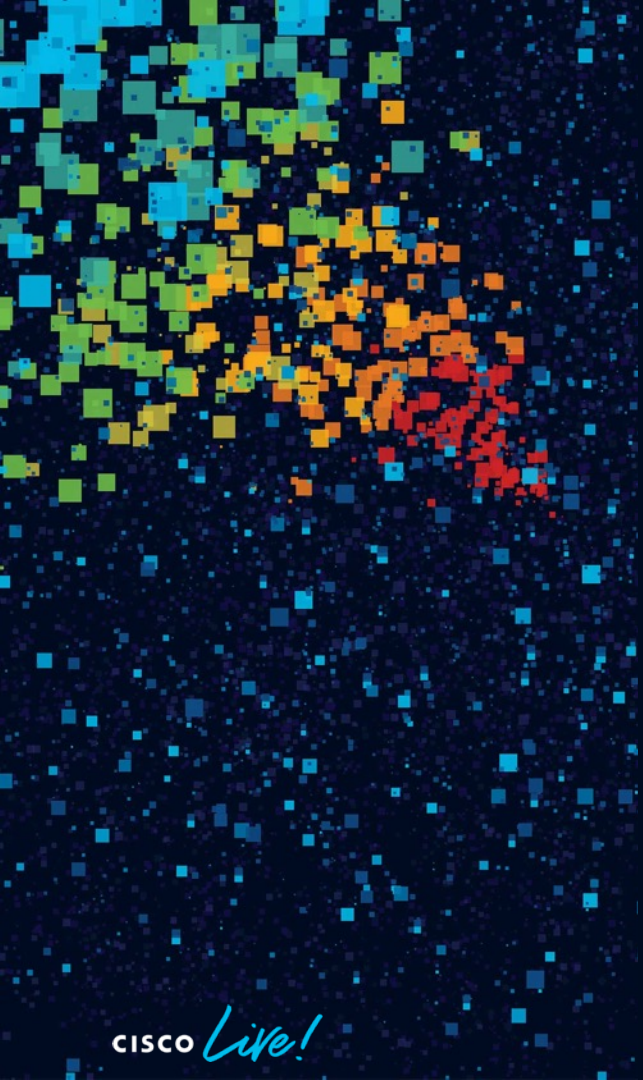
Firepower & Firepower APIs

Part 2: FMC APIs

Security Cisco Live Virtual DevNet Day

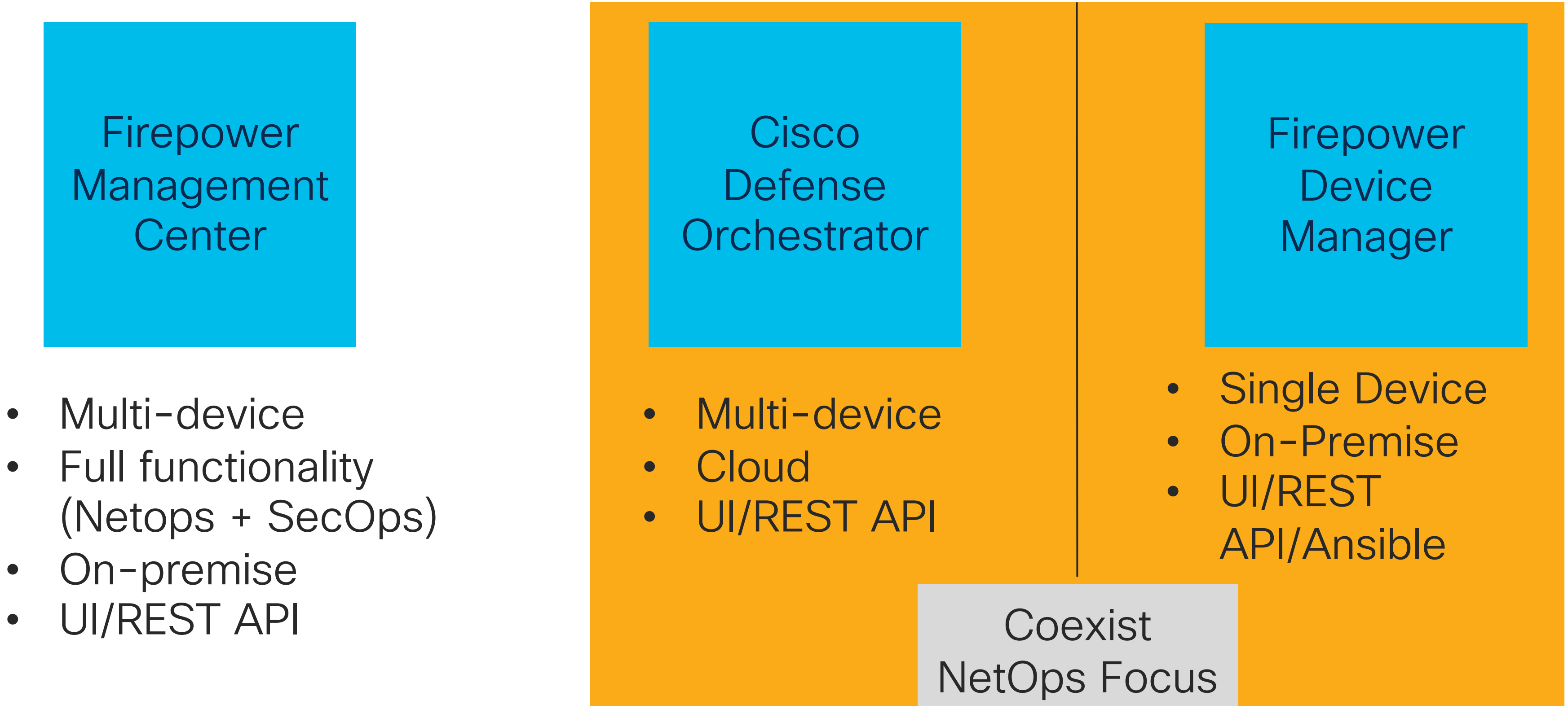
Yatish Joshi, Technical Leader
@tryjoshi



Agenda

- Firepower Management Center
- Features and capabilities
- Threat detection
- Firepower APIs

Firepower Management



Firepower Management Center

- Multi-device
- Full functionality (Netops + SecOps)
- On-premise
- UI/REST API

Cisco Defense Orchestrator

- Multi-device
- Cloud
- UI/REST API

Firepower Device Manager

- Single Device
- On-Premise
- UI/REST API/Ansible

Coexist
NetOps Focus

Firepower Management Center

- Manage NGFWs across Multiple Sites

Centralized management for multi-site deployments

- Multi-domain management
- Role-based access control
- High availability
- API/pxGrid integration
- Analytics

- Firewall and AVC
- Next Generation IPS
- Security Intelligence
- AMP
- Automated Correlation and Remediation

Manage firewalls across many sites | Control access and set policies | Investigate incidents | Prioritize response

Continuous Innovation

6.5 – Fall 2019

- FMC UI – Light Theme
- URL Filtering powered by Talos
- FMCv 300 on VMWare
- ISE SGT tags
- Usability Improvements

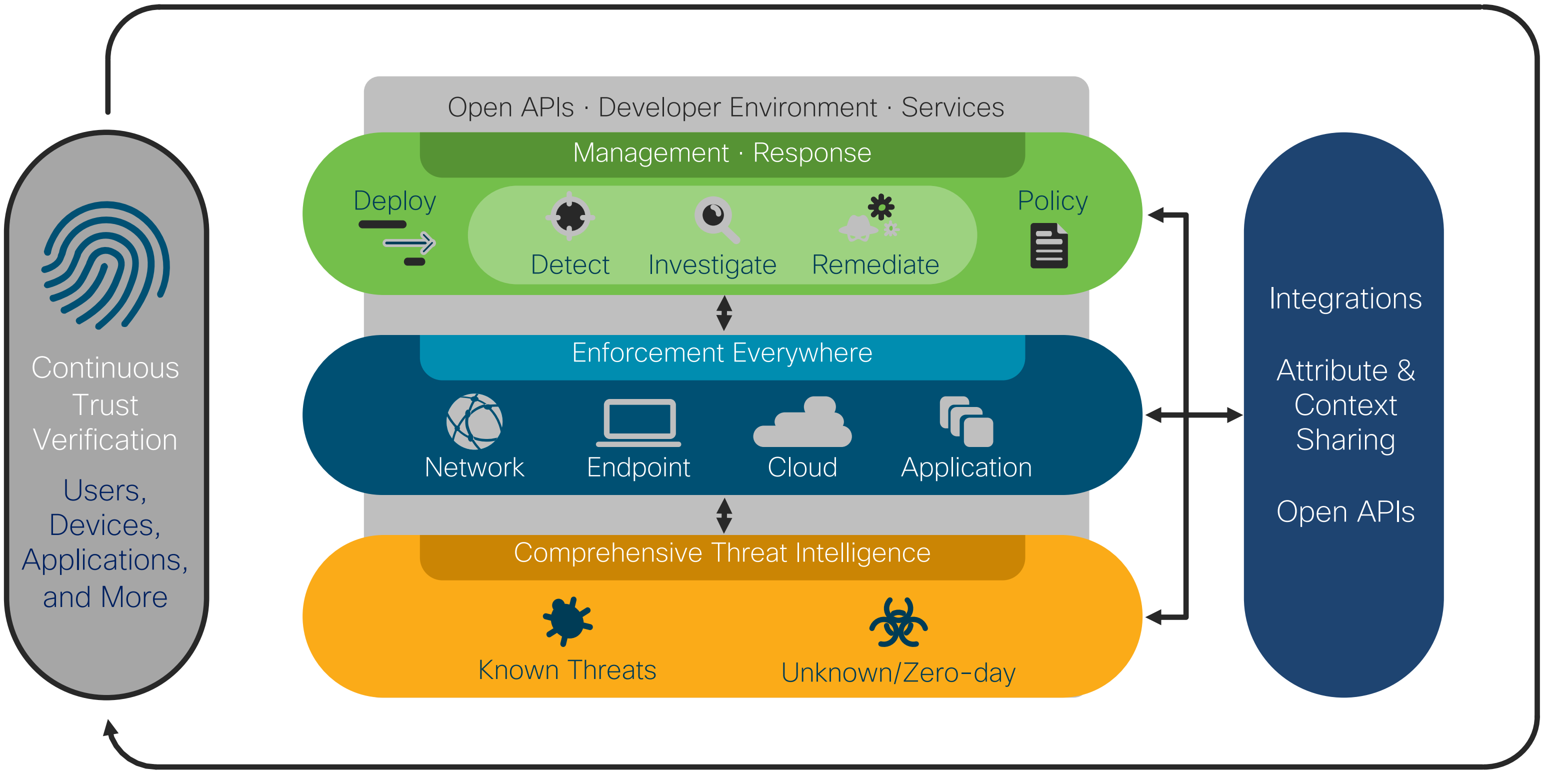
6.6 – Spring 2020

- VRF-Lite support
- Time-based ACLs
- Policy Improvements
- Faster Event Analytics
- Rule life cycle management improvements

For more details head to:
https://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html

Threat Detection

Cisco Security: Integrated Architecture


Continuous Trust Verification
Users, Devices, Applications, and More
Open APIs · Developer Environment · Services
Management · Response
Deploy
Detect
Investigate
Remediate
Policy
Enforcement Everywhere
Network
Endpoint
Cloud
Application
Comprehensive Threat Intelligence
Known Threats
Unknown/Zero-day
Integrations
Attribute & Context Sharing
Open APIs

TALOS- Comprehensive Threat Intelligence

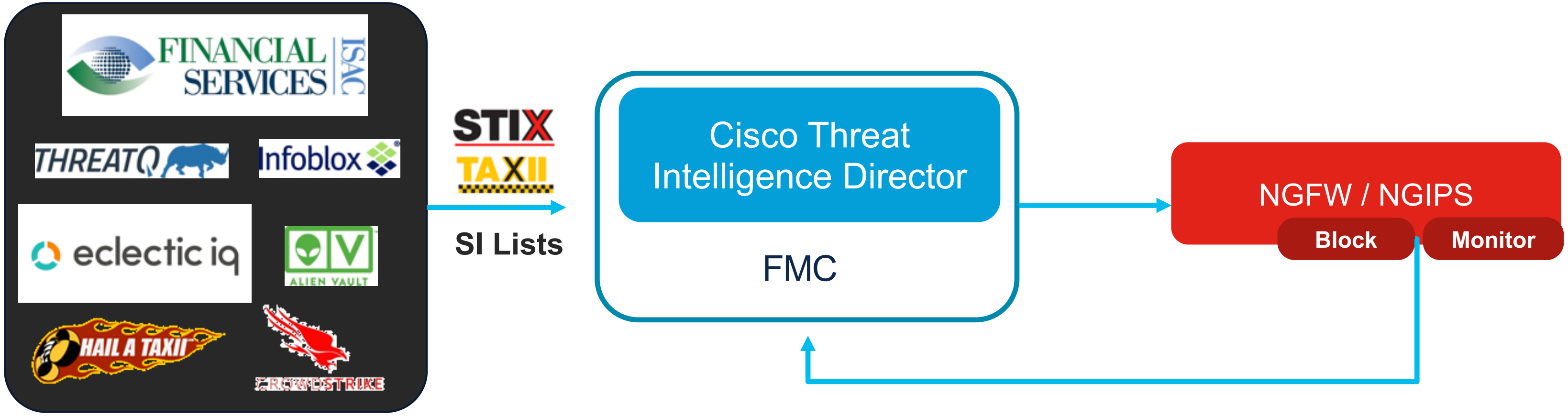
- Powers Cisco Security products with best in breed threat intelligence.
- Responsible for discovering new vulnerabilities and emerging threats.
- Maintains the official rule sets for Snort, ClamAV, Senderbase & Spam Cop.

Notable Spotlights:

- Foscam IP Camera https://blog.talosintelligence.com/2017/11/foscam-multiple-vulns.html
- Disney Circle https://blog.talosintelligence.com/2017/10/vulnerability-spotlight-circle.html
- Nest Cam IQ indoor camera https://blog.talosintelligence.com/2019/08/vuln-spotlight-nest-camera-openweave-aug-2019.html

and many more….

Cisco Threat Intelligence Director (CTID)



Ingest third-party Cyber Threat Intelligence (CTI)

Publish observables to devices

Detect and alert on incidents

- Ability to ingest 3rd party threat intelligence
- Support industry standards
- API Driven and easy to automate workflows

FMC APIs Demo

DevNet & APIs

Developer Resources @CiscoDevNet - https://developer.cisco.com

- Self paced labs
- DevNet Sandboxes (available on demand)

Learning Labs : https://developer.cisco.com/firepower/management-center/

- FMC REST API's Explained
- Modifying Policies with FMC REST APIs
- FMC objects and CRUD operations
- Threat Intelligence Director APIs

and many more!

FMC API Lab

Aim: Leverage FMC API to create an intelligence source and import threat intelligence into the FMC.

Lab Link: https://developer.cisco.com/learning/lab/firepower-restapi-111/step/1

FMC API Use Cases

Augment firewall contextual data

Automate firewall configuration

Host discovery

Manipulate objects

Vulnerability analysis

Change policy

More accurate IPS recommendations

Deploy configuration

Thank you

Possibilities

#CiscoLive | #DevNetDay