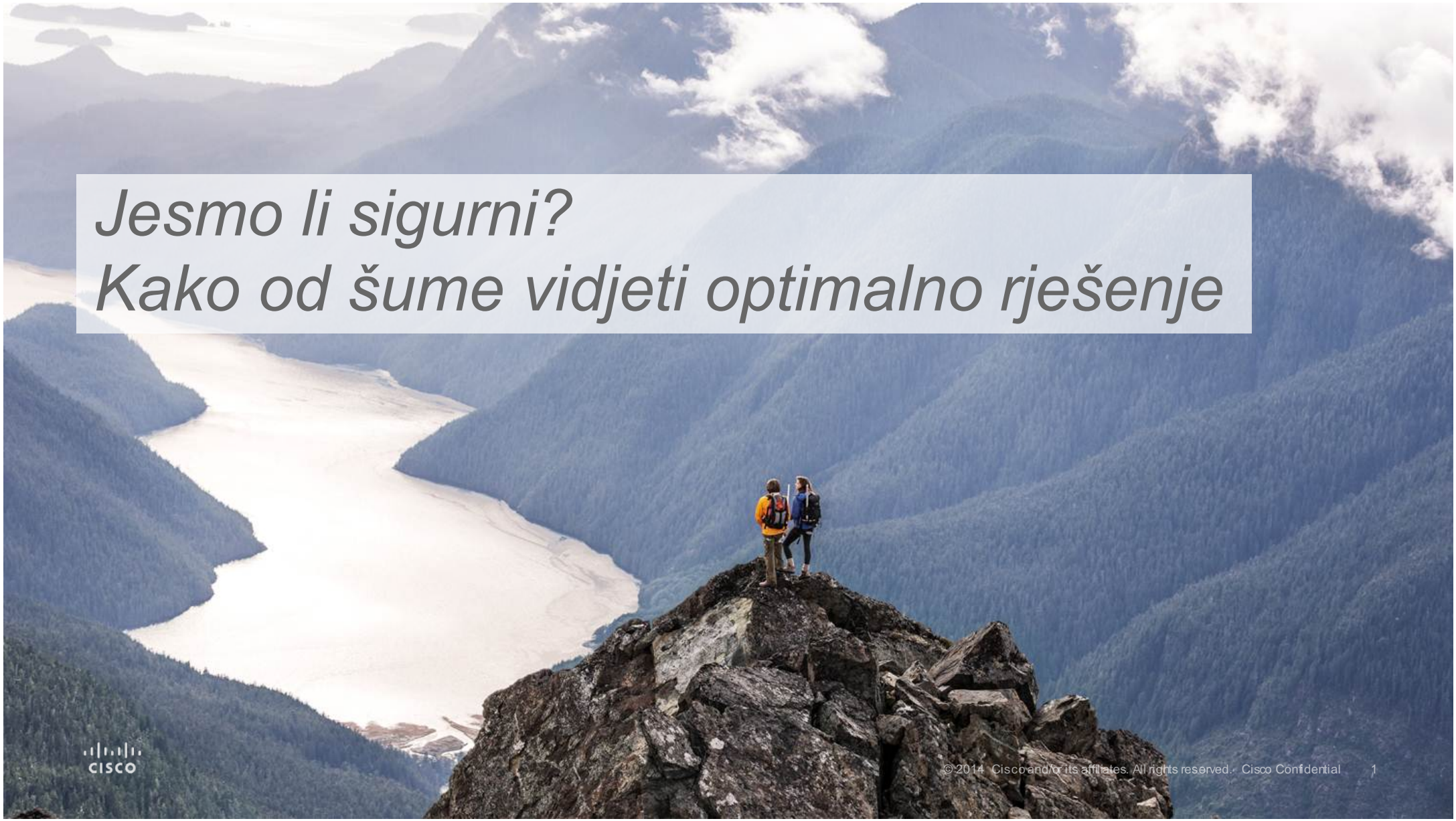
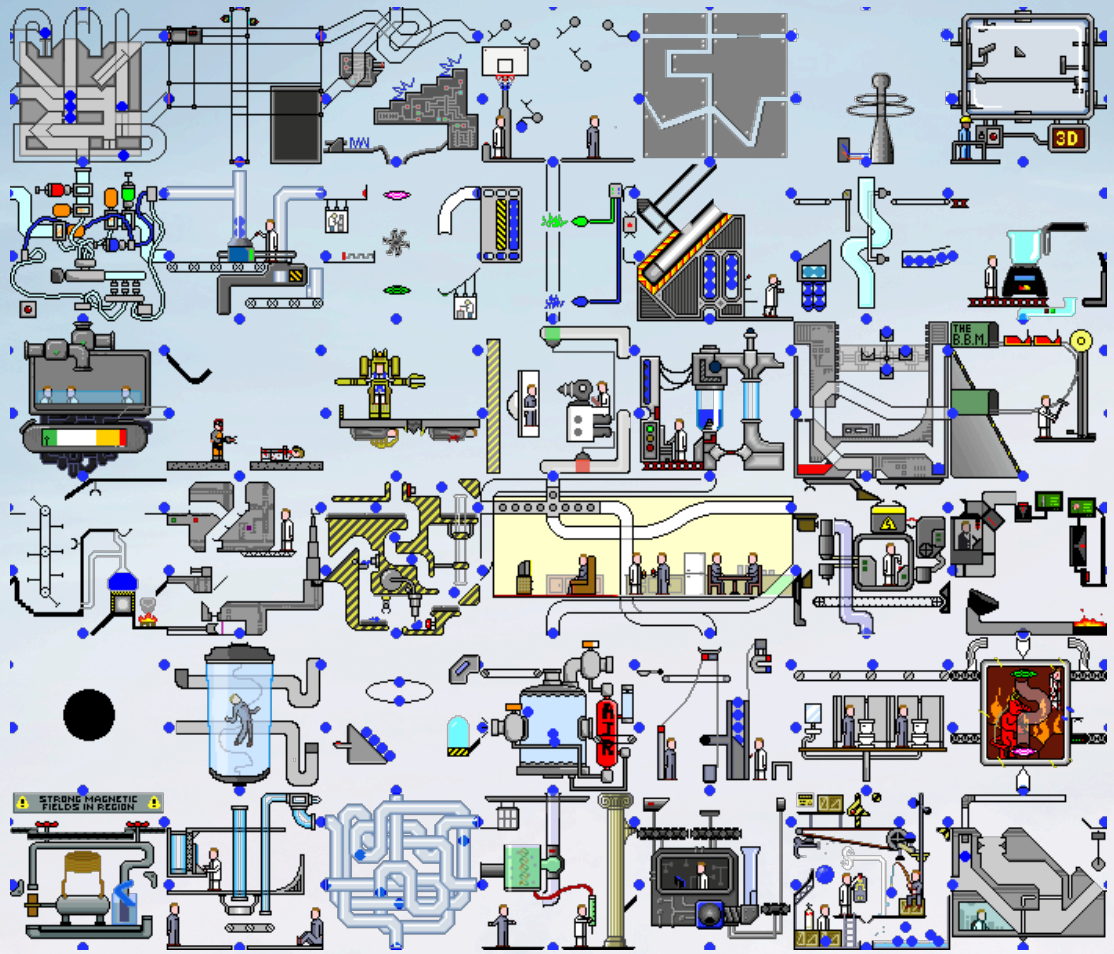
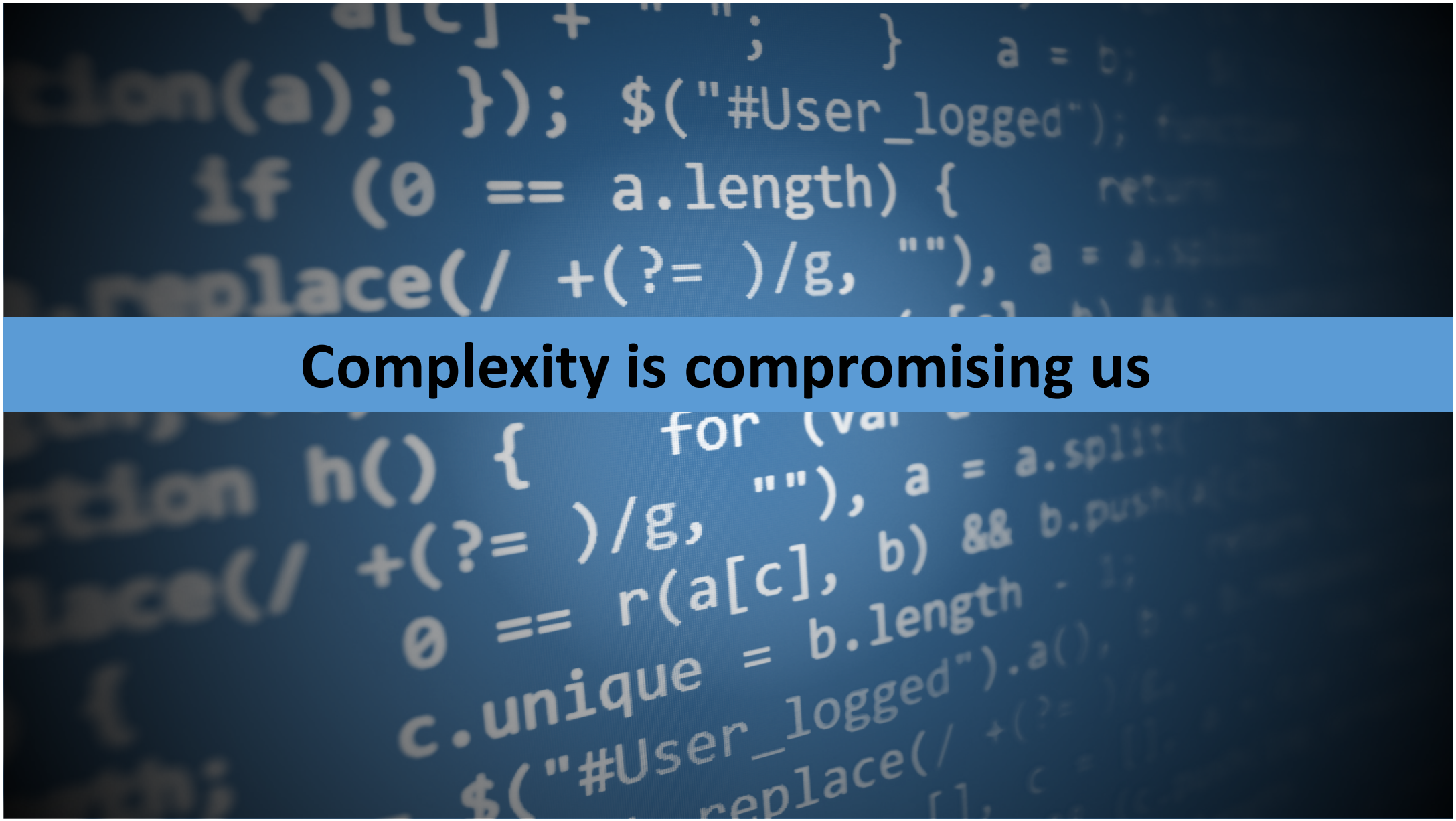


Jesmo li sigurni?
Kako od šume vidjeti optimalno rješenje

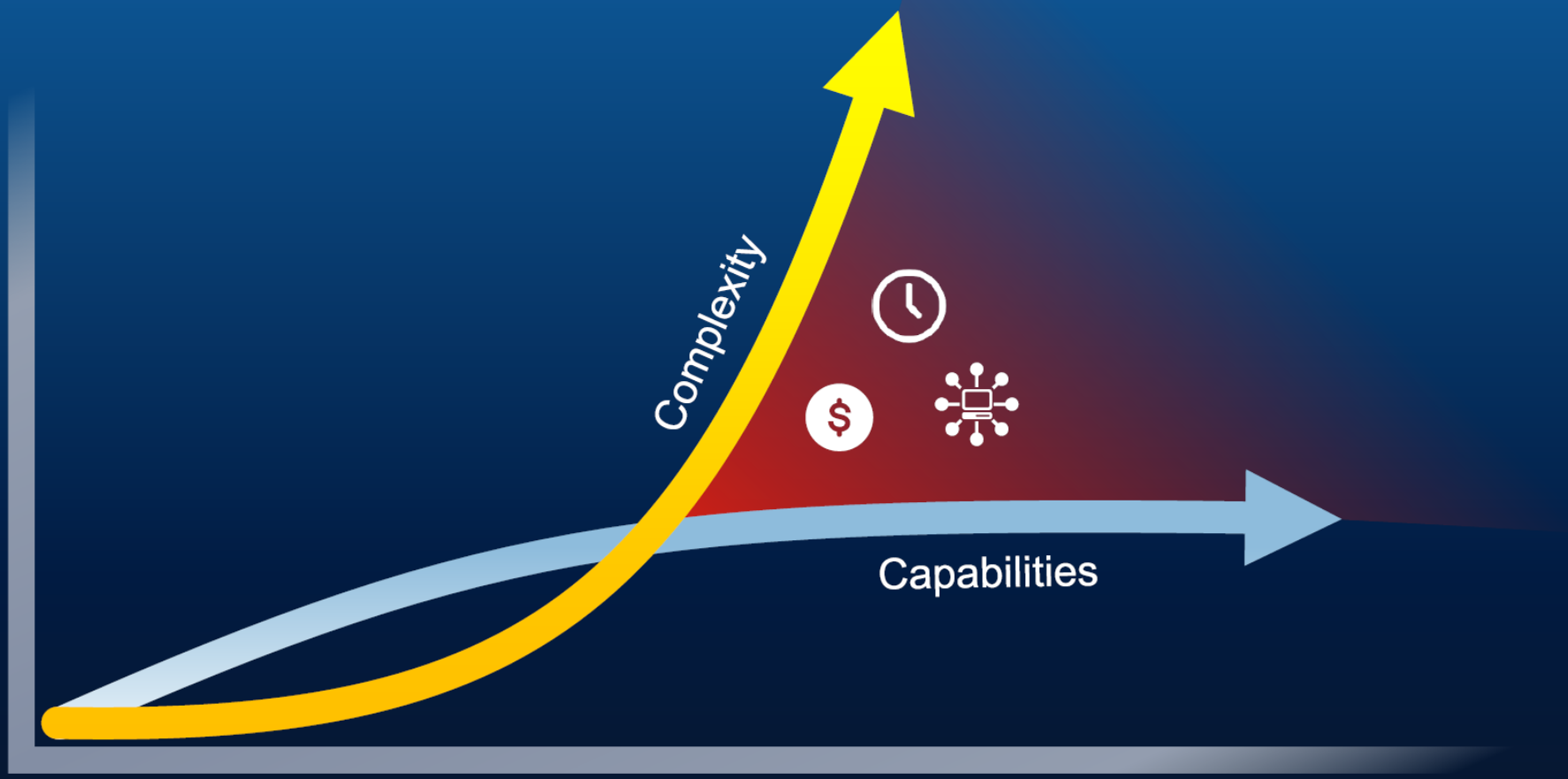
© 2014 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Fact - I : You cannot manage the complexity!




Complexity is compromising us

The Security Effectiveness Gap



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

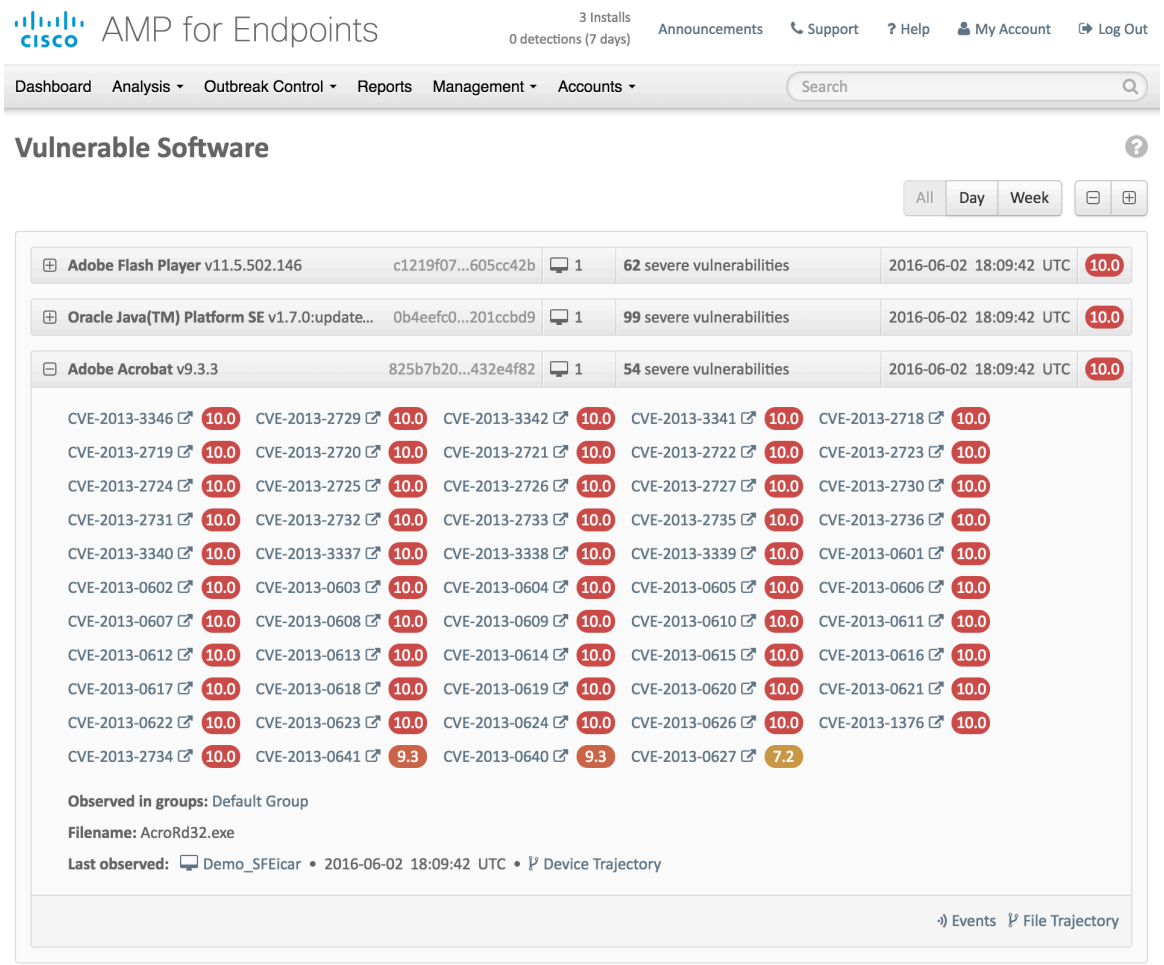
Fact - II : You need visibility to be able to control

Who is on the network

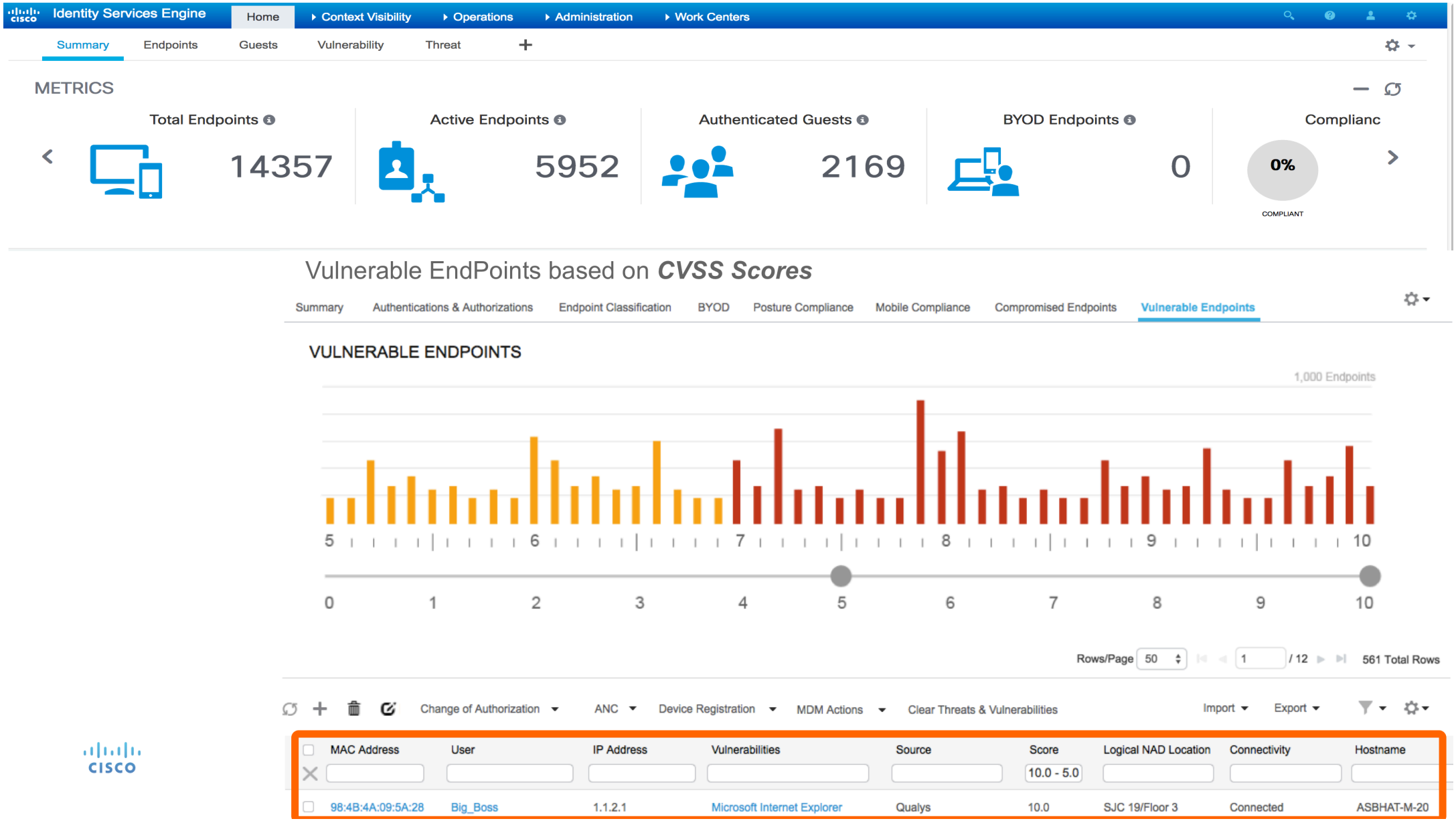
You can’t protect what you can’t see

and what are they up to?

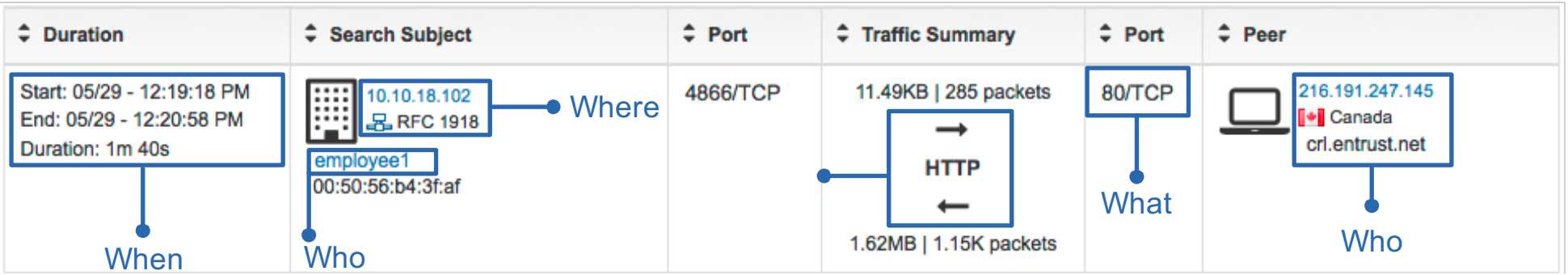
Vulnerable Endpoints



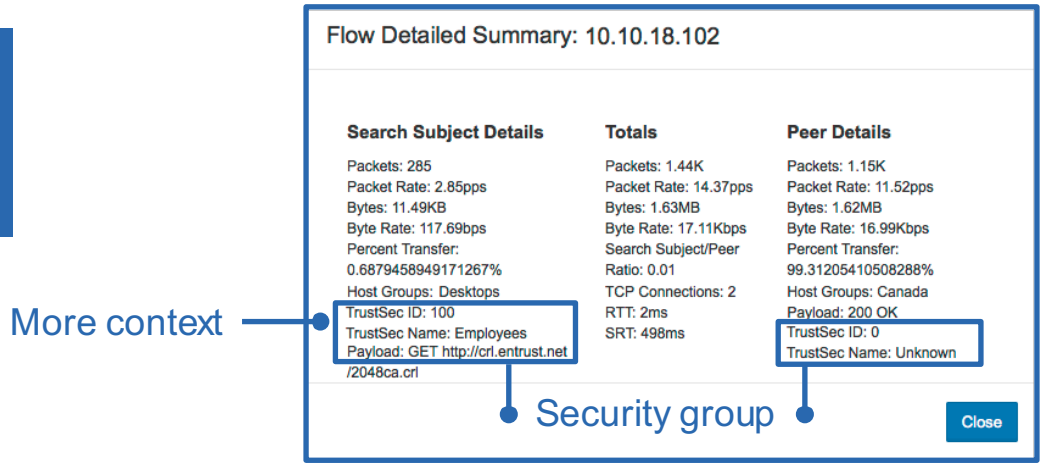
Cisco and/or its affiliates. All rights reserved.


Identity Services Engine
Home
Context Visibility
Operations
Administration
Work Centers
Summary
Endpoints
Guests
Vulnerability
Threat
METRICS
Total Endpoints
14357
Active Endpoints
5952
Authenticated Guests
2169
BYOD Endpoints
0
Compliance
0%
COMPLIANT
Vulnerable EndPoints based on CVSS Scores
Summary
Authentications & Authorizations
Endpoint Classification
BYOD
Posture Compliance
Mobile Compliance
Compromised Endpoints
Vulnerable Endpoints
VULNERABLE ENDPOINTS
1,000 Endpoints
5
6
7
8
9
10
0
1
2
3
4
5
6
7
8
9
10
Rows/Page 50
1
/ 12
561 Total Rows
Change of Authorization
ANC
Device Registration
MDM Actions
Clear Threats & Vulnerabilities
Import
Export
MAC Address
User
IP Address
Vulnerabilities
Source
Score
Logical NAD Location
Connectivity
Hostname
10.0 - 5.0
98:4B:4A:09:5A:28
Big_Boss
1.1.2.1
Microsoft Internet Explorer
Qualys
10.0
SJC 19/Floor 3
Connected
ASBHAT-M-20

Conversational Flow Record



- Highly scalable (enterprise-class) collection
- High compression => long-term storage
  - Months of data retention



More context

Security group

© 2014 Cisco and/or its affiliates. All rights reserved.

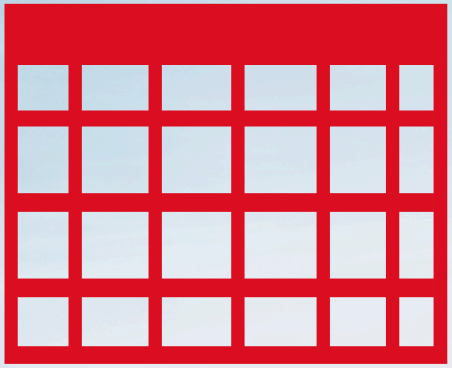
Fact - III : The goal is to have a better outcome!

Time to Detect - TTD

Industry average

200

DAYS



VS

Cisco

18.5

HOURS

15.19 hours	**6.05 hours**
May 2016	October 2016

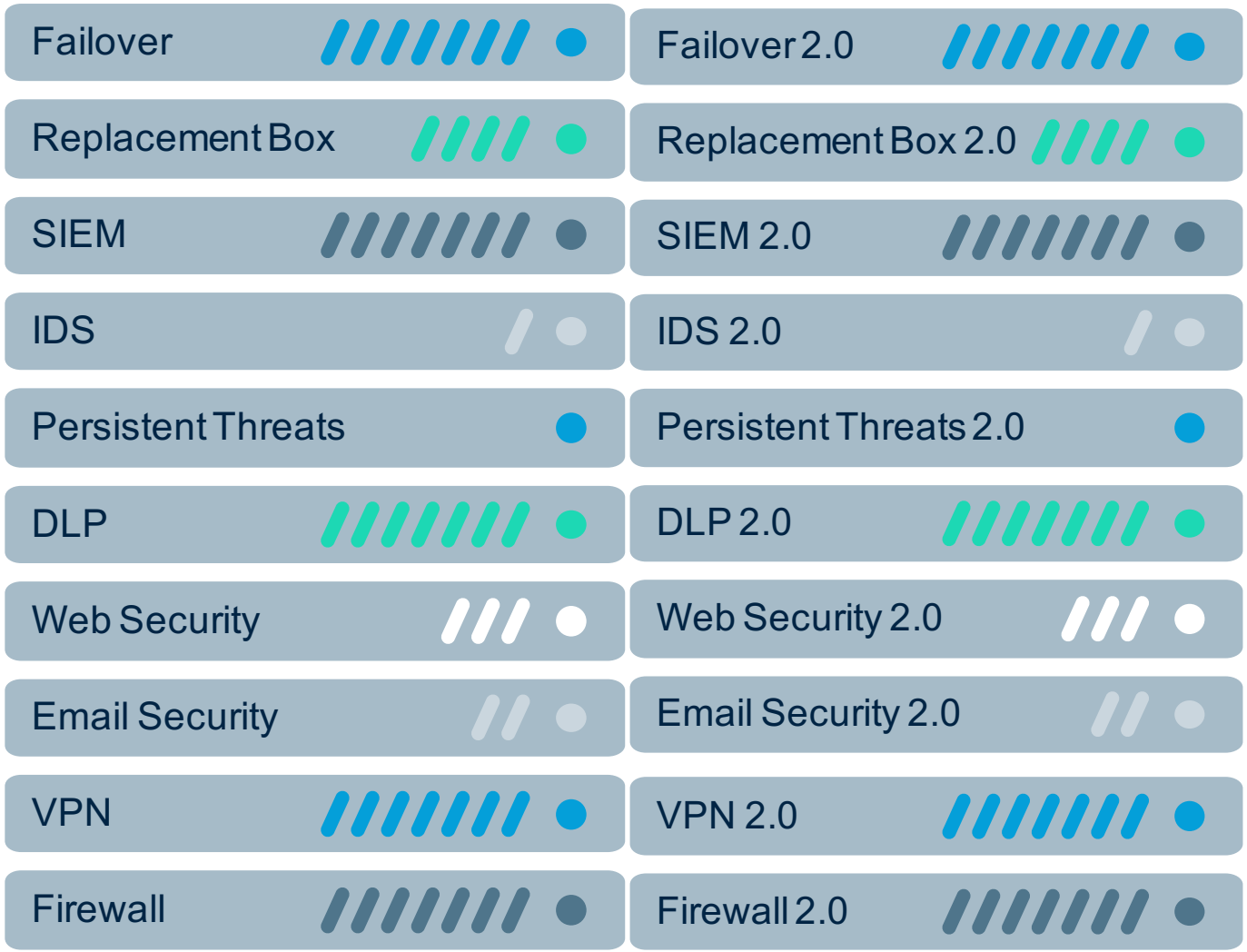
Annual sec report 2017

Last 20 years of security:

Got a problem?

BUY A BOX

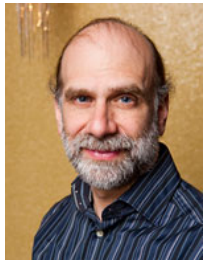
© 2014 Cisco and/or its affiliates. All rights reserved.



Your NEW security STACK

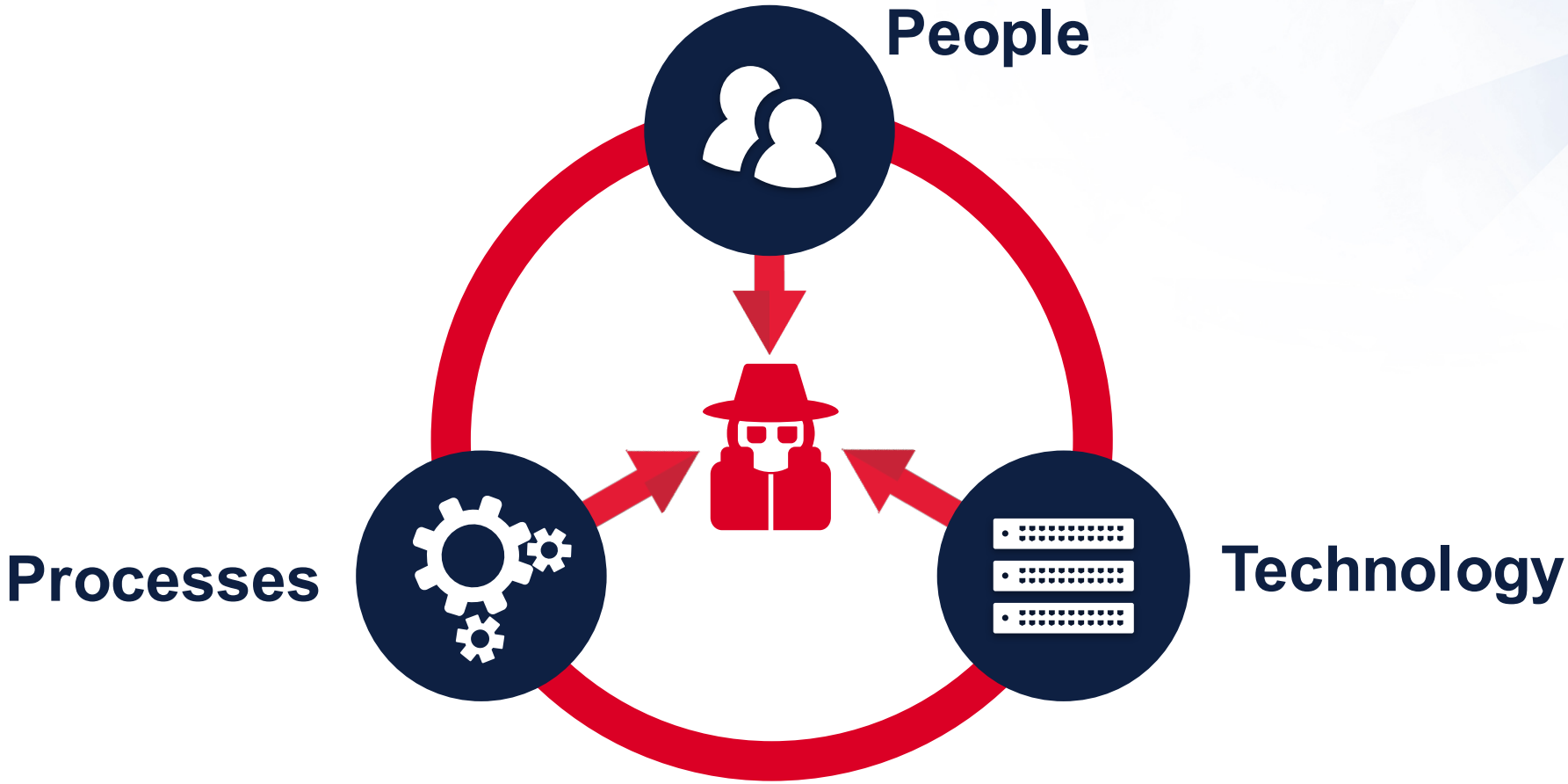
© 2014 Cisco and/or its affiliates. All rights reserved.

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.



Bruce Schneier
security guru

People – Processes - Technology



	Encryption C&C				Payment MSG
NAME	**DNS**	**IP**	**NO C&C**	**TOR**	**PAYMENT**
Locky	●	●			DNS
SamSam			●		DNS (TOR)
TeslaCrypt	●				DNS
CryptoWall	●				DNS
TorrentLocker	●				DNS
PadCrypt	●				DNS (TOR)
CTB-Locker	●			●	DNS
FAKBEN	●				DNS (TOR)
PayCrypt	●				DNS
KeyRanger	●			●	DNS

RISK is quantified threat = consider the cost of the incident, if it occurs

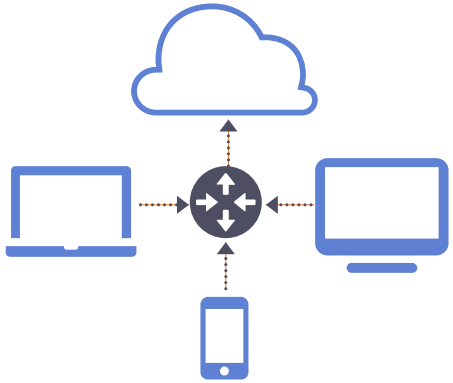
- RISK = probability x cost (impact)
- Probability is the percentage likelihood that the event will occur

- Common business scenarios:
  - The probability of an insider threat is low but the cost is high
  - The probability of a malware is high, but the cost is low
  - The probability of data loss is high, and the cost is high
  - The probability of a nation-state attack is very small, but the cost us huge
  - percentage likelihood that the event will occur

© 2014 Cisco and/or its affiliates. All rights reserved.

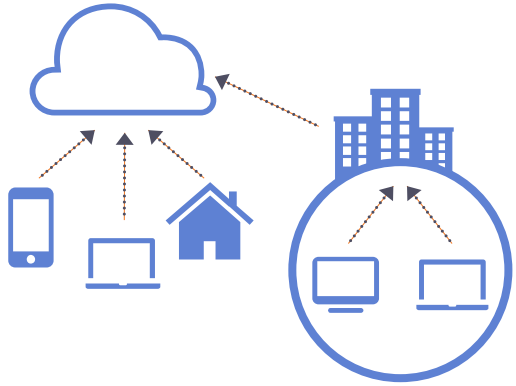
Can we predict attacks?

DNS is *Used by Every Device* on Your Network



ANY OWNER

network's DHCP tells every connected device where to point DNS



ANY TOPOLOGY

no matter how your LAN or WAN is set up, it simply works

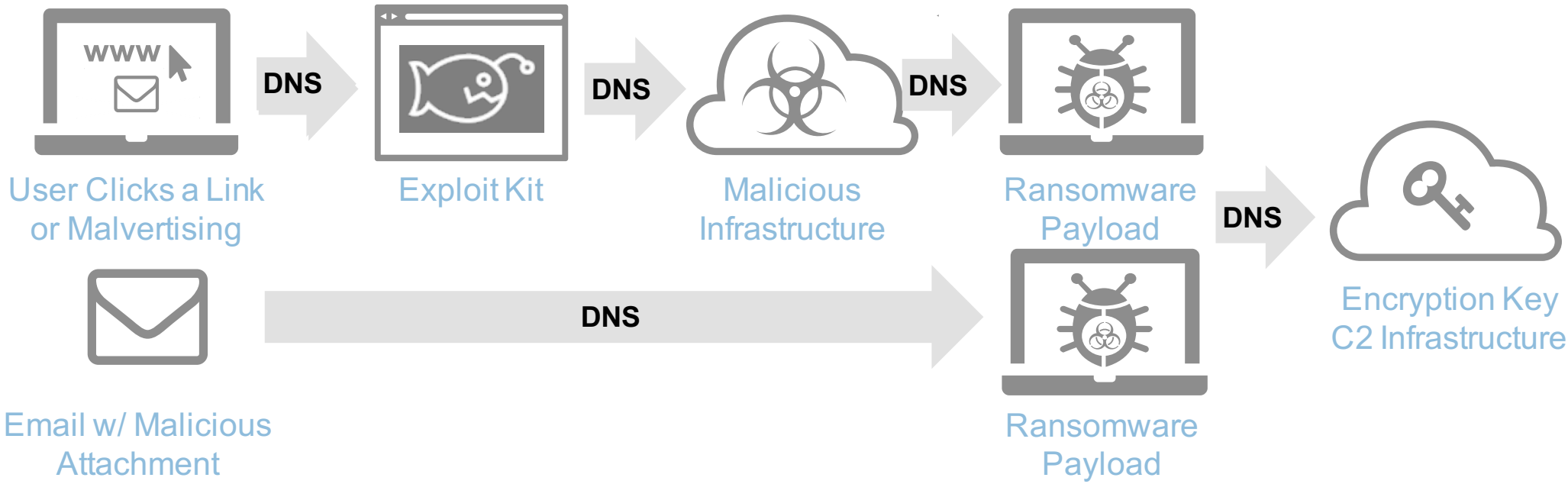
ANY OPERATING SYS

Win, Mac, iOS, Android, Linux, custom app servers, and even IoT

© 2014 Cisco and/or its affiliates. All rights reserved.

Ransomware Kill Chain with DNS

Elements of the infrastructure are involved in each phase



© 2014 Cisco and/or its affiliates. All rights reserved.

Gather Intelligence and Enforce security at the DNS Layer

Request Patterns

Used to detect:

- Compromised systems
- Command & control callbacks
- Malware & phishing attempts
- Algorithm-generated domains
- Domain co-occurrences
- Newly registered domains

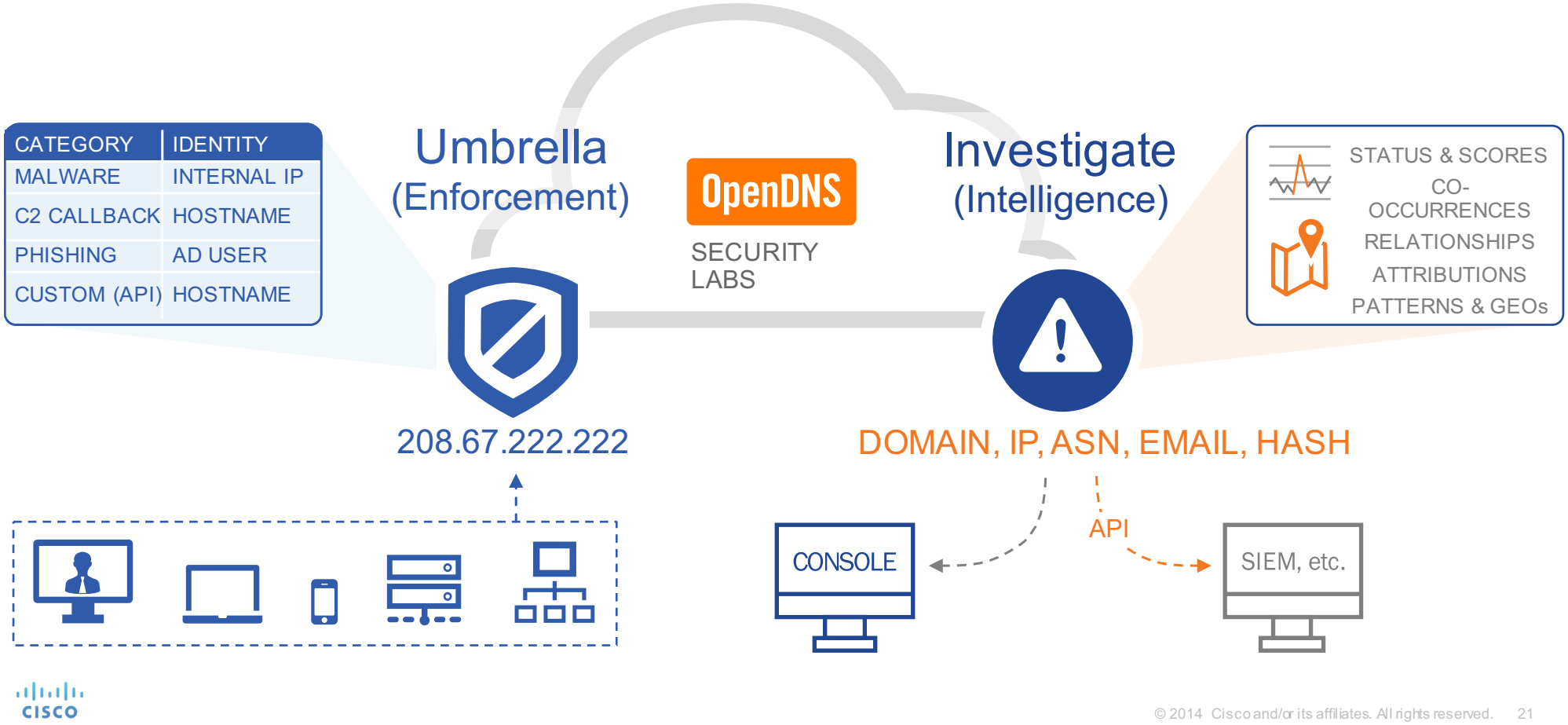
Authoritative Logs

Used to find:

- Newly staged infrastructures
- Malicious domains, IPs, ASNs
- DNS hijacking
- Fast flux domains
- Related domains

/or its affiliates. All rights reserved.

What does OpenDNS Provide



© 2014 Cisco and/or its affiliates. All rights reserved.

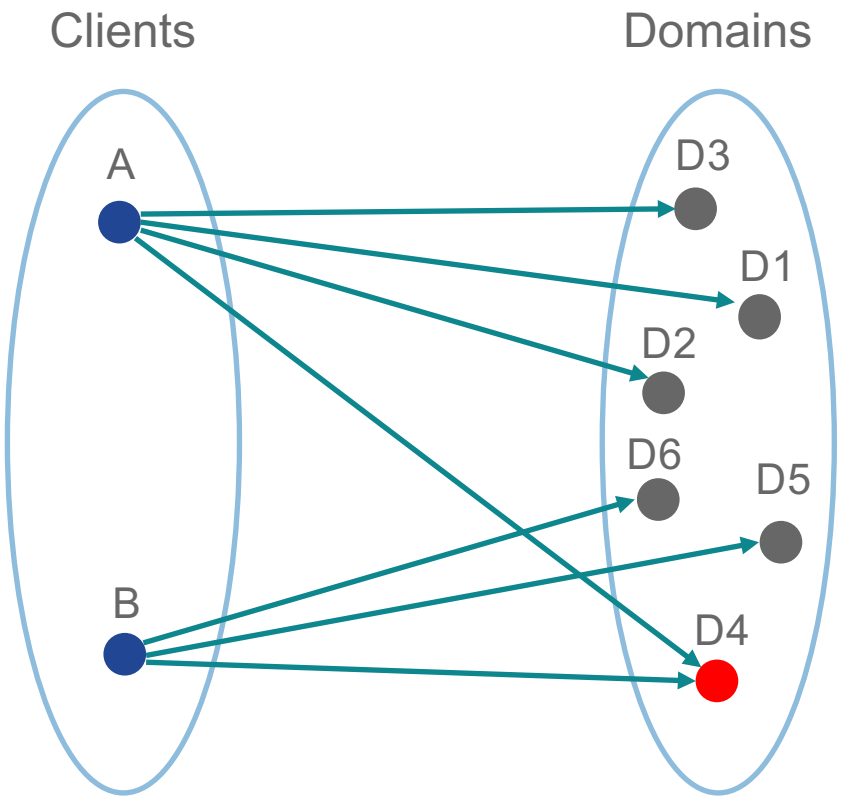
Predictive Detectors Used by OpenDNS

- SecureRank
- Co-Occurrences
- NLPRank
- DGA Detectors
- Spike Detectors

© 2014 Cisco and/or its affiliates. All rights reserved.

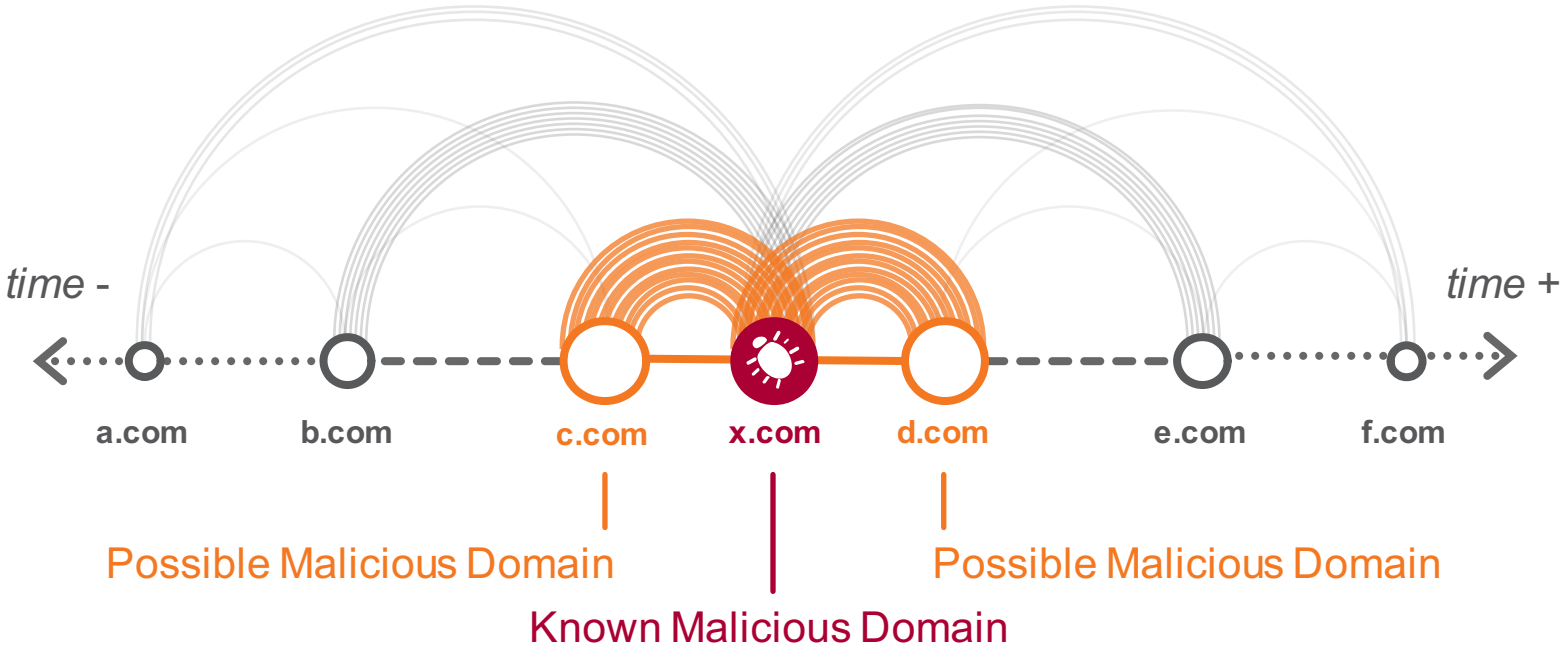
SecureRank

- Abstract DNS traffic in a bipartite graph
- **Domains requested by known infected clients but never requested by clean ones are most likely to be bad.**
- **The less visited by good clients, the higher chance a domain is bad**
- SecureRank2 is designed to identify these domains
- Negative ranks to known blacklisted domains and positive ranks to known whitelisted domains.
- Nodes are either visited or being visited, but never both



© 2014 Cisco and/or its affiliates. All rights reserved.

Co-Occurrence Rank

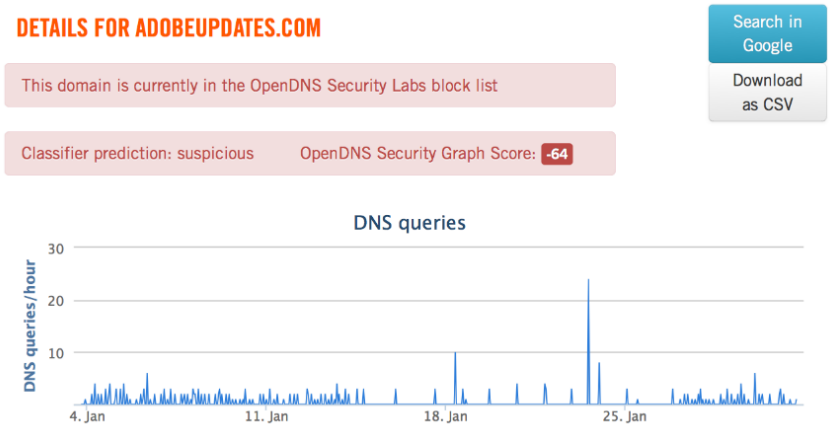


Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe

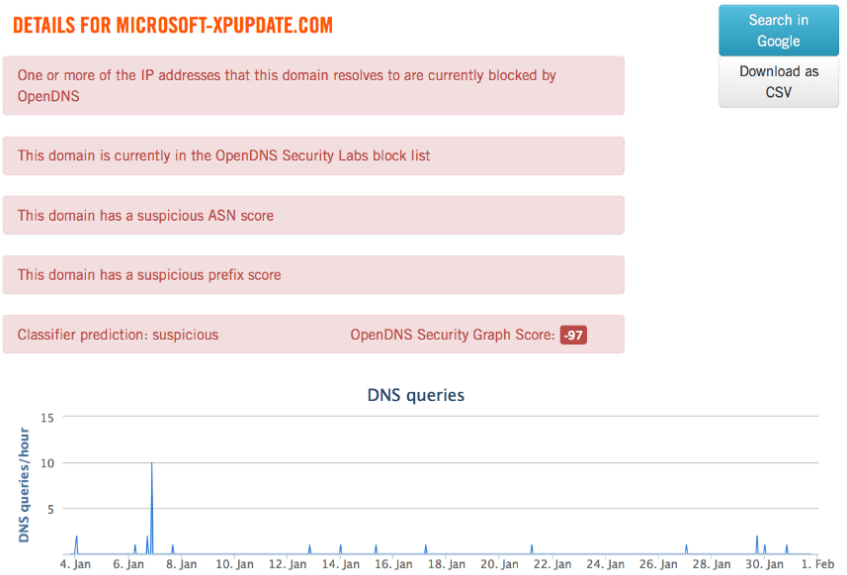
© 2014 Cisco and/or its affiliates. All rights reserved.

NLPRank Detections: DarkHotel

- adobeupdates[.]com



- microsoft-xpupdate[.]com



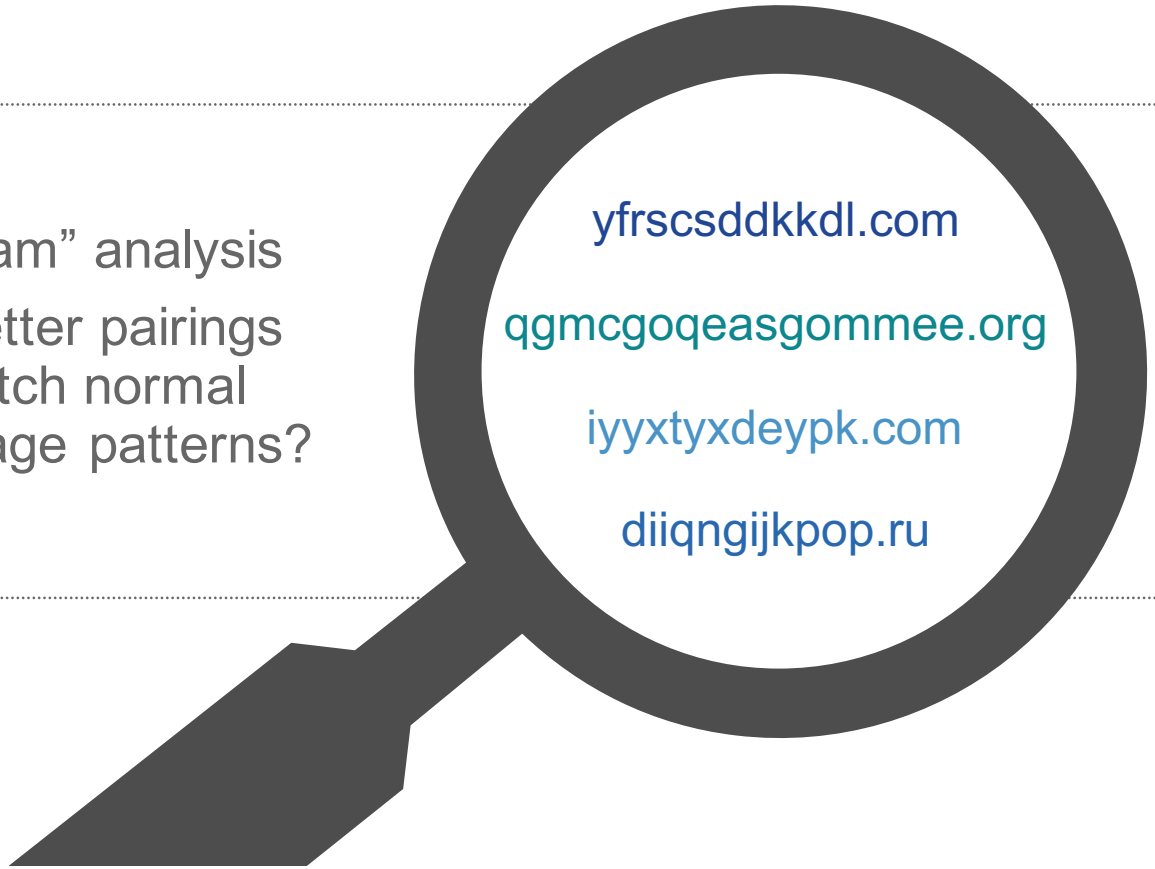
© 2014 Cisco and/or its affiliates. All rights reserved.

Anomaly Detection: Live DGA Detection

Domain Generation Algorithms: technique to generate malware domains on-the-fly & avoid hardcoding domains in payload

N-gram" analysis

Do letter pairings match normal language patterns?



Does the probability distribution of letters appear random?

© 2014 Cisco and/or its affiliates. All rights reserved.

IP Geo-Location Analysis

hosted across 28+ geo-locations

HOST INFRASTRUCTURE

location of the server
IP addresses mapped to domain

only US-located users requesting a .RU TLD

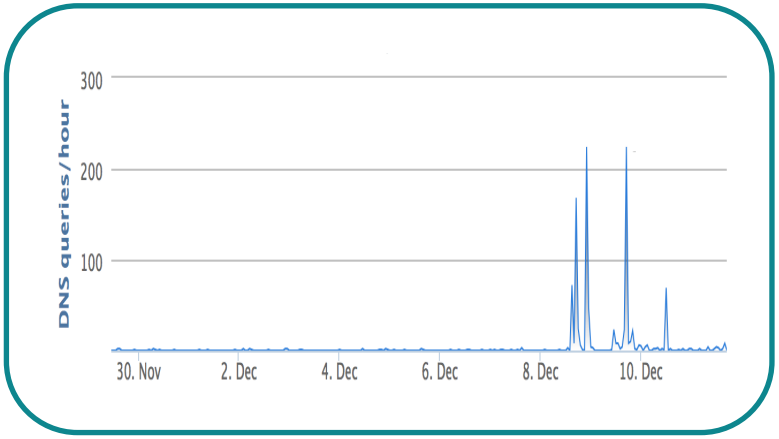
DNS REQUESTERS

location of the network & off-network device
IP addresses requesting the domain

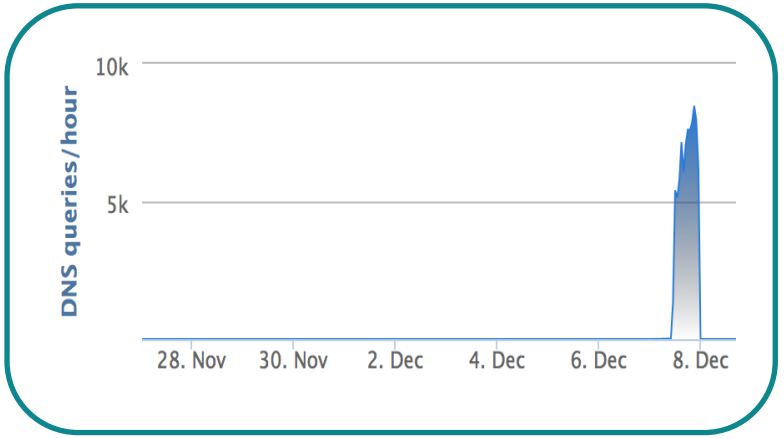
© 2014 Cisco and/or its affiliates. All rights reserved.

What Does a Malicious Connection Sounds Like?
Spike detector

What if we could model the traffic spikes as sound waves and identifies “spike behavior” typical of domains used for malware campaigns such as exploit kits, DGAs, fake software, phishing, etc…



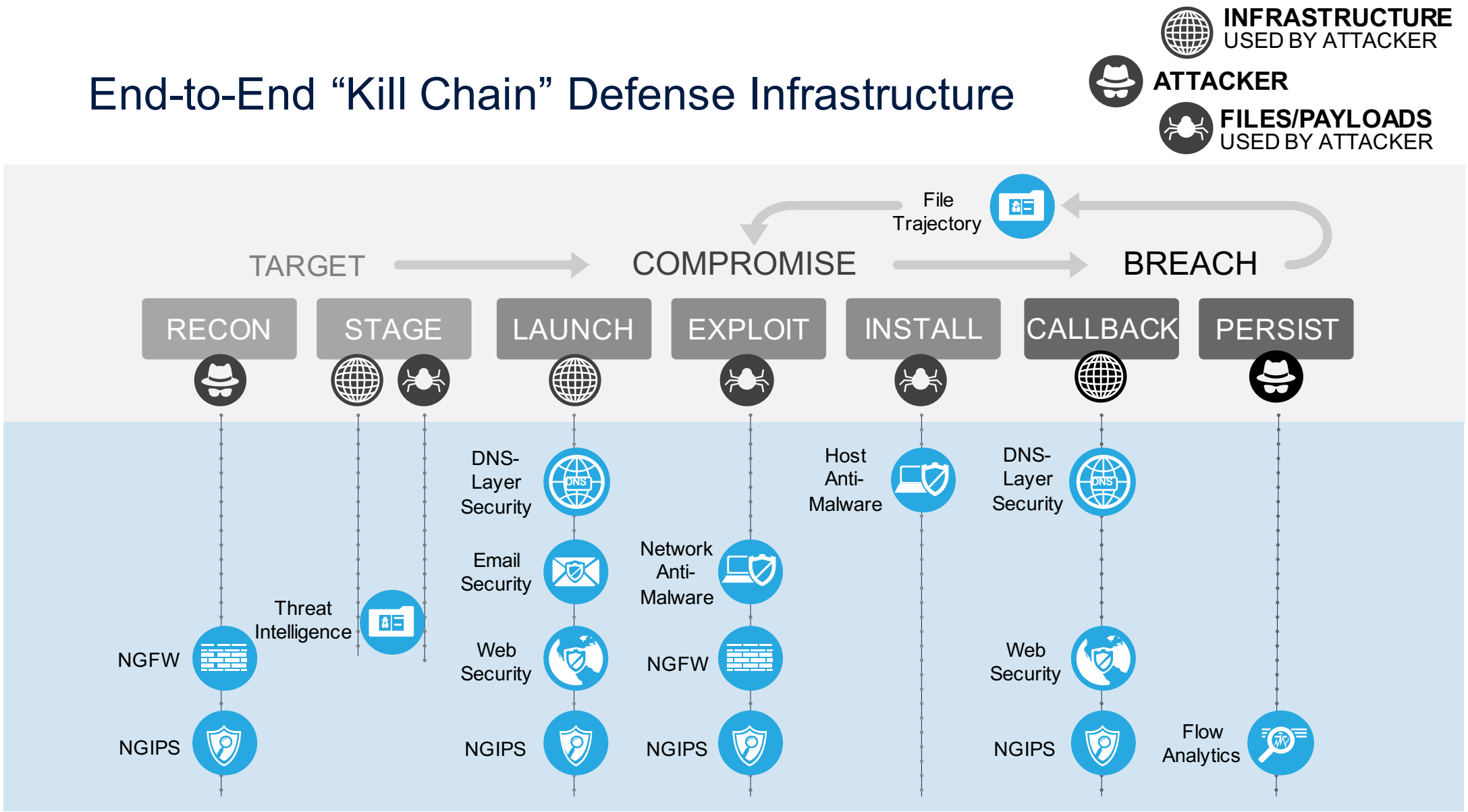
Example of An Exploit Kit



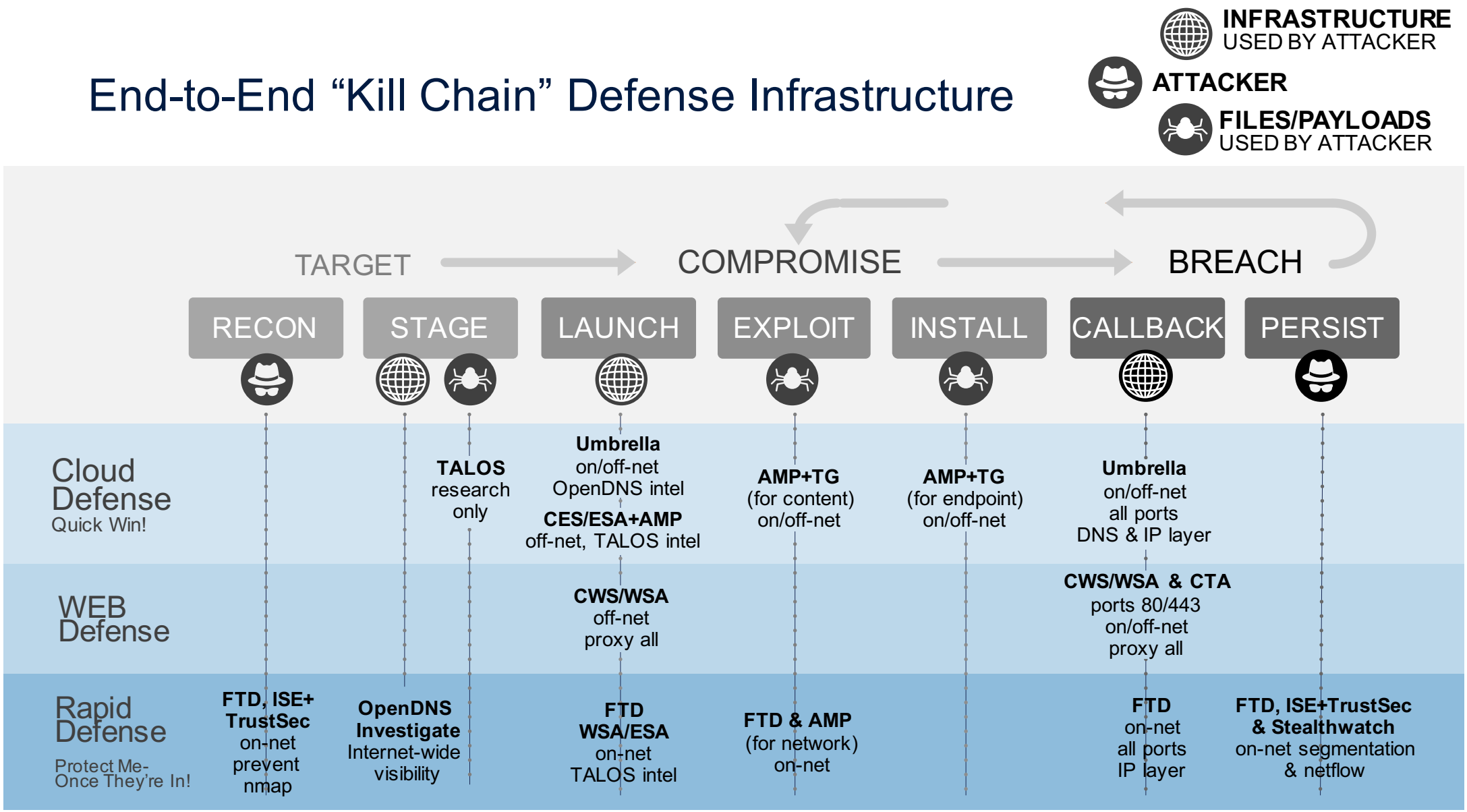
Example of a DGA

© 2014 Cisco and/or its affiliates. All rights reserved.

End-to-End “Kill Chain” Defense Infrastructure

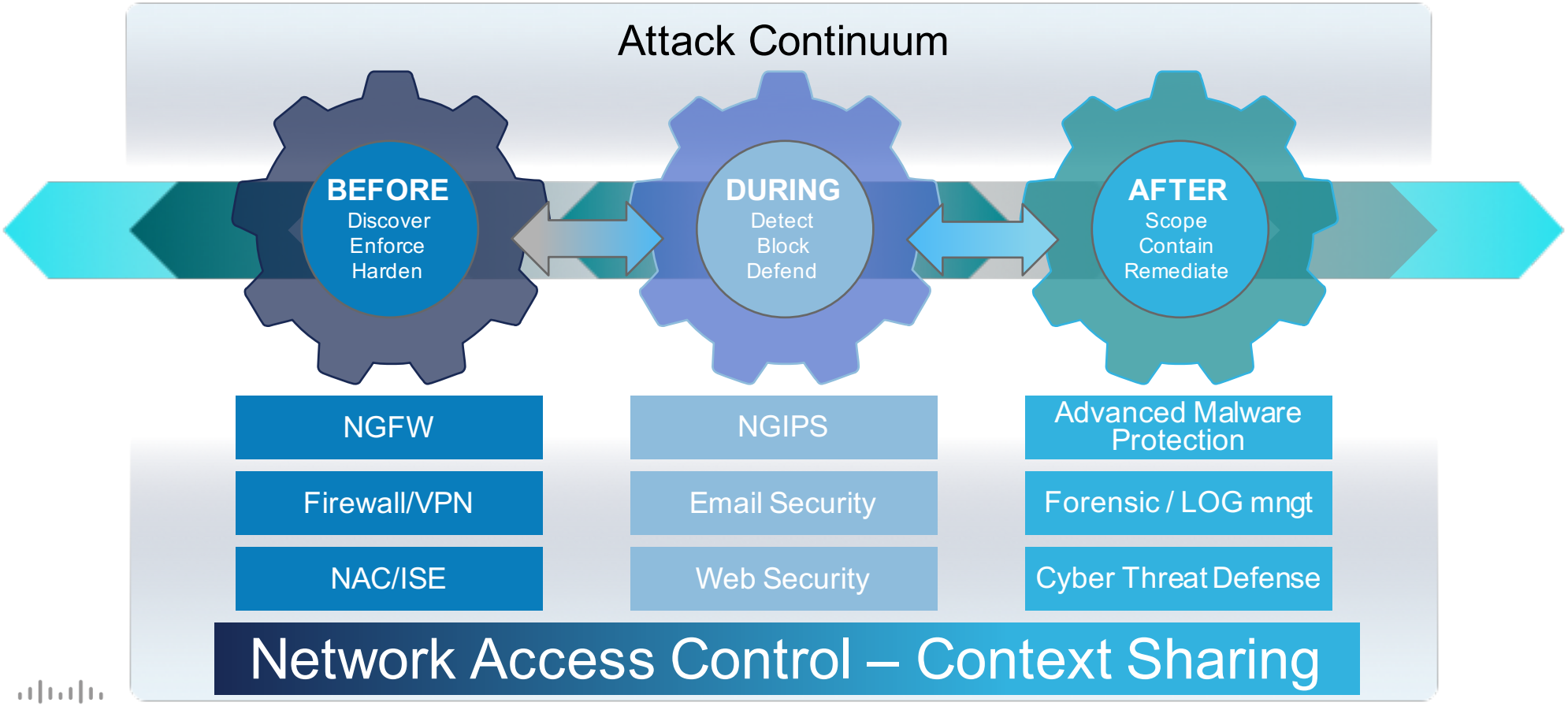


End-to-End “Kill Chain” Defense Infrastructure



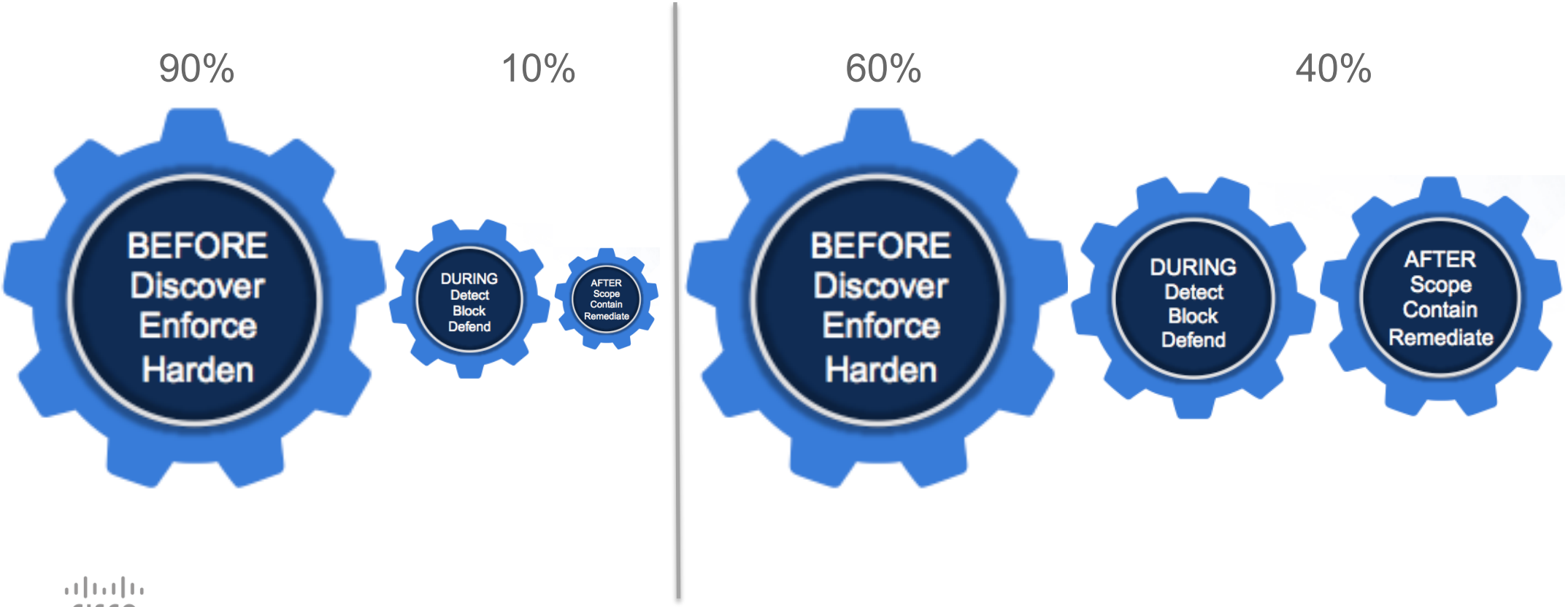
WOULD YOU
FLY IN A PLANE
MADE OUT OF
50 PLANES?
Then why are companies using up to
50 different security vendors?
cisco
There's never been a better time for security that works together.

Threat-centric security model



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

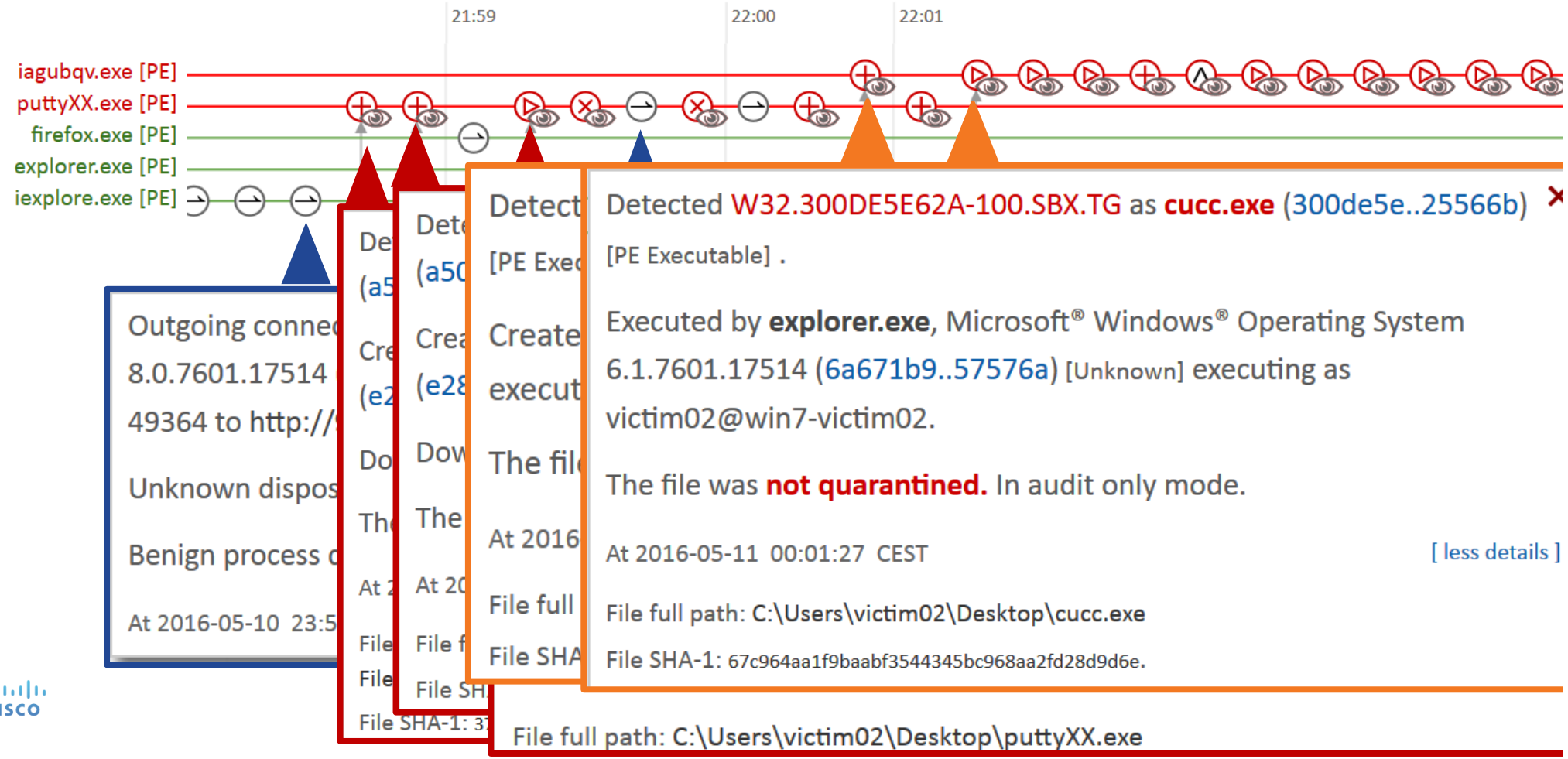
Security Maturity Model



© 2015 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Device Trajectory

For win7-victim02



THERE'S NEVER BEEN A BETTER TIME
FOR SECURITY THAT WORKS TOGETHER.
cisco