Emerging Cybersecurity Threats & Challenges

Ohio Information Security Conference
March 9, 2016
Dayton, OH

Richard Staynings
Cisco Cybersecurity

Agenda

- Cisco ASR 2016 Findings
- Current Security Challenges
- How do we go about Out-Smarting Attackers?

2016 Annual Security Report

Attackers are tapping into legitimate resources, becoming adept at deploying hard-to-detect and highly profitable campaigns

Defenders confidence is declining, but awareness is driving action to deploy new strategies

Collaboration is needed to combat today's innovative and persistent attacks and develop architecture for tomorrow

Good News

Security Weighs on the Minds of Executives

48% Of Executives Very Concerned About Security

41% Much More Concerned Than 3 Years Ago

92% Agreed that more security risk Information will be expected by investors and regulators

Security has now become the Number 1 or Number 2 Business Enterprise Risk for many organizations

Many Boards can now even spell ‘CYBERSECURITY’

We still have a way to go however!

Direct Attacks Generate Big Profits

Angler / other ransomeware attacks - More efficient and more lucrative

>> >> “Per Campaign!”

Hollywood hospital becomes ransomware victim

The cyberattack prompted the centre to declare an "internal emergency," with access to IT systems left locked and held for ransom.

By Charlie Osborne for Zero Day | February 15, 2016 -- 12:23 GMT (04:23 PST) | Topic: Security

RELATED STORIES


Security
Ransomware: How much would you pay to get your files back?


Government
Obama's gadgets: What tech does the president use?

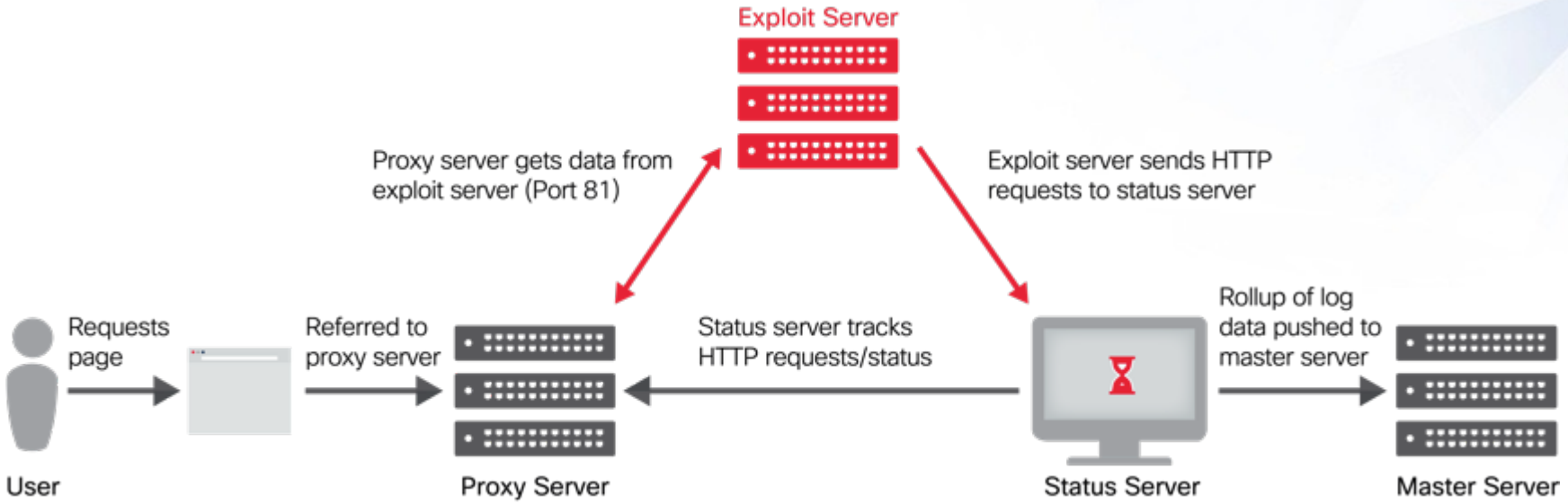

CXO
Online security? Just let me Google that, say puzzled bosses


Security
Mandated encryption backdoors? Such a bad idea, says cybersecurity agency

NEWSLETTERS

Attacker's Infrastructure is Resilient

Designed to evade and reconstitute



Many companies are playing Whack-a-mole when hunting malware

Go Back to Basics

Need for Holistic Security
– not point solutions!

We need to patch quickly!
Failure to patch could cost $millions!

THE AGE
Victoria

Hack attack on a hospital IT system highlights the risk of still running Windows XP

January 20, 2016 2.22pm EST

Victoria News | Traffic Conditions | Melbourne Liveability | Quizzes

You are here: Home » Victoria »

Royal Melbourne Hospital attacked by damaging computer virus

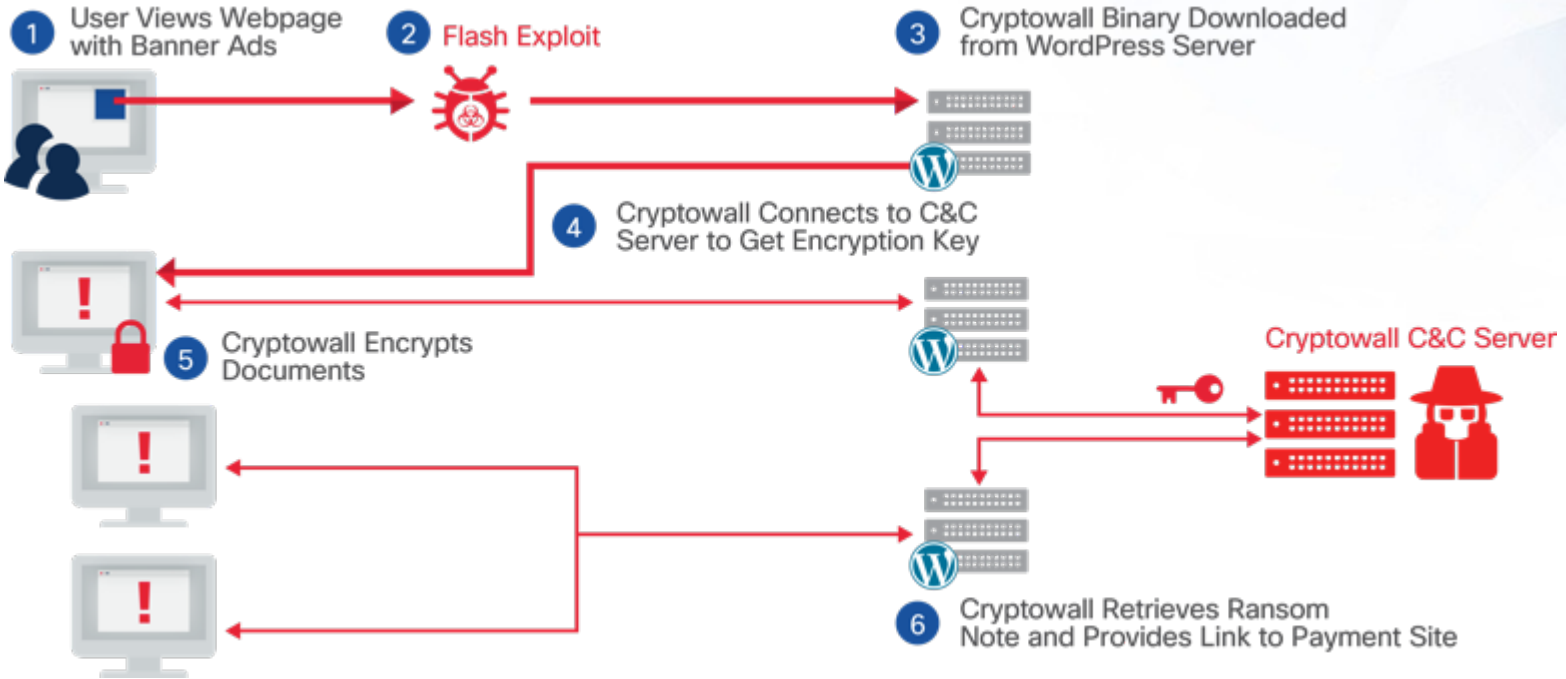
Qbot virus still attacking Royal Melbourne Hospital

A computer virus that can steal passwords is still causing headaches at one of Melbourne's largest hospitals.

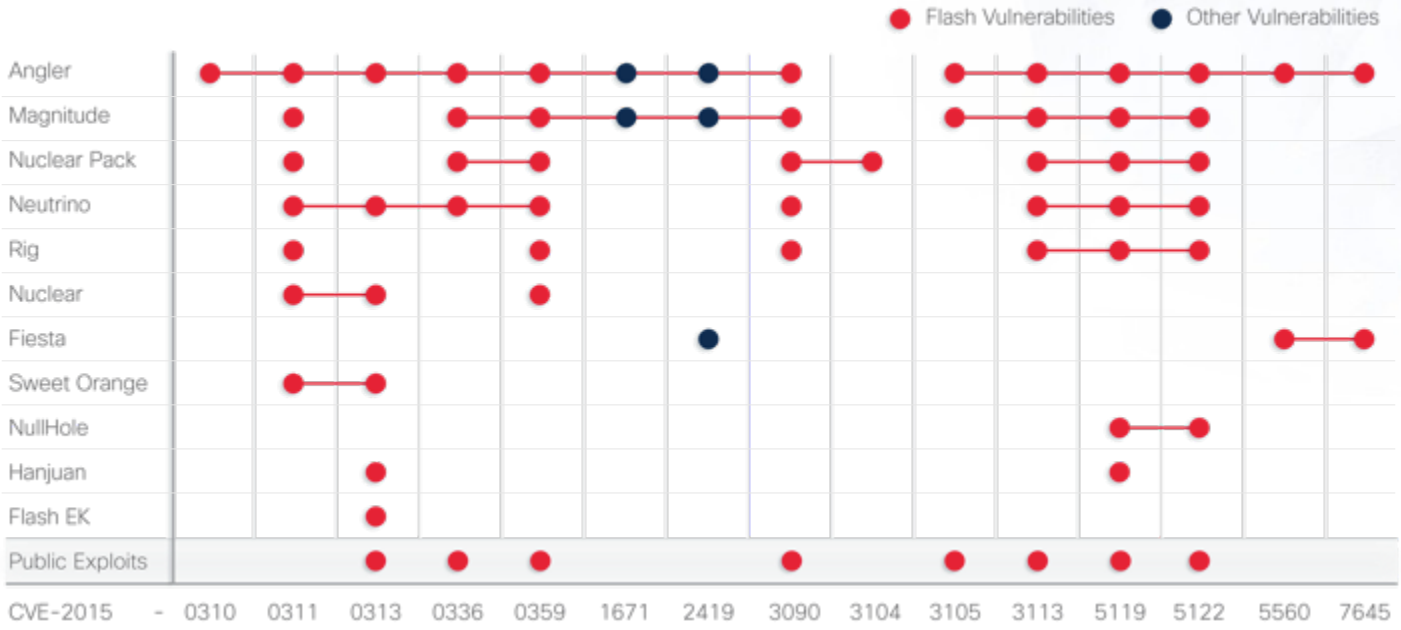
By Chris Duckett | February 2, 2016 -- 04:51 GMT (20:51 PST) | Topic: Security

Vulnerable Infrastructure is Broadly and Quickly Exploited

221 percent increase in WordPress Attacks



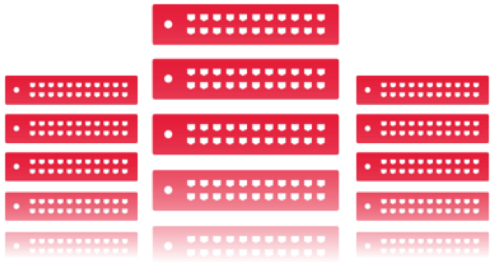
Hackers Love Flash! The less patched the better!



Flash platform is a popular threat vector for cybercriminals

DNS: A potential quick victory

A blind spot for attackers to gain command and control, exfiltrate data, and redirect traffic



91.3%

of malware uses DNS

68%

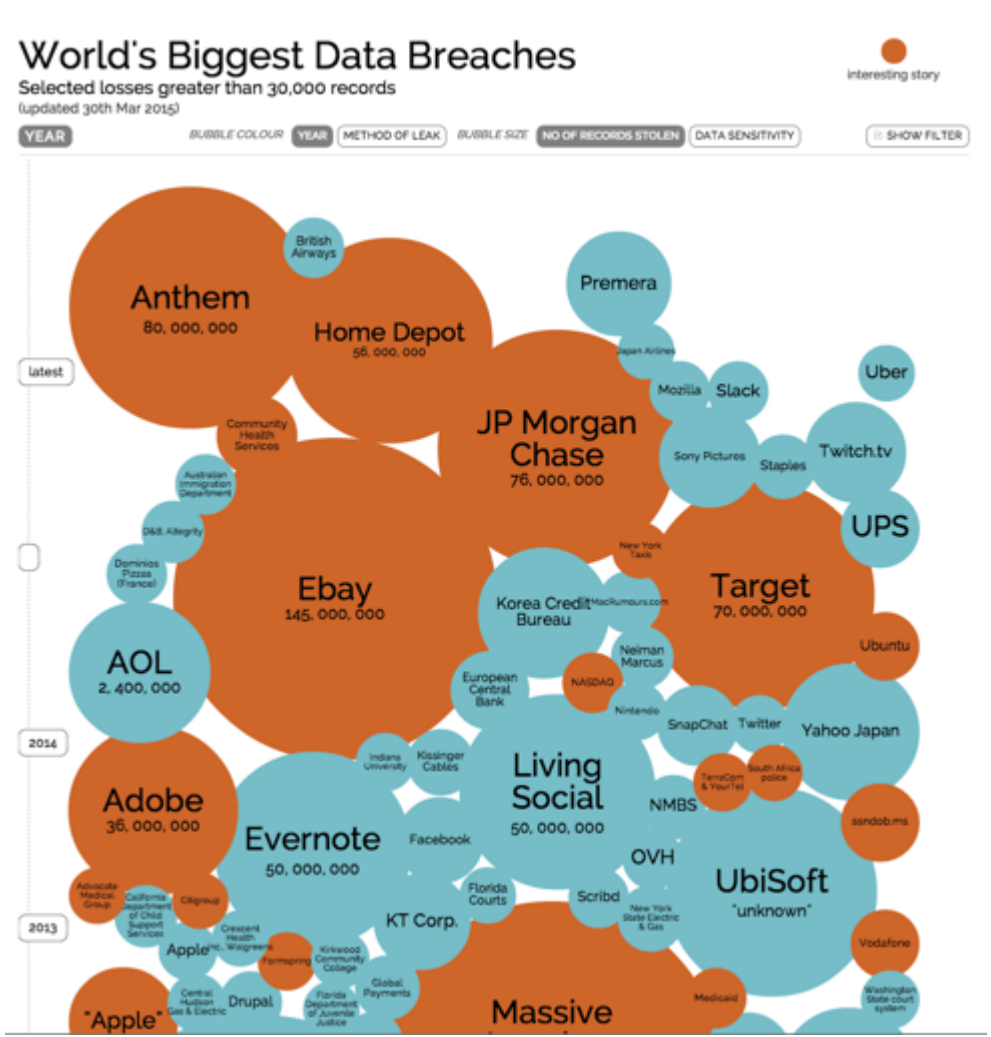
of organizations **don't** monitor it

Browser Infections: The Pest That Persists

More than

85%

of the companies studied were affected each month



Breaches are increasing in scope, size and frequency.

Its no longer a question of **"IF"** you get hacked its now one of **"WHEN"** you get hacked and …….**HOW OFTEN**?

What has Changed?

The Changing Face of …… Security

The Digital Evolution

Security Challenges

Changing Business Models

Dynamic Threat Landscape

Complexity and Fragmentation

Fortress Mentality No Longer Works

Many holes in the walls and we no longer control what's inside

BYOD

90% of organizations are not fully aware of all devices on the network

Cloud

5x to 10x more cloud services being used than known to IT

Dynamic Threat Landscape

Social Media

29% of successful breaches used social media to target the end user

Resource Shortage

12x demand over supply for security staff

Dynamic Threat Landscape

It’s a matter of Time

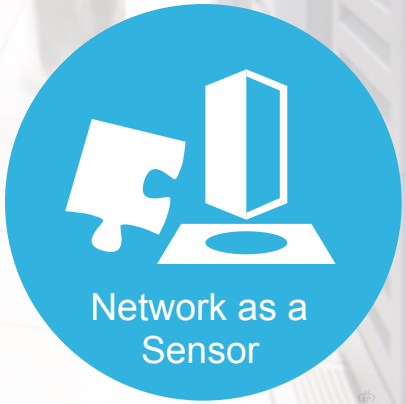
60% of data stolen in hours
80% of breaches undetected for months

Security Silos Complicate Protection

- Most organizations have between 45 and 65 security vendors
- Most don’t talk to each other – **AT ALL!**

Network as a Sensor

- Most organizations fail to understand the costs of integrating disparate security products and services
- Complex systems require lots of tuning and lots of staff to manage
- SIMPLE CAN OFTEN BE BETTER!
- Convergence of IT and OT under IOT/IOE
- The Network is the common choke point



Best of Breed is no longer an effective strategy

- Does your staff work together to form an effective team?
- Do your security applications work together?
- Are you synergizing your investments in people, process and technology?

- **If your team wouldn't work together you would start firing people!**

Cyber Attack & Threat Intelligence

Out-Smarting Attackers

Operational Trends

Plug-In Poison

Sandbox Evasion

Ransom-ware

WordPress Hosting

Obfuscation

Malicious Macro

The Importance of Good Intelligence

At Cisco we protect our global network and systems with some of the best threat intelligence that can be bought or built

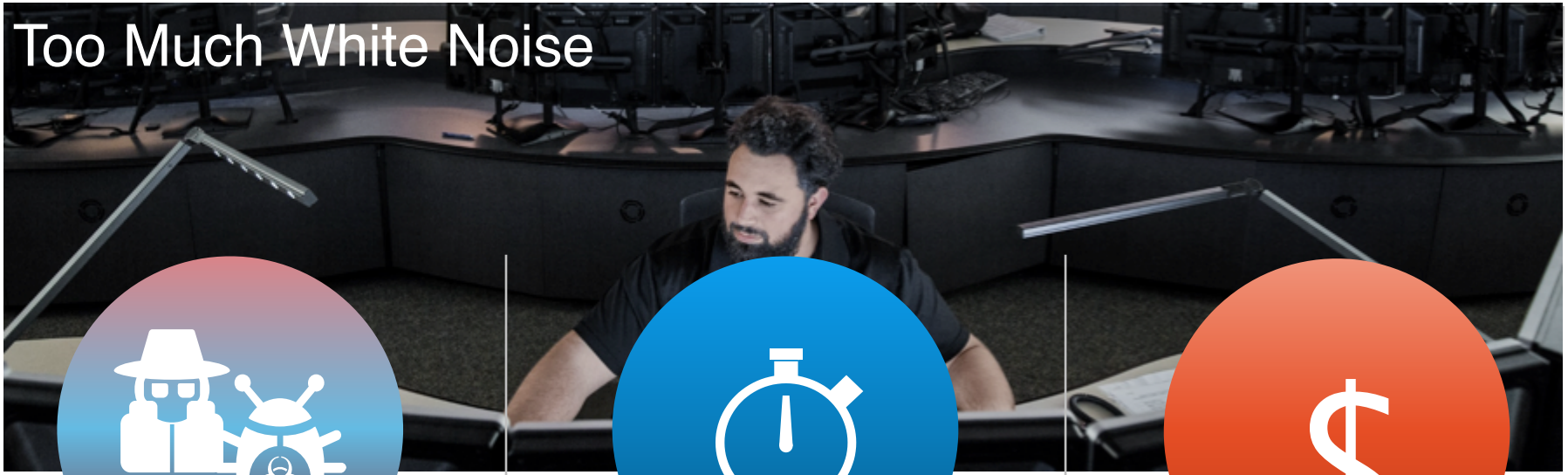
http://www.talosintel.com

Talos intelligence is shared across Cisco products and services:
SourceFire, ASA-X, AMP, ThreatGrid, ATA

Threat Intelligence: Unprecedented Breadth & Depth

100TB Security Intelligence	**150,000** Micro-applications	**5,500** IPS Signatures	**5B** Daily Email Connections
1.6M Deployed Devices	**93B** Daily Email Messages	**150M** Deployed Endpoints	**1,000** Applications
13B Web Requests	**35%** Enterprise Email	**3-5 min** Updates	**4.5B** Daily Email Blocks
120K Sandbox Reports	**75,000** FireAMP Updates	**6,000** New Clam AV Sigs	**14M** Deployed Access Gateway

Too Much White Noise



70,000
average number of security events an enterprise generates per week[1]

395
hours wasted investigating false-positives each week[2]

$1.3 million
cost per year of time wasted investigating false-positives[2]

The Pain of False-Positives

- Too many alerts to investigate
- Hard to know which alerts to prioritize
- Frustration of redundant efforts
- Risk of a real threat slipping through the cracks
- Opportunity cost of investigating false-positives

Applying Intelligence

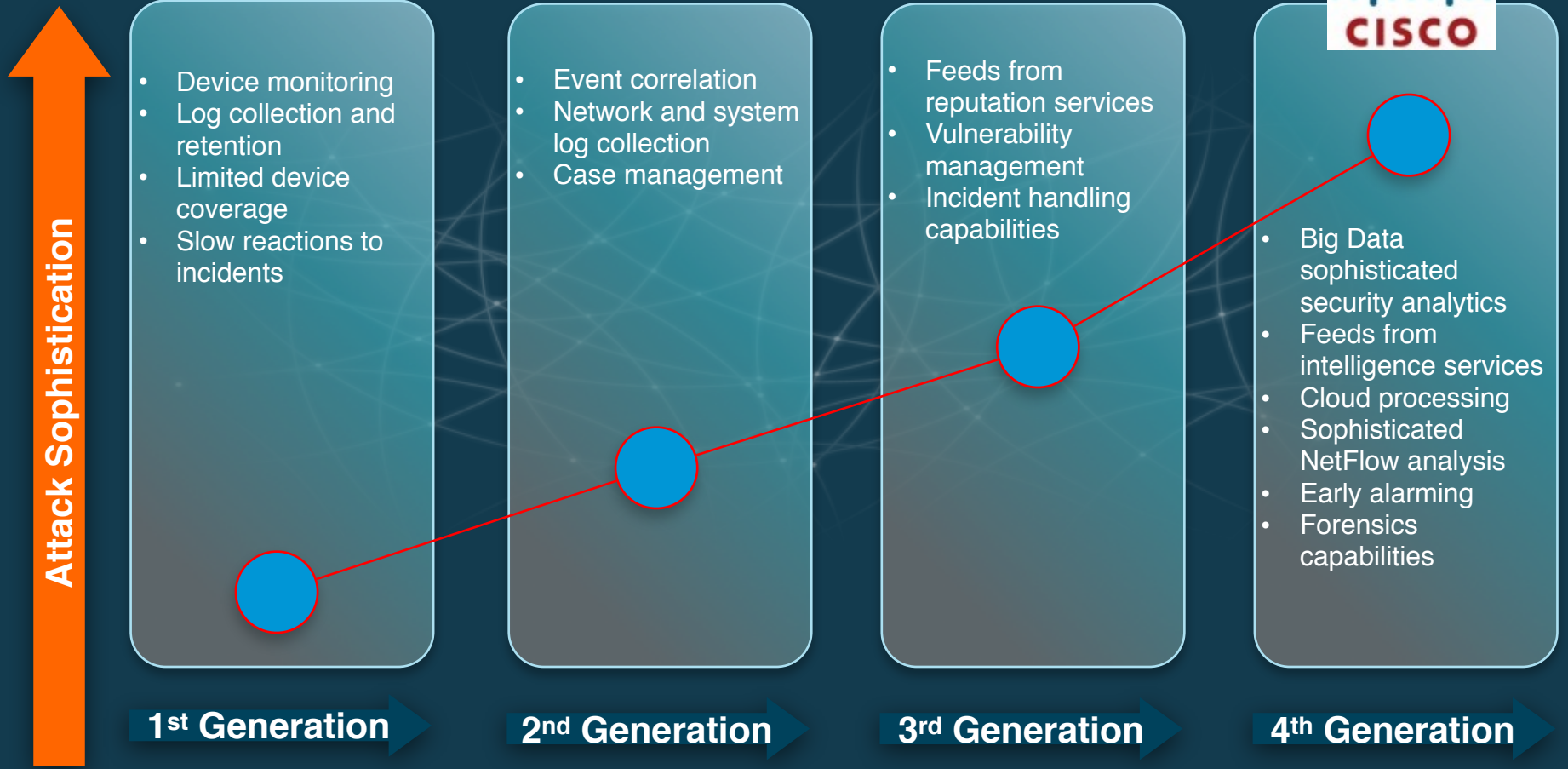
- The best Intelligence is only good if you can combine it with the right people, process and technologies
- At Cisco we've designed the next generation SOC
- We call it **OpenSOC**
- Open Sourced and available at http://github.com

Also Available As-A-Service

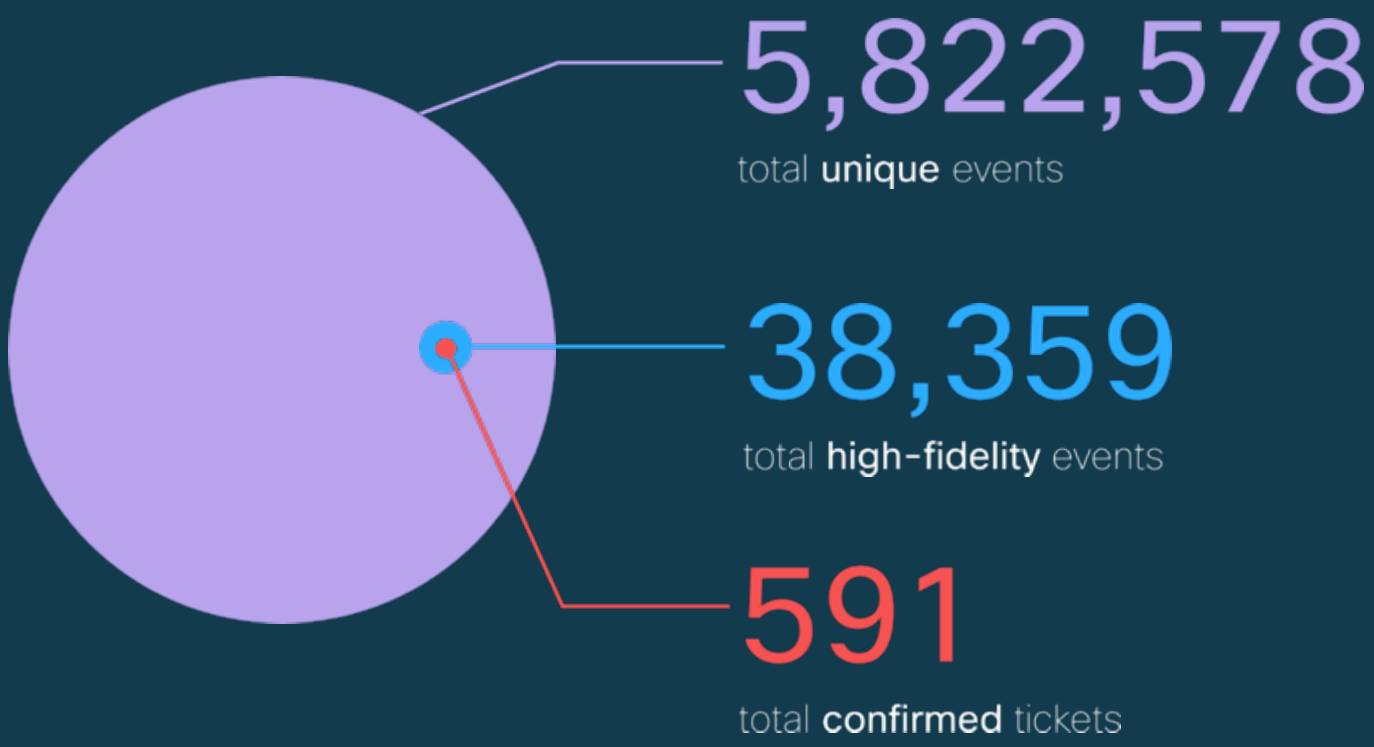
Cisco ATA
(Advanced Threat Analytics)

Cisco's RTP SOC

SOC Maturity – Generational Gaps in Protection



Actionable Intelligence



**Data collected over the course of one year - typical small organization*

Winners and Losers

Time to Detection:
Reducing Malicious Actors' Unconstrained Operational Space

June 2015 (Median)

35.3

HOURS

VS

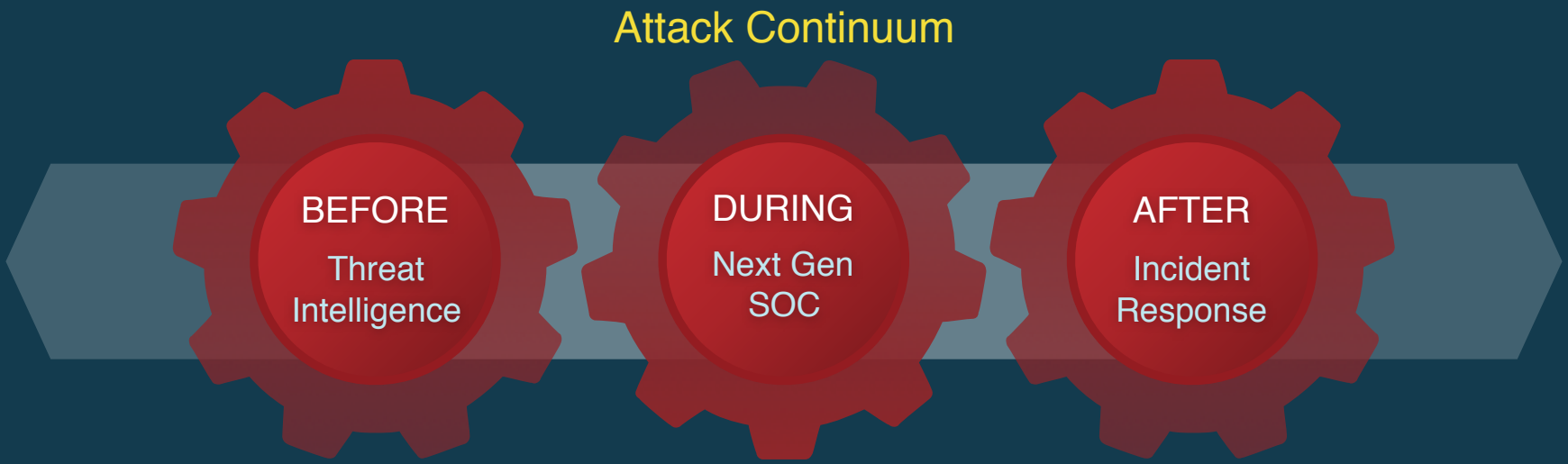
October 2015 (Median)

17.5

HOURS

Cisco far outpaces the current industry estimate of 100 to 200 days

Need for End to End Threat and Incident Handling



Continuous Treat Intelligence, Detection, Blocking and Tackling, Incident Response

Thank You

Twitter: @rstaynings

Blog: http://blog.staynings.com

Contact: http://richard.staynings.com

Cisco Security Reports can be downloaded here:

Click to download

Click to download