Transforming network operations with Closed-Loop Automation using AI Insights

Joerg Schultz, Partner Systems Architect - Distinguished Speaker
Christopher Beye, Systems Architect - Distinguished Speaker

BRKOPS-2814

slido

Please download and install the Slido app on all computers you use

Set the stage: What are your expectations of the session today?

ⓘ Start presenting to display the poll results on this slide.

That’s us …

Webex App

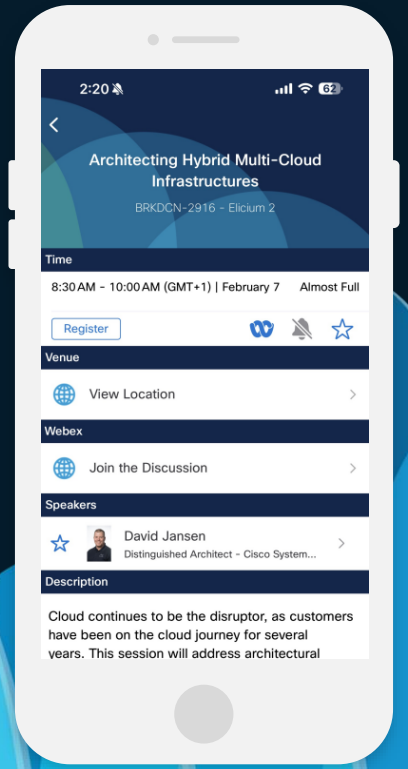
Questions?

Use the Webex app to chat with the speaker after the session

How

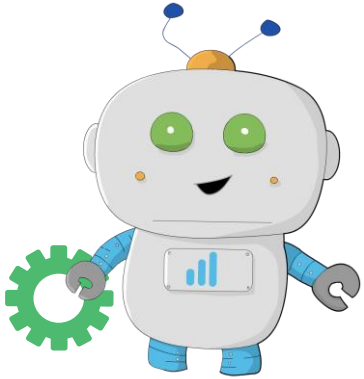
1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.



Agenda

- Introduction
- NetDevOps and CI/CD pipelines
- Let's talk Cross-Domain (Automation)
- Use case implementation
  - Cross-domain automation
  - Closed-loop automation
  - Integration with AI

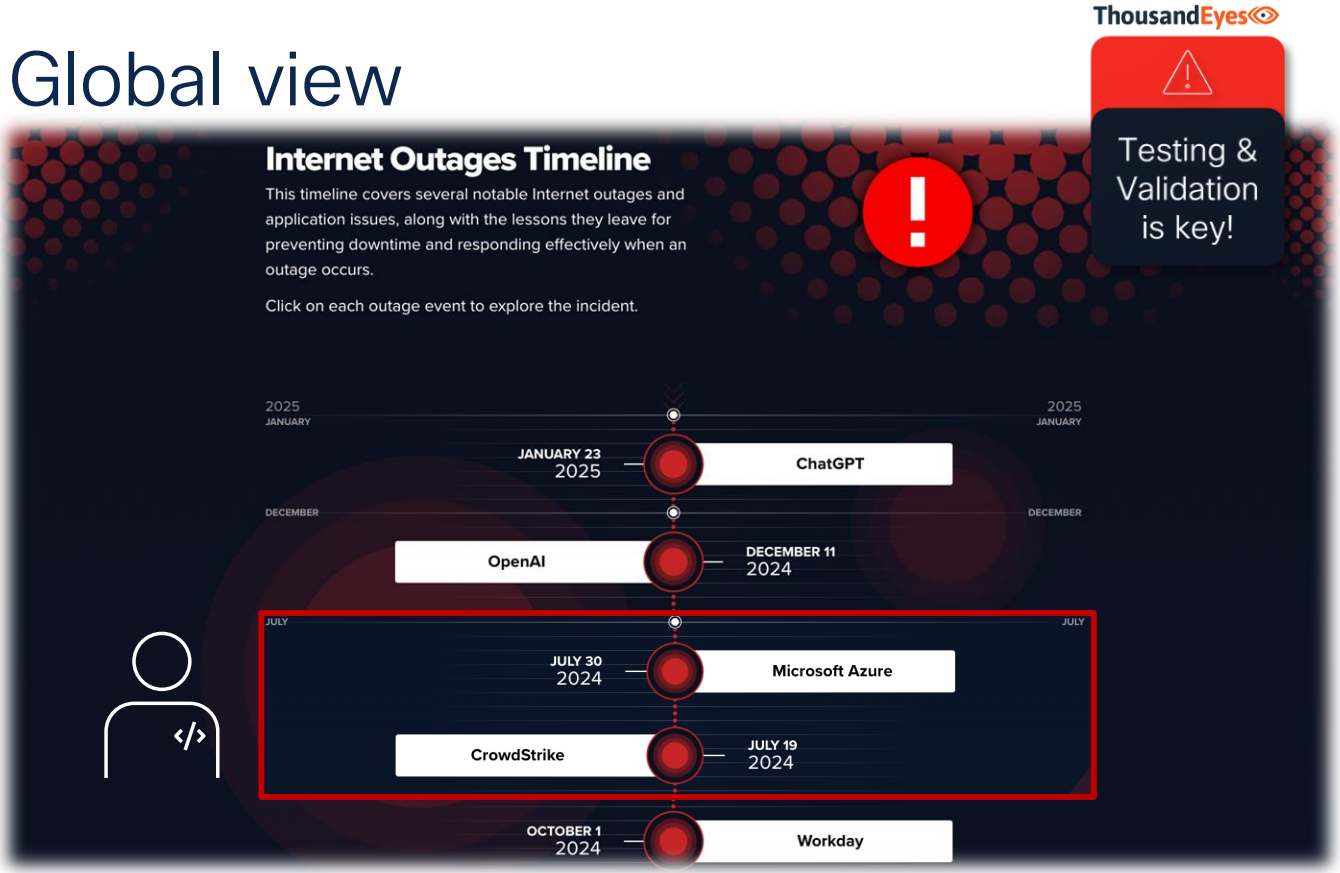


Introduction

If you like your job

Don’t break **things.**

Global view



https://www.thousandeyes.com/resources/internet-outages-timeline

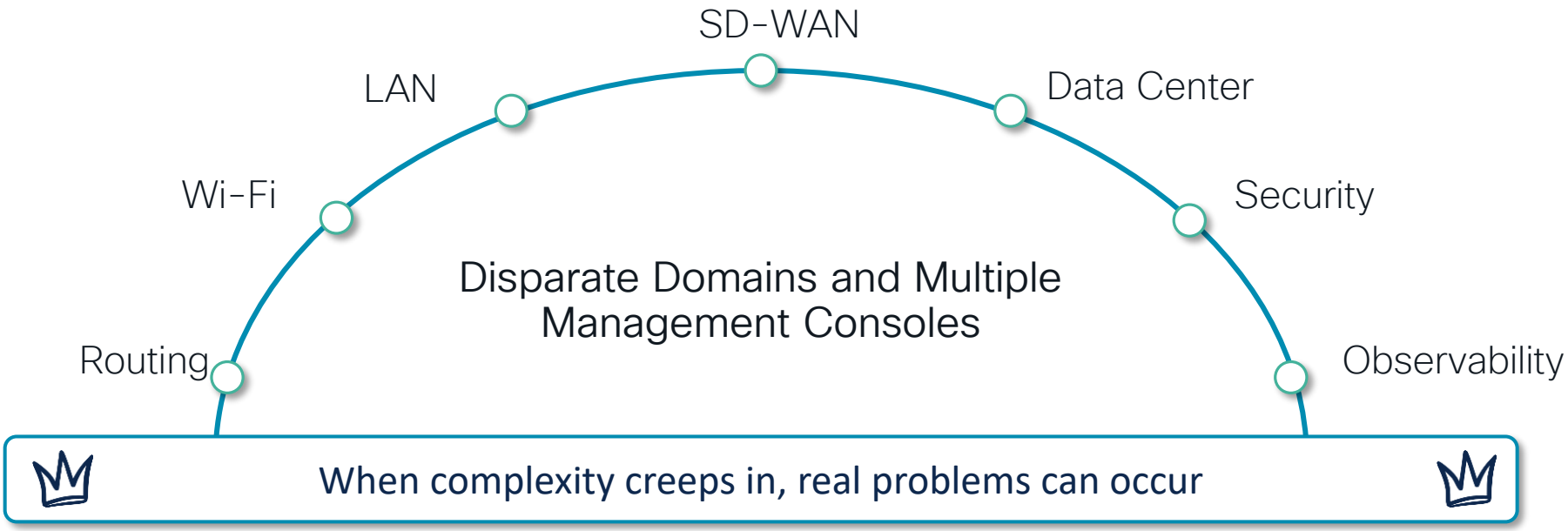
WHAT HAPPENED?

On July 19, a software update issue with Crowdstrike's security software caused widespread outages for various organizations, including airlines, banks, and hospitals.

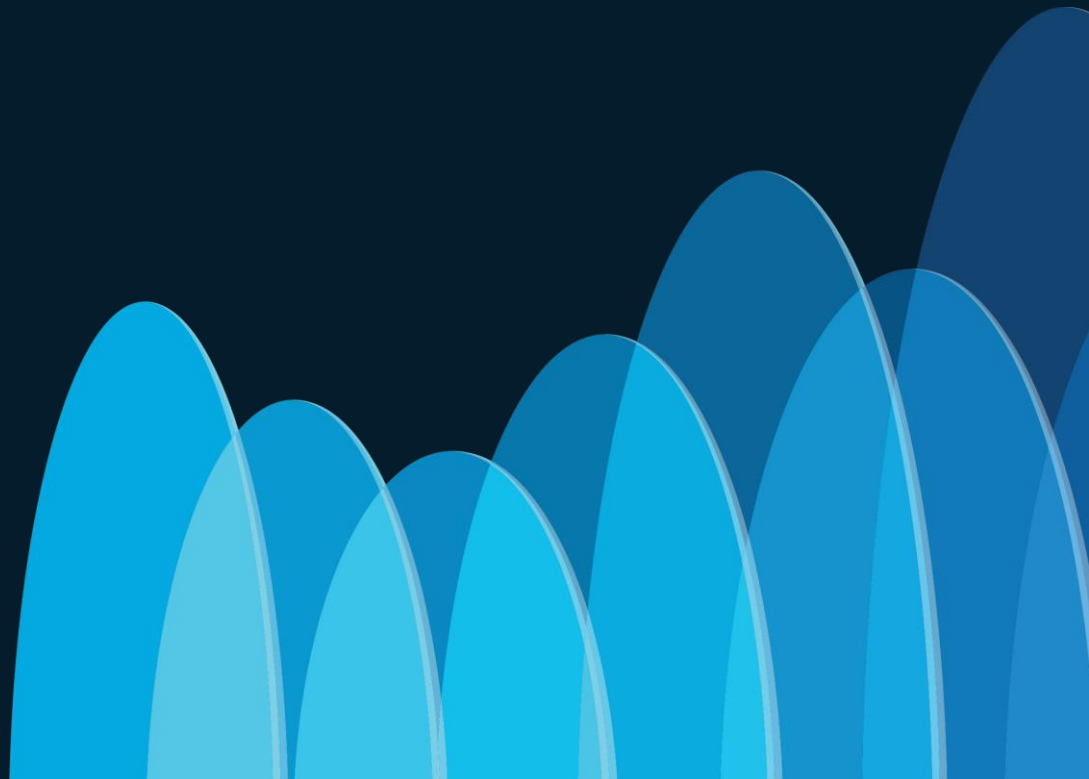
CrowdStrike stated that the problem originated from a single configuration file, which led to a logic error, resulting in system crashes and blue screens of death (BSOD) on Windows systems.

The incident highlights the critical importance of thorough testing and robust incident response strategies.

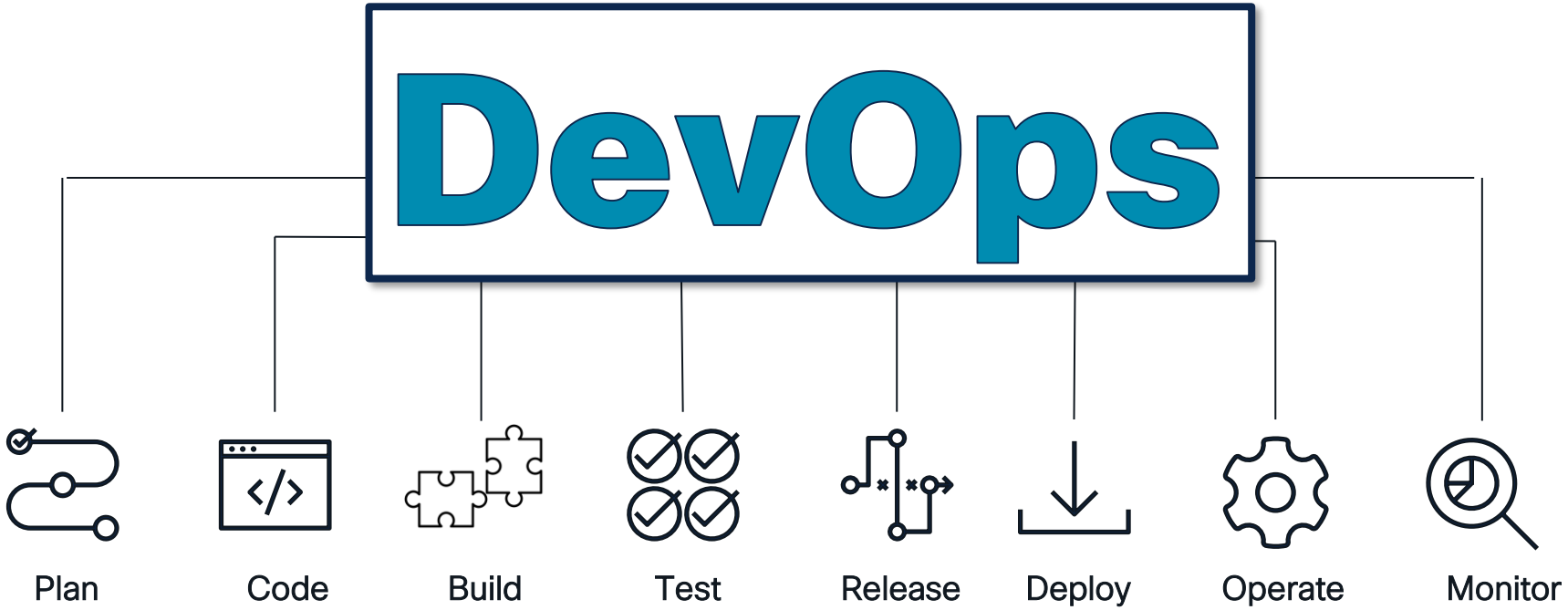
Networks are more complex now than ever before



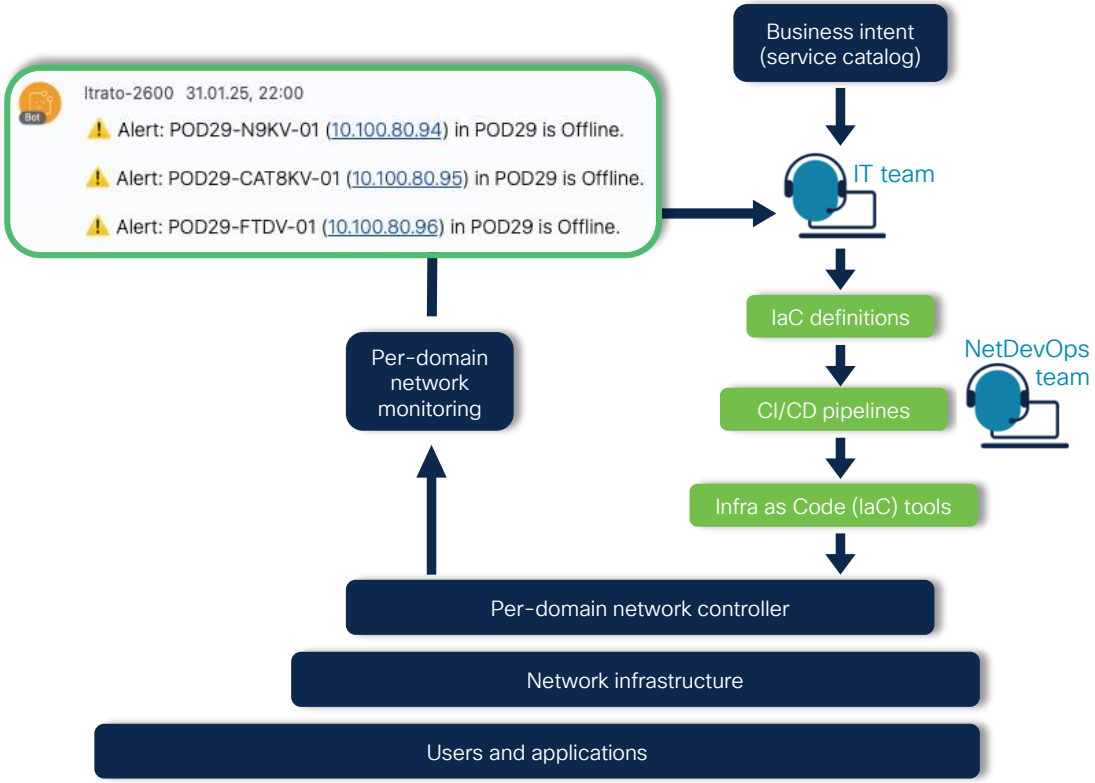
NetDevOps and CI/CD pipelines



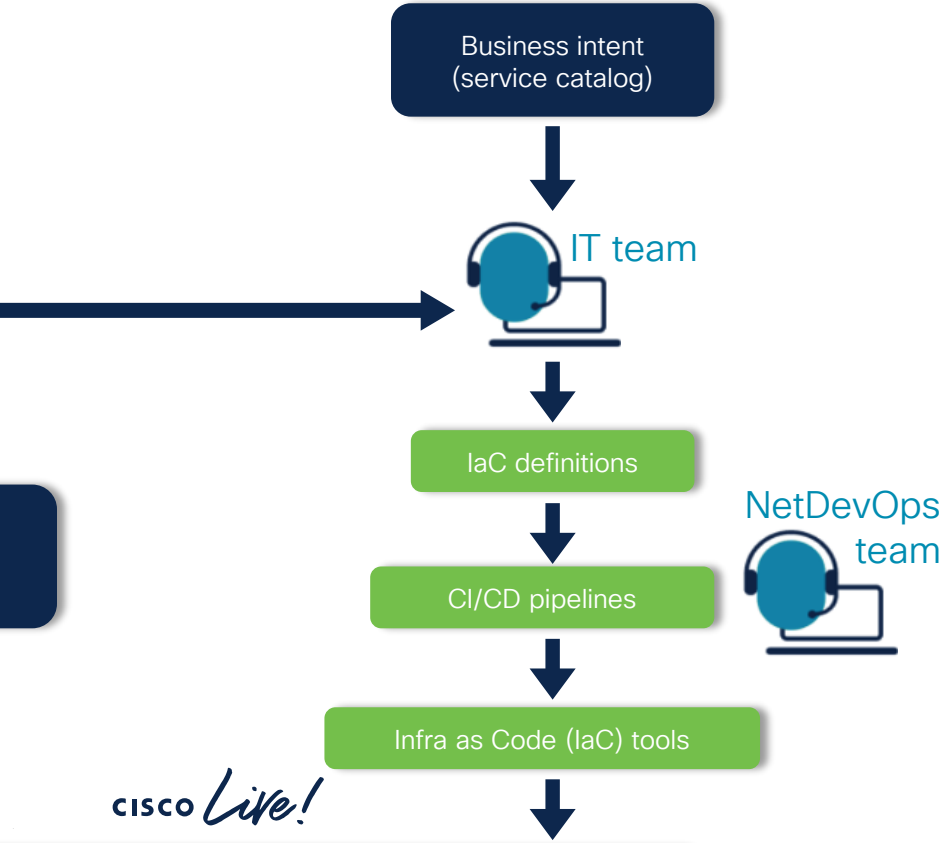
Practice what you preach …



IaC and CI/CD pipelines in automation framework



IaC and CI/CD pipelines in automation framework



Drivers to adopt IaC and NetDevOps are:

- Reduction of human errors through four-eyes principles/review process.
- Network configuration consistency.
- Enablement of changes at scale.
- Historical log of network changes (facilitating both troubleshooting and compliance audit).

IaC definitions

CI/CD pipelines

NetDevOps brings the DevOps practices

Develop

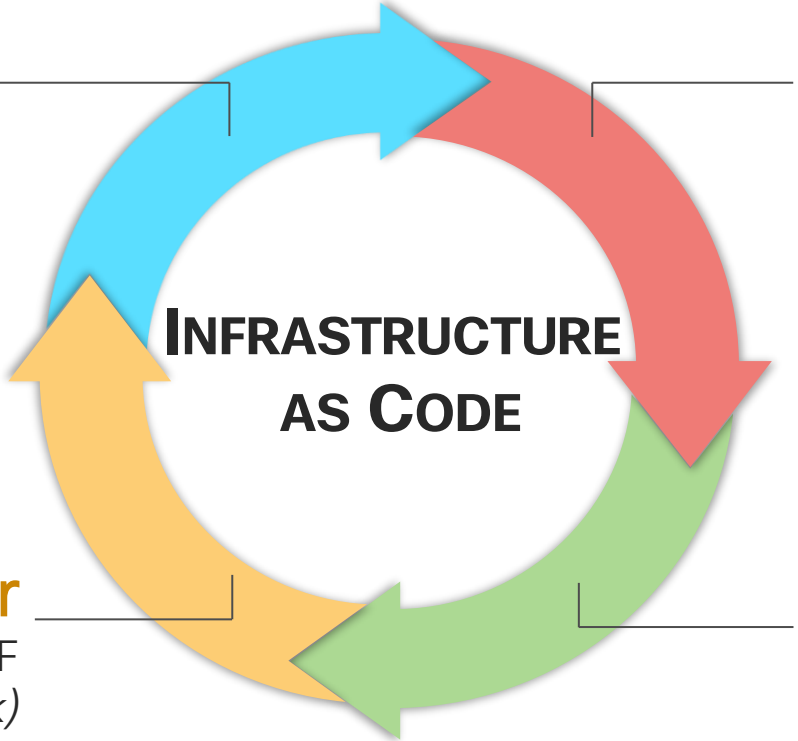
Code + Build = CI

(Continuous Integration)

Test

Test + Release = CD

(Continuous Delivery)



Monitor

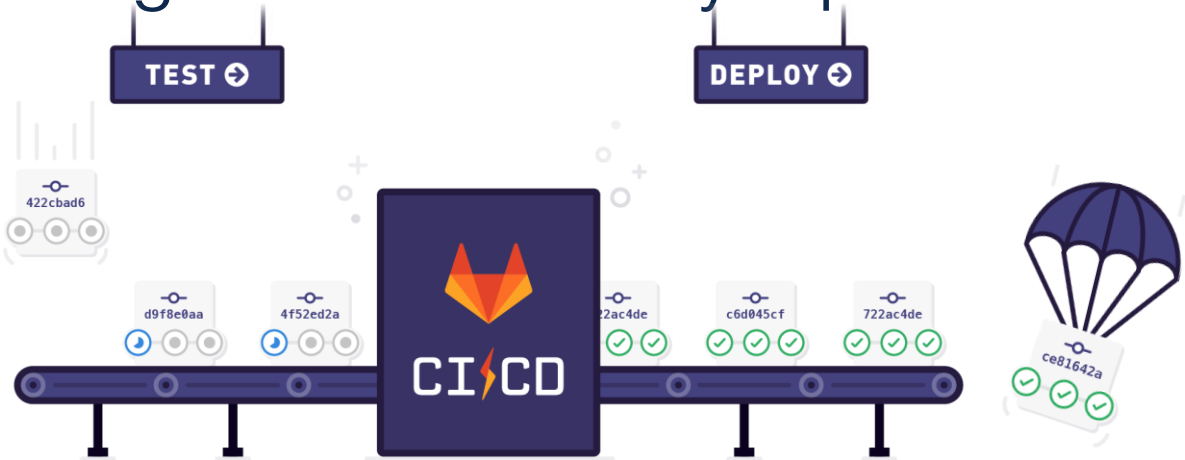
Operate + Monitor = CF

(Continuous Feedback)

Deploy

Continuous Deployment

Continuous Integration & Delivery Pipeline

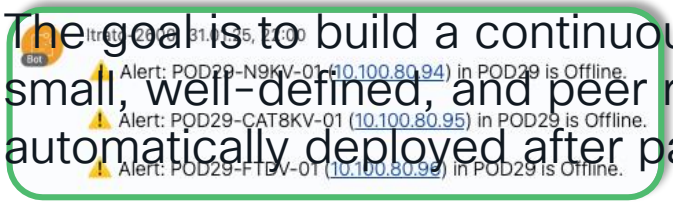


Continuous Integration: Keeping our code (= network configs/templates) in a shared repository, so we can test, collaborate and address conflicts early.

Continuous Delivery / Deployment: We can release new code (= services) often and in an incrementation fashion automatically.

Pipelines are our vehicle to do this in an automated fashion.

A typical pipeline



The goal is to build a continuous process in which small, well-defined, and peer reviewed changes are automatically deployed after passing stringent tests.

Testing & Validation is key!

Build

A **build** stage, with a job called compile.

Staging

A **staging** stage, with a job called deploy-to-stage.

Test

A **test** stage, with two jobs called test1 and test2.

Production

A **production** stage, with a job called deploy-to-prod.

A typical pipeline could consist of four stages.

Gitlab-CI pipeline

Code pushed to GitLab

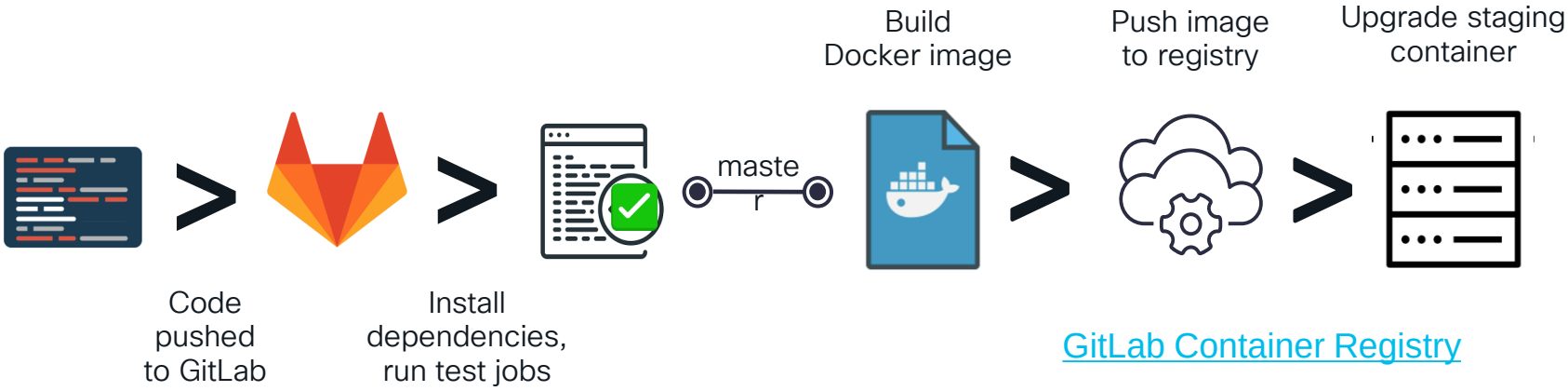
GitLab triggers GitLab Runner

Install dependencies run tests jobs

Docker

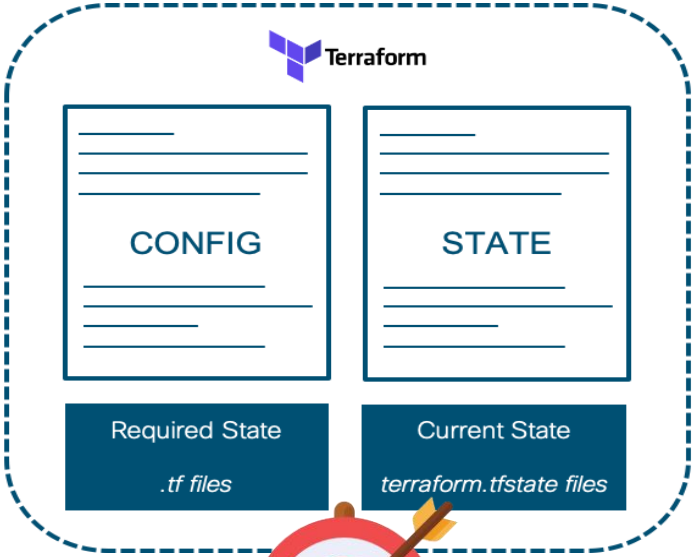
Docker Container allows developers to package their applications and dependencies into a single unit that can run consistently on any infrastructure.

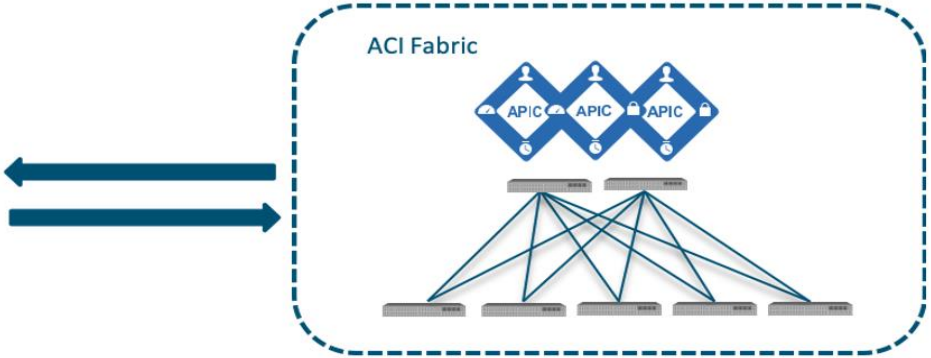
With GitLab's Docker registry, it is possible build and store Docker images directly within GitLab, using GitLab CI/CD pipelines to automate the build and deployment processes.



GitLab Container Registry

Components of Terraform with ACI





DECLARATIVE

.tf files: describe the desired state of the infrastructure that Terraform should create and manage.
Files can either be written in JSON (using the extension .tf.json), or in the *Hashicorp Configuration Language (HCL)* using the extension *`.tf`*.

terraform.tfstate files: are used to track the current state of the infrastructure, and to determine what changes need to be made to bring the infrastructure into the desired state defined in the *`.tf` files.*

Infrastructure as code tools

Attribute	Terraform	Ansible
Tool category	Orchestration	Configuration management
Approach	Immutable infrastructure	Mutable infrastructure
Language	Declarative	Imperative
Provisioning	Specializes in infrastructure provisioning	Limited support for infrastructure provisioning
Lifecycle management	Lifecycle aware. Maintains state of deployments	No lifecycle awareness
Command line operation	Yes	Yes
Agentless	Yes	Yes

Pain Points

Partner and Customer Survey

Where to start?

Organizational silos

Disintegrated tools

No cross-domain skills

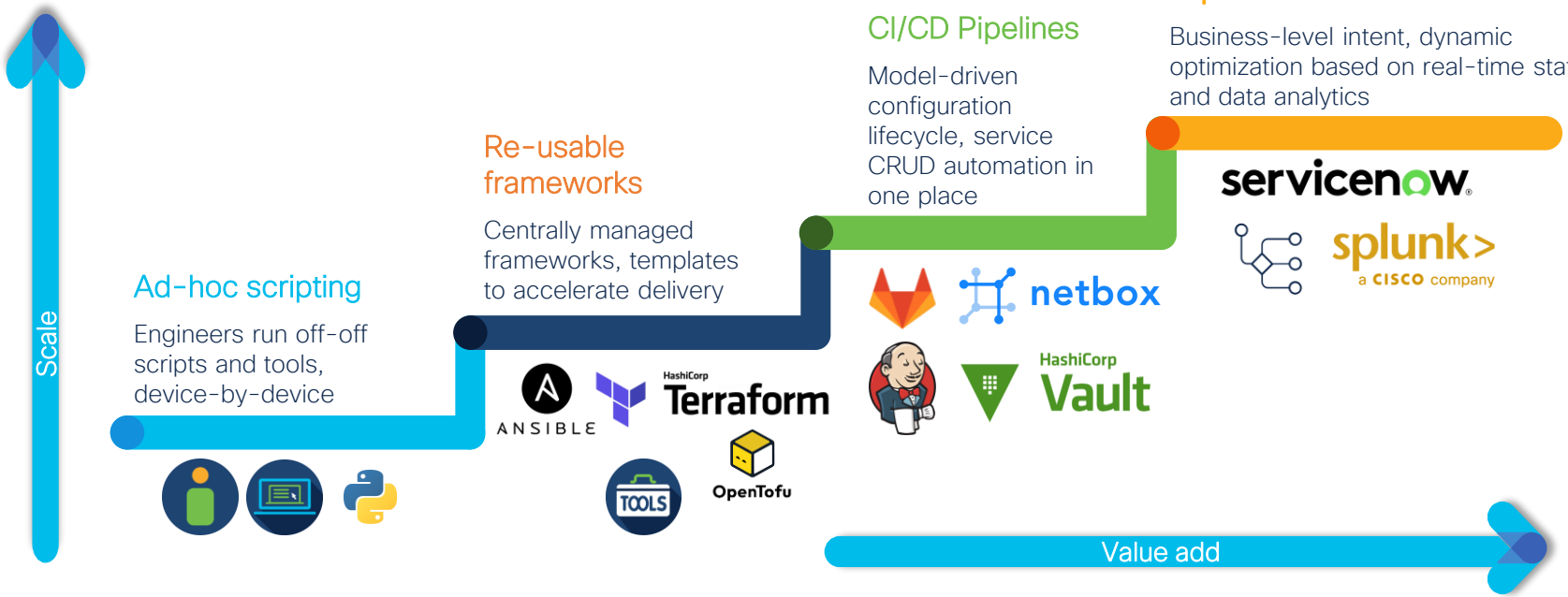
slido

Please download and install the Slido app on all computers you use

What are your painpoints?

ⓘ Start presenting to display the poll results on this slide.

Automation approach in steps

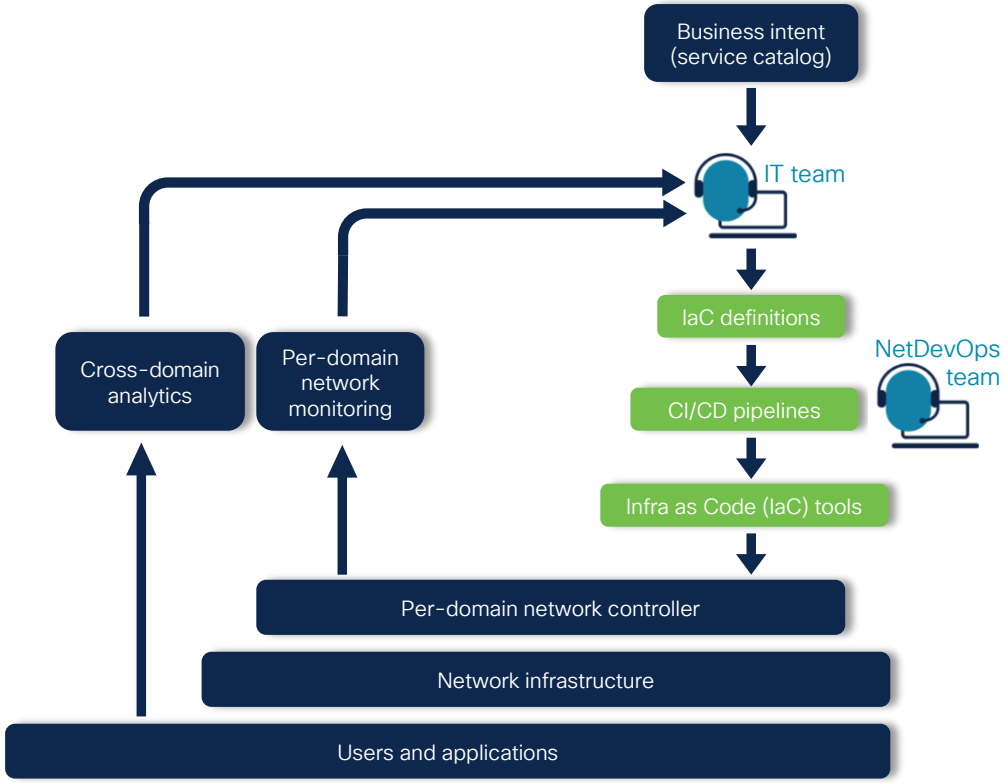


BRKOPS-2814: Transforming network operations with Closed-Loop Automation using AI Insights *Jörg Schultz & Christopher Beye*
LTRATO-2600: Closed-Loop Automation using CI/CD Pipelines with the power of AI *Jörg Schultz & Christopher Beye & Flo Pachinger*
LTROPS-3773: Three Domains in One Pipeline: Cross-Domain Automation with Catalyst Center, FTD, and NDFC using NetDevOps Approaches *Jörg Schultz & Christopher Beye*
LTROPS-2977: Cross-Domain Automation with Cisco DNA Center and ACI using CI/CD Pipelines *Jörg Schultz & Christopher Beye*
BRKEMT-2007: NetDevOps - CI/CD with Cisco DNA Center Templates as Code *Jörg Schultz & Oliver Böhmer*

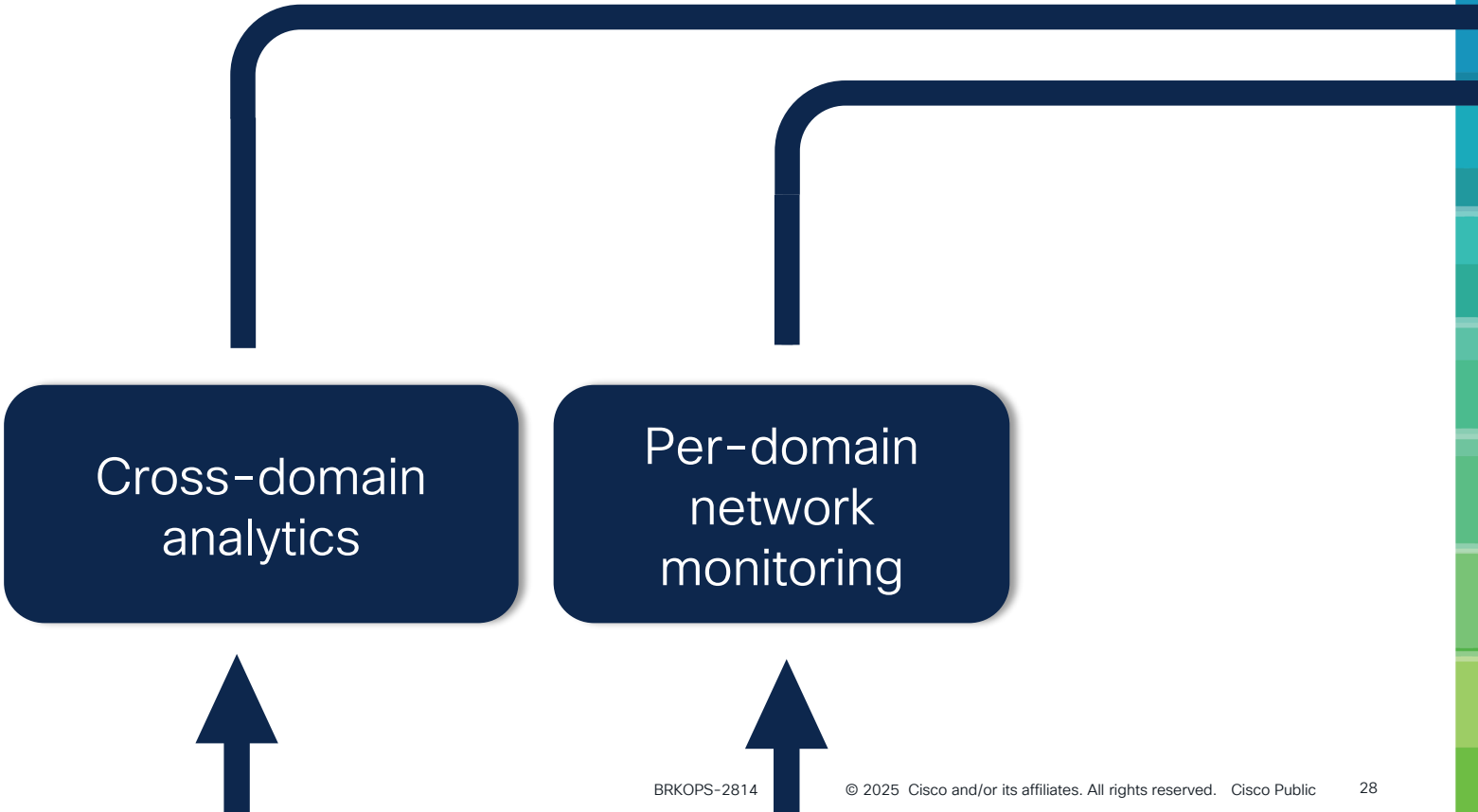
https://crossdomain-automation.tech/

Automate
Tomorrow
Today
Innovate

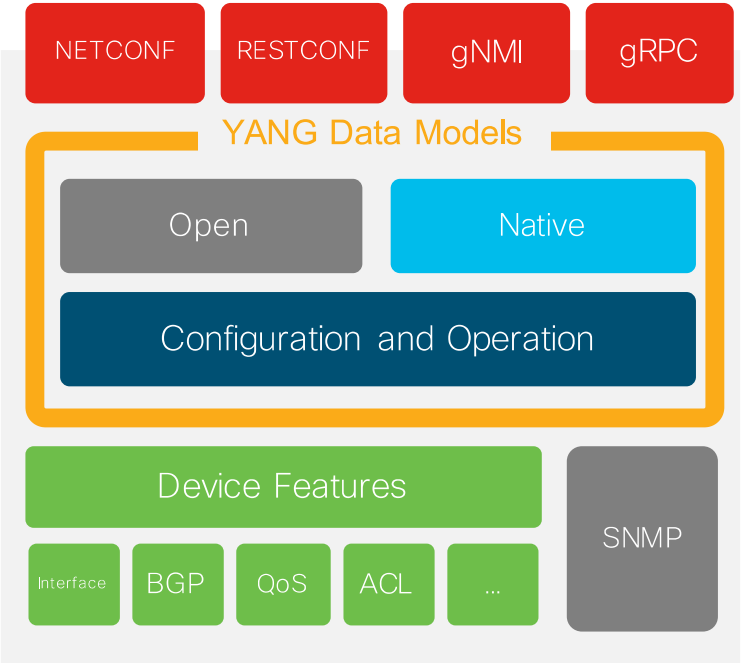
From network monitoring towards analytics

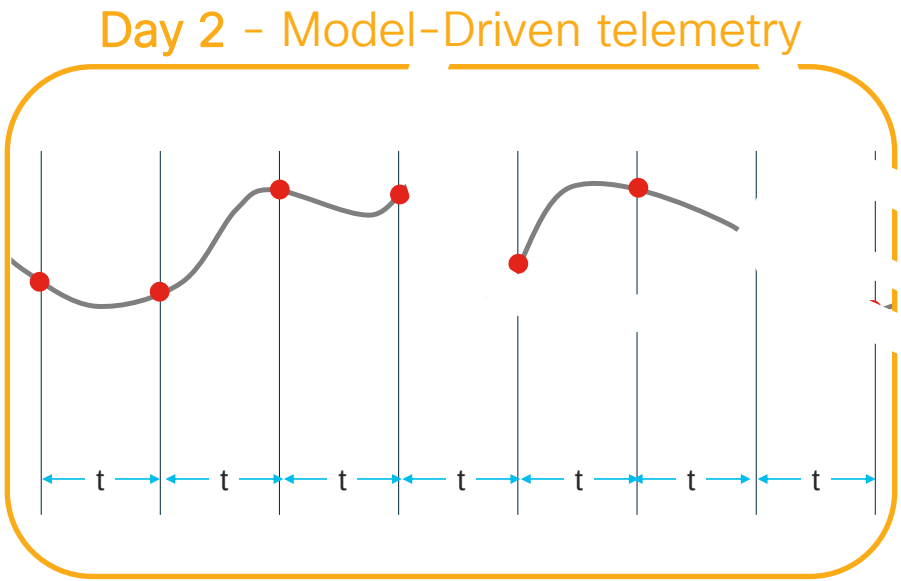


From network monitoring towards analytics



Forever YANG – Network Data Models

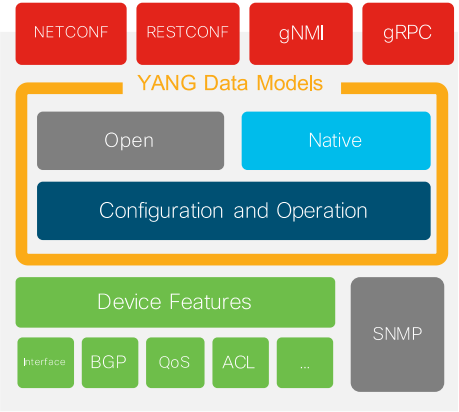


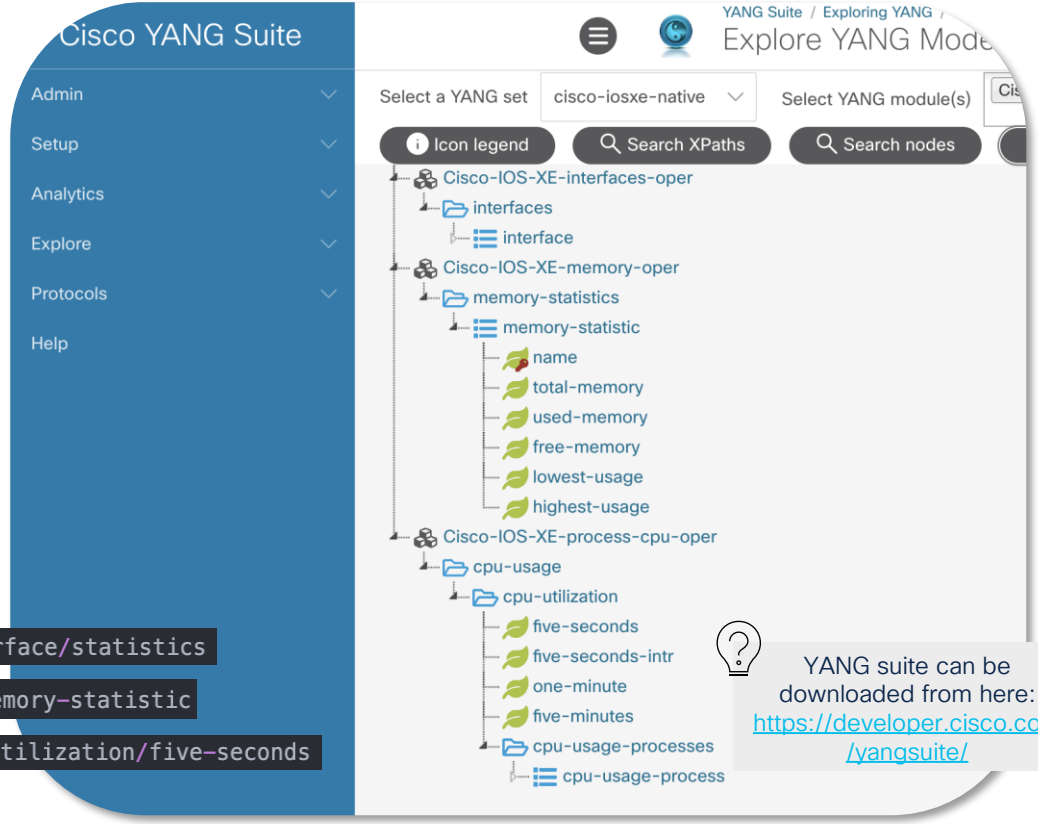


White paper – Catalyst Programmability and Automation

White paper – Model-Driven Telemetry

Forever YANG – Network Data Models



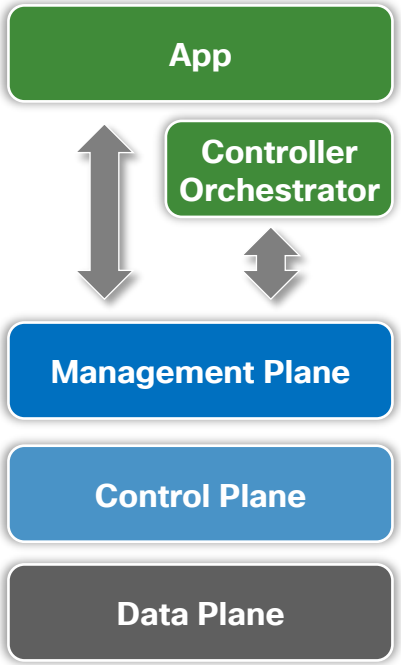


YANG suite can be downloaded from here: https://developer.cisco.com/yangsuite/

<xpath>

```
filter xpath /interfaces-ios-xe-oper:interfaces/interface/statistics
filter xpath /memory-ios-xe-oper:memory-statistics/memory-statistic
filter xpath /process-cpu-ios-xe-oper:cpu-usage/cpu-utilization/five-seconds
```

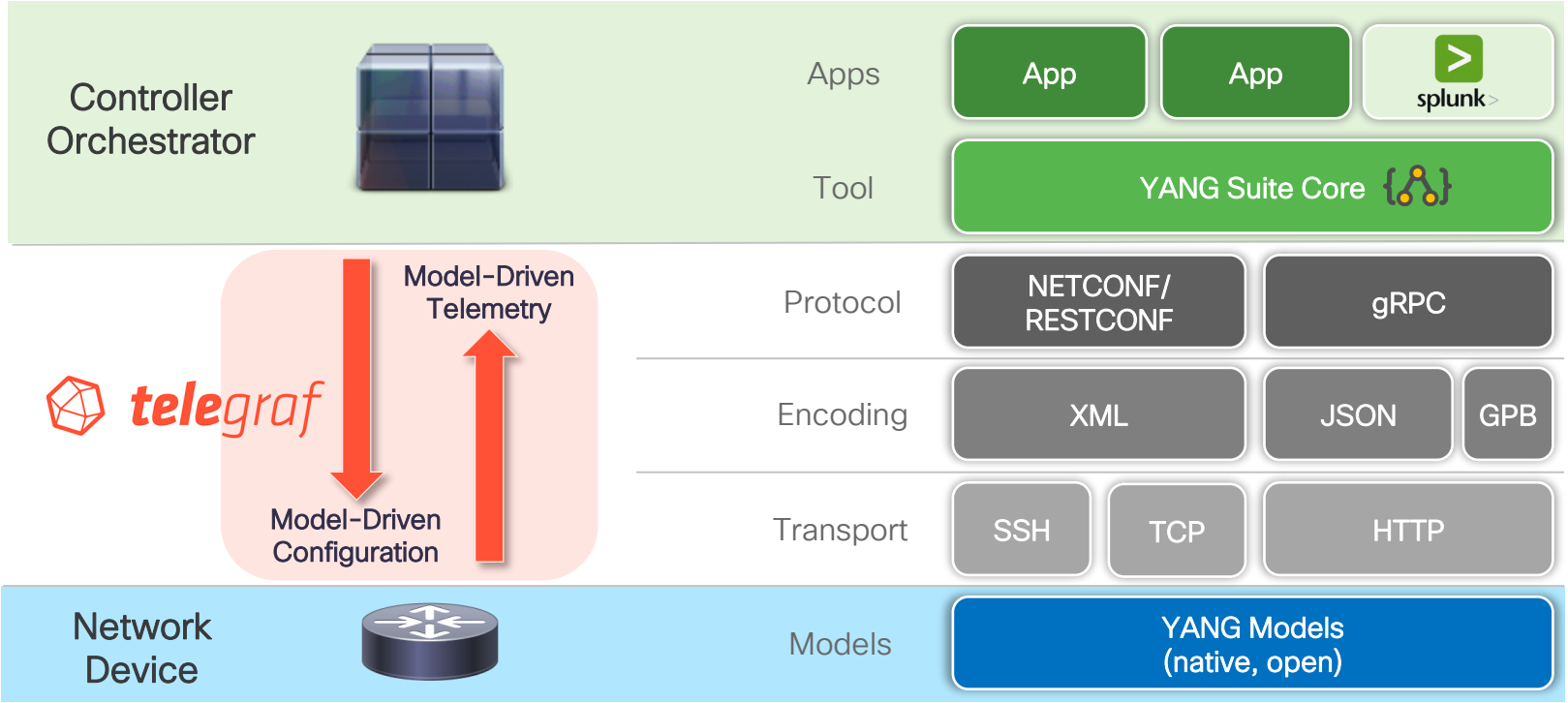
Model-Driven Manageability



https://developer.cisco.com/yangsuite

https://github.com/influxdata/telegraf/tree/master/plugins/inputs/cisco_telemetry_mdt

Model-Driven Manageability



https://developer.cisco.com/yangsuite

https://github.com/influxdata/telegraf/tree/master/plugins/inputs/cisco_telemetry_mdt

Model-Driven Manageability

Inputs MDT

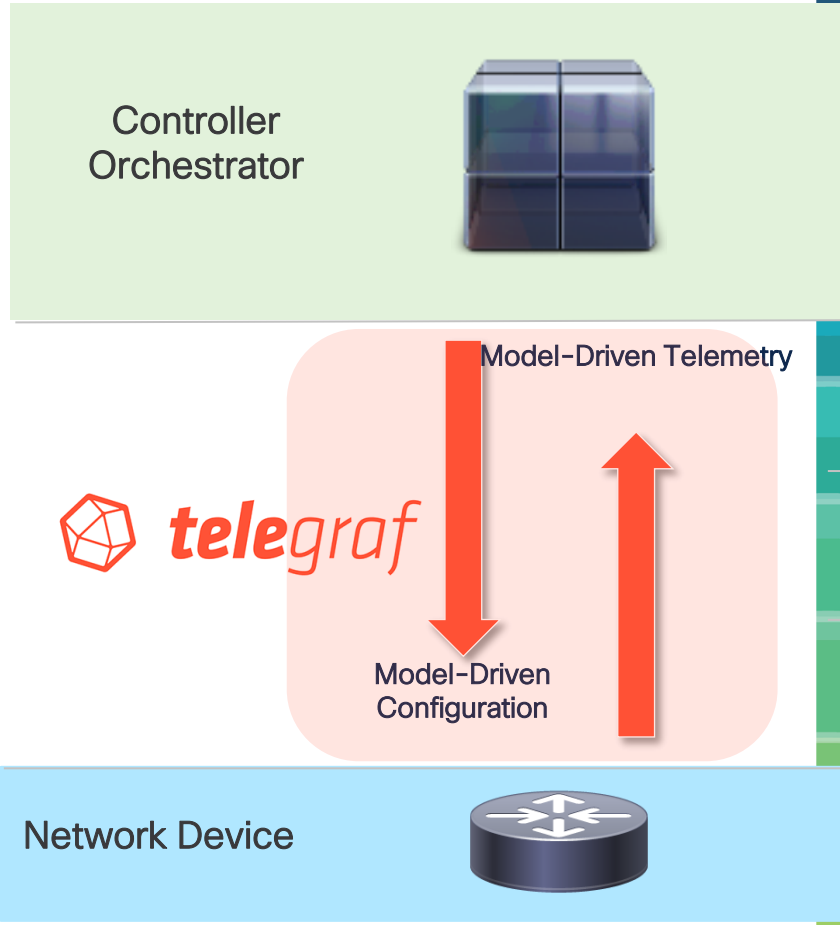
```
[[inputs.cisco_telemetry_mdt]]
 ## Telemetry transport can be "tcp" or "grpc".
 ## TLS is only supported when
 ## using the grpc transport.
 transport = "grpc"

 ## Address and port to host telemetry listener
 service_address = ":57400"

 ## Grpc Maximum Message Size, default is 4MB, increase the size.
 ## This is stored as a uint32, and limited to 4294967295.
 max_msg_size = 4000000
```

NX-OS

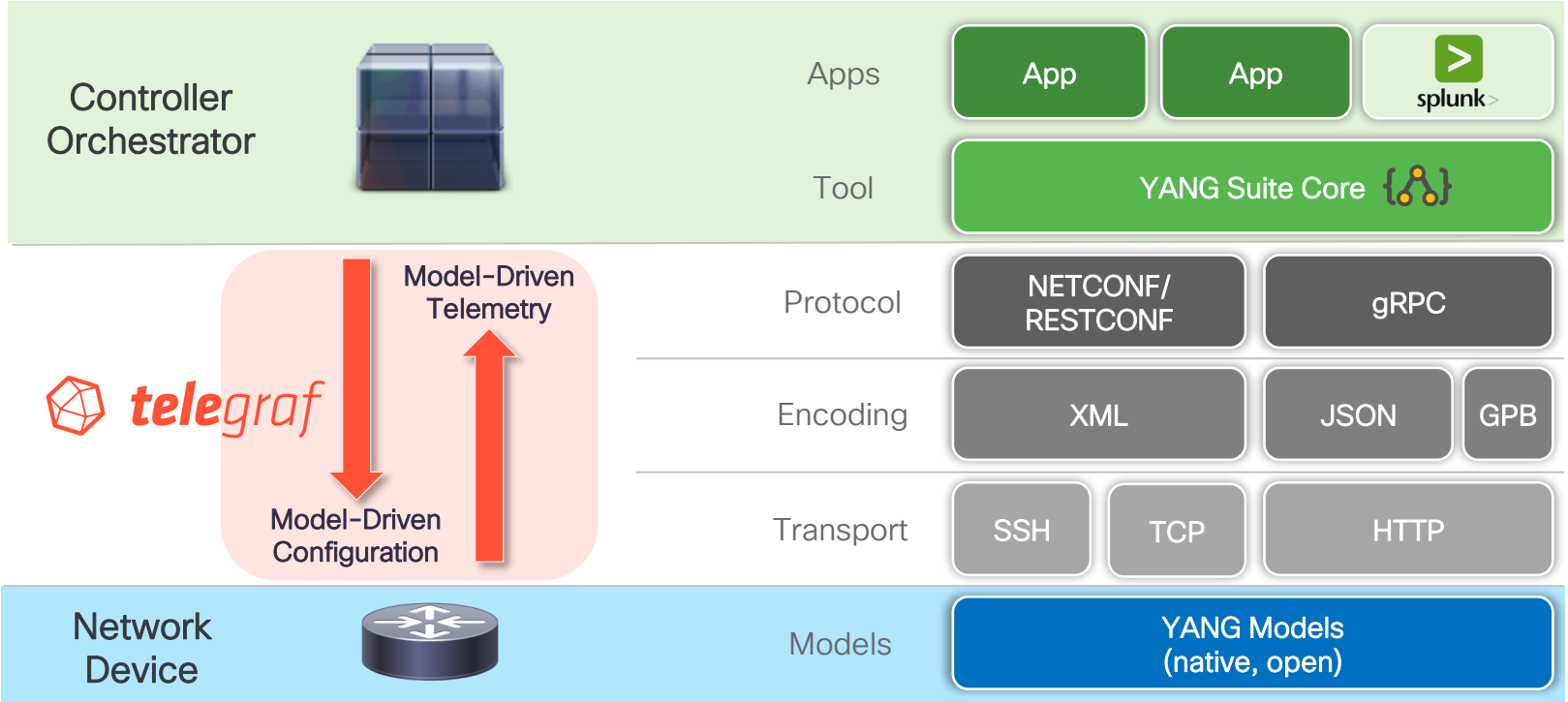
```
telemetry
  destination-group 10
    ip address 10.x.x.x port 57400 protocol gRPC encoding GPB
  sensor-group 10
    data-source YANG
    path openconfig-interfaces:interfaces/interface/state/counters
  subscription 10
    dst-grp 10
    snsr-grp 10 sample-interval 5000
```

IOS XE

```
telemetry ietf subscription 102
 encoding encode-kvgpb
 filter xpath /interfaces-ios-xe-oper:interfaces/interface/statistics
 stream yang-push
 source-address 10.x.x.x
 update-policy periodic 5000
 receiver ip address 10.x.x.x 57400 protocol grpc-tcp
```



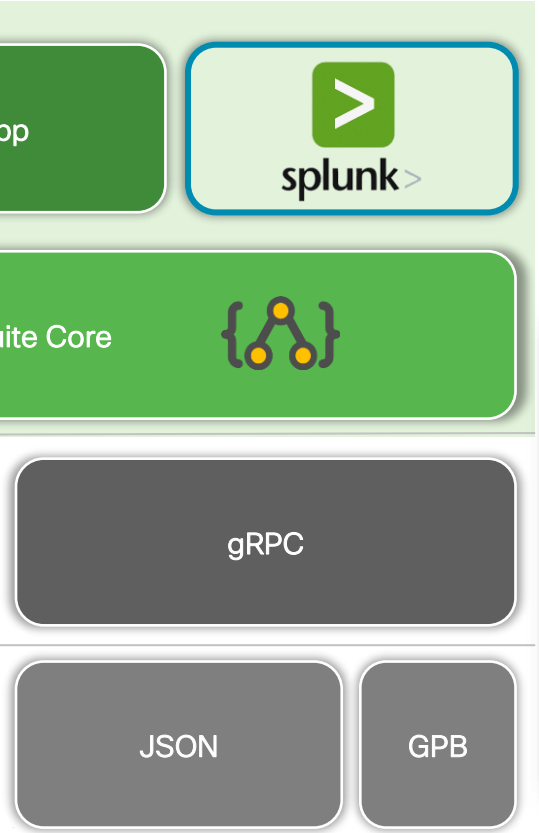
Model-Driven Manageability



https://developer.cisco.com/yangsuite

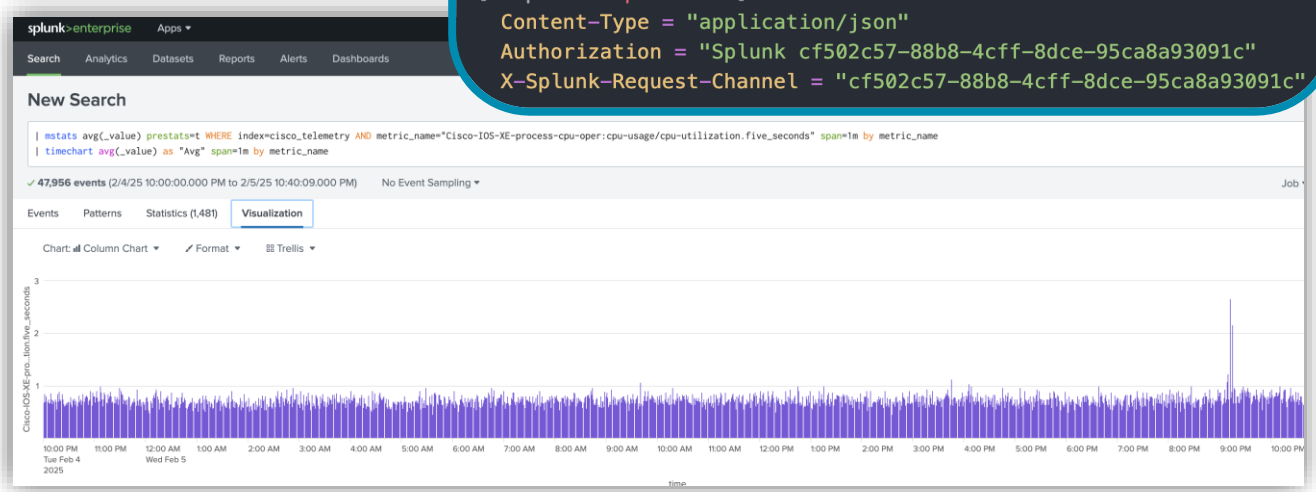
https://github.com/influxdata/telegraf/tree/master/plugins/inputs/cisco_telemetry_mdt

Model-Driven Manageability



Output plugin Telegraf to Splunk

```
# Splunk HTTP Event Collector (HEC) Output Plugin
[[outputs.http]]
  url = "https://10.x.x.x:8088/services/collector"
  data_format = "splunkmetric"
  insecure_skip_verify = true
  splunkmetric_hec_routing = true
  splunkmetric_multimetric = false
  splunkmetric_omit_event_tag = true

# Splunk HEC Token
[outputs.http.headers]
  Content-Type = "application/json"
  Authorization = "Splunk cf502c57-88b8-4cff-8dce-95ca8a93091c"
  X-Splunk-Request-Channel = "cf502c57-88b8-4cff-8dce-95ca8a93091c"
```



Splunk – Customized Dashboard

splunk>enterprise Apps ▾ Joerg Schultz ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

Cisco LIVE EMEA25 Dashboard

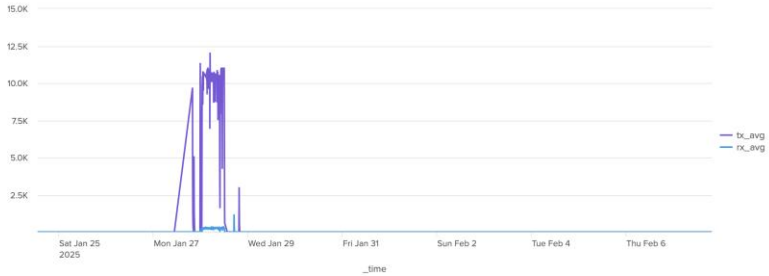
Display ▾ Actions ▾ Edit

Global Time Range

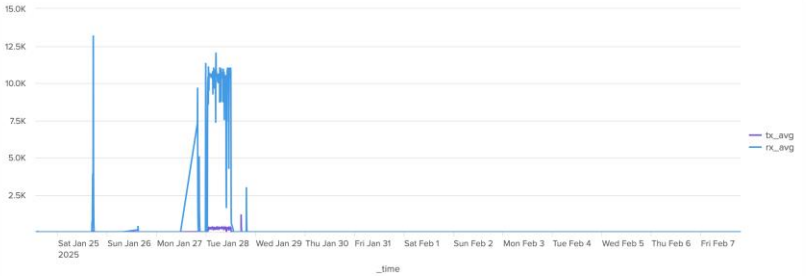
All time

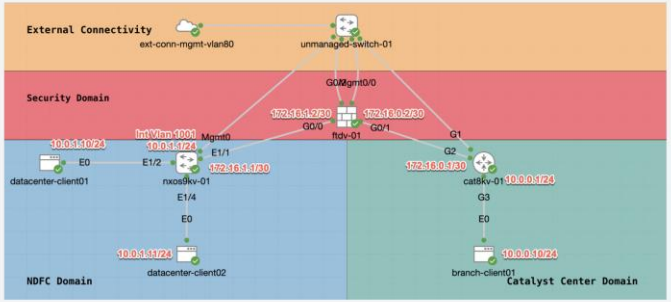
Cat8000V-0 New tab

Transmitted Packets GigabitEthernet2 (to FTD)

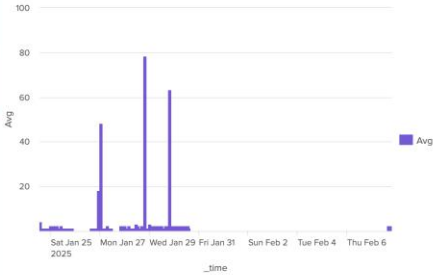


Transmitted Packets GigabitEthernet3 (to Client)

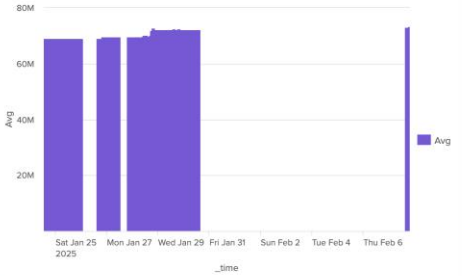




CPU Usage 5s



Memory Usage



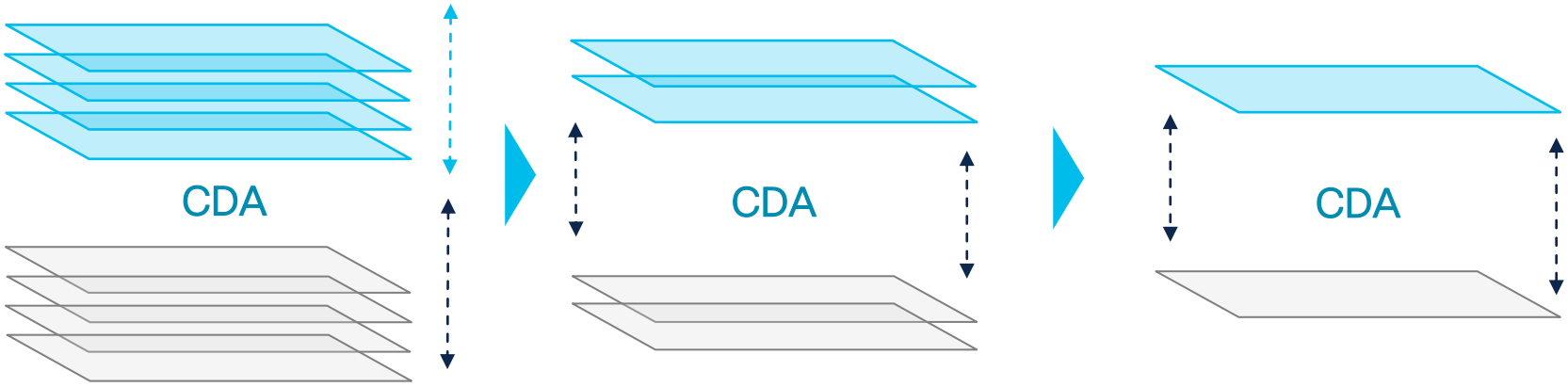
Let's talk Cross-Domain (Automation)

Convergence is the key to the future

Multiple cloud platforms

Fewer cloud platforms

Single cloud platform



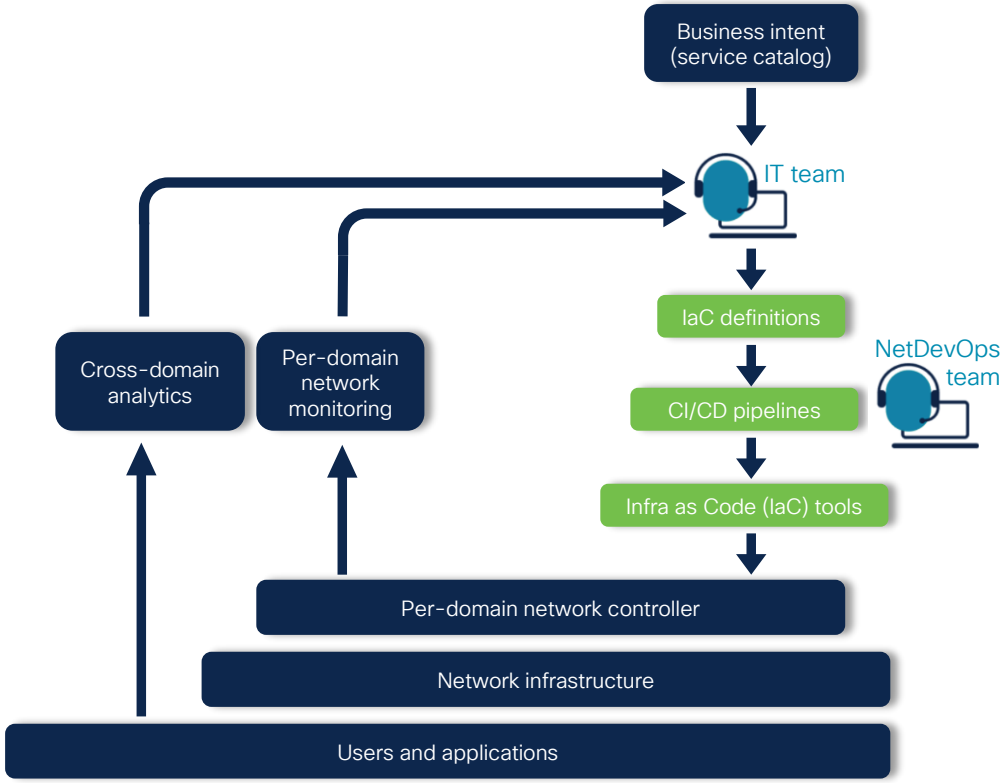
Multiple on-prem platforms

Fewer on-prem platforms

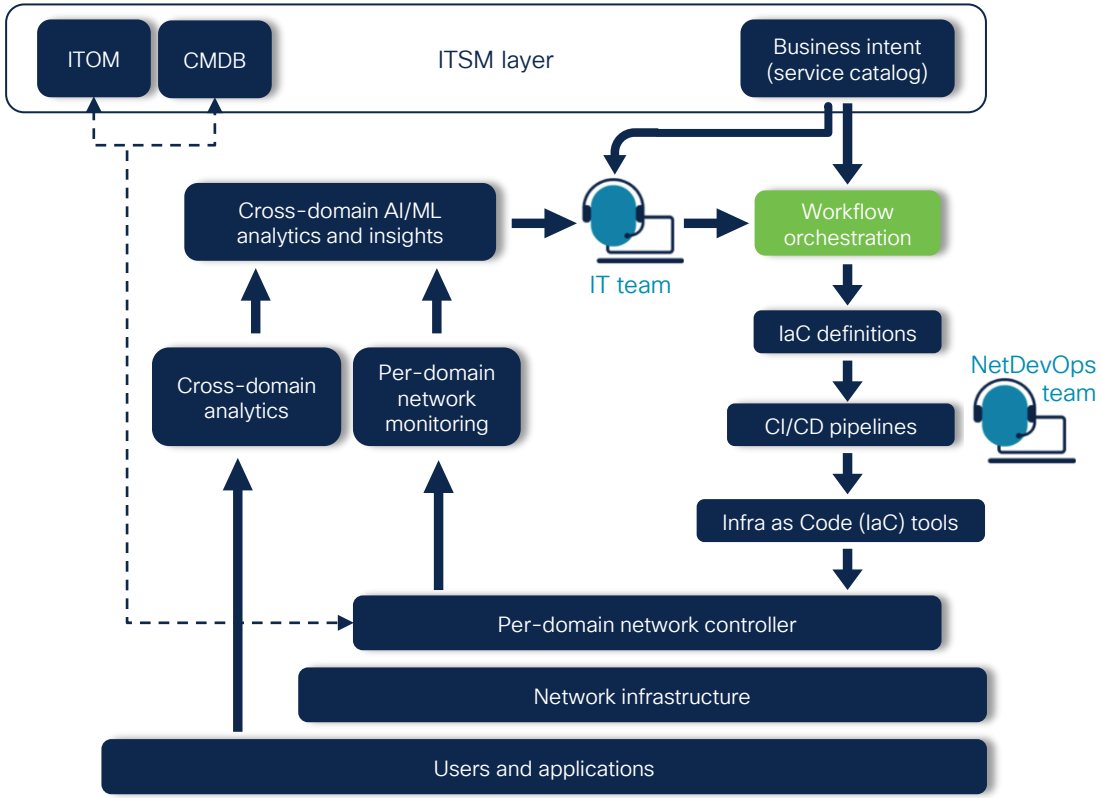
Single on-prem platform

CDA = Cross-Domain Automation

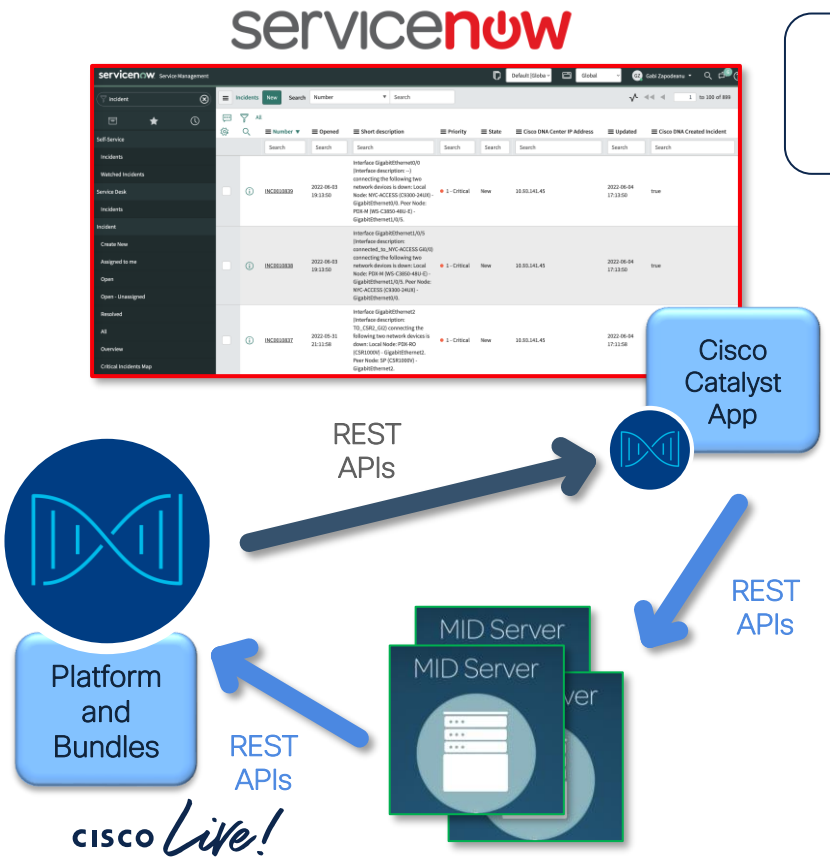
From network monitoring towards analytics

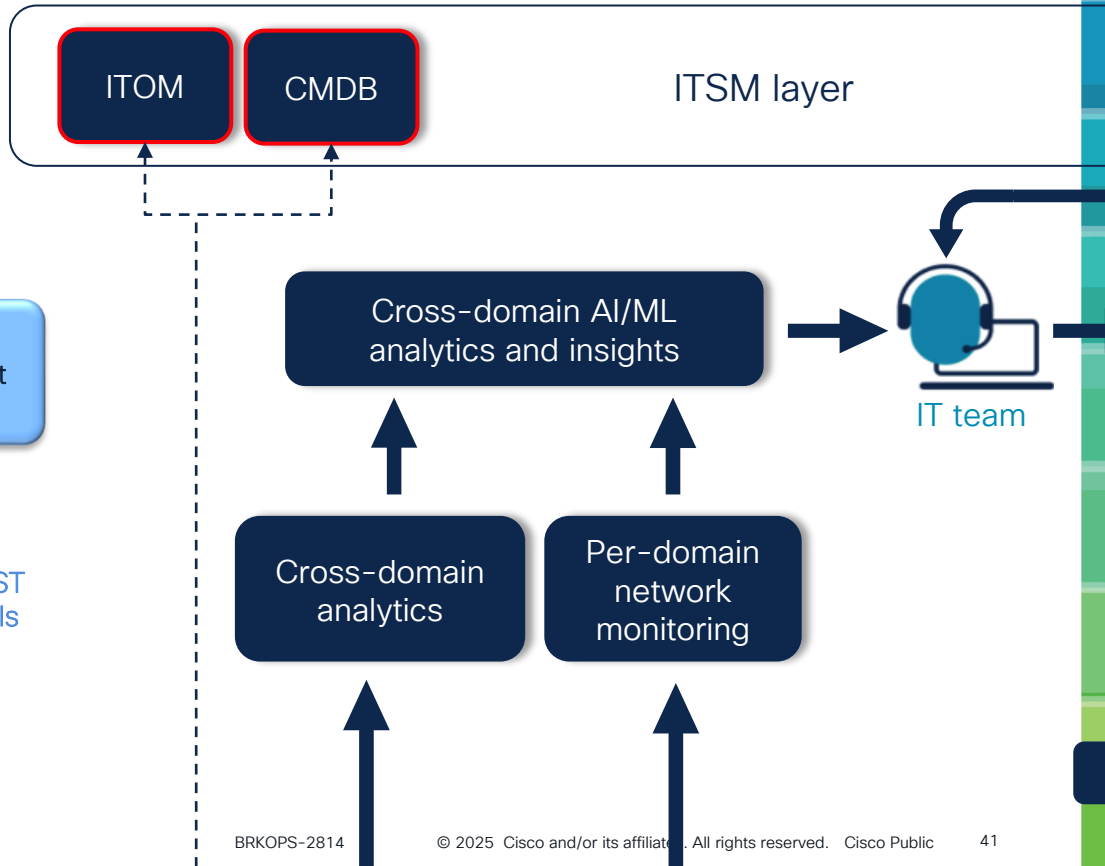


Cross-domain workflow orchestration



Cross-domain workflow orchestration



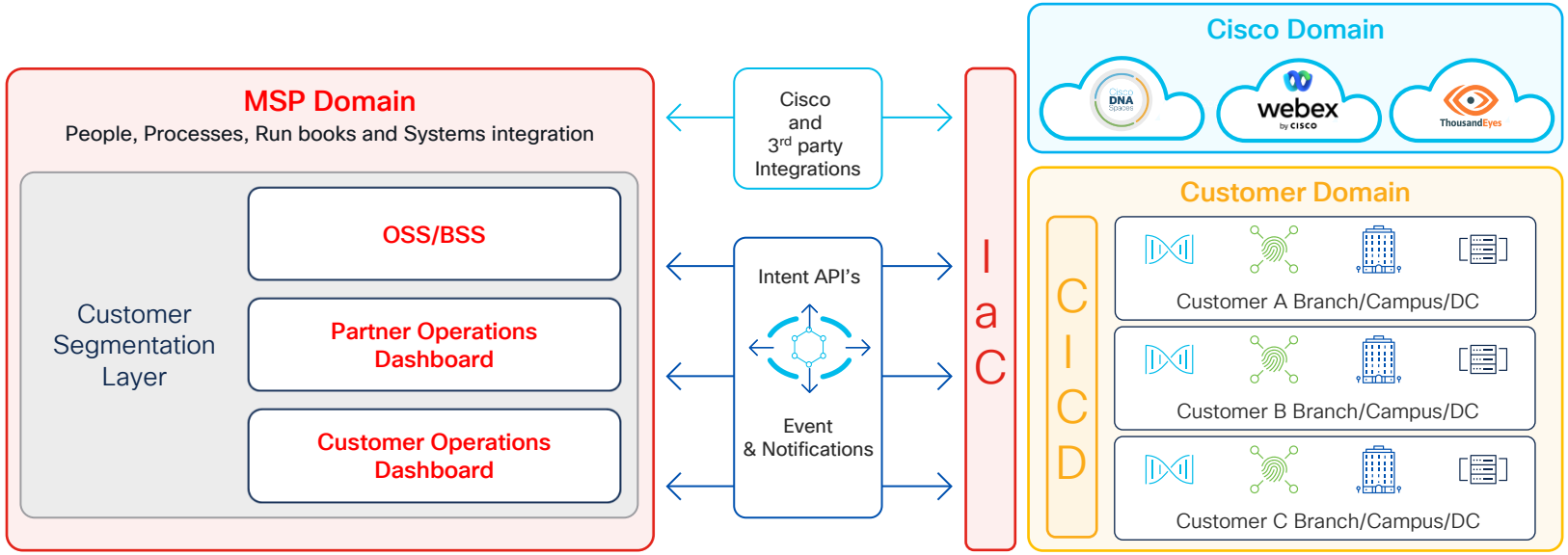


Workflow Automation

Workflow automation is the approach to automating various **business processes**, **tasks** and **workflows** in a company with minimal human intervention. Workflow automation leverages software to create a series of **automated actions** for the steps in a business process, which helps teams execute tasks efficiently and consistently.

Managed Campus: scaling to multiple customers

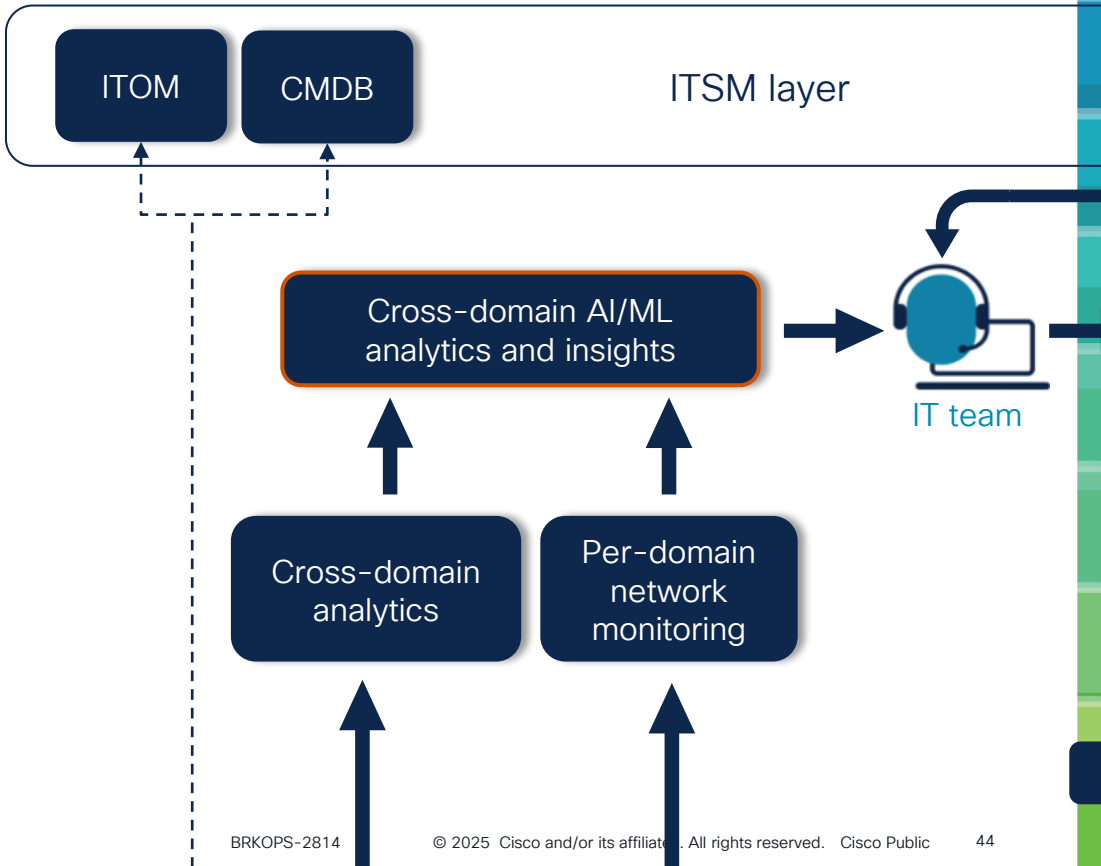
Enabling MSPs to create and support Catalyst Center Services at scale



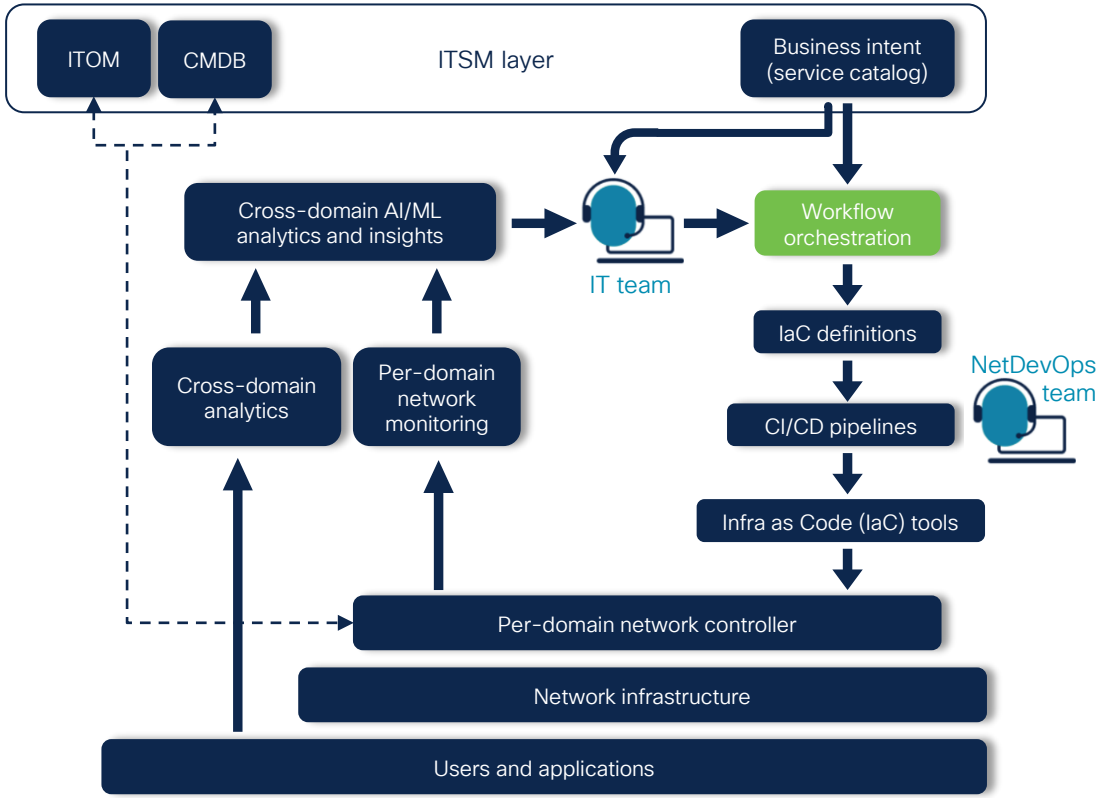
Managed Service (Provider) Dashboard

Cross-domain workflow orchestration

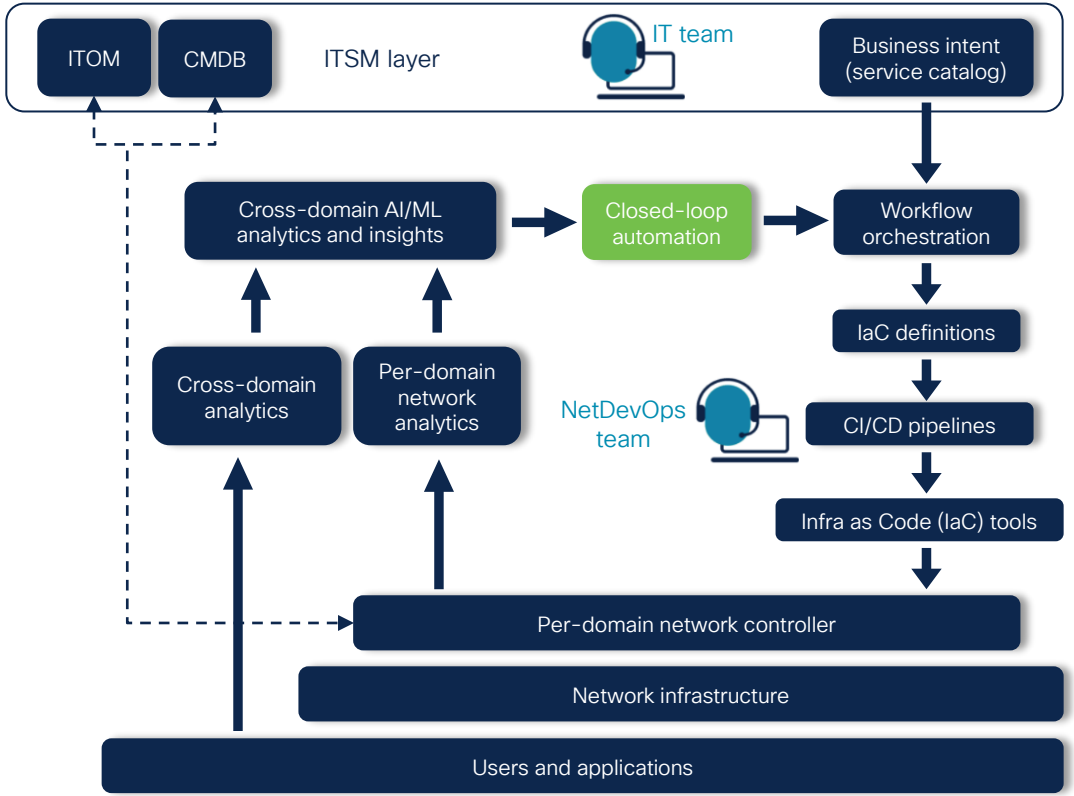
Splunk MLTK and Smart Outlier Detection Assistant Process and Workflow



Cross-domain workflow orchestration



Closed-loop automation



Benefits of **closed-loop automation** are:

- Augmented network reliability through AIOps.
- Automated fault recovery, reducing downtime and business impact of network outages.
- Incident resolution time is reduced, increasing customer experience.
- Reduction of operational cost by reduction of required manual tasks.
- Increases the benefits of IaC and CI/CD.

Use case implementation

Lab layers

servicenow

Cross-domain analytics

Orchestration

netbox

Controller

NDFC

cisco

Security Cloud Control

splunk>

Device level

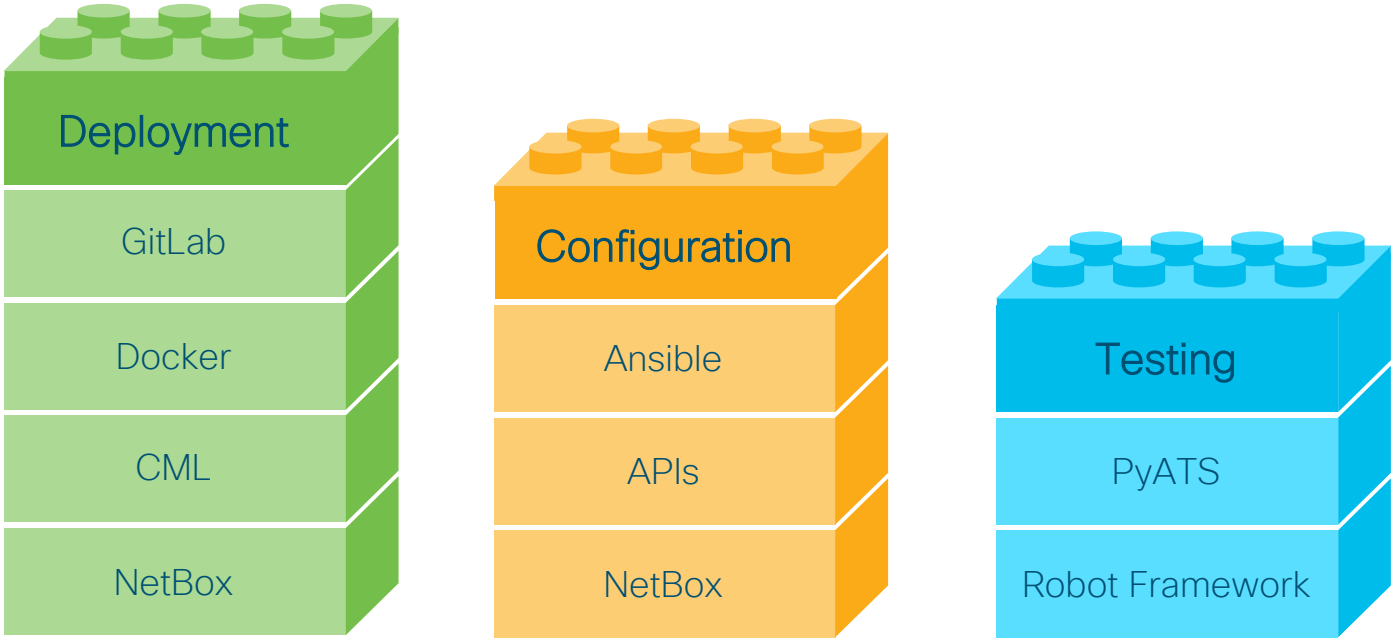
Nexus 9000V

FTDv

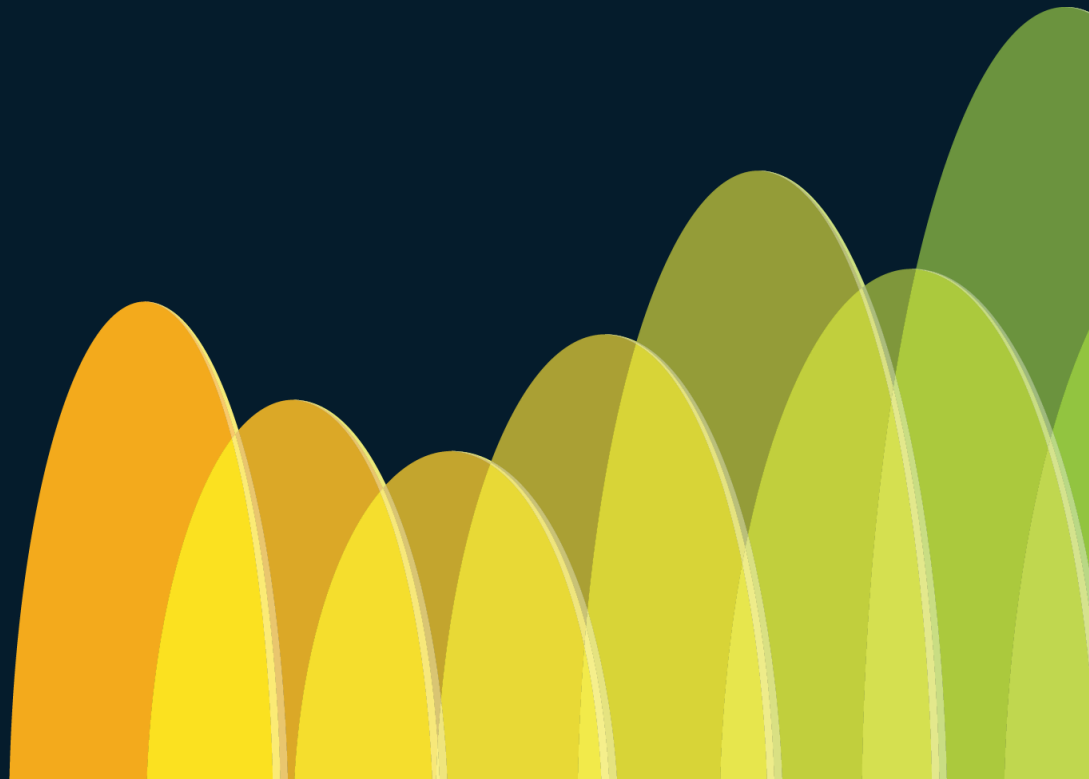
Catalyst 8000V

telegraf

Lab tool bricks



Cross-domain automation



cisco Live!

What is a Network Source of Truth (NSoT)?

- Defines the *intended* state of the network represented as *structured data*
- Should act as a single consistent data set
- Adopting an NSoT requires a significant mental shift for network engineers away from describing the network in design documents and diagrams
- NSoT becomes the authoritative reference for the network and its data *drives network automation*

Inventory

DCIM

IPAM

Configuration

Network Properties

Circuits

netbox labs

The journey to network automation starts with implementing a NSoT

Document

- Converge legacy sources of truth
- Discovery or manual capture of additional network data
- Change operational processes to start with documentation

1

Model

- Connect network data through cohesive models
- Enforce consistency across models

2

Automate

- Implement change management starting with NSoT/ intent
- Generate configs from model data
- Drive automations from dynamic inventory
- Assurance to identify/resolve operational drift

3

Only 28% of organizations have fully executed their network automation strategy.*

72% of organizations are within these two phases.*

netbox labs

We Make it Easier to Build and Manage Complex Networks

Why Use HashiCorp Vault for Network Automation?

- Centralized Secret Management – Stores and manages network credentials, API keys, SSH keys, and certificates securely
- Granular Access Control – Uses RBAC and policies to control who can access what credentials
- APIs for Automation – Fully API-driven, allowing easy integration into CI/CD pipelines
- Eliminates hardcoded credentials in automation scripts
- Enables compliance with security frameworks like ISO 27001, NIST, and CIS

CML – Cisco Modeling Labs

Browser-based, point-and-click network design, config, testing, troubleshooting

Fast setup and tear-down saves you time in the day-to-day work

Seamless connectivity with physical networks and other simulations

Ships with Cisco images and open-source images

API-first approach

Labs are persistent between sessions

Fully programmable network simulation and testing

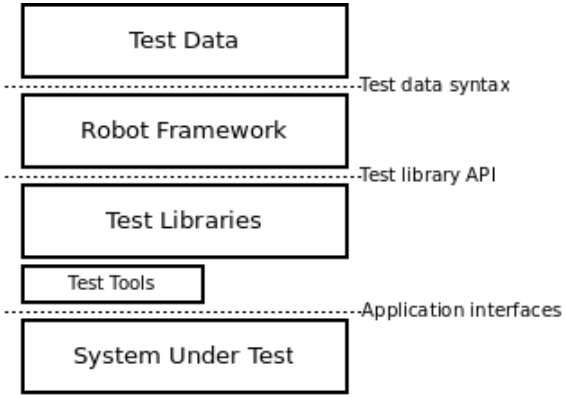
Validation and Test is critical for automation

Robot Framework:

- It is a generic, application and technology independent framework.
- A modular architecture that can be extended with bundled and self-made test libraries.
- Keyword-driven test automation framework.

pyATS:

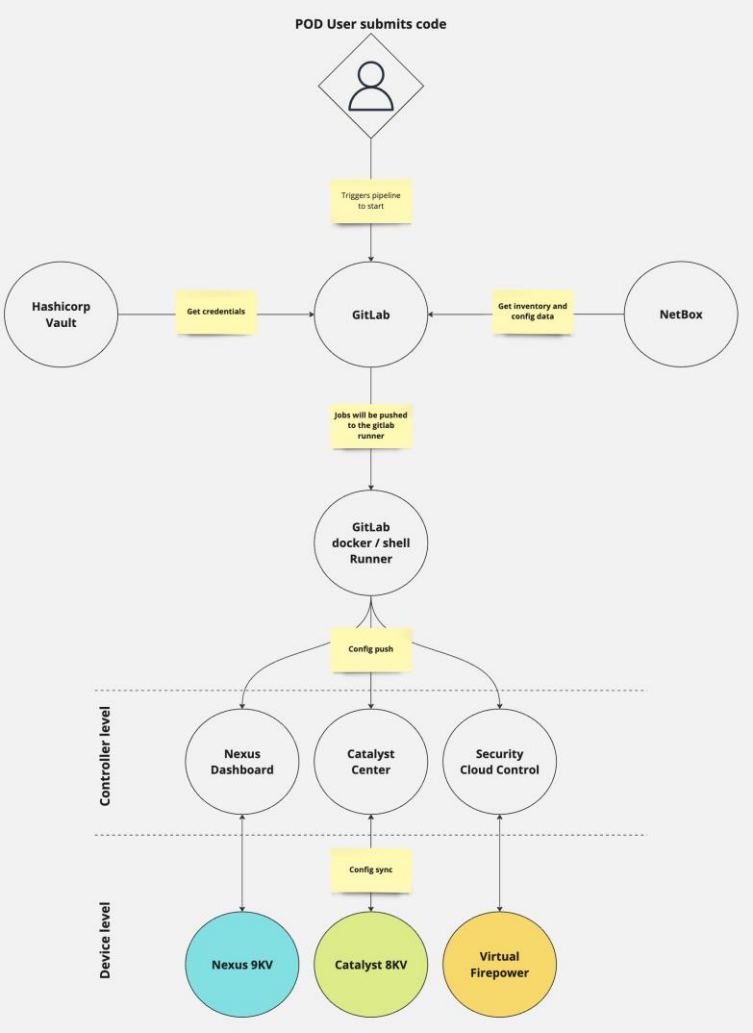
- The core of pyATS is vendor, platform, feature, and protocol agnostic.
- Genie: the standard pyATS network device library.



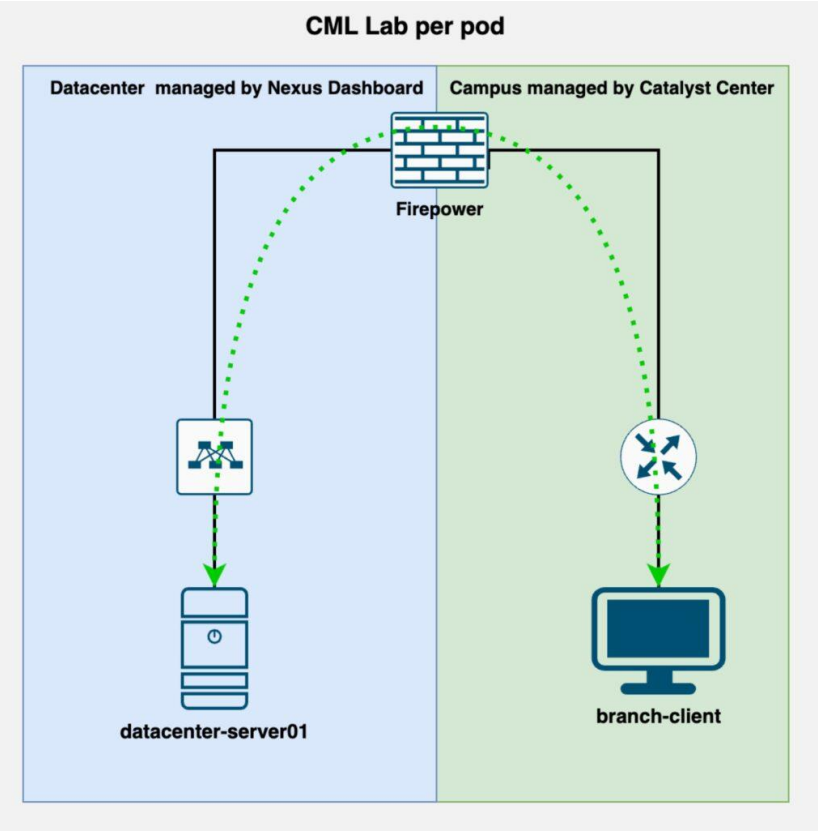
pyATS
print("Hello, CISCO!")

Cross-domain automation

- End-to-End Automation: GitLab pipeline automates config changes across branch, data center, and security domains
- Secure Access: Credentials are securely managed via HashiCorp Vault
- Accurate Configs: NetBox ensures correct device and interface updates
- Automated Execution: GitLab runner deploys configs to network controllers
- Verification: Automated tests confirm connectivity and rule enforcement



Cross-domain automation

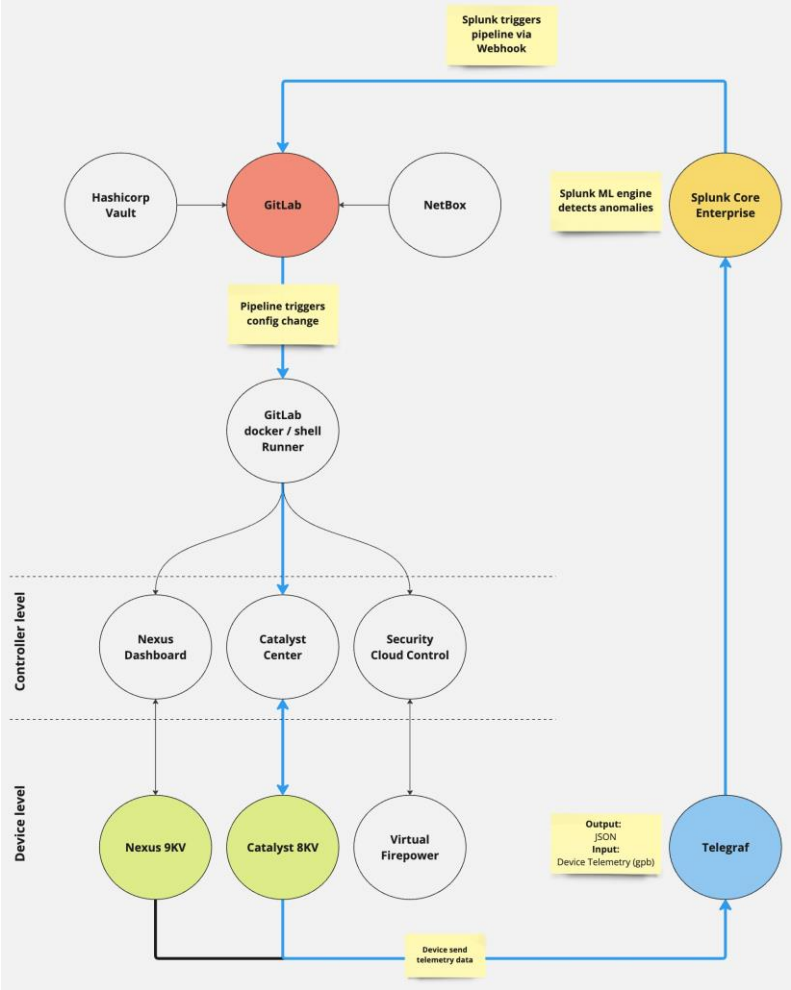


Demo time

Closed-loop automation

Process overview

- Telemetry Collection: Nexus 9KV and Catalyst 8KV send telemetry data to Telegraf.
- Trigger Response: Telegraf forwards data to Splunk for rule-based actions.
- Automated Response: Splunk triggers GitLab pipeline via Webhook for config changes.
- Config Deployment: GitLab runner applies fixes to controllers, e.g. Catalyst Center.
- Continuous Feedback: Ensures stability by automating corrective actions.

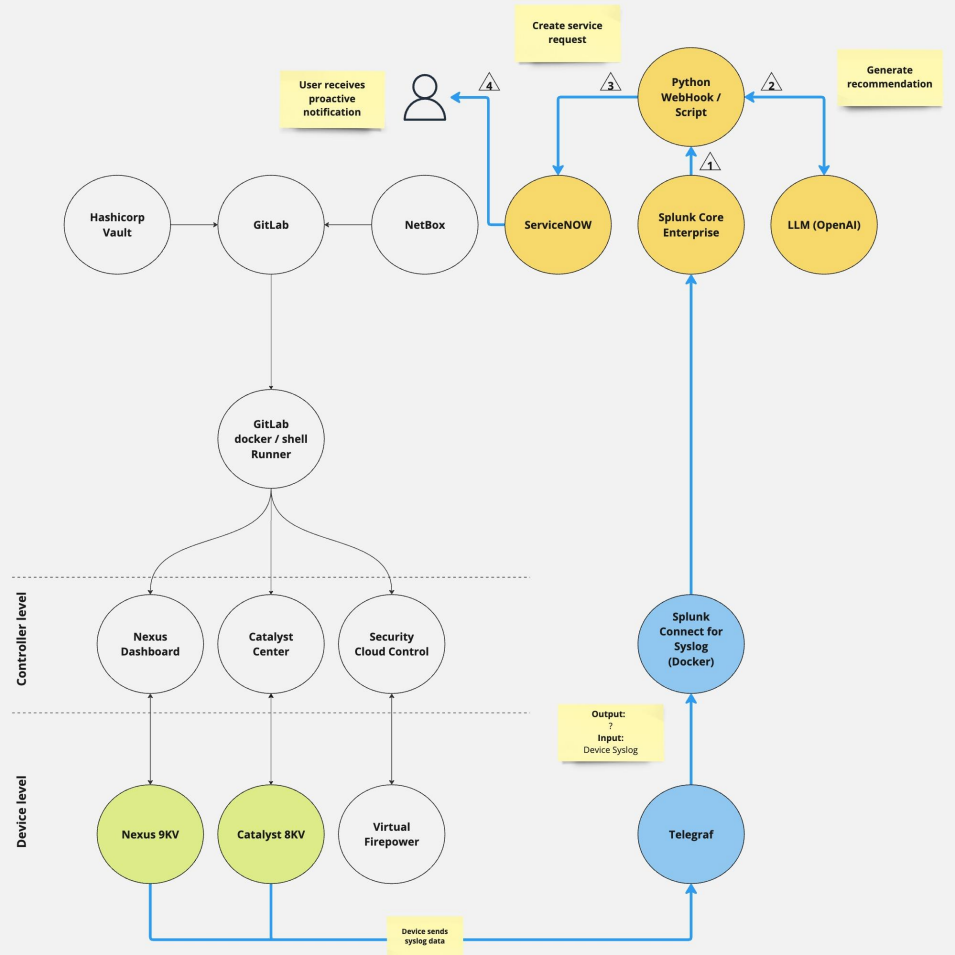


Demo time

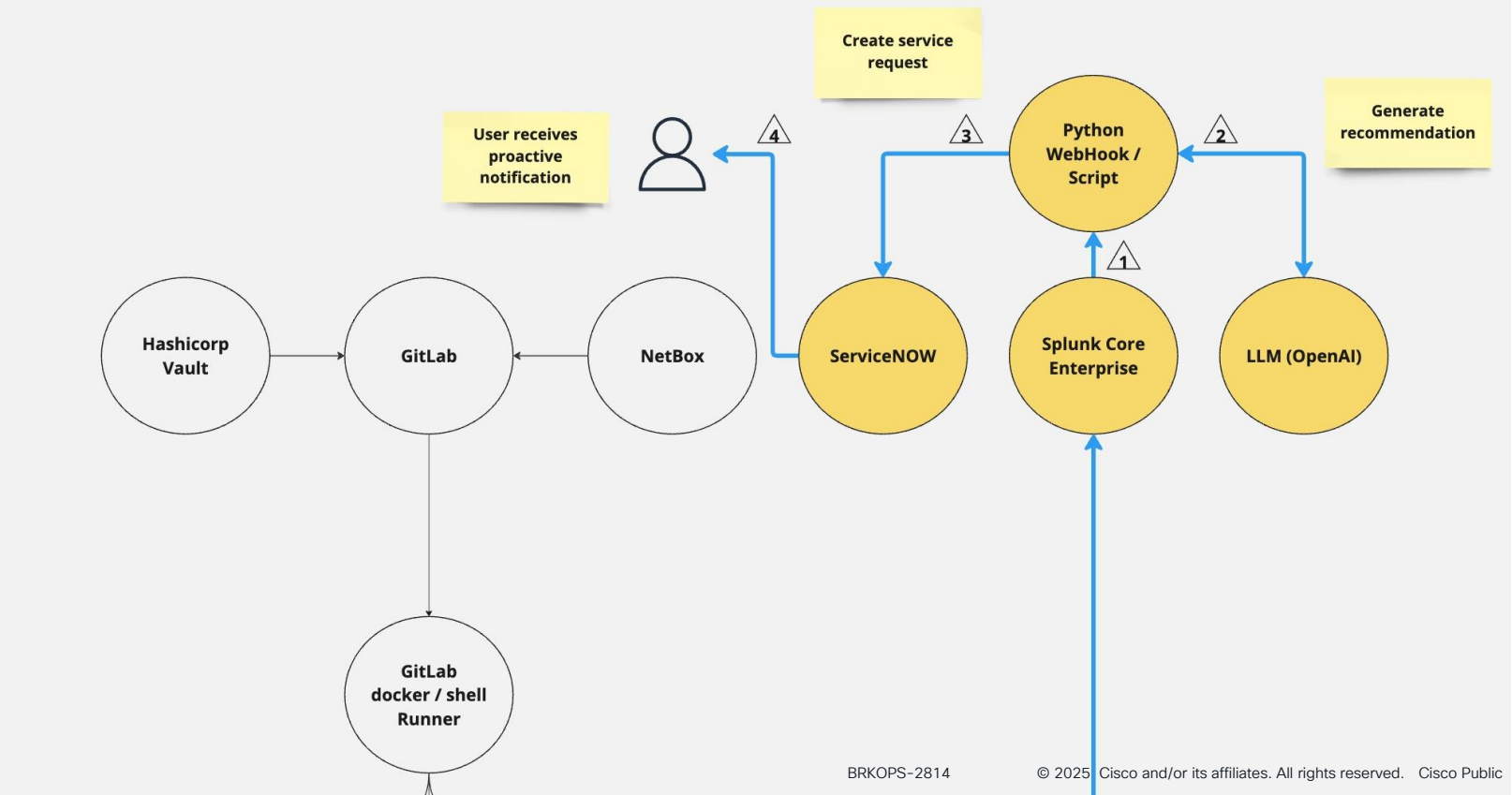
Integration with AI

Process overview

- Syslog Collection: Nexus 9KV and Catalyst 8KV send logs to Telegraf.
- Log Processing: Telegraf forwards logs to Splunk Connect for Syslog.
- Data Analysis: Splunk detects issues and sends alerts to Webhook Service.
- Automated Actions: ServiceNow tickets are created with AI-recommended solutions.
- Proactive Alerts: Users receive notifications to maintain network health.



Process overview: AI Insights



Demo time

More use cases

End-to-End Network Service Provisioning

- Automate multi-domain service provisioning across data center, WAN, and cloud environments.
- Example: Deploying a new application that requires automatic network segmentation, firewall rules, and SD-WAN policy updates across multiple vendors.

Network Security and Compliance Enforcement

- Implement automated security policies across firewalls, routers, and cloud gateways.
- Example: Detecting a malicious event (via SIEM) and dynamically updating firewall rules and zero-trust access policies across multi-vendor environments.

More use cases

Event-Driven Network Healing and Optimization

- Automate network health monitoring and response based on telemetry data.
- Example: Using AI-driven analytics (via NetFlow, SNMP, or streaming telemetry) to detect congestion and dynamically adjust QoS policies, reroute traffic, or scale cloud resources.

slido

Please download and install the Slido app on all computers you use

What other use cases do you have in mind?

ⓘ Start presenting to display the poll results on this slide.

Automate Today, Innovate Tomorrow 🚀

Call to action: Get started with our code!

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

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 ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: Insert preferred comms method

cisco Live!

GO BEYOND