

The background of the slide is a vibrant, abstract graphic. It features a series of overlapping, wavy bands of color in a rainbow spectrum, transitioning from red and orange on the left to yellow and green on the right. On the right side, there is a bright, multi-colored sunburst or starburst effect that radiates outwards, with colors ranging from blue and purple to yellow and orange. The overall composition is dynamic and energetic.

cisco *Live!*

Let's go

#CiscoLive



The bridge to possible

Creating Events Out of Data

Deep dive into ThousandEyes event detection

Arash Molavi Kakhki (Head of Research at ThousandEyes)

Prabhnit Singh (Director of Product Management)

BRKAPP-2011

CISCO *Live!*

#CiscoLive

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 9, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKAPP-2011>

Agenda

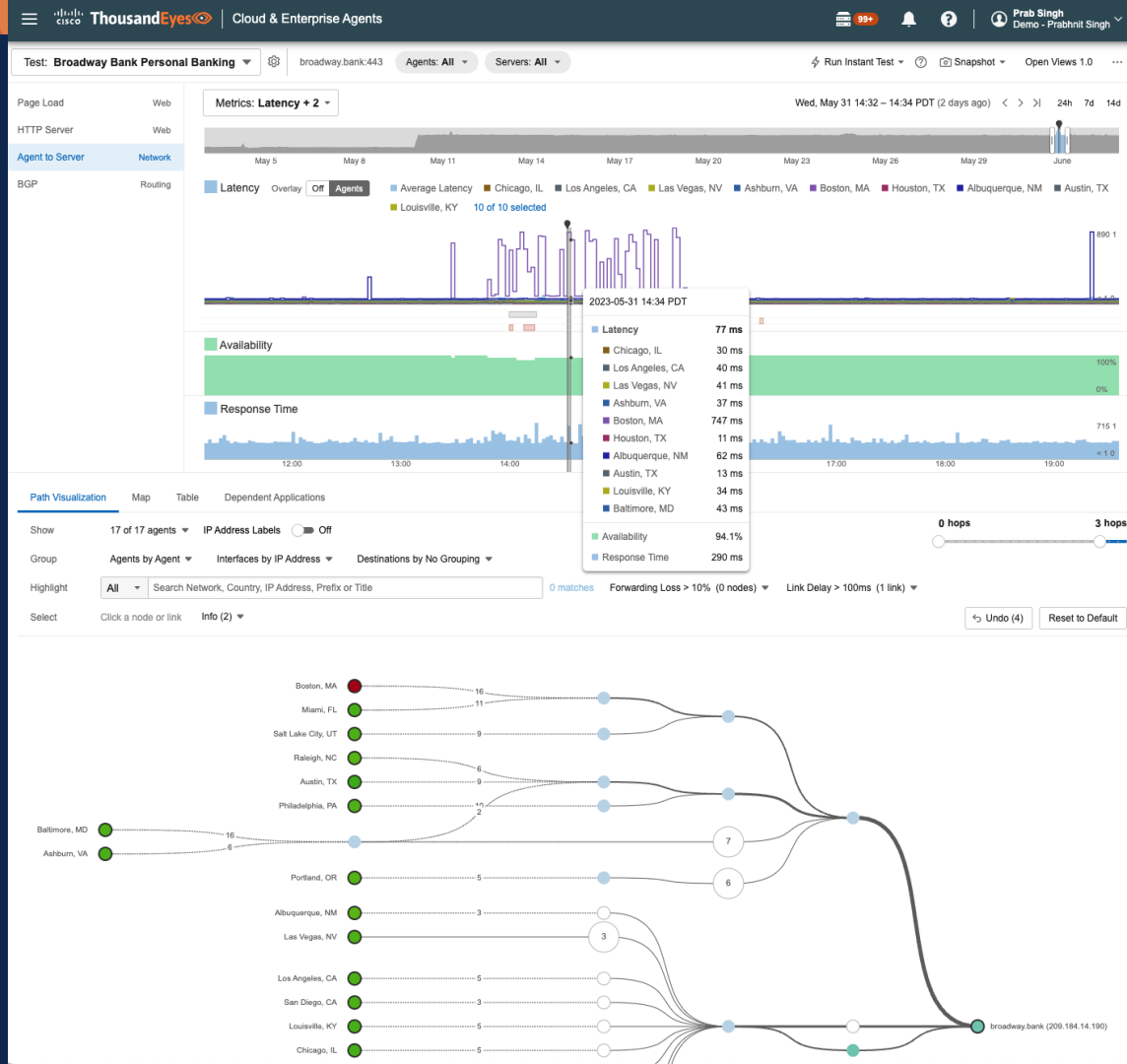
- ThousandEyes
- Making sense of data
- Alerts: the good, the bad, and the ugly
- Events, complementing alerts
- Demo, to see is to believe

ThousandEyes

How is the data collected?



CISCO *Live!*



Scale of Our Data

Data, Data,
and **More Data**

2 Billion

Daily Measurements (CEA)

30%

Year over Year Growth

Our visibility

In just one hour

740k

IPs

7.6k

ASNs

60k

Hostnames

1.5k

Cities

202

Countries

6

Continents

Extracting Insight

Is data enough?



+



=



More data!

Extracting Insight

Is data enough?



+



=



More data!



+



=



Visibility

Extracting Insight

Is data enough?



+



=



More data!



+



=



Visibility



+



=



Actionable
Observability

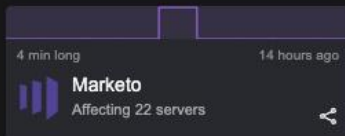
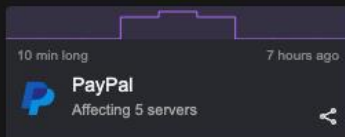
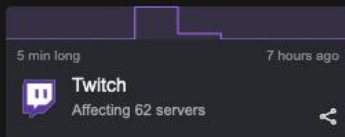
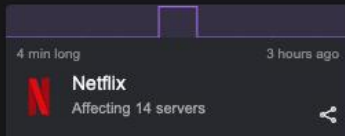
Applied Research at ThousandEyes

Making sense of data



Internet Outages Map

APPLICATIONS

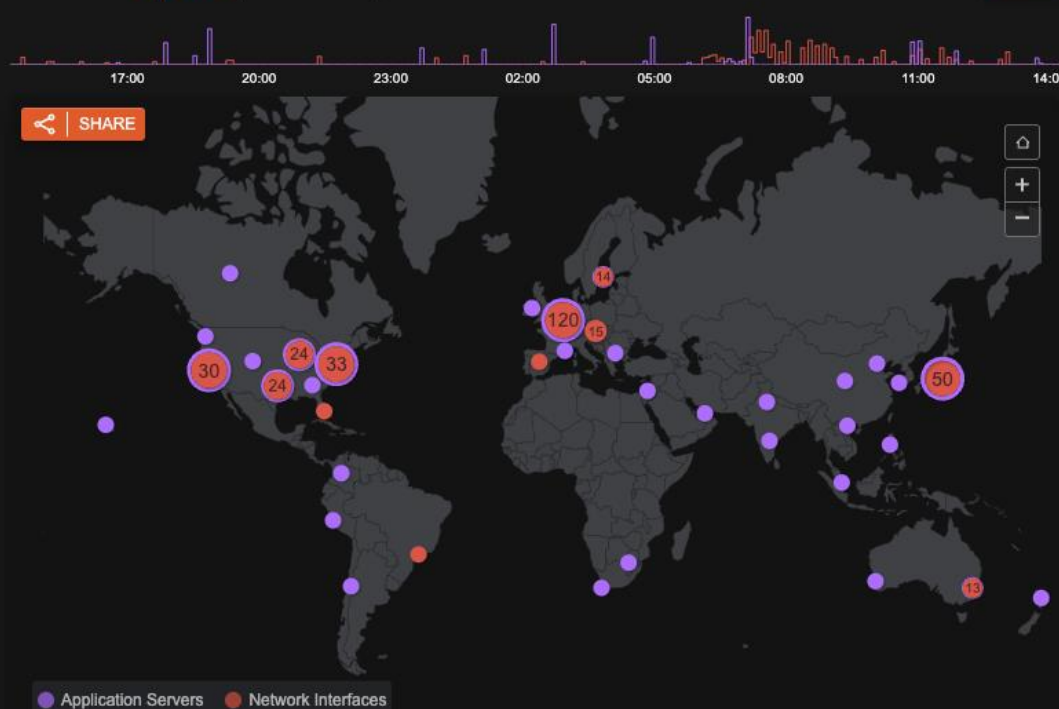


1 - 5 of 5

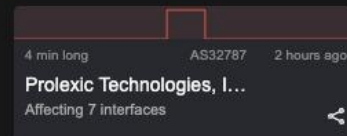
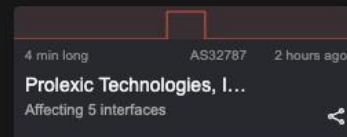
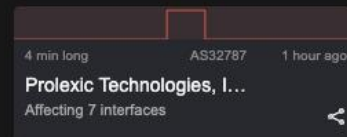
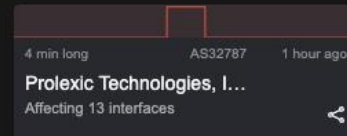
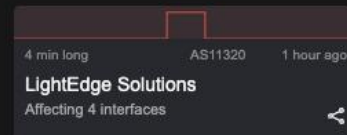
ThousandEyes | Internet Insights

Last 24 hours

LIVE



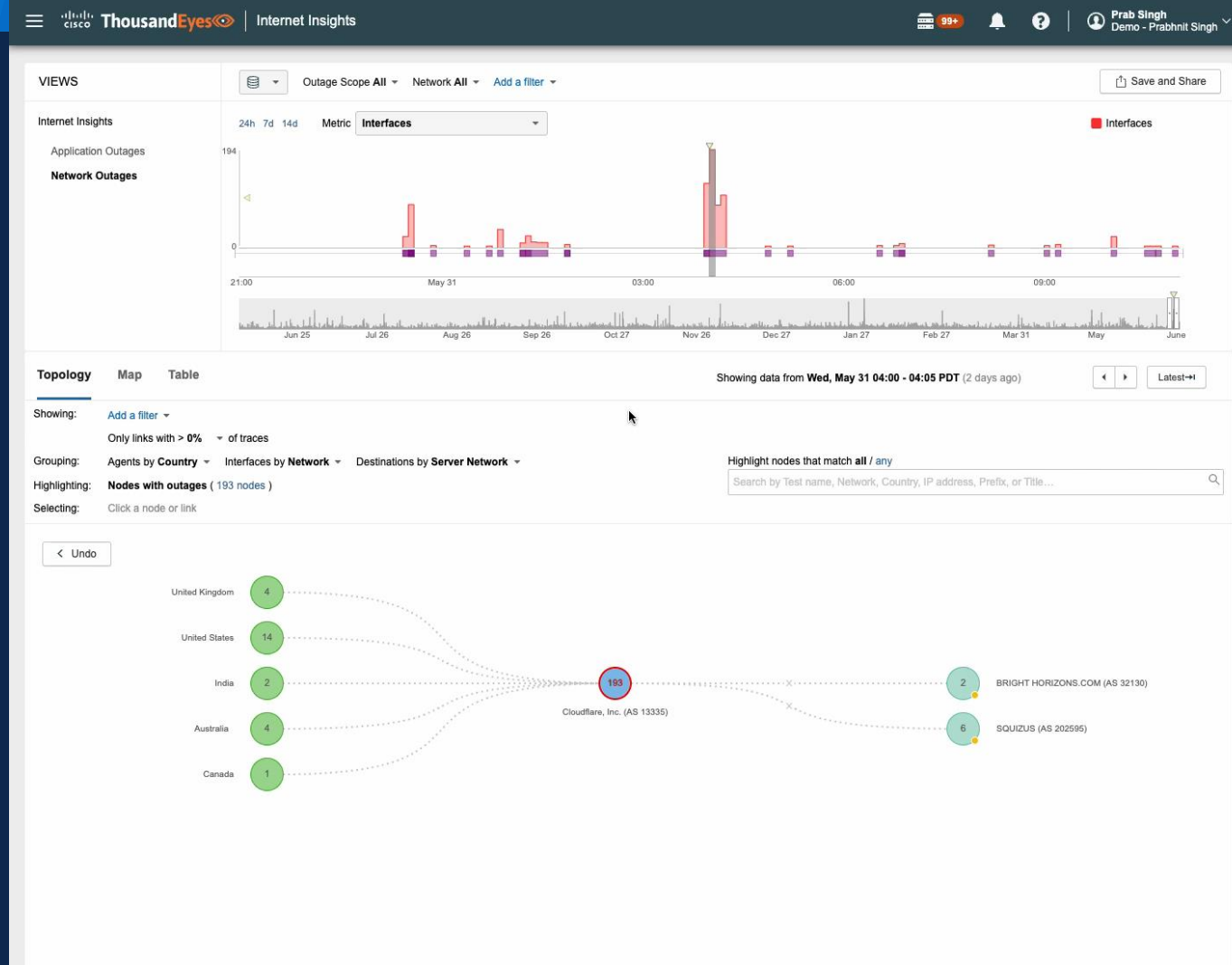
NETWORKS



1 - 5 of 36

Applied Research at ThousandEyes

Internet Insights for global outages



“Can we get these insights for our specific data”?

Trustworthy anomaly detection to democratize access to advanced troubleshooting

Steps to Resolution

0

Know there is an issue

1

What is happening?

2

What is the cause?

3

What is the fix?



Customer Story

What happened?



Global bank
experiences
an outage



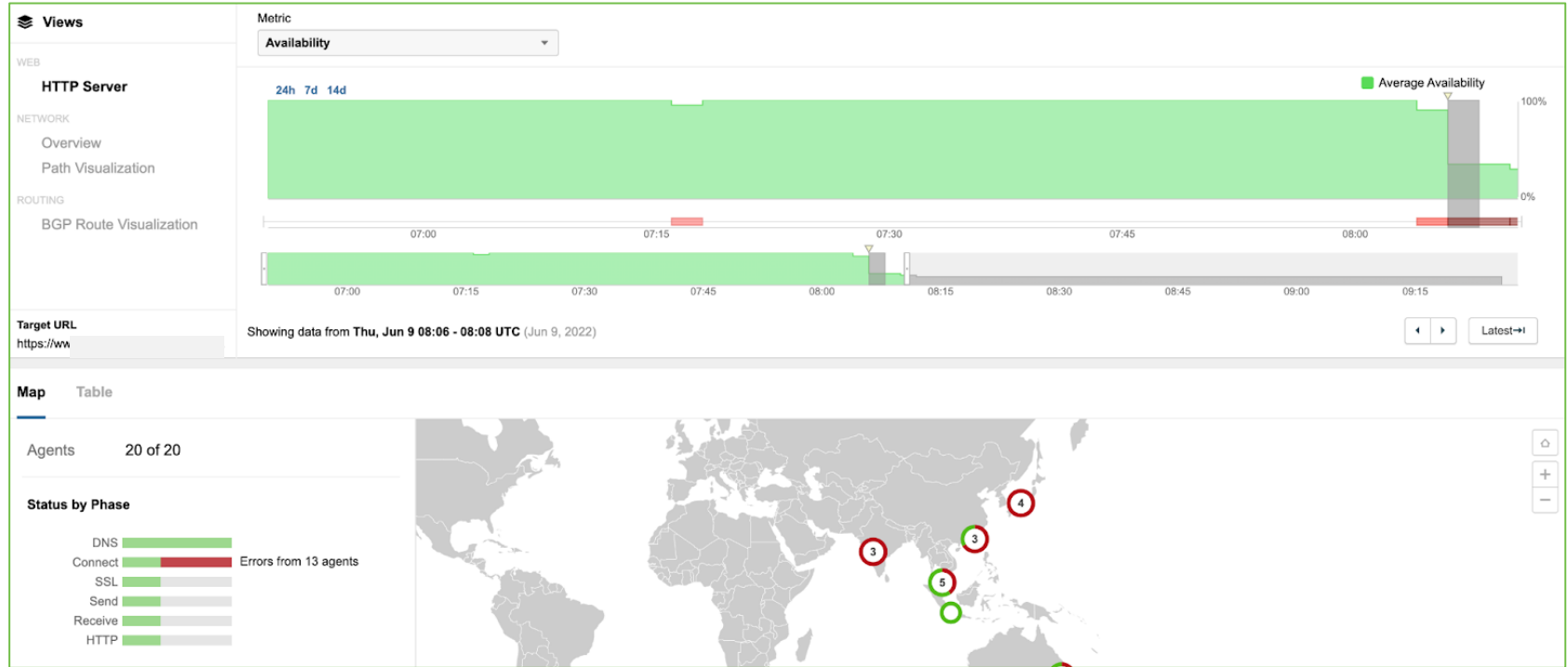
Mobile banking
becomes
unavailable



Customers
cannot withdraw
cash at ATMs

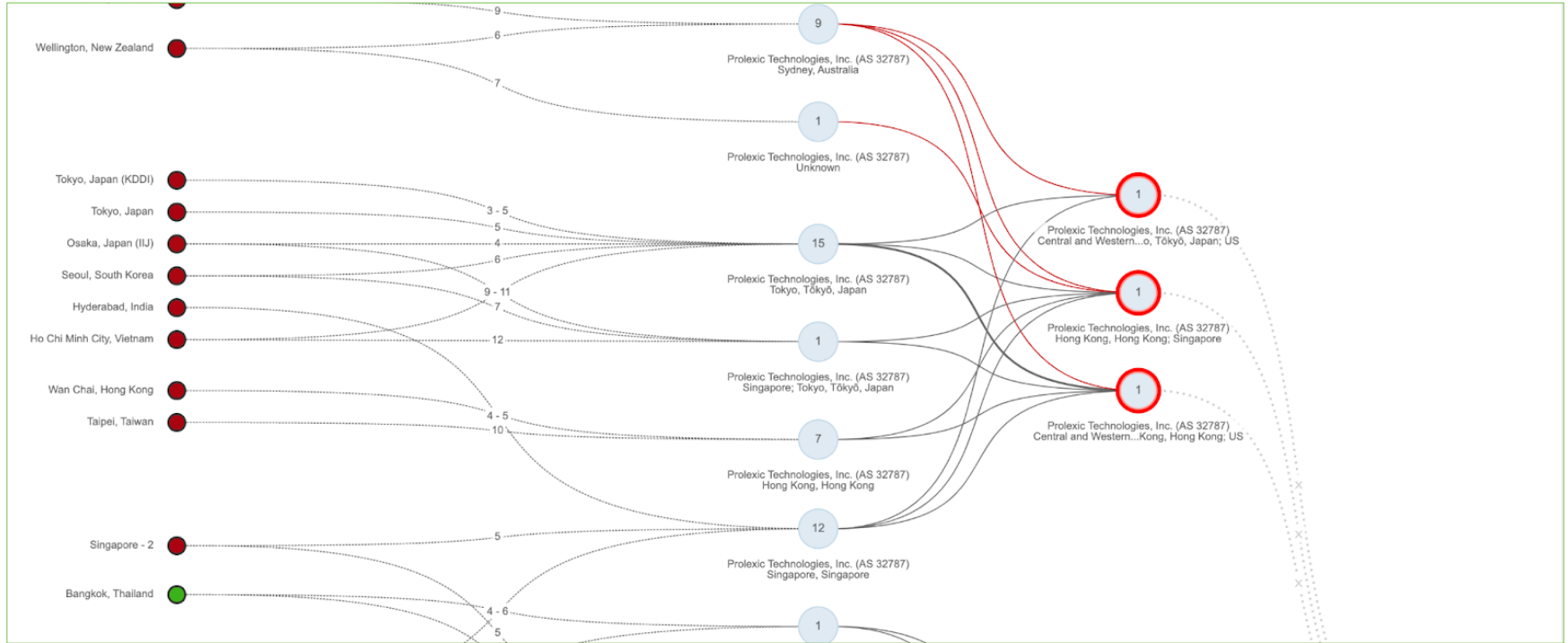
Customer Story

Gathering data



Customer Story

Hypothesize the cause



Customer Story

Confirming the hypothesis

Path Visualization

Showing: 1 of 1 Test ▾ 20 of 20 Agents ▾ 1 of 1 Server ▾ Hide IP Address labels ▾

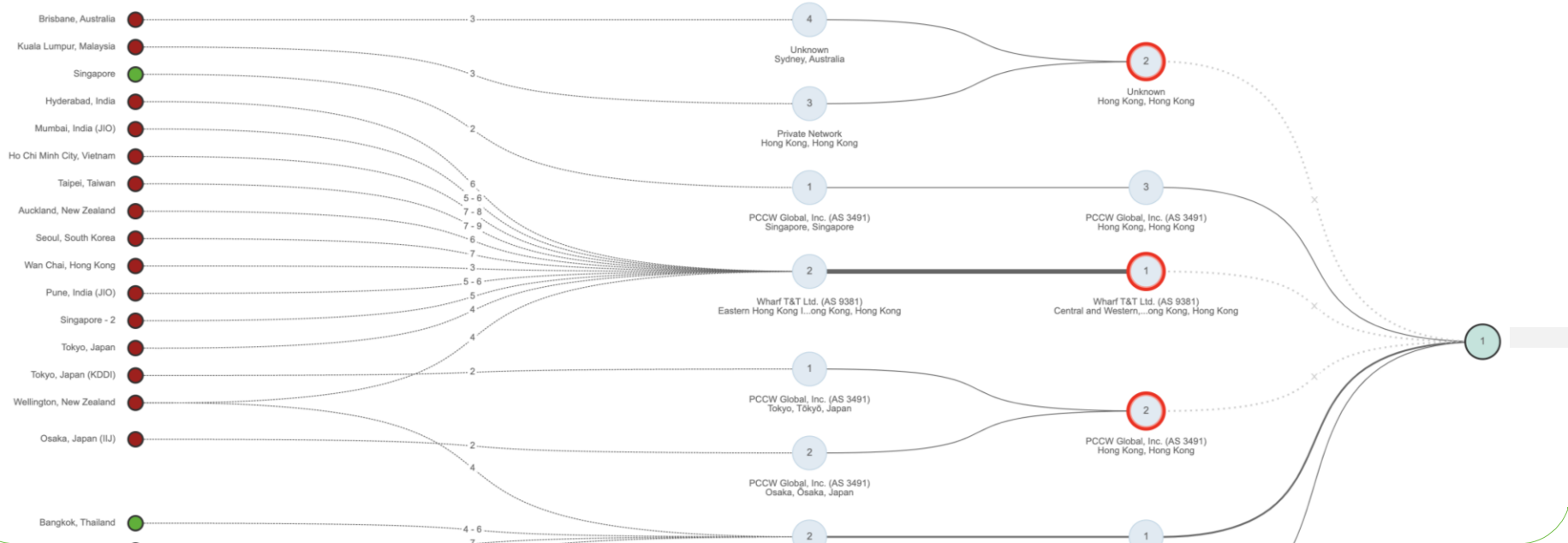
Grouping: Agents by Agent ▾ Interfaces by Network & Location ▾ Destinations by Domain ▾

Highlighting: Forwarding Loss > 10 % (4 nodes) ▾ Link Delay > 100 ms (6 links) ▾

Selecting: Click a node or link Info (4) ▾

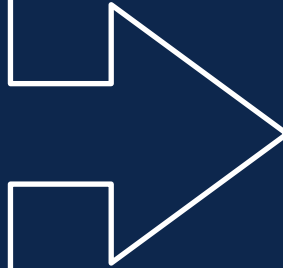
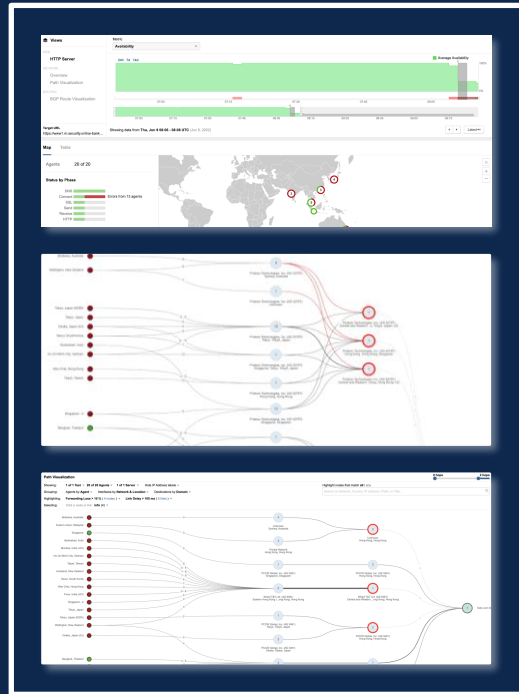
Highlight nodes that match all / any

Search on Network, Country, IP address, Prefix, or Title...



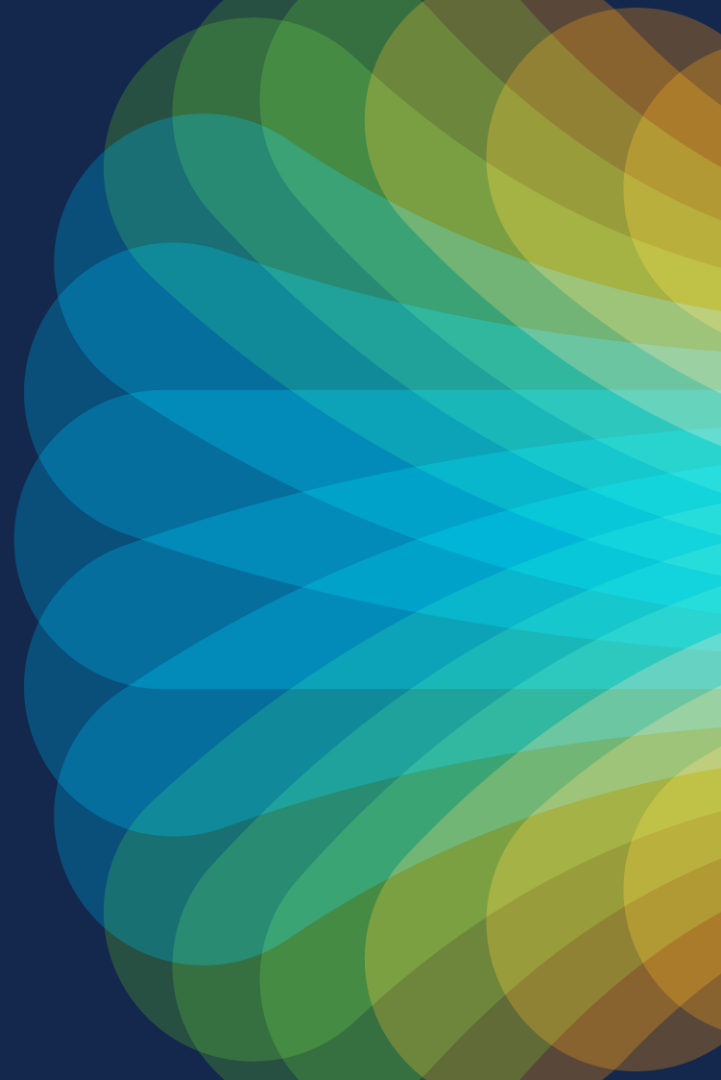
Customer Story

Putting it all together and applying a fix



Alerts

the good, the bad, and the ugly



Alerts are great if
you know what a
failure looks like

- RTT must be below 200ms
- API call must finish within 50ms
- HTTP GET response must match a regex
- Proxy must return a 404

Alerts may or may
not require action



Alerts do not
provide a root-
cause

Steps to Resolution

0

Know there is an issue

1

What is happening?

2

What is the cause?

3

What is the fix?

Alerts have poor
signal to noise ratio

Alert fatigue is real!

The screenshot shows the 'Alert Suppression' configuration page in a Cisco management interface. At the top, there's a navigation bar with a menu icon, the Cisco logo, and the path 'Alerts > Alert Suppression'. On the right of the navigation bar are icons for monitoring, a notification bell with a red '3' badge, and a help icon. Below the navigation bar is a search bar labeled 'Search by Name' and a status indicator '2 Suppression Windows'. A table lists the suppression windows with columns 'Name', 'Next Schedule', and 'Duration'. One entry is visible: 'DBB Alert Suppression' with a next schedule of 'Sat, Feb 11, 2023 00:00 UTC' and a duration of '1 day'. Below the table is a section titled 'Alert Suppression Window Settings' with two tabs: 'GENERAL' and 'SCHEDULE'. The 'GENERAL' tab is active, showing fields for 'Name' (DBB Alert Suppression), 'Tests' (356 of 366 tests selected), and an 'Enabled' checkbox which is checked. The 'SCHEDULE' tab is also visible, showing fields for 'Starts' (10/08/2022 at 00:00 UTC), 'Duration' (24 hours, 0 minutes), 'Repeat' (Every Day), and 'End Repeat' (Never). A 'Cancel' button is located at the bottom right of the settings panel.

Alerts > Alert Suppression

Search by Name 2 Suppression Windows

Name	Next Schedule	Duration
DBB Alert Suppression	Sat, Feb 11, 2023 00:00 UTC	1 day

Alert Suppression Window Settings

GENERAL

Name DBB Alert Suppression

Tests 356 of 366 tests selected

☒ Enabled

SCHEDULE

Starts 10/08/2022 00:00 UTC - Coordinated Universal Time

Duration 24 hours 0 minutes

Repeat Every Day

End Repeat Never

Cancel



“Alerts are great, but not enough”

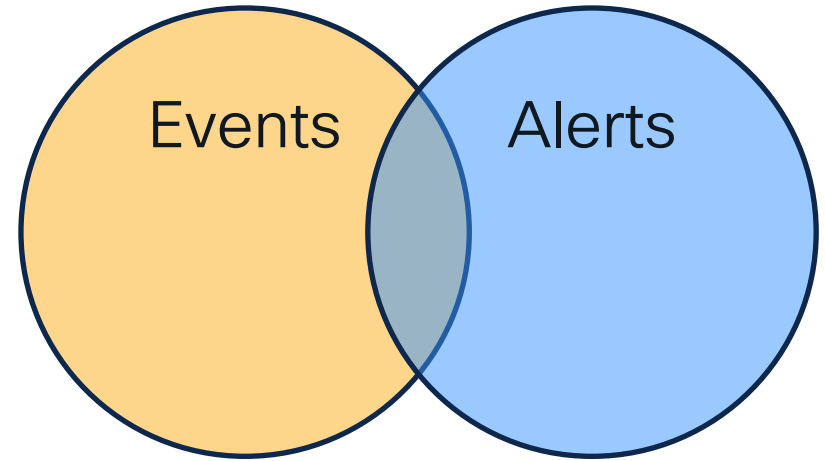
Every on-call engineer!

Events

from visibility to action



Events
complement alerts,
not replace them



Events offer a root-
case

Steps to Resolution

0

Know there is an issue

1

What is happening?

2

What is the cause?

3

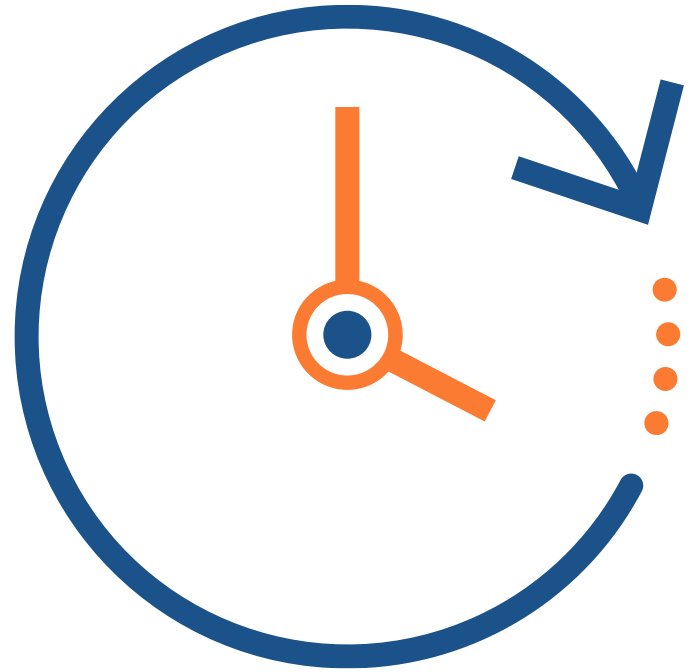
What is the fix?

Events require no
config or a priori
knowledge about
how failures look



Events improve the
signal to noise ratio

Events significantly
decrease time to
resolution



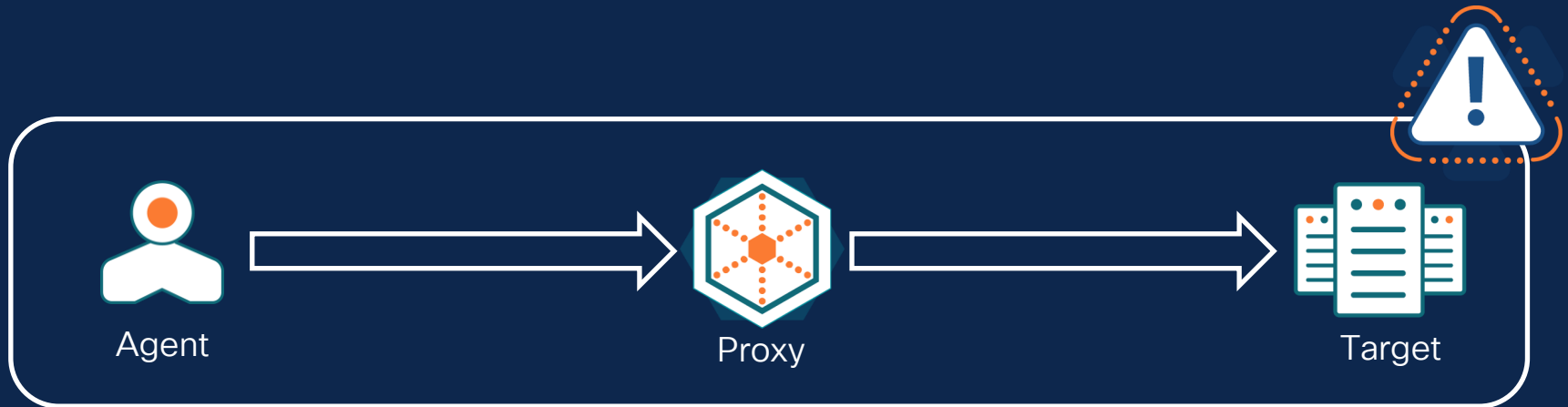
Demo

to see, is to believe



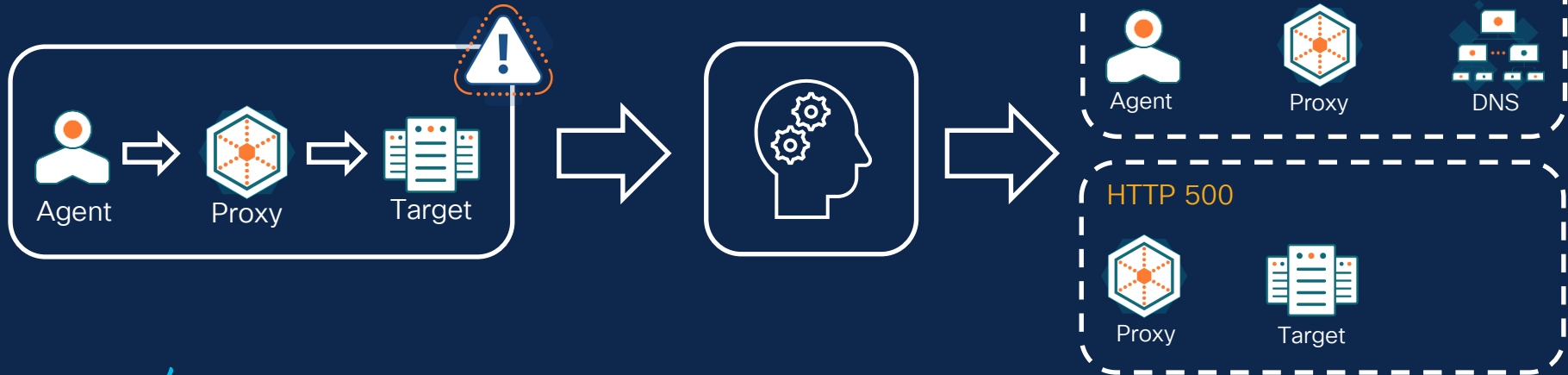
Detecting Events

1. List the symptoms
 - Filter out the noise



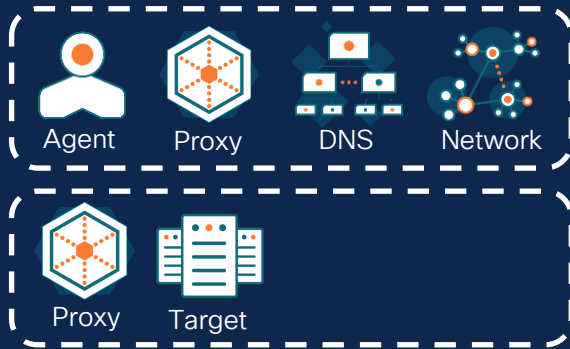
Detecting Events

1. List the symptoms
2. List the suspects



Detecting Events

1. List the symptoms
2. List the suspects
3. Find the culprit



Event		
type	proxy	
start	01:05 UTC	
end	01:45 UTC	
tests	agents	hosts

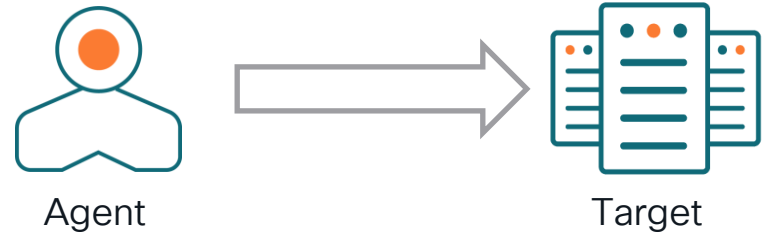
- Events are degradation from status quo



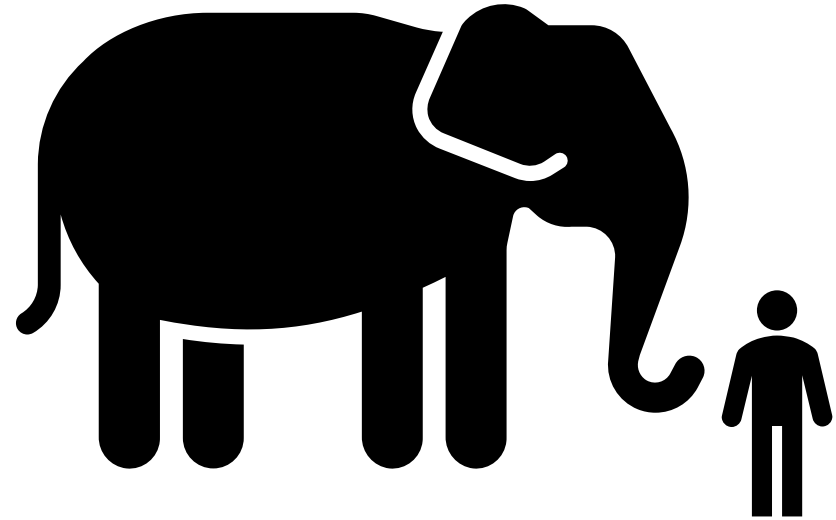
- Events are degradation from status quo
- Exact root-cause can't always be found



- Events are degradation from status quo
- Exact root-cause can't always be found
- Events should not be generated without enough evidence



- Events are degradation from status quo
- Exact root-cause can't always be found
- Events should not be generated without enough evidence
- Decisions should be based on entire data



Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

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



The bridge to possible

Thank you

CISCO *Live!*

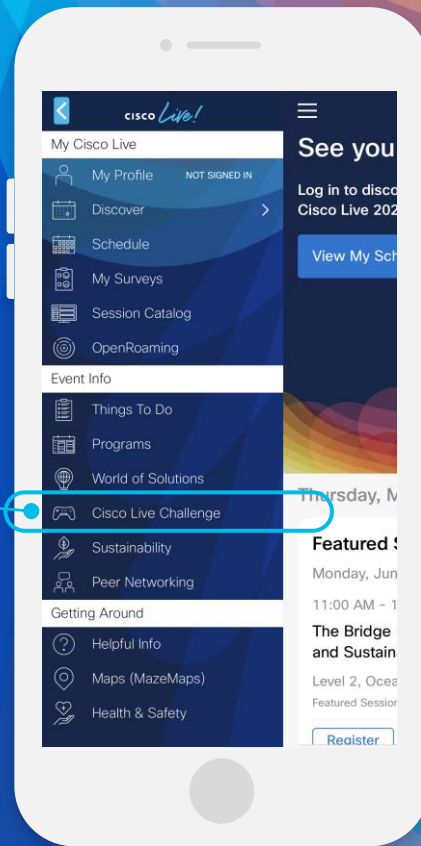
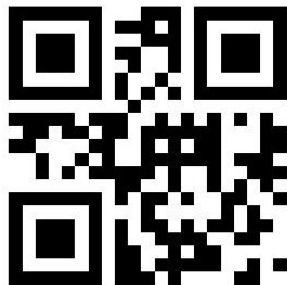
#CiscoLive

Cisco Live Challenge

Gamify your Cisco Live experience!
Get points for attending this session!

How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The background is a vibrant, abstract graphic. It features a central bright white light source from which numerous colorful rays emanate, creating a sunburst or starburst effect. The rays transition through a spectrum of colors including yellow, orange, red, and various shades of blue and green. Overlaid on this are several large, semi-transparent, wavy shapes in similar color tones, giving the overall image a sense of motion and energy.

cisco *Live!*

Let's go

#CiscoLive