redhat

intel

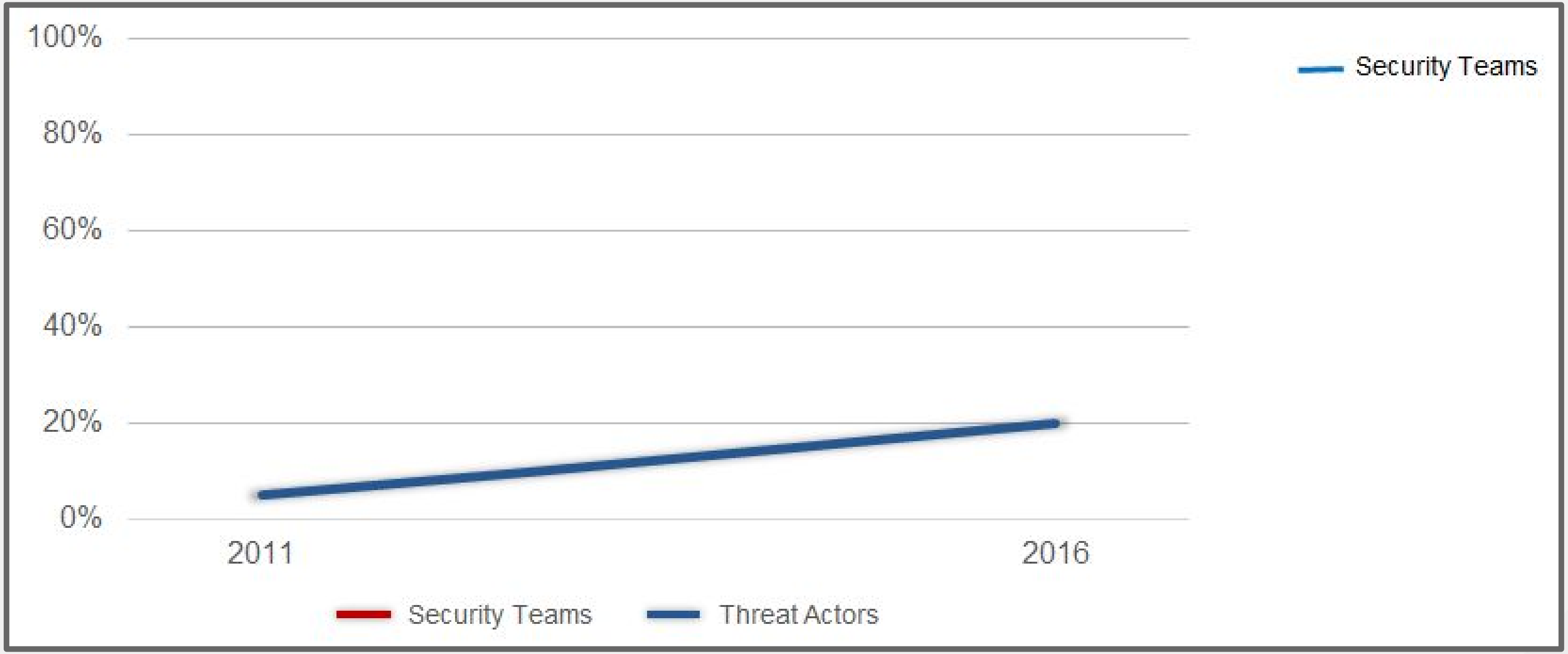
2017 Defense in Depth

October 3rd, 2017 | Tysons Corner, VA | Sheraton Tysons Hotel

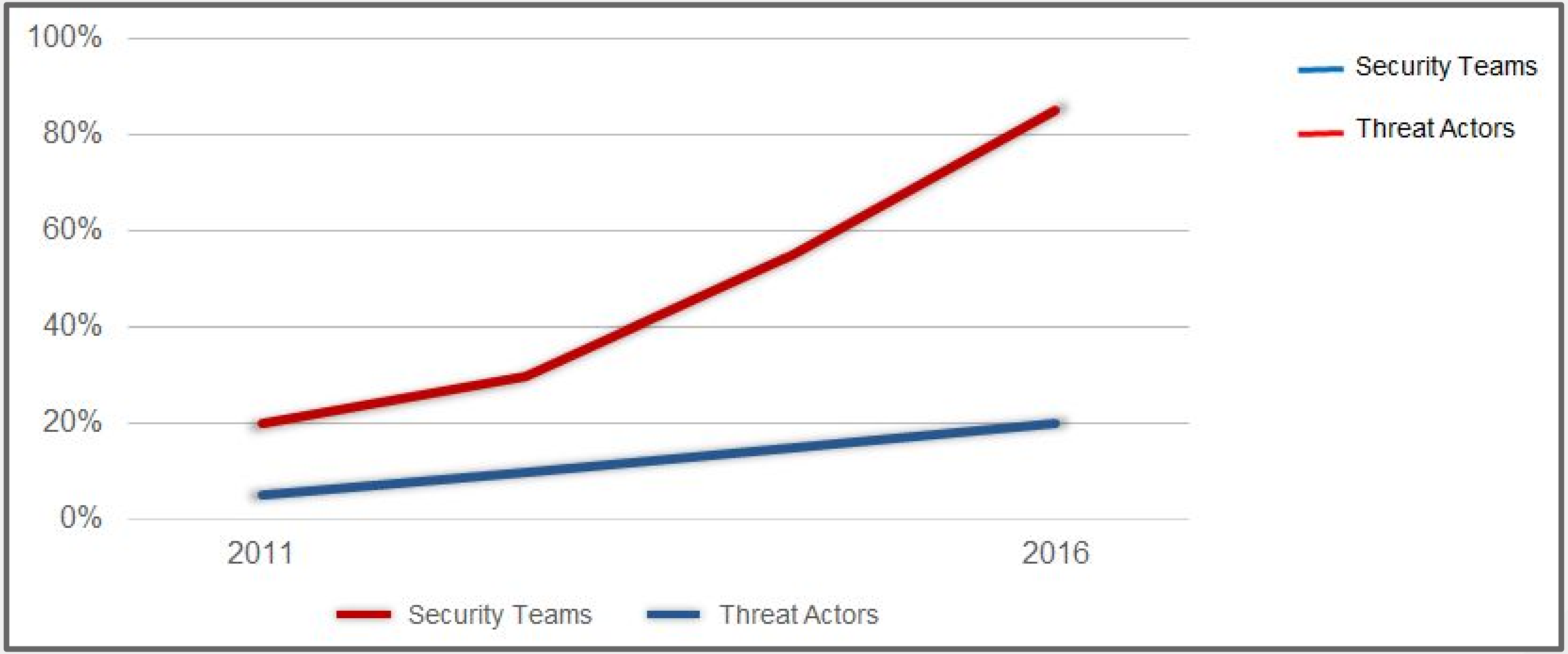
WHY ARE WE LOSING THE INFOSEC BATTLE?

how do we get back into the race?

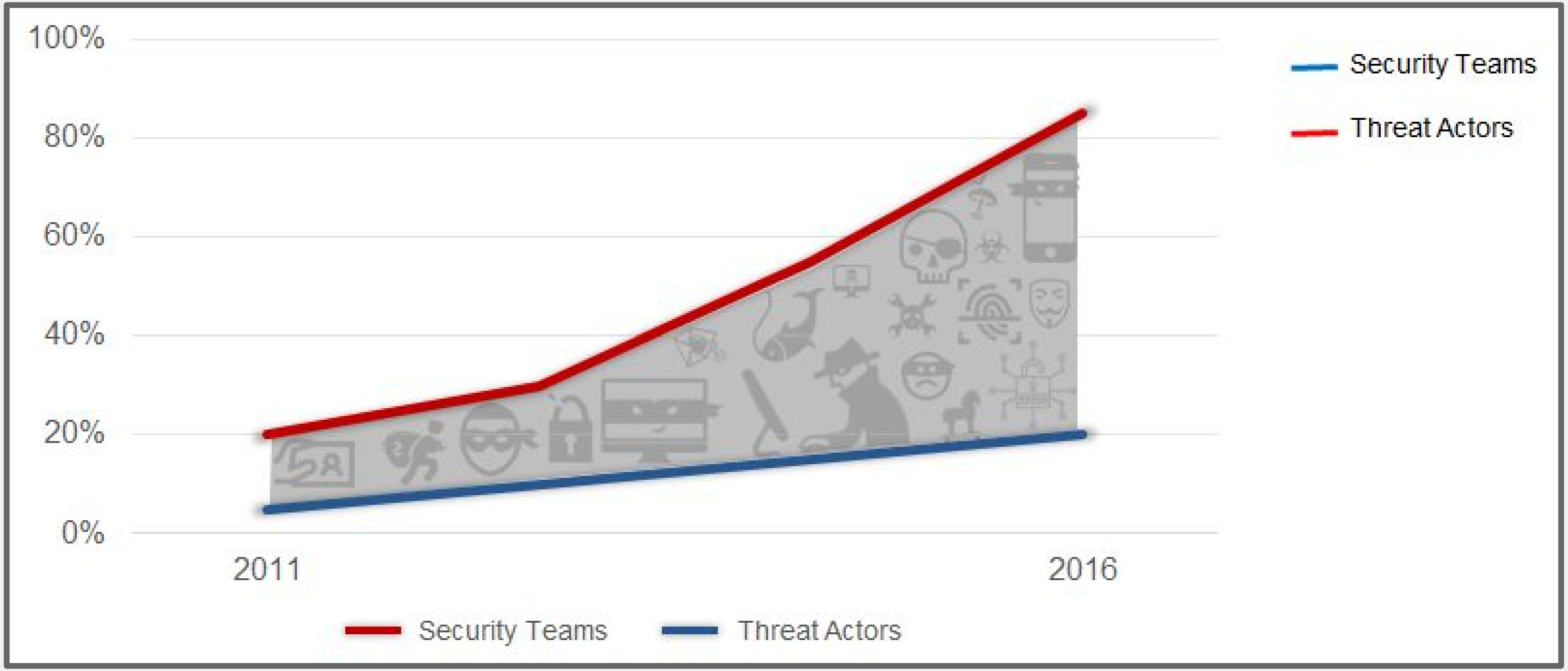
Why we are still losing the InfoSec battle

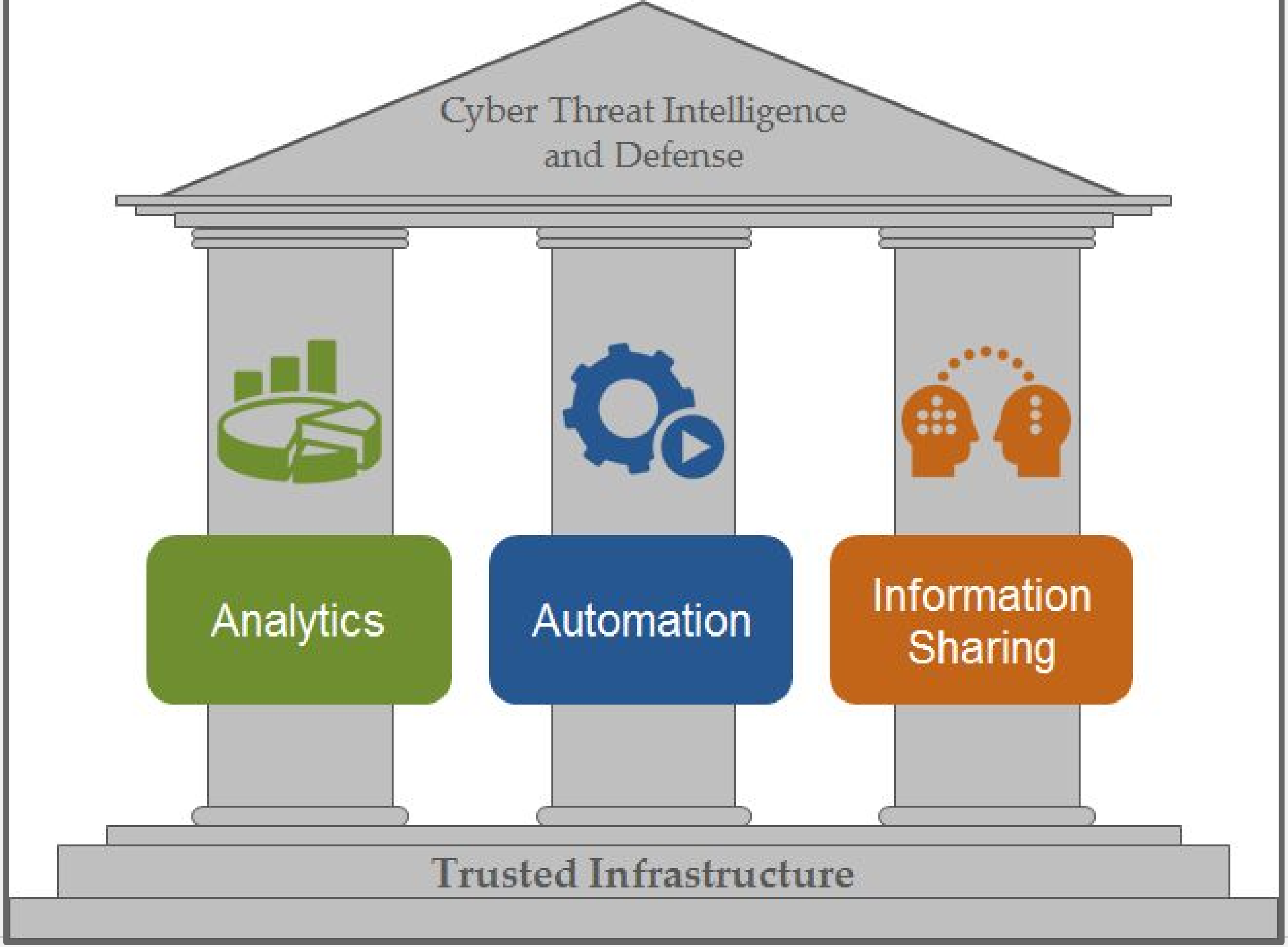


Why we are still losing the InfoSec battle



Why we are still losing the InfoSec battle




Cyber Threat Intelligence and Defense
Analytics
Automation
Information Sharing
Trusted Infrastructure

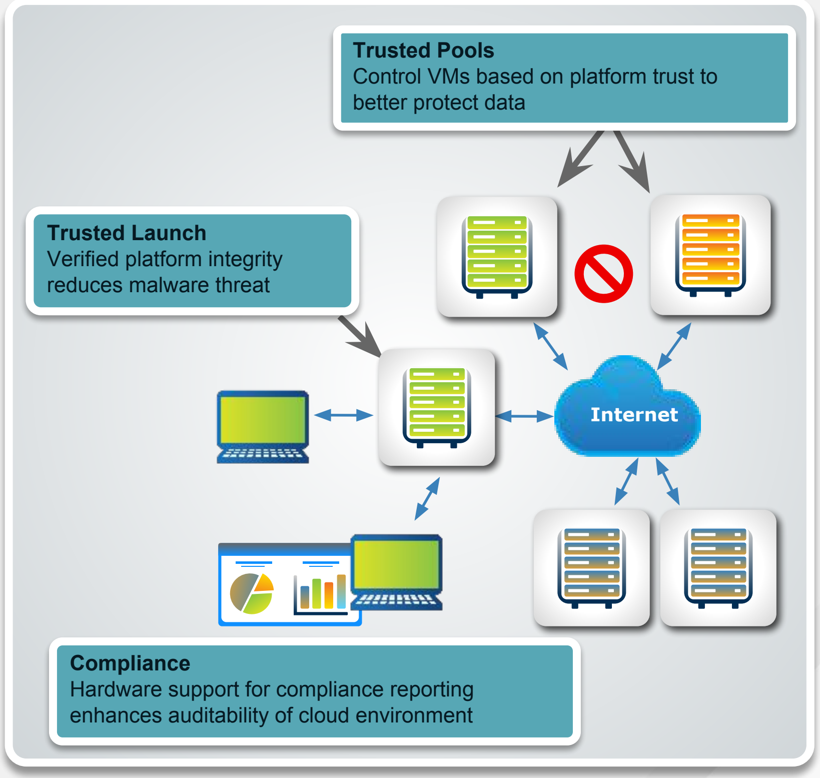
Trusted Compute Pools

Addresses critical needs in virtualized & cloud use models

- Provides control to ensure only trustable hypervisor is run on platform
- Protecting server prior to virtualization software boot
- Launch-time protections that complement run-time malware protections
- Compliance Support

Control VMs based on platform trust

- Pools of platforms with trusted hypervisor
- VM Migration controlled across resource pools
- Similar to clearing airport checkpoint and then moving freely between gates

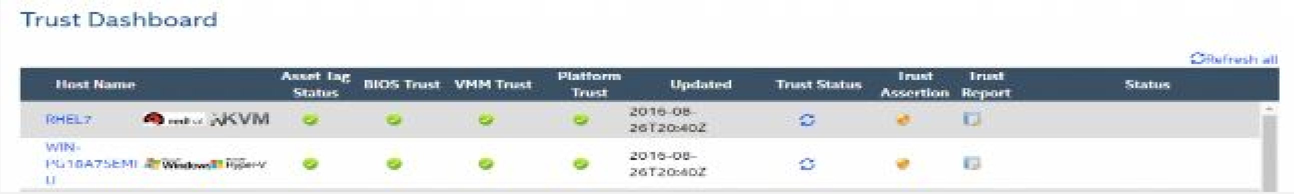


Trusted Pools
Control VMs based on platform trust to better protect data

Trusted Launch
Verified platform integrity reduces malware threat

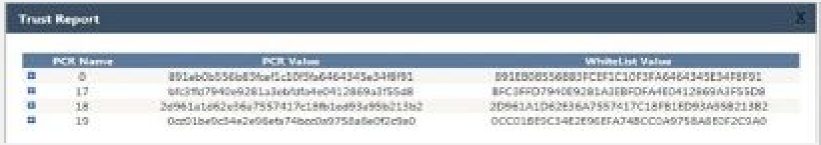
Compliance
Hardware support for compliance reporting enhances auditability of cloud environment

OpenCIT



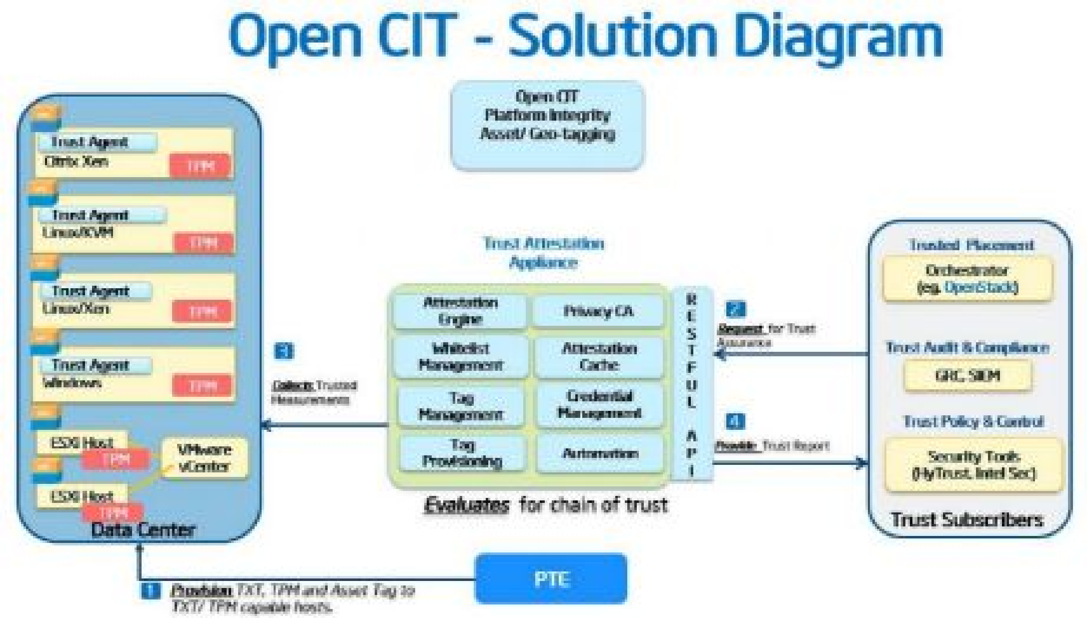
Trust Dashboard

Host Name		Asset Tag Status	BIOS Trust	VMM Trust	Platform Trust	Updated	Trust Status	Trust Assertion	Trust Report	Status
RHEL7	redhat KVM	●	●	●	●	2016-08-26T20:40Z	⟳	●	▢	
WIN-PG18A75EMIU	Windows Hyper-V	●	●	●	●	2016-08-26T20:40Z	⟳	●	▢	



Trust Report

	PCR Name	PCR Value	WhiteList Value
⊞	0	891eb0b556b83fcef1c10f3fa6464345e34f8f91	891EB0B556B83FCEF1C10F3FA6464345E34F8F91
⊞	17	bfc3ffd7940e9281a3ebfdfa4e0412869a3f55d8	BFC3FFD7940E9281A3EBFDFA4E0412869A3F55D8
⊞	18	2d961a1d62e36a7557417c18fb1ed93a95b21382	2D961A1D62E36A7557417C18FB1ED93A95B21382
⊞	19	0cc01be0c34e2e96efa748cc0a9758a8e0f2c3a0	0CC01BE0C34E2E96EFA748CC0A9758A8E0F2C3A0



Open CIT - Solution Diagram

Key Features

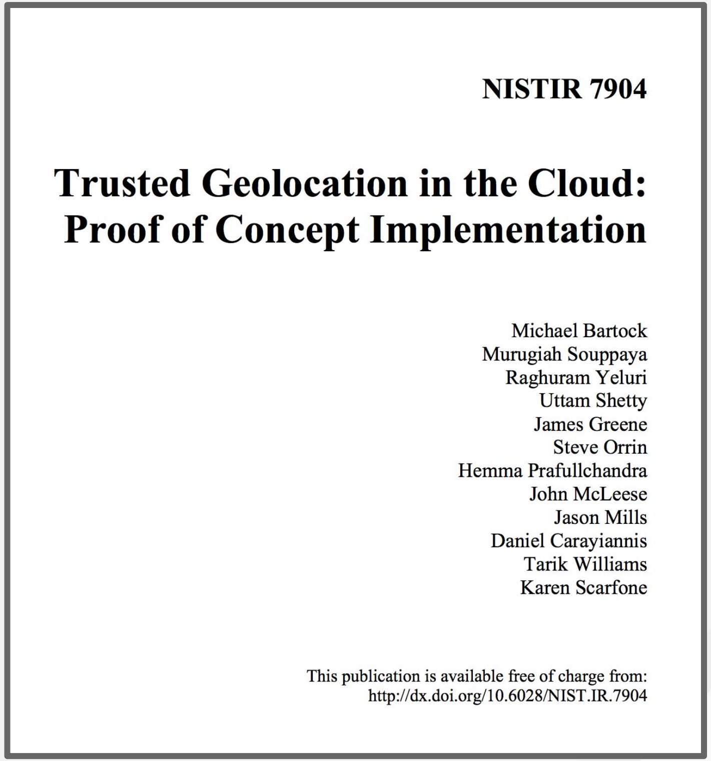
- Establish chain of trust of BIOS, firmware, OS kernel & hypervisor by verifying against configured good values (whitelists)
- Ability to tag/verify hosts with custom attributes stored in TPM
- OpenStack & VMWare integration
- Mutual SSL authentication
- RESTful API
- User defined TLS policies

Trusted Infrastructure

NIST IR-7904 Reference Architecture

- Joint Collaboration between NIST, Intel Corporation, and Software Vendors to demonstrate the ability to control and audit workload and data provisioning based on system trust and geo-location

http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.7904.pdf



NISTIR 7904

Trusted Geolocation in the Cloud: Proof of Concept Implementation

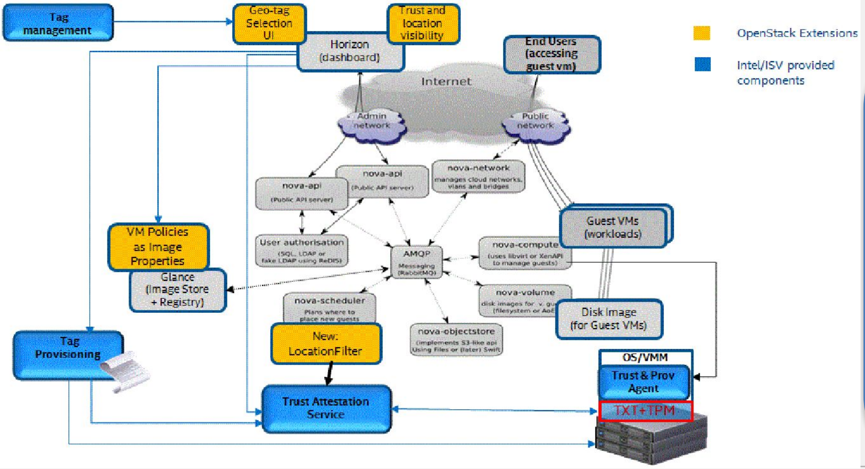
Michael Bartock
Murugiah Souppaya
Raghuram Yeluri
Uttam Shetty
James Greene
Steve Orrin
Hemma Prafullchandra
John McLeese
Jason Mills
Daniel Carayiannis
Tarik Williams
Karen Scarfone

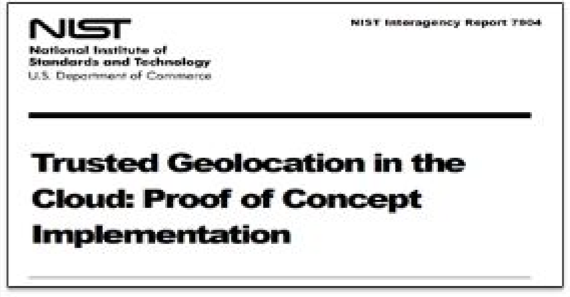
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.7904

Attested Server Tagging & Trusted Geo-location in the Cloud

- Many Trusted Compute Pools Early Adopters also require:
  - GEO tagging
- Regulatory Compliance Requirements:
  - EU data protection directives (95/46/EC)
  - FISMA (geo-tag)
  - Payment Card Industry (PCI-DSS) (asset tag)
  - HIPPA (Asset Tag)

A PoC of the NIST IR 7904 solution is at the NIST National Cyber Center of Excellence (NCCOE) in Rockville, MD


Tag management
Geo-tag Selection UI
Trust and location visibility
Horizon (dashboard)
End Users (accessing guest vm)
Internet
Admin network
Public network
nova-api (Public API server)
nova-api (Public API server)
nova-network manages cloud networks, vlans and bridges
User authorisation (SQL, LDAP or fake LDAP using ReDIS)
AMQP Messaging (RabbitMQ)
nova-compute (uses libvirt or XenAPI to manage guests)
Guest VMs (workloads)
VM Policies as Image Properties
Glance (Image Store + Registry)
nova-scheduler Plans where to place new guests
nova-volume disk images for v. gu (filesystem or AoE
nova-objectstore (implements S3-like api Using Files or (later) Swift
Disk Image (for Guest VMs)
New: LocationFilter
Tag Provisioning
Trust Attestation Service
OS/VMM
Trust & Prov Agent
TXT+TPM
🟨 OpenStack Extensions
🟦 Intel/ISV provided components



NIST

National Institute of Standards and Technology

U.S. Department of Commerce

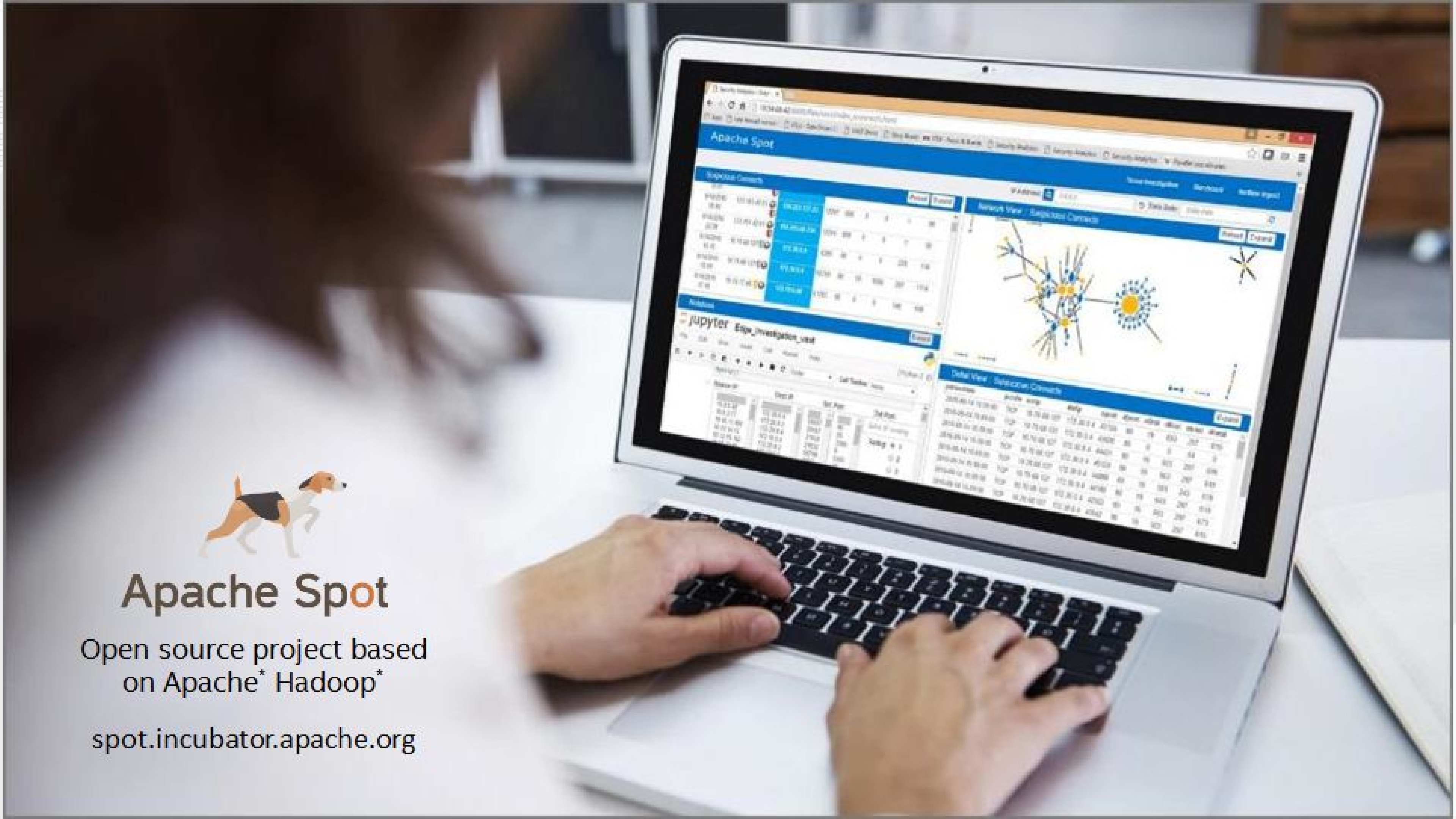
NIST Interagency Report 7904

Trusted Geolocation in the Cloud: Proof of Concept Implementation

NIST IR 7904 –USG recommendation for "Trusted Geolocation in the Cloud"

Trusted resource pool based on hardware-based secure technical measurement capability

- **Platform attestation and safer hypervisor launch** - Provide integrity measurement and enforcement for the compute nodes
- **Trust-based secure migration** - Provide geolocation measurement and enforcement for the compute nodes


Apache Spot
Suspicious Connects
Network View : Suspicious Connects
Detail View : Suspicious Connects
jupyter
Reset
Expand

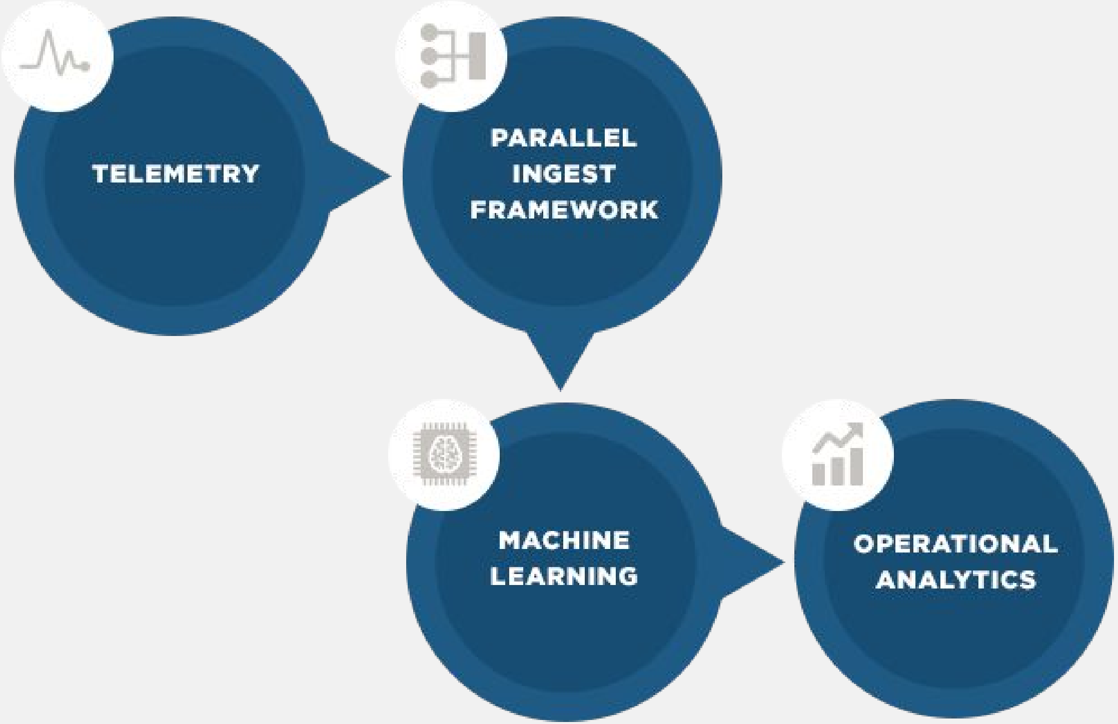
Apache Spot

Open source project based on Apache* Hadoop*

spot.incubator.apache.org

- Network Flows (nfcapd)
- DNS (PCAP)
- Proxy

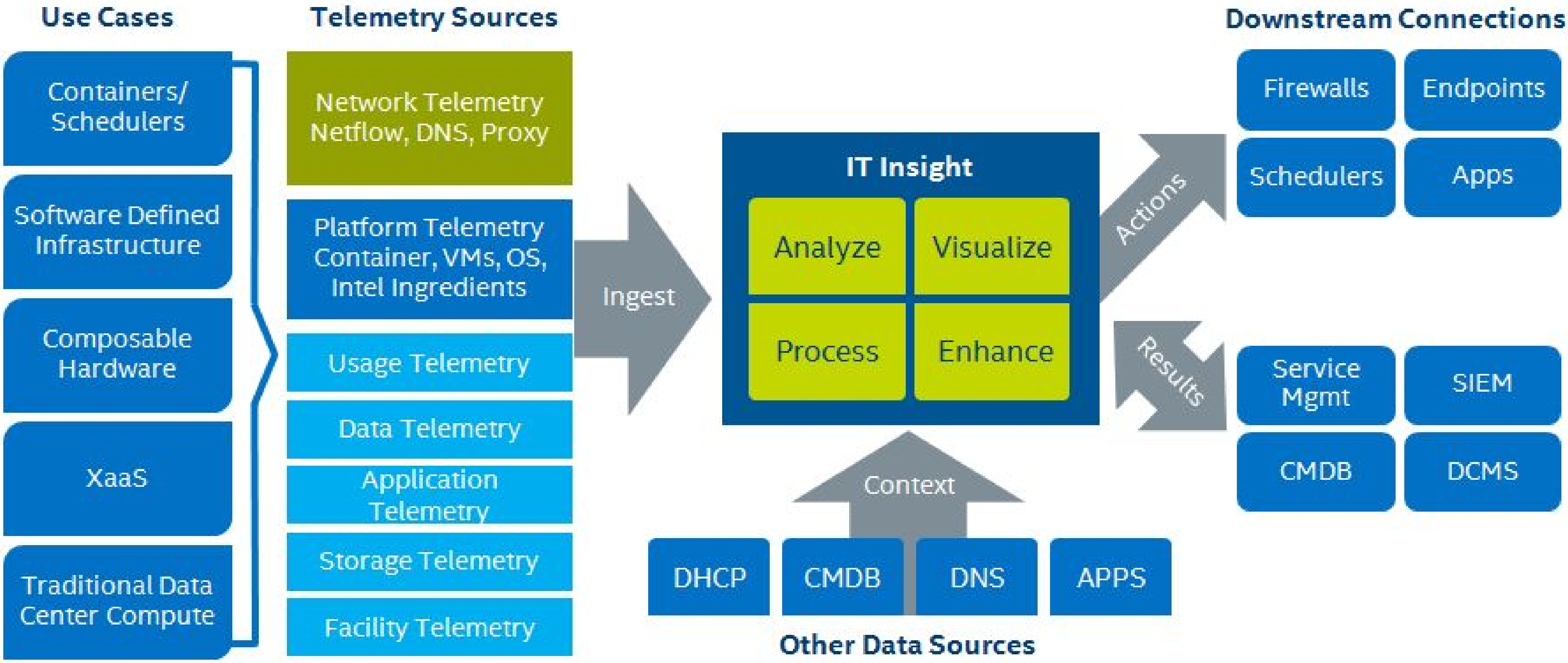
- Open source decoders
- Load data in Hadoop



- Filter billions of events to a few thousand
- Unsupervised learning

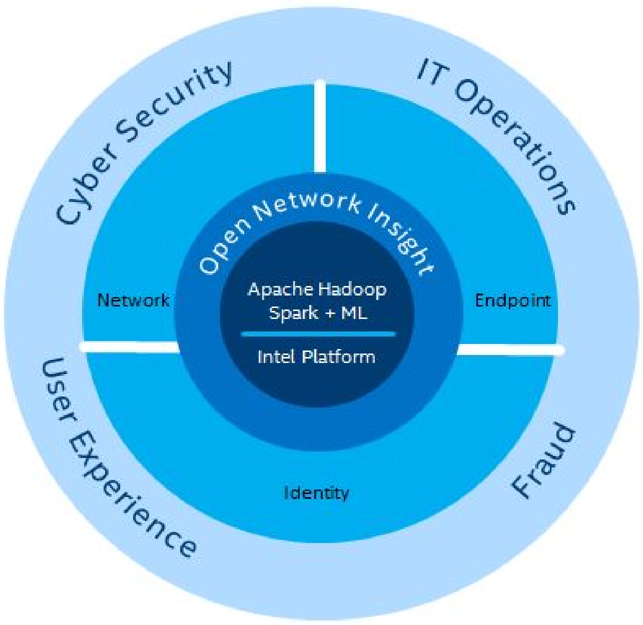
- Visualization, attack heuristics noise filter

The Apache Spot Solution Approach



The Apache Spot Solution Approach

Spot Open Data Models

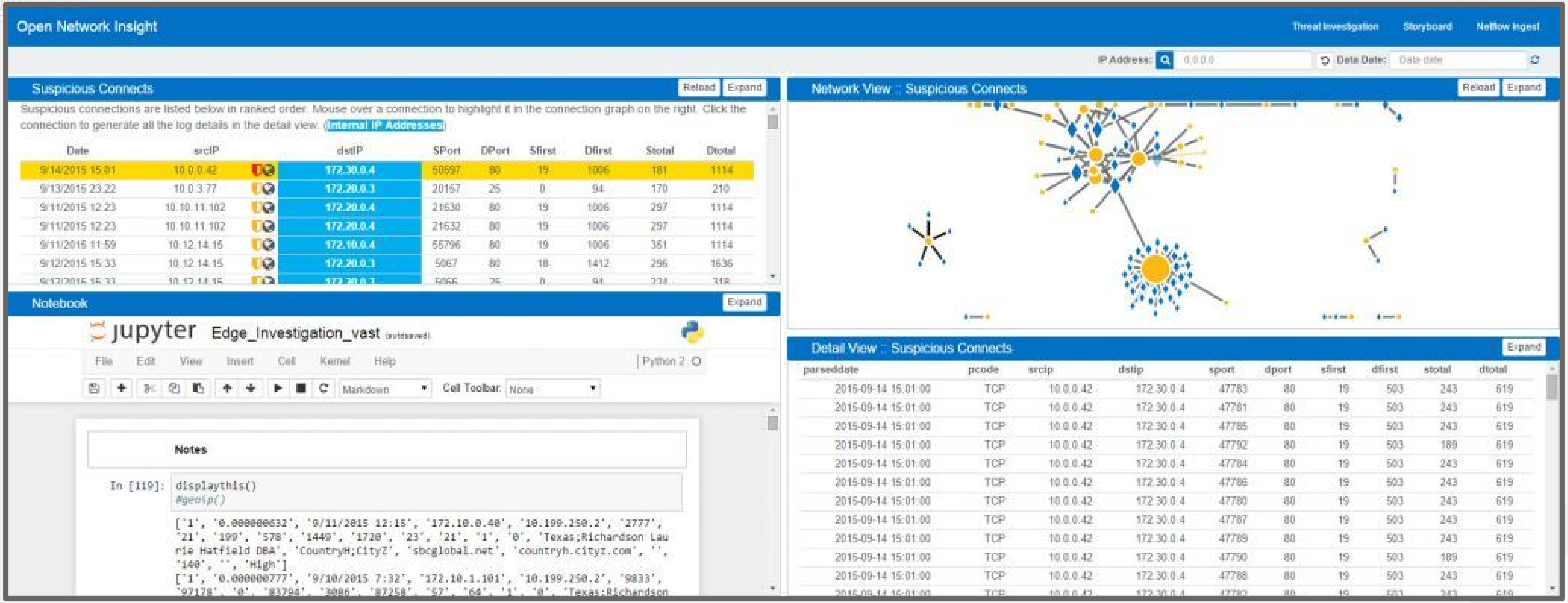


Extending Analytics

Enhanced and Additional Algorithms

- Broader Event Data Types
- Correlation for Incident Response
- Predictive Research
- Root Cause Analysis
- Wider Scope of Analysis

Threat Intelligence Powered by Analytics



Suspicious Connects

Suspicious connections are listed below in ranked order. Mouse over a connection to highlight it in the connection graph on the right. Click the connection to generate all the log details in the detail view. (Internal IP Addresses)

Date	srcIP	dstIP	SPort	DPort	Sfirst	Dfirst	Stotal	Dtotal
9/14/2015 15:01	10.0.0.42	172.30.0.4	50597	80	19	1006	181	1114
9/13/2015 23:22	10.0.3.77	172.20.0.3	20157	25	0	94	170	210
9/11/2015 12:23	10.10.11.102	172.20.0.4	21630	80	19	1006	297	1114
9/11/2015 12:23	10.10.11.102	172.20.0.4	21632	80	19	1006	297	1114
9/11/2015 11:59	10.12.14.15	172.10.0.4	55796	80	19	1006	351	1114
9/12/2015 15:33	10.12.14.15	172.20.0.3	5067	80	18	1412	296	1636
9/12/2015 15:33	10.12.14.15	172.20.0.3	5066	25	0	94	224	318

Notes

```
In [119]: displaythis()
          #geoip()

          ['1', '0.000000632', '9/11/2015 12:15', '172.10.0.40', '10.199.250.2', '2777',
          '21', '199', '578', '1449', '1720', '23', '21', '1', '0', 'Texas;Richardson Lau
          rie Hatfield DBA', 'CountryH;CityZ', 'sbcglobal.net', 'countryh.cityz.com', '',
          '140', '', 'High']
          ['1', '0.000000777', '9/10/2015 7:32', '172.10.1.101', '10.199.250.2', '9833',
          '97178', '0', '83794', '3086', '87250', '57', '64', '1', '0', 'Texas;Richardson
```

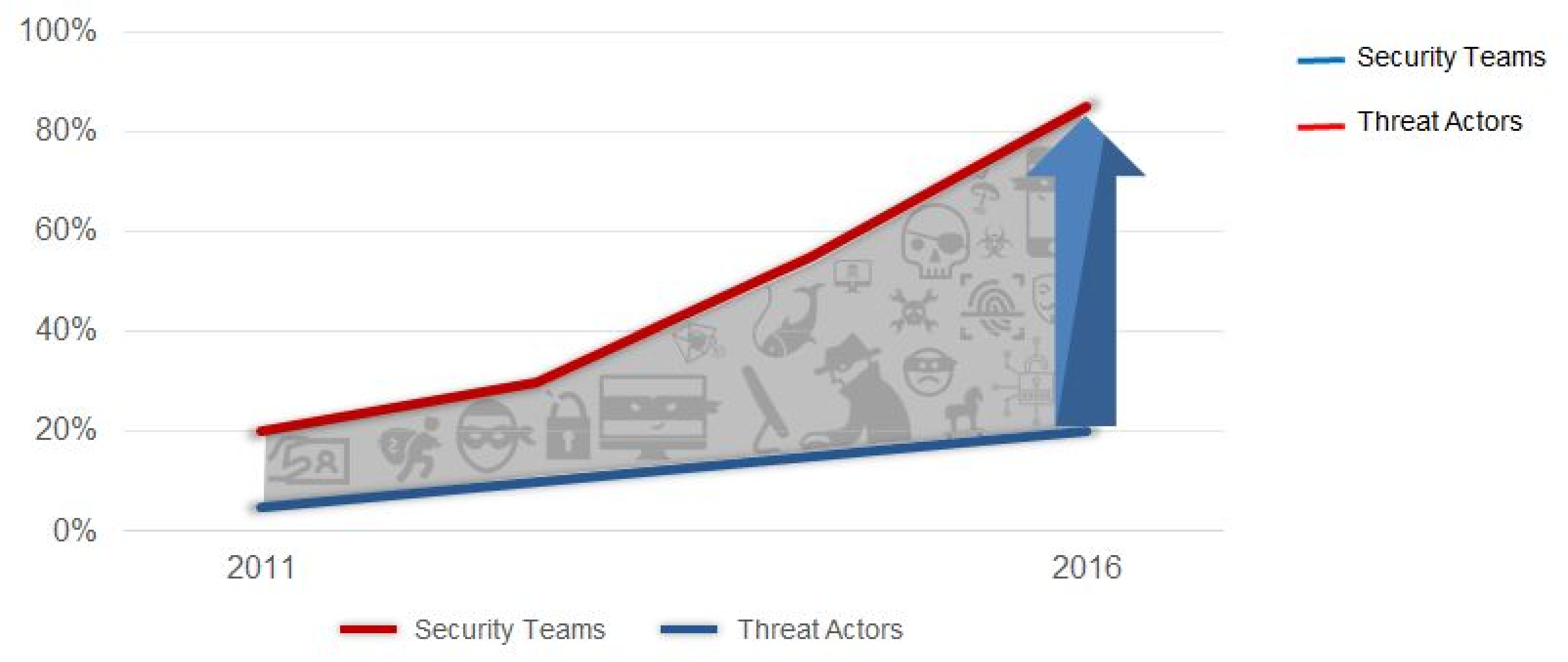
Detail View :: Suspicious Connects

parseddate	pcode	srcip	dstip	sport	dport	sfirst	dfirst	stotal	dtotal
2015-09-14 15:01:00	TCP	10.0.0.42	172.30.0.4	47783	80	19	503	243	619
2015-09-14 15:01:00	TCP	10.0.0.42	172.30.0.4	47781	80	19	503	243	619
2015-09-14 15:01:00	TCP	10.0.0.42	172.30.0.4	47785	80	19	503	243	619
2015-09-14 15:01:00	TCP	10.0.0.42	172.30.0.4	47792	80	19	503	189	619
2015-09-14 15:01:00	TCP	10.0.0.42	172.30.0.4	47784	80	19	503	243	619
2015-09-14 15:01:00	TCP	10.0.0.42	172.30.0.4	47786	80	19	503	243	619
2015-09-14 15:01:00	TCP	10.0.0.42	172.30.0.4	47780	80	19	503	243	619
2015-09-14 15:01:00	TCP	10.0.0.42	172.30.0.4	47787	80	19	503	243	619
2015-09-14 15:01:00	TCP	10.0.0.42	172.30.0.4	47789	80	19	503	243	619
2015-09-14 15:01:00	TCP	10.0.0.42	172.30.0.4	47790	80	19	503	189	619
2015-09-14 15:01:00	TCP	10.0.0.42	172.30.0.4	47788	80	19	503	243	619
2015-09-14 15:01:00	TCP	10.0.0.42	172.30.0.4	47782	80	19	503	243	619

Automation and Information Sharing Enhances Security

- Capabilities
  - Automated provisioning of patches & updates
  - Automated system/node refresh
  - Dynamic Security controls
  - SW defined Network and Host Security services
  - Automated Workload configuration for Security Baselines
  - Automated Compliance
- Benefits
  - Real time threat response and mitigation (get the human out of the loop)
  - Reduce window of exposure
  - Reduce risk during active attacks and campaigns
- Information Sharing - Beyond IoC’s!
  - Sharing Automation scripts, techniques, and best known practices must be a key part of the Information Sharing

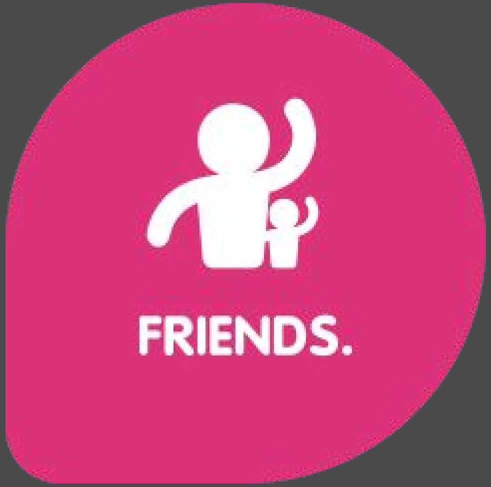
Closing the Threat Gap with Analytics, Automation, and Information Sharing



THE
FEDORA
PROJECT
COMMUNITY

WE CAN DO MORE WHEN WE WORK TOGETHER

- 100% free, legal, redistributable
- Software. Artwork. Project Code. **EVERYTHING.**
- **Never cutting corners.**



- **Everyone has something to give.**
- Thousands of active contributors.
- Disagreement, then discussion, then consensus.

- **Technical excellence.**
- Upstream collaboration.
- Our features become part of others.

- **Innovation.**
- We don’t wait for others to do the heavy lifting.
- Rapid release cycle.
- Community R&D lab.

fedora
SECURITY LAB

Fedora Red Team

- Offensive tooling
- Exploit Curation
- Offensive Standards
- Offensive Reference Architectures

https://fedoraproject.org/wiki/SIGs/Red_Team

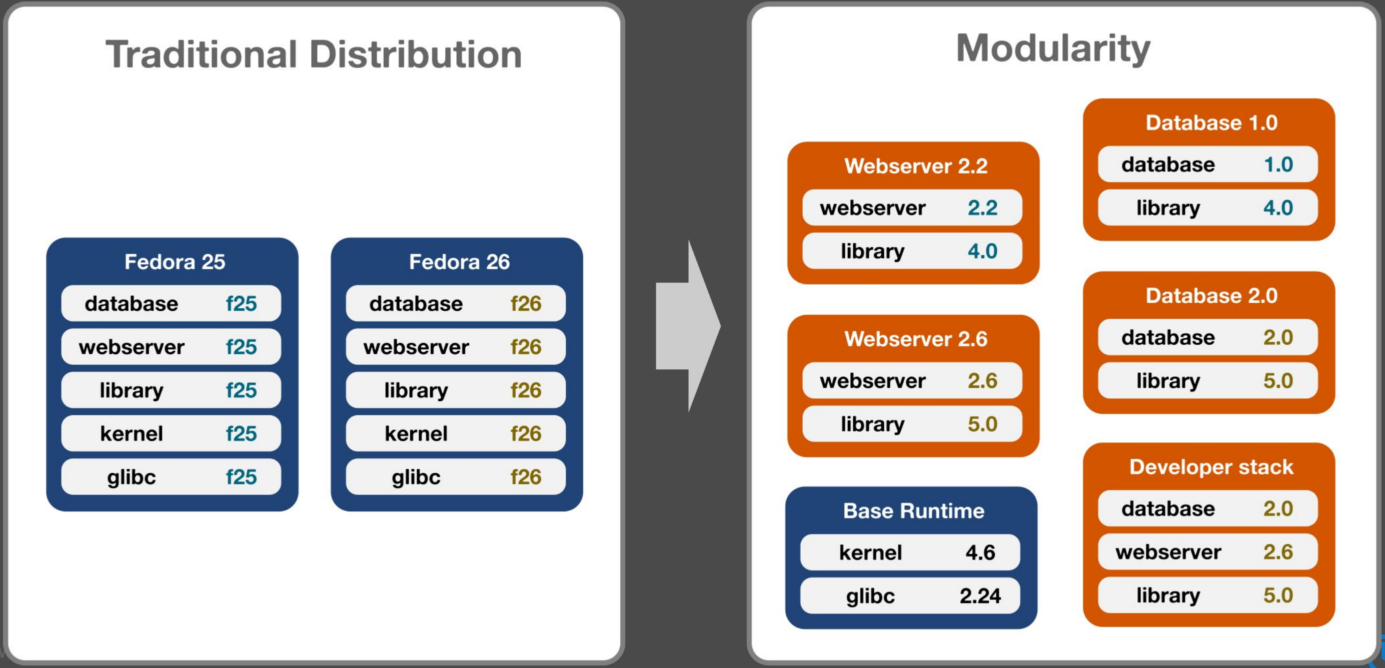
Fedora Blue Team

https://tbd

- Defensive tooling
- Active Cyber Defense platforms
- Reference architectures

NSC

fedora modularity



Traditional Distribution

Fedora 25	
database	f25
webserver	f25
library	f25
kernel	f25
glibc	f25

Fedora 26	
database	f26
webserver	f26
library	f26
kernel	f26
glibc	f26

Modularity

Webserver 2.2	
webserver	2.2
library	4.0

Webserver 2.6	
webserver	2.6
library	5.0

Base Runtime	
kernel	4.6
glibc	2.24

Database 1.0	
database	1.0
library	4.0

Database 2.0	
database	2.0
library	5.0

Developer stack	
database	2.0
webserver	2.6
library	5.0

Thank you!