cisco Live!

#CiscoLive

cisco The bridge to possible

eStreamer or Syslog

Which one to choose for Firewall Security Events
Part 2– Interactive Demo

Seyed Khadem, Technical Solutions Architect, CSTA
Dinkar Sharma, Technical Marketing Engineer, CSTA
@Seyed54119008, @Dinkar88

BRKSEC-2125

Cisco Webex App

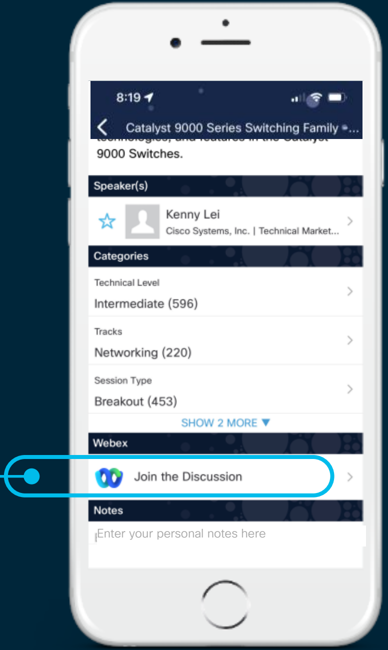
Questions?

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 17, 2022.



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

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2125

CISCO Live!

Demo: Lab

Introduction

Seyed Khadem

- 15+ years as a developer, 4 years at Cisco
- Current Fav programming language: Python, PHP fan
- Part Developer, part evangelist, part security analyst

- Hobbies
  - Video Games
    - Civ, Minecraft, Star Wars
  - Skiing
  - Books
    - Stormlight Archive
    - Name of Wind
    - Wheel of Time

Why SIEM?

- Operational Intelligence for the customer, single pane of glass for all security events
- Mesh Cisco data with a diverse ecosystem of devices and network interfaces
- Streamline Incident Management and make real-time decisions
- Search at scale, create custom dashboards, alerts and reporting
- Automate the security management process
- Offload data to central focal point for compliance asset inventory

Cisco Integration Products

- Splunk
  - Supports both eStreamer and Syslog data ingest
    - Cisco Firepower App for Splunk (Analytics) - https://splunkbase.splunk.com/app/4388/
    - Cisco Firepower eStreamer App (Technical Add-On) - https://splunkbase.splunk.com/app/3662/
- Arcsight
  - https://github.com/CiscoSecurity/fp-05-firepower-cef-connector-arcsight
- Sentinel Connector
  - CEF based, future integration with JSON
  - https://docs.microsoft.com/en-us/azure/sentinel/data-connectors-reference
- Partner Products
  - Qradar - IBM Supported DSM
  - https://www.ibm.com/docs/en/dsm?topic=cisco-firepower-management-center

Cisco eStreamer enCore client (eStreamer CLI)

- Python 3, Install on Linux (RHEL 7&8, Ubuntu, CentOS)
- Core Application behind all SIEM integration products
- Supports Multiple output formats
  - CEF, JSON, and Key Value Pair (Splunk)
- Enriches Record Metadata into single events vs direct output provided by eStreamer
- eStreamer eNcore Client
  - https://github.com/CiscoSecurity/fp-05-firepower-cli

Client Configuration

- More than 50 different configuration parameters, details available at
  - https://www.cisco.com/c/en/us/td/docs/security/firepower/70/api/eNcore/eNcore_Operations_Guide_v08.html - Section 6.x
  - Main decisions, output format? CEF, Splunk, JSON? Filter Events? Logging Level? Log Policy?
- CPU and Worker Thread Sizing Chart
  - Expected volume? 95% of Firepower data are connection events

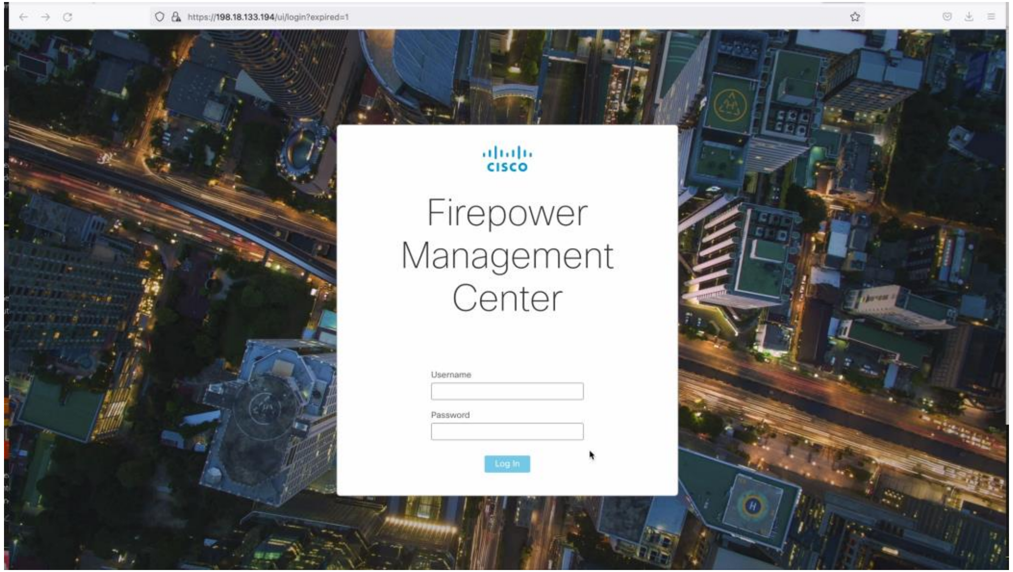
Event Rate (per second)	Worker Threads	Batch Size (recommended)
Less than <2000	1	2
2000-4000	4	100 (default)
4000-6000	8	250
8000+	12	500

Case Study - Getting Data In with Splunk

- Cisco Firepower Splunk App - https://splunkbase.splunk.com/app/4388/
- Cisco Firepower Technical Add-On for eStreamer - https://splunkbase.splunk.com/app/3662/
- Syslog
  - Install Analytics App for CIM Normalization
  - Configure FMC to send data to Splunk via port 514
- eStreamer
  - Setup client certificate
  - Configure estreamer client
  - Run Test & Start Commands
    - Youtube setup eStreamer Splunk (> 12min)
    - https://www.youtube.com/watch?v=pEXM5PVkvH8&feature=youtu.be

Live Demo – How do we get data into Splunk?

Use Case #1 : My organization wants to use Firepower eStreamer protocol to ingest additional telemetry available on IPS events. What steps are involved?

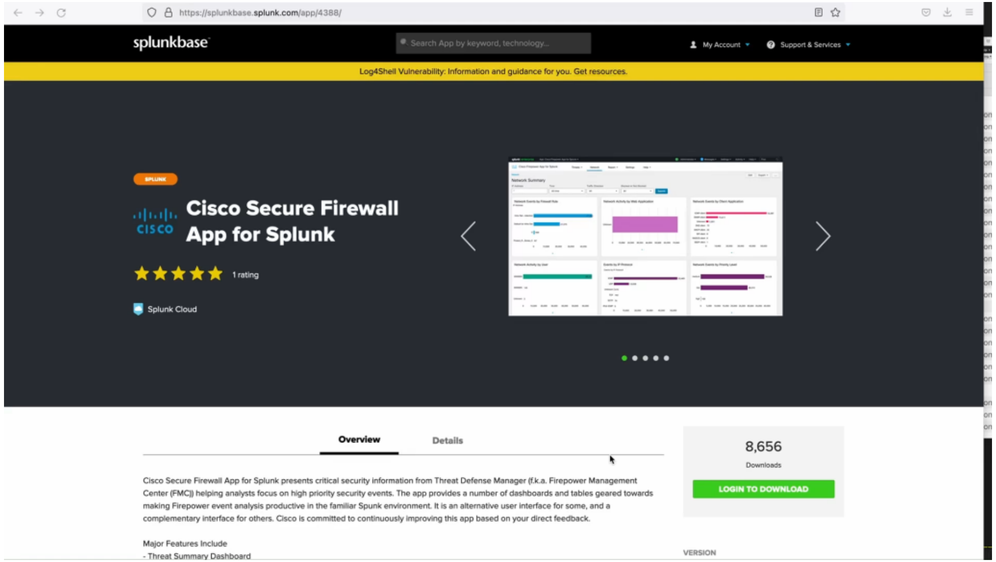


https://198.18.133.194/ui/login?expired=1

Firepower Management Center

Live Demo – IPS Impact Levels

Use Case #2 : How many Impact Level 1 Intrusion Events have been detected within the last 24 hours? How many were not blocked by current Firepower rule set and what is the impact to the organization?



Log4Shell Vulnerability: Information and guidance for you. Get resources.

Cisco Secure Firewall App for Splunk

Overview | Details

8,656 Downloads

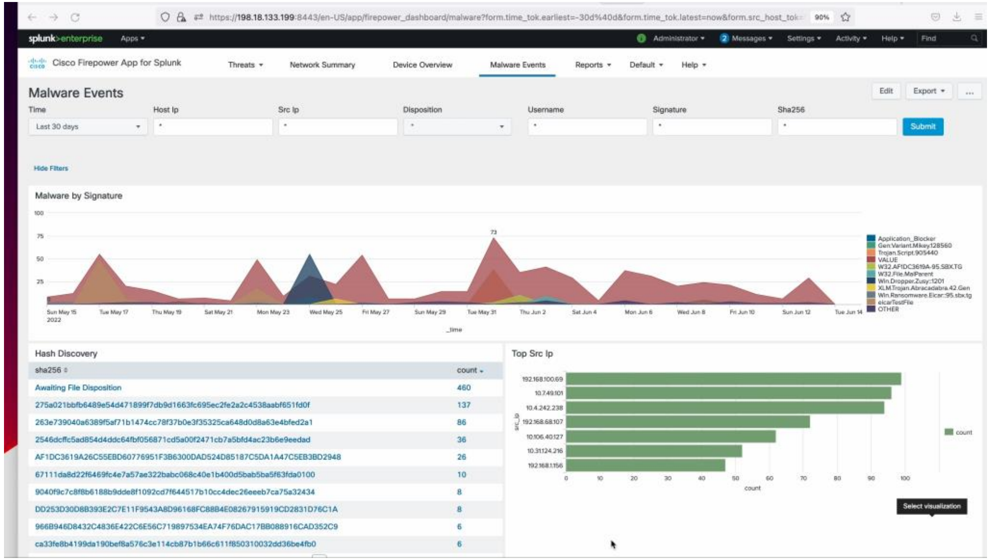
Cisco Secure Firewall App for Splunk presents critical security information from Threat Defense Manager (f.k.a. Firepower Management Center (FMC)) helping analysts focus on high priority security events. The app provides a number of dashboards and tables geared towards making Firepower event analysis productive in the familiar Spunk environment. It is an alternative user interface for some, and a complementary interface for others. Cisco is committed to continuously improving this app based on your direct feedback.

Major Features Include
- Threat Summary Dashboard

VERSION

Live Demo - Cross Product Correlation in Splunk

- Use Case #3 : What is the AMP reputation score of network malware events discovered in Firepower? What is the network traceability of those devices and what internal hosts are affected?



https://198.18.133.199:8443/en-US/app/firepower_dashboard/malware?form.time_tok.earliest=-30d%40d&form.time_tok.latest=now&form.src_host_tok=

Malware Events

Time: Last 30 days

Host Ip: *

Src Ip: *

Disposition: *

Username: *

Signature: *

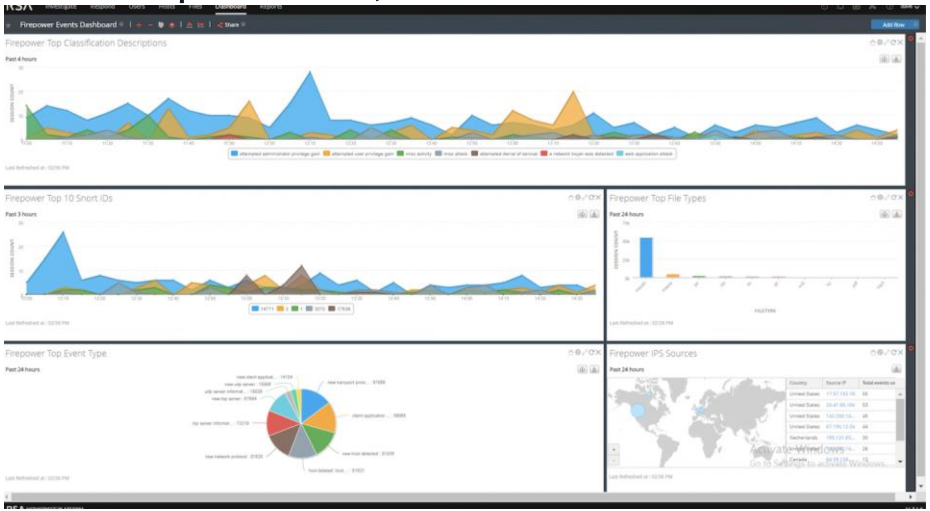
Sha256: *

Hash Discovery

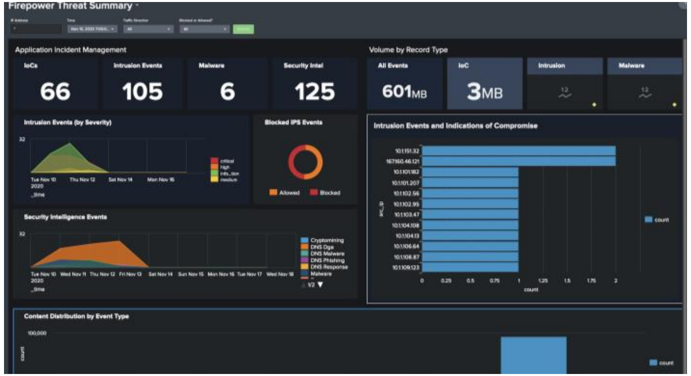
sha256	count
Awaiting File Disposition	460
275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f	137
263e739040a6389f5af71b1474cc78f37b0e3f35325ca648d0d8a63e4bfed2a1	86
2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad	36
AF1DC3619A26C55EBD60776951F3B6300DAD524D85187C5DA1A47C5EB3BD2948	26
67111da8d22f6469fc4e7a57ae322babc068c40e1b400d5bab5ba5f63fda0100	10
9040f9c7c8f8b6188b9dde8f1092cd7f644517b10cc4dec26eeeb7ca75a32434	8
DD253D30D8B393E2C7E11F9543A8D96168FC88B4E08267915919CD2831D76C1A	8
966B946D8432C4836E422C6E56C719897534EA74F76DAC17BB088916CAD352C9	6
ca33fe8b4199da190bef8a576c3e114cb87b1b66c611f850310032dd36be4fb0	6

What’s Next?

- FMC 7.2-7.4+ enhanced eStreamer interface with built in enrichments
- New Splunk UI, Netwitness Partnership, Enhancements to Sentinel



RSA Netwitness



Dark Theme UI

Contact Us

Email: encore-community@cisco.com

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

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

cisco Live!

#CiscoLive