

CISCO *Live!*



#CiscoLive



The bridge to possible

Threat Centric Network Security

Cisco Firepower NGFW Solutions

Ted Bedwell – Distinguished Engineer

@tedbedwell

BRKSEC-2480



#CiscoLive



- I live within a one hour drive from Washington D.C. and Baltimore Maryland
- 18+ Years building Network Security Products
- Before that I was a backbone engineer for a multi-national datacenter company (aka BGP Jockey)

Cisco Webex App

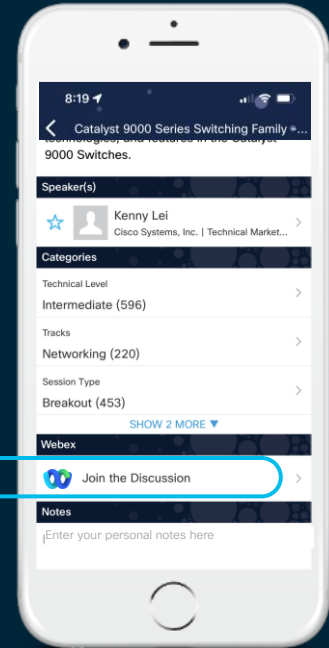
Questions?

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

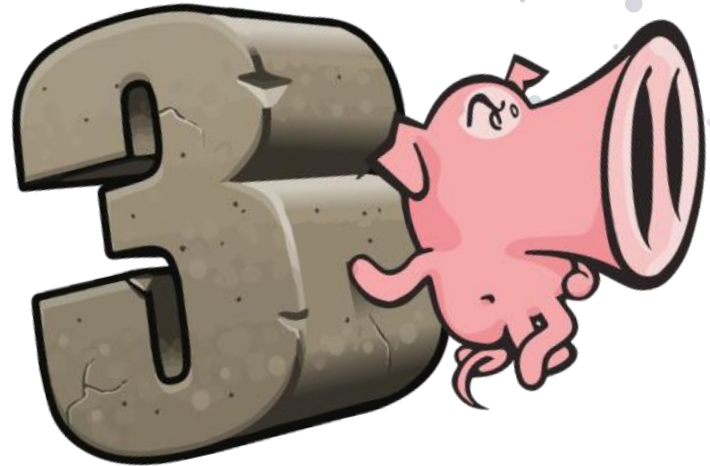
Webex spaces will be moderated by the speaker until June 17, 2022.



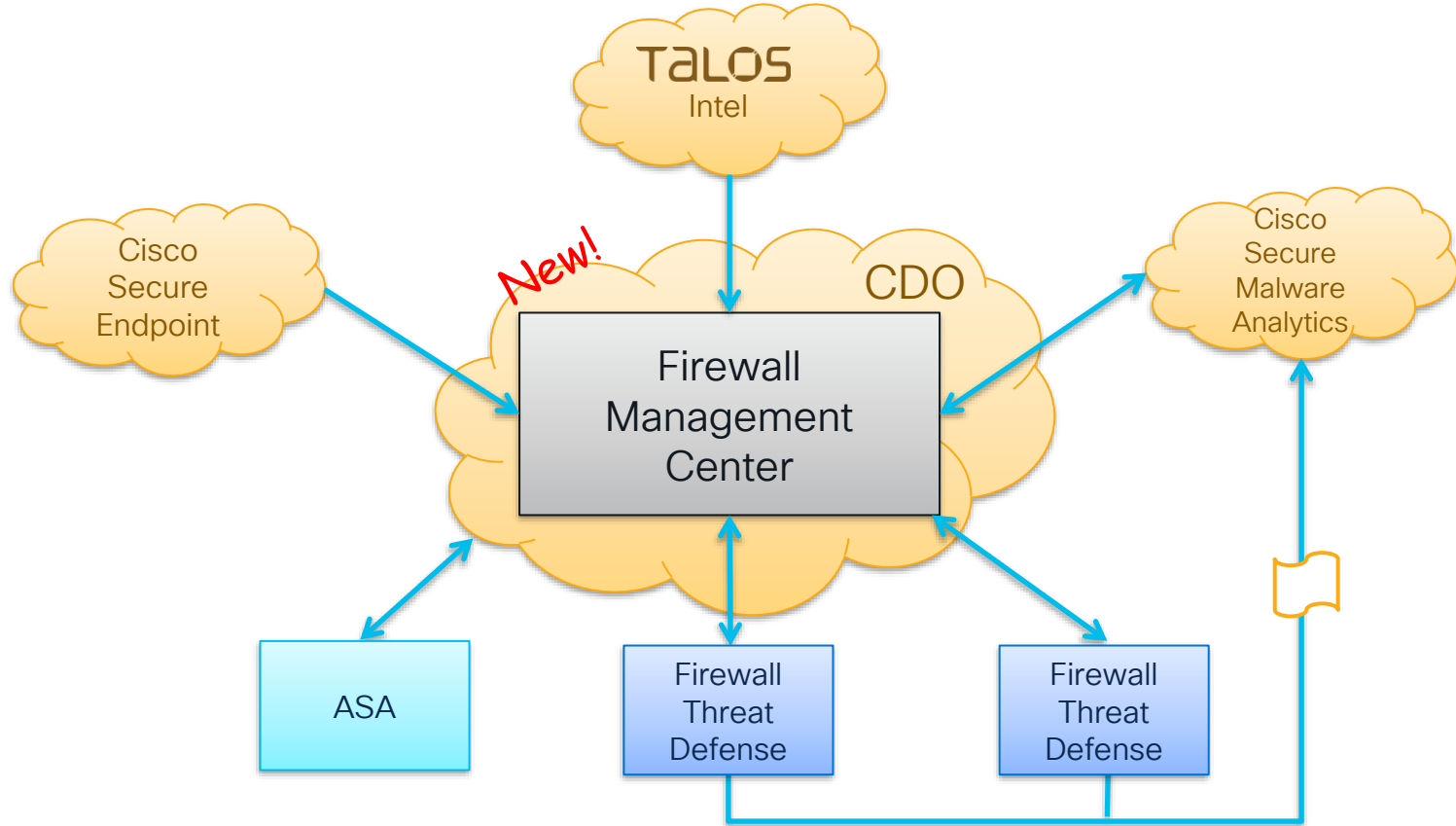
<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2480>

Agenda

- Secure Firewall Solution Introduction
- Secure Firewall Threat Technology Lightning Survey
- Snort 3 – What's it all about?
- Cisco Threat Intelligence Director
- Q&A

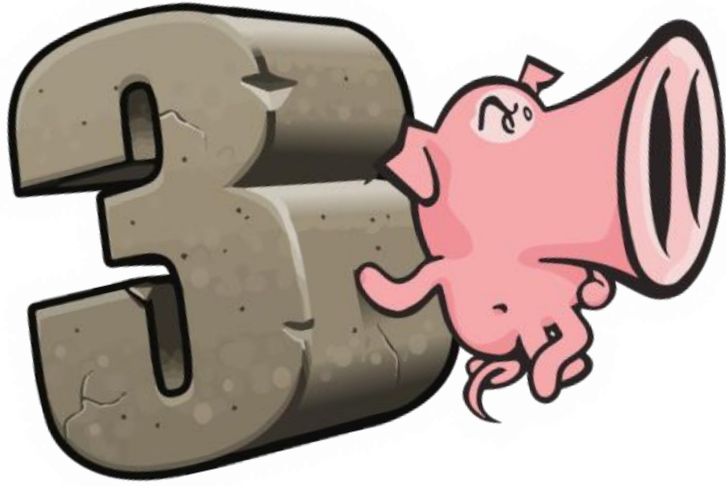


Secure Firewall Solution

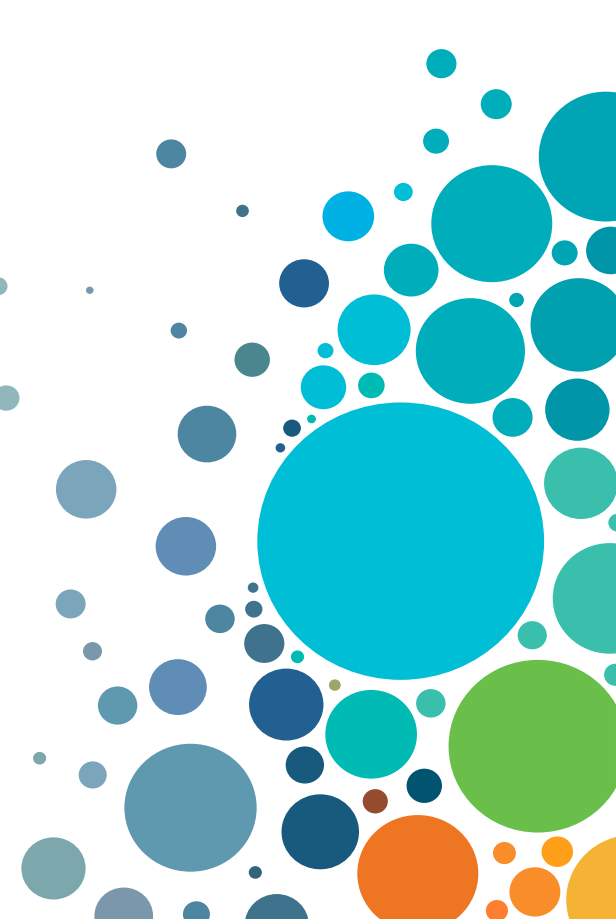


Firepower Threat Technologies

- IPS – Protocol Aware Deep Packet Inspection
- Security Intelligence – Categorized Indicators from Talos
- URL Filtering – Threat categorizations from Talos
- Advanced Malware Protection (AMP) for Networks
- Real-time Network Awareness & Indications of Compromise



What's it all about?



What is Snort?

It is an open source intrusion prevention system capable of real-time traffic analysis and packet logging.

With over 5 million downloads and over 600,000 registered users, it is the most widely deployed intrusion prevention system in the world.

snort.org



“This program is meant to be a packet logger but is useful for other things. As a packet logger, it can become sort of a "poor man's Intrusion Detection System" in that you can collect traffic of interest for later (manual) examination. It can also function as just a packet plane sniffer, decoding IP, TCP, UDP, ICMP and ARP traffic...

Snort 0.96 - README

Martin Roesch - December 21, 1998

1998...lets set the stage.

- 168 dog years ago
 - (Everyone knows Internet Years are even shorter than dog years)
- Cisco ships it's thousandth GSR 12000
- AOL 4.0 launched using ALL of the world's CD production capacity for several weeks.
- Nintendo 64 & Game Boy Color were the must have Christmas Gifts!
- The biggest baddest Intel® processor available was the Pentium® II Xeon
 - Running at 450Mhz
 - Supporting dual-processor Servers!



What is Snort?

It is an open source intrusion prevention system capable of real-time traffic analysis and packet logging.

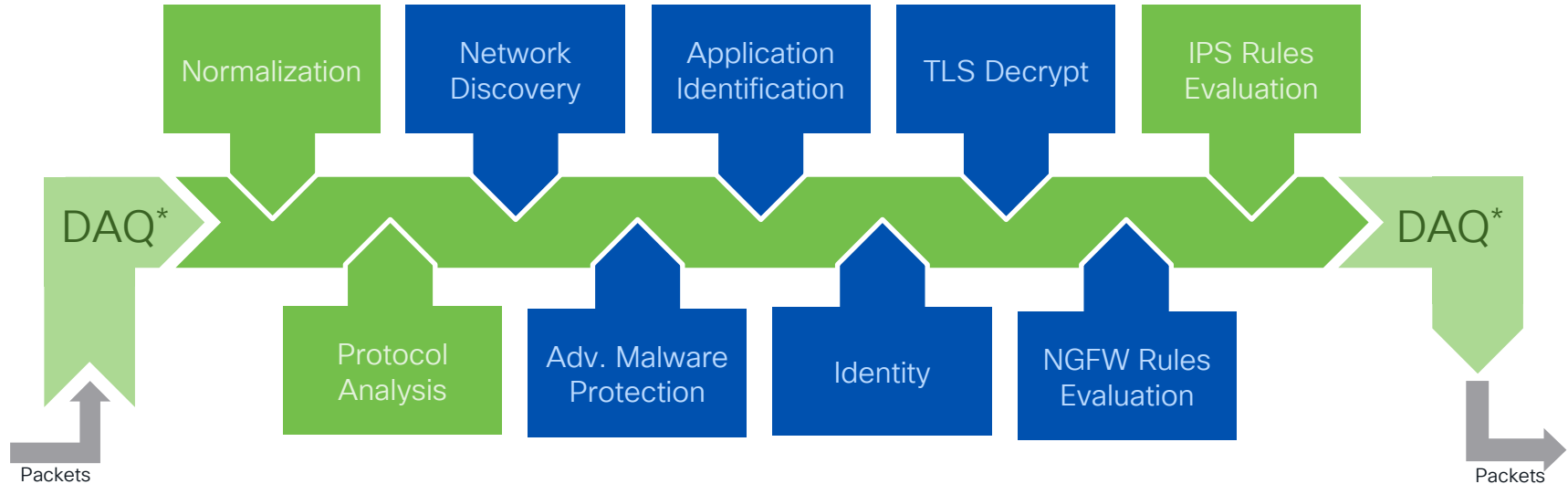
With over 5 million downloads and over 600,000 registered users, it is the most widely deployed intrusion prevention system in the world.

snort.org

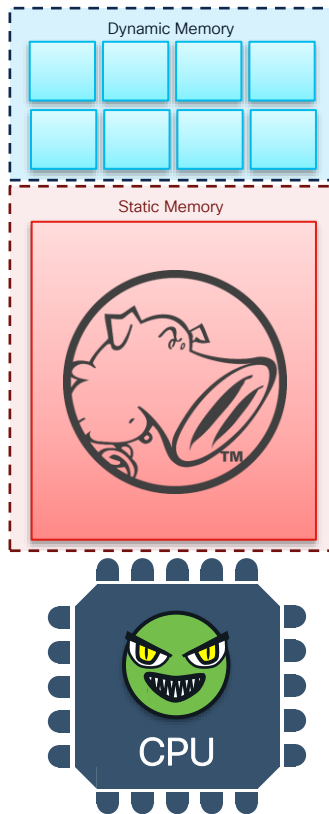


In Reality...

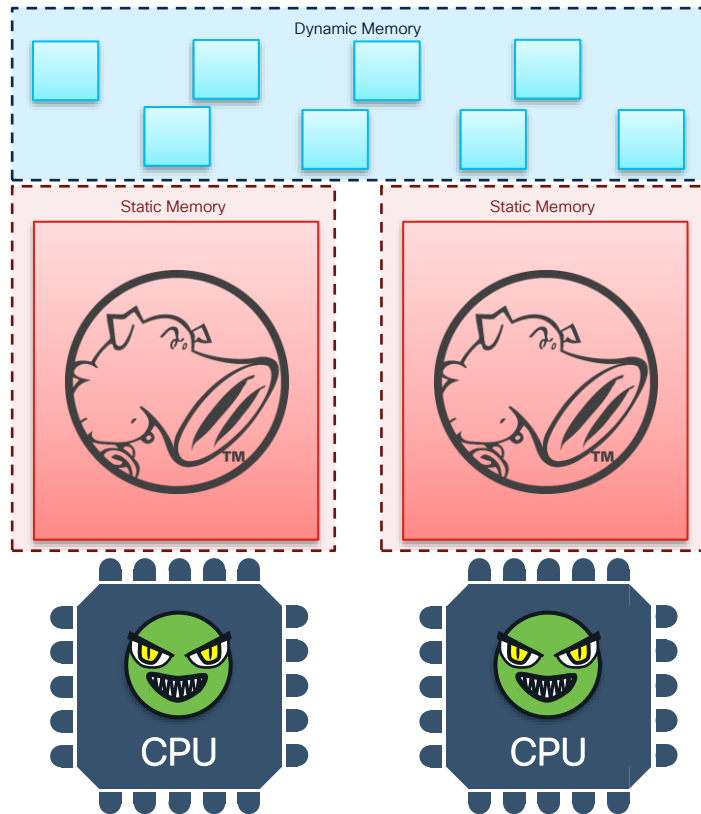
...Snort is a flexible high-performance packet processing engine



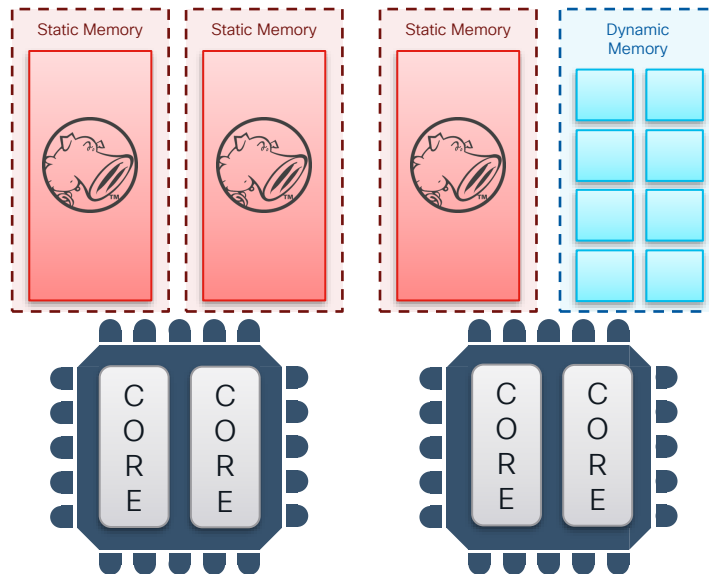
Snort Architectural Evolution



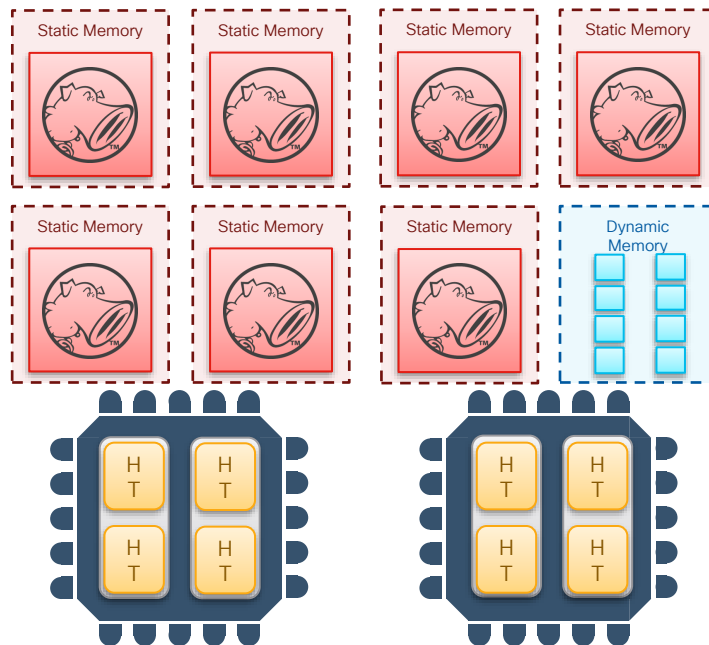
Snort Architectural Evolution



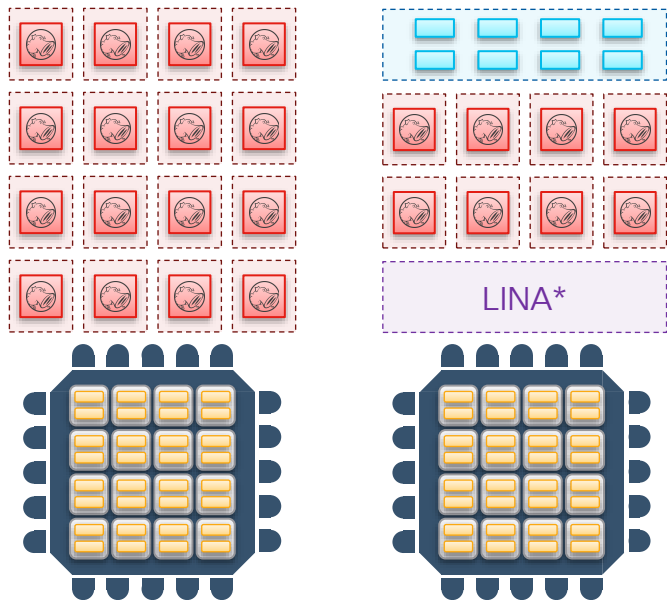
Snort Architectural Evolution



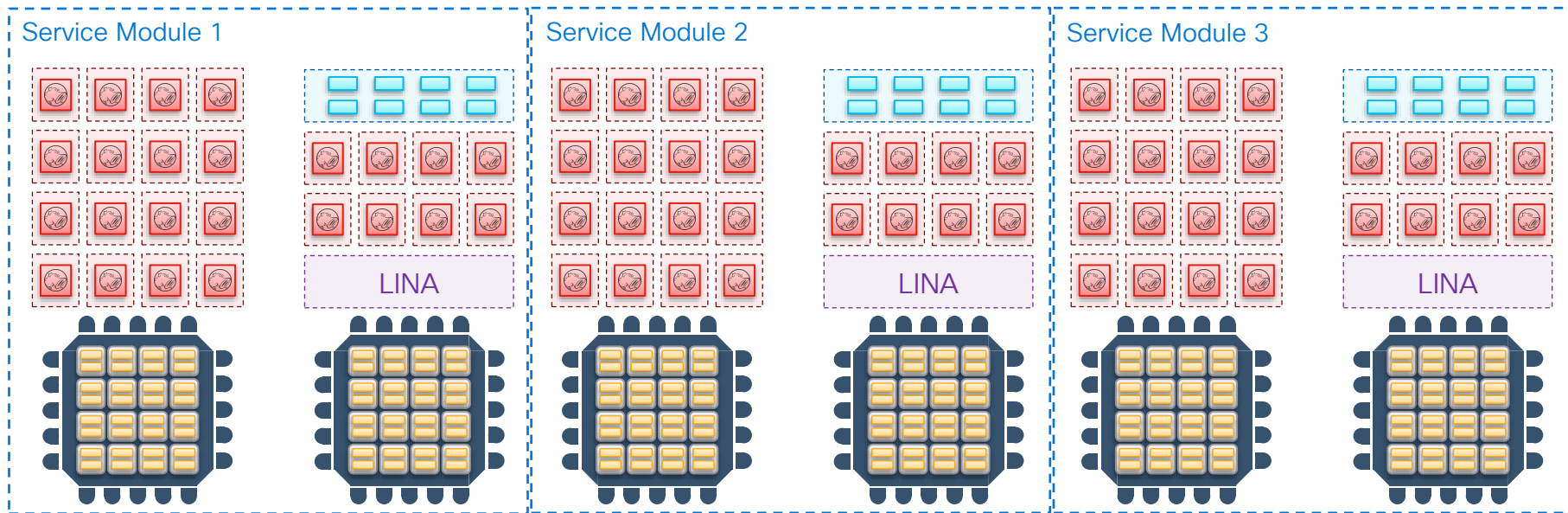
Snort Architectural Evolution



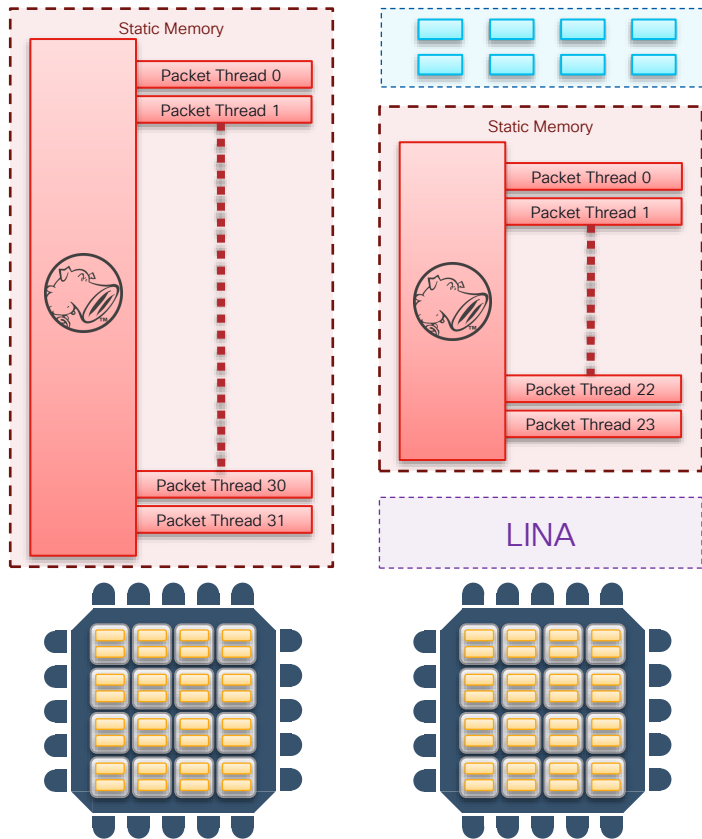
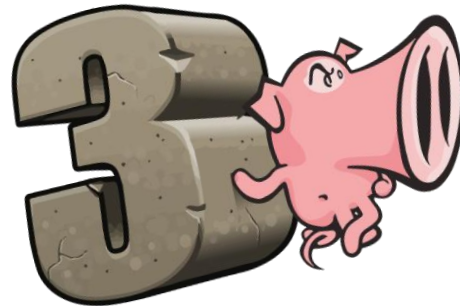
Snort Architectural Evolution



Snort Architectural Evolution



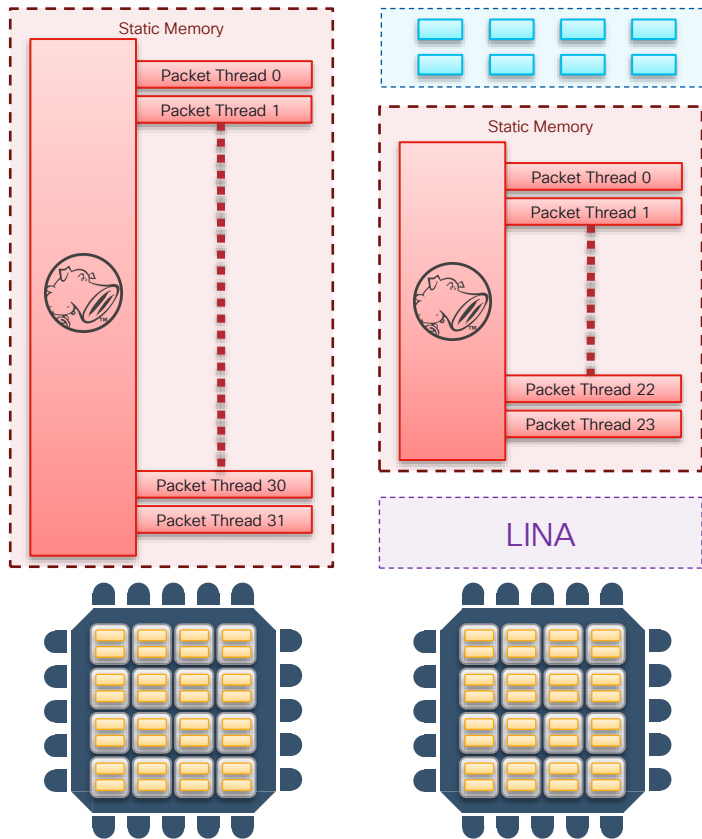
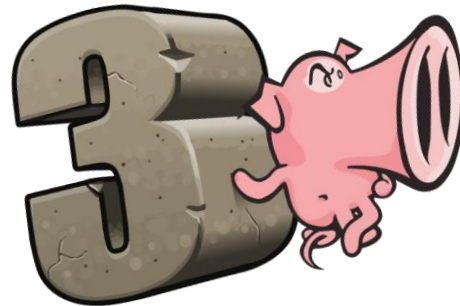
Snort 3 to the Rescue!!!



Re-architecture leads to much improved resource utilization

- More rules per instance
- Deeper inspection depth
- Larger caches = reduced churn

Snort 3 to the Rescue!!!



TL;DR

“The latest generation of multi-core Secure Firewall platforms will get greater threat efficacy and scalability through software alone”

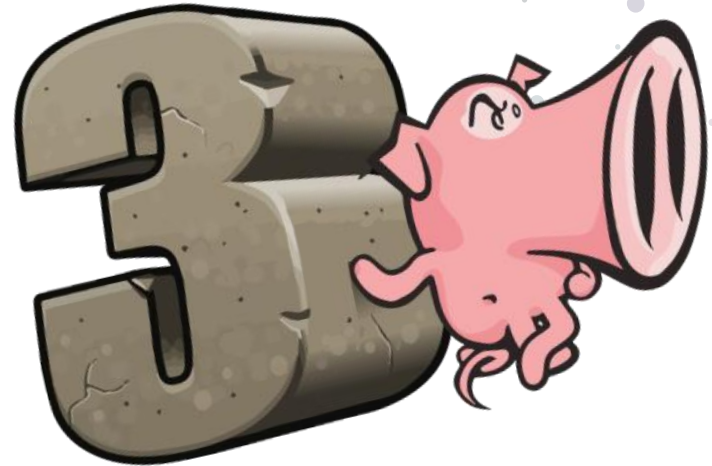
Available now in all releases ≥ 7.0 !

Open Source Available to Everyone Today

<http://snort.org/snort3>

Agenda

- Secure Firewall Solution Introduction
- Secure Firewall Threat Technology Lightning Survey
- Snort 3 – What's it all about?
- **Cisco Threat Intelligence Director**
- Q&A



“Automation is the only way to keep up with the volume of emerging threats in our network” – Cisco InfoSec

Security teams require the ability to:

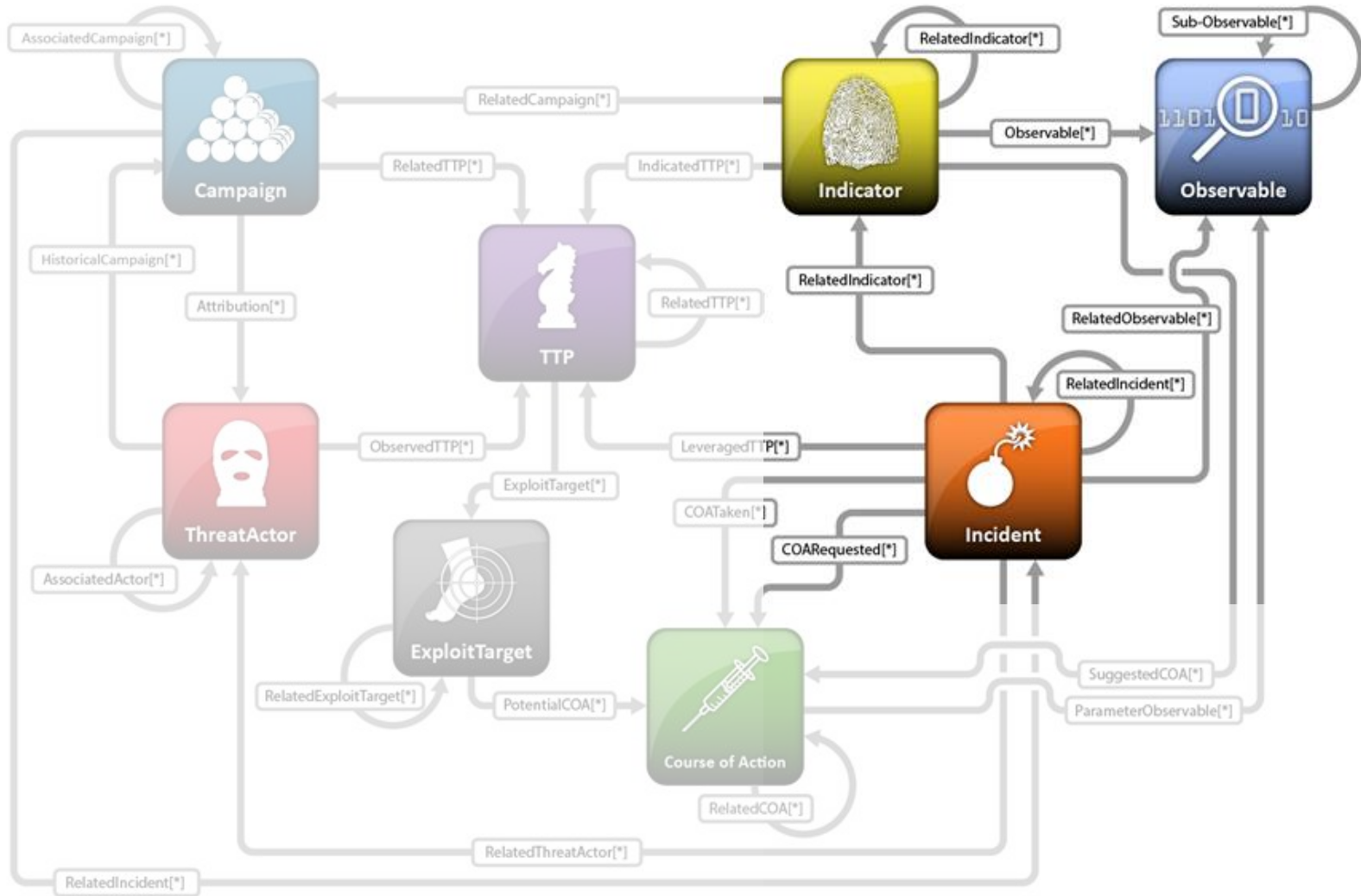
- Automate ingestion and operationalization of intelligence
- Support industry standards for intelligence sharing
- Correlate events to complex Indicators
- Automatically augment intelligence sources with analyzed events

How do we do this?

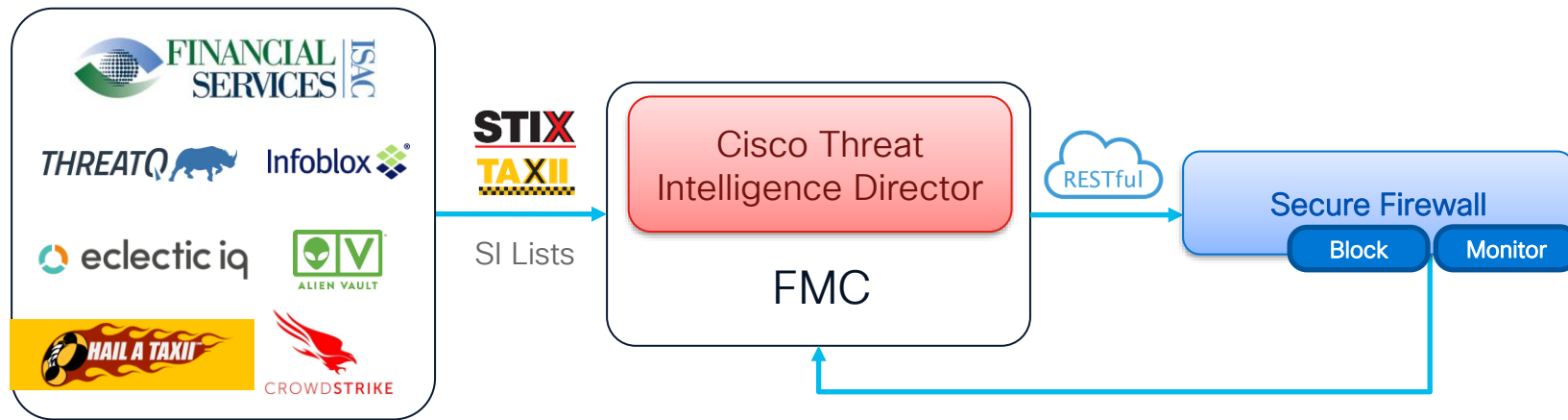
STIX

Structured
Threat
Information
eXpression

<https://stixproject.github.io/>



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

<https://blog.talosintelligence.com/2019/05/one-year-later-vpnfilter-catastrophe.html>

THURSDAY, MAY 23, 2019

One year later: The VPNFilter catastrophe that wasn't



Cisco Talos first disclosed the existence of VPNFilter on May 23, 2018. The malware made headlines across the globe, as it was a sophisticated piece of malware developed by a nation state, infecting half a million devices, and poised to cause havoc. Yet the attack was averted. The attacker's command and control (C2) infrastructure was seized by the FBI, preventing the attacker from broadcasting orders to compromised devices. The attacker lost control of the infected systems, and potential catastrophe was prevented.



SUBSCRIBE TO OUR FEED



Posts



Comments



Subscribe via Email

BLOG ARCHIVE

▼ 2019 (120)

► JUNE (7)

▼ MAY (25)

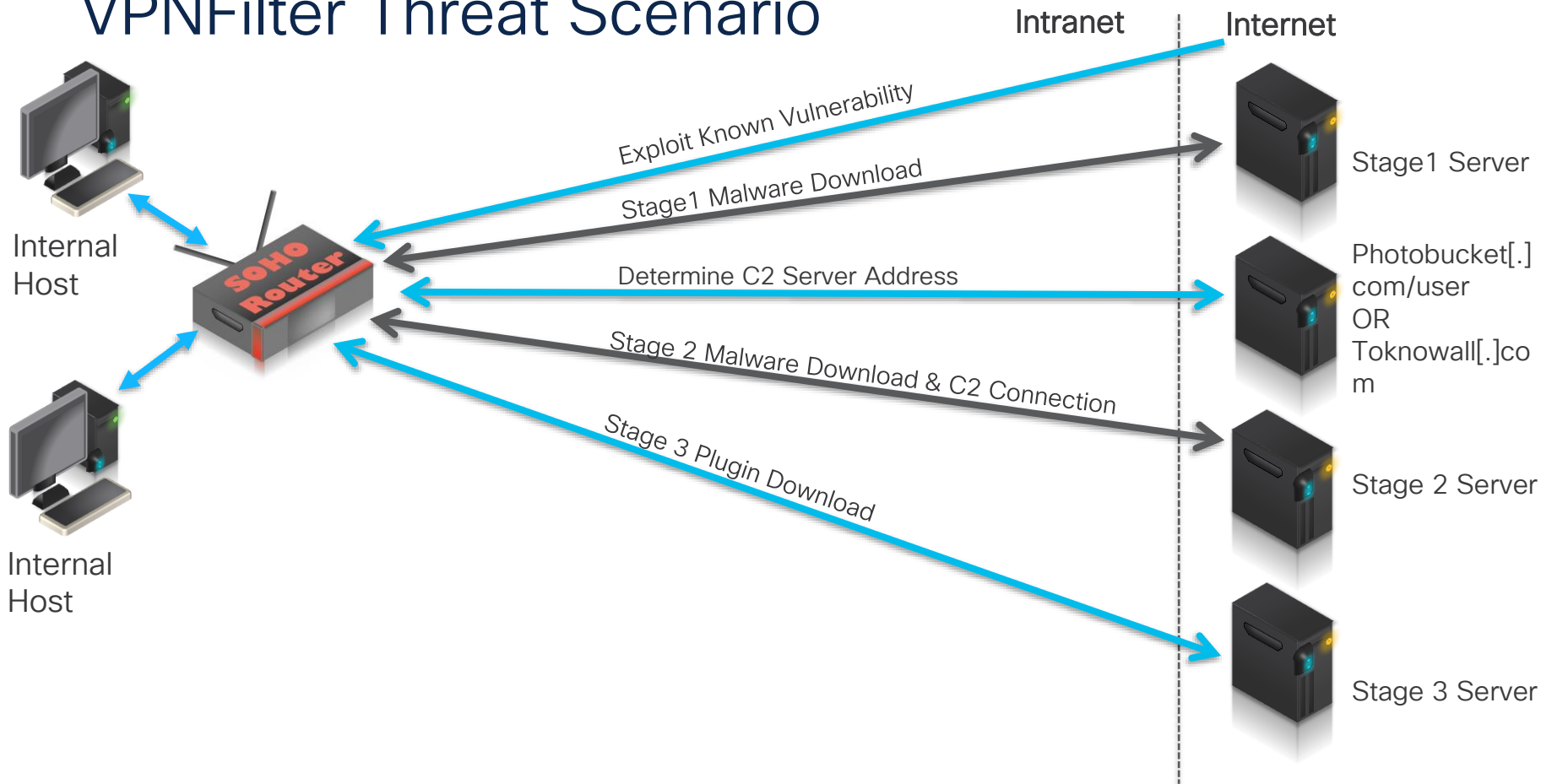
Using Firepower to defend against encrypted RDP at...

Threat Roundup for May 24 to May 31

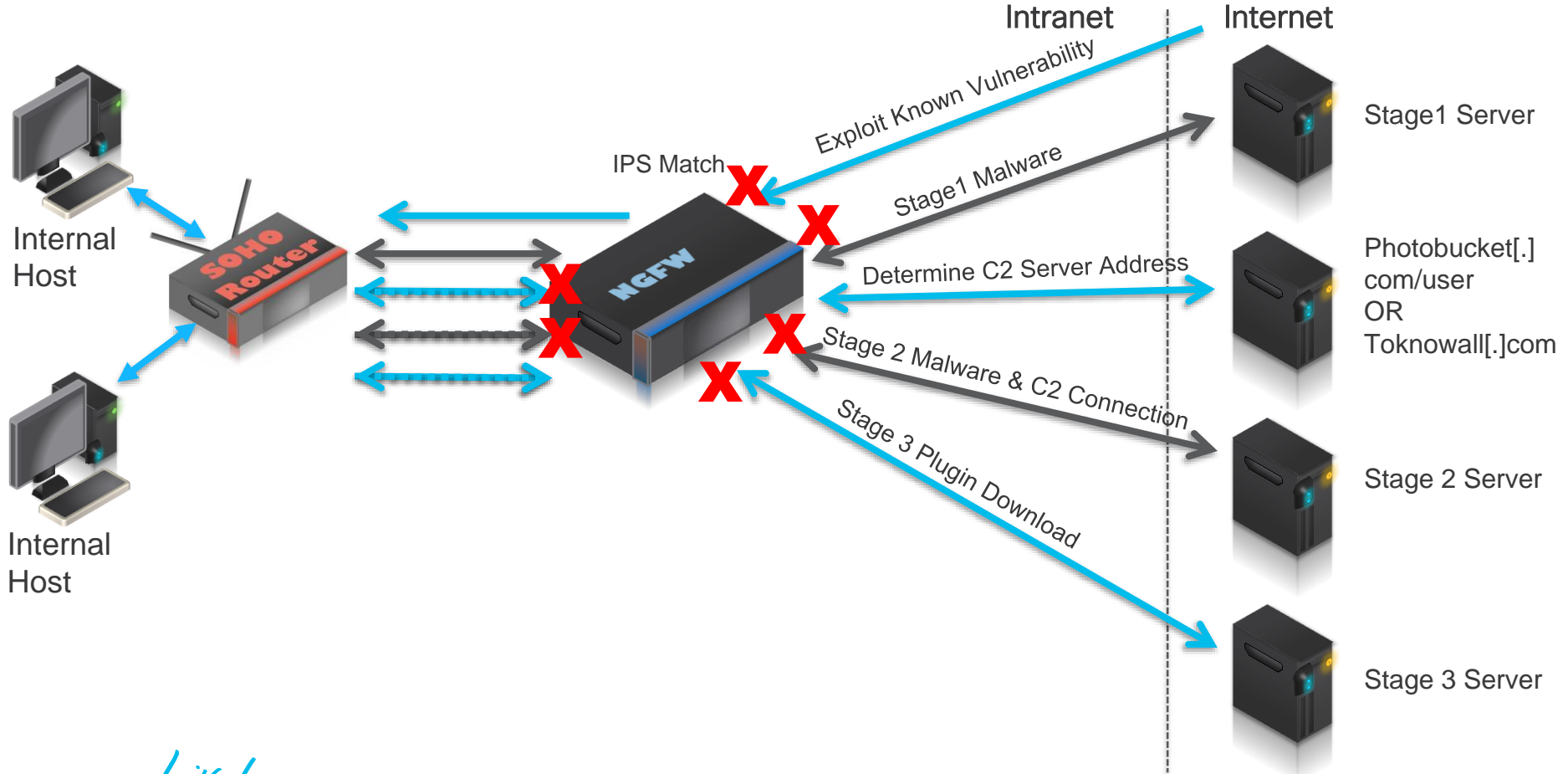
Threat Source newsletter (May 30)

10 years of virtual dynamite: A high-level

VPNFilter Threat Scenario



VPNFilter – Identifying a Compromised System



VPNFilter Indicator from CTID

Stage 1

1

INDICATOR PATTERN

SHA-256

f8286e29faa67ec765ae0244862f6b7914fcdde104...

afd281639e26a717aead65b1886f98d6d6c258736...

OR

URL

photobucket.com/user/katyperry45/library/

toknowall.com/

AND

SHA-256

50ac4fcd3fbc8abcaa766449841b3a0a684b3e217...

0e0094d9bd396a6594da8e21911a3982cd737b4...

OR

IPV4

91.121.109.209

217.12.202.40

AND

SHA-256

9683b04123d7e9fe4c8c26c69b09c2233f7e1440f...

d6097e942dd0fdc1fb28ec1814780e6ecc169ec6d...

3

Stage 3

2

Stage 2

The Secure Firewall Delivers a Comprehensive set of Threat Centric Capabilities

Talos Security Intelligence

Advanced Malware Protection for Networks

Indications of Compromise

Threat Centric URL Filtering

Passive Network Discovery

Cisco Threat Intelligence Director Operationalizes Threat Intelligence

Simple Custom Files

STIX/TAXI

Correlation

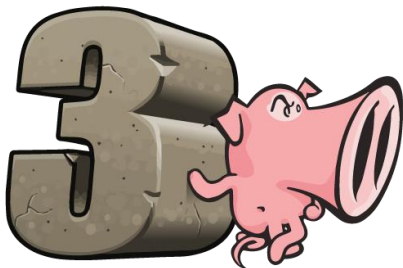
Open API

Upload or HTTP

Complex Indicators

Context

Snort 3 Delivers Increased Threat Efficacy and Performance



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.



Security Operations

SECURE X (XDR)

Managed Detection and Response Services

Security, Orchestration, Automation and Response

Incident Response and Remediation Services

Threat Visibility & Hunting

Device Insights

Kenna Vuln Mgmt

Secure Cloud Insights

3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed



Cisco Secure Client

VPN
Posture
Telemetry
Threat
Query

ThousandEyes (Visibility)

Device Mgmt
 Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE)

ZERO TRUST

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Threat Protection | Secure Access Control | Managed Remote Access

Reliable | Scalable | Flexible

Umbrella/Duo

ZTNA DNS-layer security Secure web gateway L7 firewall + IPS Cloud access security broker/shadow IT
 RAaaS SSL decryption Remote browser isolation Data loss prevention Cloud malware detection

SDWAN

Cisco Meraki SDWAN SDWAN by Viptela Secure Firewall ThousandEyes Cloud DDoS, WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

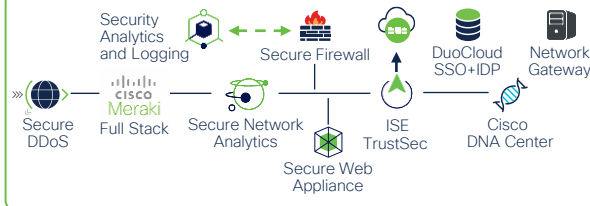
Network Edge Cisco Meraki SDWAN SDWAN by Viptela Secure Firewall ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

Industrial Router Industrial Firewall Industrial Switch/AP Cyber Vision ISE TrustSec

ZERO TRUST
Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility



Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

Cloud Native Security APIC
 Secure Workload Secure Application by AppDynamics

App Observability | Detection | Response

Hybrid Private Public Cloud
 Secure Cloud Analytics Secure Firewall
 ThousandEyes Secure DDoS, WAF/Bot

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

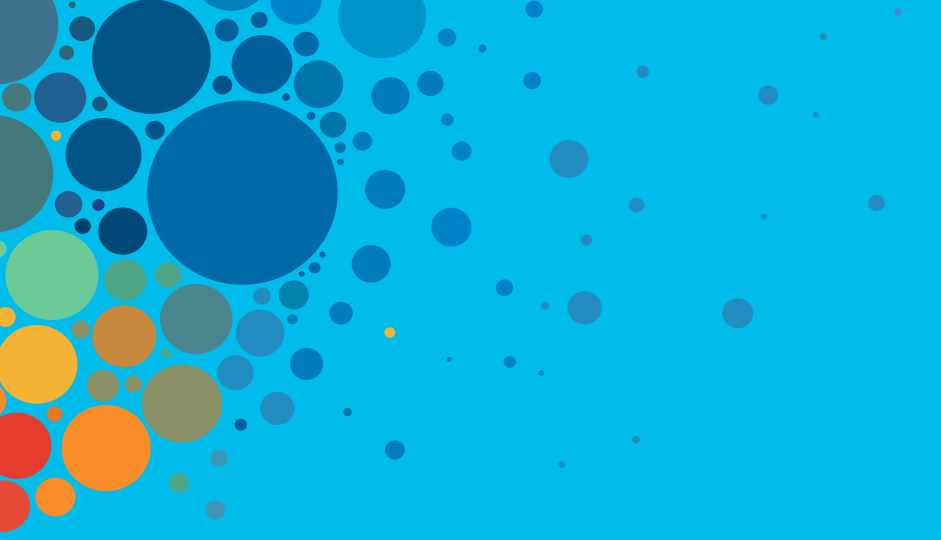
Cisco Guided Study Groups

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



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive

The background features a collection of circles of various sizes and colors, including shades of blue, green, orange, and red, scattered across the right side of the slide. The circles vary in opacity and size, creating a dynamic, abstract pattern.

Network Discovery & Indications of Compromise

Network Discovery

- Passive detection of protected assets
- Identification of key vectors
 - Operating System
 - Services
 - Client Applications
- Enables Critical Threat Detection
 - Impact Assessment
 - IPS Rule Recommendation
- Enrich with Active Scanning!
 - NMAP, Qualys, Nessus, etc..

Indications of Compromise

- Correlation of disparate security events to update the Network Map state information with flags that indicate nefarious activity
 - Threat detections contextually specific to host compromise
 - Security Intelligence connections to known bad IP addresses
 - AMP for Networks malware detection
 - AMP for Endpoints malware detection and Big Data analytics driven host indications

Edit Indications of Compromise Settings

Note: To detect Indications of Compromise, you must enable each IOC rule here and also enable the features, such as Security Intelligence logging and intrusion and malware protection, that the rules below depend on.

☒ Enable IOC 40 out of 40 Rules Enabled

Category ▲	Source	Event Type	Description	Enabled
Adobe Reader Compromise	Malware Events	PDF Compromise Detected by AMP for Endpoints	Generic Adobe Reader Compromise	<input checked="" type="checkbox"/>
Adobe Reader Compromise	Malware Events	Adobe Reader launched shell	A shell was launched on the host by Adobe Reader	<input checked="" type="checkbox"/>