Mid-Atlantic CIO Forum Welcome

March 2018, Fulton MD

Rev: July 2017

Agenda

Topic	Presenter	Time
Cisco Welcome & the Needed Security Tools & Strategies	Nick Hamilton & Bryan Brown (Cisco)	9 to 9:30
Real Security War Stories: Best Practices for Keeping the Bad Guys at Bay	Jaeson Schultz (Cisco TALOS)	9:30 to 10:30
Break		
Security Strategy for Today's Expanded Attack Surface	David Manning (Presidio)	11 to 11 50
Lunch		12 to 1
Security Networking Group Meeting	Chris Ireland & John Holmes	1 PM to 2:30 PM

Welcome

To the Cisco Maple Lawn Campus

Collaborate + Create = Innovate

Cisco Workplace Transformation 2012–2017

+17%	+17%	+15%	-11%
Increase in Employee Engagement	Increase in Workplace Satisfaction	Increase in Work/Life Balance	Decrease in Safety Incidents

Cisco Enterprise and What We Must Protect

15 billion NetFlows

170 countries

26 k Remote Workers

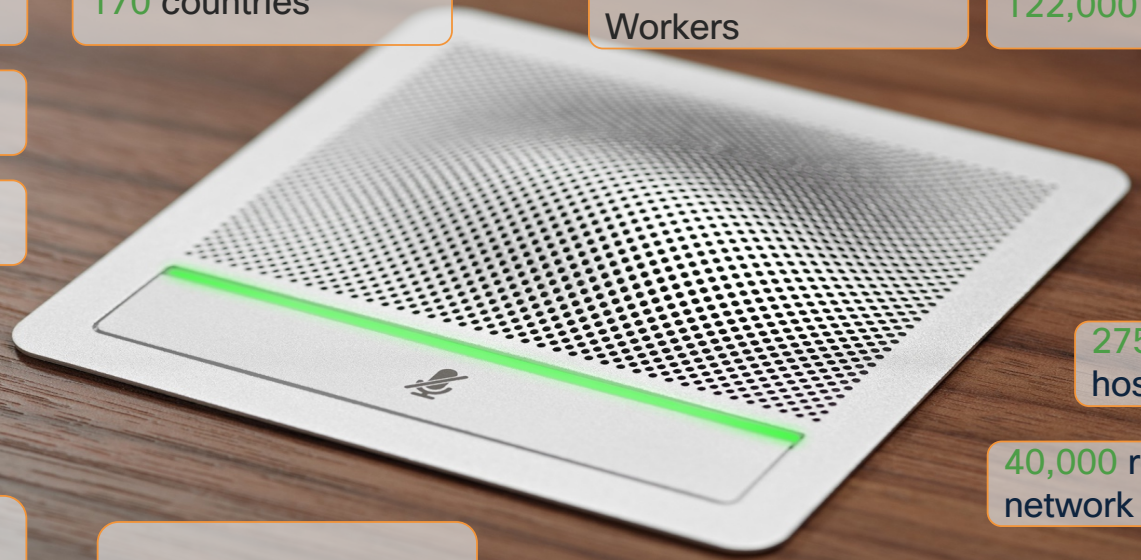
122,000 employees

4.8 billion DNS records

68,000 FTEs

2 billion system events

56,000 vendors



75 million web transactions

275,000 Total hosts

40,000 routers on network

1.2M web transactions automatically blocked

94% of incoming emails blocked (ESA)

12 Critical Enterprise Production DCs

47TB traffic inspected

1500 Labs globally

More than 25,000 Channel Partners

Over 100 Application Service Providers

750GB system logs collected

Secure, Intelligent Platform for Digital Business

Security is Foundational

Reinvent the Network

Embrace a Multi-Cloud World

Unlock the Power of Data

Employee and Customer Experience

Increased Pace of Innovation

Transition to Bryan

Why are you here today ?

"Growth tops the list of business priorities reported by CIOs for 2018, according to Gartner's 2018 CIO Agenda Report. … all CIOs (95 percent) consistently expect cyber-threats to rise and affect their organization."

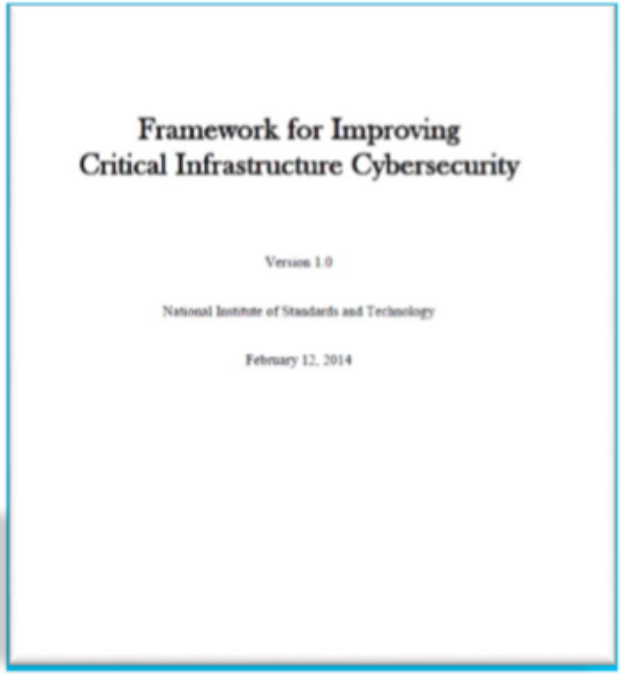
"..reforming cyber risk as a strategic business risk versus just an information technology or an information security risk." Sarah Stephens, head of cyber, content and new technology risks at insurance broker JLT, based in London

Learn more about the Security landscape and how to address your organization's Security needs…

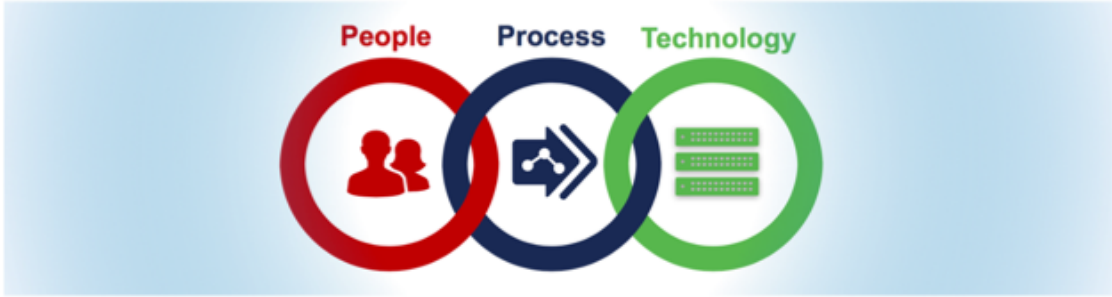
NIST

National Institute of Standards and Technology

U.S. Department of Commerce



Promoting Cybersecurity Best Practices



Framework covers all three

STRENGTHENING THE CYBERSECURITY OF FEDERAL NETWORKS AND CRITICAL INFRASTRUCTURE

Executive Order

May 2017

"Effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cybersecurity risk."

Core Functions & Categories

Function		Category	
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

- Know what you have
- Secure what you have
- Spot threats quickly
- Take action immediately
- Restore operations

Technology Doesn't Cover Everything

Function		Category		People	Process	Technology
ID	Identify	ID.AM	Asset Management	Applies	Applies	Applies
		ID.BE	Business Environment	Applies	Applies	
		ID.GV	Governance	Applies	Applies	
		ID.RA	Risk Assessment	Applies	Applies	Applies
		ID.RM	Risk Management Strategy	Applies	Applies	
PR	Protect	PR.AC	Access Control	Applies	Applies	Applies
		PR.AT	Awareness and Training	Applies	Applies	
		PR.DS	Data Security	Applies	Applies	Applies
		PR.IP	Information Protection Processes and Procedures	Applies	Applies	Applies
		PR.MA	Maintenance	Applies	Applies	Applies
		PR.PT	Protective Technology	Applies	Applies	Applies
DE	Detect	DE.AE	Anomalies and Events	Applies	Applies	Applies
		DE.CM	Security Continuous Monitoring	Applies	Applies	Applies
		DE.DP	Detection Processes	Applies	Applies	
RS	Respond	RS.RP	Response Planning	Applies	Applies	
		RS.CO	Communications	Applies	Applies	
		RS.AN	Analysis	Applies	Applies	Applies
		RS.MI	Mitigation	Applies	Applies	Applies
		RS.IM	Improvements	Applies	Applies	
RC	Recover	RC.RP	Recovery Planning	Applies	Applies	
		RC.IM	Improvements	Applies	Applies	
		RC.CO	Communications	Applies	Applies	

- **Only half** of the Framework's Categories are addressed by **technology**
- Highlights the importance of both **people and process** in cybersecurity

NIST CSF
Ciscolive.com

View all Sessions

Introduction to NIST Cybersecurity Framework for Your Security Architecture & Plan - BRKSEC-1021

Michael Lin, Systems Engineering Manager , Cisco

We have all heard it in the news... Higher Education institutions, K-12 school districts, government, retailers, financial institutions, service providers, etc, are all targets for hackers and victims of DDOS and ransomware attacks. In today's dynamic security environment, it's no longer a matter of "if" an attacker will get in, but "when." And when compromised, what is the plan to get operations restored as effectively and quickly as possible. Professionals need to evolve their strategy from a point-in-time approach to a continuous model that addresses the full attack continuum- before, during and after an attack. Those that are tasked with security need to understand that having a security strategy/plan is not just solved by applying technology, but also people and process. In this breakout session, you will learn to apply the NIST (National Institute of Standards and Technology) Cybersecurity Framework to your institution's security plan. Lastly, this session will show you how Cisco's threat centric solutions are mapped to the NIST Framework.

Event

2017 Las Vegas

Focus

Best Practices

Level

Introductory

Solutions

Secure Access, Secure Identity, TrustSec

Technology

Enterprise Architecture, Security

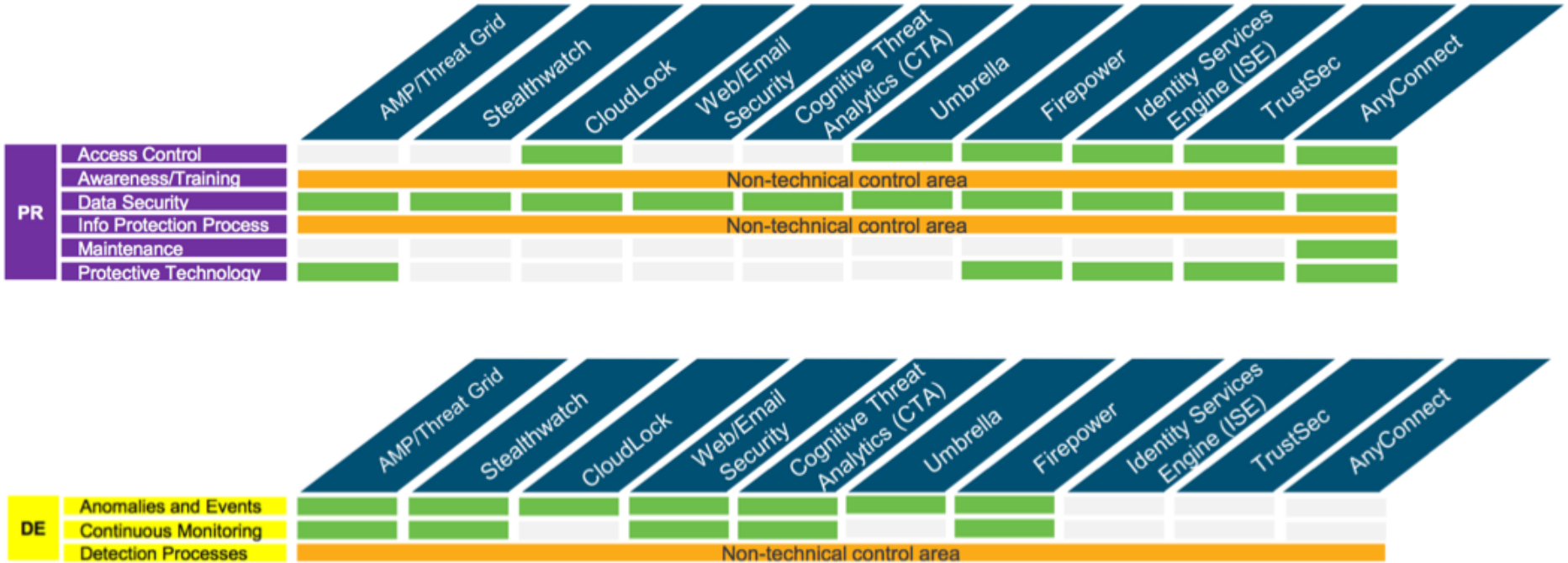
Documents

Session Presentation

Watch Session

Session Video

NIST CSF
Ciscolive.com



cisco.com/go/security

Cisco Security Report

cisco.com/go/security

Burst Attacks – 42% of organizations experienced DDoS, most lasting only a few minutes.

IOT – 31% has experienced attacks on IOT infrastructure.

NYETYA – installed on more then 1 Million computers.

60% of Malicious Domains tied to SPAM Campaigns

SandBox Evasion Tactics…

Security is perceived as the most common benefit of using the cloud.

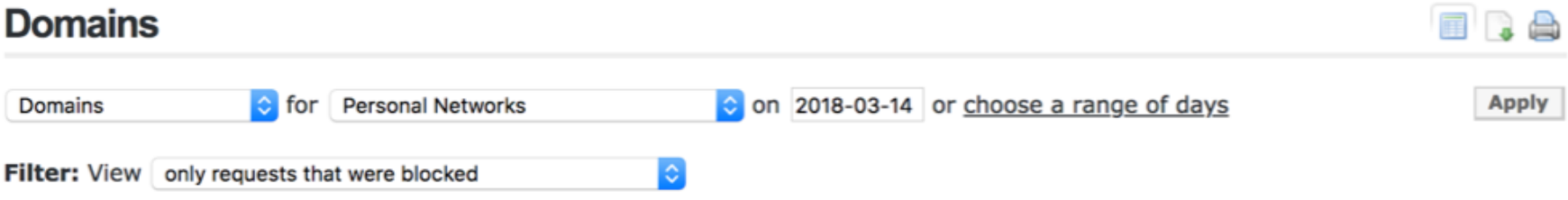
Encryption – Malware using Encryption to bypass detection

Cisco Security Report

cisco.com/c/en/us/products/security/security-reports.html

Near
from
72%

OpenDNS.com



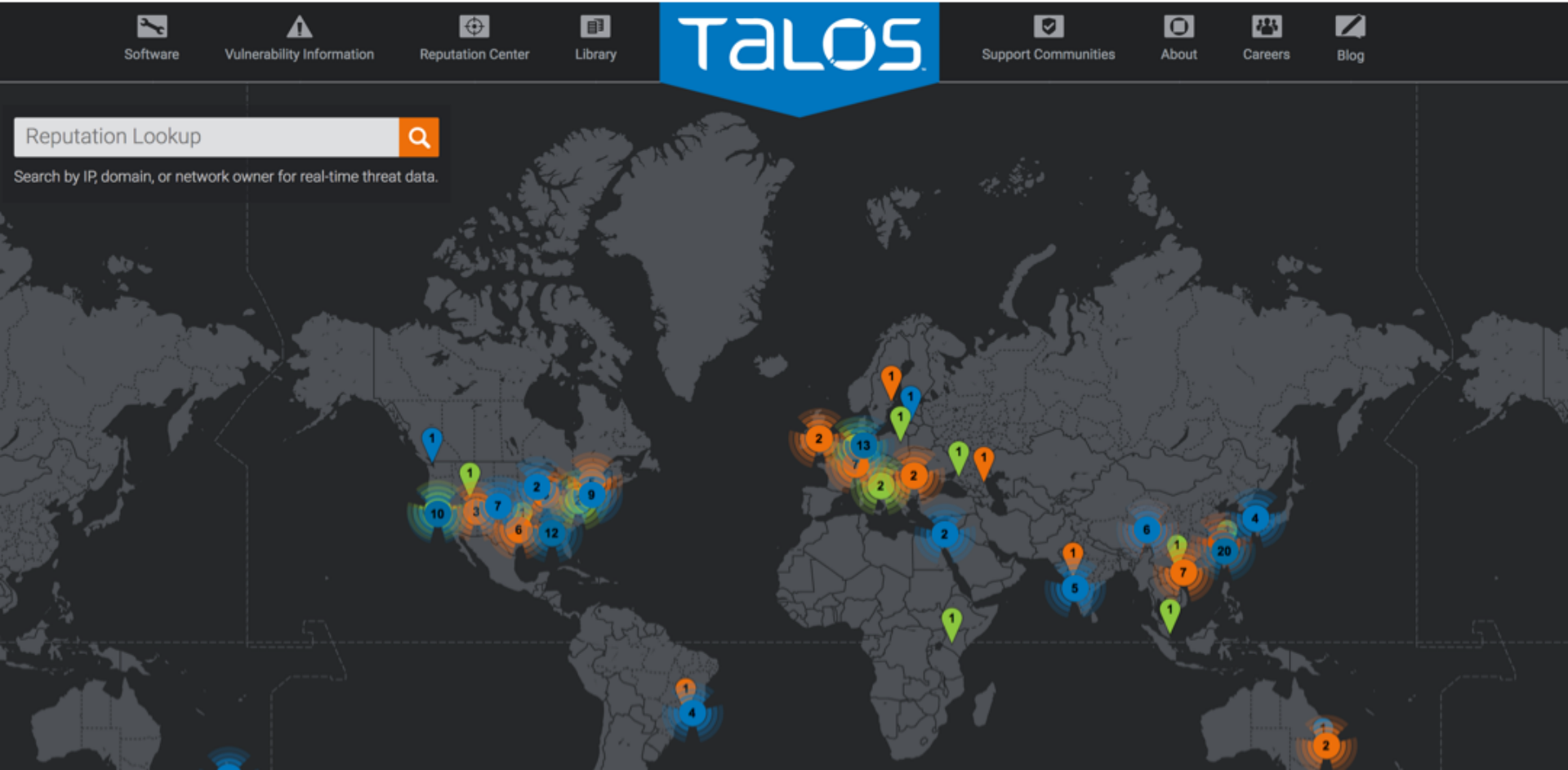
This domain is blocked.

Site blocked. [DOMAIN] is not allowed on this network. This has been logged. Go see Mom if this is an issue you care to discuss with her...

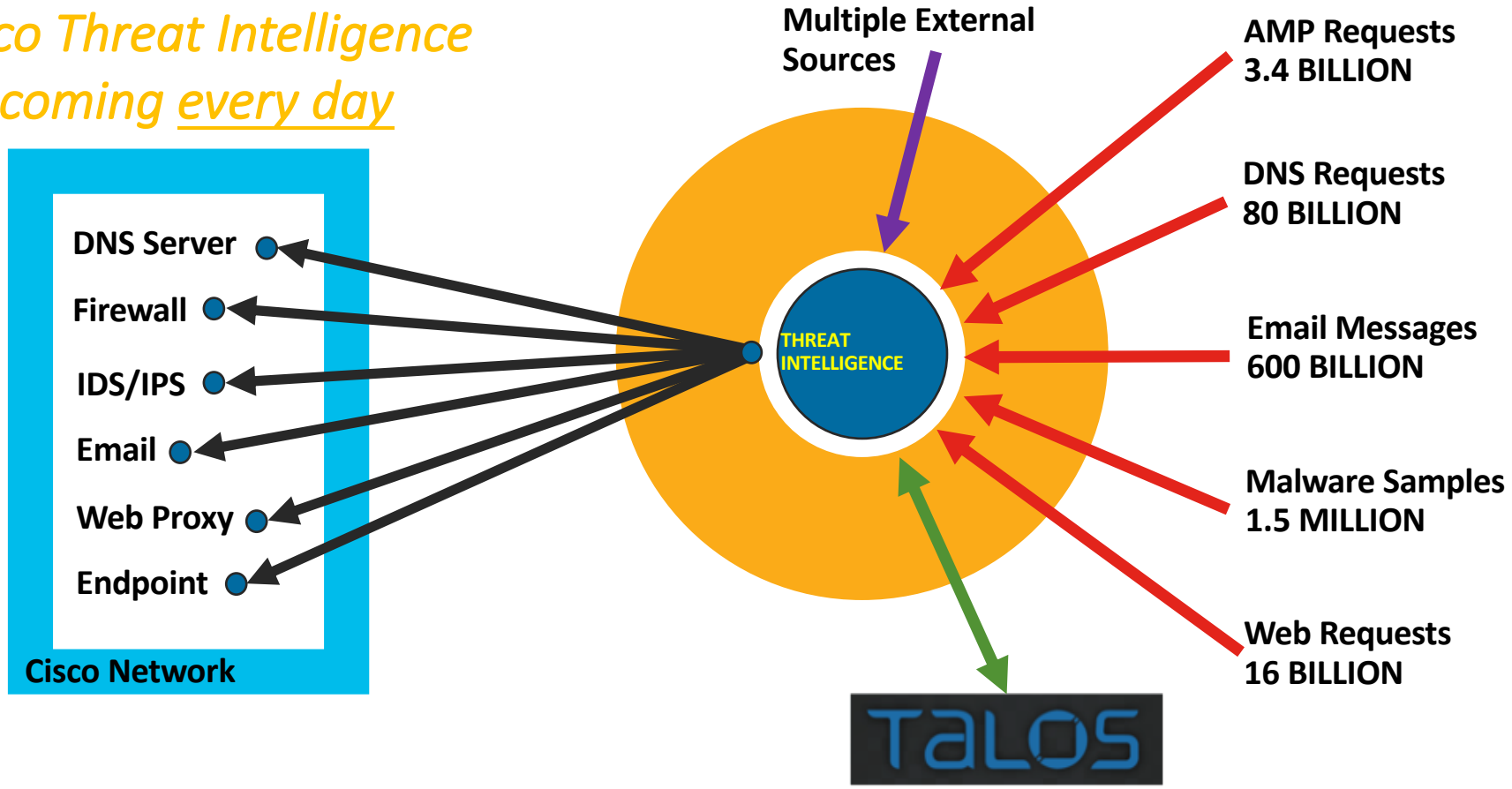
OpenDNS GUIDE

example.com

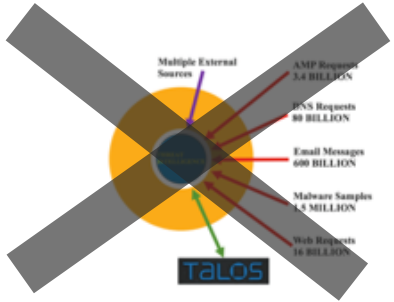
Talosintelligence.com

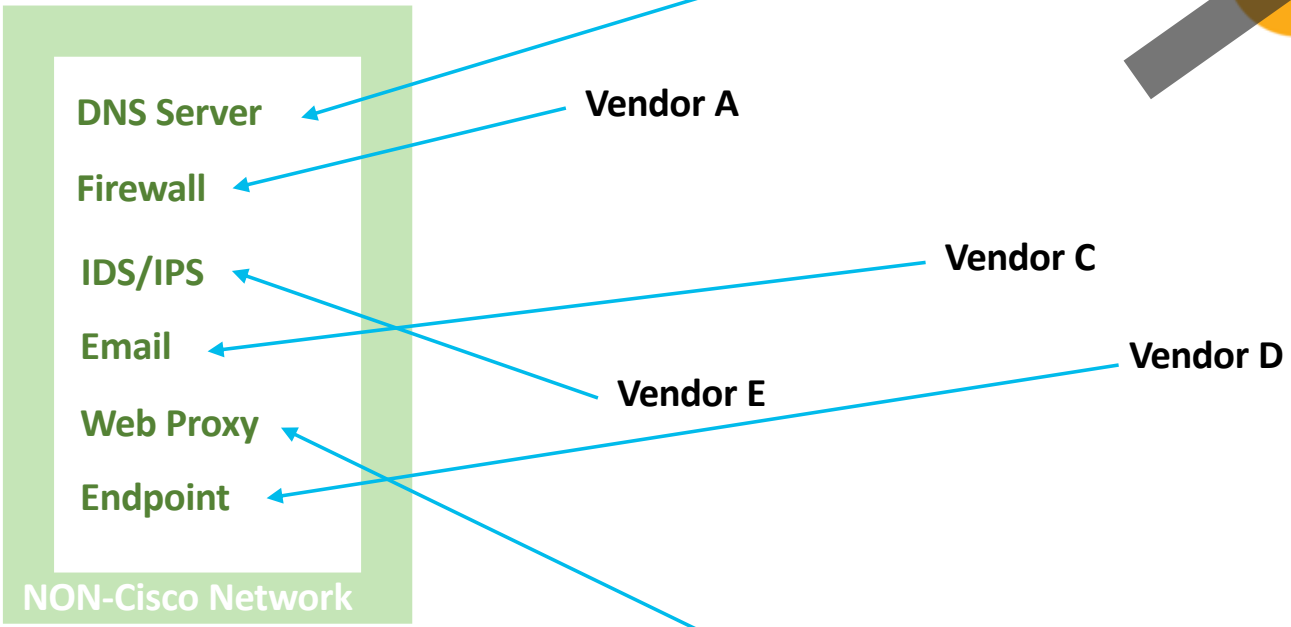


Cisco Threat Intelligence - Incoming every day

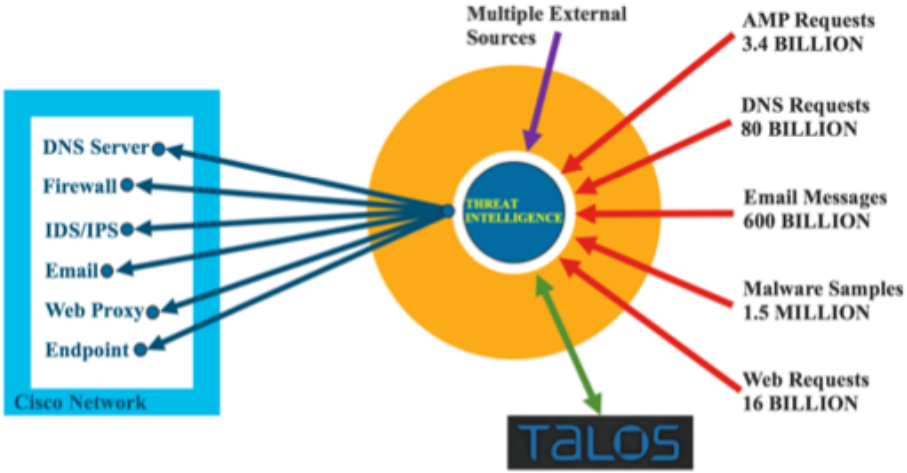


Threat Intelligence
- Who is doing Threat Intel?





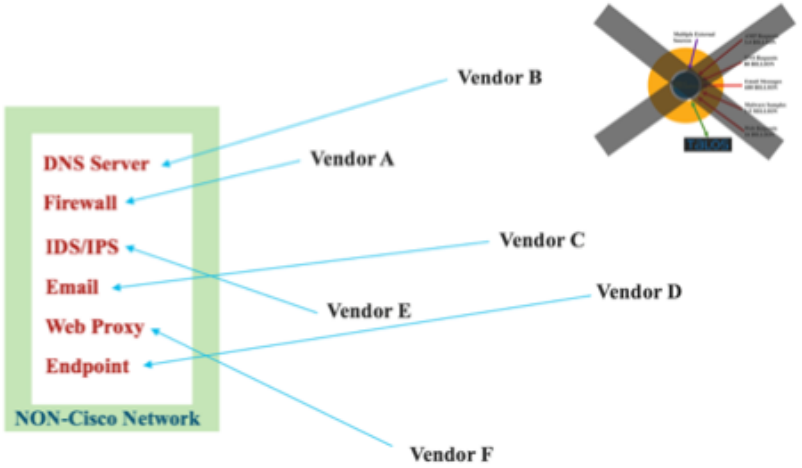
Cisco End to End Security



In respect of Threat Intelligence:

- Strategic investment ✔
- Architecture for action ✔
- Consistent treatment ✔

Multi Vendor Security



In respect of Threat Intelligence:

- Strategic investment ?
- Architecture for action ?
- Consistent treatment ?