Cisco live!

January 28 - February 1, 2019 • Barcelona

cisco

IMAGINE

INTUITIVE

BRKCLD-2431

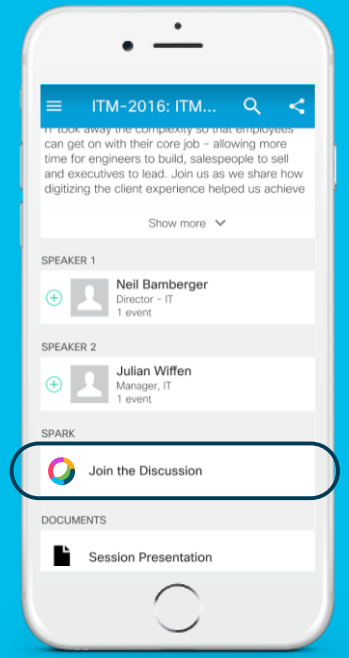
Secure Your Enterprise Apps!

A journey in automating application security and deploying policy control in a cloud world

Scott Ryan

Global Technical Solution Architect

scryan@cisco.com @saryan210



cs.co/ciscolivebot#BRKCLD-2431

Cisco Webex Teams

Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

How

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

Agenda

- Security Threats and Changing Landscape
- Journey to Securing Enterprise Applications in a Cloud World
- Operational Shifts “People, Process, and Tools”
- Securing the Enterprise Application Development Lifecycle
- Automating Securing the Enterprise Application Development Lifecycle
- Summary and Call To Action

Security Threats and Changing Landscape

The Changing Landscape

Devices / Users

Anywhere / Anything
Identity-as-a-Service
Unsecured IOT Devices

Network

As-a-Service Model
Software Defined
Networking

Storage

Data Protection
Regulations (GDPR)
Data Virtualization
Storage-as-a-Service

Applications

Anywhere
Secure SDLC
Cloud Native &
Microservice
Architecture

Compute

Serverless Compute
Containers

Cost of Data Breaches

- Average total cost of a data breach: $3.86M
- Average cost per lost or stolen record: $148
- The mean time to identify (MTTI) was 197 days
- The mean time to contain (MTTC) was 69 days

- Average cost of a breach with Automation $2.88M
- Without automation, estimated cost is $4.43M
- $1.55M Net Difference

Securing Applications

- Application security encompasses measures taken to improve the security of an application often by finding, fixing and preventing security vulnerabilities during the life cycle of the application.
- Different techniques are used to surface such security vulnerabilities at different stages of an applications lifecycle such design, development, deployment, upgrade, maintenance.
- Securing the identity and access between users/devices and applications from anywhere
- Increase agility to deploy applications while increasing security and compliance.

Application Security Trends

Application Vulnerabilities

Serious application security vulnerabilities continues to increase at a rate that makes remediation nearly impossible

Reusable Software Vulnerabilities

70% of applications comprised of reusable software (3rd party, Open Source) that inherit these vulnerabilities

Microservices Vulnerabilities

More vulnerabilities per line of code than traditional applications

Mobile Applications Vulnerabilities

85% of mobile apps violated one or more of the OWASP Mobile Top 10

Embed Security Testing

Embed security within the SDLC process with monitoring to achieve significantly better application security and compliance

**Reference – "2018 Application Security Statistics Report"

Top Application Security Challenges

- Manual and complex identity and access management for users/devices and applications from anywhere
- Limited Realtime Visibility, Monitoring, and Enforcement consistency
- Mapping Business Policy to Application Deployment Policy
- Not all applications are equal "Cloud Enabled vs. Cloud Native"
- Lack of automating security testing and embedding security into the Application Development Lifecycle
- Changing the SECOPS and NETOPS process and culture

Journey to Securing Enterprise Applications in a Cloud World

Cisco live!

Journey to Securing Enterprise Applications in a Cloud World

Current State

- Manual and complex identity and access management for users/devices and applications from anywhere
- Limited Security Visibility, Monitoring, and Enforcement consistency
- Automating security into the Application Development Lifecycle
- Mapping Business Policy to Application Deployment Security Policy
- Not all applications require the same security "Cloud Enabled vs. Cloud Native"
- Complex SECOPS and NETOPS process and culture

Future State

- Deploy segmentation and automate Identity and Access Control
- Automate realtime visibility and monitoring tools for the Application Development Lifecycle
- Automate security enforcement into the Application Development Lifecycle
- Integrate ITSM tools to automated business policy into security enforcement policies
- Deploy the proper security architecture and enforcement for your cloud applications
- Align your operational Process, People and Tools to provide the agility and security needed to support a DevOps and SecDevOps environment for cloud applications.

The Journey

Analytics for Assurance

Predictive performance with machine learnin

Secure Foundation

Rapid threat detection and mitigation

Intent-based Network

Constantly learning, adapting, protecting

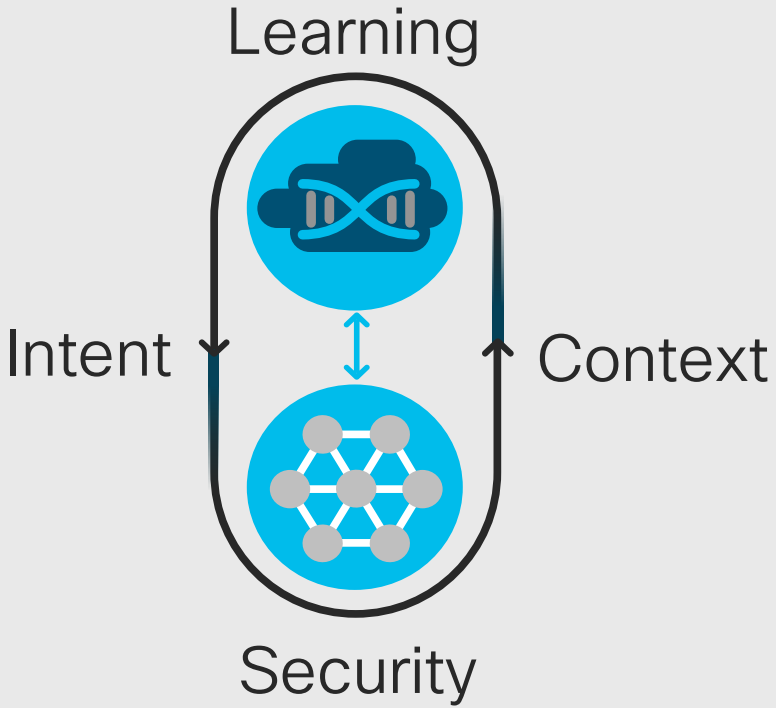
Policy Based Automation

Simplify, scale network deployment for Cloud, Mobile, IoT

Infrastructure Readiness

Open and Programmable

Leveraging an Intent-based Approach



Powered by intent. Translate business intent to network policy

Informed by context. Constant visibility into all traffic patterns

Constantly learning. Machine learning at scale to provide increasing intelligence

Constantly protecting. See and predict issues and threats and respond faster.

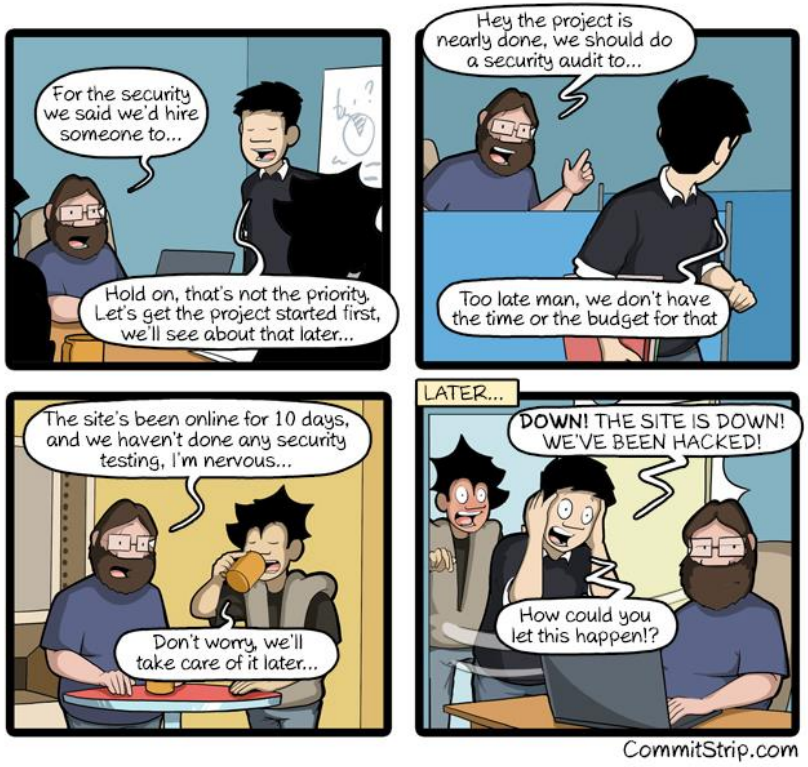
The Journey to the Future State

- The Journey is different for every customer
  - Static
  - Scripting/Templates
  - Automation
  - Orchestration
  - Intent
- Increase agility to deploy applications while increasing security and compliance.
- Driving consistency in securing applications deployed anywhere and accessed from anywhere
- Securing Enterprise Cloud Applications with an Intent Driven Process and Architecture

Operational Shifts

“People, Process, and Tools”

Security is beyond architecture and technology



Security is beyond architecture and technology

People

Tools & Technology

Process

People

Roles & Responsibility

Business

Development

Operations

Security

Innovation Acceleration and Individual Priorities

Business

Speed to Market while while retaining brand trust and compliance

Developers

Freedom to access the best platforms and tools for increased agility

Operations Team

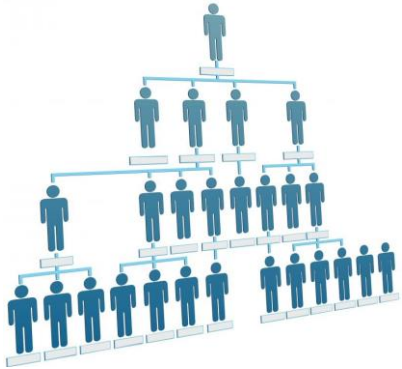
One consistent environment to eliminate silos and drive efficiency

Security Team

Visibility and control across one hybrid environment without slowing innovation

People

Organization Changes



Changing Organization Structures to align with new Development and Operational Models

People

Organization Changes

Limited Resources

Simplifying Responsibility

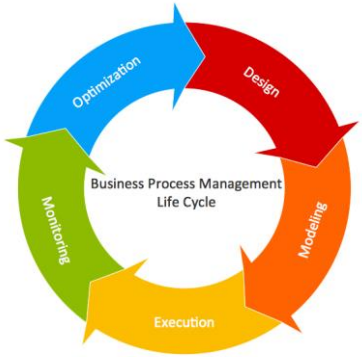
Functional Abstraction

Intent Based

Process

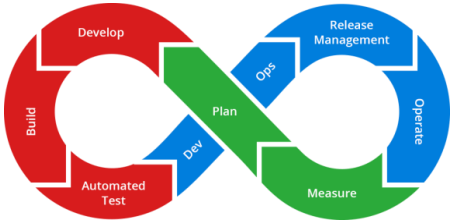
Defining Intent

Business Process



Software Development Process

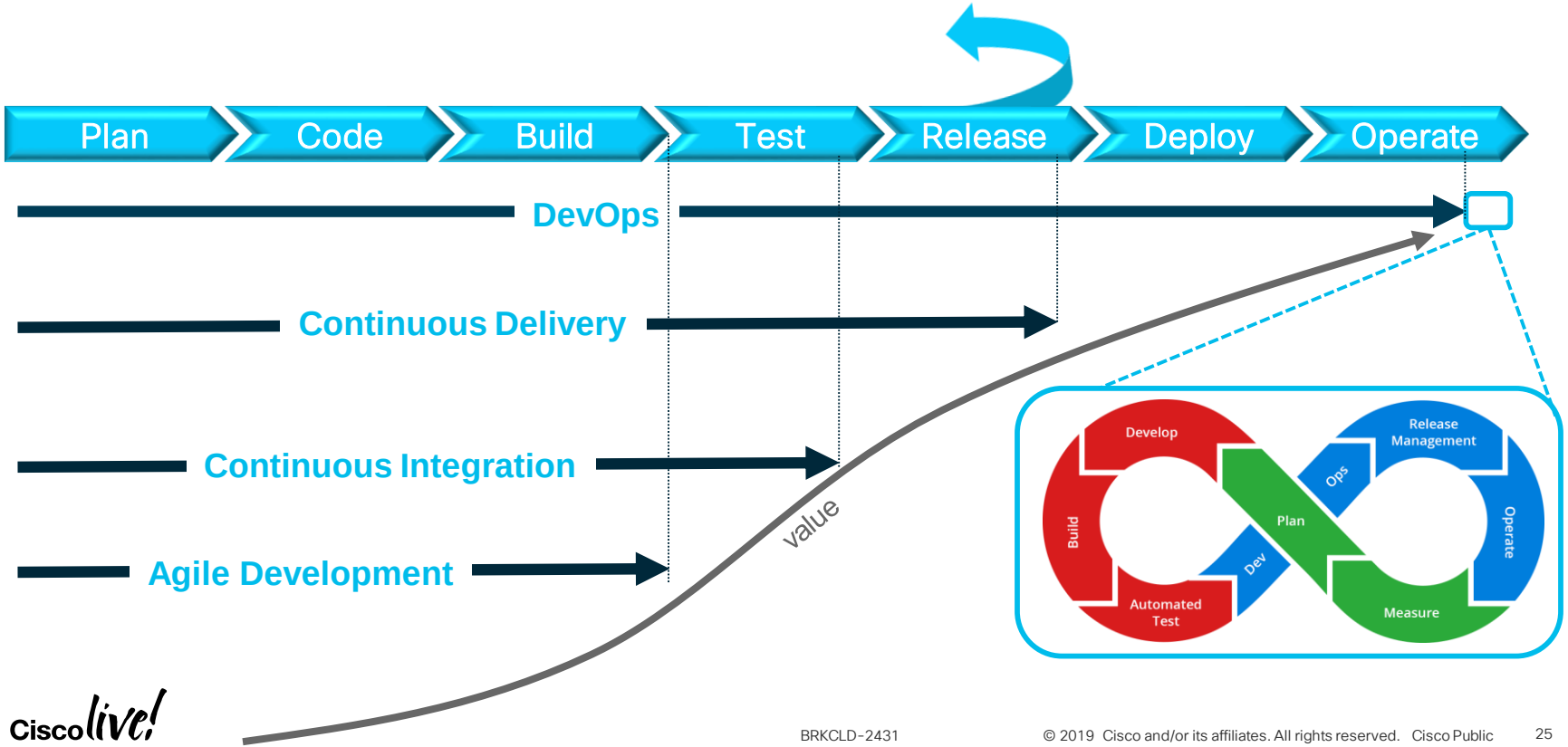
CI/CD Pipeline



Securing Enterprise Application Deployment Lifecycle

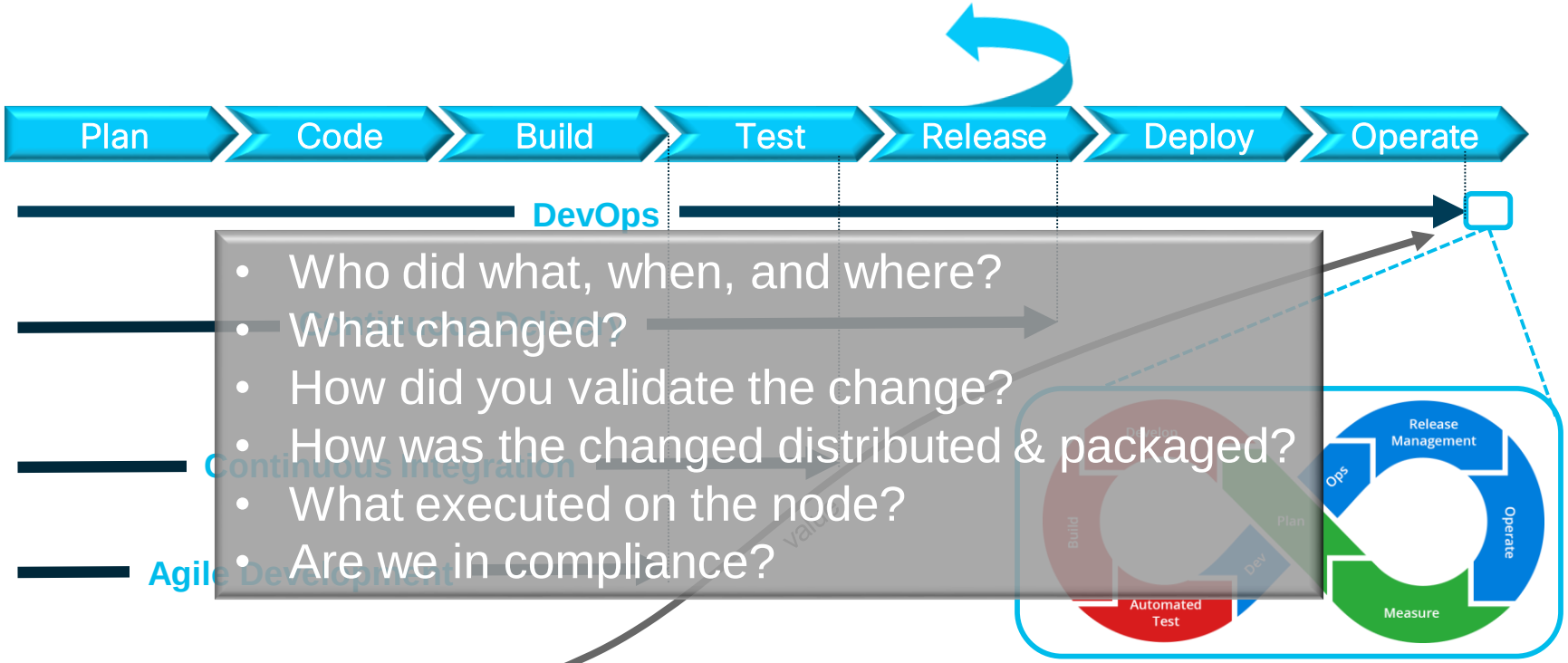
Software Development Lifecycle

Continuous Integration (CI) / Continuous Delivery (CD)



Software Development Lifecycle

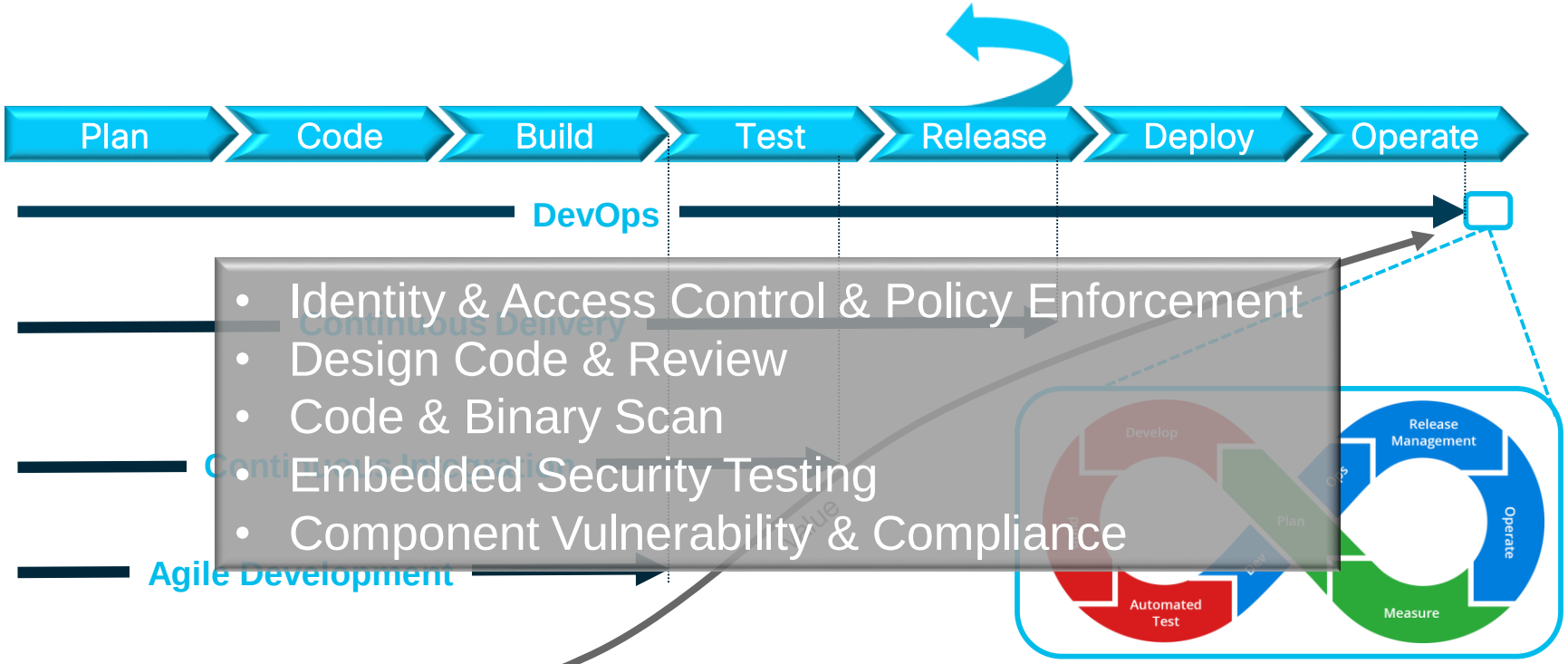
Continuous Integration (CI) / Continuous Delivery (CD)



- Who did what, when, and where?
- What changed?
- How did you validate the change?
- How was the changed distributed & packaged?
- What executed on the node?
- Are we in compliance?

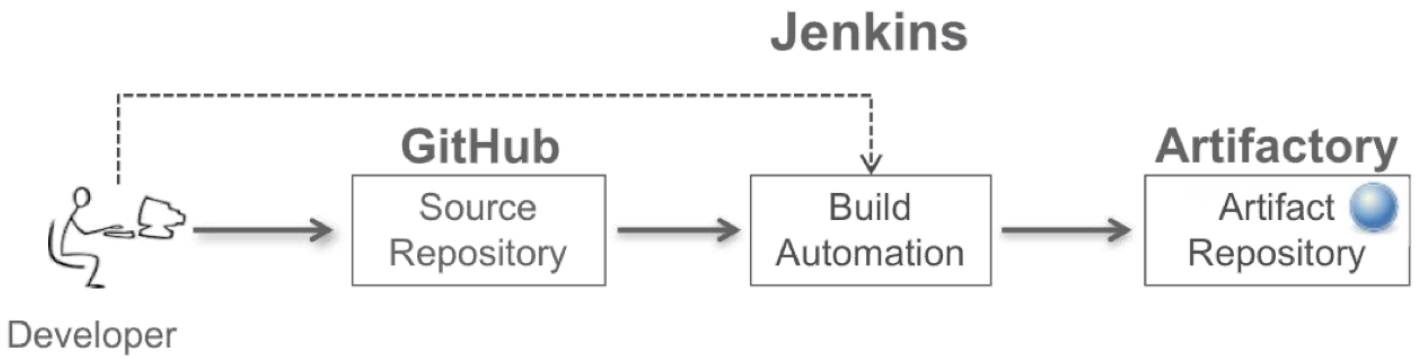
Software Development Lifecycle

Continuous Integration (CI) / Continuous Delivery (CD)

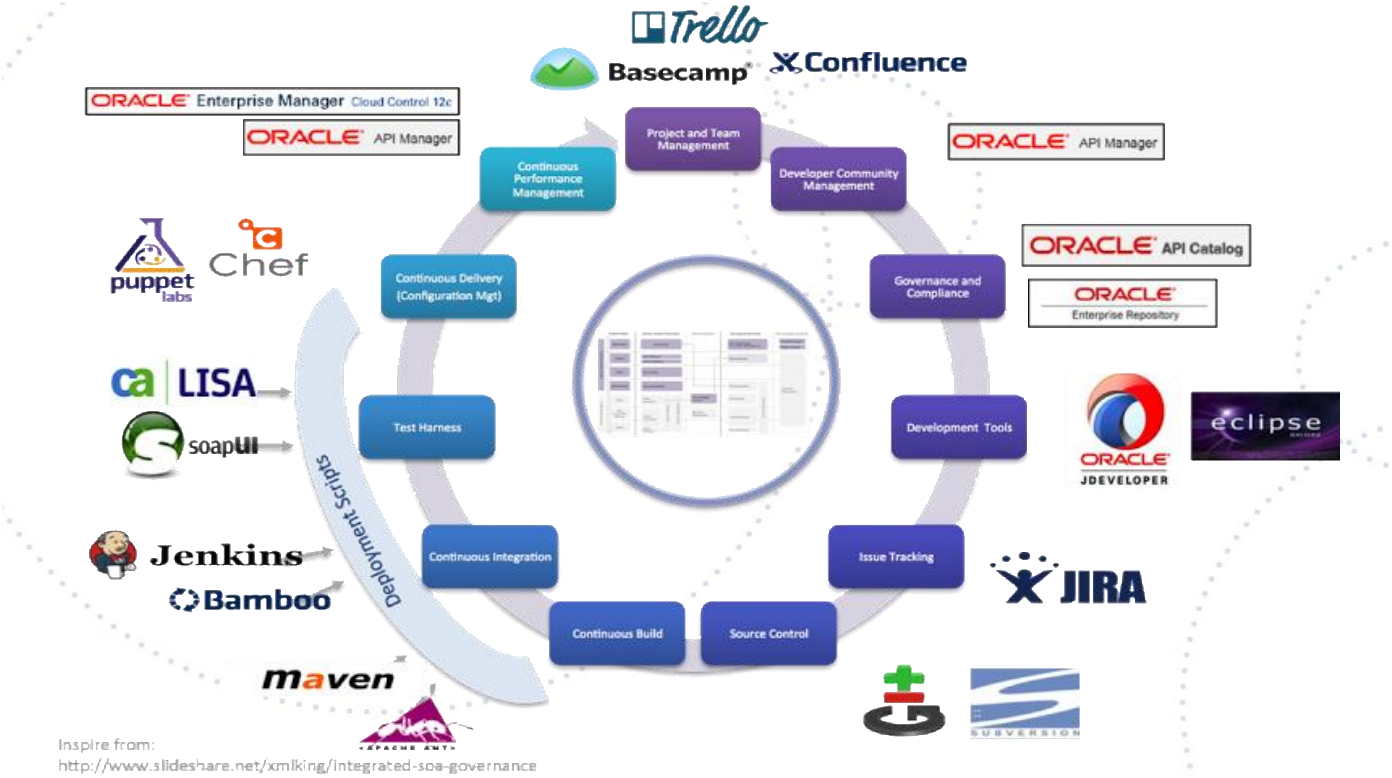


- Identity & Access Control & Policy Enforcement
- Design Code & Review
- Code & Binary Scan
- Embedded Security Testing
- Component Vulnerability & Compliance

Typical Software Development and Automation



Managing and Securing the Code



http://www.soa4u.co.uk/2015/04/a-word-about-microservice-architectures.html

Re-Think Security

Need For Speed

Automating Security

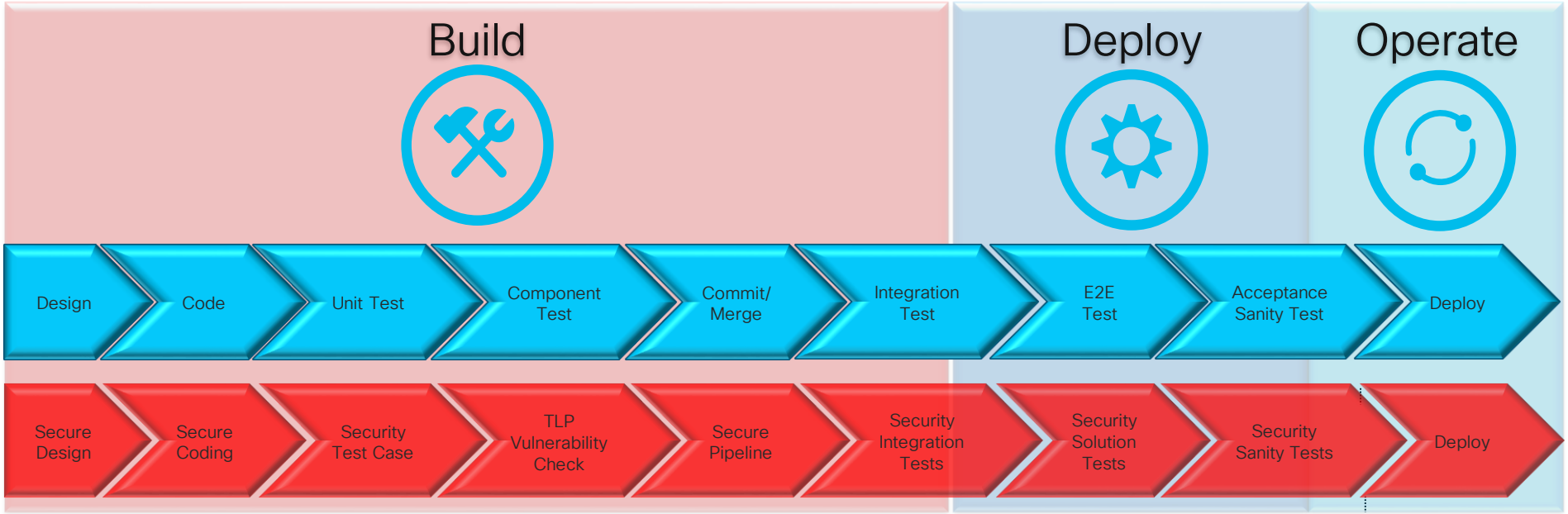
- Fast & Agile
- Competitive Differentiator

Securing Enterprise Application Deployment Lifecycle

- *DevSecOps* and *DevOpsSec*
- *Frictionless Security, Rugged DevOps, Security At Speed*
- Process of integrating secure development best practices and methodologies into development and deployment processes
- Security-as-a-Service
- Security As Code

Securing Enterprise Application Deployment Lifecycle

SecDevOps Approach – Continuous Integration and Delivery Pipeline (CI/CD)



DevOps + Security Model = SecDevOps

Securing Enterprise Application Deployment Lifecycle

Applying a Cloud Security Model

Build

- Security Standards and Architectures
- Threat Analysis and Protection
- Quality Management
- Common Secure Services

Operate

- Data Encryption & Protection
- Assessment Activities
- Intrusion Detection & Prevention Systems
- Security Governance

Monitor

- Policy and Compliance
- Transparency to Enable Customers
- Secure Cloud Supply Chain
- Application Layer Data & Event Monitoring
- Analytics & Real Time Feedback

Securing Enterprise Application Deployment Lifecycle

Automating Security

Centralize Security Testing Services

Extensible UI & API's

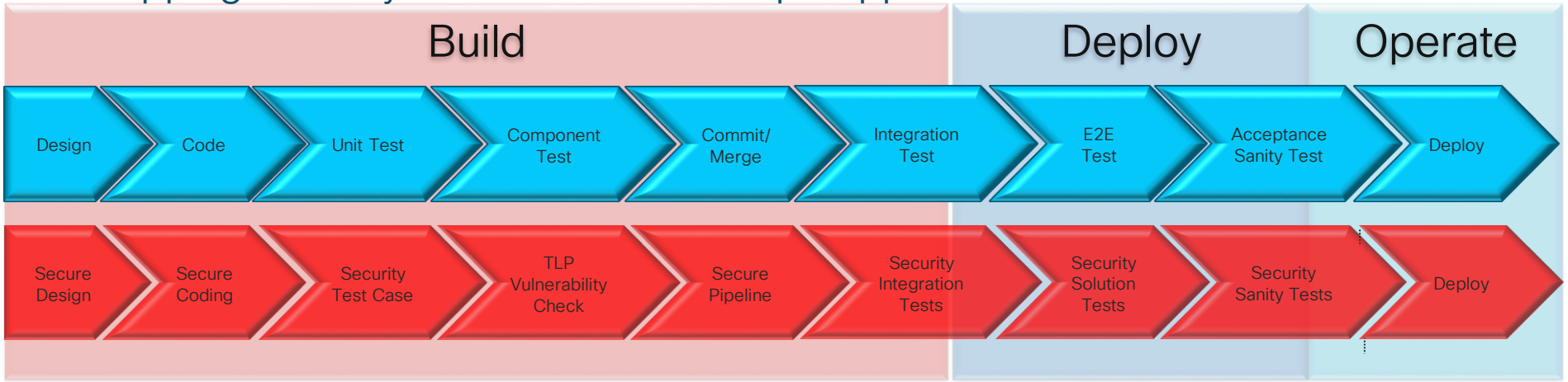
Policy Based "Intent Based"

Modular Architecture

Cloud Based Offering

Securing Enterprise Application Deployment Lifecycle

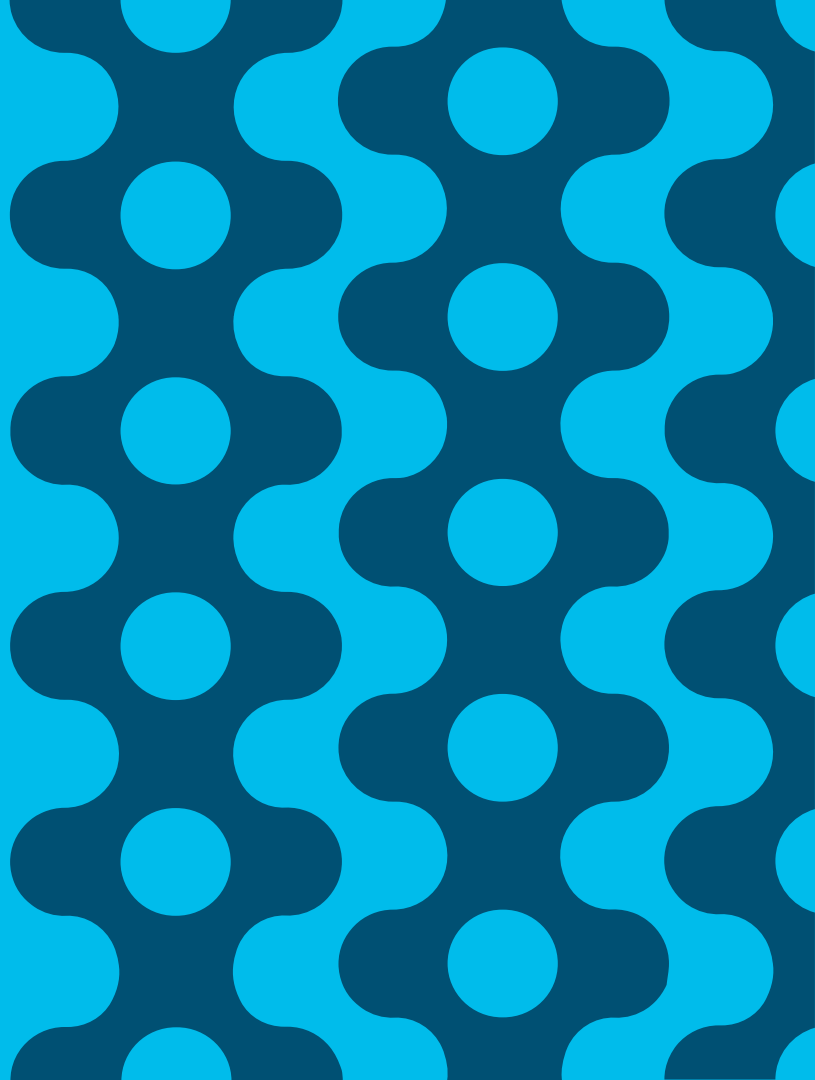
Mapping Security Tools to a SecDevOps Approach



- Qualys Vulnerability Scanning
- Qualys WAS testing (OWASP top 10 testing)
- Qualys Compliance Check Scanning
- Black Duck / Whitesource Open Source Vulnerability
- CIS OS Server Benchmarks & Hardening
- Visibility/Monitoring – AppD, Tetration, Stealthwatch

- CIS Docker Host Hardening Validation
- Docker Bench Security Tool
- Docker Image Vulnerability Scanning
- Infrastructure Hardening Validation
- Nmap/sslyze Crypto Tests
- Credentials brute-force testing

Automating Securing the Enterprise Application Lifecycle



Cisco live!

Automating Securing the Enterprise Application Lifecycle

Evolution of Security for SecOps and DevOps teams

Identity and Access Control

Application Vulnerability Checking

Segmentation

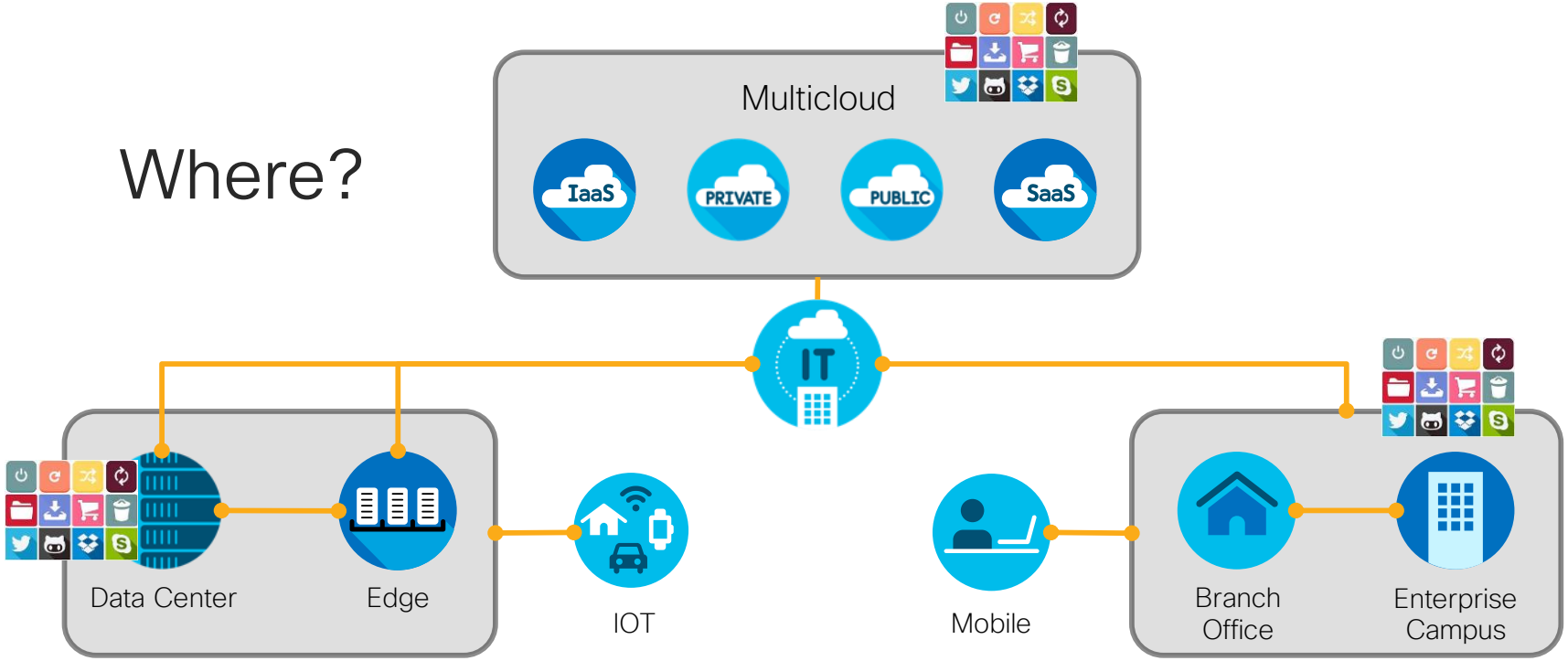
Secure Coding and Programming

Realtime Visibility and Analytics

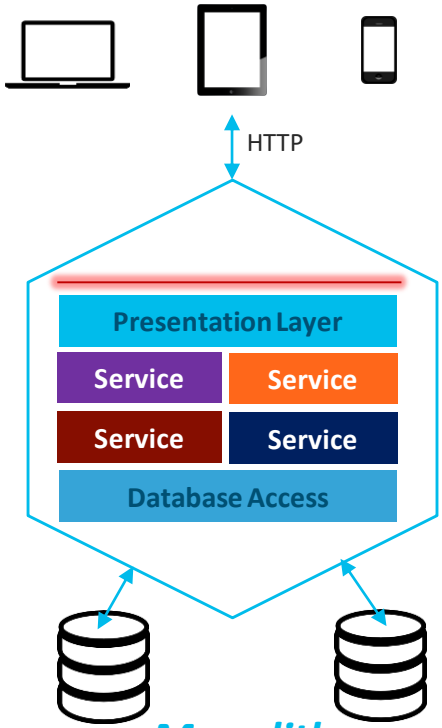
Automating Securing the Enterprise Application Lifecycle

Enterprise Application Deployments

Where?

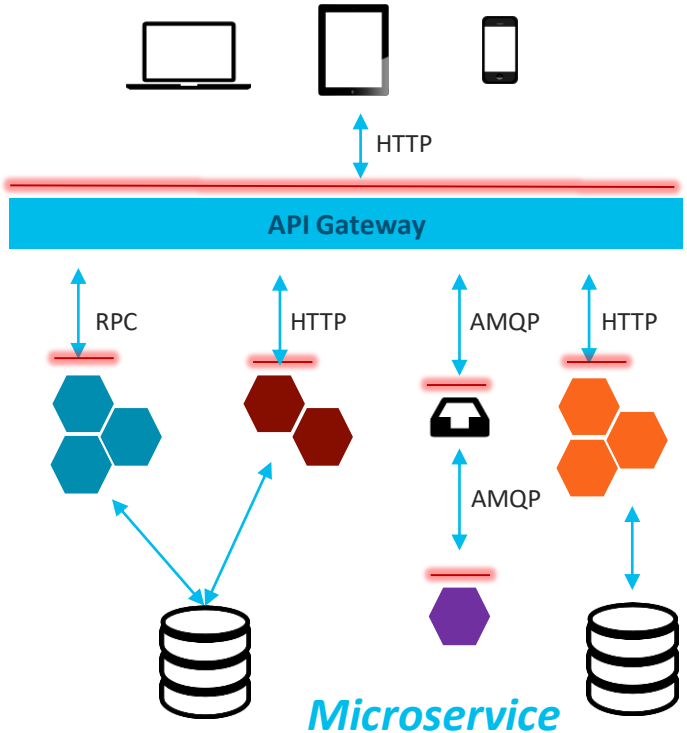


Cloud Enabled Application Architecture



Monolith
"Cloud Enabled"

Cloud Native Application Architecture

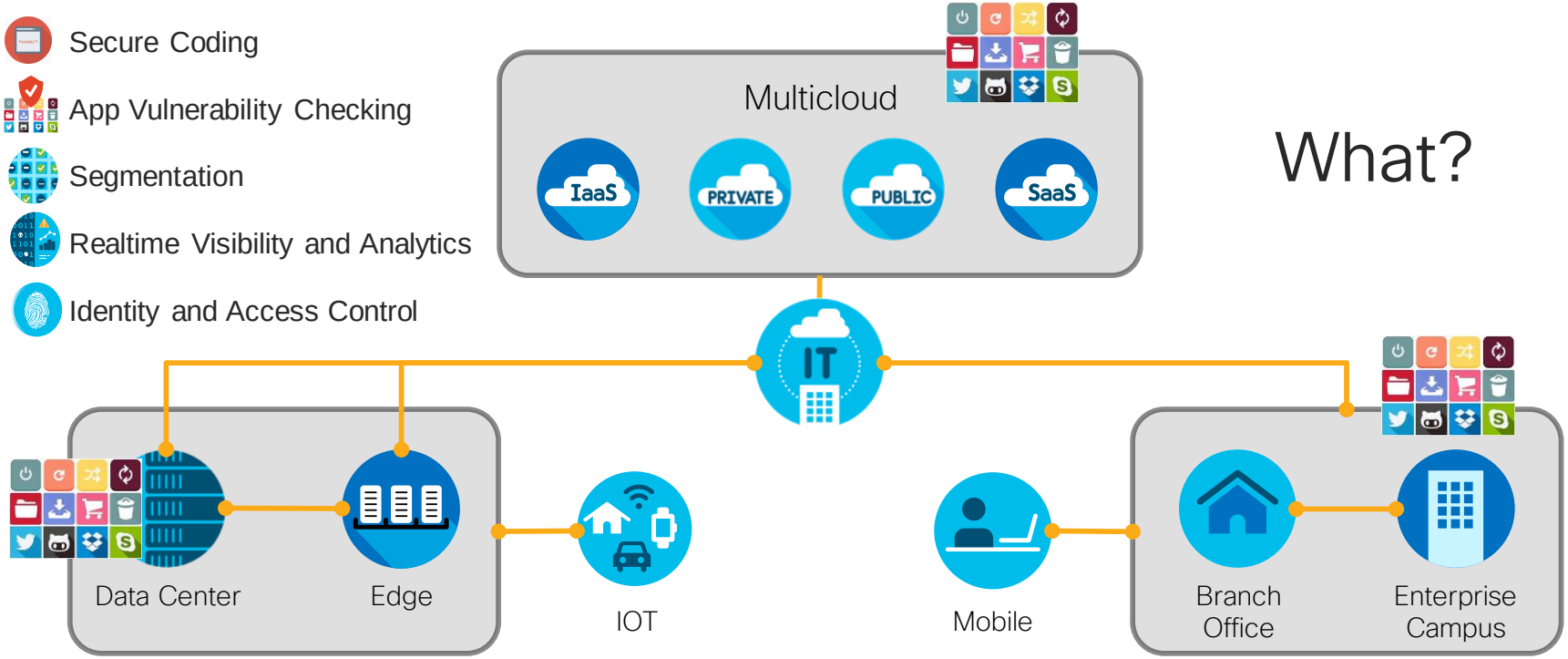


Microservice
"Cloud Native"

Automating Securing the Enterprise Application Lifecycle

Enterprise Application Deployments

- Secure Coding
- App Vulnerability Checking
- Segmentation
- Realtime Visibility and Analytics
- Identity and Access Control



What?

Automating Securing the Enterprise Application Lifecycle

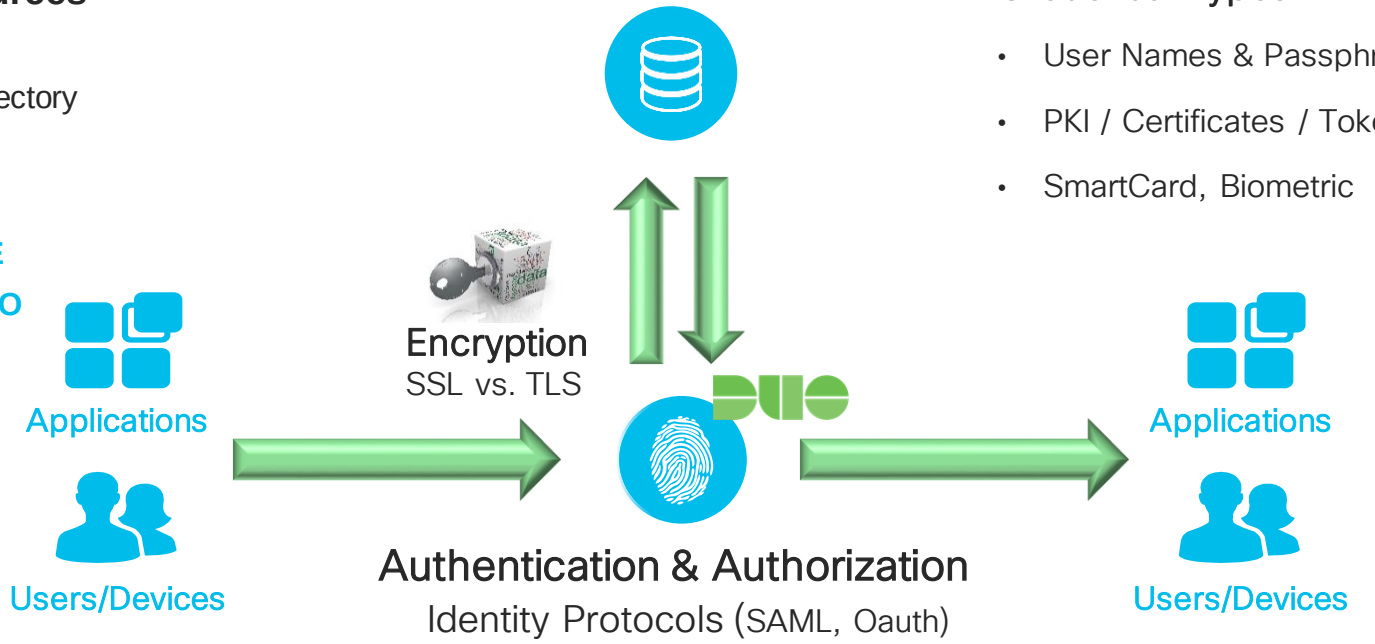
Identity and Access Control

Identity Sources

- LDAP
- Active Directory
- IDaaS
- IdP
- **Cisco ISE**
- **Cisco DUO**

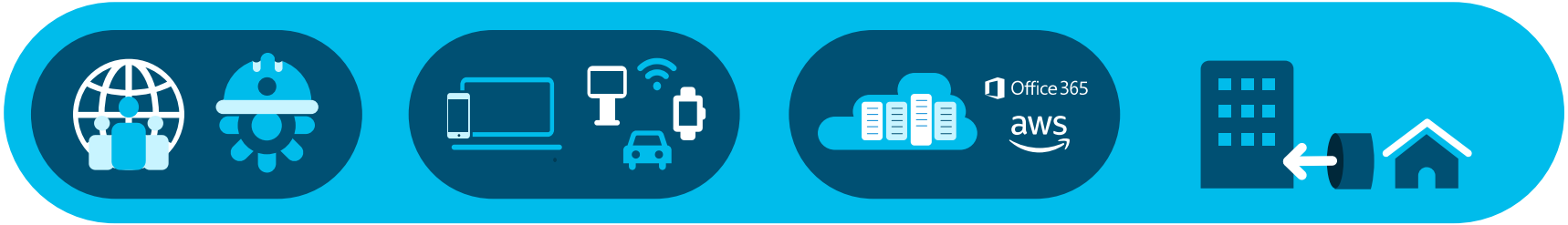
Credential Types

- User Names & Passphrases
- PKI / Certificates / Tokens
- SmartCard, Biometric



Automating Securing the Enterprise Application Lifecycle

Changing Identity and Access Controls for the Application Lifecycle



Any User
- Employee
- Contractor
- Vendor

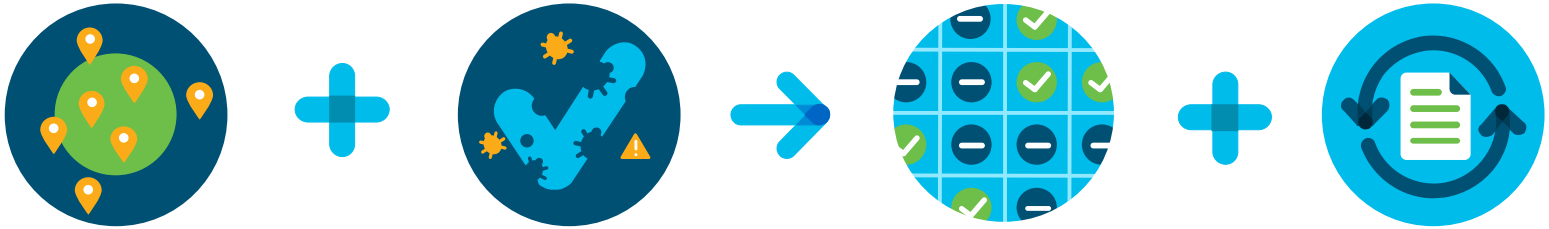
Any Device
- Corporate-Issued
- Bring-Your-Own
- IoT

Any App
- Data Center
- Multicloud
- SaaS

In Any Location
- On-Premises
- On-VPN
- Off-Network

Automating Securing the Enterprise Application Lifecycle

Changing Identity and Access Controls for the Application Lifecycle



Location ≠ Trust

Don't grant access to data based on where requests originate in the Network, Data Center, and/or Cloud

Trust Erosion

Don't rely only on one-time verification of user, device, and workload trust

Restrict Access

Prioritize enforcing the least privileges for the least time for your high-risk data

Automate Policy

Adjust access using dynamic context to improve policy efficacy and simplicity

Automating Securing the Enterprise Application Lifecycle

Changing Identity and Access Controls for the Application Lifecycle

Threat-Centric

Basic level of security maturity to prevent attacks via an intelligence-based policy – then detect, investigate, and remediate

Dynamic Context

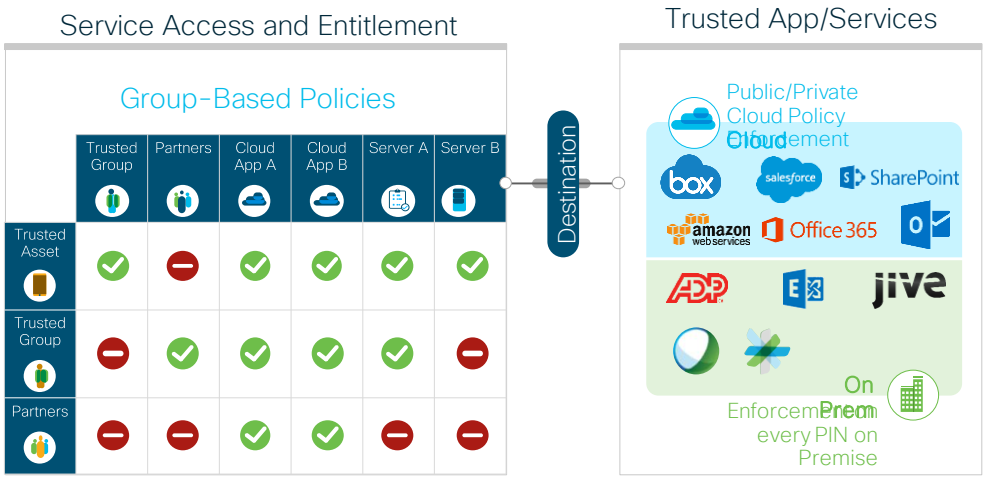
Trust-Centric

Good security practice to verify before granting access via a identity-based policy – for any user, any device, any app, in any location

Automating Securing the Enterprise Application Lifecycle

Changing Identity and Access Controls for the Application Lifecycle

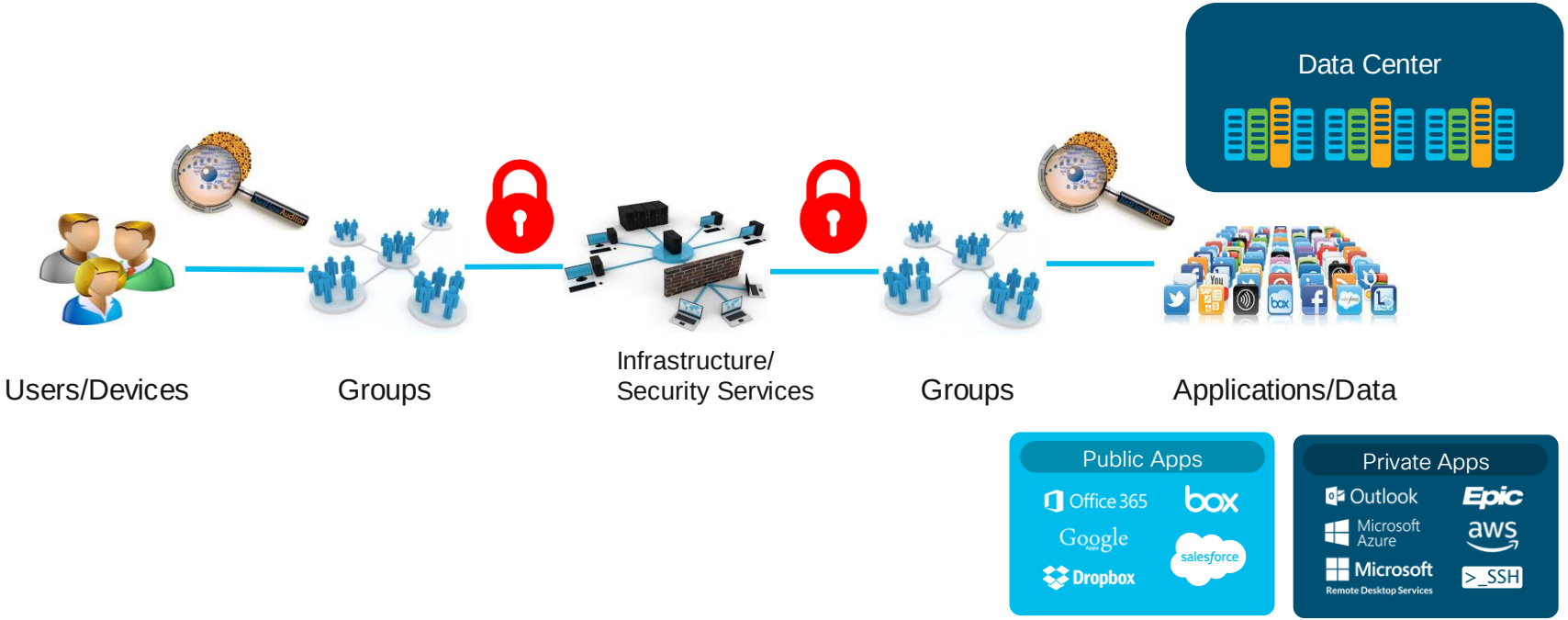
POLICY INTENT



Move from Static to Dynamic

Automating Securing the Enterprise Application Lifecycle

Policy



Automating Securing the Enterprise Application Lifecycle

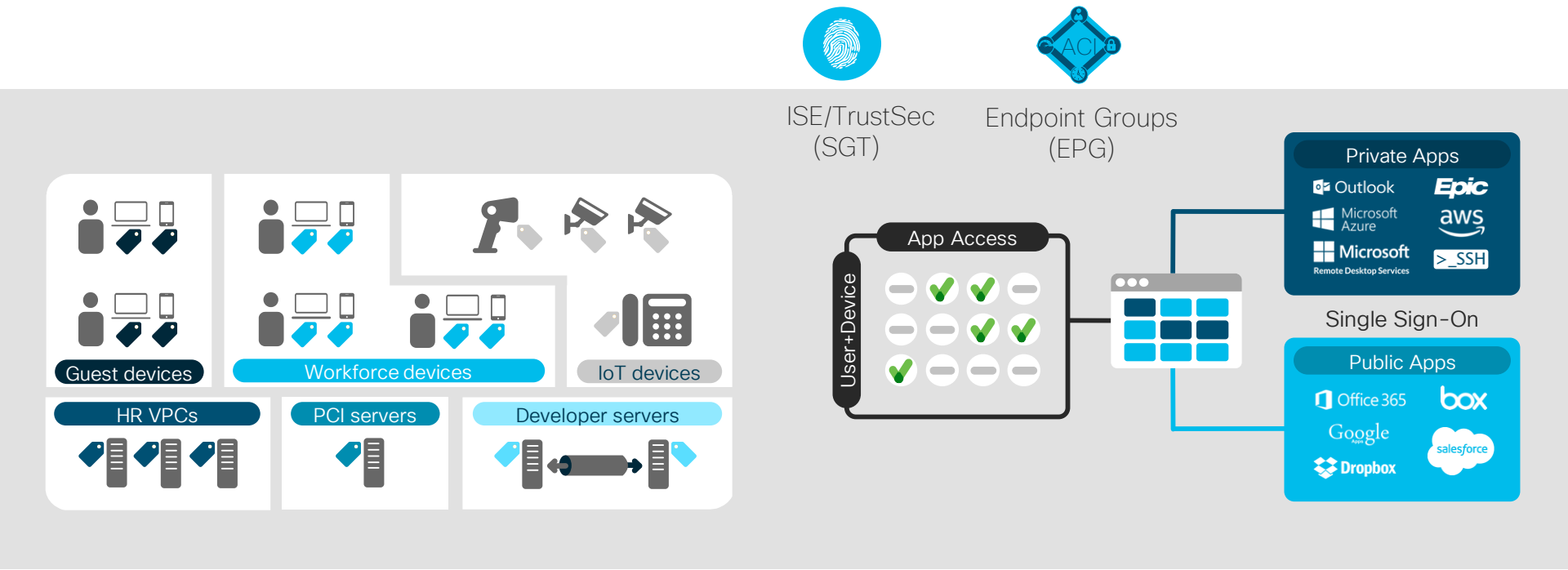
Group-Based Policy Domains

- Group membership are not shared between domains

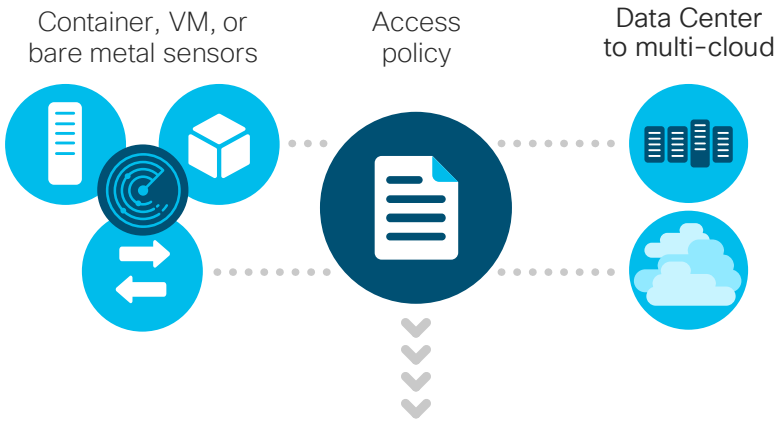
- Cloud environments and vendor-specific domains are increasingly using group-based policies

Automating Securing the Enterprise Application Lifecycle

Segmentation – Reduce the Attack Surface within Application Deployments

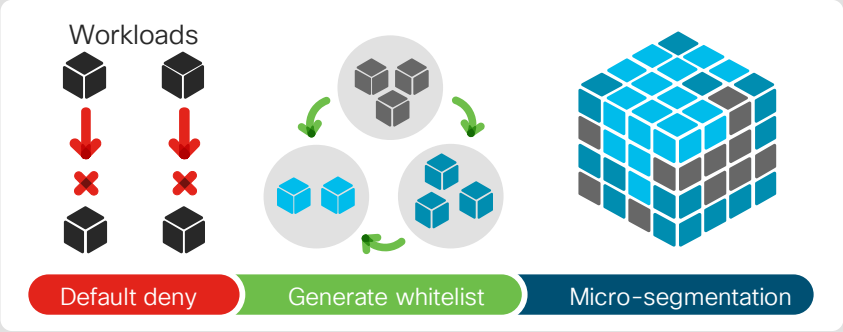


Realtime Application Visibility and Behaviour



Analyze East-West traffic and score vulnerabilities

Cluster groupings using machine learning



Tetration - Realtime Application Visibility and Behaviour

Tetration - Realtime Application Visibility and Behaviour

Architecture overview

Access mechanism

- Web GUI
- REST API
- Event notification
- Cisco Tetration apps

Analytics engine

- Third-party sources (configuration data)
- Cisco Tetration™
- Bring your own data (streaming telemetry)

Data collection layer

- Software sensor and enforcement
- Embedded network sensors (telemetry only)
- ERSPAN sensors (telemetry only)

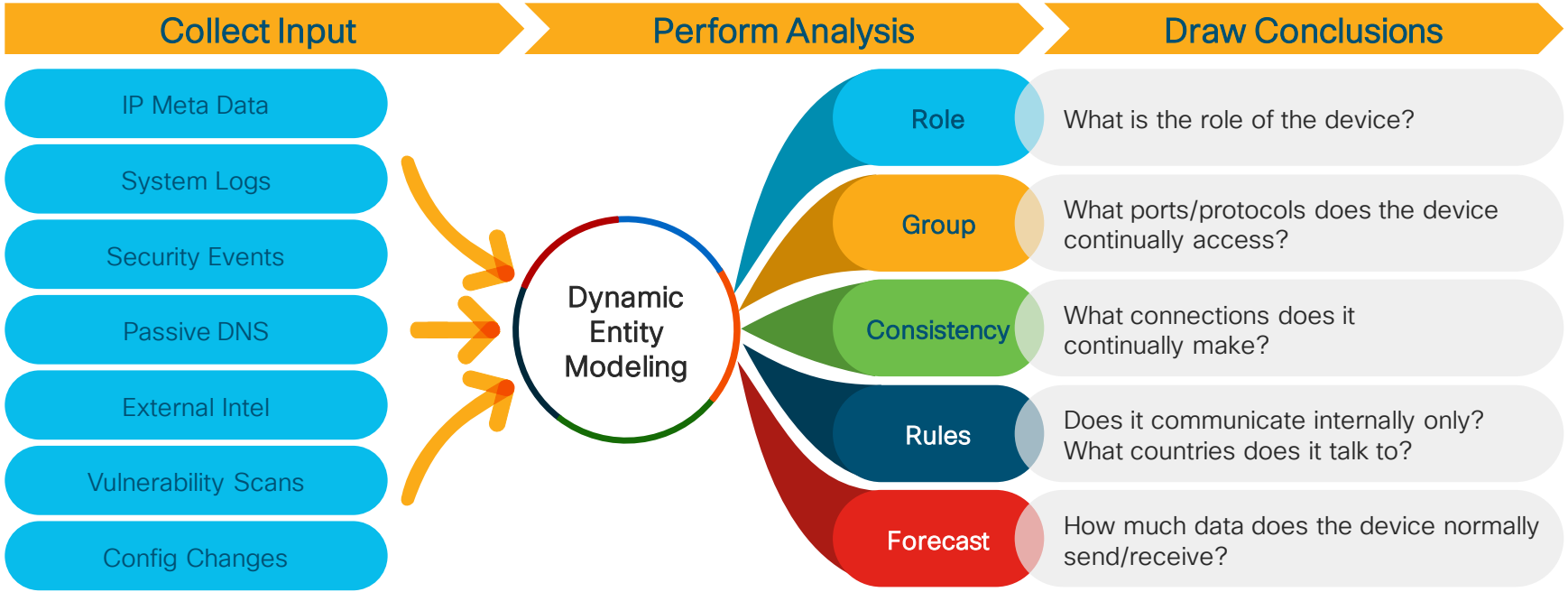
Stealthwatch – Realtime Network Visibility and Security Anomalies

- VPC Flow Logs
- Other data sources

- NetFlow
- Mirror port
- Other data sources

Stealthwatch – Realtime Network Visibility and Security Anomalies

- Dynamic Entity Modeling



Application Security

Visibility and Monitoring – Integrate Realtime Telemetry and Analytics

- Integrate RealTime Network Telemetry to provide context for policy enforcement to control application communication with Stealthwatch.
  - Monitor and Enforce Network Policy through ISE
- Integrate RealTime Application Telemetry to provide context for policy enforcement to control application communication Tetration.
  - Dynamically Discover and Profile Applications during the Application Lifecycle.
  - Monitor and Enforce Application Deployment Policy

Automating Securing the Enterprise Application Lifecycle

Identity, Segmentation, Visibility & Analytics

Developers
Operations

As-a-Service Portal

servicenow

Business

ISE
User/Device/App
Access Control

Stealthwatch
Network and Security Analytics

Tetration
Application Insights and Enforcement

Automating Securing the Enterprise Application Lifecycle

Identity, Segmentation, Visibility & Analytics Recommendations

- Simplify and Strengthen Identity and Access Control by deploying ISE and DUO
- Integrate real time telemetry into the entire Application Lifecycle to provide proper context for identity and policy enforcement with Tetration and Stealthwatch
  - Provide Dynamic Application Profiling in a Application Development environment
  - Provide Realtime Network and Security Analytics
- Simplify Key Management by deploying centralize KM or move to a KMaaS
- “No Trust” Policy from an API’s perspective – Secure all API’s with Strong Auth, Key/Certs, and Encryption (Prefer TLS)

Automating Securing the Enterprise Application Lifecycle

Application Vulnerability Checking

Scan Based Approach

Integrate/Plugin

Black Duck

Protecode

Palamida

OpenLogic

Whitesource

Contrast Security

Automating Securing the Enterprise Application Lifecycle

Application Vulnerability Checking

- Manual Code and Best Practices Reviews
- SAST – Static Application Security Testing “White Box Testing”
  - Byte or Binary Code is Analyzed for weaknesses
- DAST – Dynamic Application Security Testing “Black Box Testing”
  - Analyze Applications in Real-Time

- Examples:
  - AppSensor, OWASP Java Encoder, OWASP HTML Sanitizer

Application Vulnerability Checking

Common Vulnerabilities and Exposures (CVE)

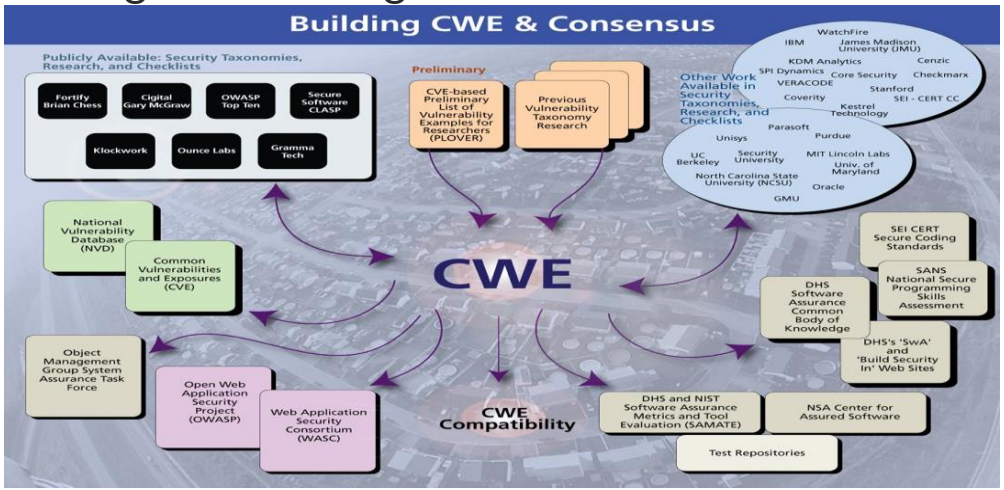
- Dictionary of publicly-known information
- Tools use CVE to cross-reference vulnerabilities
- Cisco has blocks for reporting new vulnerabilities
- Used in vulnerability alerting including Tetration

ADVISORY/ALERT	IMPACT	CVE	LAST UPDATED	VERSION
Search Advisory/Alert Name	All	Search CVE	Most Recent	
PHP Security Update for January 19, 2017	High		2017 Jan 20	1.0
Multiple OpenStack Products Disk Image Processing Denial of Service Vulnerability	Medium	CVE-2015-5162	2017 Jan 20	3.0
Oracle Outside In Technology RTF Parsing Code Execution Vulnerability	High	CVE-2017-3293	2017 Jan 20	1.0
Adobe Flash Player Memory Corruption Vulnerability	High	CVE-2017-2926	2017 Jan 20	2.0
McAfee ePolicy Orchestrator Cross-Site Scripting Vulnerability	Medium	CVE-2017-3902	2017 Jan 19	1.0
Cisco Unified Communications Manager Web Interface Cross-Site Scripting Vulnerability	Medium	CVE-2017-3802	2017 Jan 19	2.0
Oracle Critical Patch Update for January 2017	Critical	CVE-2015-0250 CVE-2015-1788 ...	2017 Jan 19	3.0
Oracle Outside In Technology PDF Parser Confusion Code Execution Vulnerability	High	CVE-2017-3271	2017 Jan 19	1.0
Cisco Email Security Appliance Filter Bypass Vulnerability	Medium	CVE-2017-3800	2017 Jan 19	1.1
QEMU Plan 9 File System Symbolic Link Privilege Escalation Vulnerability	High	CVE-2016-9602	2017 Jan 18	1.0

Application Vulnerability Checking

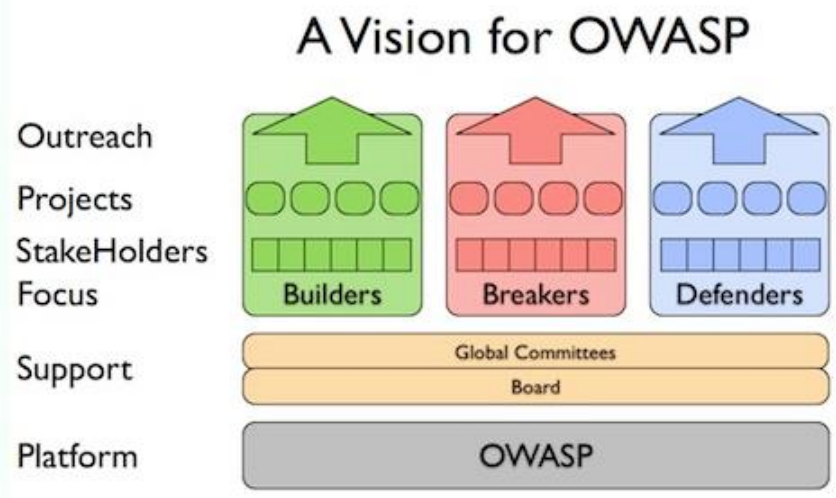
Common Weakness Enumeration (CWE)

- Unified, measurable set of software weaknesses
- Encourages more effective discussion and description
- Use software security tools and services to find weaknesses
- Better understanding and management architecture and design weaknesses



Application Vulnerability Checking

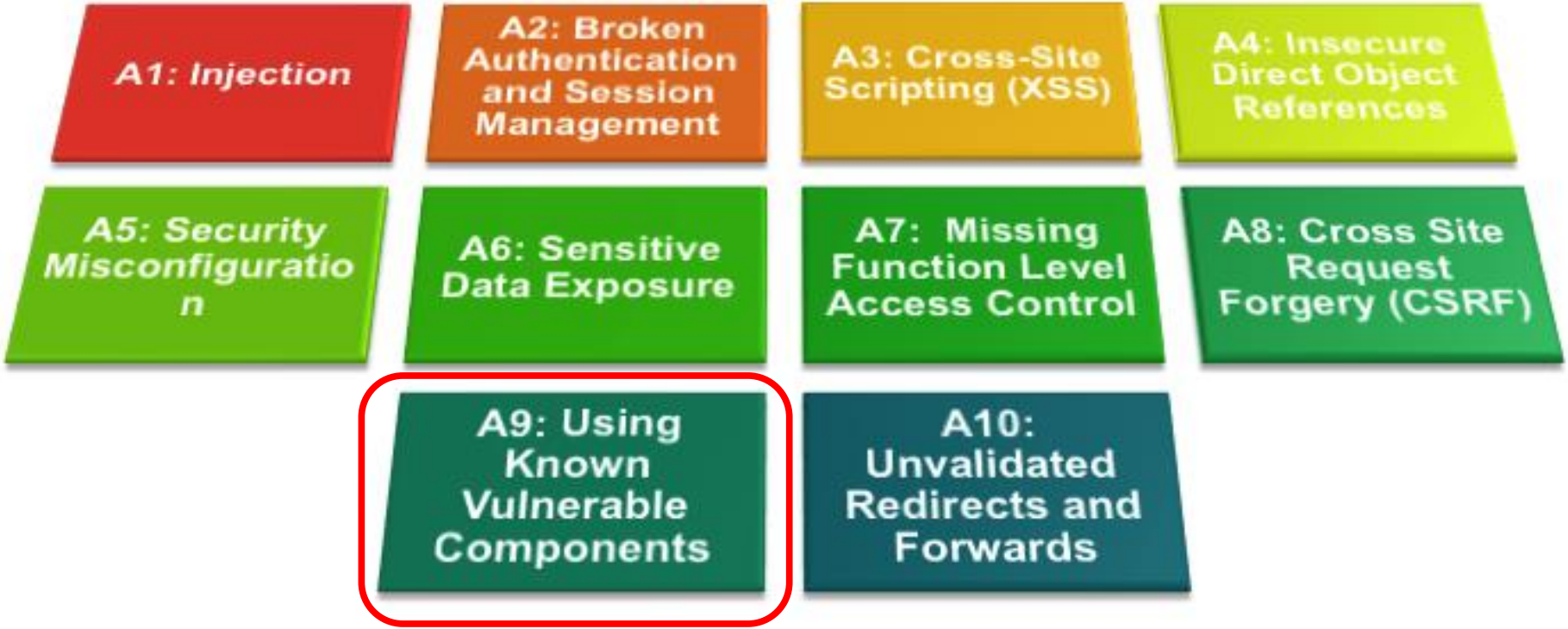
Open Web Application Security Project (OWASP)



- Global organization
  - Security of Web software
- Group of open projects
  - Secure design and test
- OWASP Top 10
- Application Security Verification Standard (ASVS)
  - Three-tirered Standard on how to achieve Basic Wed-Service Securities (200 recommdations)

Application Vulnerability Checking

OWASP Top 10



Application Vulnerability Checking

OWASP Application Security Verification Standard (ASVS)

- List of application security requirements or tests that can be used by architects, developers, testers, security professionals, and even consumers to define what a secure application is.
- Introduced June 2008
- Current version: v3.0.1 (July 2016)**
- Next version: ASVS 3.0.1 will be going directly to 4.0 soon

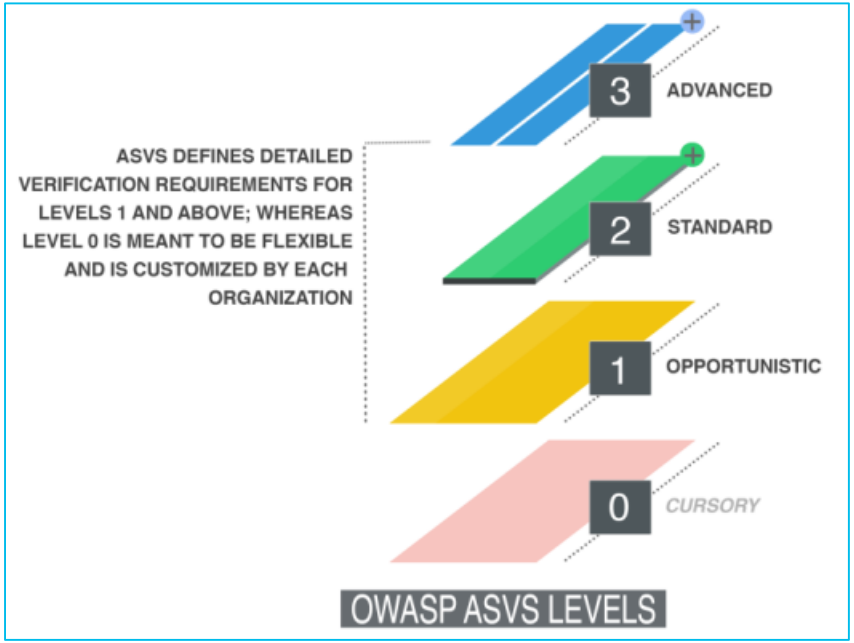
**Reference Documents:

https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf

https://github.com/OWASP/ASVS

Application Vulnerability Checking

OWASP Application Security Verification Standard (ASVS)



- **ASVS Level 3** – for applications that „shoot missiles" ;)
- **ASVS Level 2** – for applications that contain sensitive data
- **ASVS Level 1** – for all software

OWASP Security Recommendations

Top 10 is NOT ENOUGH

- Application Security Verification Standard (ASVS) should be what you targeting
- Review the 200 recommendations with your development teams. Not all will apply.
- Policy enforcement of the security recommendations need to be “Realistic” or they will not be used.

Secure Coding and Programing

Common Programing Mistakes

- “Trust” Exposed API’s
- “Trust” Client-side Validation
- Insufficient Data Format Validation
- Assuming strings are properly terminated, or data length fields carry proper values
- Character length versus Byte length
- Missing range checks
- Implicit and/or flexible data typing


```
var strFanName = txtFanName.Text.Trim();
var strPlayerList = txtPlayerList.SelectedValue.Trim();
var strComments = txtComments.Text.Trim();

// store the detials in variables
var fanName = Server.HtmlEncode(strFanName);
var favPlayer = Server.HtmlEncode(strPlayerList);
var fanComment = Server.HtmlEncode(strComments);

// prepare the message
var fanMessage = "Hey '" + fanName + "'. <br />Your jersey is begin printed.<br /><br />" +
                 "Thanks for voting '" + favPlayer + "'.<br />" +
                 "Your comment '" + fanComment + "' has been recorded.";

// show the message
lblStatus.Text = fanMessage;
```

Secure Coding and Programing

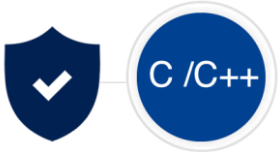
Programming Best Practices

Input Validation Frameworks / Process

Define Modular Boundaries & Expose Secure API's

Continuously Test & Validate Input

Secure Standard Libraries



Coverity, Jtest, Xcode SA

AppScan, WebInspect

OWASP Java Encoder & HTML Sanitizer

AppSensor

Automating Securing the Enterprise Application Lifecycle

Secure Coding and Programing Recommendations

- Validate Authenticity of the Tools, OS, Code
  - Validate from the source (GitHub), Secure Repository, Signed Images
  - Validate hardened OS – Follow Latest CIS Hardening Recommendations
- Secure Coding and Programming Best Practices
  - Realistically implement the 200 OWASP Application Security Verification Standards
- Embed SAST & DAST into the CI/CD process and fully use.
  - AppScan, WebInspect, AppSensor, OWASP Java Encoder, WASP HTML Sanitizer
- Integrating and embedding security checks into the IDE (Integrated Development Environment)

Summary

Journey to Securing Enterprise Applications in a Cloud World

Current State

- Manual and complex identity and access management for users/devices and applications from anywhere
- Limited Security Visibility, Monitoring, and Enforcement consistency
- Mapping Business Policy to Application Deployment Security Policy
- Not all applications require the same security "Cloud Enabled vs. Cloud Native"
- Automating security into the Application Development Lifecycle
- Changing the SECOPS and NETOPS process and culture

Future State

- Deploy segmentation and automate Identity and Access Control
- Automate realtime visibility and monitoring tools for the entire application lifecycle
- Integrate ITSM tools to automated business policy into security enforcement policies
- Deploy the proper security architecture and enforcement for your cloud applications
- Automate security enforcement into the Application Development Lifecycle
- Align your operational Process, People and Tools to provide the agility and security needed to support a DevOps and SecDevOps environment for cloud applications.

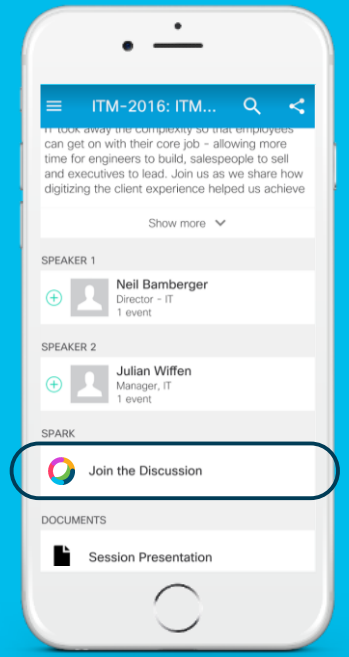
Building the Foundation for the Journey

- Deploying the foundational capabilities and functions needed to delivery consistent application security within the Application Development Lifecycle
  - Identity and Access Control – ISE/SDA and DUO
  - Segmentation – Implement a Segmentation strategy via ACI or TrustSec
  - Application Visibility and Monitoring – Tetration and Stealthwatch
  - Security and Network Operational Team Changes – Leverage DevOps and SecOps Approach
  - Drive Business Policy and Business Logic (ITSM) into Application Development Lifecycle
- Leverage a SecDevOps Approach
  - Embed & Automate Security Testing, Validation, and Tracking
  - Security-as-a-Service Model / Security As Code
  - Automate Tracking and Fixing Security Issues via Integrated Collaboration Tools

Call To Action

Call To Action

- Automate Security into your Enterprise Application Lifecycle
  - Automate Identity and Access Control – Deploy ISE and DUO
  - Automated Segmentation – Deploy ACI and/or TrustSec
  - Automate Application Profiling and Enforcement – Deploy Tetration
  - Automate Netowork and Security Analytics – Deploy Stealthwatch
- Leverage a DevOPS and SecDevOPS approach to optimize process with the tool/technologies to align to the proper organization changes
- Integrate and Automate security into the Platforms
  - Hyperflex, CCP, Public Cloud (Azure, AWS, Google)
- Integrate and Automate Intent into Application Deployment (Including Business Logic)



cs.co/ciscolivebot#BRKCLD-2431

Cisco Webex Teams

Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

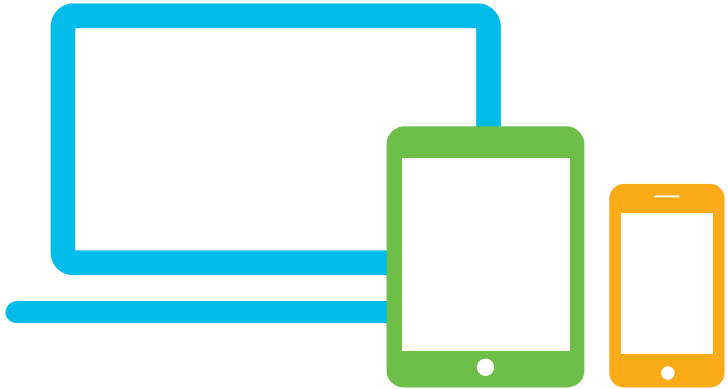
How

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

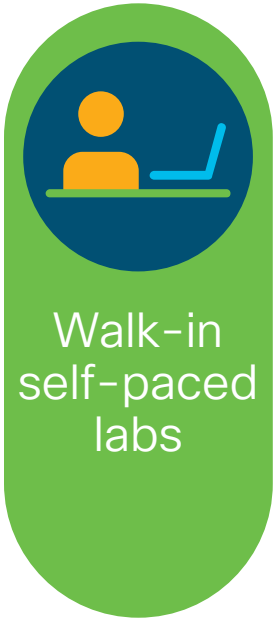
Complete your online session survey

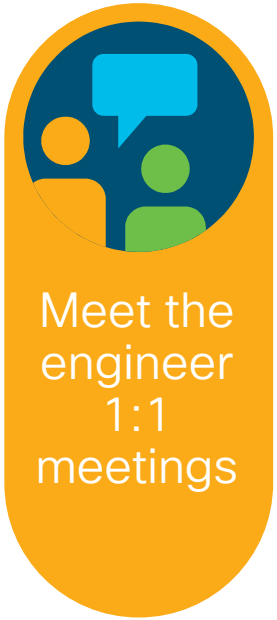
- Please complete your Online Session Survey after each session
- Complete 4 Session Surveys & the Overall Conference Survey (available from Thursday) to receive your Cisco Live T-shirt
- All surveys can be completed via the Cisco Events Mobile App or the Communication Stations

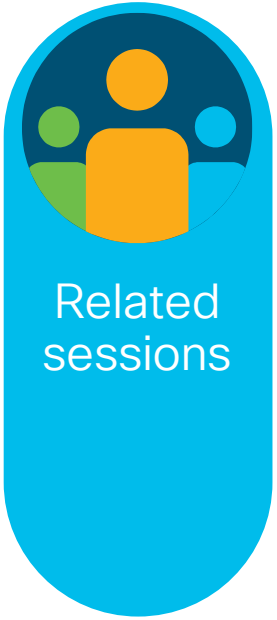
Don't forget: Cisco Live sessions will be available for viewing on demand after the event at ciscolive.cisco.com



Continue Your Education







Thank you

CISCO

IMAGINE

INTUITIVE