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

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

- KPI monitoring
  - Policy, Standard and Guidelines
- Threat Intelligence service
  - Awareness and Training
- Vulnerability assessment
  - Penetration testing and Tabletop exercise
- Data Security / Compliance

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

- Critical System Recovery Plan (Service Continuity Plan)
Enterprise Security

ES and a bifurcated ISOC dashboard
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

<table>
<thead>
<tr>
<th></th>
<th>LATAx</th>
<th>FMS</th>
<th>PAYSR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>93.33%</td>
<td>100%</td>
<td>88%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>NCC</th>
<th>LAFD</th>
<th>LAPD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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
Tomorrow...Today

ITSI multi-KPI Alerts and Notable Events
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