Possibilities

#CiscoLive

Using ML to Reduce Network Management Operational Risk

Edgar A. Murillo, Sr. Solution Architect

DGTL-PSOCX-2497

Agenda

- Introduction
- Benchmarking
- Fingerprinting
- Automated Fault Management & Network Early Warning
- Conclusion

Benchmarking

Common Questions

- What is my exposure to security risks compared to my peers (PSIRTs)
- What is my exposure to known hardware issues compared to other companies (Field Notices)
- What's the level of supportability of my network compared with my competitors (EoL)
- Is my network too diverse? Should I reduce the number of platforms?

Benchmarking leverages a global database of almost 3 million devices to answer these questions.

Benchmarking is Using Statistical Analysis to Measure Your Risk Exposure

PSIRTs | EOX & PSIRTs | HW SW LDoS | Field Notice | HW Diversity | SW Diversity | Action Items

How do I compare for Unique Vulnerable PSIRTs exposure?

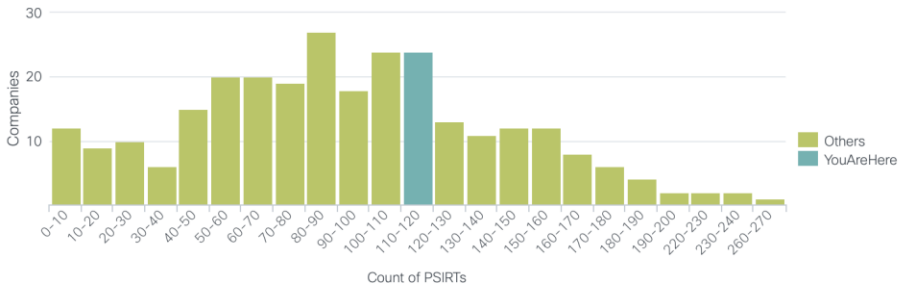
Cisco does not evaluate new PSIRTs on devices that have reached LDoS, there could be more PSIRTs exposure not shown here

Best Customer Count	Your Count	Global Median Count	Worst Customer Count
1 → 0	110 → 0	84 ↘ -10	267 → 0
Compared to Yesterday	Compared to Yesterday	Compared to Yesterday	Compared to Yesterday

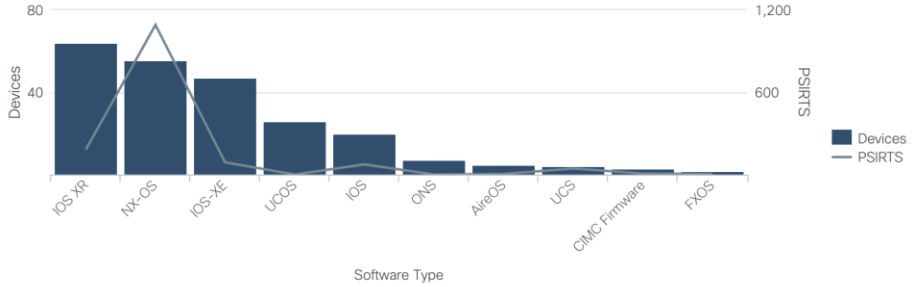
1m ago

PSIRTs Distribution and Software Type

Distinct PSIRT Exposure Count Compared to Others



Your Software Type Distribution with PSIRT Counts Overlay



The Power of Statistics and Benchmarking

With the power of Statistics and Benchmarking we:

- Give you visibility to key network supportability indicators (PSIRTs, Field Notices, Hardware EoL, Software EoL)
- Measure how your company is performing against peers
- A plan to minimize network operational risk by reducing exposure to security risks and known hardware issues

Fingerprinting

Preparing Fingerprint data for Machine Learning

- Fingerprint
  - Anonymized Global Data
  - Hardware, Software, Features from the configuration
  - No names, addresses, or raw configuration

What data is needed for anonymous profile?

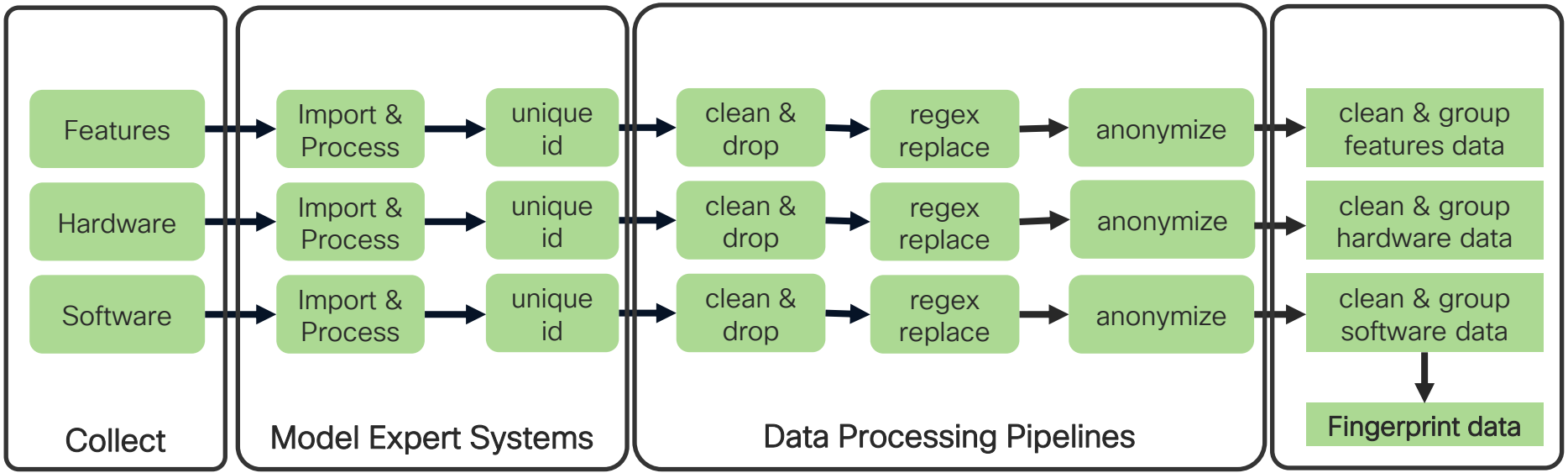
- Hardware, Software & Configuration

```
Router#show inventory
NAME: "CISCO3925-CHASSIS", DESCR: "CISCO3925-CHASSIS"
PID: CISCO3925-CHASSIS , VID: V02, SN: FTX1543ALZ9

NAME: "Cisco Services Performance Engine 100 for Cisco 3900 ISR on Slot 0", DESCR: "Cisco Services Perf
PID: C3900-SPE100/K9   , VID: V04 , SN: FOC15405ZAW

NAME: "4 port clear channel T1/E1 HWIC
PID: HWIC-4T1/E1       , VID: V02 , SN:

NAME: "PVDM3 DSP DIMM with 64 Channels
PID: PVDM3-64          , VID: V01 , SN:

NAME: "1000BASE-SX SFP", DESCR: "1000BAS
PID: SFBR-5716PZ       , VID: 001, SN: A

NAME: "1000BASE-SX SFP", DESCR: "1000BAS
PID: SFBR-5766PZ       , VID:    , SN: A

NAME: "C3900 AC-POE Power Supply 1", DES
PID: PWR-3900-POE      , VID: V03, SN: S
```

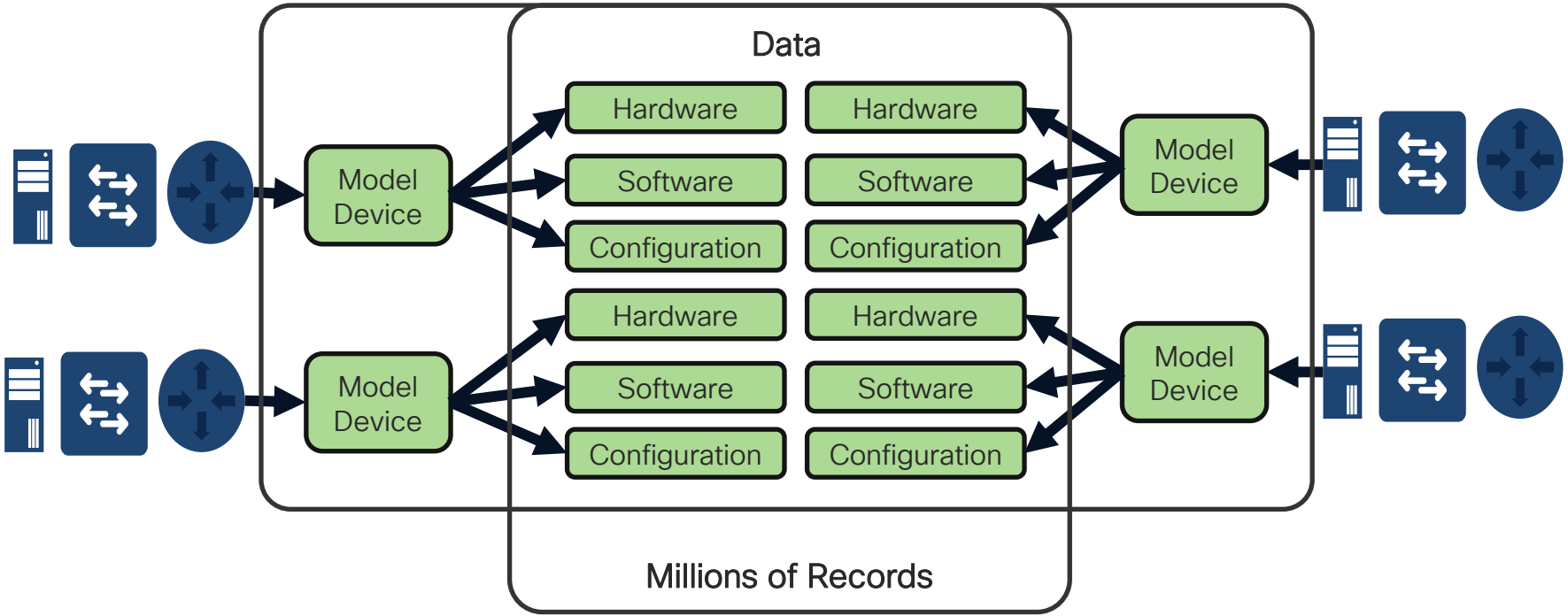
```
Router#show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.2(4)M7,

Router uptime is 11 weeks, 6 days, 22 minutes
System returned to ROM by power-on
System restarted at 10:49:01 UTC Thu Feb 7 2019
System image file is "flash:c3900-universalk9-mz.SPA.152-4.M7.bin"
Last reload type: Normal Reload
Last reload reason: power-on

Cisco CISCO3925-CHASSIS (revision 1.0) with C3900-SPE100/K9 with 995328K/5324
Processor board ID FTX1543ALZ9
3 Gigabit Ethernet interfaces
1 terminal line
4 Channelized (E1 or T1)/PRI ports
1 Virtual Private Network (VPN) Module
DRAM configuration is 72 bits wide with parity enabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)
```

```
Router#show run
Building configuration...
!
! Last configuration change at 19:57:06 UTC Wed Mar 13 2019 by
! NVRAM config last updated at 19:57:11 UTC Wed Mar 13 2019 by
! NVRAM config last updated at 19:57:11 UTC Wed Mar 13 2019 by
version 15.2
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
og datetime msec
ryption

900-universalk9-mz.SPA.152-4.M7.bin

akH$h14vZKBihh0Fxb.5KMn0Q0

n

isco.com
.x
```

Vectorize - Developing a Fingerprint



The Starting Point with Data



You are here

Now we have thousands of these. What can you do with them?

```
15_6 C2900_UNIVERSALK9_Mz_spa SYSTEM IOS 15_6_3_M3a ISR_Power_
_ES2_16_P WAN_Interface_Cards HWIC_4T1_E1 Voice_Interface_Card
isco_2900_Series_Integrated_Services_Routers CISCO2911_K9 dial
nfiguring_POTS_Dial_Peers NTP_Update_Calendar IP_SLAs_Responde
r_system_shutdown fhrp_hsrp_mib_IOS sip_redirect_processing_en
sage_logger SNMP_Trap_isdn_chan_not_avail Cisco_Discovery_Prot
_resume_support cef_dcef_cisco_express_forwarding Dis_outbound
ass_Support_IOS multicast_music_on_hold_support_for_call_manag
_peer_IOS tcl_ivr_2_0_call_initiation_and_callback snmp_trap_c
_access_lists Duplex_operation_on_an_interface_IOS CDP_Disable
n_initiation_protocol_for_voip NBAR Egress_NetFlow_Accounting
```

```
15_3 C2951_UNIVERSALK9_Mz_spa SYSTEM IOS 15_3_3_M5 Cisco_2900_
ds HWIC_1DSU_T1 Voice_Interface_Cards VIC2_4FXO Voice_Interfac
M3_64 Transceiver_Modules GLC_SX_MMD ISR_Power_Supplies PWR_29
d_IP_Phone_7900_Series CP_7960G Cisco_Unified_IP_Phone_7900_Se
nified_IP_Phone_7900_Series CP_7960G Cisco_Unified_IP_Phone_79
sco_Unified_IP_Phone_7900_Series CP_7960G Cisco_Unified_IP_Phc
0G Cisco_Unified_IP_Phone_7900_Series CP_7960G Cisco_Unified_I
P_7960G Cisco_Unified_IP_Phone_7900_Series CP_7960G Cisco_Unif
ies CP_7960G Cisco_Unified_IP_Phone_7900_Series CP_7960G Cisco
0_Series CP_7960G Cisco_Unified_IP_Phone_7900_Series CP_7960G
e_7900_Series CP_7960G Cisco_Unified_IP_Phone_7900_Series CP_7
Authorization AAA_Interim_Accounting_IOS AAA_Method_Lists_Enha
```


```
15_3 C2951_UNIVERSALK9_Mz_spa SYSTEM IOS 15_3_3_M5 Cisco_2900_
ds HWIC_1DSU_T1 Voice_Interface_Cards VIC2_4FXO Voice_Interfac
M3_64 Transceiver_Modules GLC_SX_MMD ISR_Power_Supplies PWR_29
d_IP_Phone_7900_Series CP_7960G Cisco_Unified_IP_Phone_7900_Se
nified_IP_Phone_7900_Series CP_7960G Cisco_Unified_IP_Phone_79
sco_Unified_IP_Phone_7900_Series CP_7960G Cisco_Unified_IP_Phc
0G Cisco_Unified_IP_Phone_7900_Series CP_7960G Cisco_Unified_I
P_7960G Cisco_Unified_IP_Phone_7900_Series CP_7960G Cisco_Unif
ies CP_7960G Cisco_Unified_IP_Phone_7900_Series CP_7960G Cisco
0_Series CP_7960G Cisco_Unified_IP_Phone_7900_Series CP_7960G
e_7900_Series CP_7960G Cisco_Unified_IP_Phone_7900_Series CP_7
Authorization AAA_Interim_Accounting_IOS AAA_Method_Lists_Enha
```



```
15_6 C2900_UNIVERSALK9_Mz_spa SYSTEM IOS 15_6_3_M3a ISR_Power_
_ES2_16_P WAN_Interface_Cards HWIC_4T1_E1 Voice_Interface_Card
isco_2900_Series_Integrated_Services_Routers CISCO2911_K9 dial
nfiguring_POTS_Dial_Peers NTP_Update_Calendar IP_SLAs_Responde
r_system_shutdown fhrp_hsrp_mib_IOS sip_redirect_processing_en
sage_logger SNMP_Trap_isdn_chan_not_avail Cisco_Discovery_Prot
_resume_support cef_dcef_cisco_express_forwarding Dis_outbound
ass_Support_IOS multicast_music_on_hold_support_for_call_manag
_peer_IOS tcl_ivr_2_0_call_initiation_and_callback snmp_trap_c
_access_lists Duplex_operation_on_an_interface_IOS CDP_Disable
n_initiation_protocol_for_voip NBAR Egress_NetFlow_Accounting
```

Similarity Question 1:

How can I quickly determine how similar my device is to other devices of interest?

Where Fingerprint began: Data Explosion in Search

- With pool of 1000 possible HW/SW/Config values, and a desire to search all combinations of 5 features:
  - 1 HW Feature
  - 1 SW Feature
  - 3 Configuration Features

$$\frac{1000!}{5!(1000-5)!} =$$

Cisco CX has identified more than **25,000** unique values for hardware, software, and features

8,250,291,250,200

Use Machine Learning to solve this problem

Generalizes information to find “nearest” matches

Avoids dealing with all possible combinations.

Uses mathematical representations

Much less computationally expensive for searching.

Improves innovation in other areas

More efficient way to prepare the data to solve problems.

Similarity – Unsupervised ML

How similar are these two devices?

```
15_6 C2900_UNIVERSALK9_Mz_spa SYSTEM IOS 15_6_3_M3a ISR_Power_
_ES2_16_P WAN_Interface_Cards HWIC_4T1_E1 Voice_Interface_Card
isco_2900_Series_Integrated_Services_Routers CISCO2911_K9 dial
nfiguring_POTS_Dial_Peers NTP_Update_Calendar IP_SLAs_Responde
r_system_shutdown fhrp_hsrp_mib_IOS sip_redirect_processing_en
sage_logger SNMP_Trap_isdn_chan_not_avail Cisco_Discovery_Prot
_resume_support cef_dcef_cisco_express_forwarding Dis_outbound
ass_Support_IOS multicast_music_on_hold_support_for_call_manag
_peer_IOS tcl_ivr_2_0_call_initiation_and_callback snmp_trap_c
_access_lists Duplex_operation_on_an_interface_IOS CDP_Disable
n_initiation_protocol_for_voip NBAR Egress_NetFlow_Accounting
```

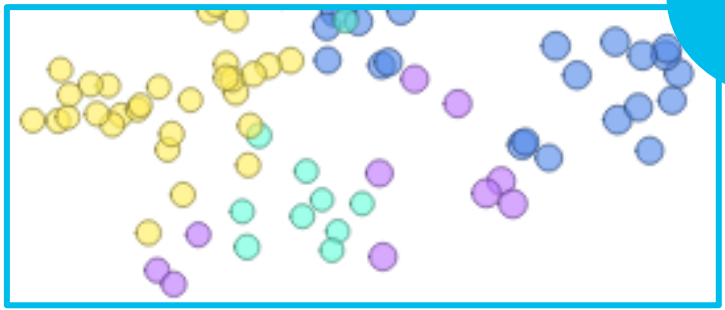
```
15_3 C2951_UNIVERSALK9_Mz_spa SYSTEM IOS 15_3_3_M5 Cisco_2900_
ds HWIC_1DSU_T1 Voice_Interface_Cards VIC2_4FXO Voice_Interfac
M3_64 Transceiver_Modules GLC_SX_MMD ISR_Power_Supplies PWR_29
d_IP_Phone_7900_Series CP_7960G Cisco_Unified_IP_Phone_7900_Se
nified_IP_Phone_7900_Series CP_7960G Cisco_Unified_IP_Phone_79
sco_Unified_IP_Phone_7900_Series CP_7960G Cisco_Unified_IP_Pho
0G Cisco_Unified_IP_Phone_7900_Series CP_7960G Cisco_Unified_I
P_7960G Cisco_Unified_IP_Phone_7900_Series CP_7960G Cisco_Unif
ies CP_7960G Cisco_Unified_IP_Phone_7900_Series CP_7960G Cisco
0_Series CP_7960G Cisco_Unified_IP_Phone_7900_Series CP_7960G
e_7900_Series CP_7960G Cisco_Unified_IP_Phone_7900_Series CP_7
Authorization AAA_Interim_Accounting_IOS AAA_Method_Lists_Enha
```

ML can do this easily:

Product Family	Software Type	Software Version	Similarity
Cisco 2900 Series Integrated Services Routers	IOS	15.6(3)M4	1.00
Cisco 2900 Series Integrated Services Routers	IOS	15.5(3)M7	0.84
Cisco 2900 Series Integrated Services Routers	IOS	15.3(3)M3	0.83
Cisco 2900 Series Integrated Services Routers	IOS	15.2(3)T2	0.83

One by One

One vs. Many



ML Similarity Use Cases

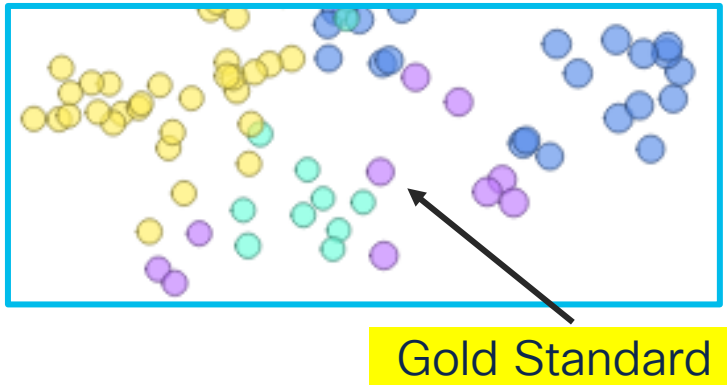
A device crashed. Do I have anything else in my network that is similar to that one?

Product Family	Software Type	Software Version	Similarity
Cisco 2900 Series Integrated Services Routers	IOS	15.6(3)M4	1.00
Cisco 2900 Series Integrated Services Routers	IOS	15.5(3)M7	0.84
Cisco 2900 Series Integrated Services Routers	IOS	15.3(3)M3	0.83
Cisco 2900 Series Integrated Services Routers	IOS	15.2(3)T2	0.83

I have a Gold standard device. How similar are other devices to that one?

Can I see ALL my devices on one view and find outliers?

Use ML Dimensionality Reduction with Data Visualization



Question 2:

How can I see all of my devices at once?

Data Visualization with Dimensionality Reduction

Question 3:

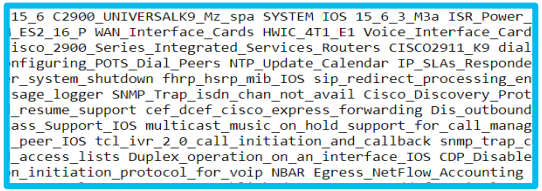
How can I determine which device fingerprints CAN have a problem?

Risk Identification- Supervised ML

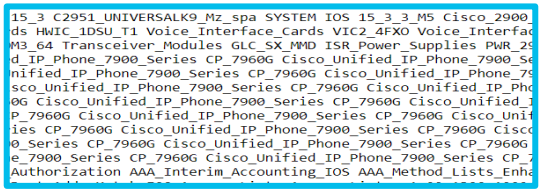
Cisco has millions of fingerprints

Training

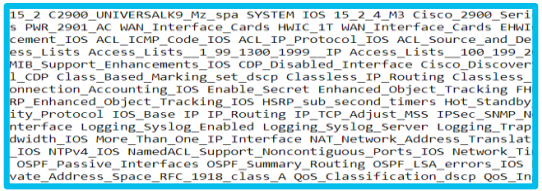
If I know of Fingerprints that have crashed in the past, can I predict future crashes?



No known crashes



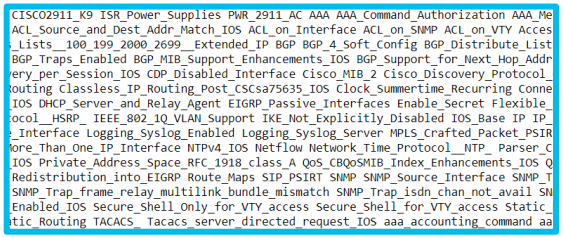
Saw a crash



No known crashes

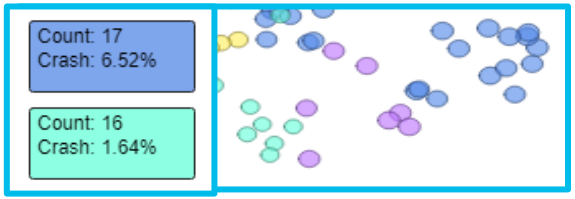
Predicting

What is probability of any fingerprint showing a crash?



Crash Probability: xx%

+



Historical Cluster Crashes seen

=

Device Risk Score

Rank riskiest devices to find previously unknown devices at risk

Compare redundant devices to ensure they are identical

Match to Gold standards to ensure configurations are compliant

Find outliers from groups in one view

Find end of life device migration options using similarity of configuration

Other Fingerprint Use Cases

Identify differing roles of network devices based on similarity

Find similar devices to a device that has been diagnosed with a SW bug

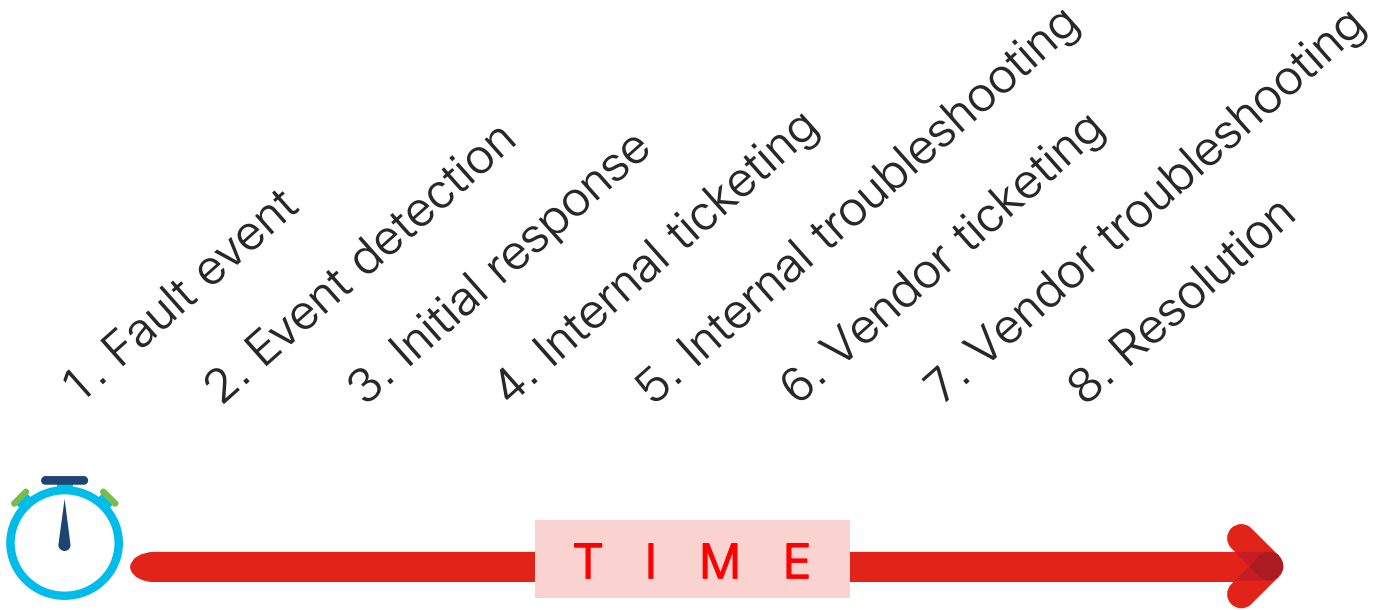
Find similarity to crashes in your customer devices from other devices around the world (Internal)

Ensure software compliance tracks are all similar and consistent devices

Determine most common hardware/software for a given configuration (Internal)

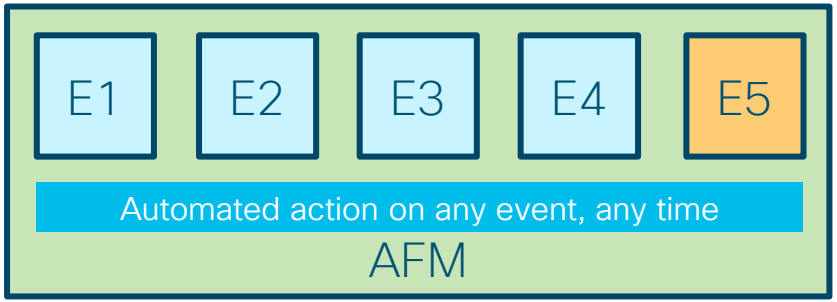
Automated Fault Management & Network Early Warning

Fault Management Timeline

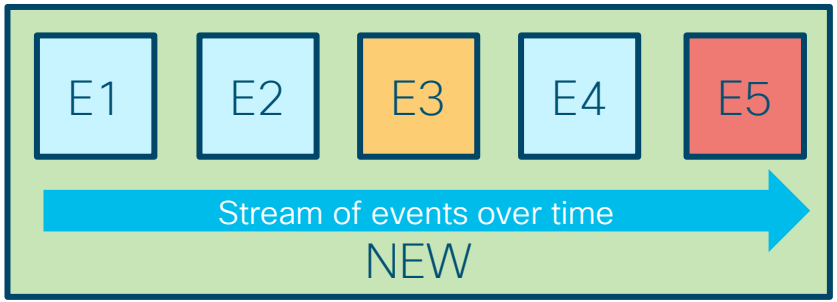


How can the ENTIRE process improve?

Both what and when matter for syslog signatures



- Automated Fault Management
  - Take action when E5 is seen
  - Identify something HAS happened

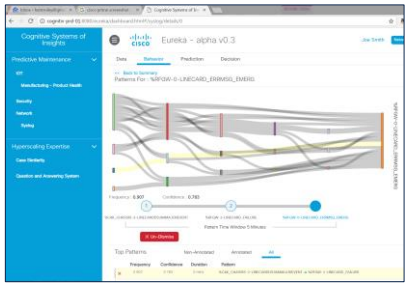


- Network Early Warning
  - See E1-E3, predict E5 is coming
  - Identify something CAN happen, with some probability
  - Can trigger Automation @E3

NEW ML and AFM combined value

FEEDBACK LOOP

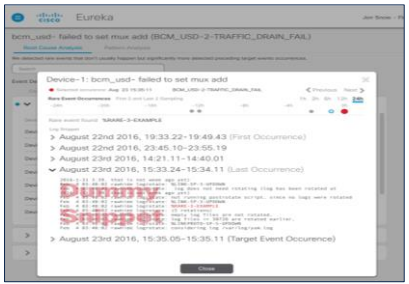
Behavior



Pattern Mining

Analysis of voluminous historical data to find the specific pattern(s) leading to the future appearance of a specific target event

Validate



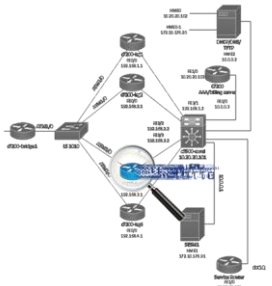
SME Validation

Is the result accurate?

FEEDBACK LOOP

Assign the recommended action

Predict



Run-Time Rules Deployment

Deployment of verified predictive rules into real-time pattern classification engines

Preempt

Integration (AFM)

Output integrated into existing workflows, operations systems for early warning and automation

AUTOMATE PRE-DETERMINED RECOMMENDED ACTIONS

Network Early Warnings with Automated Fault Management objectives

Conclusion

Conclusion

- Cisco CX is using statistical formulas to compare network performance and risk between customers.
- In areas of support, Cisco CX is using ML algorithms to significantly limit and/or prevent occurrence of service network impact.
- Cisco CX uses the power of Fingerprinting to quickly compare devices and determine areas of high or low risk.

Thank you

Cisco.com/go/bcs

Where the energy from Cisco Live continues
and a collaborative journey begins.

Plan. Explore. Connect. Let's Go.

Cisco
Customer Experience

Continue your Pathway to Success

Visit CX On Demand beginning June 4

Cisco Live Day 2 Keynote	Alvio Barrios	Liz Centoni	Todd Nightingale
CX Demos	CX Cloud	CX Cloud for Partners	Business Critical Services
Innovation Channel	**Innovation Talk** Collaborative Intelligence + Future Innovations: How Cisco CX Accelerates Customer Success Tony Colon, Pat Tittiranonda		**Product & Strategy Overview** How CX Uses ML/AI to Reduce Your Operational Risk Chris Rittler
Product or Strategy Overview Sessions	**Managed Services** • Accelerate Transformation with Cisco Managed Services **Support Services** • Leverage Cisco Support Services for Business Continuity **Cloud** • Optimizing the Application Experience in a Cloud Native World **IoT** • Best Practices for Deploying Large Scale IoT Devices		**Enterprise** • ITSM OS Update - Closed Loop Between Cisco DNA Center and Service Now • Accelerate and Prepare the Groundwork for Your Cisco DNA Center Implementation • Outsmarting SD-WAN Threats **Security** • How to Adapt Your Workforce Needs During Changing Times **Service Provider** • Virtualization in Mobility

cisco Live!

Possibilities

#CiscoLive