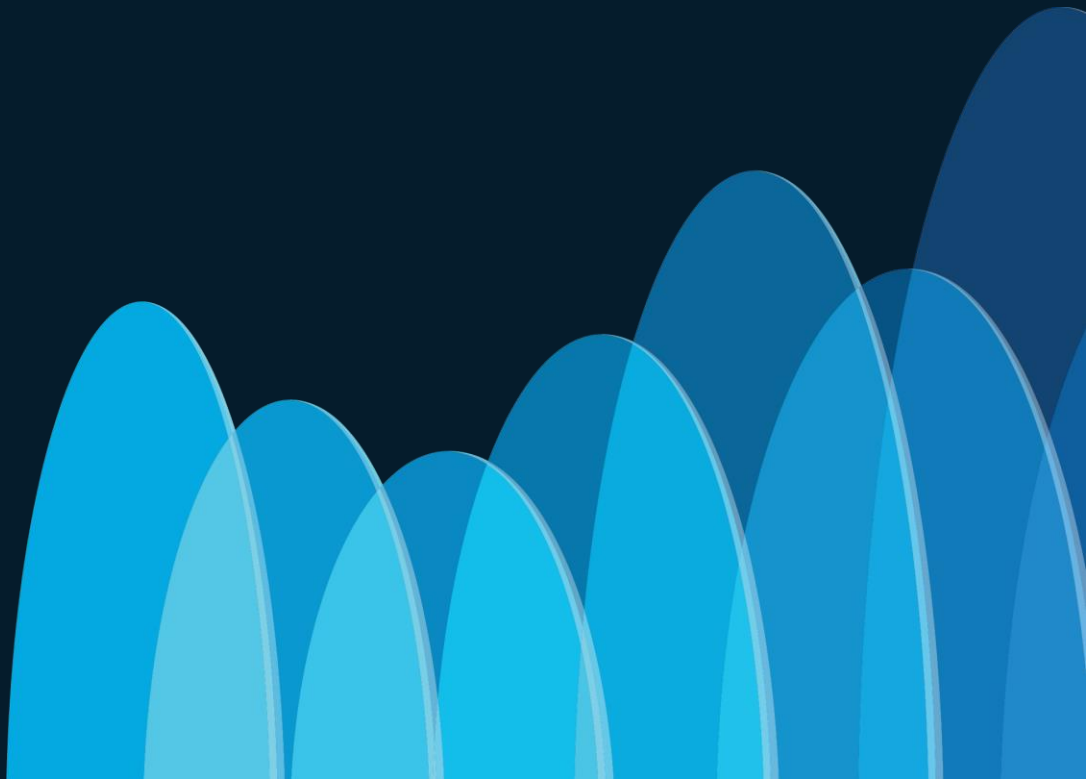
2 Monitor



3 Analyze/Investigate

4 Act

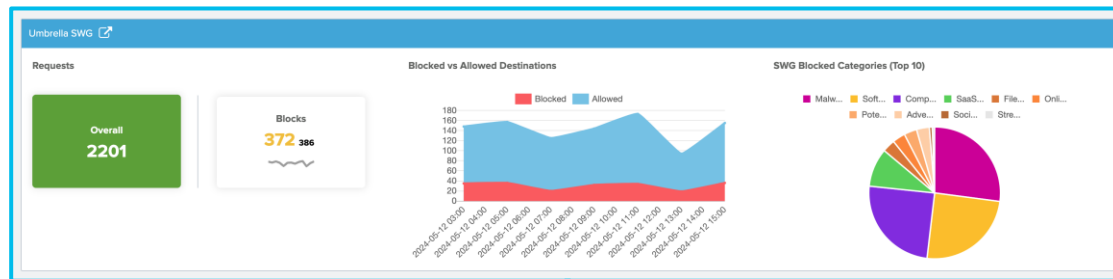
Granularity AND Speed



Granularity AND Speed

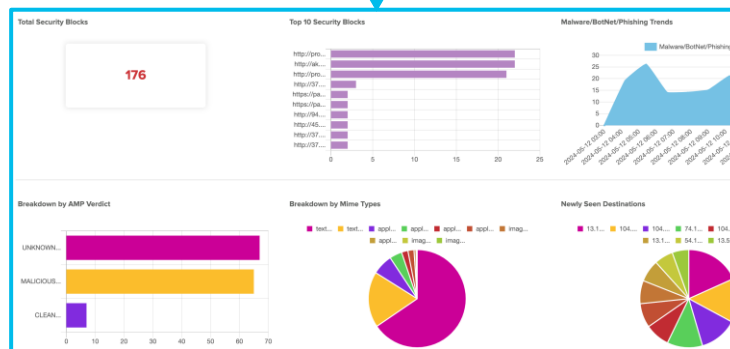
'/total-requests/{0}?from={1}&to={2}&limit=1&offset=0&timezone={3}'

Speed/IO



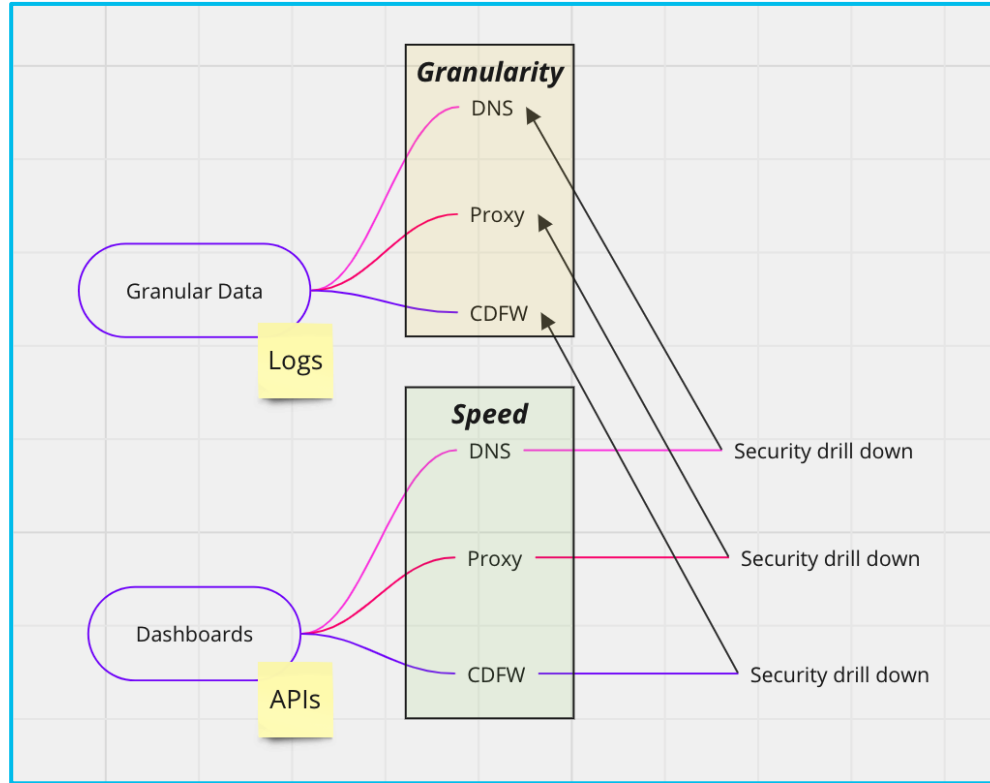
Granularity

"query": 'index="' + proxyIndex + "'
sourcetype = cisco:umbrella:proxy
(category=" *Cryptomining* " OR
category=" *Command and Control* "
OR...

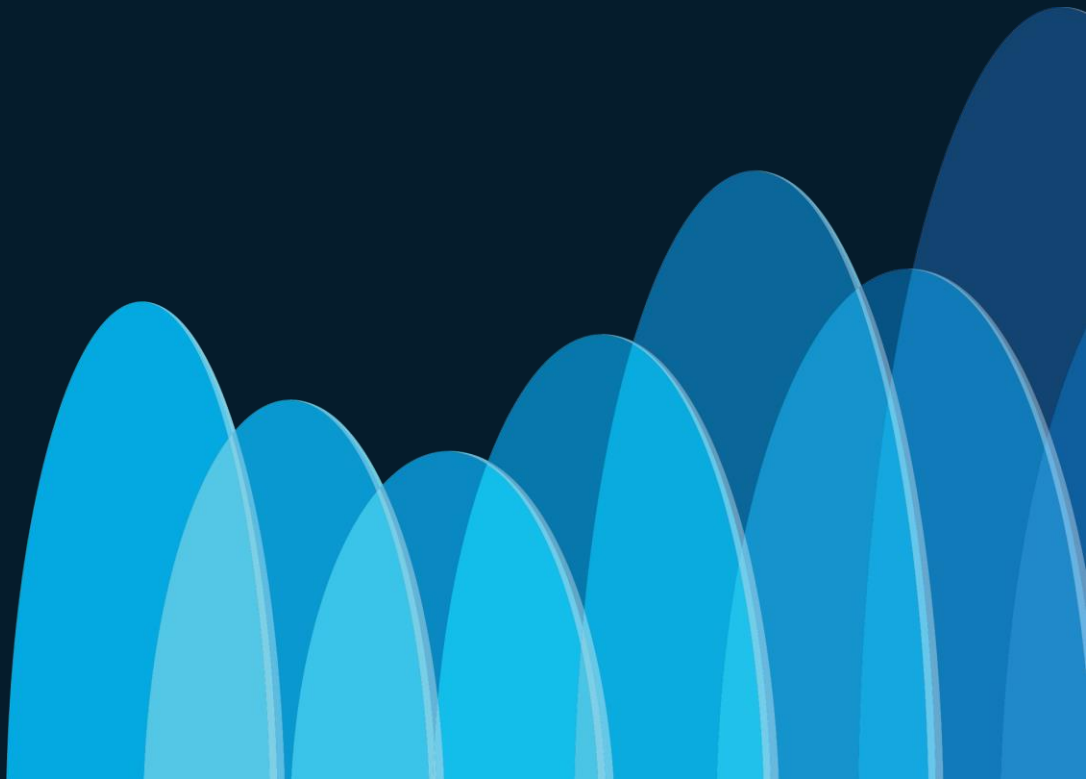


Granularity AND Speed

To Summarize



Transparency



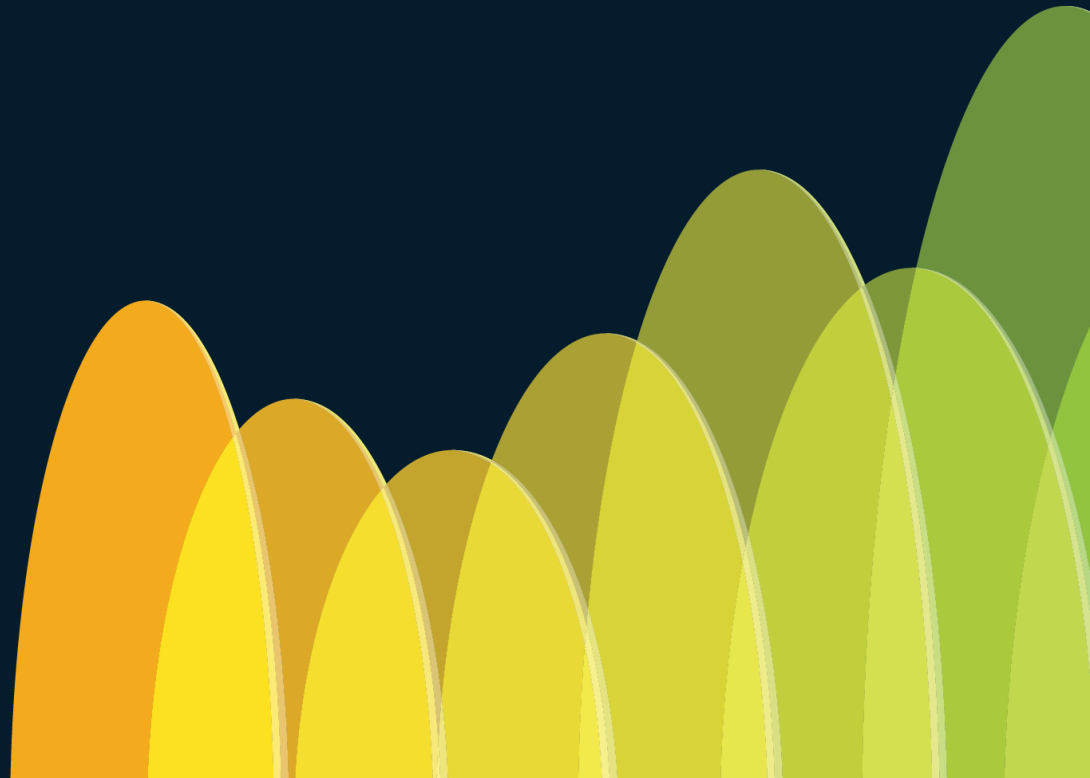
Transparency

```
headers = {'Content-Type': 'application/json',  
          'Accept': 'application/json',  
          'User-Agent': 'CiscoCloudSecurityAppForSplunk/python-requests/3x',  
          'timerange': time_range}
```



```
{"userAgent": "CiscoCloudSecurityAppForSplunk/python-requests/3x",  
 "count": 2242,  
 "requests": [  
   {"path": "/reports.us/v2/total-requests/dns",  
    "verb": "GET",  
    "count": 6},  
   {"path": "/reports.us/v2/total-requests/firewall",  
    "verb": "GET",  
    "count": 6},  
   {"path": "/reports.us/v2/total-requests/proxy",  
    "verb": "GET",  
    "count": 6}.....]}
```

Resources



Resources

- [API Documentation](#)
- [Umbrella API Quick Start 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 claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert 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



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC