

CISCO *Live!*

ALL IN

#CiscoLive



The bridge to possible

# The Art of Designing ThousandEyes Alert Rules

Yazan Albikawi, Implementation Engineer

BRKOPS-2076



#CiscoLive

# Cisco Webex App

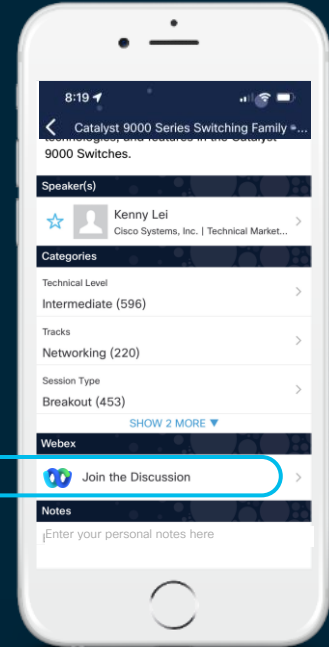
## Questions?

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 17, 2022.



<https://cicolive.ciscoevents.com/cicolivebot/#BRKOPS-2076>

# Alert Fatigue



# Session Objective

Your main key takeaways

- When is the right time to trigger an Alert
- How to address different types of network issues with Alert rules
- Alert optimization
- Identify the performance thresholds



# Agenda

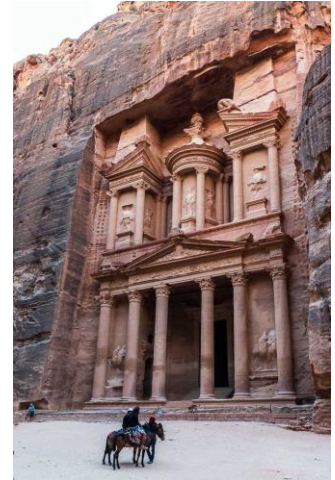
- ThousandEyes overview
- How to work with ThousandEyes Alerts
- Demo, How to Read and Create Alert Rules
- The Story: Clark and The Alert challenge
- Cloud Service Scenario
- Hosted Service Scenario
- Conclusion

# About your speaker



Yazan Albikawi

- Focus areas: Network and Solution Design, Implementation, Consultation
- Technology Area: Security, Network observability and Design
- Based in Krakow, Poland
- I come from Jordan



# ThousandEyes Overview



# Introduction to ThousandEyes

A SaaS based I/internet and cloud intelligence solution

## Network and Application Synthetics

- Application performance, network and routing
- Hop-by-hop path visibility across all networks

## End User monitoring

- Client-based agent monitoring endpoint performance
- End-to-end path and performance observability

## Internet Insights

- Collecting and correlating data from different ISPs
- Real-time internet and application outage detection

## Single pane of glass

- All collected data visualized in one management console
- Reporting and dashboard capabilities



# How to work with ThousandEyes Alerts

# Working with Alerts

“If there is something strange in the network whom we call ?”

Alerts are a notification generated by ThousandEyes platform, based on test results when they meet a certain condition defined by admin

Alert will be sent to you in different notification methods like:

- Email



- Webhooks



- Integrations



servicenow



# Alert Architecture

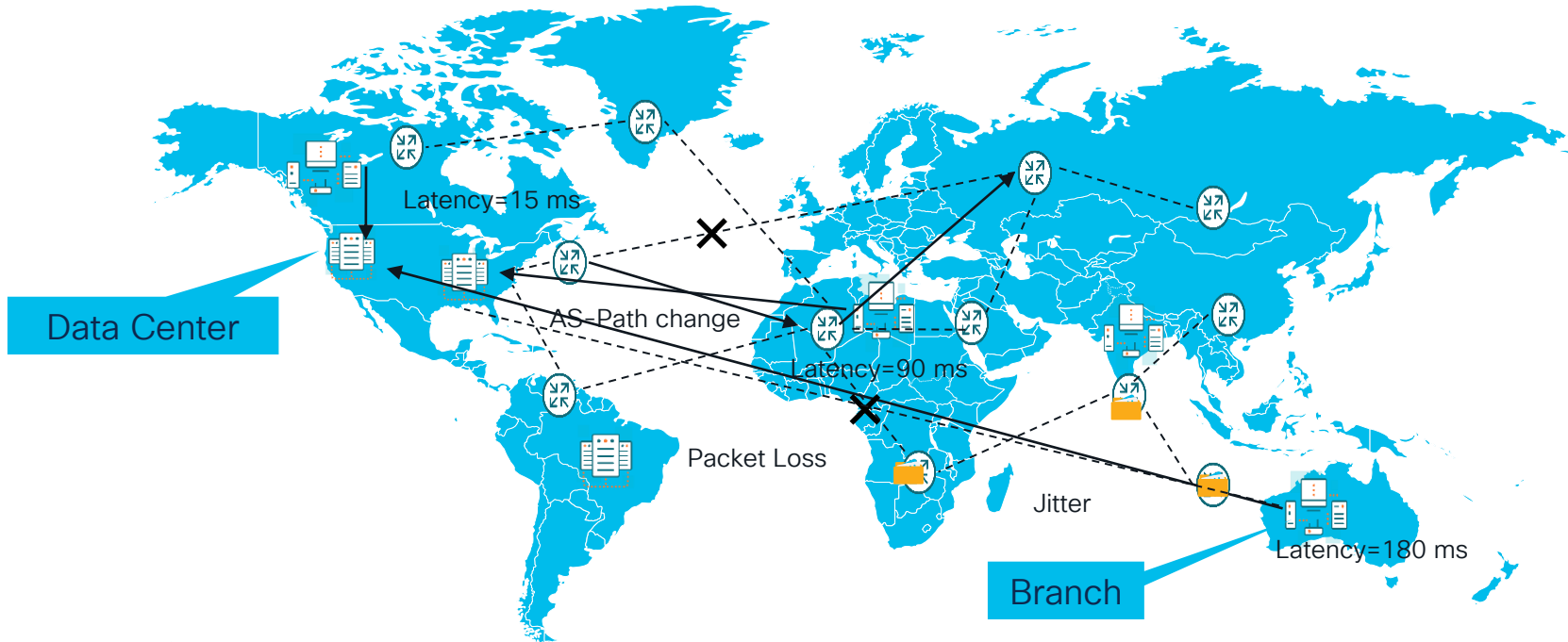
- Alert Rules, define tests, agents and threshold
- Metrics will be based on test types



*Note: Not all alerts will have a test, some will be based on other collected data like endpoint agents LAN statistics*

# Alert Rules Examples

- Network and Routing Alerts



# Alert Rules Examples

## Network Tests

- Metrics measured

Packet Loss, Latency, Jitter and optional Bandwidth, Throughput

- Path traces

Data for path like number of hops, length, and hop details

Event	Condition
High Latency in Asia-pacific	Latency $\geq$ 180 ms
High Network Packet loss	Loss $\geq$ _%
High Network Jitter	Jitter $\geq$ _ ms
QOS Marking change	Any hop not in DSCP #
Network loop Detected	Path length > _



# Alert Rules Examples

## BGP Routing

- Metrics measured

AS-path, Route reachability and Route update

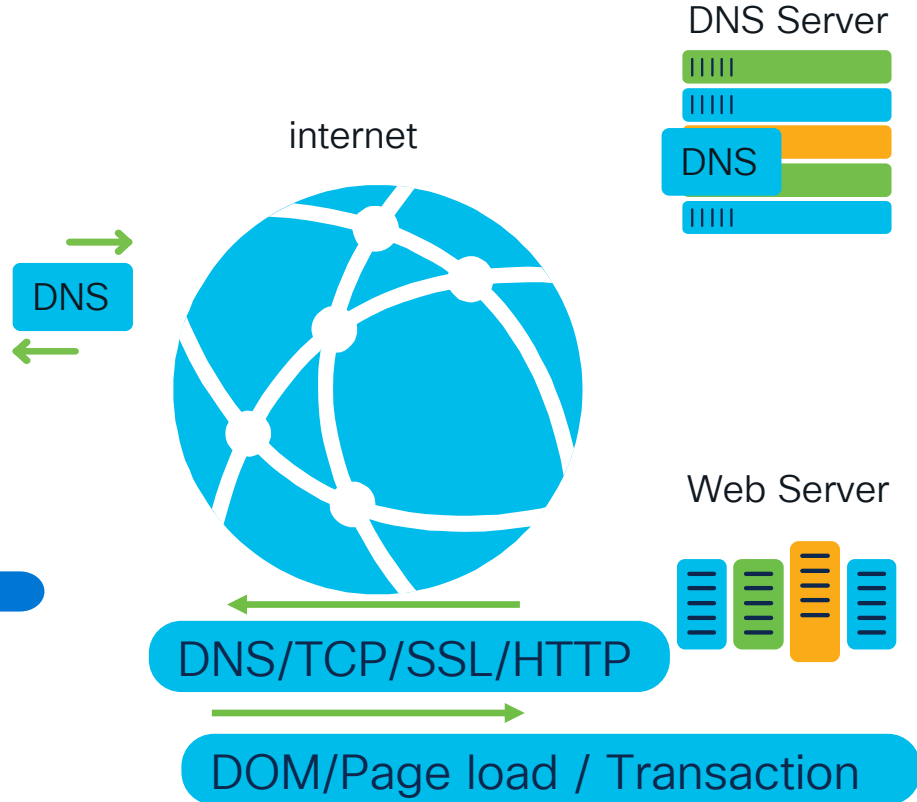
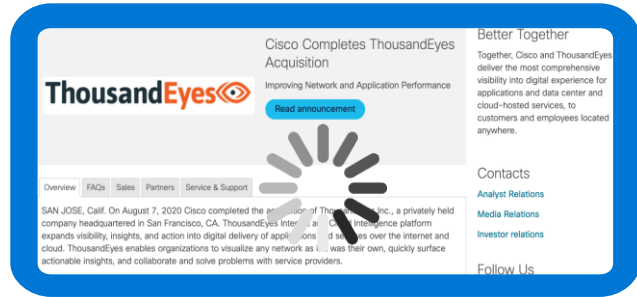


Event	Condition
Route Flaps	Path changes > 1 & reachability < 100%
Prefix hijack	BGP ASN not in ....
DDOS mitigation activated	BGP ASN in ... or prefix not in ..
Upstream provider change	BGP HOP# from origin not in ..



# Alert Rules Examples

- DNS & Web Alerts





# Alert Rules Examples

## DNS & Web Alerts

- Metrics
- DNS->Resolution time, availability
- Web->Response time, wait, load time, Transaction duration

Event	Condition
Slow DNS Response	Resolution time > 20ms
DNS Mapping change/ Spoofing	Mapping not in x.x.x.x
Slow transaction	Duration > __ms
Embed URL Not working	Any component domain in __ & component load incomplete
Slow Throughput	Throughput < __Kbps



# Alert Rules Examples

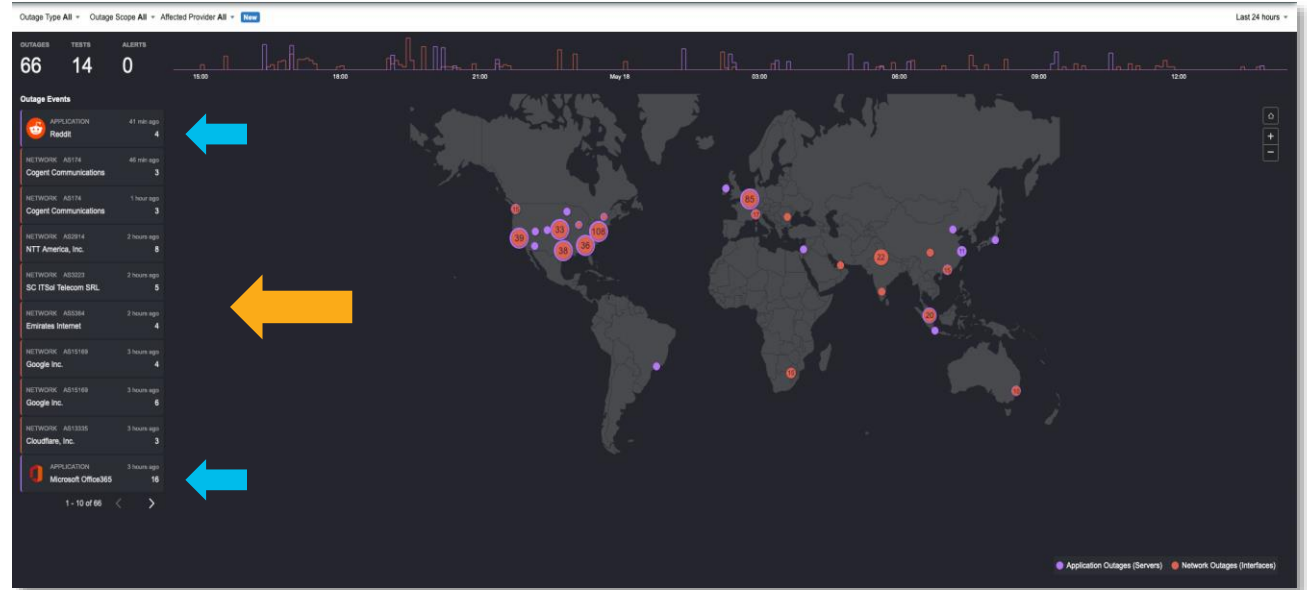
## Internet Insights

### Application outage

- Affected applications
- Outage error type
- Location

### Network outage

- Affected domain
- ASN
- Locations
- Interfaces



# Alert Rules Examples

## Internet Insights

### Metrics

- Application Outage -> locations, Test count, domains
- Network Outage -> ASN, location, domains, Test count, Interfaces

Event	Condition
Google workspace App outage	Affected App in Google workspace
Application Outage due to DNS	Affected app in ___ & Outage Error Type in DNS
CDN Network Outage in US	Locations in United States & affected domain in ___
Network Outage Services Impact	Affected tests count & location in ___



# Alert Rules Design Best Practices

## Baseline measurement

Categorize the service

Frequency of the Events

Notification Options

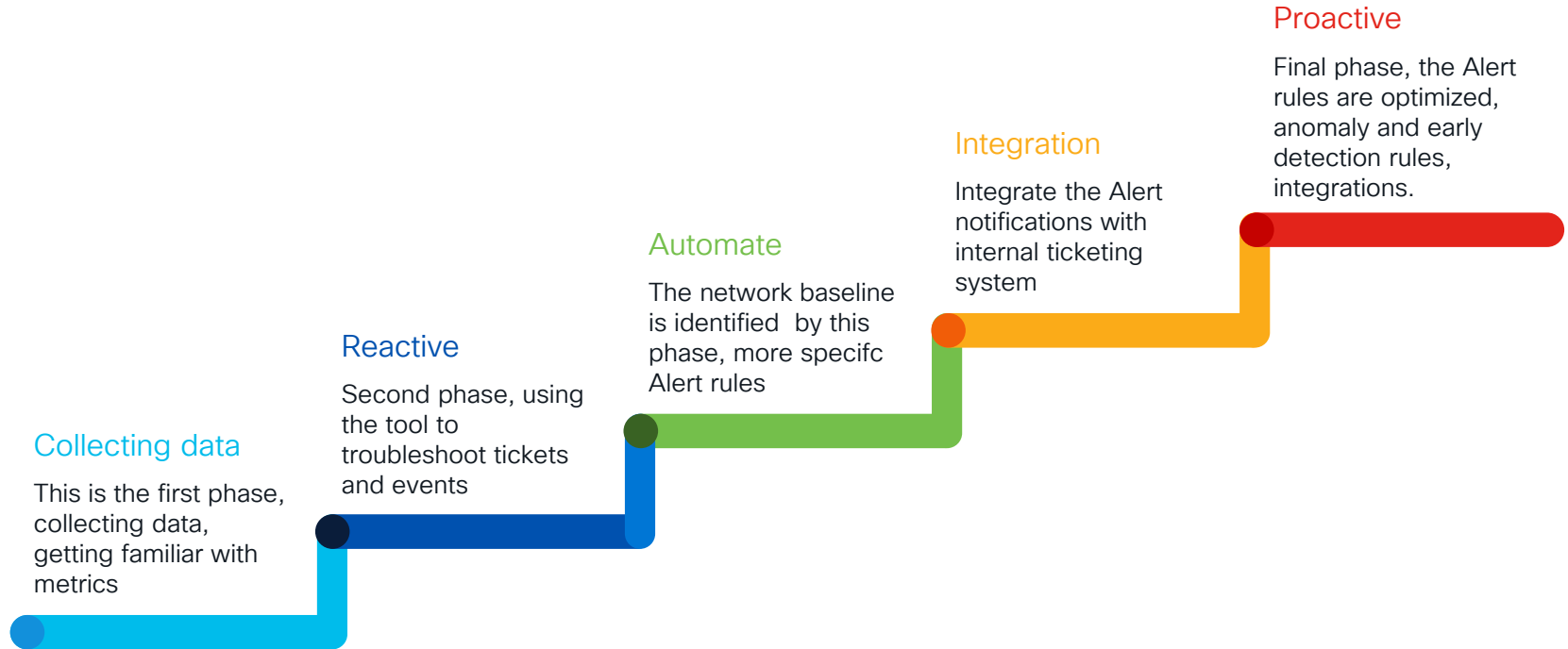
Optimization

## Services Benchmark

- Cloud Hosted → Official documentation and support
- Internal service → Development team and user experience



# Alert Deployment Stages



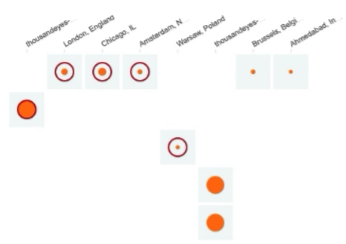
# Demo, How to Read and Create Alert Rules

- Cloud & Enterprise Agents >
- Endpoint Agents >
- Devices >
- Internet Insights >
- Dashboards**
- Alerts 5 >
- Reports >
- Sharing >
- Account Settings >

Default (Yazan-Dashboard) - Refreshed 1 min ago + Add Widget

**Alert Grid**

1 day



SalesForce

Web - Page Load

SiteParis-to-SitePoland

Voice - RTP Stream

O365-Outlook Flow test

Web - Transaction

Paris-To-Poland (Overlay)

Web - HTTP Server

Paris-to-Netherlands (Overlay)

Web - HTTP Server

5 active alerts

14 cleared or disabled alerts in the last 24 hours.

**Tests**

12 hours

Test Name	Test Type	Alert Status ↓	Trending (12h) / Current Values
SalesForce <a href="https://www.salesforce.com/">https://www.salesforce.com/</a>	Web - Page Load	2 alerts	3308.6 ms 100%
SiteParis-to-SitePoland @thousandeye-PR435	Voice - RTP Stream	2 alerts	N/A
O365-Outlook Flow test <a href="https://outlook.office365.com/">https://outlook.office365.com/</a>	Web - Transaction	1 alert	0% N/A 1 errors
Facebook <a href="https://www.facebook.com/">https://www.facebook.com/</a>	Web - HTTP Server		94.44% 234.21 ms
MS Teams Transport relay Audio world.fr.teams.microsoft.com	Network - Agent to Server		N/A N/A
MS Teams Transport relay Video world.fr.teams.microsoft.com	Network - Agent to Server		N/A N/A
Paris-to-Netherlands (Overlay) <a href="http://172.13.13.13">http://172.13.13.13</a>	Web - HTTP Server		0% N/A
Paris-To-Netherlands (Underlay) 10.130.13.2	Network - Agent to Server		100% N/A
Paris-To-Poland (Overlay) <a href="http://172.15.15.15">http://172.15.15.15</a>	Web - HTTP Server		0% N/A
Paris-To-Poland (Underlay) 10.120.15.5	Network - Agent to Server		100% N/A

I wish this page would...

# The Story: Clark and The Alert challenge





# Alerts challenge

Clark is the network administrator of Central Science

Central Science is a fictitious company focused on Climate research



Thanks to Cisco ThousandEyes he is now able to identify problems faster and more effectively

However, they are having some challenges with Alert Rules in multiple scenarios

1. A lot of notifications
2. False positives
3. Default settings



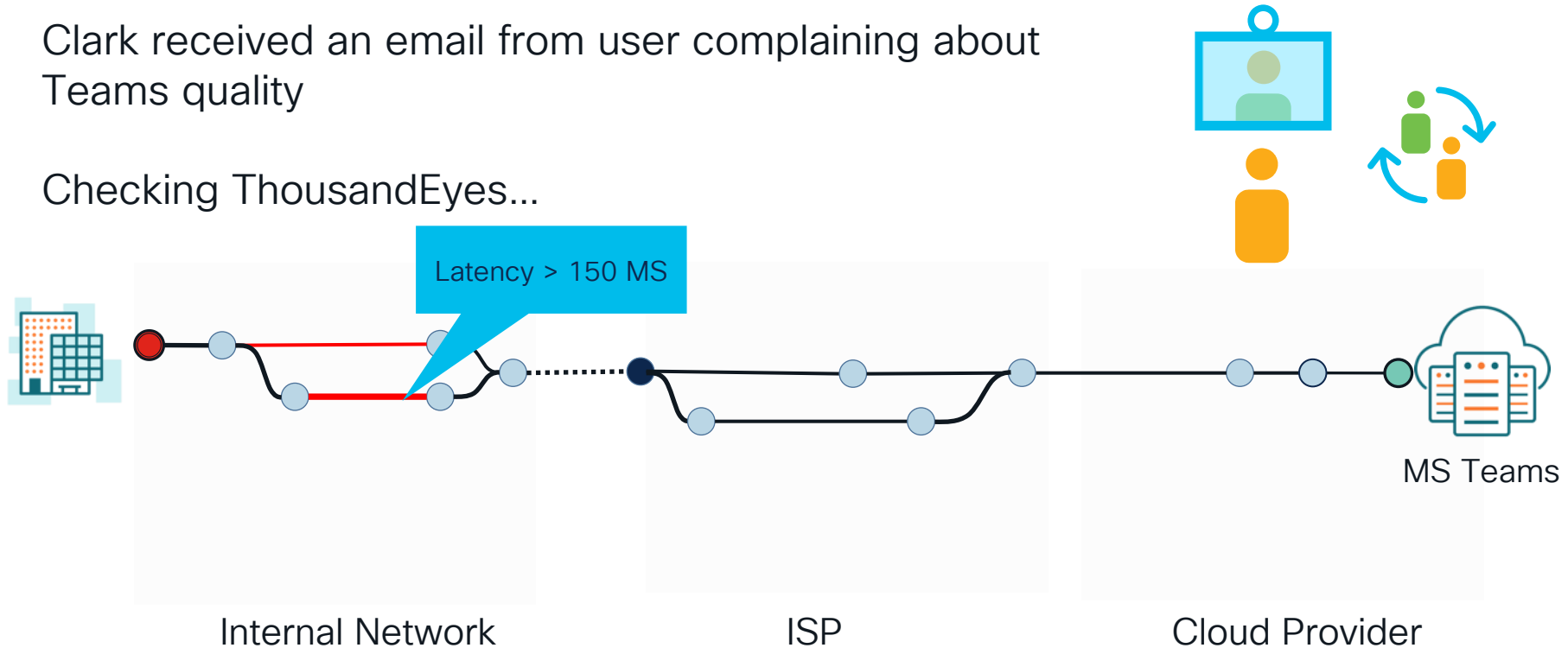
# Cloud Service Scenario- MS Teams Alert Rules



# MS Teams User Experience

Clark received an email from user complaining about Teams quality

Checking ThousandEyes...



# MS Teams Alert Rules

- Checking the Alert rule already configured

The screenshot shows the configuration page for an alert rule. The 'Alert Conditions' section is highlighted with a red box and contains the following configuration: 'All' conditions are met by 'any of' 1 agent, 2 of 4 times in a row. Below this, there are two conditions: 'Latency' is greater than or equal to 100 ms, and 'Packet Loss' is greater than or equal to 10%.

- Generalized Alert
- Default Metrics
- Logical operator AND
- Frequency of event

Alert didn't trigger due to ALL instead of ANY



# MS Teams Alert Rules

- Baseline Measurement

Service category: Critical

Separate Alert rules for tests, Transport relay, MS Teams Edge, RTP

- Service Benchmark

Cloud hosted service, source of truth is the official documentation

Metric	Target
Latency (one way)	< 50ms
Latency (RTT or Round-trip Time)	< 100ms
Burst packet loss	<10% during any 200ms interval
Packet loss	<1% during any 15s interval
Packet inter-arrival Jitter	<30ms during any 15s interval
Packet reorder	<0.05% out-of-order packets



# MS Teams Alert Rules

- Network packet loss

Packet loss is important as such trigger will happen at notice or early stage

- Latency and Jitter

Spike of latency will not generate effect as much of packet loss, trigger will happen in more persistent occurrence

Alert rule name	Condition	Frequency
MS Teams High packet loss	Packet loss > 2%	2 in 2 rounds
MS Teams High latency	Latency > 100 MS	2 in 3 rounds
MS Teams High Jitter	Jitter > 30 MS	2 in 3 rounds
Network Low MOS (RTP)	MOS < 4	2 in 3 rounds



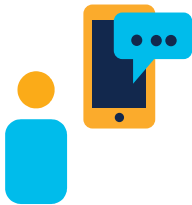
# Hosted Service scenario- Web response time challenge



# Web response time challenge

Central Science depends on multiple web applications for all users, remote and local.

Clark complains about the notifications



**HTTP Server Alert**

Alert ID: 9666568  
Test Name: Rule 11 tech  
URL: <https://rule11.tech>

**Alert Rule: Default HTTP response time - Response Time  $\geq$  Average Response Time + 2 standard deviations**

No. of Agents: 1  
Start Date: *1 Minute Ago*  
2021-11-13 20:34:00 UTC

Agent	Metrics @ Alert Start
Dreamland Poland	Response Time: 524 ms





# Web response time challenge

## Checking the alert rule condition configured

**ALERT CONDITIONS**

All conditions are met by     of  time in a row:

**i** Note: Dynamic baseline is calculated based on last 24 hour period, and standard deviation is calculated over a 3 hour window

- Dynamic baseline
- Frequency of event

- The alert rule is missing a fixed threshold
- Standard deviation might be very noisy
- The condition created on assumption that above dynamic average is a bad event



# Dynamic Baselines Metric Measurement

Automatically establish a baseline based on the last 24 hour period.

- Standard deviation STDEV

Response Time  Dynamic  Std deviations

**Note:** Dynamic baseline is calculated based on last 24 hour period, and standard deviation is calculated over a 3 hour window

- Percentage change

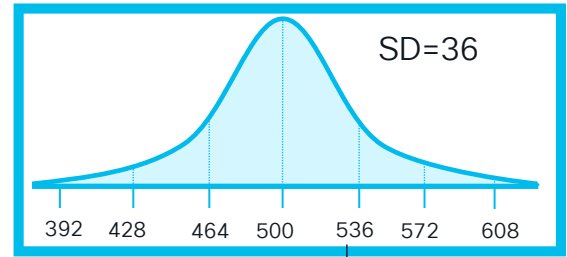
Response Time  Dynamic  %

**Note:** Dynamic baseline is calculated based on last 24 hour period

- Absolute value

Response Time  Dynamic  ms

**Note:** Dynamic baseline is calculated based on last 24 hour period



Mean for the last 3 hours=500 ms



# Dynamic baselines best practices

Best suited for pattern behavior notification

Alert on fluctuation of test results

Fine tuning and analytics required

Optimization



## Important notes

- Standard deviation can be very noisy for stable average
- Add more fixed or static metric to reduce noise



# Web response time alert rule

- Baseline Measurement

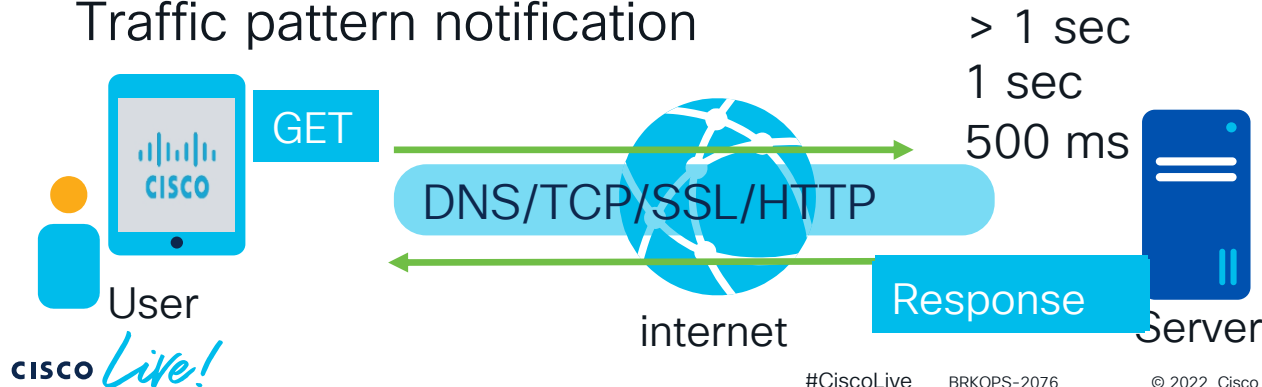
  - Service category: Necessary

  - Alert rules based on severity and impact

- Service Benchmark

  - User experience test

  - Traffic pattern notification



# Web response time alert rule

## Traffic pattern notification

CL2022 ▾ Last 14 days ▾

📷 ⬇️ Add Widget ⋮

### Average Response Time - Top 5

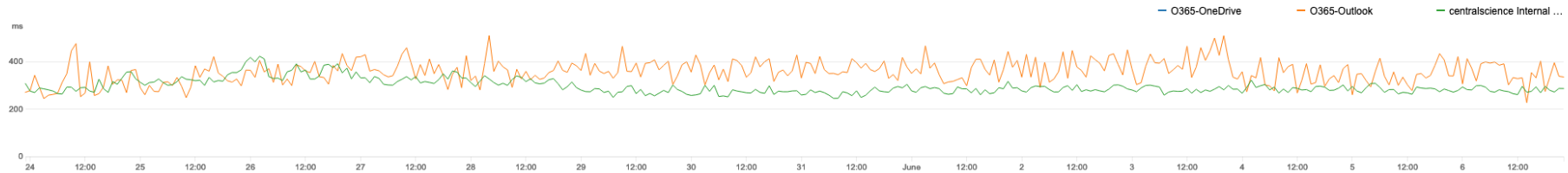
Web - HTTP Server — Response Time ⓘ Data suppressed

■ All



### HTTP Response Time

Web - HTTP Server — Response Time • 3 Tests ⓘ Data suppressed



# Web response time alert rule configuration

Alerts levels are important for early detection (same condition different scale)

Pattern notification based on standard deviation

Alert rule name	Condition	Frequency	Severity
HTTP Response and pattern	Response time > 2*STDEV & Response time > 300ms	2 out of 3 rounds	Info
HTTP Response LEVEL1	Response time > 200ms & Response time < 500ms	2 out of 3 rounds	Minor
HTTP Response LEVEL2	Response time > 500ms & Response time < 1000ms	2 out of 3 rounds	Major
HTTP Response LEVEL3	Response time > 1000ms	2 out of 3 rounds	Critical

# Conclusion



# Conclusion

01 Early detection

02 Categorization of service

03 Fixed thresholds and benchmark

04 Continuous optimization

Smooth operation, proactive measurements, integration ready deployment and better user experience

MTR



Support services

24/7

Success







“Strategy is a fancy word for coming up with a long-term plan and putting it into a plan.”

- Ellie Pidot

# Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



# Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. [www.cisco.com/go/certs](http://www.cisco.com/go/certs)

## Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



## Learn



### Cisco U.

IT learning hub that guides teams and learners toward their goals

### Cisco Digital Learning

Subscription-based product, technology, and certification training

### Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

### Cisco Learning Network

Resource community portal for certifications and learning



## Train



### Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

### Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

### Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



## Certify



### Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

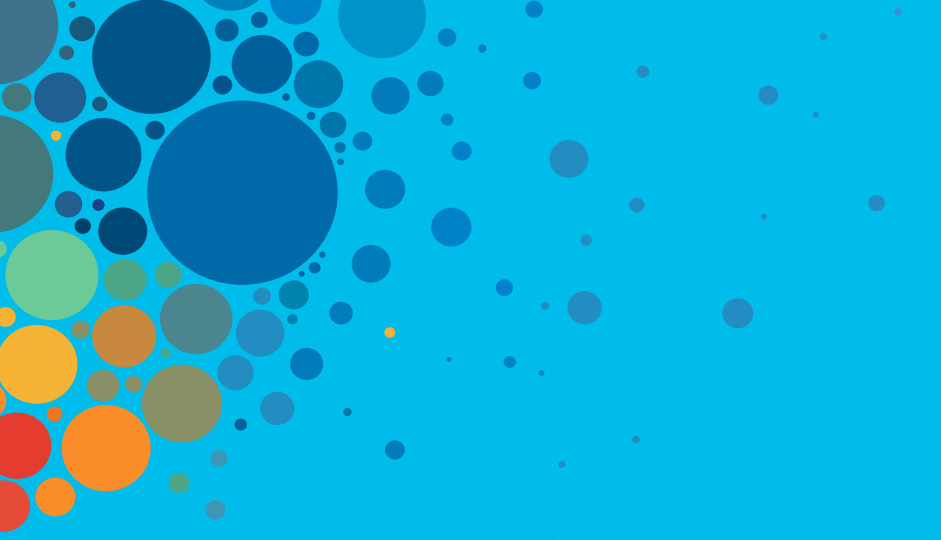
### Cisco Guided Study Groups

180-day certification prep program with learning and support

### Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



# 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](http://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLive

CISCO *Live!*

ALL IN

#CiscoLive