Welcome to Tomorrow ... Today

The need and benefit of merging of IT and Security in today's ever connected world of security and IT

Tim Lee

CISO, City of LA

Ernie Welch

Sales Engineer, Splunk

.conf2016

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

City of Los Angeles

- 2nd largest city in U.S
- Population: 4 Million
- Annual visitors: 43 Million
- 43 departments, 35,000 FTE
- Critical Infrastructure Sectors

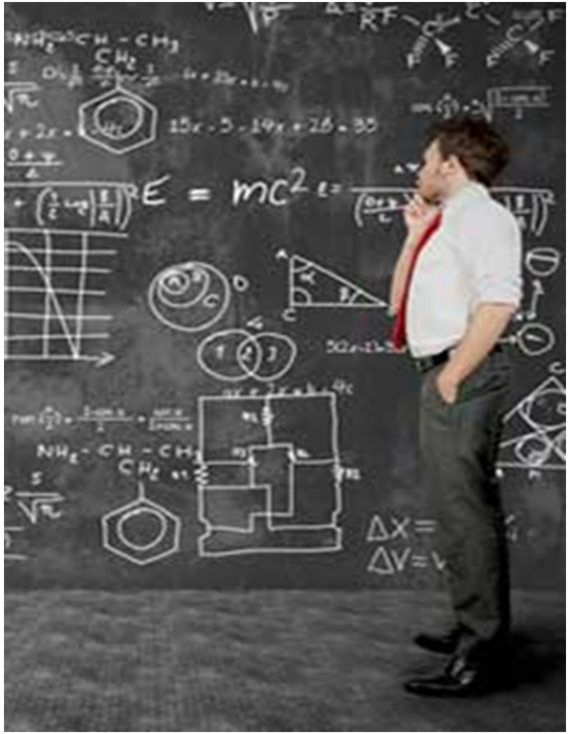
Mayor’s Executive Directive on Cybersecurity

“I’m creating this Cyber Intrusion Command Center (CICC) so that we have a single, focused team responsible for implementing enhanced security standards across city departments and serving as a rapid reaction force to cyber-attacks,”

Mayor Eric Garcetti

Challenges

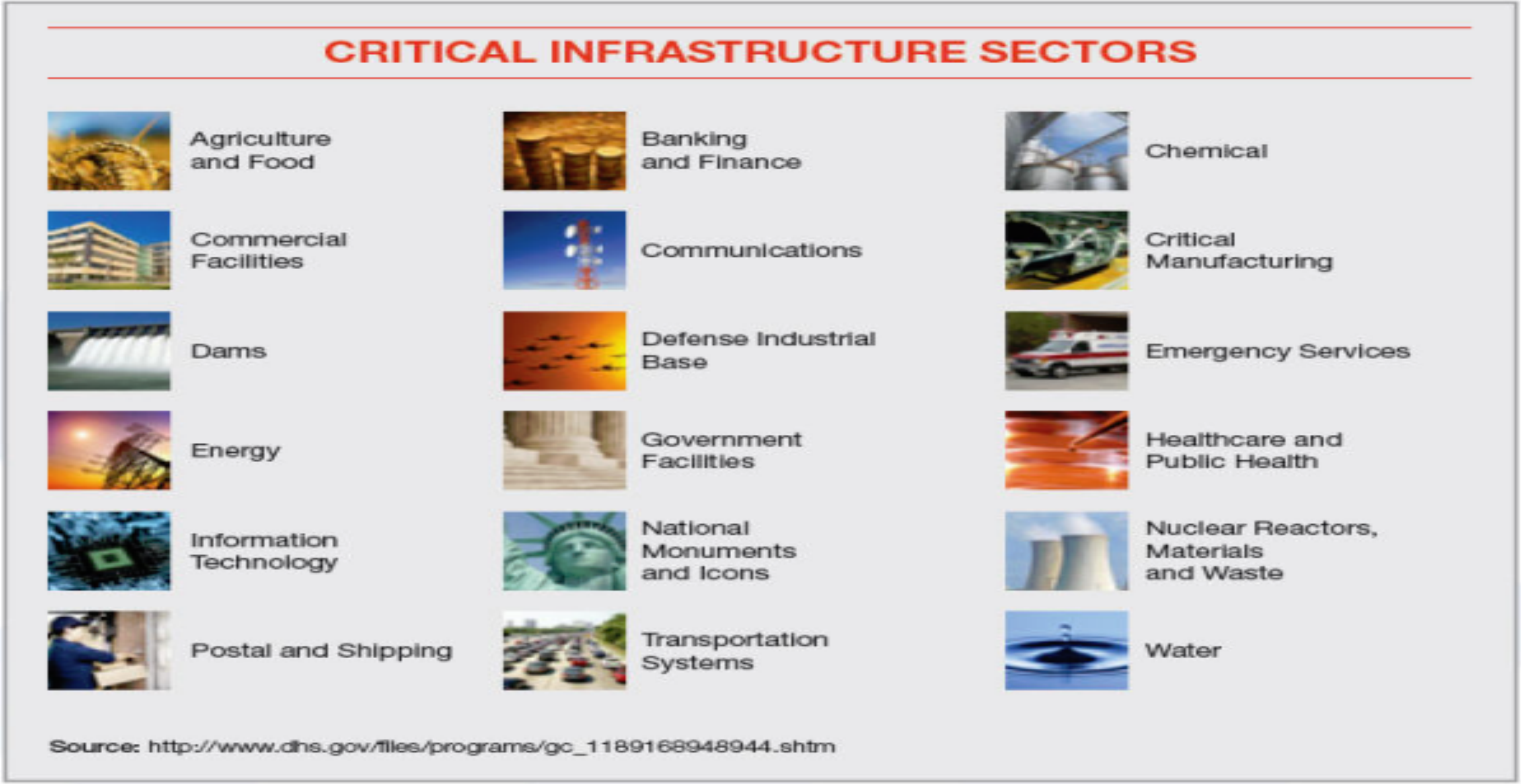
- “Siloed” SOCs/NOCs
- Dispersed and massive log capturing
- Lack of centralized Incident Management capabilities
- No threat intelligence analysis and sharing platform
- Limited Situation Awareness (SA) and security metrics city-wide



Solution

Integrated SOC

Critical Asset Protection (CAP)



CRITICAL INFRASTRUCTURE SECTORS

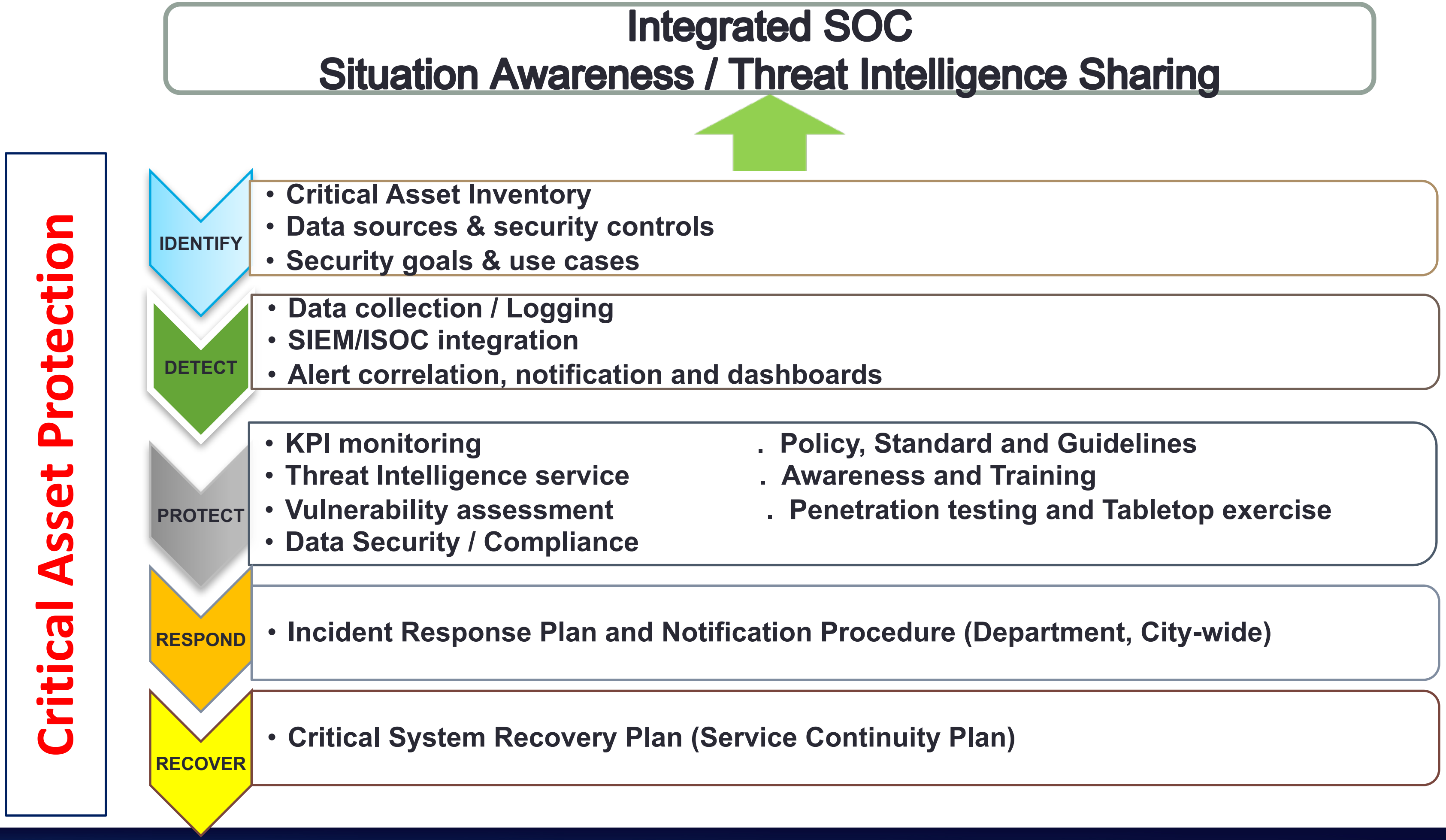
Agriculture and Food	Banking and Finance	Chemical
Commercial Facilities	Communications	Critical Manufacturing
Dams	Defense Industrial Base	Emergency Services
Energy	Government Facilities	Healthcare and Public Health
Information Technology	National Monuments and Icons	Nuclear Reactors, Materials and Waste
Postal and Shipping	Transportation Systems	Water

Source: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

Critical Asset

*A **"Critical Asset"** is defined as any system, whether physical or virtual, so vital to the City of Los Angeles and its citizens, that the incapacity or destruction of such systems, or the unauthorized access and/or dissemination of the information contained therein, would have a debilitating impact on the City's security, economic security, public health or safety, or any combination of those matters.*

Integrated SOC
Situation Awareness / Threat Intelligence Sharing



Critical Asset Protection

IDENTIFY

- Critical Asset Inventory
- Data sources & security controls
- Security goals & use cases

DETECT

- Data collection / Logging
- SIEM/ISOC integration
- Alert correlation, notification and dashboards

PROTECT

- KPI monitoring
- Threat Intelligence service
- Vulnerability assessment
- Data Security / Compliance

. Policy, Standard and Guidelines
. Awareness and Training
. Penetration testing and Tabletop exercise

RESPOND

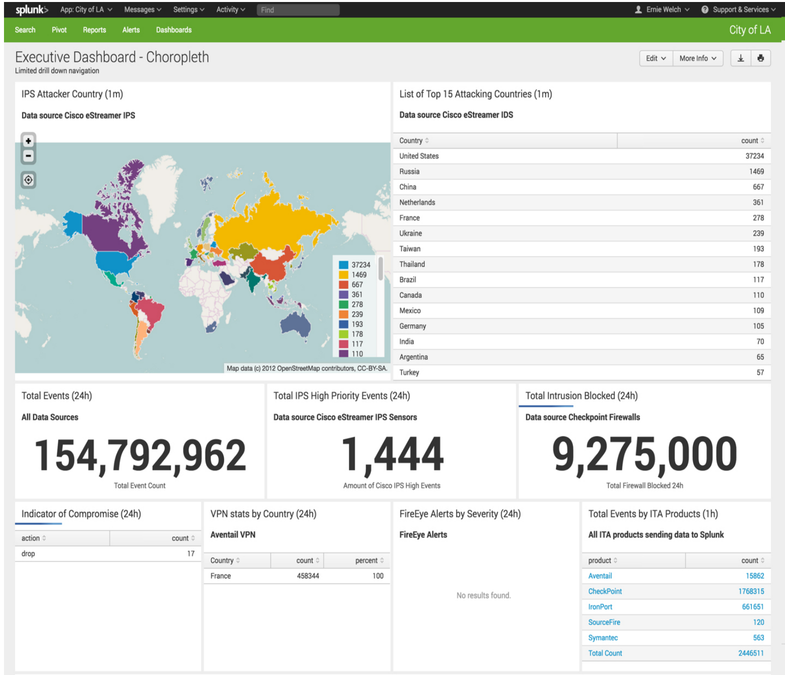
- Incident Response Plan and Notification Procedure (Department, City-wide)

RECOVER

- Critical System Recovery Plan (Service Continuity Plan)

Enterprise Security

ES and a bifurcated ISOC dashboard



Executive Dashboard - Choropleth

Limited drill down navigation

IPS Attacker Country (1m)

Data source Cisco eStreamer IPS

Map data (c) 2012 OpenStreetMap contributors, CC-BY-SA.

List of Top 15 Attacking Countries (1m)

Data source Cisco eStreamer IDS

Country	count
United States	37234
Russia	1469
China	667
Netherlands	361
France	278
Ukraine	239
Taiwan	193
Thailand	178
Brazil	117
Canada	110
Mexico	109
Germany	105
India	70
Argentina	65
Turkey	57

Total Events (24h)

All Data Sources

154,792,962

Total Event Count

Total IPS High Priority Events (24h)

Data source Cisco eStreamer IPS Sensors

1,444

Amount of Cisco IPS High Events

Total Intrusion Blocked (24h)

Data source Checkpoint Firewalls

9,275,000

Total Firewall Blocked 24h

Indicator of Compromise (24h)

action	count
drop	17

VPN stats by Country (24h)

Aventail VPN

Country	count	percent
France	458344	100

FireEye Alerts by Severity (24h)

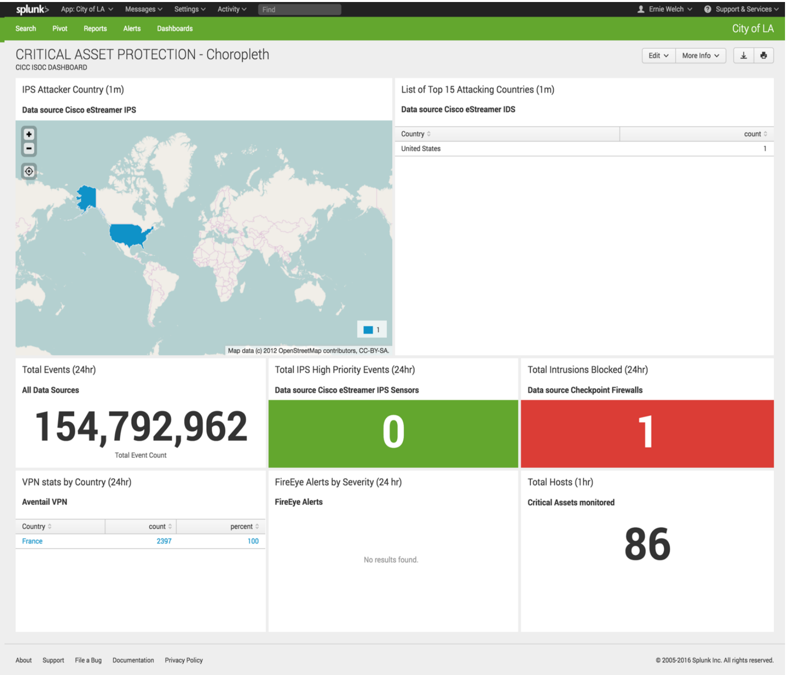
FireEye Alerts

No results found.

Total Events by ITA Products (1h)

All ITA products sending data to Splunk

product	count
Aventail	15862
CheckPoint	1768315
IronPort	661651
SourceFire	120
Symantec	563
Total Count	2446511



CRITICAL ASSET PROTECTION - Choropleth

CICC ISOC DASHBOARD

IPS Attacker Country (1m)

Data source Cisco eStreamer IPS

Map data (c) 2012 OpenStreetMap contributors, CC-BY-SA.

List of Top 15 Attacking Countries (1m)

Data source Cisco eStreamer IDS

Country	count
United States	1

Total Events (24hr)

All Data Sources

154,792,962

Total Event Count

Total IPS High Priority Events (24hr)

Data source Cisco eStreamer IPS Sensors

0

Total Intrusions Blocked (24hr)

Data source Checkpoint Firewalls

1

VPN stats by Country (24hr)

Aventail VPN

Country	count	percent
France	2397	100

FireEye Alerts by Severity (24 hr)

FireEye Alerts

No results found.

Total Hosts (1hr)

Critical Assets monitored

86

About Support File a Bug Documentation Privacy Policy

© 2005-2016 Splunk Inc. All rights reserved.

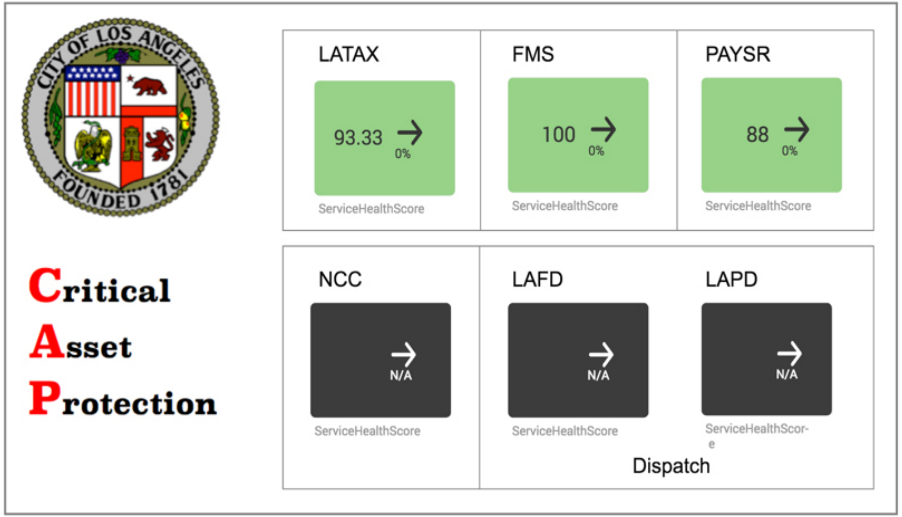
IT Service Intelligence

Current Deployment

- We’ve deployed 5 of the 43 departments within City of LA
- We’re modeled 38 Services
- We’ve created 30 individual glass tables
- We’re monitoring 160 KPI’s
- We’ve enabled ML for anomaly detection / adaptive thresholds
- We’re using Multi-KPI Alerting for advanced notifications

IT Service Intelligence

Role Based Access Control



Critical
Asset
Protection

LATAX
93.33 → 0%
ServiceHealthScore

FMS
100 → 0%
ServiceHealthScore

PAYSR
88 → 0%
ServiceHealthScore

NCC
→ N/A
ServiceHealthScore

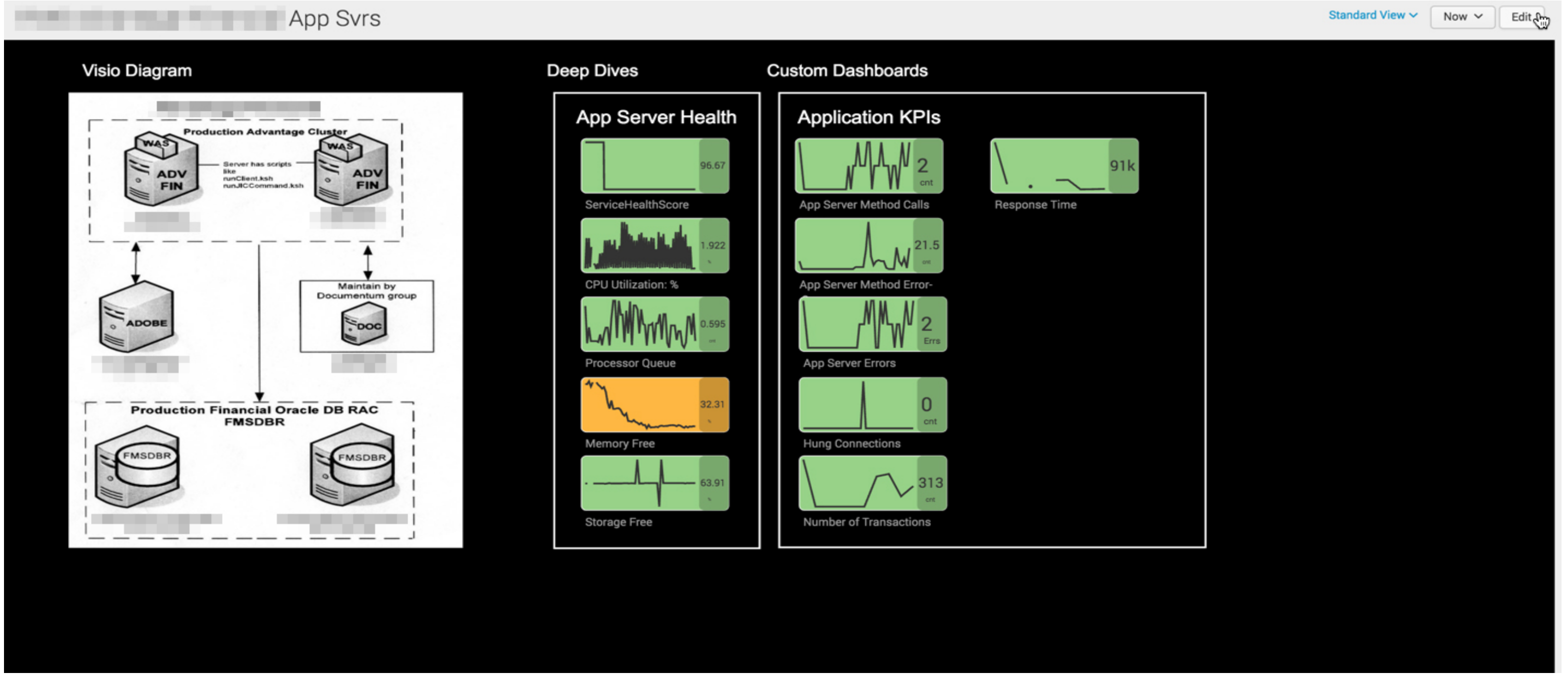
LAFD
→ N/A
ServiceHealthScore

LAPD
→ N/A
ServiceHealthScor-
e

Dispatch

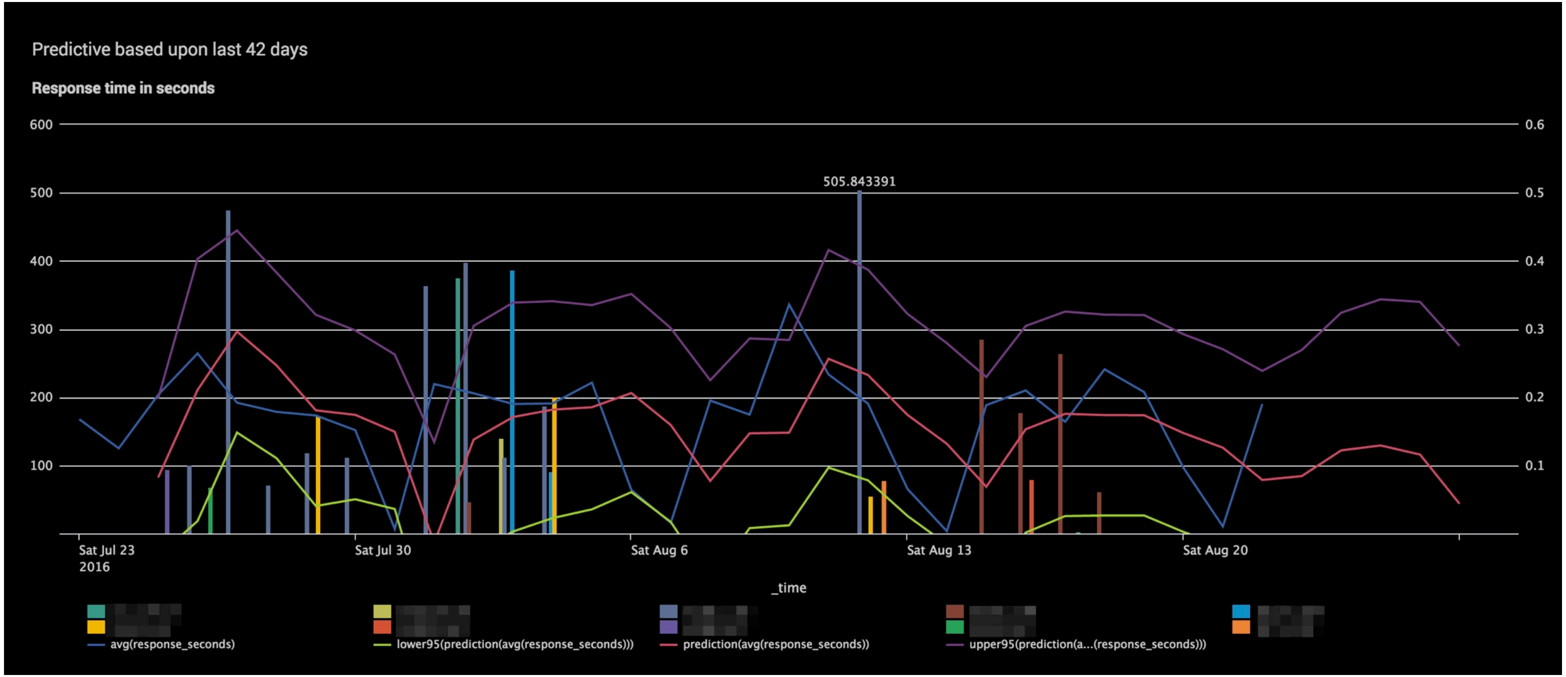
IT Service Intelligence

Using multi glass tables



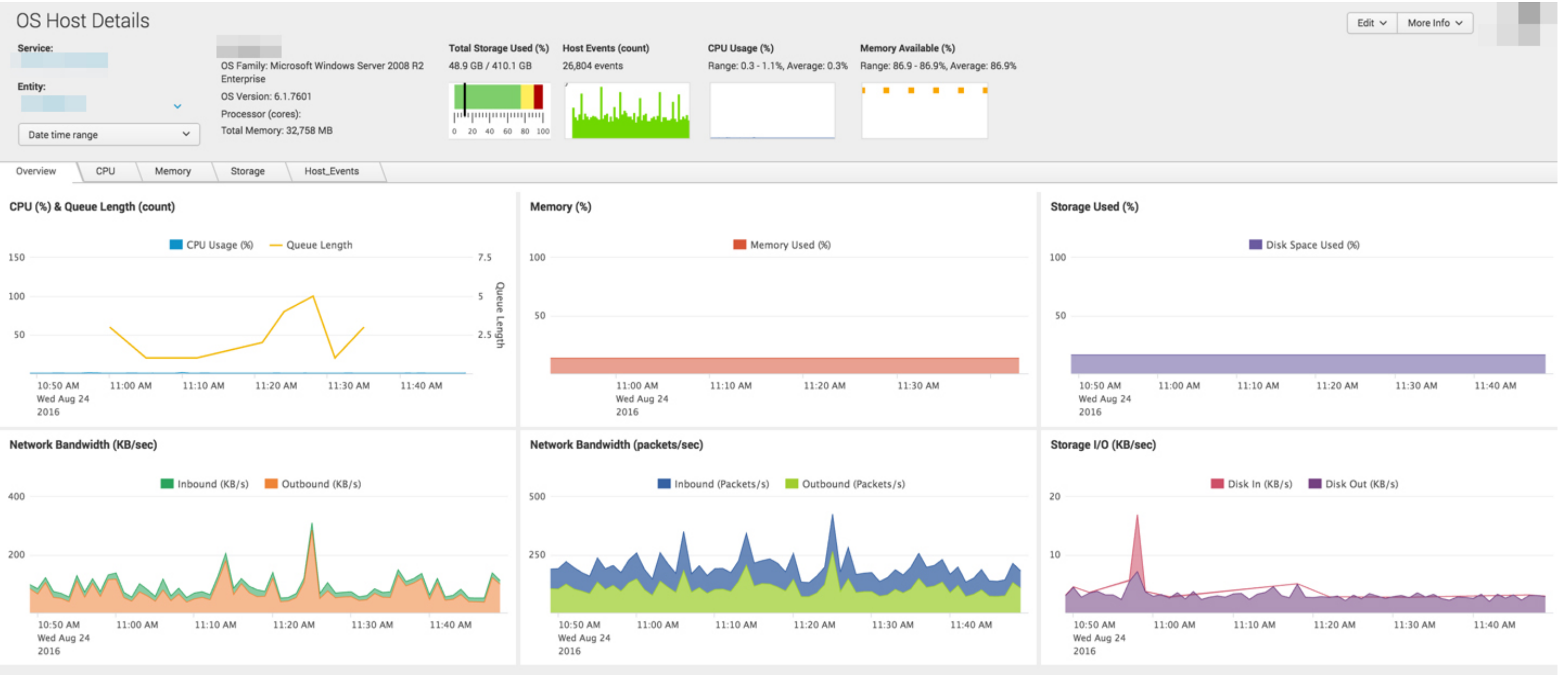
IT Service Intelligence

Leveraging core dashboards from ITSI



IT Service Intelligence

Deep Dives and OS Host Details



OS Host Details

Service: [redacted]

Entity: [redacted]

Date time range

[redacted]

OS Family: Microsoft Windows Server 2008 R2 Enterprise

OS Version: 6.1.7601

Processor (cores):

Total Memory: 32,758 MB

Total Storage Used (%): 48.9 GB / 410.1 GB

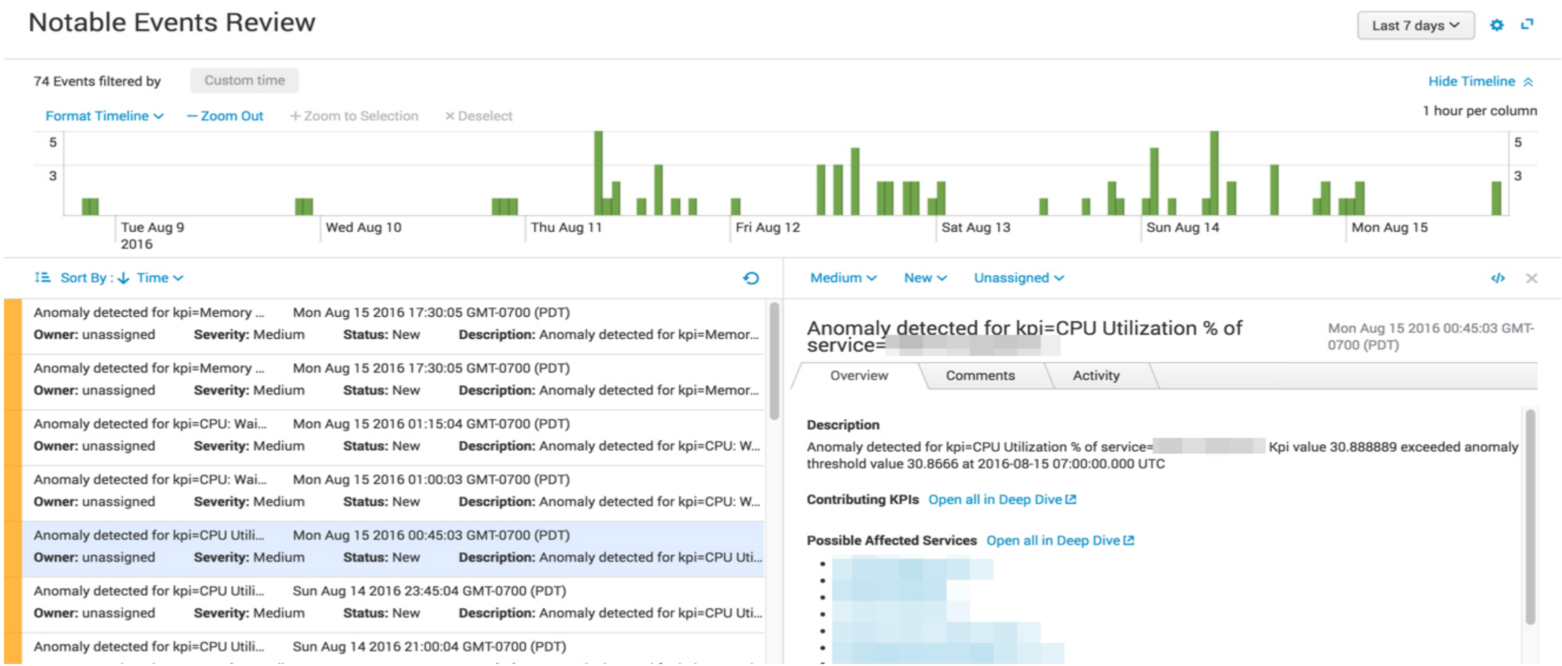
Host Events (count): 26,804 events

CPU Usage (%): Range: 0.3 - 1.1%, Average: 0.3%

Memory Available (%): Range: 86.9 - 86.9%, Average: 86.9%

Tomorrow…Today

ITSI multi-KPI Alerts and Notable Events



Notable Events Review

Anomaly detected for kpi=Memory … Mon Aug 15 2016 17:30:05 GMT-0700 (PDT)
Owner: unassigned **Severity:** Medium **Status:** New **Description:** Anomaly detected for kpi=Memor…

Anomaly detected for kpi=Memory … Mon Aug 15 2016 17:30:05 GMT-0700 (PDT)
Owner: unassigned **Severity:** Medium **Status:** New **Description:** Anomaly detected for kpi=Memor…

Anomaly detected for kpi=CPU: Wai… Mon Aug 15 2016 01:15:04 GMT-0700 (PDT)
Owner: unassigned **Severity:** Medium **Status:** New **Description:** Anomaly detected for kpi=CPU: W…

Anomaly detected for kpi=CPU: Wai… Mon Aug 15 2016 01:00:03 GMT-0700 (PDT)
Owner: unassigned **Severity:** Medium **Status:** New **Description:** Anomaly detected for kpi=CPU: W…

Anomaly detected for kpi=CPU Utili… Mon Aug 15 2016 00:45:03 GMT-0700 (PDT)
Owner: unassigned **Severity:** Medium **Status:** New **Description:** Anomaly detected for kpi=CPU Uti…

Anomaly detected for kpi=CPU Utili… Sun Aug 14 2016 23:45:04 GMT-0700 (PDT)
Owner: unassigned **Severity:** Medium **Status:** New **Description:** Anomaly detected for kpi=CPU Uti…

Anomaly detected for kpi=CPU Utili… Sun Aug 14 2016 21:00:04 GMT-0700 (PDT)

Anomaly detected for kpi=CPU Utilization % of service=[redacted]

Mon Aug 15 2016 00:45:03 GMT-0700 (PDT)

Description

Anomaly detected for kpi=CPU Utilization % of service=[redacted] Kpi value 30.888889 exceeded anomaly threshold value 30.8666 at 2016-08-15 07:00:00.000 UTC

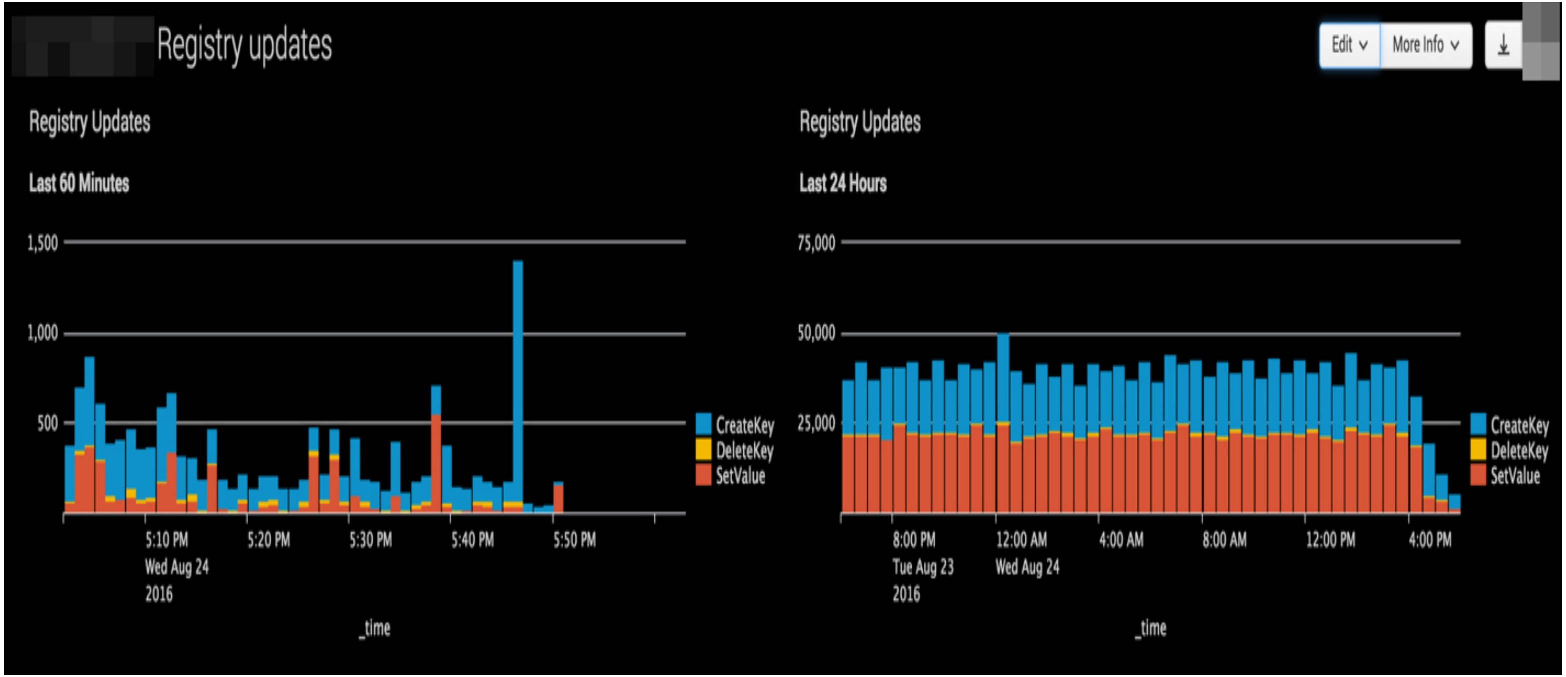
Contributing KPIs Open all in Deep Dive

Possible Affected Services Open all in Deep Dive

- [redacted]

ITSI & Security

Starting to tie it all together



Lessons Learned

- Start getting events into Splunk ASAP
- Engage Business Service SME’s early
  - DB Servers
  - Web Servers
  - App Servers
- Leverage KPI Base Searches – much more efficient
- Leverage Threshold templates – Saves time, builds standards

What Now?

Related breakout sessions and activities…

THANK YOU

.conf2016

splunk>