

INTUITIVE

Cisco *live!*

5-8 March 2019 • Melbourne, Australia

#CLMEL



How We Secured The Commonwealth Games and Other Major Events

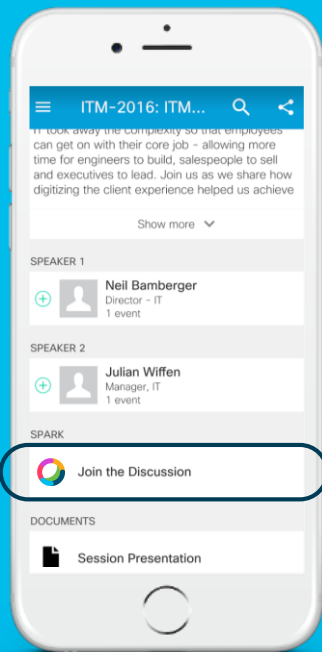
Matt Carling – Security Architect
BRKCIP-1697



#CLMEL



INTUITIVE



cs.co/ciscolivebot#BRKCIP-1697

Cisco *live!*

Cisco Webex Teams



Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

How

- 1 Open the Cisco Events Mobile App
- 2 Find your desired session in the “Session Scheduler”
- 3 Click “Join the Discussion”
- 4 Install Webex Teams or go directly to the team space
- 5 Enter messages/questions in the team space

Perception, fibs, and reality



What my wife thought I was
doing

Source : Wikipedia
https://en.wikipedia.org/wiki/Gold_Coast,_Queensland

Ciscolive!



What I told my kids I was doing

Source : Marco Verch
<https://www.flickr.com/photos/30478819@N08/36392467215>



What I really did

Source : Me!

Agenda

- Some numbers
- Games Legacies
- Threats
- Architectural approach
- Statistics
- Lessons Learnt

Background

About the Games

April 4 - 15 2018



30 Locations including
18 Games Venues

1,000 Hours
of Sport!

1.5 BILLION
VIEWERS



6,600 Athletes
& Officials



❖ 70 Countries
❖ 18 Sports

23 Broadcast Locations



3,500 accredited representatives

- GOLDOC will grow to over 2,000 employees
- The Optus GOLDOC delivery team will expand to 152 during Games time



15,000 Volunteers

History in the making

- A list of firsts...
 - First time the Games has been held outside an Australian Capital City
 - First time an equal number of medals will be contested for men and women
 - First time the Para Events have been fully incorporated into the schedule
 - First time that Women's Rugby 7's, the Para Triathlon and Beach Volleyball have featured at the Games
- By the numbers...
 - 6,600+ Athletes and Team officials
 - 71 Commonwealth Nations represented
 - 18 Sporting Disciplines
 - 7 Para-Sports Events
 - 15,000+ Volunteers
 - Global Audience of 1.5+ Billion Viewers
 - 86 Individual Records
 - 9 New World Records!



Products and Services

Planning – Support - Security

- **Optus – The Official Network Provider**
- **Cisco - The Official Network Hardware Provider**
- Products
 - IP/MPLS Backbone
 - Wired LAN
 - Wireless LAN
 - Security
 - Data Center Computing
- Advanced Services
 - Planning and Design Support
- Technical Support Services
 - Remote HTOM Support (24x7)
 - Onsite Security Ops Support (TOC)
 - Spare Part Logistics (Dedicated Depots)



Games Infrastructure

Data Centre - Networking - Security

17
Product Lines

1,800+
Parts

8,364 LAN ports

18
Competition
Venues

625
Wi-Fi Access Points



Games Time Operations

Technology Operations Center



288

MAN
HOURS

Technical Support
Services

192

Broadcast Hours

27

TOC Headcount

12

DAYS OF
COMPETITION

10

TAC cases



People Impacted

Olympic Family and Spectators



1.5 Billion

Global TV Audience

2,000

Accredited Professionals

35,000

In-venue Spectators

1,250

Media Professionals

6,600

Athletes

From

71

Countries

15,000

Volunteers

Our Olympic and Commonwealth Games Legacy

Outcomes for the community



- BIG Initiative
- Innovation Centres
- STEMNET
- NetAcad



<http://www.ciscolondon2012.co.uk/our-olympic-legacy/>

Outcomes for the community



- Cisco Pan Am Games Technology Legacy Program
 - Sporting Venues
 - Canadian High Schools, colleges, and universities
 - Connected North schools
 - Not for profit organisation
- Sheridan College SIRT research centre

Sheridan

Outcomes for the community



- Cisco Urban Innovation Legacy Project - Porto Maravilha
- Olympic City Technical Program



Outcomes for the community



- Technology redeployment into Queensland public safety network in support of their community

Threats

Critical Assets

Games and Sponsors



Brand Reputation
Results Systems
Ticketing Systems
Core Games Systems
Confidential Information
Infrastructure
Websites

Government



Country Reputation
Confidential Information
Government Services
Government Websites

Critical Infrastructure



Communications
Transportation
Energy
Financial Services
Police

Internet Users



Banking Information
Credit Cards
Social Accounts
PII

Main Threats

Games and Sponsors



Denial of Service
Sites Defacement
Fake Websites
Tickets Fraud
Phishing
Unauthorised Access
Information Theft

Government



Hacktivism
Espionage
Denial of Service
Sites Defacement
Information Theft

Critical Infrastructure



Cyberterrorism
Hacktivism
Denial of Service
Information Theft
Ransomware

Internet Users



Banking Fraud
Credit Card Fraud
Identity Theft
Data Leaks
Ransomware
Denial of Service

GC2018 Cyber Security Coordination

Games and Sponsors



24x7 dedicated team
Cyber Security Core Team

Symantec GOLDOC
Optus Cisco
Acquia

Government



- Focus on incidents targeting government websites

QLD Gov CIO

Critical Infrastructure



Physical presence at the Command & Control Centers

Focus on Critical Infrastructure Protection

ACSC
CERT Australia

Internet Users



Coordination among CERTs and Service Providers

Situational awareness Monitoring

ACSC
CERT Australia

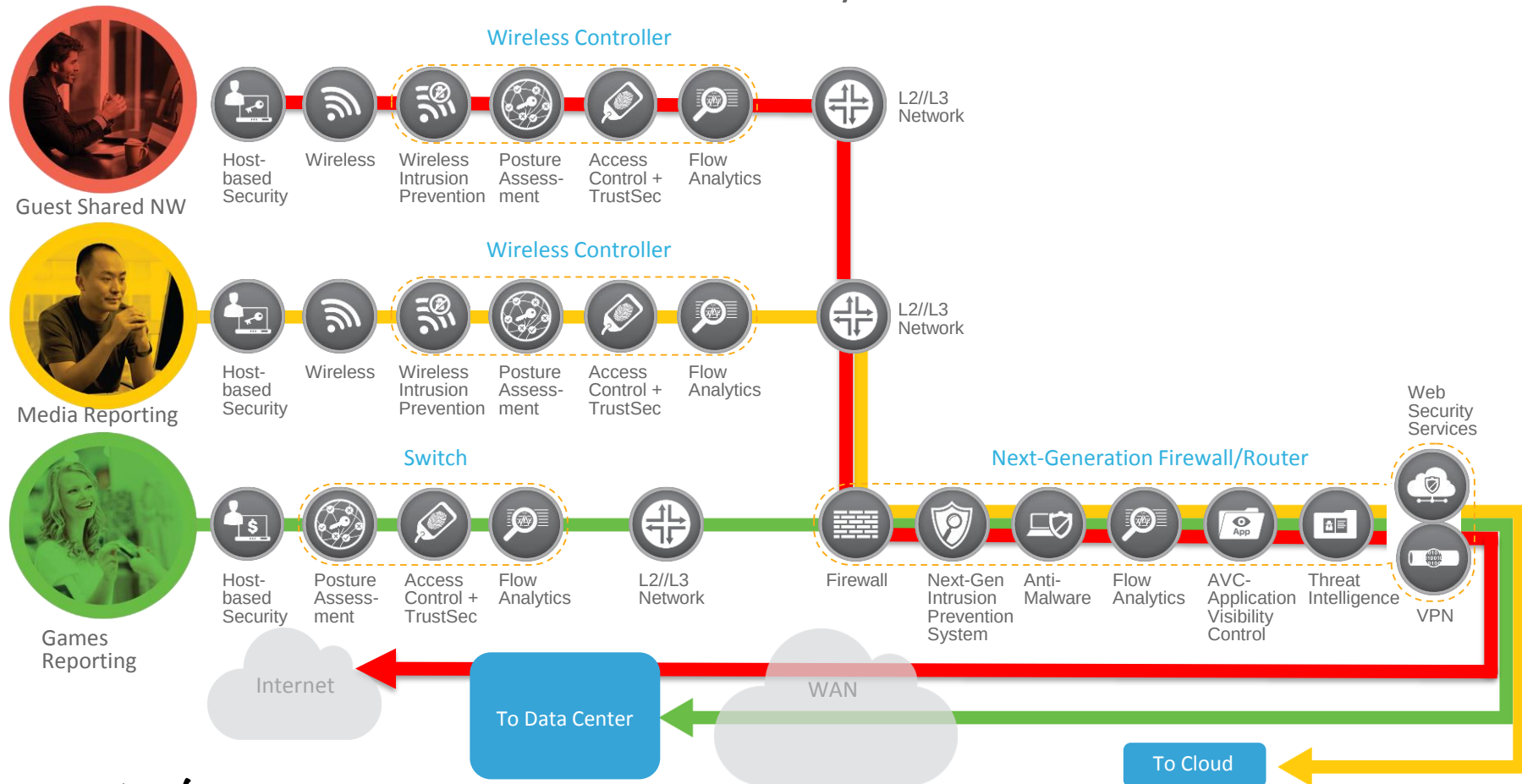
Operations Centre Coordination

- The Gold Coast Headquarters maintained two Operations Centers (one upstairs/one downstairs)
- The Main Operations Center (MOC) held Emergency Services (Police, Fire, Health), Transportation, and City, State and Federal government liaison personnel (Including Army) and Gold Coast staff
- The Technical Operations Center (TOC) held Vendors (AToS, Motorola, Cisco, Symantec), CERT, QLD-CIO, Gold Coast Cyber, and all Gold Coast technical staff (Scoring, Venue Liaison, Help Desk...)
- All communication between the MOC and TOC were handled by Senior Leadership.

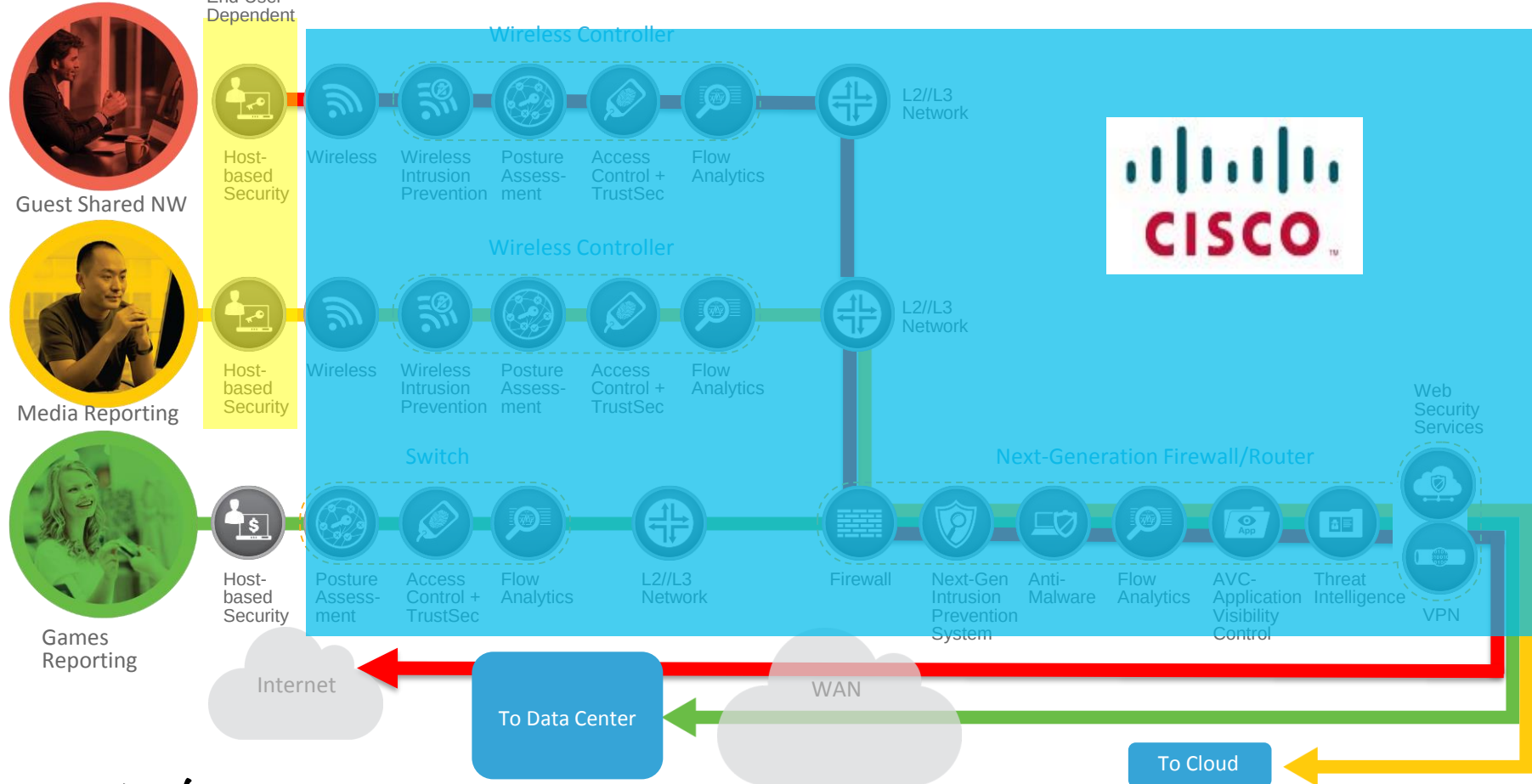


A good architecture

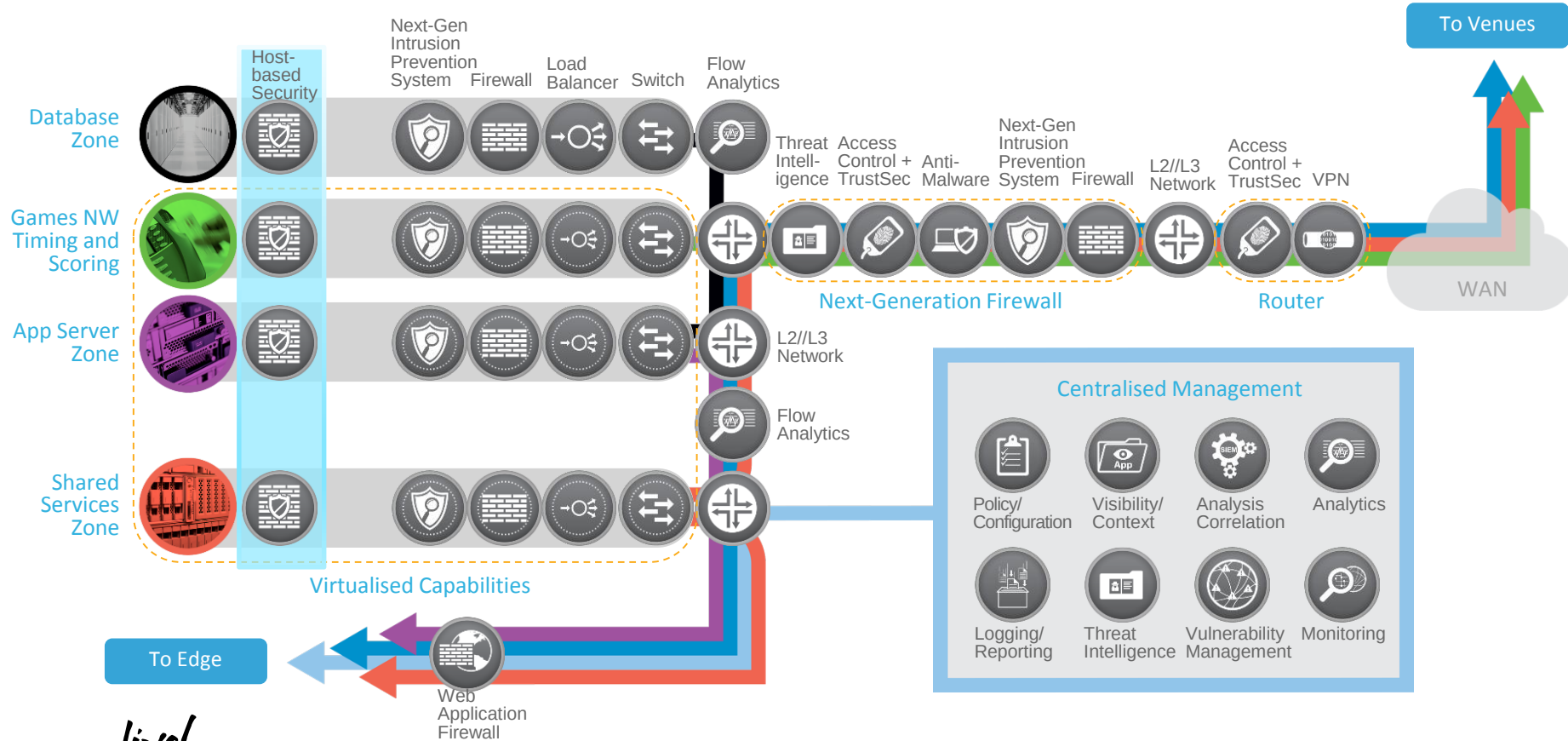
GoldOC 2018 Security: Venue



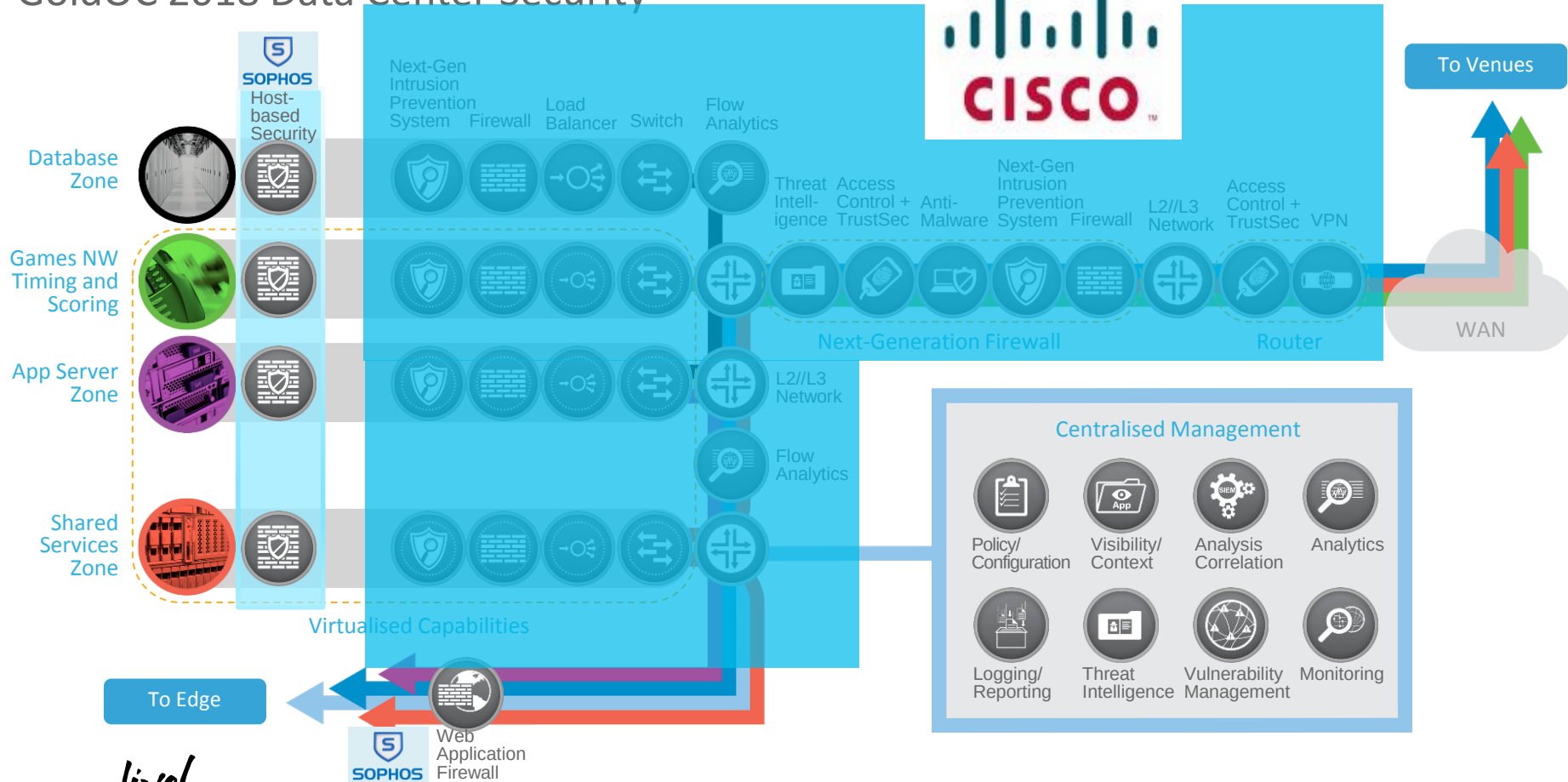
GoldOC 2016 Security: Venue



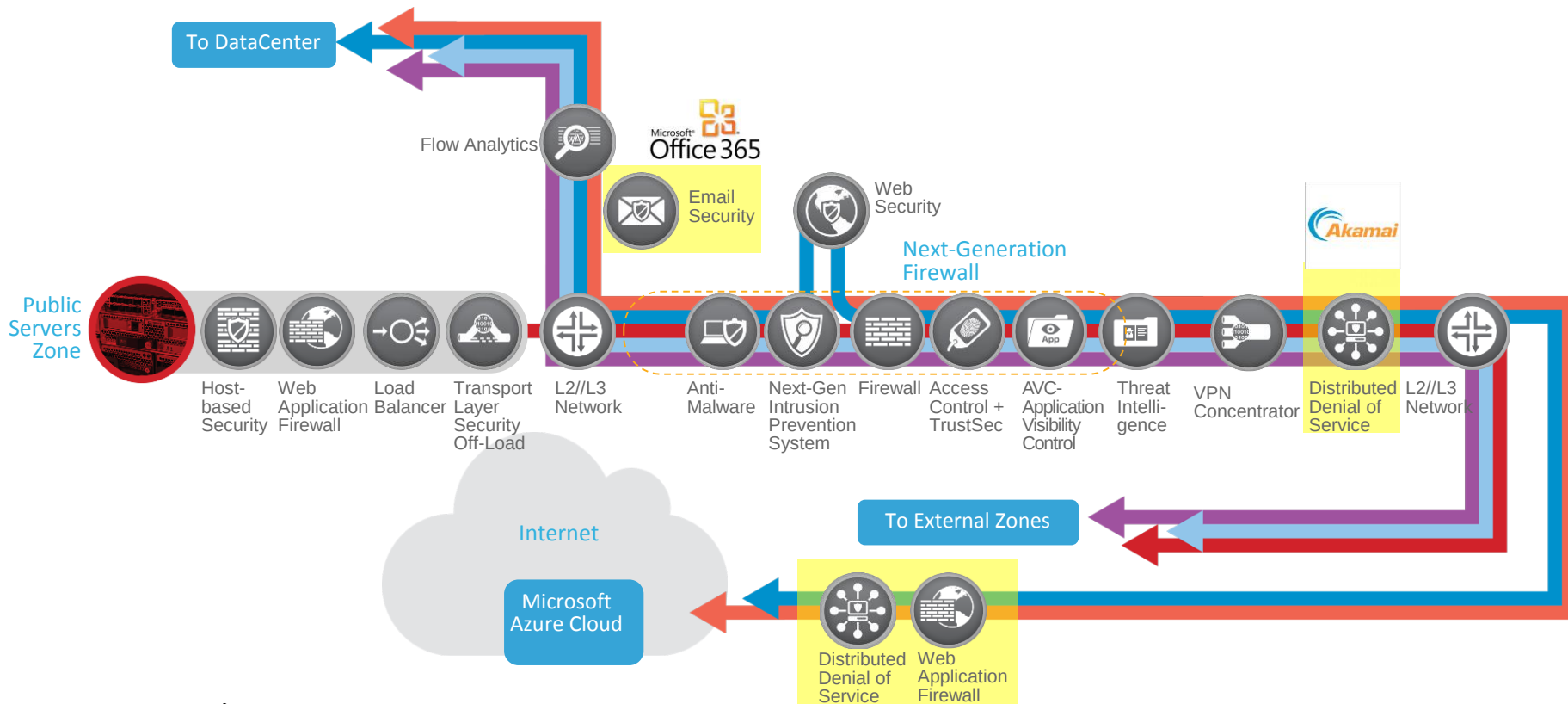
GoldOC 2018 Data Center Security



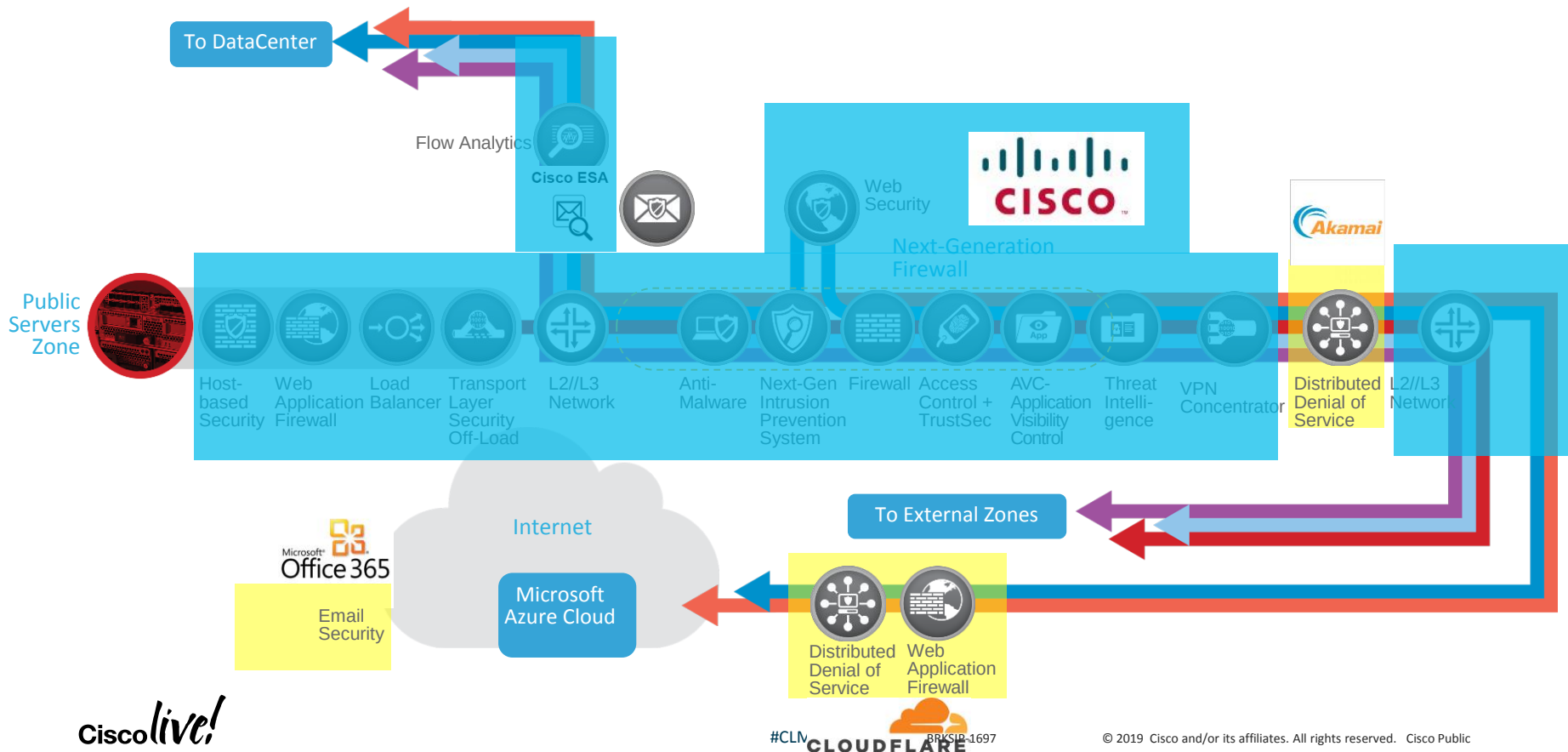
GoldOC 2018 Data Center Security



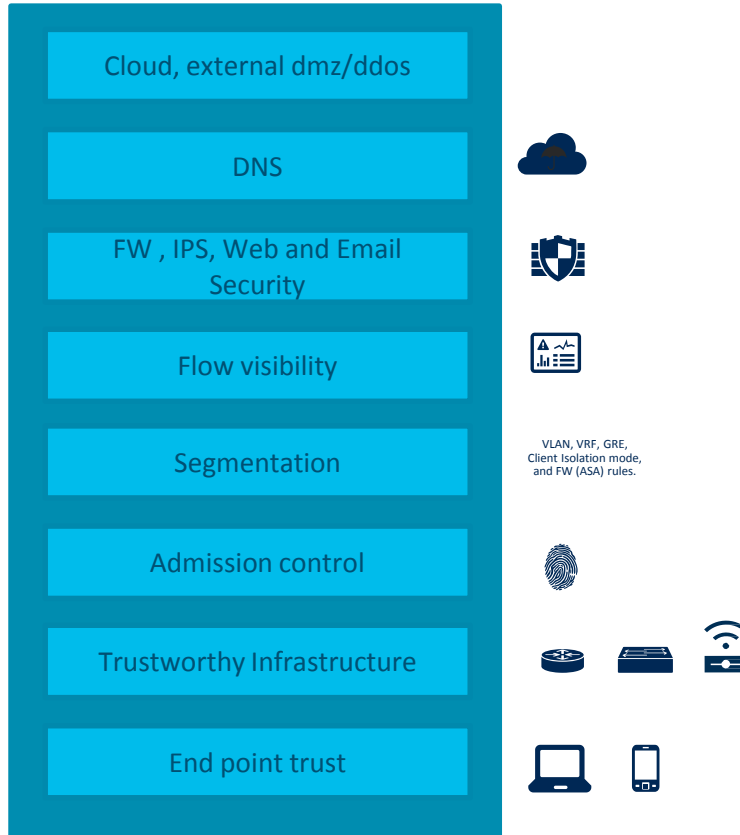
GoldOC 2018 Edge Security



GoldOC 2018 Edge Security



Client Group WiFi



Internet Only

DNS Umbrella Threat Protection

NGFW

Stealthwatch

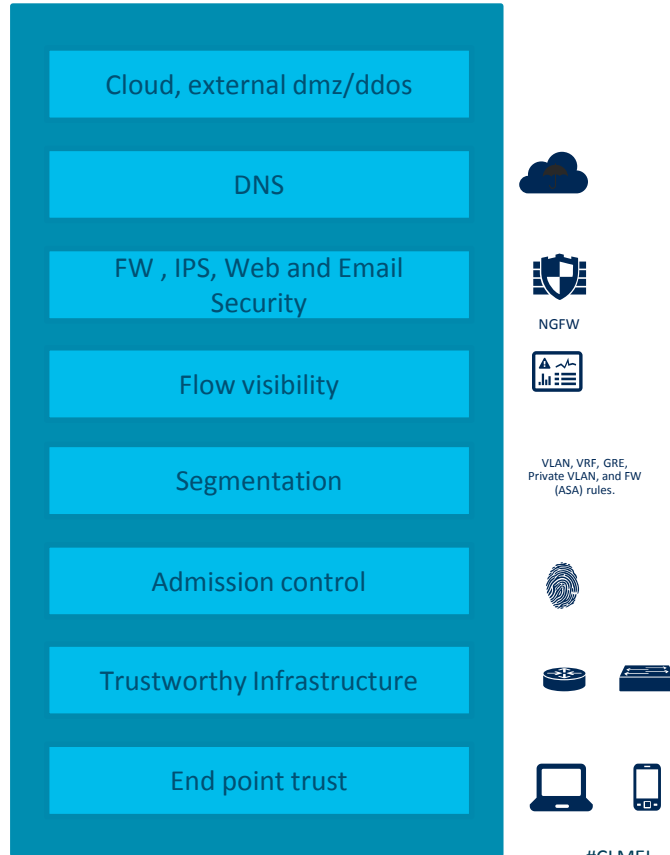
FlexConnect with Client Isolation Mode

.1x ISE

Optus Managed

Untrusted

Client Group Wired



Internet Only

DNS Umbrella Threat Protection

NGFW

Stealthwatch

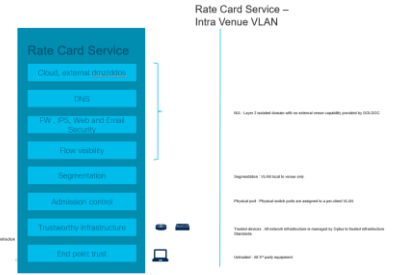
VRF / Private VLAN

.1x ISE

Optus Managed

Untrusted

Cisco *live!*



Security Statistics



Cisco Cloud Email Security



Cisco *live!*

Cloud Email Security

Operational Security

1,009,187

Total Attempted Emails

2

Cloud Email Security
Appliances

117,831

Total Threat Messages

131,833

Total Graymails

4,651

Spam
Detected

9

Viruses

4

AMP Detection



Cisco *live!*

Cisco Stealthwatch

Operational Security



143,191,117

Total Flows Per Second
19 Mar – 15 Apr 2018

51,113,968

Average Daily Flows Per
Second

498

Flows with Known Malicious
Servers

70.36m

Longest Flow with
Known Malicious

83T/41.9%

HTTPS

23.5T/11.9%

NFS

17.9T/9%

Undefined UDP

15.4T/7.8%

Streaming Audio/Video

14.5T/7.3%

Undefined TCP

14.1T/7.1%

HTTPS (Unclass)

12T/6.1%

HTTP

5T/2.5%

VPN

3.3T/1.7%

P2P File

2.1T/1%

HTTP (Unclass)

3.3T/.97%

NTP

Flow visibility

Stealthwatch

- Critical service monitoring
- Trusted protocol abuse
- External and internal scanning detection
- Policy compliance





Cisco Threatgrid

Operational Security



440

Total Threatgrid Submissions

14.67

Avg Submissions per day

420

Submitted by ESA

20

Submitted by User

2m 21s

Avg Analysis
Time

6

Convictions

20

Unique File Types

Analysis Report

ID	9510d137a783edc865c0031283f078eb
OS	Windows 7 64-bit
Started	4/10/18 04:48:51
Ended	4/10/18 04:52:54
Duration	0:04:03
Sandbox	mtv-work-046 (pilot-d)
Filename	Breakdown of Unpaid Invoices.doc
Magic Type	data
Analyzed As	rtf
SHA256	dedcf231ceafd0c0e5ae2df888c2e2cfc47f3501c0b53153c1c64ee22b679b
SHA1	68f2bc55506134d24ded369cb7ae96836f925201
MD5	c9640b6ca88416bce7417e46eb4eb5e1

Behavioral Indicators

➔	➕ Document Created an Executable File	Severity: 100	Confidence: 100	Created New Executable File
	➕ Microsoft Equation Editor (EQNEDT32.exe) Launched Child Process	Severity: 95	Confidence: 100	
	➕ Process Hollowing Detected	Severity: 100	Confidence: 95	
	➕ RTF Containing PE File	Severity: 95	Confidence: 100	
➔	➕ Document Contains an Embedded Executable File	Severity: 90	Confidence: 100	Downloaded Executable File
➔	➕ A Document File Established Network Communications	Severity: 100	Confidence: 90	Network Connection
	➕ Document Launched Utility Application	Severity: 100	Confidence: 90	
➔	➕ Registry Persistence Mechanism Refers to an Executable in a User Data Directory	Severity: 90	Confidence: 100	Created Persistence
	➕ Process Modified a File in a System Directory	Severity: 90	Confidence: 100	
➔	➕ Office Document Launches a Command Shell	Severity: 90	Confidence: 100	Opened "cmd.exe"
➔	➕ Document Deleted Resiliency Registry Key	Severity: 90	Confidence: 90	Deleted critical software



Cisco *live!*

Cisco Umbrella

Operational Security

376,394,859 Total DNS Requests 19 Mar – 15 Apr 2018		13,442,674 Average Daily DNS Resolutions	
174,929 Total Blocked Resolutions		6,247 Average Daily Blocked Resolutions	
40k C2	39K Malware	57K Destination Lists	
656 Phishing		10K Categories	



Indicators of Compromise

Direct Attacks Against Enterprise Admins



1.4 Malware Phishing

[Previous](#)[Next](#)

Threat: DHL Malspam with Hancitor Payload

Summary:

We received intelligence of a malicious SPAM, leading to a Hancitor infection as its payload. Cisco reported that enterprise administrator [REDACTED] received such e-mail, but the e-mail was promptly dropped by the e-mail security solution. We then verified the incident by checking MSS monitored logs and Umbrella for the post-compromise indicators. So far, we can safely report that only [REDACTED] received the e-mail and there were no malicious incidents.

Detection and Response

Detection



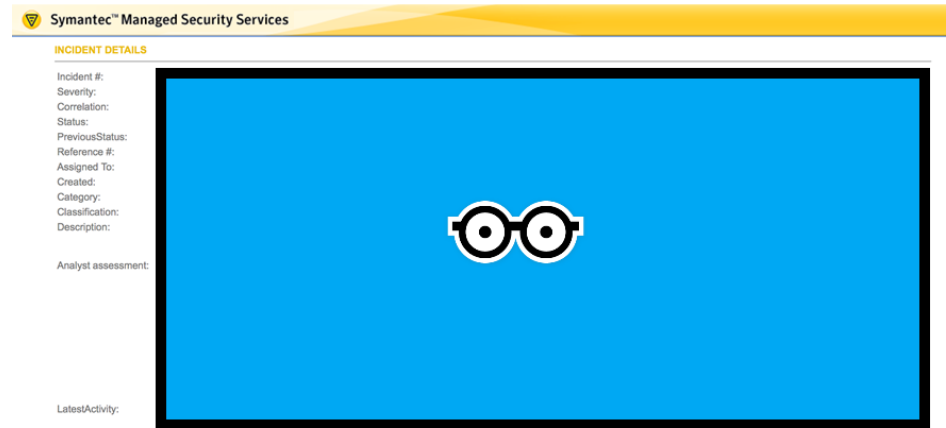
- The primary detection systems were
 - Umbrella (DNS filtering)
 - Symantec SIEM (endpoint logs)
 - Email Security Appliance (email)
 - Stealthwatch (network)



Symantec SIEM – Response Flow



- The SIEM would send email to the team to investigate an issue.
- The team would use Umbrella and Stealthwatch to identify the end user, and see if the issue was on one host, or many. (Any lateral movement, internal to external communication or DNS lookups to malicious domains)
- The GC2018 Shift Lead would create a case for the appropriate team to respond (Desktop, Network, Server)



Umbrella – Response Flow

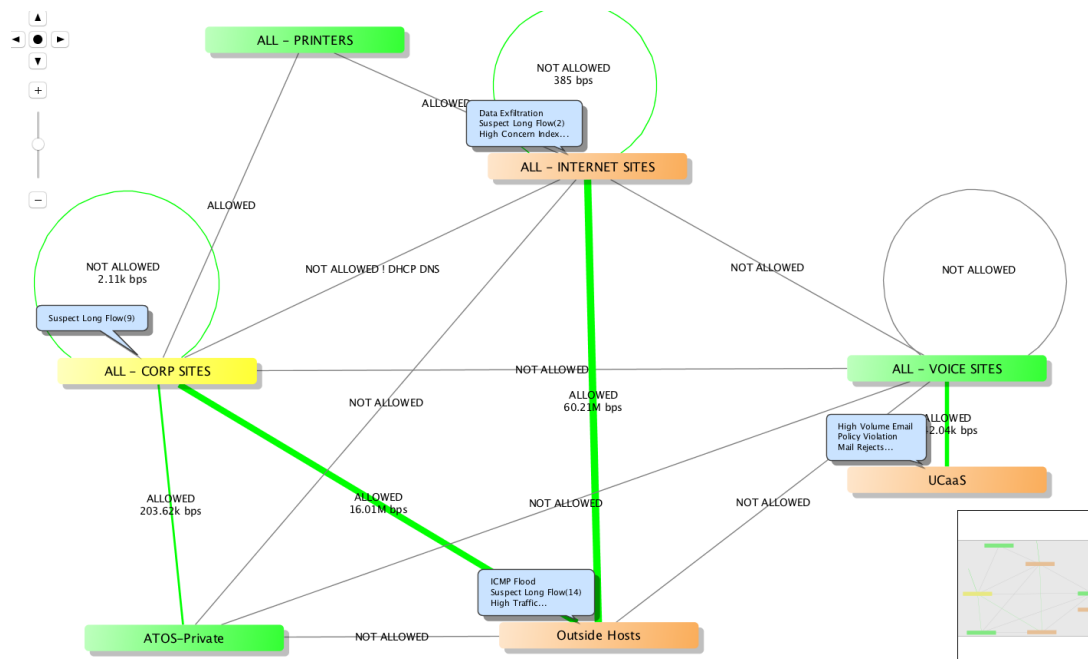


AD Users	10.16.128.22	Blocked	Malware	Mar 24, 2018 at 4:48 PM
AD Users	10.16.128.22	Blocked	Malware	Mar 24, 2018 at 4:48 PM
Internal Networks	10.56.64.5	Blocked	Malware	Mar 24, 2018 at 4:48 PM
Internal Networks	10.52.19.1	Blocked	Malware	Mar 24, 2018 at 4:19 PM
Networks		Blocked	Malware	Mar 24, 2018 at 4:17 PM
Networks		Blocked	Malware	Mar 24, 2018 at 4:17 PM
AD Users	10.23.160.207	Blocked	Malware	Mar 24, 2018 at 4:13 PM
AD Users	10.25.128.4	Blocked	Malware	Mar 24, 2018 at 4:09 PM

- Umbrella was monitored continuously by the Security Team
- For Malware infections, the GC2018 Shift Leader created a case for the desktop team to investigate and remediate.
- For C2 infections, the Security Team used Stealthwatch to see what devices were communicating with the infected host.
- Coordination was conducted using chat; Case notes were updated, investigated and closed.

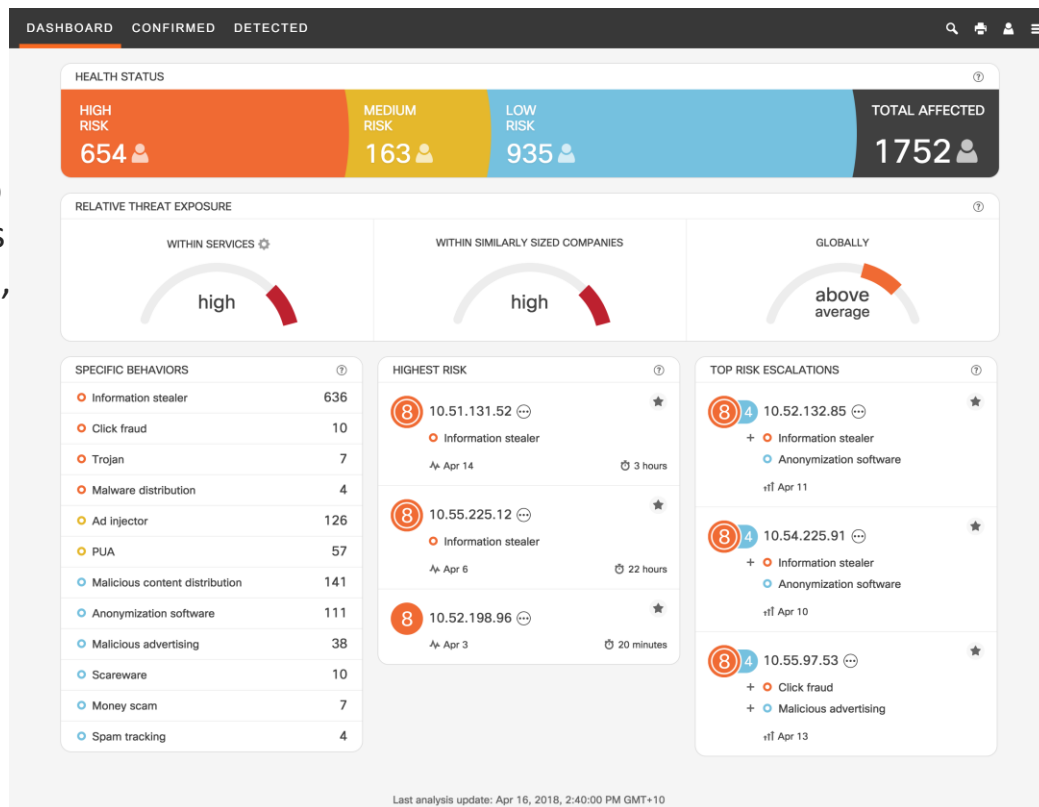
Stealthwatch Real-Time Monitoring

- The Network has rules about which groups can or cannot communicate
- This diagram shows the rules in real-time.
- Lateral policy violations are flagged and investigated
- Some issues:
 - Network mis-configuration
 - Out of policy traffic
 - Malicious traffic



Stealthwatch – Response Flow

- Cognitive summarised complex Stealthwatch data into easily addressed issues.
- The team used Umbrella and Stealthwatch to identify the end user, and see if the issue was on one host, or many. (Any lateral movement, internal to external communication or DNS lookups to malicious domains)
- The GC2018 Shift Lead would create a case for the appropriate team to respond (Desktop, Network, Server)



Lessons learnt

Lessons Learnt



- The Communications between the security partners onsite worked well – and access to comms both on and offsite was beneficial to staff coming on and off shift.
- The Onsite Cisco Security Team were invaluable not only for the Internal View of the operations but also as a Contact Point for the Delivery Teams.
- A well designed network which incorporates segmentation / zones, traffic isolation, visibility / telemetry, and control points is critical.
- Umbrella and Stealthwatch were invaluable for visibility insights – both threat and policy especially where end points and systems were 3rd party or unmanaged.
- Difficult to baseline a traffic and applications for correct known behavior with a short ramp up period. Maximise the value of any lead up or test events by having security and monitoring in place prior.

Summary – Agility is Key

- The games were successful to due to preparations made by the organising committee defenders
- As with all networks, security events were detected but no production or critical systems were impacted
- Roll on Tokyo 2020 ! 😊



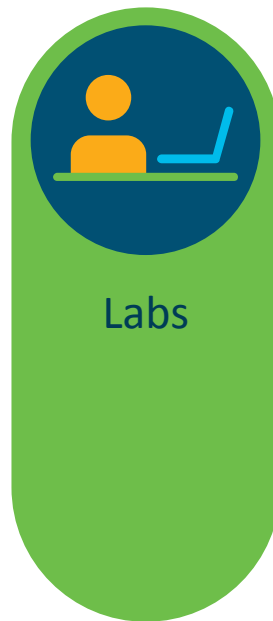
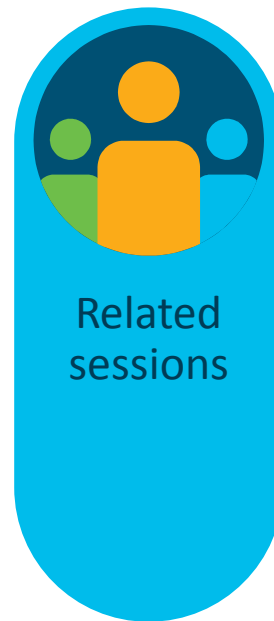


Q & A



INTUITIVE

Continue your education



Complete your online session evaluation

- Give us your feedback and receive a complimentary **Cisco Live 2019 Power Bank** after completing the overall event evaluation and 5 session evaluations.
- All evaluations can be completed via the Cisco Live Melbourne Mobile App.
- Don't forget: Cisco Live sessions will be available for viewing on demand after the event at:

<https://ciscolive.cisco.com/on-demand-library/>





Thank you



INTUITIVE



INTUITIVE