cisco The bridge to possible

Splunk+Firewall

Best practices to visualize and operationalize security events using APIs

Gregg Berson, Engineering Leader

cisco Live!

DEVNET-2245

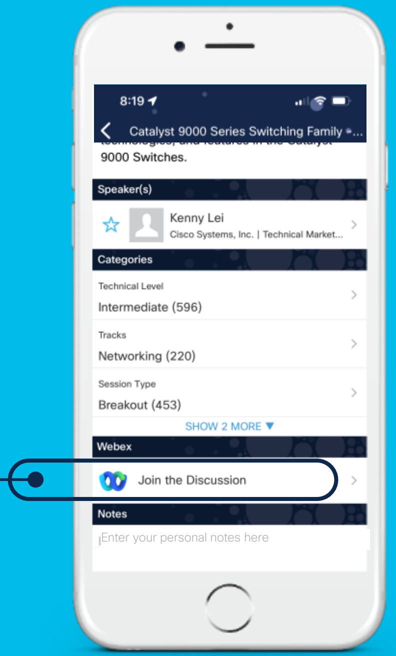
Cisco Webex App

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



8:19

Catalyst 9000 Series Switching Family ...

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

Webex spaces will be moderated
until February 24, 2023.

Agenda

- Firewall Threat Defense Introduction
- Cisco Secure eStreamer Client Add-On
- Cisco Threat Intelligence Director
- Integrating Splunk+Firewall
- Demo
- Conclusion

Firewall Management Center

Manage Firewall Threat Defense across Multiple Sites

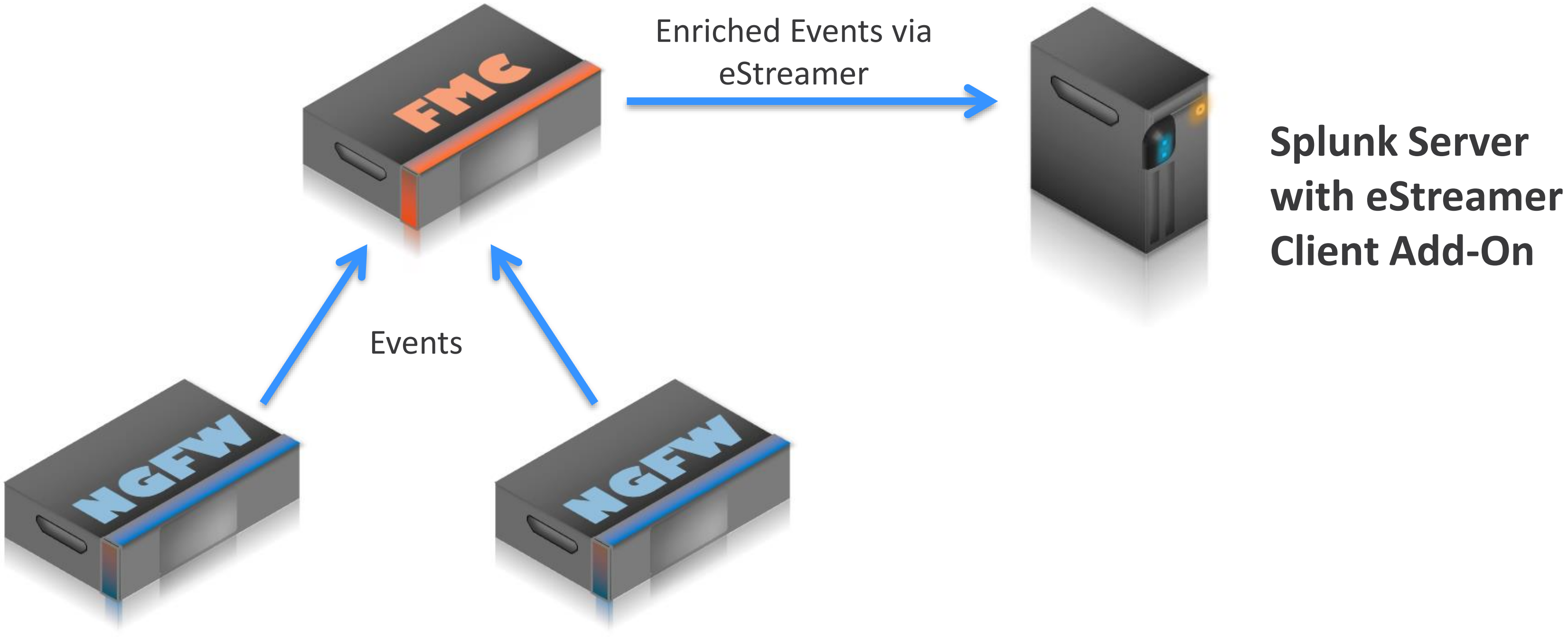
Centralized management for multi-site deployments

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

- Firewall and AVC
- NGIPS
- Security Intelligence
- AMP
- Automated Correlation and Remediation

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

NGFW Deployment with Splunk



Splunk Server with eStreamer Client Add-On

Cisco Secure eStreamer Client Add-On

- eStreamer allows users to stream events from their FMC to external clients
- Supported event types:
  - Network Connections
  - Intrusions with Packets
  - Malware and File
  - Correlation
  - More
- Cisco Secure eStreamer Client Add-on for Splunk
  - eStreamer client that supports Splunk (CIM format)
  - Version 5.1.0 now available
  - Link to the Splunk Add-on: https://splunkbase.splunk.com/app/3662/

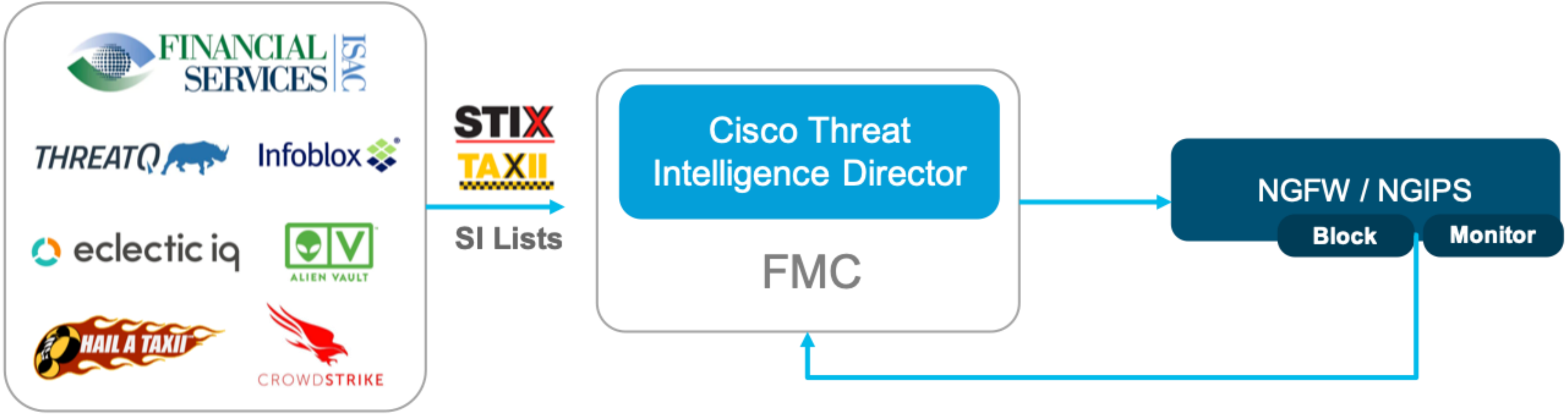
Threat Intelligence Director

> *“More intelligence sources become available everyday, but products that are expected to provide utility from that intelligence aren’t evolving to operationalize it”*

- Security groups need the following in a product:
  - Ability to ingest threat intelligence from a wide variety of sources
  - Operationalize the intelligence
  - Complex correlation and analysis on detected events
  - Automatable with well defined APIs

Our answer?

Cisco Threat Intelligence Director (CTID)



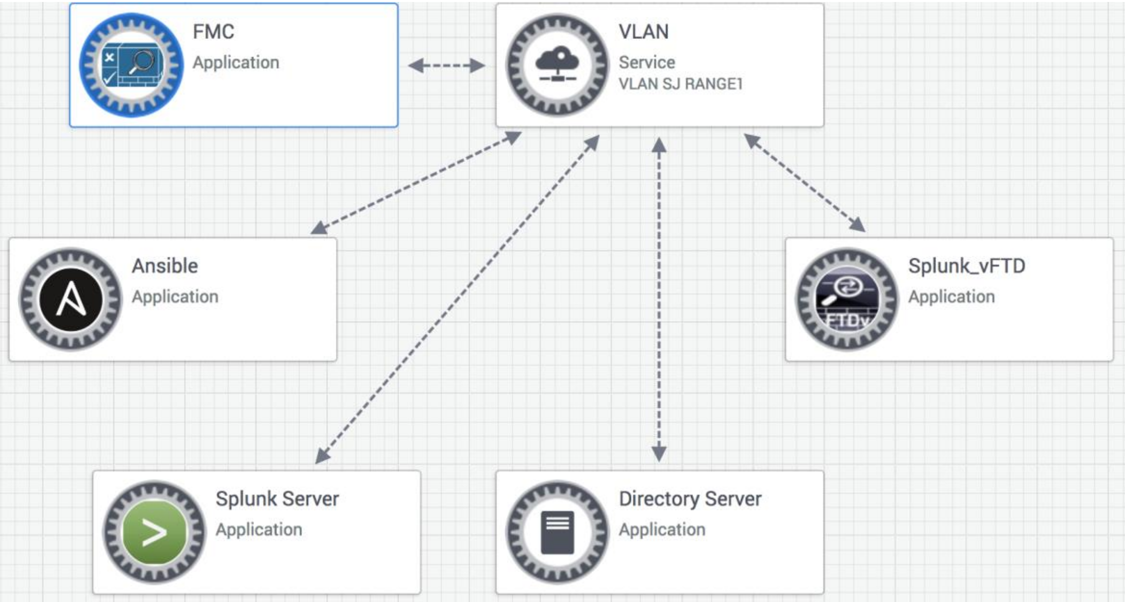
Step 1
Ingest third-party Cyber Threat Intelligence (CTI)

Step 2
Publish observables to sensors

Step 3
Detect and alert on incidents

Splunk+Firewall Lab

Integrating Splunk+Firewall Lab



Sandbox

https://devnetsandbox.cisco.com/RM/Diagram/Index/2dc005dc-a5bf-4b44-8ae2-074d61076b50?diagramType=Topology

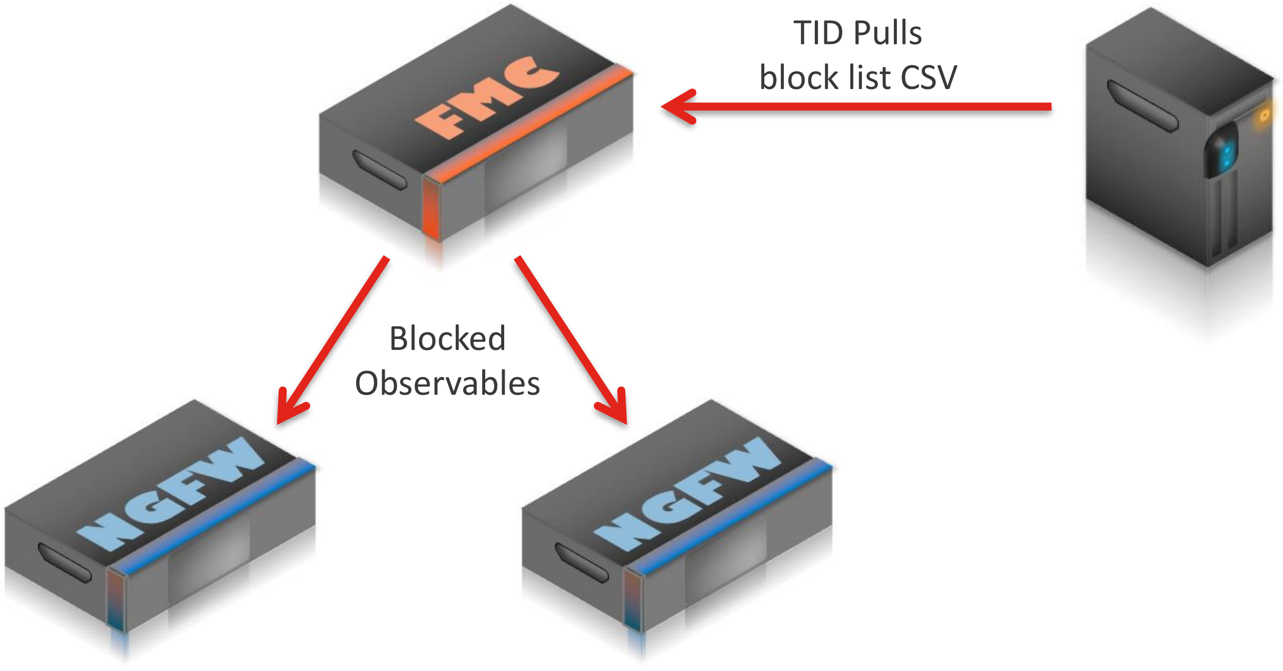
Learning Lab

https://learninglabs.cisco.com/lab/firepower-estreamer-splunk/step/1

Demo

Recap

Blocking Observables from Splunk



TID Pulls
block list CSV

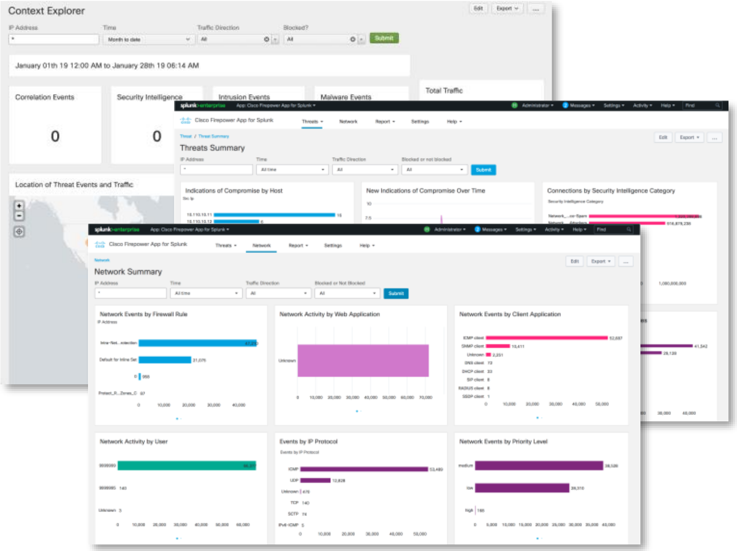
Blocked
Observables

Splunk Server with eStreamer Client Add-on

Splunk+Firepower – Demo Overview

1. Enhanced the functionality of Firewall Splunk app
2. Modified Splunk app to block observables
3. Demoed Threat Intelligence Director (TID)
4. Demonstrated block IPs on Firewall Threat Defense from Splunk

Cisco Secure Firewall App for Splunk


Context Explorer
January 01th 19 12:00 AM to January 28th 19 06:14 AM
Correlation Events
Security Intelligence
Intrusion Events
Malware Events
Total Traffic
Location of Threat Events and Traffic
Cisco Firepower App for Splunk
Threats Summary
Indications of Compromise by Host
New Indications of Compromise Over Time
Connections by Security Intelligence Category
Network Summary
Network Events by Firewall Rule
Network Activity by Web Application
Network Events by Client Application
Network Activity by User
Events by IP Protocol
Network Events by Priority Level

- Version 1.7.0 released
- Major Features:
  - Threat Summary Dashboard
    Advanced Impact Event analysis with directionality
  - Network Event data dashboard with IoCs and Firewall Rule usage (Allow/Block)
  - Context Explorer with Geo-location Map
  - Link back to FMC for File Trajectory and Host Profiles
  - Filters for CIDR Blocks and Allow/Block Rule actions

https://splunkbase.splunk.com/app/4388/

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the " Attendee Dashboard” at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

- Visit the Cisco Showcase for related demos.
- Book your one-on-one Meet the Engineer meeting.
- Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

The bridge to possible

Thank you

cisco Live!

ALL IN