
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Automating Security

Just Because You Can, Doesn't Mean You Should!

TK Keanini, VP and CTO for Cisco Secure
@tkeanini1

BRKSEC-2354

Cisco Webex App

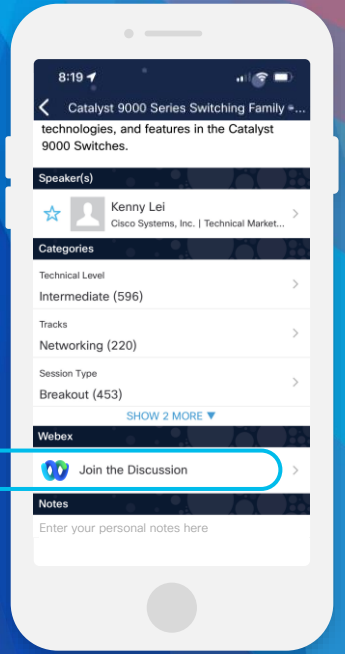
Questions?

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/#BRKSEC-2354

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

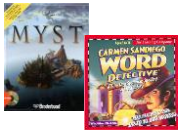
Agenda

- Introduction
- Retrospective
- Best Practices
  - Testing & Threat Modeling
- Summary & Resources

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Hello My Name is TK Keanini

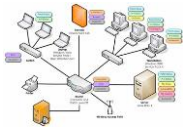
(Pronounced Kay-Ah-Nee-Nee)



Broderbund

Cisco Systems

Morgan Stanley



nCircle
Proactive Network Security

Lancope

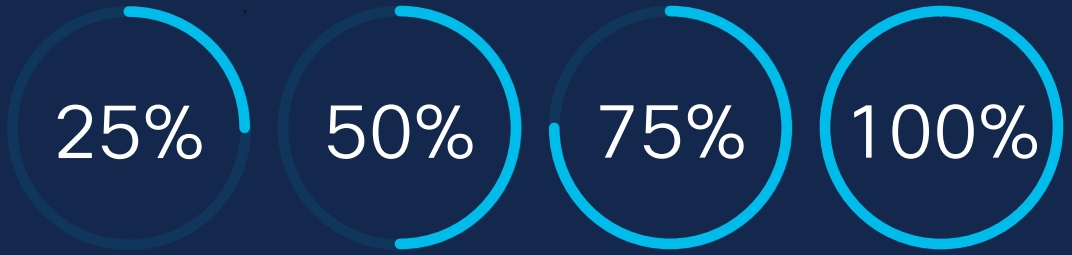
CISCO

58 Years in a Nutshell

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

How many of you have a goal to automate your security?

What percentage of your infrastructure is automation-ready?



The term **automation** was coined in the automobile industry about 1946 to describe the increased use of automatic devices and controls in mechanized production lines.

The origin of the word is attributed to D.S. Harder, an engineering manager at the Ford Motor Company at the time.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Going from Human-Scale to Machine Scale

In-Product Automation	Examples ▸ DNAC – automation/orchestration of network configuration ▸ ISE – automation/orchestration of network security policy ▸ CDO – it is called common defence orchestrator
Workflow Orchestration	Examples ▸ Cisco Extended Detection & Response (XDR) Orchestration ▸ SecureX Orchestration ▸ No-Code, Low-Code, sharing of Workflows
Code	Examples ▸ Python scripts to published APIs ▸ DevNET

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Automation Objectives

Analytics for Insight and Understanding

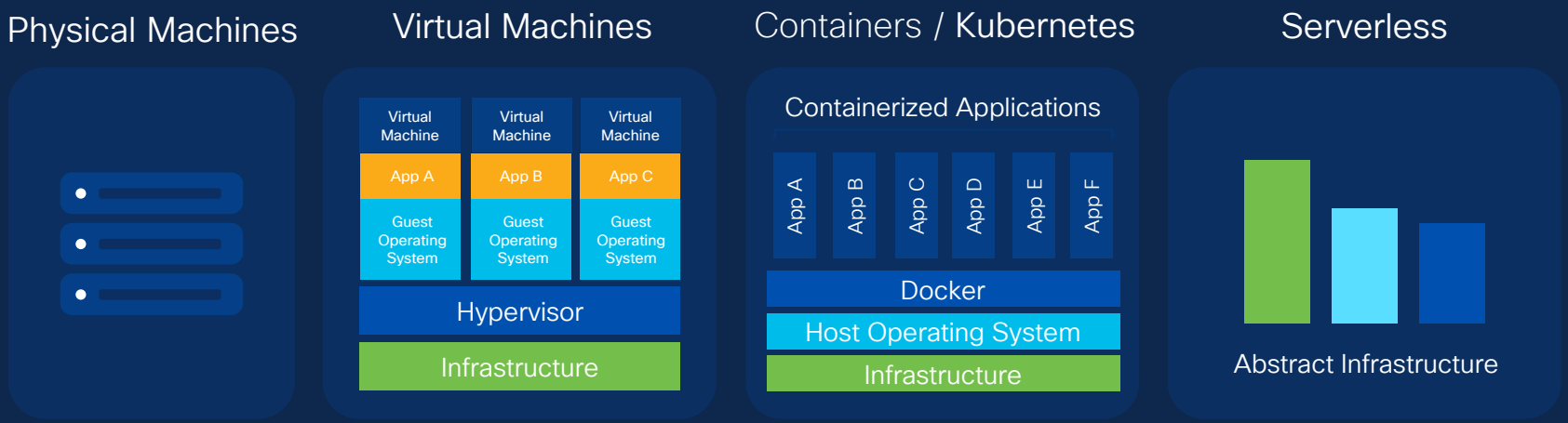
Testing for Assurance of Evidence of Success

Administrative Provisioning/ Deprovisioning to Scale Operations

Mitigation and Remediation to Scale our Defensive Actions

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Environments Vary in Their Capability



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

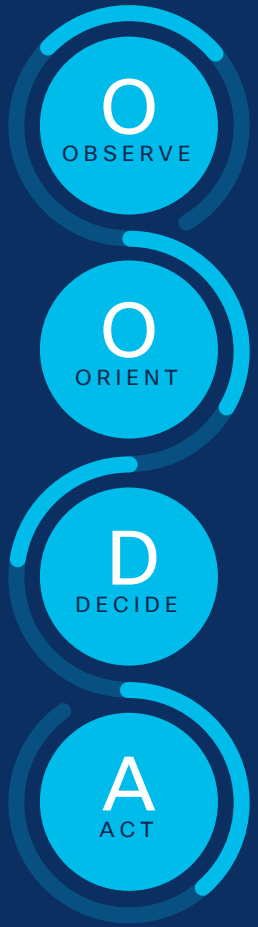
John Boyd's OODA Loop

BOYD

The fighter pilot who changed the art of war.

Robert Coram | ISBN: 0316796883

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public



The OODA Loop

Human Scale

Domain of **Manual** Processes

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

The OODA Loop

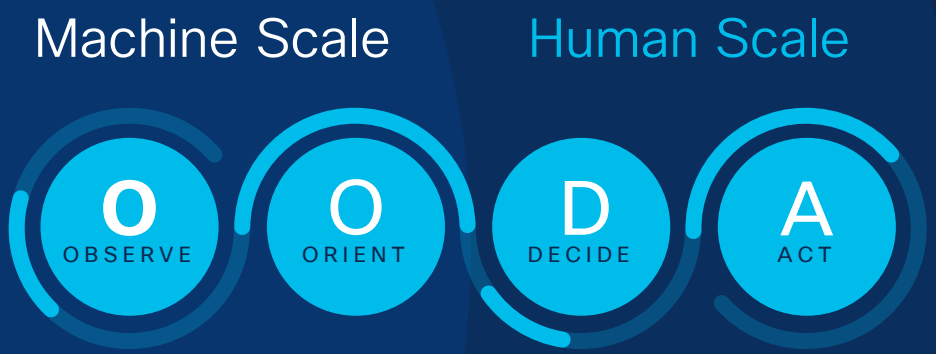
Human Scale

The OODA Loop

Machine Scale

Domain of **Automated** Processes

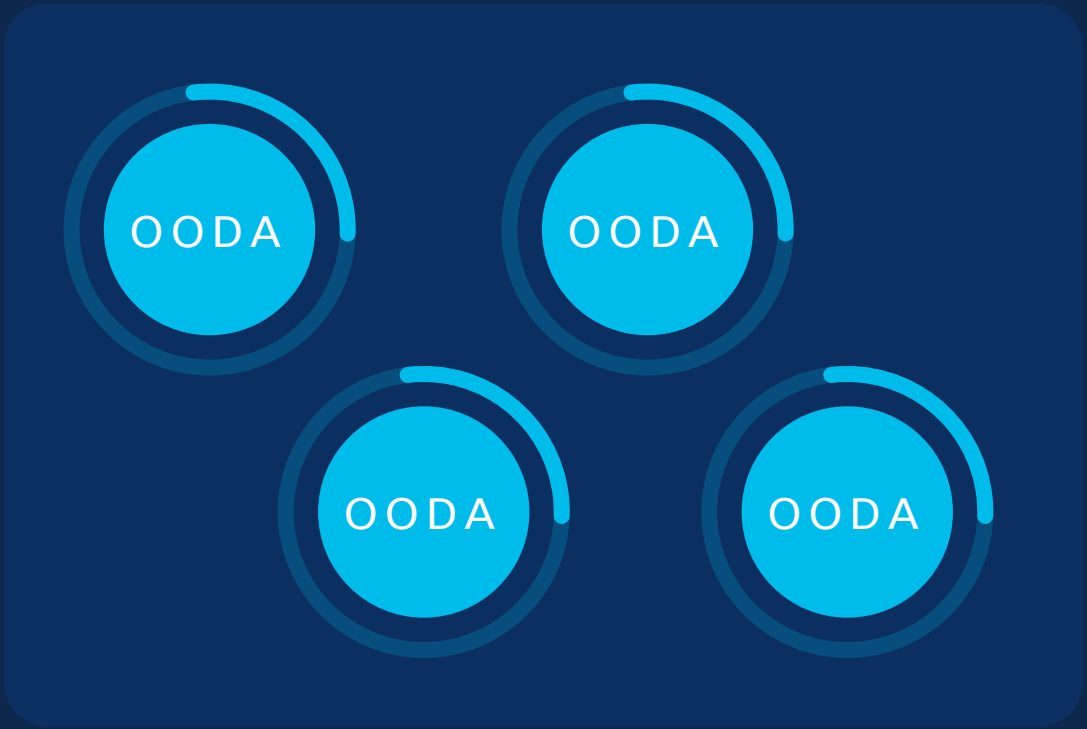
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public



- We must recognize that machines are required to observe at Machine Scale.
- Analytical processes bring machine scale observations down to Human scale understanding.
- Ideally Decisions can be made at machine speed and automated but not all of them can. Some require human interaction.
- Actions change the state of the world and require a new Observation.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

OODA Loop Systems



The opponent with the quicker tempo is in control of the conflict

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

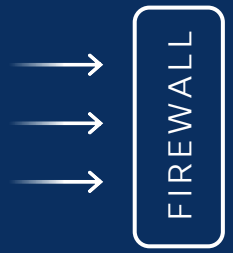
Introduction Summary

- Computers help us mechanize work; automate tasks
- All automation has an objective it seeks to achieve
- Computer environments vary in their ability to be automated
- We will use John Boyd's OODA loop to model the automation lifecycle
- We must consider Human-scale and Machine-scale as one
- Units within the larger end-to-end system all have their own OODA loops
- You achieve situational dominance when your OODA loop is at a higher tempo than your adversary

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Firewalls Gone Wild

Inbound traffic



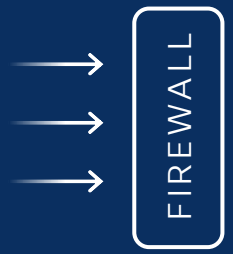
If traffic matches a (blacklist) signature

OBSERVE/ORIENT

Block it!

DECIDE/ACT

Threat actor spoofed UDP traffic that matches the blacklist with source address or Top Level Domain Servers

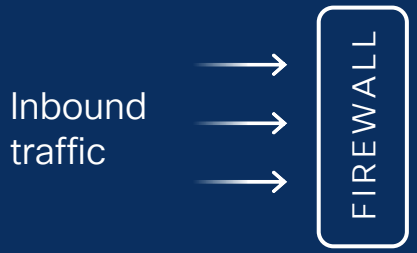


Firewall started blocking Top Level Domain Servers

RESULT: Automation cripples production!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Firewalls Gone Wild Anti-Pattern



If traffic matches a (blacklist) signature

OBSERVE/ORIENT

Block it!

DECIDE/ACT

Spoof:
Adversary can author observations

OBSERVE | ORIENT | DECIDE | ACT

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Actors “Living off the Land”

- Attackers will use your automation against you!
  - Automating malware distribution via native software updates
  - Host automation done via PowerShell

REMEMBER

Any automation you have could be equally as useful to your adversary!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Testing Your Automation

Automated Testing: Overview

Treat your Infrastructure as Code

Static Analysis	Unit Test
Integration Test	End-to-End Test

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Automated Testing: Static Analysis

- Testing without runtime
- ‘lint’ the code – catch all the erroneous syntax errors

Tool	Linters
Terraform	• conftest • terraform validate • tflint
docker	• dockerfile lint • hadolint • dockerfilelint
kubernetes	• kube-score • kube-lint • yamllint

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Automated Testing: Unit Test

- Treat your Infrastructure as Code
- Carefully define what is a Unit
- Use the OODA or the OO/DA model to define unit boundaries
- Instantiate, run, then tear down that Unit
- Does it work as expected?

Tool	Use With
Terratest	Terraform, Kubernetes, Packer, Docker, Cloud APIs
Kitchen-terraform	Terraform

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

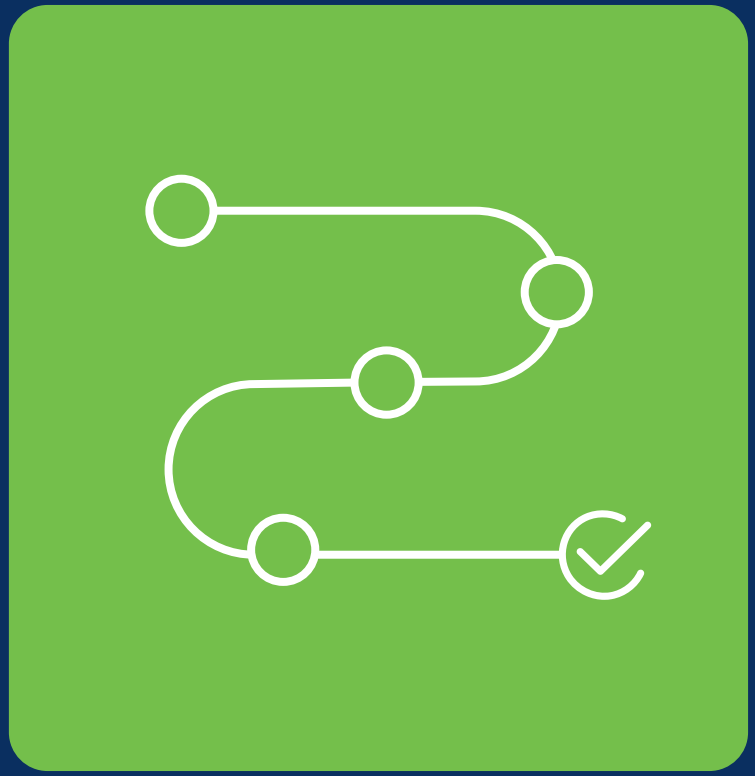
Automated Testing: Integration Test

- Do your Units work together?
- Do the OO units drive actions in the DA units?
- Create a diagram for the stages of your automation
- Author your test so that they address the stages

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Automated Testing:
End to End Test

- Can you afford to test all of your automation across the entire enterprise?
- Can you stage your entire end to end security system?
- Consider incremental updates to the end to end test



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Modeling Your Automation

Threat Modeling

- What is my automations objective?
- What are the threats?

S	Spoof
T	Tampering
R	Repudiation
I	Information Disclosure
D	Denial of Service
E	Escalation of Privilege

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Modeling: Spoof

Spoof: Fraudulent acts on automation input

- Can threat actors spoof anything on the input criteria?
  - Credentials
  - IP Addresses
  - ARP
  - Mobile Number
  - Man in the middle?
- To what degree can you trust the input?
- What are the consequences/impact?

S
T
R
I
D
E

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Modeling: Tampering

Tampering: intentional modification of objects in a way that would make them harmful to the system

- How are you checking integrity?
- What would be the impact?

S
T
R
I
D
E

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Modeling: Repudiation

Repudiation: the authenticity is being "repudiated"

- What proof do you have of the integrity or original data?
- Are there audit trails to the automation to prove its integrity?
  - If a threat actor performed an action, what evidence would you have?

S
T
R
I
D
E

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Modeling: Information Disclosure

Information Disclosure: Data leak or privacy breach

- What information if learned by the threat actor would be harmful?
- If the threat actor could man-in-the-middle, what could they learn that would be harmful?
- Deterministic Patterns that can be used against you?
  - Playbooks
  - Standard procedures
  - Time of day weaknesses

S
T
R
I
D
E

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Modeling: Denial of Service

Denial of Service: An attack on any part of the system resulting in service outage

- What are all the touch points of the automation and are any of them:
  - Vulnerable to a volumetric attack
  - Vulnerable to a computational attack
- How would you be notified of a Denial of Service event?
- What countermeasures do you have in place?

S T R I D E

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Modeling: Escalation of Privilege

Escalation of Privilege: At any point in the automation could privileges be escalated?

- First stop: Is anything running as root and why must it run as root?
- Least Privilege principal
- At any point, if privileges were escalated, what is the detection methods and what are the countermeasures?

S
T
R
I
D
E

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Threat Modeling

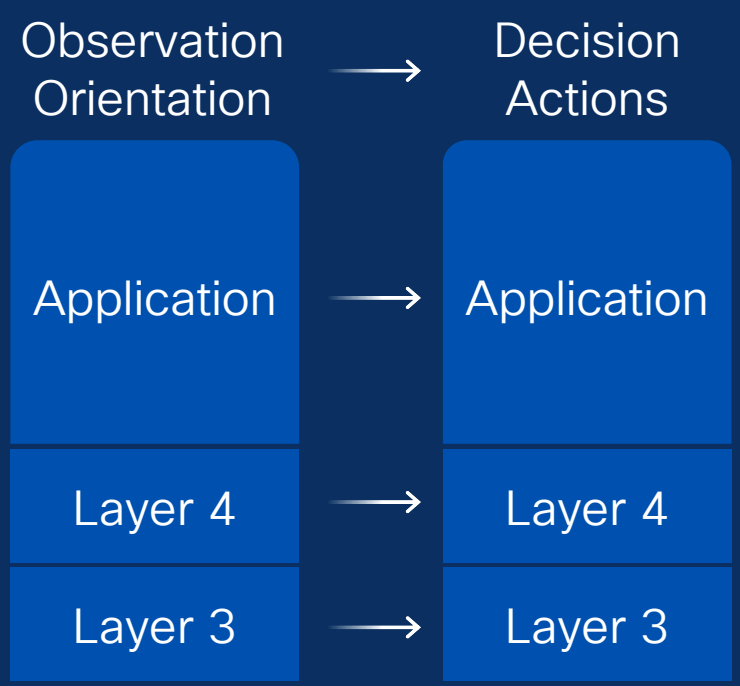
Use S.T.R.I.D.E to evaluate your automation in design and in production

- **S** Spoof
- **T** Tampering
- **R** Repudiation
- **I** Information Disclosure
- **D** Denial of Service
- **E** Escalation of Privilege

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Balancing Precision on Detection & Protection

- Detection at the applications layer (ie URL) should not have a crude block of a port/IP
- Try and match the precision of the automation with that of what triggered the automation



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Summary

- Use OODA loop to understand the phases of your Automation
- Be sensitive to the precision of O,O matches the D,A
- Use Automated Testing or Peer Review to provide evidence of success
- Use Threat Modeling to ensure your Security Automation is safe

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

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 Challenge** for every survey completed.

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

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

cisco Live!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Technologies

General Security Technologies

Learn about the different shades of cyber security in our daily lives and join us for a journey through various topics, from the depths f the darknet to the peak of crypto-analysis.

START

Monday, June 5 | 1:00 p.m.
BRKSEC-1639
An Introduction to Risk-Based Vulnerability Management

Monday, June 5 | 3:00 p.m.
BRKMER-2003
Meraki with Secure Network Analytics and XDR: Threat Detection for the Rest of Us

Monday, June 5 | 4:00 p.m.
BRKSEC-1023
Accelerate your SOC with Cisco XDR

Tuesday, June 6 | 1:00 p.m.
BRKSEC-2084
Seeing is Believing: Unlocking XDR Outcomes with Visibility

Tuesday, June 6 | 2:30 p.m.
BRKSEC-2101
Malware Execution As A Service: a Deep Dive into CSMA Advanced File Analysis

Wednesday, June 7 | 10:30 a.m.
BRKSEC-2095
Cisco XDR with Email: Protect, Analyze and Evolve the SMTP Conversation

Wednesday, June 7 | 1:00 p.m.
BRKSEC-2113
Cisco XDR - Making sense of the Solution and how it's a Security Productivity Tool

Thursday, June 8 | 9:30 a.m.
BRKSEC-2178
Extended Detection with Cisco XDR: Security analytics across the enterprise

Thursday, June 8 | 10:30 a.m.
BRKSEC-2931
Building, Proving, and Extending Detections in Secure Analytics

FINISH

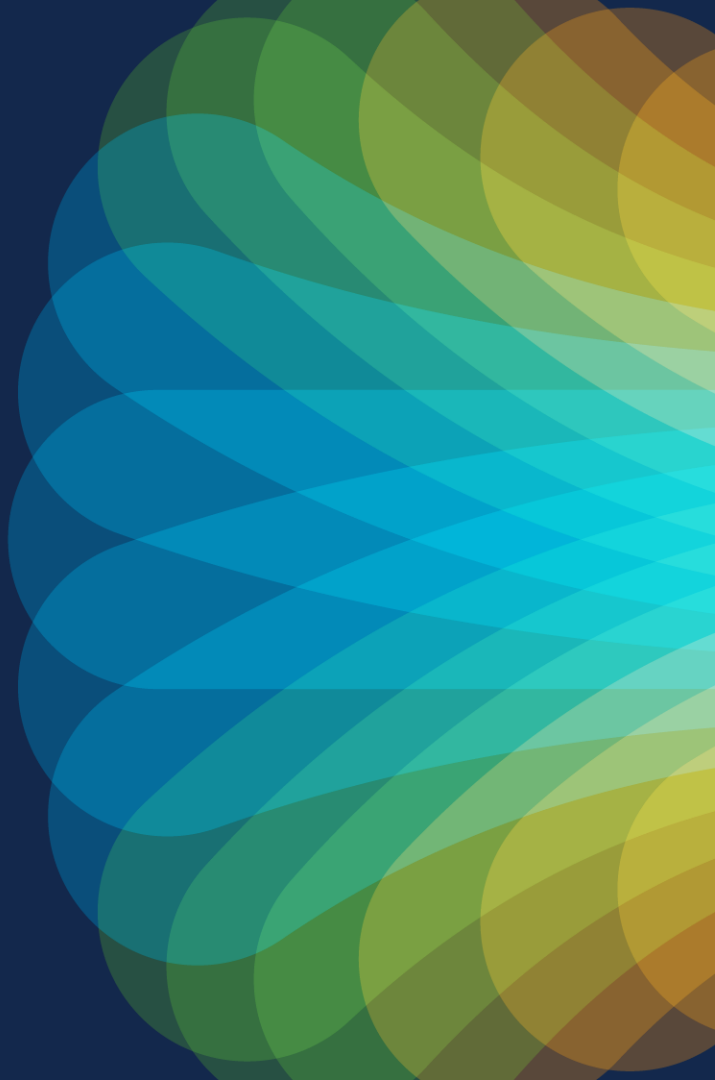
Thursday, June 8 | 1:00 p.m.
BRKSEC-3116
Automating your Cisco XDR Workflows: from Threat Hunting, to Finding and Confirming Incidents, to Responding!

If you are unable to attend a live session, you can watch it On Demand after the event

cisco Live!

The bridge to possible

Thank you



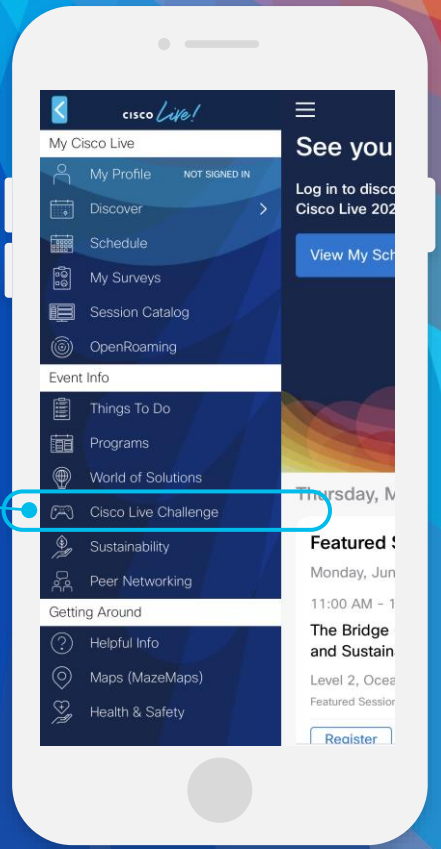
Cisco Live
Challenge

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:



cisco Live!

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public


cisco Live!
Let's go
#CiscoLive