cisco Live!

Let's go

#CiscoLive

The bridge to possible

Threat Detection & Protection

Leveraging MITRE in Secure Firewall

Dr. Yatish Joshi, Technical Leader
@tryjoshi

BRKSEC-2146

Who am I?

- Technical Leader in Firewall Management & Integrations team
  - Product Owner & Architect
- My team is responsible for:
  - Ingestion & Operationalization of threat intelligence across the firewall
  - URL filtering
  - Malware Detection
  - Geolocation
  - And much more!

Cisco Webex App

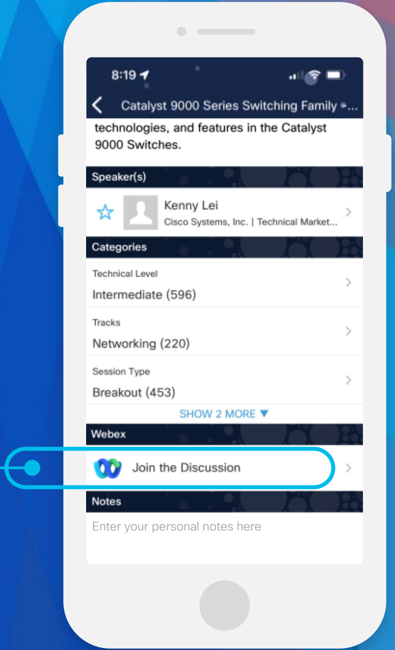
Questions?

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.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2146

Agenda

- Overview of Secure Firewall
- What is MITRE?
- Demo
- Conclusion

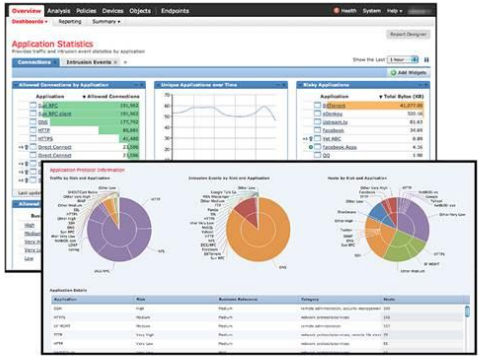
Overview of Secure Firewall

Secure Firewall Management Center

Centralized management for multi-site deployments

- Multi-domain management
- Role-based access control
- High availability
- API/pxGrid integration
- Firewall and AVC
- NGIPS
- AMP
- Security Intelligence
- Physical and virtual options

Firewall Management Center



Manage firewalls across many sites

Control access and set policies

Investigate incidents

Prioritize responses

Secure Firewall Threat Defense

Best of Breed

Threat-Focused stops vulnerability exploitation

High Availability

Intrusion Prevention

Firewall, VPN and Routing

Application Visibility and Control

Analytics and Visibility

Malware Protection

URL Filtering

SSL Decrypt and Network Profiling

Identity-based Policy Control

Single OS + Single Management

MITRE

MITRE

- Founded in 1958.
- Key Innovations
  - STIX & TAXII with DHS
  - MITRE ATT&CK framework
  - CVE (Common Vulnerabilities and Exposures) Database
  - SQUINT
  - And much more!

Old School Intelligence vs STIX

IPs

88.166.23.127
193.23.244.244
2.3.69.209
146.0.32.144
50.7.161.218
128.31.0.39
213.61.66.116

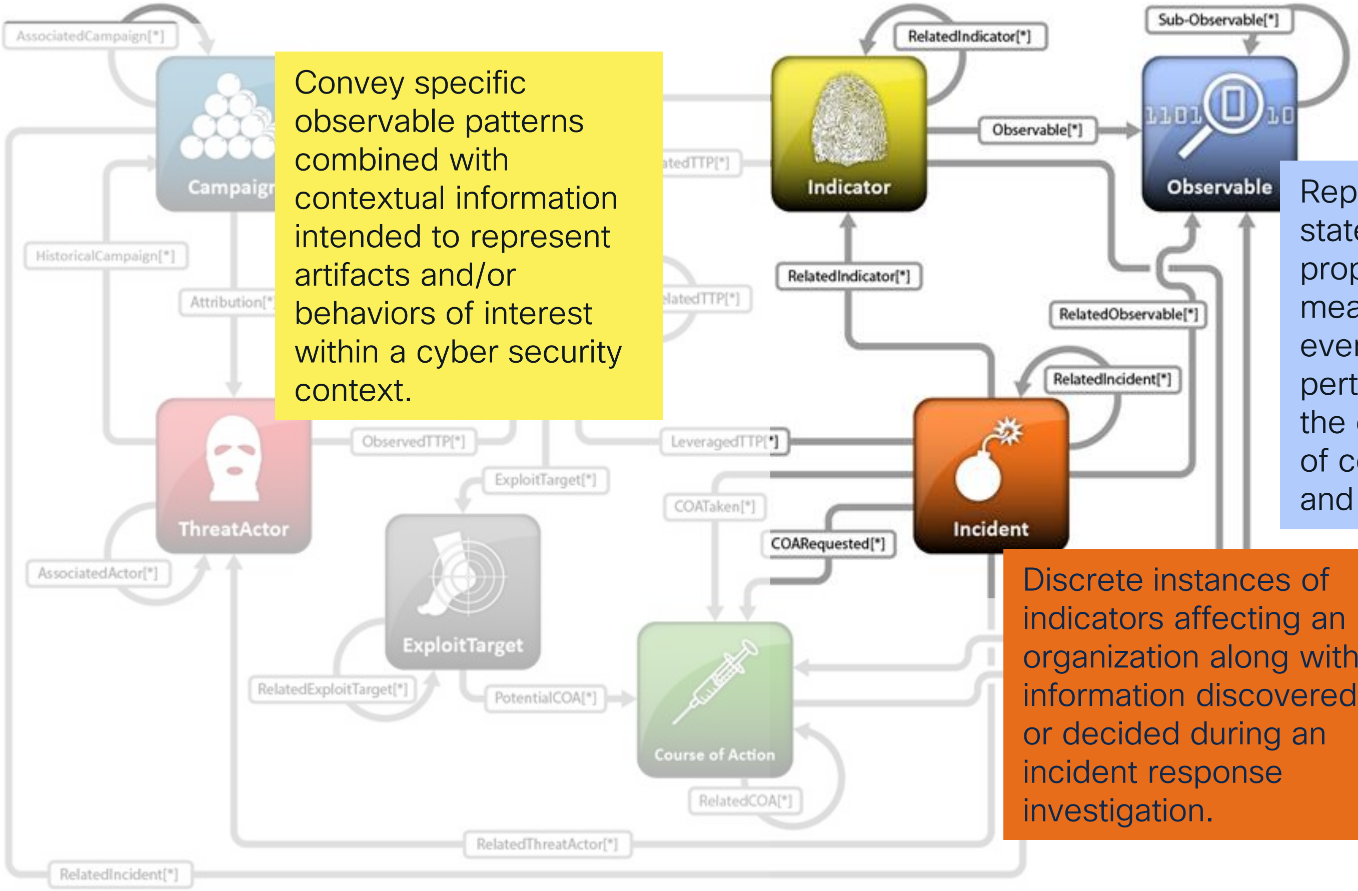
Domains/URLs

holland-cruz.com
robertson-ellis.com
johnston.com
brown-gibson.biz
snyder-clayton.biz

File SHAs

4e3bf660929f6427c0c5a592ee1692b76aa01954e8e02c66d9abe72b749c24cf
4cb2868695d21608f9d67eb3994f2948ea5a4f441d8baea453be7a10a9b8e6cf
0548da8ad8f64c778ef584411f7e84eb49b776af25618b94bc71d65d92c611e5
2062524f318a5313a168d400424463796d093fb2ed31336eeb7191c7b7461a72
04d5a2cf14cad950053fb9b3e0c47e62c4c769ddaa35bf6979e4540230878a34
a73d6764511fe9adee31a7e5ceff3d150a613409b6537098f6f3b7c1332c9f0e
1c32220e0dd90a05662dba2679898e92ddc987b022743897c3a3f920f7a0a0c0
891e39b9e5788328f057e90589dfac61ab999b086dee4de9eb148f7cfa5ddd50

STIX Data Model

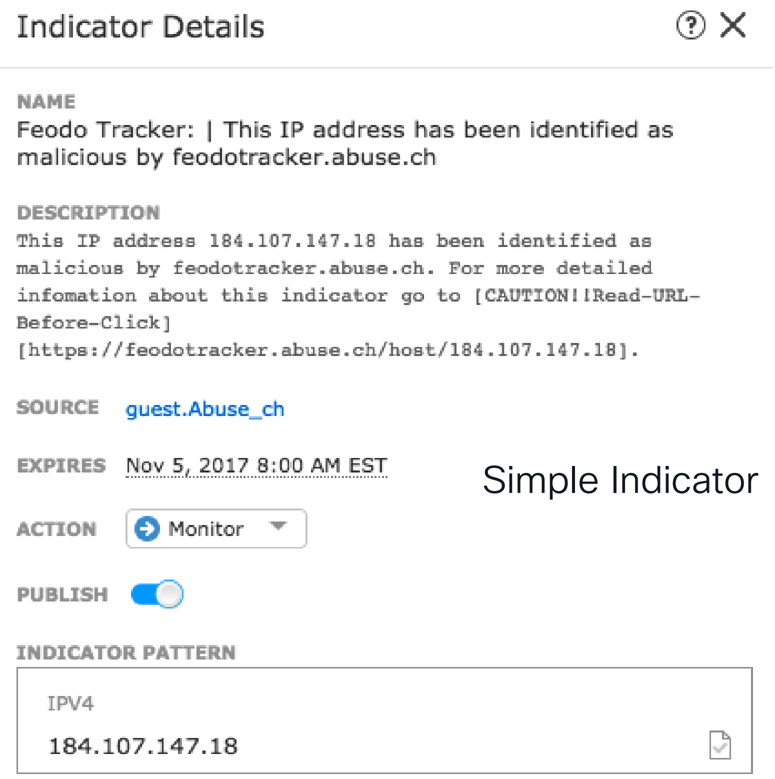


Convey specific observable patterns combined with contextual information intended to represent artifacts and/or behaviors of interest within a cyber security context.

Represent stateful properties or measurable events pertinent to the operation of computers and networks

Discrete instances of indicators affecting an organization along with information discovered or decided during an incident response investigation.

Intelligence from STIX



Indicator Details

NAME
Feodo Tracker: | This IP address has been identified as malicious by feodotracker.abuse.ch

DESCRIPTION
This IP address 184.107.147.18 has been identified as malicious by feodotracker.abuse.ch. For more detailed infomation about this indicator go to [CAUTION!!Read-URL-Before-Click] [https://feodotracker.abuse.ch/host/184.107.147.18].

SOURCE guest.Abuse_ch

EXPIRES Nov 5, 2017 8:00 AM EST

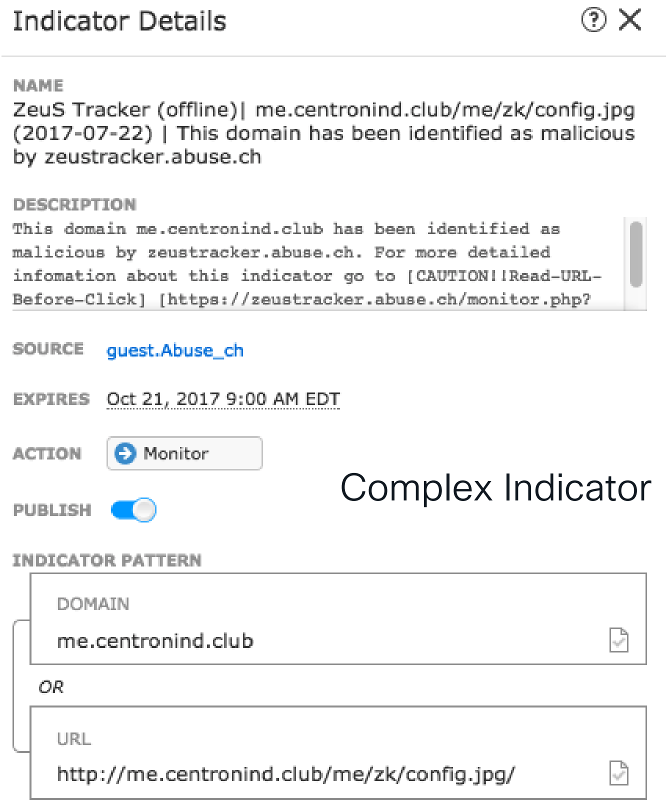
ACTION Monitor

PUBLISH

INDICATOR PATTERN

IPV4
184.107.147.18

Simple Indicator



Indicator Details

NAME
ZeuS Tracker (offline)| me.centronind.club/me/zk/config.jpg (2017-07-22) | This domain has been identified as malicious by zeustracker.abuse.ch

DESCRIPTION
This domain me.centronind.club has been identified as malicious by zeustracker.abuse.ch. For more detailed infomation about this indicator go to [CAUTION!!Read-URL-Before-Click] [https://zeustracker.abuse.ch/monitor.php?

SOURCE guest.Abuse_ch

EXPIRES Oct 21, 2017 9:00 AM EDT

ACTION Monitor

PUBLISH

INDICATOR PATTERN

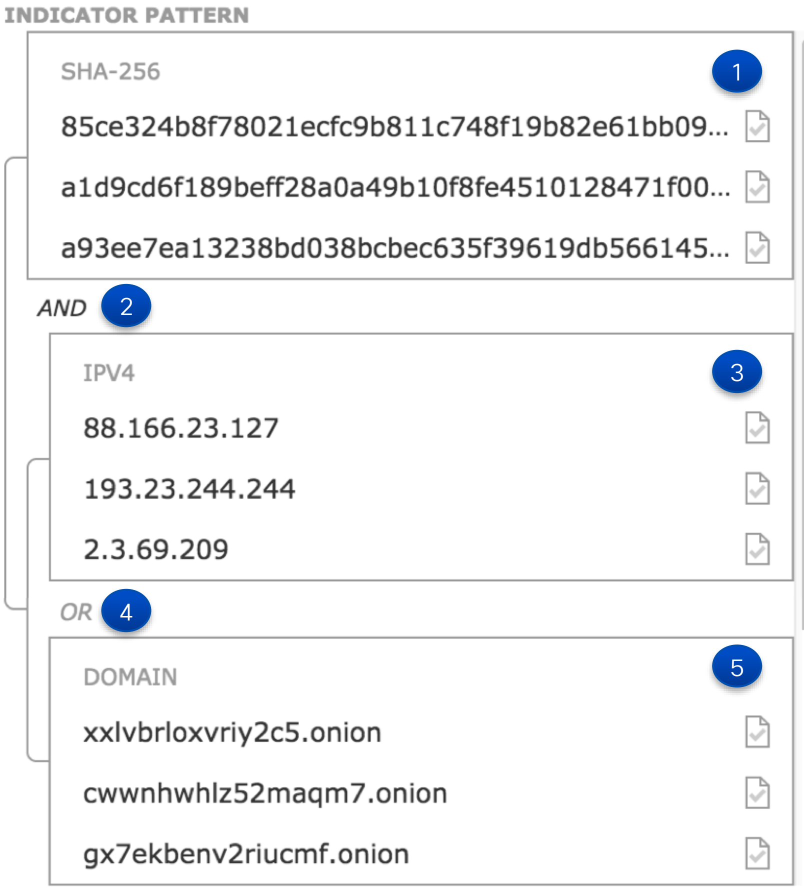
DOMAIN
me.centronind.club

OR

URL
http://me.centronind.club/me/zk/config.jpg/

Complex Indicator

Complex Intelligence from STIX



INDICATOR PATTERN

SHA-256 1

85ce324b8f78021ecfc9b811c748f19b82e61bb09...

a1d9cd6f189beff28a0a49b10f8fe4510128471f00...

a93ee7ea13238bd038bcbec635f39619db566145...

AND 2

IPV4 3

88.166.23.127

193.23.244.244

2.3.69.209

OR 4

DOMAIN 5

xxlvbrloxvriy2c5.onion

cwwnhwhlz52maqm7.onion

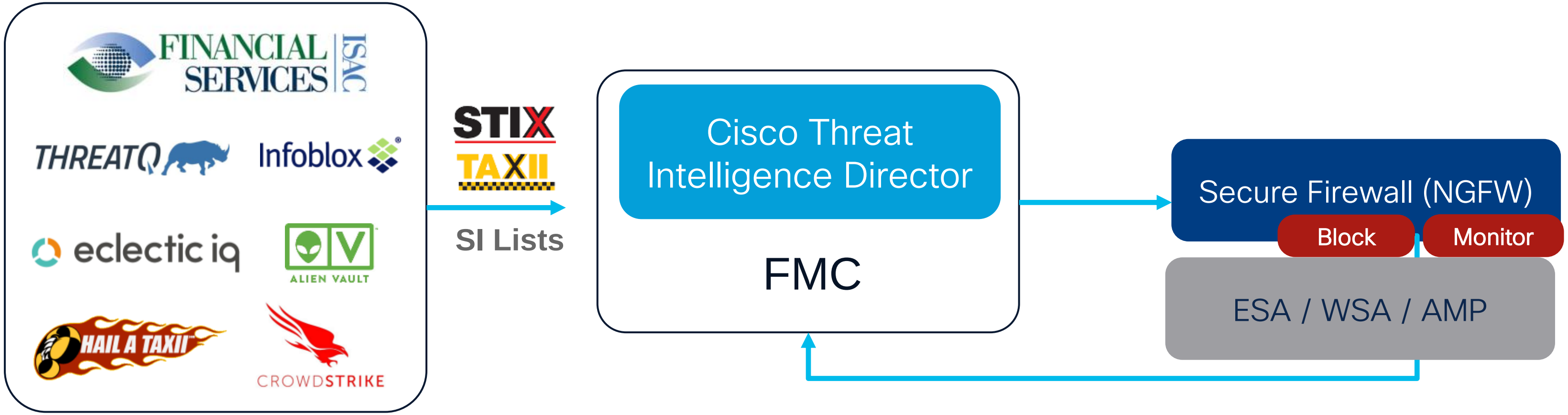
gx7ekbenv2riucmf.onion

Exploit or Malware File

AND

C&C Connection

Leveraging STIX & TAXII in Secure Firewall



Step 1
Ingest third-party Cyber Threat Intelligence (CTI)

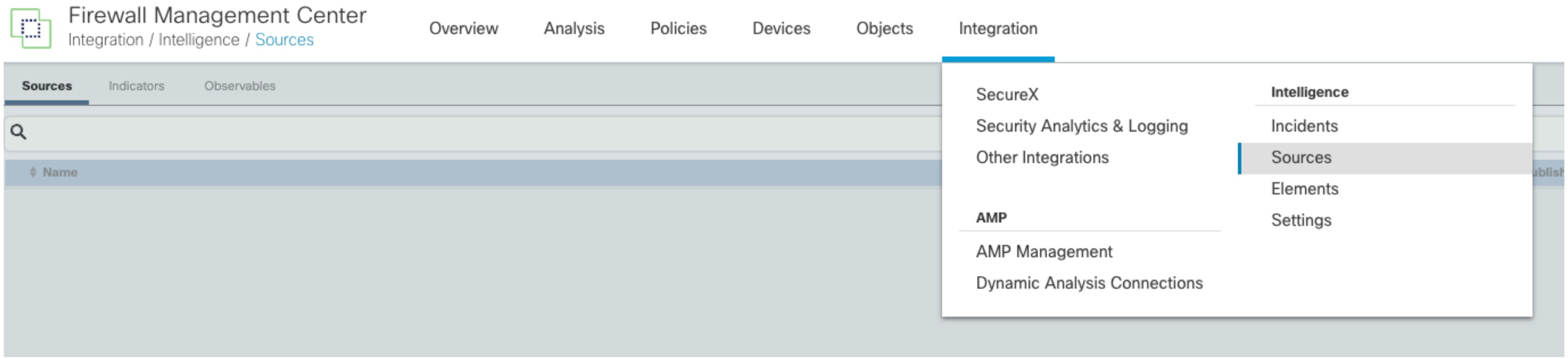
Step 2
Publish observables to sensors

Step 3
Detect and alert on incidents

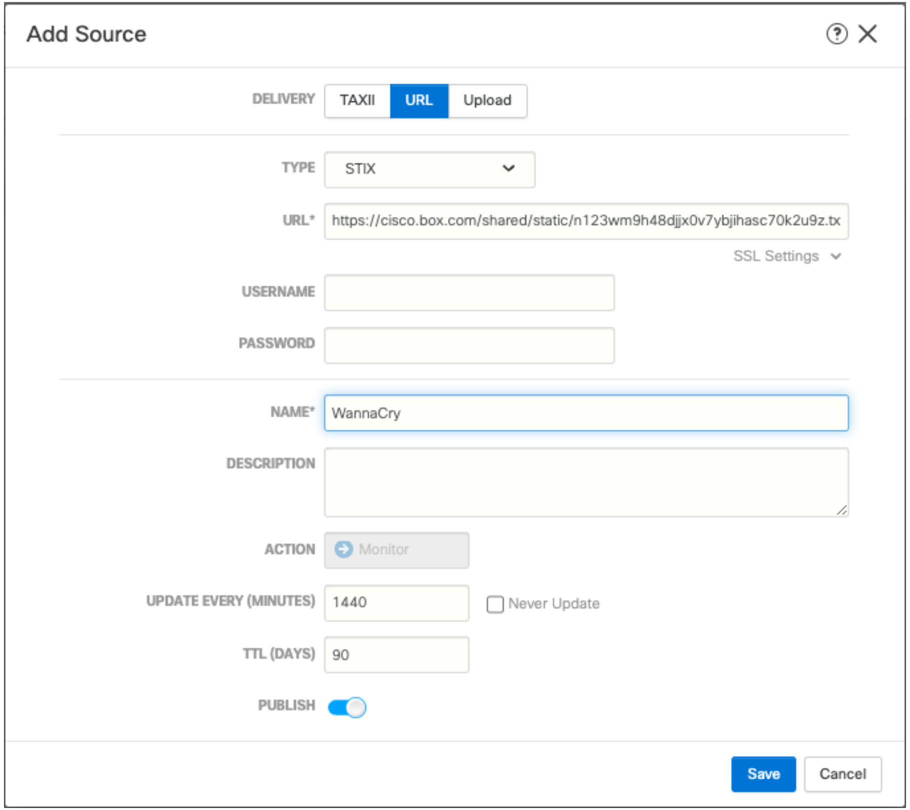
Cisco Threat Intelligence Director

Available on the Firewall Management Center since v6.2.2.

- Integrations → Intelligence



Adding Intelligence Sources



Add Source

DELIVERY: TAXII | **URL** | Upload

TYPE: STIX

URL*: https://cisco.box.com/shared/static/n123wm9h48djjx0v7ybjihasc70k2u9z.tx

USERNAME:

PASSWORD:

NAME*: WannaCry

DESCRIPTION:

ACTION: Monitor

UPDATE EVERY (MINUTES): 1440 □ Never Update

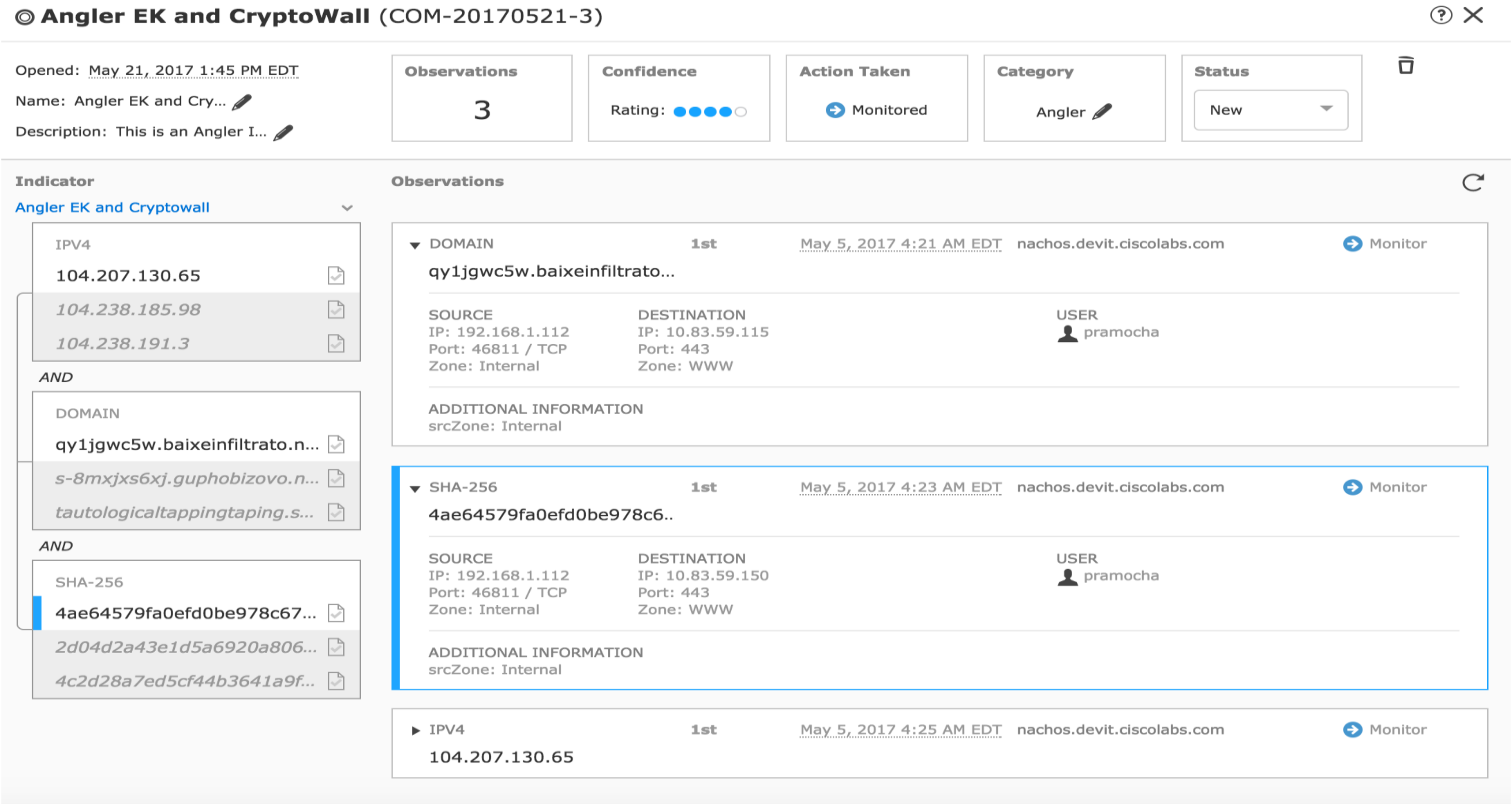
TTL (DAYS): 90

PUBLISH: ●

Sources-> Click on + icon to add a new Source

- Supports multiple delivery formats
- Easy configuration
- REST APIs available
- Easy to automate

Advanced Correlation of Attacks



◎ **Angler EK and CryptoWall** (COM-20170521-3)

Opened: May 21, 2017 1:45 PM EDT

Name: Angler EK and Cry...

Description: This is an Angler I...

Observations	Confidence	Action Taken	Category	Status
3	Rating: ●●●●○	Monitored	Angler	New

Indicator

Angler EK and Cryptowall

IPV4
- 104.207.130.65
- *104.238.185.98*
- *104.238.191.3*

AND

DOMAIN
- qy1jgwc5w.baixeinfiltrato.n...
- *s-8mxjxs6xj.guphobizovo.n...*
- *tautologicaltappingtaping.s...*

AND

SHA-256
- 4ae64579fa0efd0be978c67...
- *2d04d2a43e1d5a6920a806...*
- *4c2d28a7ed5cf44b3641a9f...*

Observations

DOMAIN 1st May 5, 2017 4:21 AM EDT nachos.devit.ciscolabs.com Monitor

qy1jgwc5w.baixeinfiltrato...

SOURCE	DESTINATION	USER
IP: 192.168.1.112 Port: 46811 / TCP Zone: Internal	IP: 10.83.59.115 Port: 443 Zone: WWW	pramocha

ADDITIONAL INFORMATION
srcZone: Internal

SHA-256 1st May 5, 2017 4:23 AM EDT nachos.devit.ciscolabs.com Monitor

4ae64579fa0efd0be978c6..

SOURCE	DESTINATION	USER
IP: 192.168.1.112 Port: 46811 / TCP Zone: Internal	IP: 10.83.59.150 Port: 443 Zone: WWW	pramocha

ADDITIONAL INFORMATION
srcZone: Internal

IPV4 1st May 5, 2017 4:25 AM EDT nachos.devit.ciscolabs.com Monitor

104.207.130.65

MITRE ATTA&CK Framework

- Globally-accessible knowledgebase of threat tactics and techniques based on real-world observations
- Created to tackle 4 main issues:
  - Adversary behaviors
  - Lifecycle models
  - Applicability to real environments
  - Common taxonomy
- Available for Enterprise, Mobile & ICS
- Check out https://attack.mitre.org/

ATTA&CK Framework – Enterprise Tactics

- Reconnaissance: gather information for future operations
- Resource Development: establish resources to support operation
- Initial Access: trying to get into your network
- Execution: trying to run malicious code
- Persistence: maintain their foothold
- Privilege Escalation: gain higher lever permissions
- Defense Evasion: avoid detection

ATTA&CK Framework – Enterprise Tactics (2)

- Credential Access: steal account names and passwords
- Discovery: gain knowledge about the environment
- Lateral Movement: move through your network
- Collection: gather information to meet their objectives
- Exfiltration: steal data
- Command & Control: communicate with compromised systems and control them
- Impact: manipulate, destroy or interrupt system and data

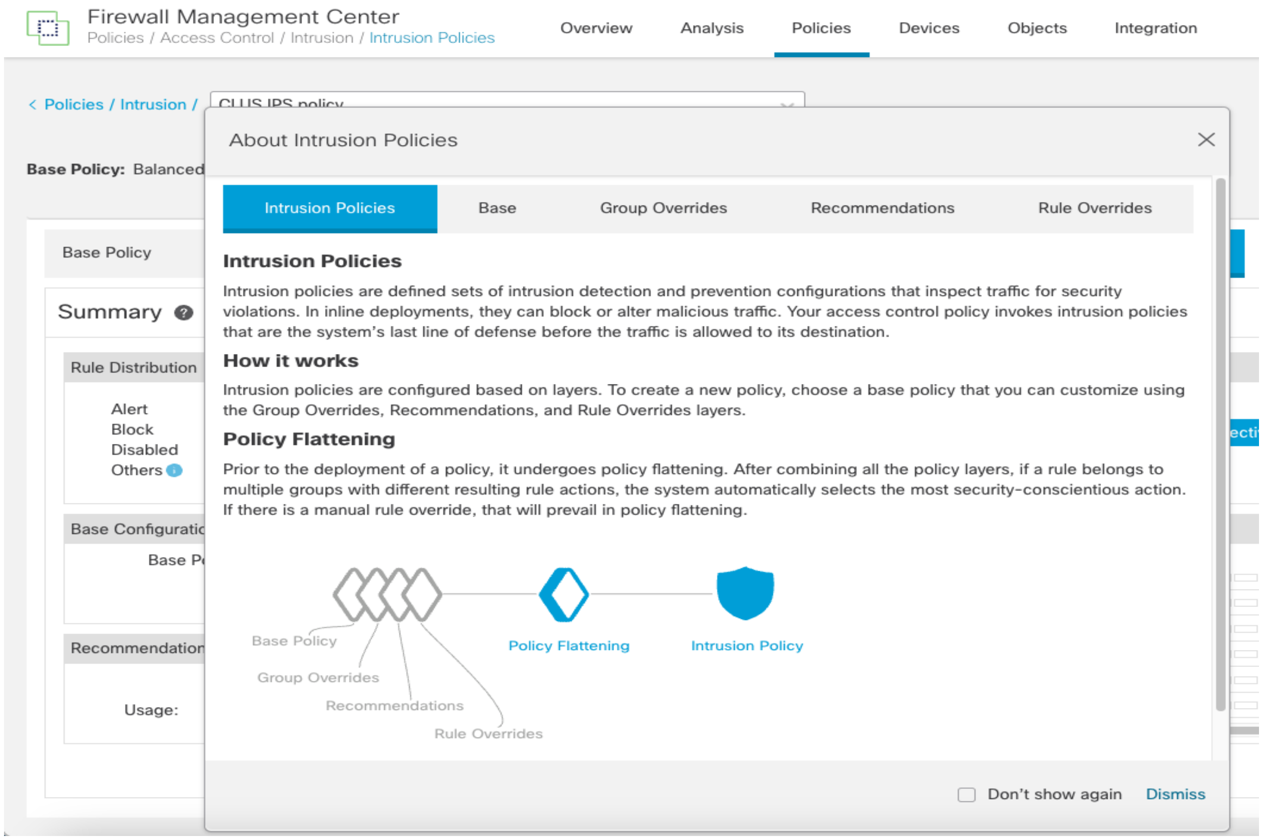
MITRE ATTA&CK & 7.3.0 Release

- New in the 7.3 Release!
  - Content provided by Cisco Talos.
  - Installed as part of Lightweight Security package (LSP).
  - Available for configuration in Intrusion policy.
  - Intrusion Events GUI showcase MITRE group and ATTA&CK Information.

Caveats & Supported Platforms

- Requires Firewall Management Center at v7.3.0.
- Firewalls (NGFW) should be at least v7.0.0.
- Snort3 only.
- Intrusion Policy should be included in AC policy.

Firewall Intrusion Policy



About Intrusion Policies

Intrusion Policies | Base | Group Overrides | Recommendations | Rule Overrides

Intrusion Policies

Intrusion policies are defined sets of intrusion detection and prevention configurations that inspect traffic for security violations. In inline deployments, they can block or alter malicious traffic. Your access control policy invokes intrusion policies that are the system's last line of defense before the traffic is allowed to its destination.

How it works

Intrusion policies are configured based on layers. To create a new policy, choose a base policy that you can customize using the Group Overrides, Recommendations, and Rule Overrides layers.

Policy Flattening

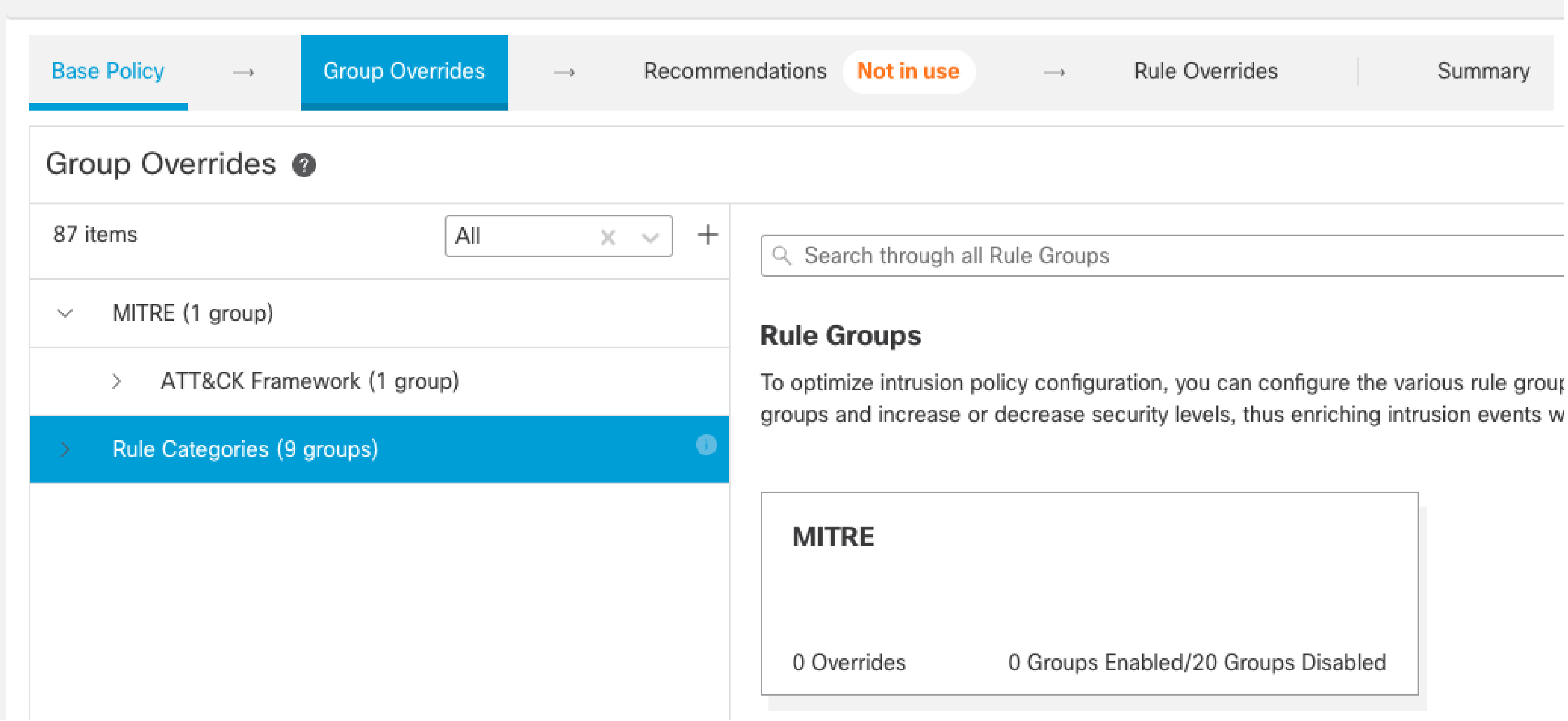
Prior to the deployment of a policy, it undergoes policy flattening. After combining all the policy layers, if a rule belongs to multiple groups with different resulting rule actions, the system automatically selects the most security-conscientious action. If there is a manual rule override, that will prevail in policy flattening.

□ Don't show again Dismiss

MITRE Rule Groups are available as part of Intrusion Policy

- Policies -> Intrusion Policy
- Intrusion Policy Guide

Intrusion Policy – Group Overrides



Base Policy → Group Overrides → Recommendations Not in use → Rule Overrides | Summary

Group Overrides ?

87 items All × ⌄ +

- MITRE (1 group)
  - ATT&CK Framework (1 group)
- Rule Categories (9 groups)

Search through all Rule Groups

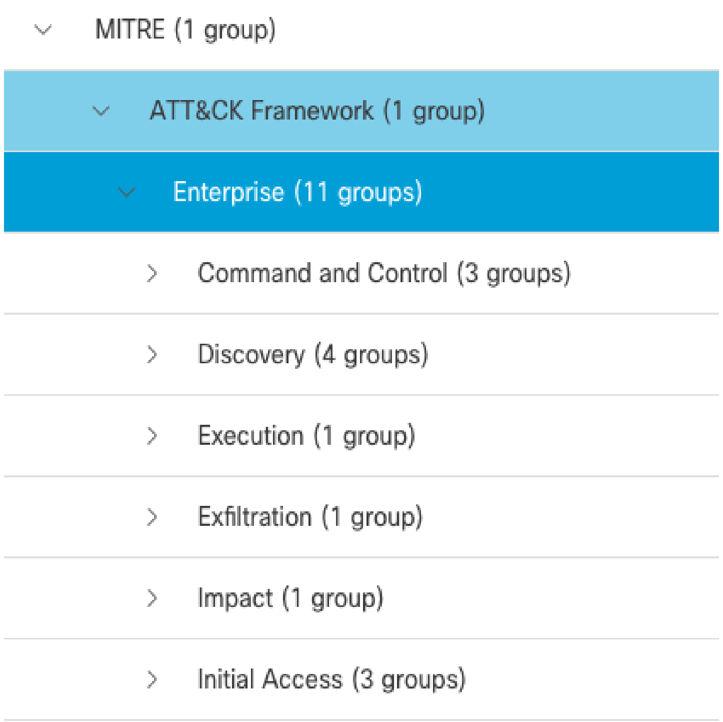
Rule Groups

To optimize intrusion policy configuration, you can configure the various rule grouŗ groups and increase or decrease security levels, thus enriching intrusion events w

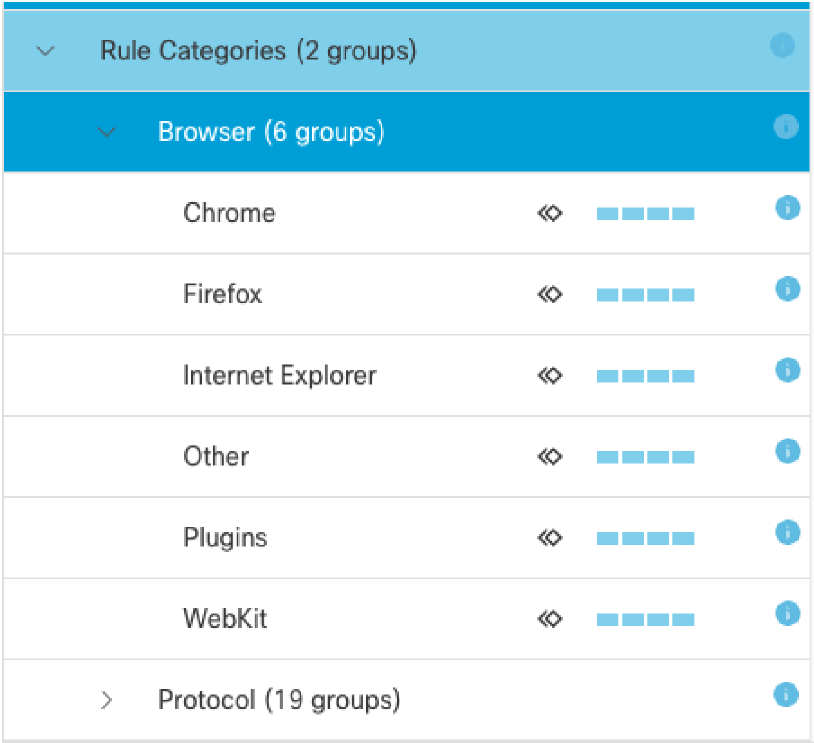
MITRE

0 Overrides 0 Groups Enabled/20 Groups Disabled

Intrusion Policy – MITRE Expanded View



- MITRE (1 group)
  - ATT&CK Framework (1 group)
    - Enterprise (11 groups)
      - Command and Control (3 groups)
      - Discovery (4 groups)
      - Execution (1 group)
      - Exfiltration (1 group)
      - Impact (1 group)
      - Initial Access (3 groups)

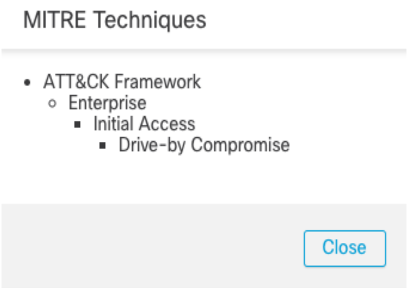


- Rule Categories (2 groups)
  - Browser (6 groups)
    - Chrome
    - Firefox
    - Internet Explorer
    - Other
    - Plugins
    - WebKit
  - Protocol (19 groups)

Intrusion Events

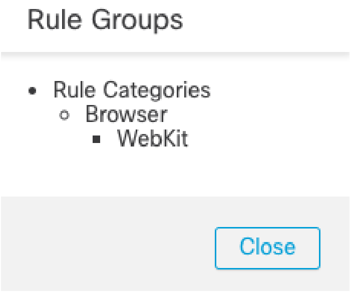
- Analysis →Intrusion → Events

- Two new columns in Intrusion Events
    - MITRE
    - Rule Group
    - Expanded View available



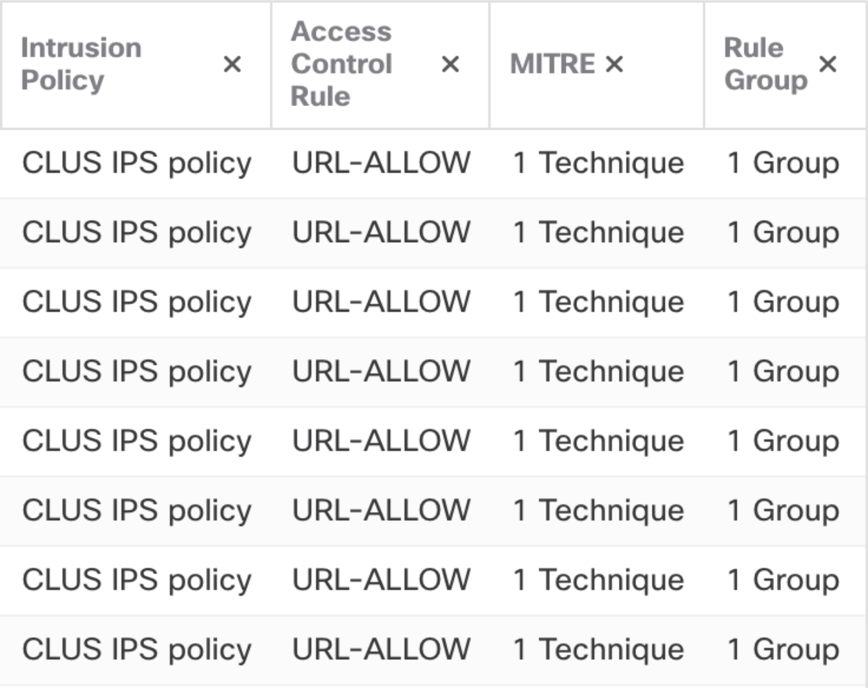
MITRE Techniques

- ATT&CK Framework
    - Enterprise
        - Initial Access
            - Drive-by Compromise



Rule Groups

- Rule Categories
    - Browser
        - WebKit



Intrusion Policy ×	Access Control Rule ×	MITRE ×	Rule Group ×
CLUS IPS policy	URL-ALLOW	1 Technique	1 Group
CLUS IPS policy	URL-ALLOW	1 Technique	1 Group
CLUS IPS policy	URL-ALLOW	1 Technique	1 Group
CLUS IPS policy	URL-ALLOW	1 Technique	1 Group
CLUS IPS policy	URL-ALLOW	1 Technique	1 Group
CLUS IPS policy	URL-ALLOW	1 Technique	1 Group
CLUS IPS policy	URL-ALLOW	1 Technique	1 Group
CLUS IPS policy	URL-ALLOW	1 Technique	1 Group

DEMO

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

The bridge to possible

Thank you

cisco Live!

Let's go

#CiscoLive