You make **possible**

Cisco pxGrid 2.0 for IoT Platform Integration to Increase Visibility & Security

Nancy Cam-Winget, Distinguished Engineer
Syam Appala, Principal Engineer

@ncamwing

DEVNET 1476

Barcelona | January 27-31, 2020

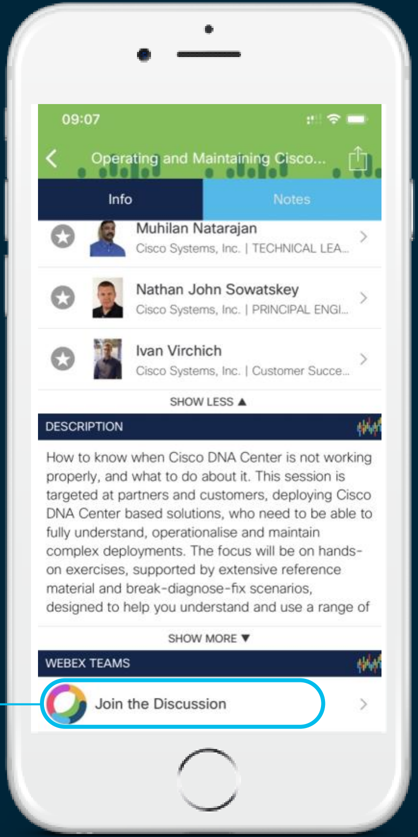
Cisco Webex Teams

Questions?

Use Cisco Webex Teams 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



09:07

Operating and Maintaining Cisco...

Info | Notes

Muhilan Natarajan
Cisco Systems, Inc. | TECHNICAL LEA...

Nathan John Sowatskey
Cisco Systems, Inc. | PRINCIPAL ENGI...

Ivan Virchich
Cisco Systems, Inc. | Customer Succe...

SHOW LESS ▲

DESCRIPTION

How to know when Cisco DNA Center is not working properly, and what to do about it. This session is targeted at partners and customers, deploying Cisco DNA Center based solutions, who need to be able to fully understand, operationalise and maintain complex deployments. The focus will be on hands-on exercises, supported by extensive reference material and break-diagnose-fix scenarios, designed to help you understand and use a range of

SHOW MORE ▼

WEBEX TEAMS

Join the Discussion

Agenda

- Cisco pxGrid Overview
- How to Develop using pxGrid
- Industrial IOT (IIOT) Use Case
- Getting Started

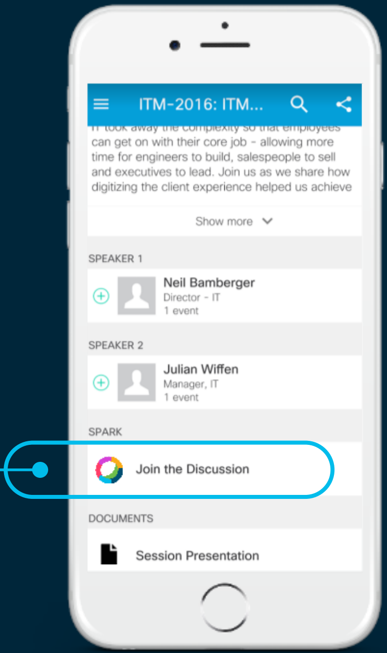
Cisco Webex Teams

Questions?

Use Cisco Webex Teams 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



ITM-2016: ITM...

IT took away the complexity so that employees can get on with their core job - allowing more time for engineers to build, salespeople to sell and executives to lead. Join us as we share how digitizing the client experience helped us achieve

Show more

SPEAKER 1

Neil Bamberger
Director - IT
1 event

SPEAKER 2

Julian Wiffen
Manager, IT
1 event

SPARK

Join the Discussion

DOCUMENTS

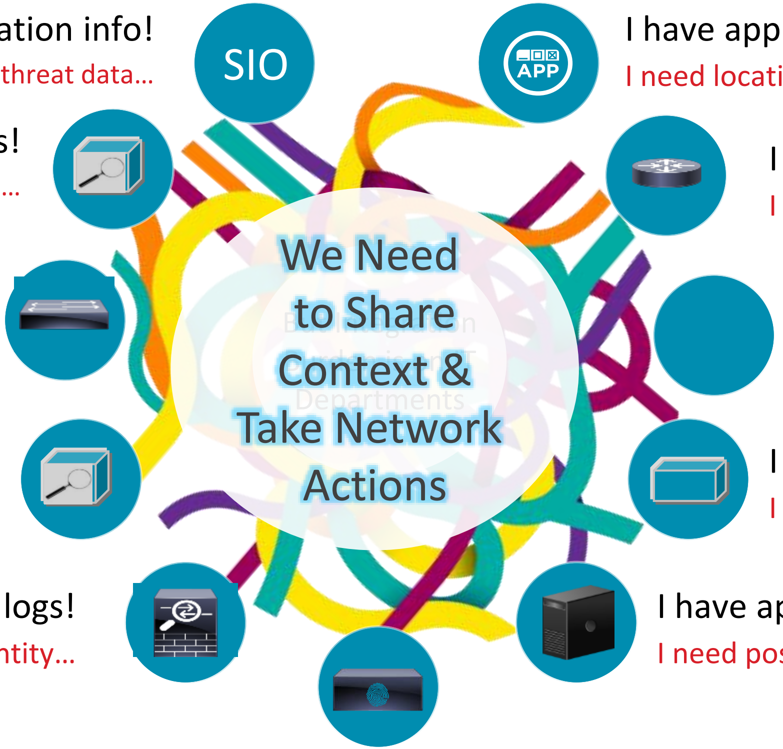
Session Presentation

cs.co/ciscolivebot#

Cisco pxGrid Overview

Context is the Currency of the Solution Integration Realm

…but it's not easy to execute



I have reputation info!
I need threat data…

I have sec events!
I need reputation…

I have NetFlow!
I need entitlement…

I have threat data!
I need reputation…

I have firewall logs!
I need identity…

I have identity & device-type!
I need app inventory & vulnerability…

I have app inventory info!
I need posture…

I have MDM info!
I need location…

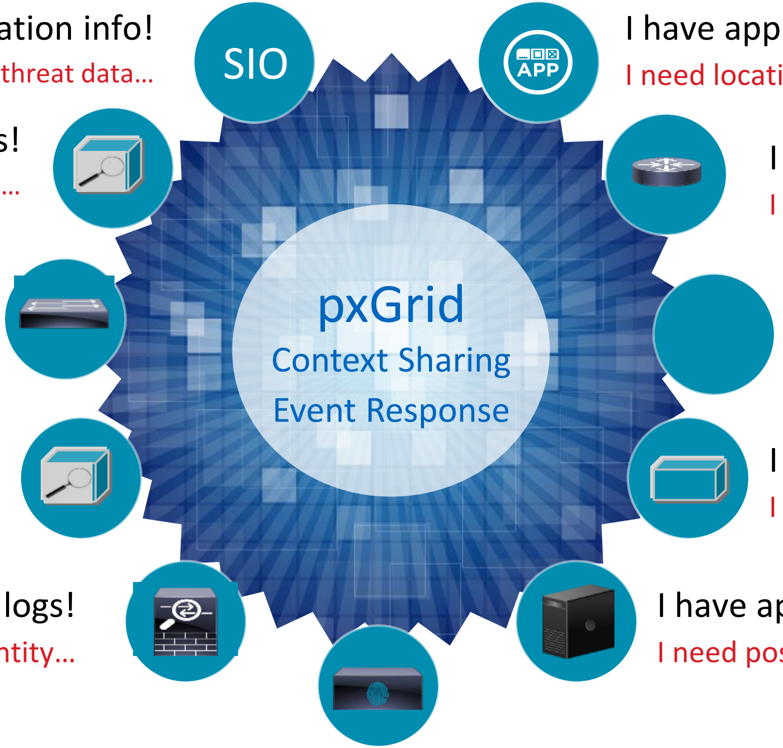
I have location!
I need identity…

I have NBAR info!
I need identity…

I have application info!
I need location & auth-group…

Context is the Currency of the Solution Integration Realm

…but it’s not easy to execute…but pxGrid accomplishes this



I have reputation info!
I need threat data…

I have application info!
I need location & auth-group…

I have sec events!
I need reputation…

I have NBAR info!
I need identity…

I have NetFlow!
I need entitlement…

I have location!
I need identity…

I have threat data!
I need reputation…

I have MDM info!
I need location…

I have firewall logs!
I need identity…

I have app inventory info!
I need posture…

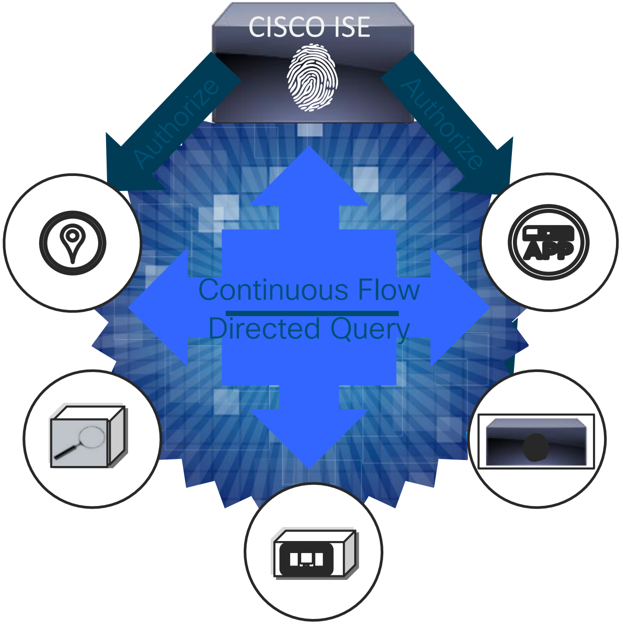
I have identity & device-type!
I need app inventory & vulnerability…

How pxGrid Works: Partners Connecting to Cisco Security Platforms…and to Other Partners

Publisher: Authenticate → Authorize → Publish

Subscriber: Authenticate → Authorize → Discover → Subscribe → Query

Cisco ISE as pxGrid Controller



I have location!
I need app & identity…

I have application info!
I need location & device-type

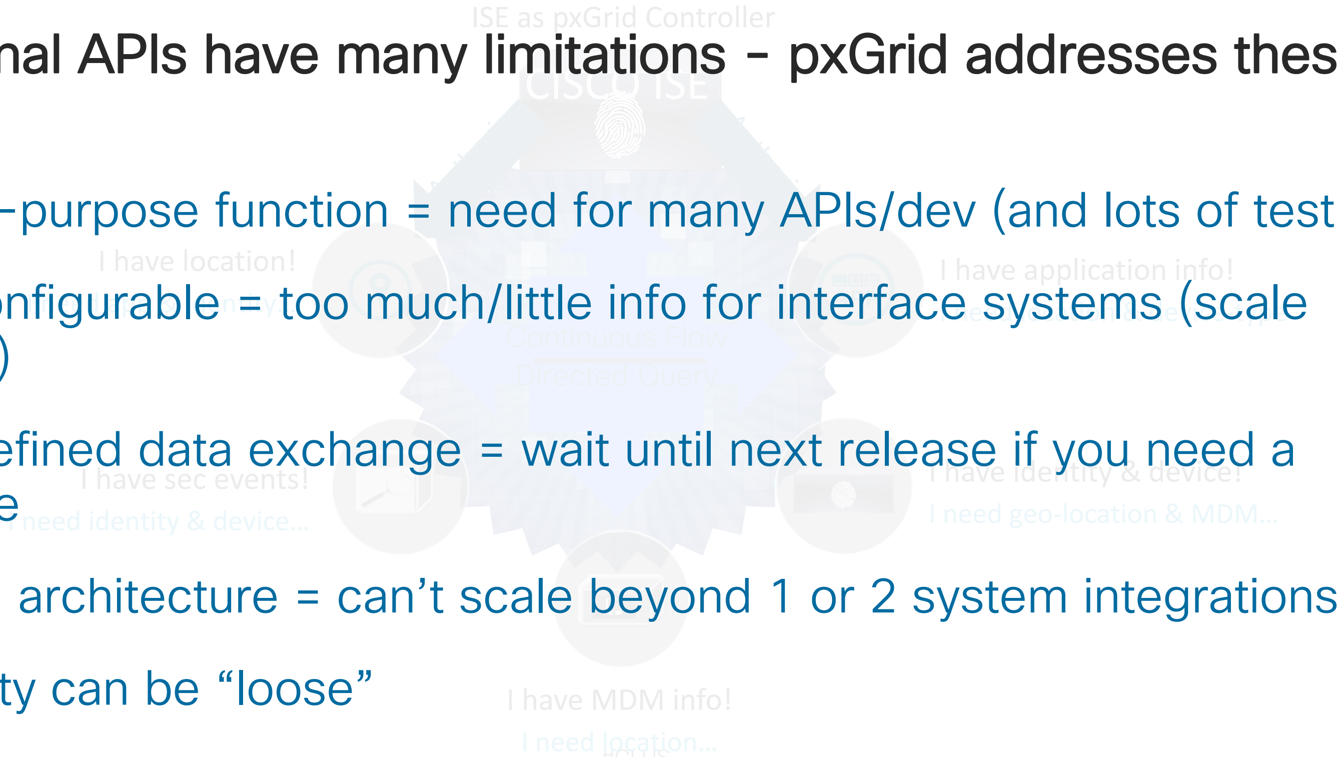
I have sec events!
I need identity & device…

I have identity & device!
I need geo-location & MDM…

I have MDM info!
I need location…

How pxGrid Works: Partners Connecting to Cisco Security Platforms…and to Other Partners

Publisher: Authenticate → Authorize → Publish
Subscriber: Authenticate → Authorize → Discover → Subscribe → Query



Traditional APIs have many limitations - pxGrid addresses these issues:

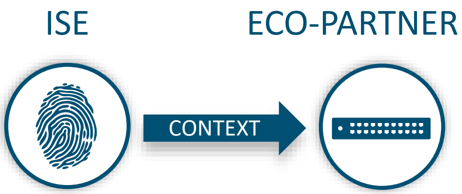
- Single-purpose function = need for many APIs/dev (and lots of testing)
- Not configurable = too much/little info for interface systems (scale issues)
- Pre-defined data exchange = wait until next release if you need a change
- Polling architecture = can't scale beyond 1 or 2 system integrations
- Security can be "loose"

Cisco pxGrid – Context-Sharing & Network Mitigation

Connecting Partners & Cisco Security Platforms, Connecting Partners-to-Partners

1

ISE Makes Customer IT Platforms User/Identity,
Device and Network Aware



ISE

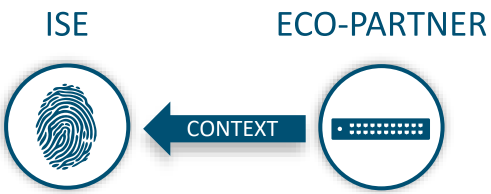
ECO-PARTNER

CONTEXT

ISE Shares User/Device & Network Context with IT Infrastructure

2

Make ISE a Better Network Policy Platform for Customers



ISE

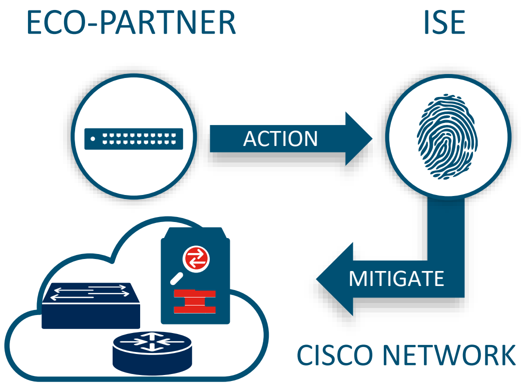
ECO-PARTNER

CONTEXT

ISE Receives Context from Eco-Partners to Make Better Network Access Policy

3

Help Customer IT Environments Reach
into the Cisco Network



ECO-PARTNER

ISE

ACTION

MITIGATE

CISCO NETWORK

BENEFITS

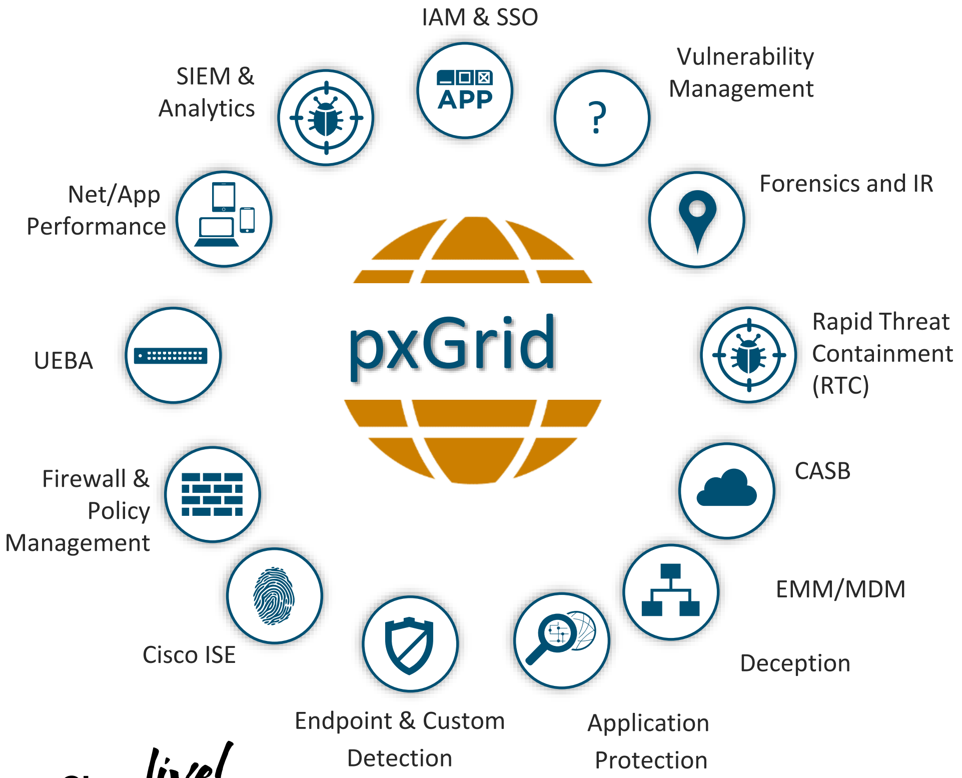
Puts "Who, What Device, What Access" with Events. Way Better than Just IP Addresses!

Creates a Single Place for Comprehensive Network Access Policy thru Integration

Decreases Time, Effort and Cost to Responding to Security and Network Events

pxGrid – Industry Adoption Critical Mass

50+ Partner Product Integrations and 12 Technology Areas



- Application Protection: Arxan, DB Networks
- SIEM and Analytics: HanSight, Hawk*, Huntsman*, LogRhythm*, Micro Focus NetIQ*, Splunk*, TripWire*, IBM- Qradar, Secureonix
- CASB: Elastica*, NetSkope, Skyhigh
- Deception: Attivo, illusive*, TrapX*
- Endpoint and Custom Detection: Invincea*, Redshift*, ThreatTrack, CloudPost Networks***, McAfee DXL, TriagingX
- Firewall and Policy Management: Bayshore*, Check Point, InfoBlox*, Intelliment, Cisco FMC*
- Forensics and IR: Cisco Cognitive Threat Analytics*, Lumeta, Endace, Cisco Stealthwatch*, Lemonfish*, TripWire*, WireX Systems
- IAM/SSO: Ping Identity, Secureauth*, Situational
- Other: Cisco WSA, Ark NSS****, Cisco ISE PIC
- Threat Intelligence: Infocyte*
- UEBA: E8*, Exabeam*, Fortscale*, Niara, Greenlight****
- Vulnerability Management: Rapid 7*, SAINT*, Tenable*, Tripwire*

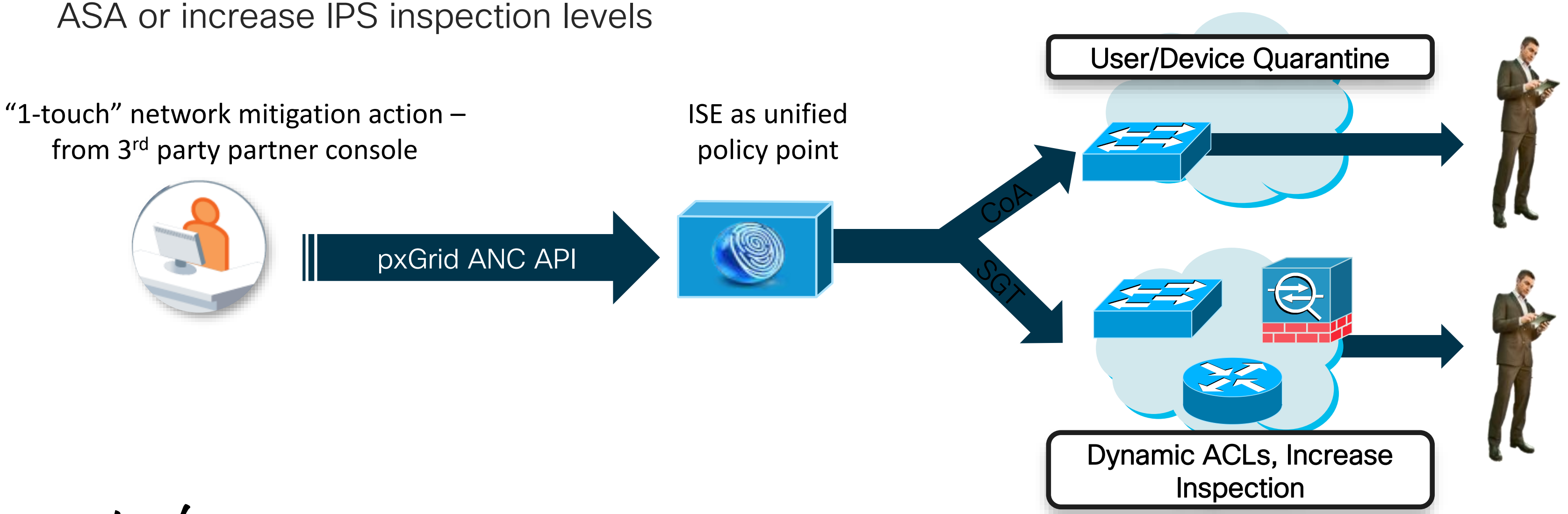
Solutions
* Rapid Threat Containment, ** Regulatory and Compliance Solution
***IoT, ****Regulatory and Compliance

pxGrid: Adaptive Network Control

Makes Cisco Infrastructure a Unified Event Response Network

Adaptive Network Control provides the ability to:

- Quarantine user devices from 3rd party products, such as SIEM systems
- Enlist other Cisco infrastructure in the network response – such as dynamic ACLs on switches and ASA or increase IPS inspection levels


"1-touch" network mitigation action – from 3rd party partner console
pxGrid ANC API
ISE as unified policy point
CoA
SGT
User/Device Quarantine
Dynamic ACLs, Increase Inspection

How to Develop using pxGrid 1.0

pxGrid 1.0 Architecture & Components

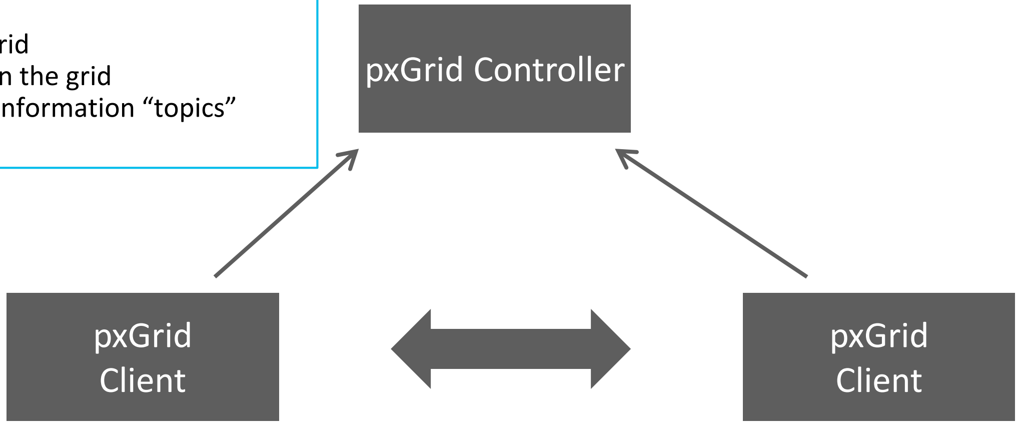
XMPP

Client based

XML

pxGrid Controller Responsible for Control Plane:

- Establishing the “grid” instance
- Authenticating clients on to the grid
- Authorizing what clients can do on the grid
- Maintaining directory of context information “topics” available on the grid



pxGrid Clients (Eco-Partner Platforms) Responsible for:

- Utilizing pxGrid Client Libraries (in SDK) to communicate with the pxGrid Controller
- If sharing contextual information, publishing it to a “topic”
- If consuming contextual information, subscribing to appropriate “topic”
- Filtering “topics” to exclude unwanted information
- Ad-hoc query to “topics”

Cisco pxGrid 1.0 Summary

- Visibility into *"who is connecting", "who is accessing what"*
- Centralized, policy-based authorization – *"who can do what"*
- Secure, bidirectional connectivity
- Mutual certs-based authentication, pre-shared key (PSK)
- Flexible consumption APIs – real-time (XMPP), on-demand (XMPP), bulk transfer (REST)
- Client contextual needs support through semantic, syntactic filtering
- Ability for peers to negotiate out-of-band, secure p2p connection
- Standardize schemas & information models through XML
- Dynamic topic support with authorizations on publish, subscribe and publisher actions
- Dynamic discovery of topics available on pxGrid 1.0
- Scalable to thousands of nodes

Cisco pxGrid 1.0 SDK Components & Function

Component	Function
Grid Client Library (GCL) in C and Java	• Software libraries for embedding in partner system • Connects partner system to the pxGrid
Sample pxGrid Data Output	• Sample data from Cisco ISE across a pxGrid connection to test with
Sample Data Generator	• Generates live session data across a pxGrid connection • Uses Cisco ISE user/device session data
pxGrid Controller Virtual Machine for Testing	• ISO of bundled Cisco ISE and pxGrid Controller for local testing in your lab
Hosted Testing Sandbox	• Enables developer to connect to an already setup test environment
pxGrid Documentation: Tutorials, Development Guides, testing guides,	• Complete documentation to guide the developer from concept to implementation to verification testing

How to Develop using pxGrid 2.0

pxGrid 2.0 addresses ...

REST-WS

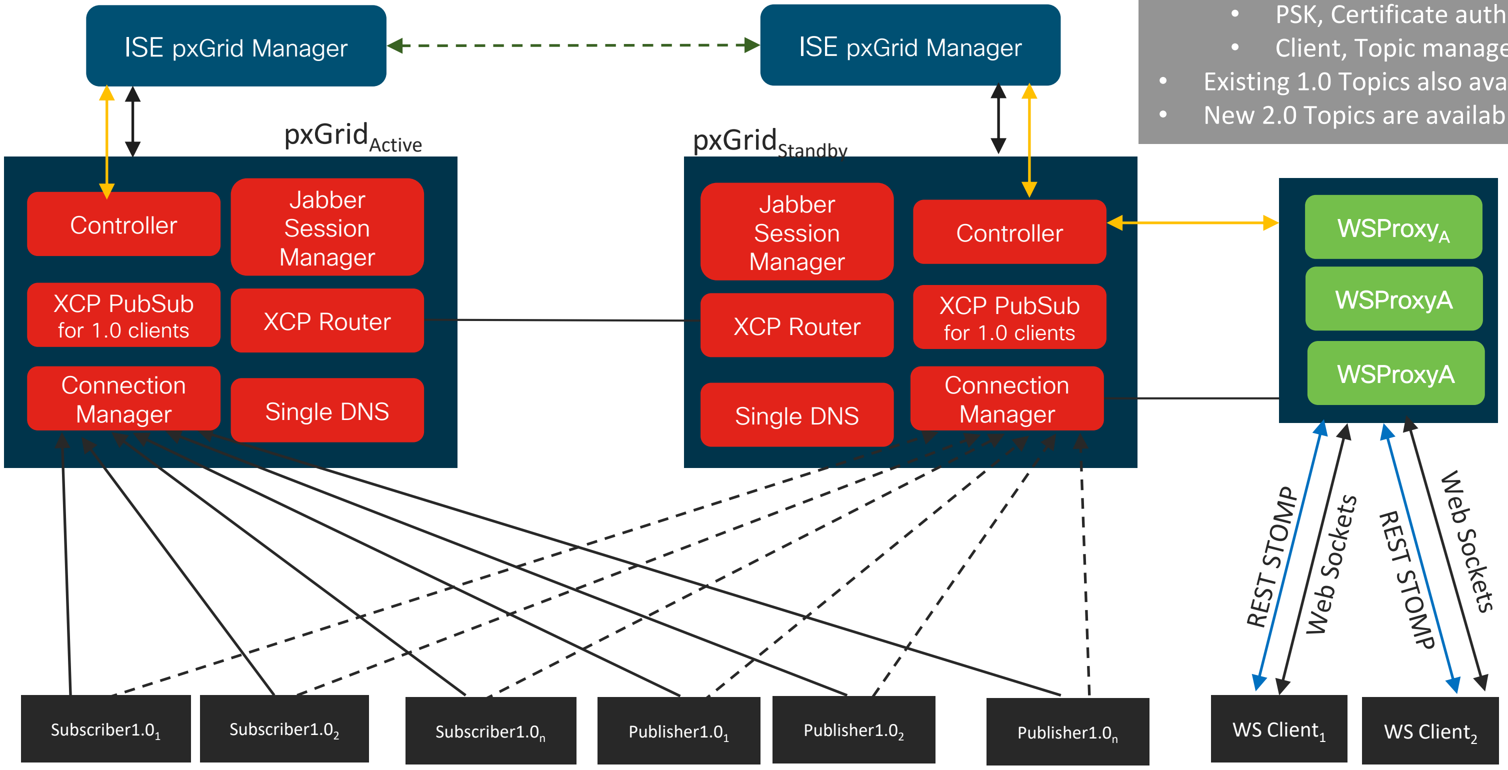
Clientless

JSON

- Ease of adoption with clientless approach
  - *No SDK or language dependency*
- Horizontal scalability
- Maintain backward compatibility with pxGrid 1.0
- Reduce technical support & integration effort
- pxGrid 1.0 support remains
- pxGrid 1.0 clients will continue to work with 1.0 Topics
  - Pubsub “Data” is bridged between pxGrid 1.0 and pxGrid 2.0

pxGrid 2.0 Architecture

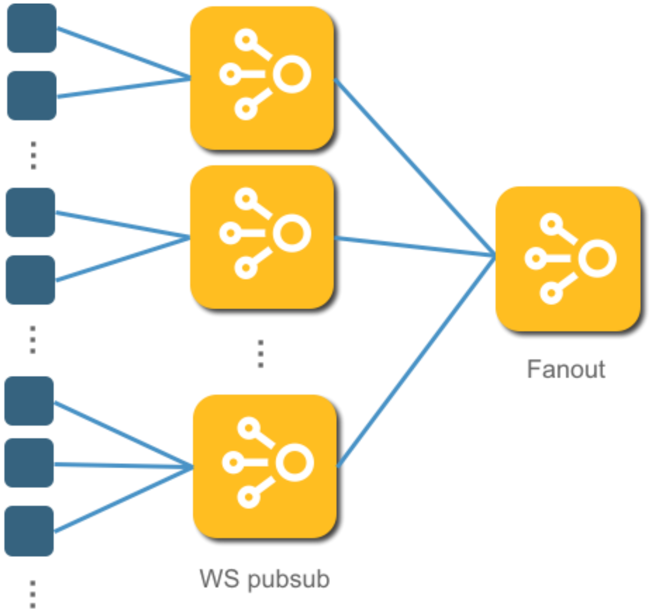
- REST (STOMP model) for control plane, queres
- Web Sockets for Pub/Sub
- Web Sockets proxy deployed in Active-Active
- Similar to pxGrid v1.0
  - Topic Discovery
  - PSK, Certificate authentication
  - Client, Topic management
- Existing 1.0 Topics also available on 2.0
- New 2.0 Topics are available only for 2.0 clients



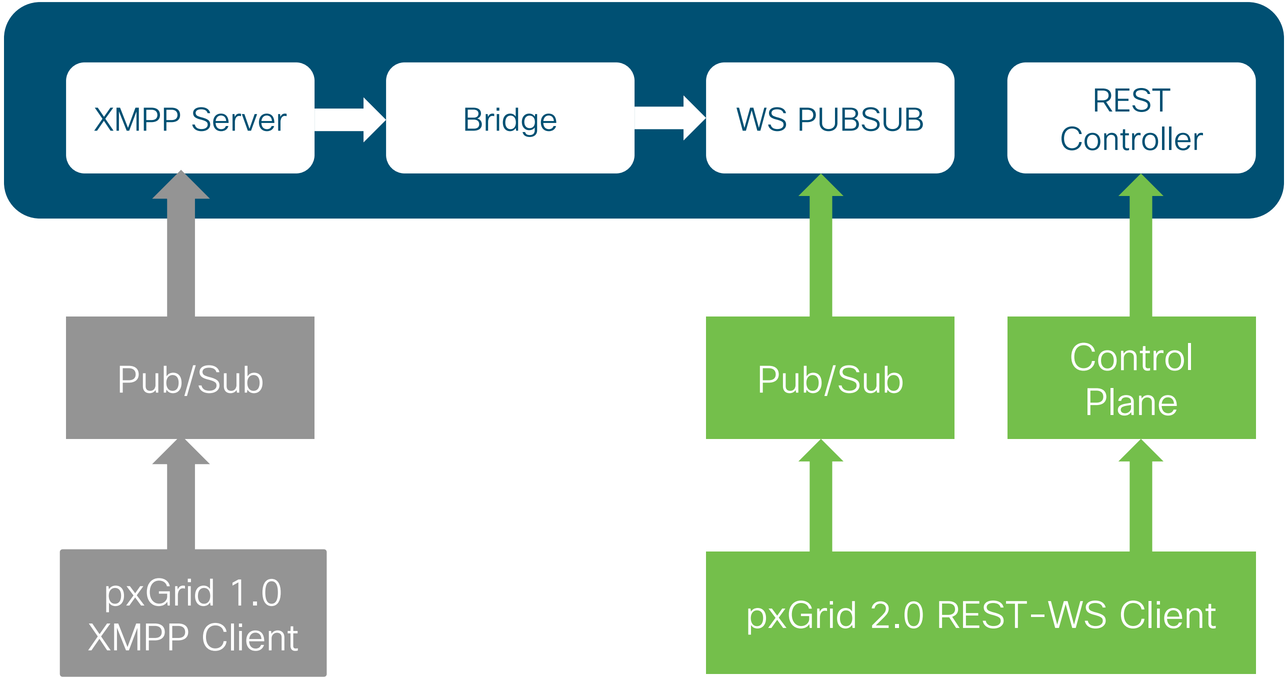
cisco Live!

pxGrid 2.0 Internals

- REST for authentication, authorization control plane and queries
- Web sockets for pubsub
- Uses Simple Text Oriented Messaging Protocol (STOMP) message format
  - Façade for any messaging system
  - STOMP is mostly a message format
  - Defines simple semantics such as Connect/Disconnect, Send/Subscribe etc. with frames modelled on HTTP
- Provides horizontal scaling through fan out



Support for pxGrid 1.0 Clients in pxGrid 2.0



Parity between pxGrid 1.0 and pxGrid 2.0

pxGrid 1.0 *vs* pxGrid 2.0

	pxGrid 1.0	pxGrid 2.0
Consumer	• SDK based • XMPP queries • XMPP pubsub	• Agentless: no SDK required • REST API calls for registration • STOMP pubsub • Websocket transport layer
Provider	• Requires SDK • XMPP Discovery/Authz API • XMPP authentication • XMPP query handlers • XMPP pubsub publisher	• No SDK • REST Discovery/Authz API • Webapp authentication provider • REST API handlers • STOMP pubsub • Websocket transport layer
Pubsub	• TCP Transport • XML parsing • Single instance • Dynamic topics support	• WebSockets transport • Data is opaque • Horizontal scaling with multiple active instances • Dynamic topics support
Control Plane	• XMPP Discovery, Authc, Authz • XMPP component • Clients require SDK	• REST + STOMP • Written as a Webapp • No SDK required
Topics	• ISE topics are published and available both on pxGrid 1.0 & pxGrid 2.0 • Dynamic topics created on pxGrid 1.0 are available for pxGrid 1.0 clients only • pxGrid 1.0 clients can subscribe to ISE pxGrid 1.0 topics • pxGrid 2.0 clients can subscribe to ISE pxGrid 1.0 or ISE pxGrid 2.0 topics	• Topics created on pxGrid 2.0 are available to pxGrid 2.0 clients only

How to Install and Test Using the pxGrid 2.0

- Install Cisco ISE 2.3 or later ISO on a VM

- Follow the steps and review the sample code specified in pxGrid devnet website

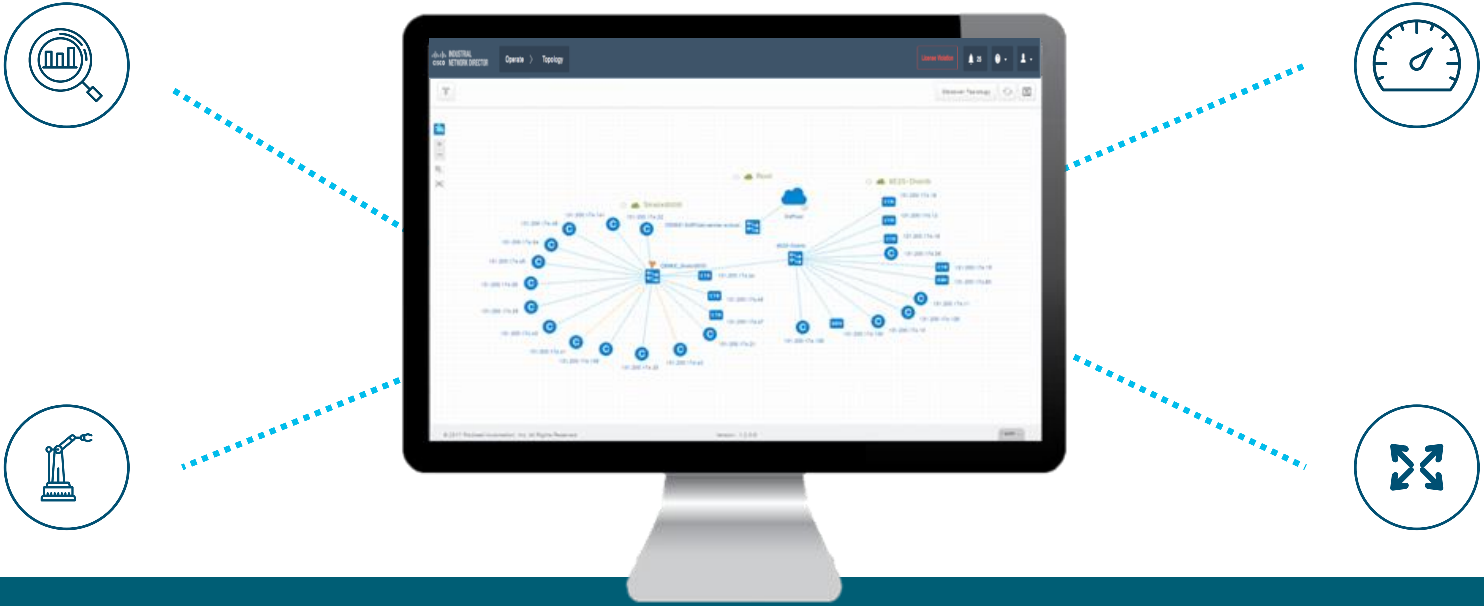
  https://developer.cisco.com/docs/pxgrid/

- pxGrid 2.0 client application documentation –

  https://github.com/cisco-pxgrid/pxgrid-rest-ws/wiki/pxgrid-consumer

ISE – Industrial Network Director (IND) Industrial IOT Use Case

Cisco Industrial Network Director
Network Management, Simplified & Automated



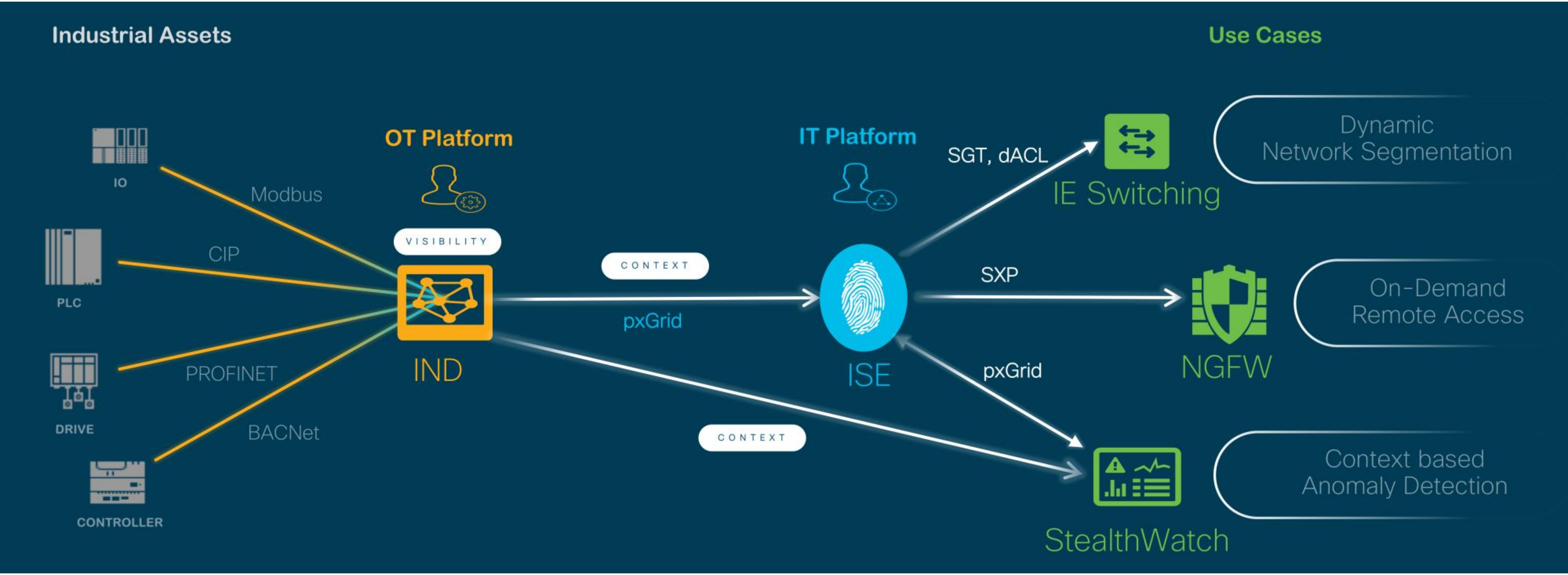
Plug-and-Play server for Zero-Touch Switch Commissioning

Improved Industrial Asset Visibility & Network Troubleshooting with Automation Context

REST APIs for Integration with Automation Systems

OT intent driven security workflows through ISE integration

OT Intent Driven Security Policies



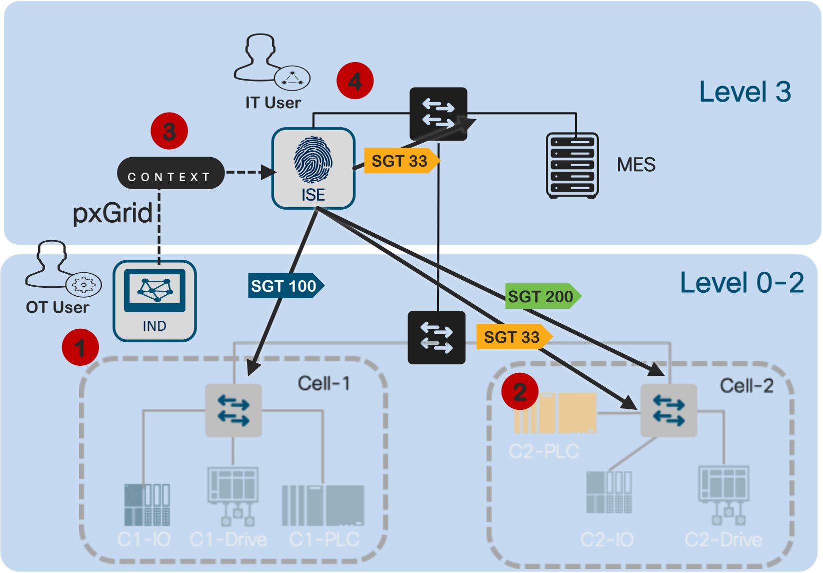
cisco Live!

Cell Segmentation

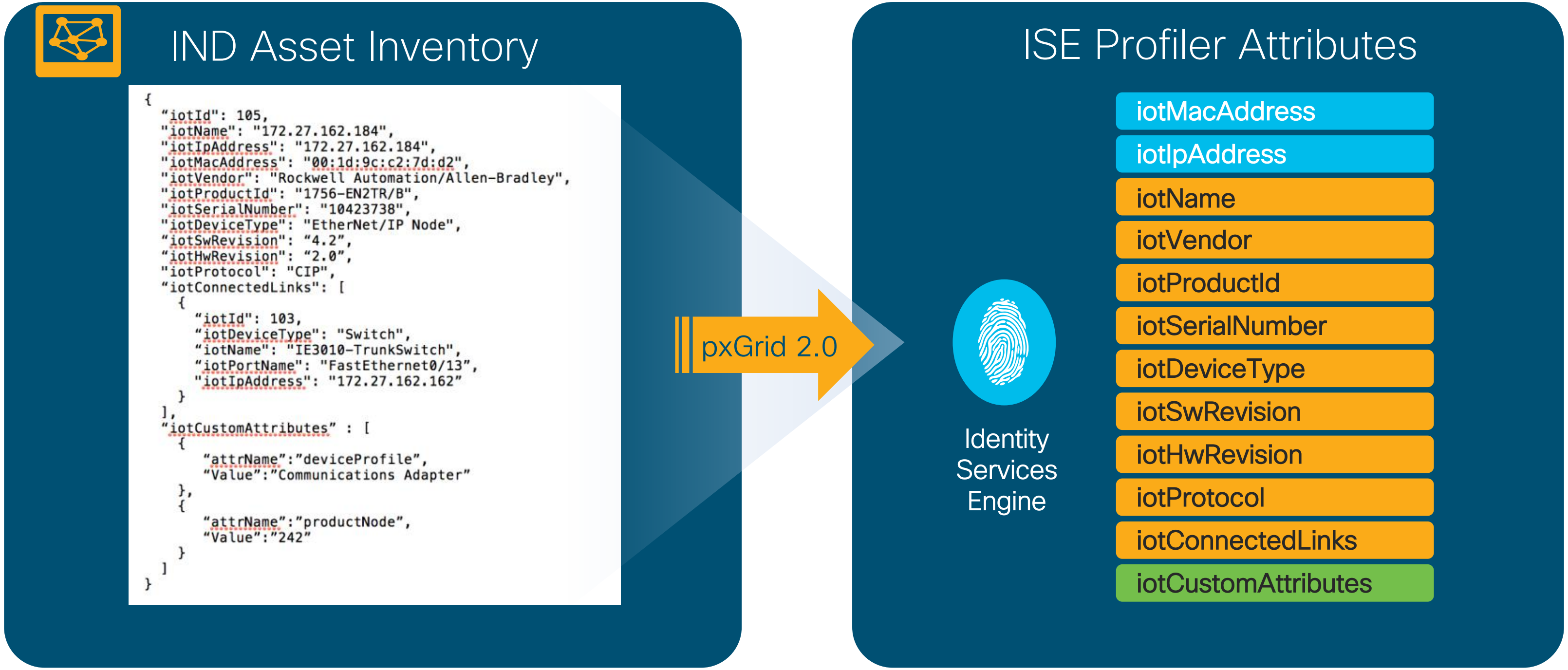
	SGT 33	SGT 100	SGT 200
SGT 33	✓	✓	✓
SGT 100	✓	✓	✗
SGT 200	✓	✗	✓

Requirement

- Segment the industrial network such that only certain assets can communicate with each other
- OT user (not IT) knows the control system, and must therefore have the ability classify the assets into segments at any time



Industrial Asset Visibility in ISE through IND



IND Asset Inventory

```
{
  “iotId": 105,
  "iotName": "172.27.162.184",
  "iotIpAddress": "172.27.162.184",
  "iotMacAddress": "00:1d:9c:c2:7d:d2",
  "iotVendor": "Rockwell Automation/Allen-Bradley",
  "iotProductId": "1756-EN2TR/B",
  "iotSerialNumber": "10423738",
  "iotDeviceType": "EtherNet/IP Node",
  “iotSwRevision": “4.2”,
  “iotHwRevision": “2.0”,
  "iotProtocol": "CIP",
  “iotConnectedLinks": [
    {
      “iotId": 103,
      “iotDeviceType": "Switch",
      “iotName": "IE3010-TrunkSwitch",
      “iotPortName": "FastEthernet0/13”,
      "iotIpAddress": "172.27.162.162”
    }
  ],
  “iotCustomAttributes” : [
    {
       “attrName”:”deviceProfile”,
       “Value”:”Communications Adapter”
    },
    {
       “attrName”:”productNode”,
       “Value”:”242”
    }
  ]
}
```

ISE Profiler Attributes

- iotMacAddress
- iotIpAddress
- iotName
- iotVendor
- iotProductId
- iotSerialNumber
- iotDeviceType
- iotSwRevision
- iotHwRevision
- iotProtocol
- iotConnectedLinks
- iotCustomAttributes

ISE profiling rules based on attributes like *Make, Model, Serial Number, Device Type* etc. instead of just IP address

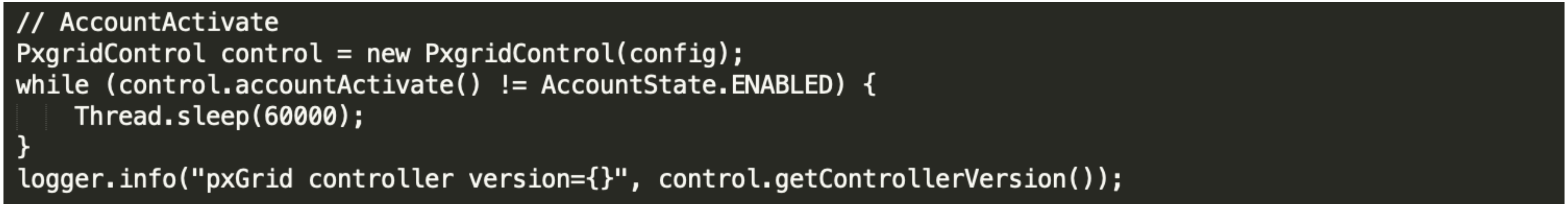
Custom Attributes allows IND to signal higher order information that is common to a group of assets

IND integration with ISE using pxGrid 2.0

1. Enable pxGrid service on ISE 2.4
2. Provision IND certificate in ISE and vice-versa
3. Enable pxGrid profiling probe in ISE
4. Approve IND pxGrid client account on ISE
5. IND creates “com.cisco.endpoint.asset” service & “/topic/com.cisco.endpoint.asset” topic
6. IND publishes on “/topic/com.cisco.endpoint.asset” topic & ISE subscribers to the topic
7. ISE receives custom attributes from ISE & uses them to classify IOT assets and perform segmentation

Sample Context-In Publish Code

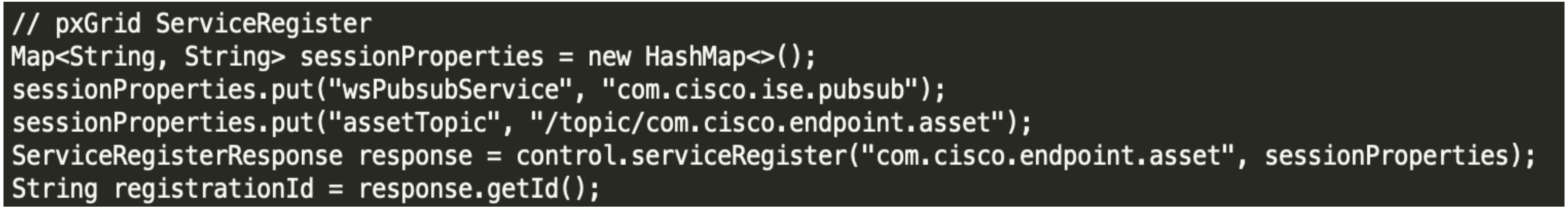
Account Activate – Requires admin to approve the new node



```
// AccountActivate
PxgridControl control = new PxgridControl(config);
while (control.accountActivate() != AccountState.ENABLED) {
    Thread.sleep(60000);
}
logger.info("pxGrid controller version={}", control.getControllerVersion());
```

Service Register to register the service “com.cisco.ise.pubsub”

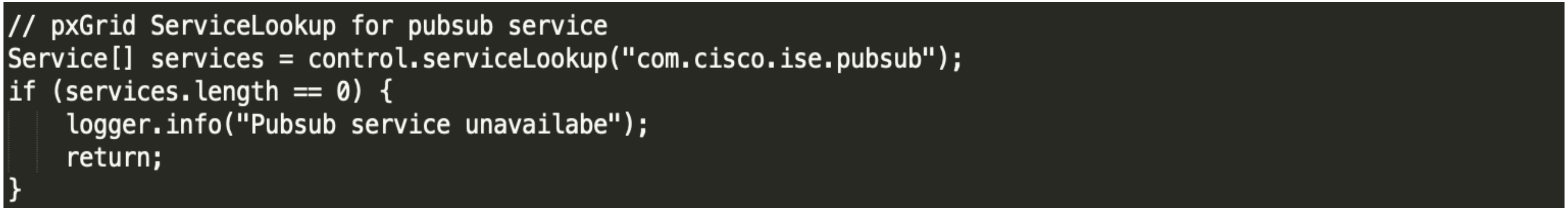
Service Register to register the topic “/topic/com.cisco.endpoint.asset”



```
// pxGrid ServiceRegister
Map<String, String> sessionProperties = new HashMap<>();
sessionProperties.put("wsPubsubService", "com.cisco.ise.pubsub");
sessionProperties.put("assetTopic", "/topic/com.cisco.endpoint.asset");
ServiceRegisterResponse response = control.serviceRegister("com.cisco.endpoint.asset", sessionProperties);
String registrationId = response.getId();
```

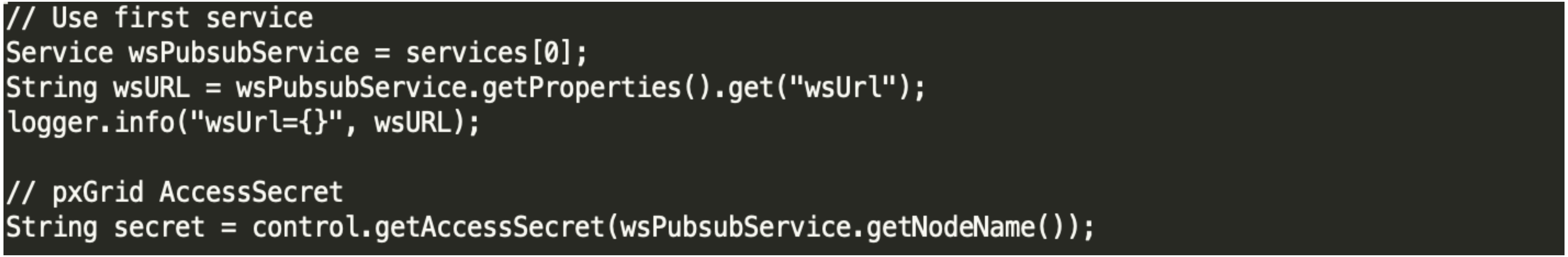
Sample Context-In Publish Code

“com.cisco.ise.pubsub” PubSub Service Lookup



```
// pxGrid ServiceLookup for pubsub service
Service[] services = control.serviceLookup("com.cisco.ise.pubsub");
if (services.length == 0) {
    logger.info("Pubsub service unavailabe");
    return;
}
```

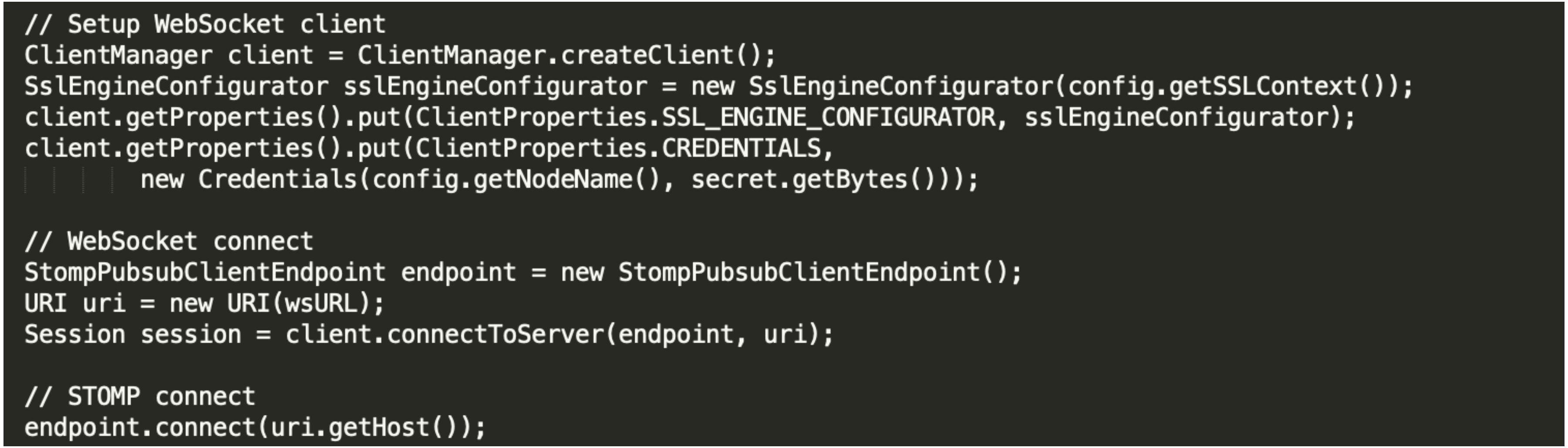
Get Access Secret to “com.cisco.ise.pubsub” PubSub Service



```
// Use first service
Service wsPubsubService = services[0];
String wsURL = wsPubsubService.getProperties().get("wsUrl");
logger.info("wsUrl={}", wsURL);

// pxGrid AccessSecret
String secret = control.getAccessSecret(wsPubsubService.getNodeName());
```

Sample Context-In Publish Code

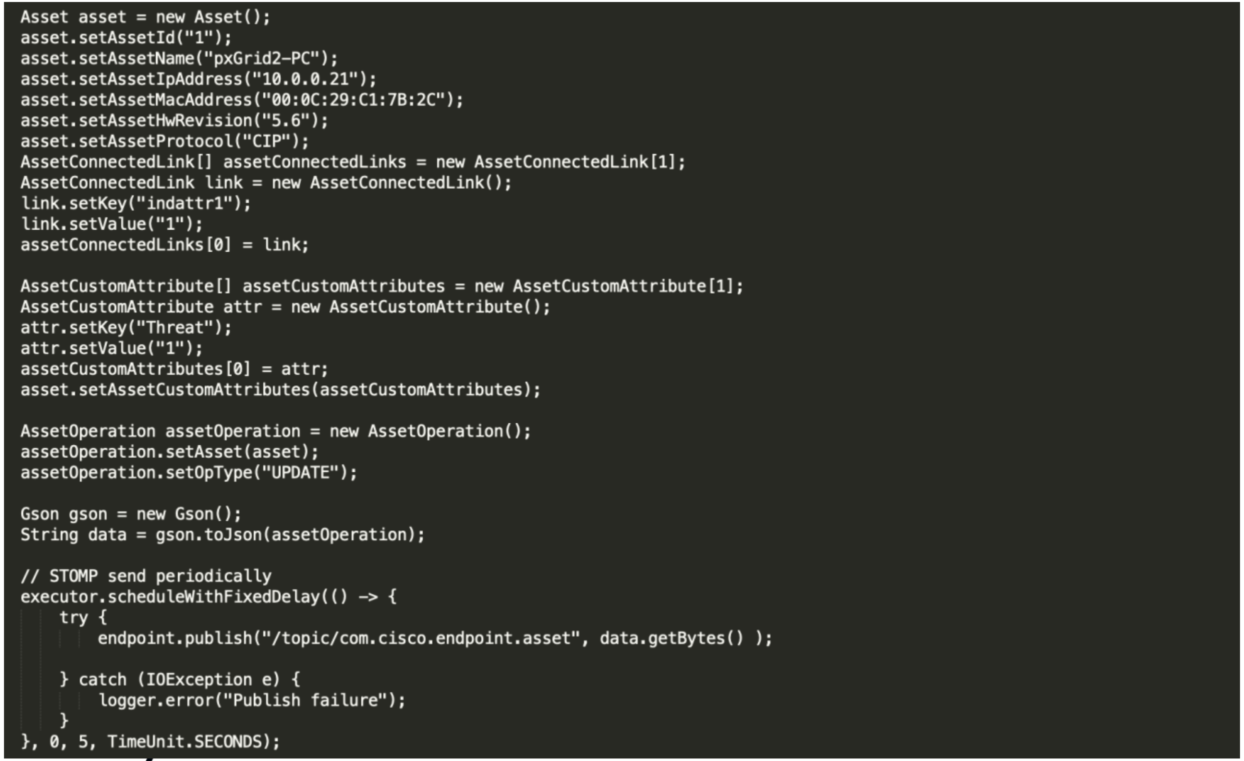
Setup WebSocket Client & Connect



```
// Setup WebSocket client
ClientManager client = ClientManager.createClient();
SslEngineConfigurator sslEngineConfigurator = new SslEngineConfigurator(config.getSSLContext());
client.getProperties().put(ClientProperties.SSL_ENGINE_CONFIGURATOR, sslEngineConfigurator);
client.getProperties().put(ClientProperties.CREDENTIALS,
        new Credentials(config.getNodeName(), secret.getBytes()));

// WebSocket connect
StompPubsubClientEndpoint endpoint = new StompPubsubClientEndpoint();
URI uri = new URI(wsURL);
Session session = client.connectToServer(endpoint, uri);

// STOMP connect
endpoint.connect(uri.getHost());
```

Sample Context-In Publish Code

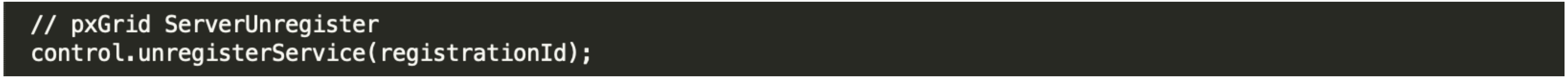
Publish Asset Attributes to “/topic/com.cisco.endpoint.asset” topic



```java
Asset asset = new Asset();
asset.setAssetId("1");
asset.setAssetName("pxGrid2-PC");
asset.setAssetIpAddress("10.0.0.21");
asset.setAssetMacAddress("00:0C:29:C1:7B:2C");
asset.setAssetHwRevision("5.6");
asset.setAssetProtocol("CIP");
AssetConnectedLink[] assetConnectedLinks = new AssetConnectedLink[1];
AssetConnectedLink link = new AssetConnectedLink();
link.setKey("indattr1");
link.setValue("1");
assetConnectedLinks[0] = link;

AssetCustomAttribute[] assetCustomAttributes = new AssetCustomAttribute[1];
AssetCustomAttribute attr = new AssetCustomAttribute();
attr.setKey("Threat");
attr.setValue("1");
assetCustomAttributes[0] = attr;
asset.setAssetCustomAttributes(assetCustomAttributes);

AssetOperation assetOperation = new AssetOperation();
assetOperation.setAsset(asset);
assetOperation.setOpType("UPDATE");

Gson gson = new Gson();
String data = gson.toJson(assetOperation);

// STOMP send periodically
executor.scheduleWithFixedDelay(() -> {
    try {
        endpoint.publish("/topic/com.cisco.endpoint.asset", data.getBytes() );

    } catch (IOException e) {
        logger.error("Publish failure");
    }
}, 0, 5, TimeUnit.SECONDS);
```

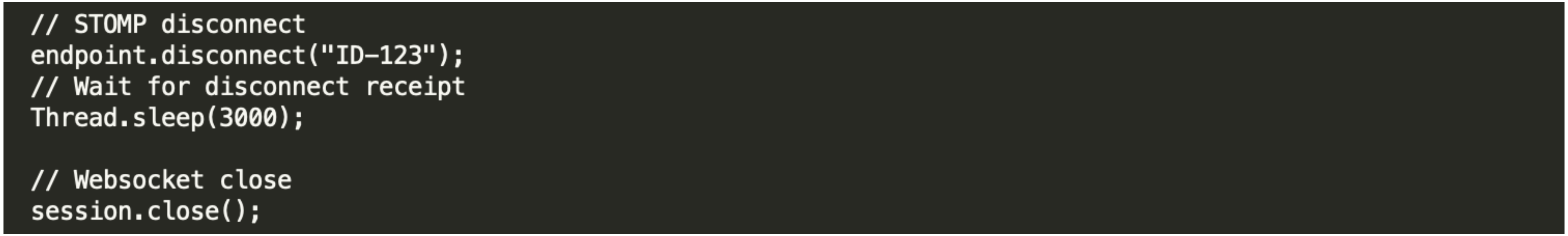
Sample Context-In Publish Code

UnRegister service “com.cisco.ise.pubsub”



```
// pxGrid ServerUnregister
control.unregisterService(registrationId);
```

Disconnect & Close WebSocket Connection



```
// STOMP disconnect
endpoint.disconnect("ID-123");
// Wait for disconnect receipt
Thread.sleep(3000);

// Websocket close
session.close();
```

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

- Demos in the Cisco Showcase
- Walk-In Labs
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you

cisco

You make **possible**