RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: STR-F03

INTEGRATED SECURITY OPERATIONS CENTER (ISOC) FOR CYBERSECURITY COLLABORATION

TIMOTHY LEE

CHIEF INFO SECURITY OFFICER
CITY OF LOS ANGELES

#RSAC

Background – City of Los Angeles

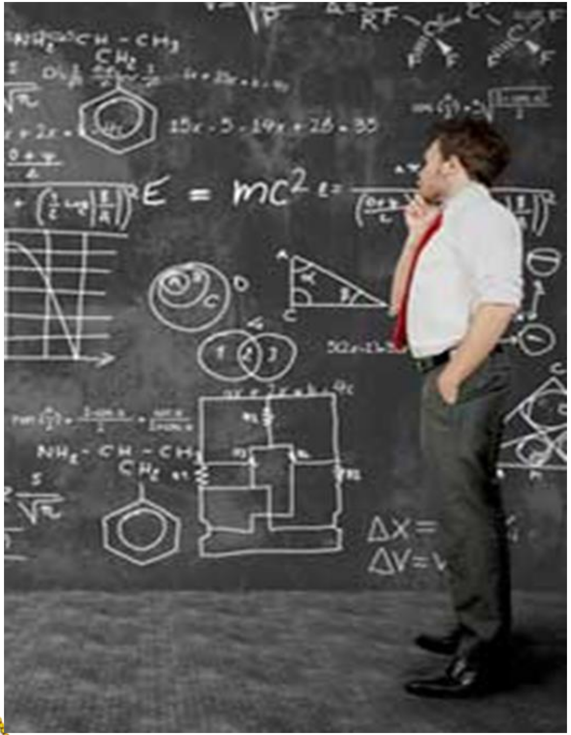
- 4 Million people, 465 sq mi, 15 Council District
- 2nd largest city in US
- Employment: 1.81 million
- Annual visitors: 42.21 Million
- 43 departments, 35,000 FTE
- Port of LA, Airport, Water and Power (3 Proprietary Departments) managing their own networks
- Information Technology Agency (ITA) manages the rest

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

Business Challenge



- IT Security Team is understaffed
- Dispersed log capturing capabilities
- Minimal use of collaboration tools
- Lack of Incident Management platform
- No integrated threat intelligence program
- Limited situation awareness (SA) and operational metrics for City as a whole
- Imbalance in Detection and Response capability
- “Siloed” SOCs/NOCs

Solution

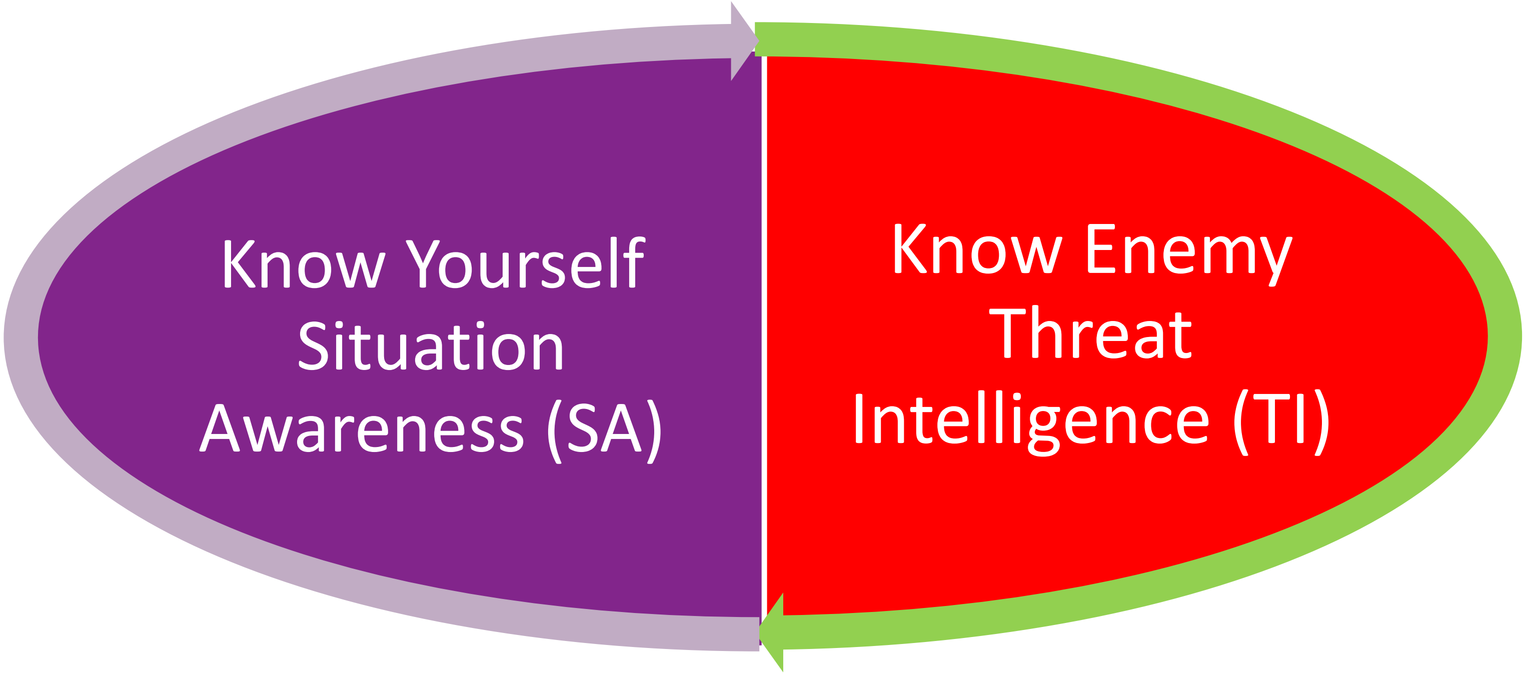
Integrated Security Operations Center (ISOC)

Know yourself, Know the enemy

"If you know the enemy and know yourself, you need not fear the result of a hundred battles."

— Sun Tzu, The Art of War

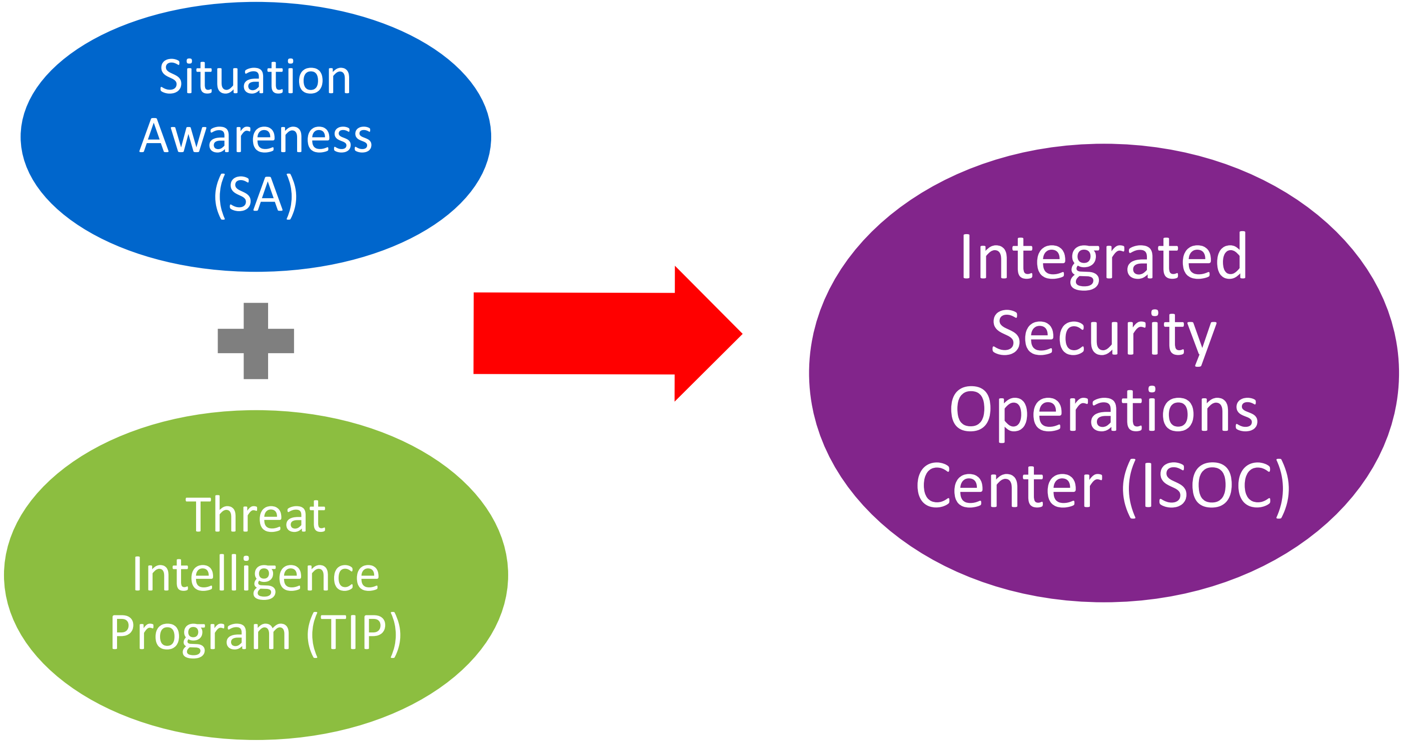
Know yourself, Know your Enemy



Know Yourself
Situation
Awareness (SA)

Know Enemy
Threat
Intelligence (TI)

Integrated Security Operations Center



Situation Awareness (SA)

Threat Intelligence Program (TIP)

Integrated Security Operations Center (ISOC)

Situation Awareness

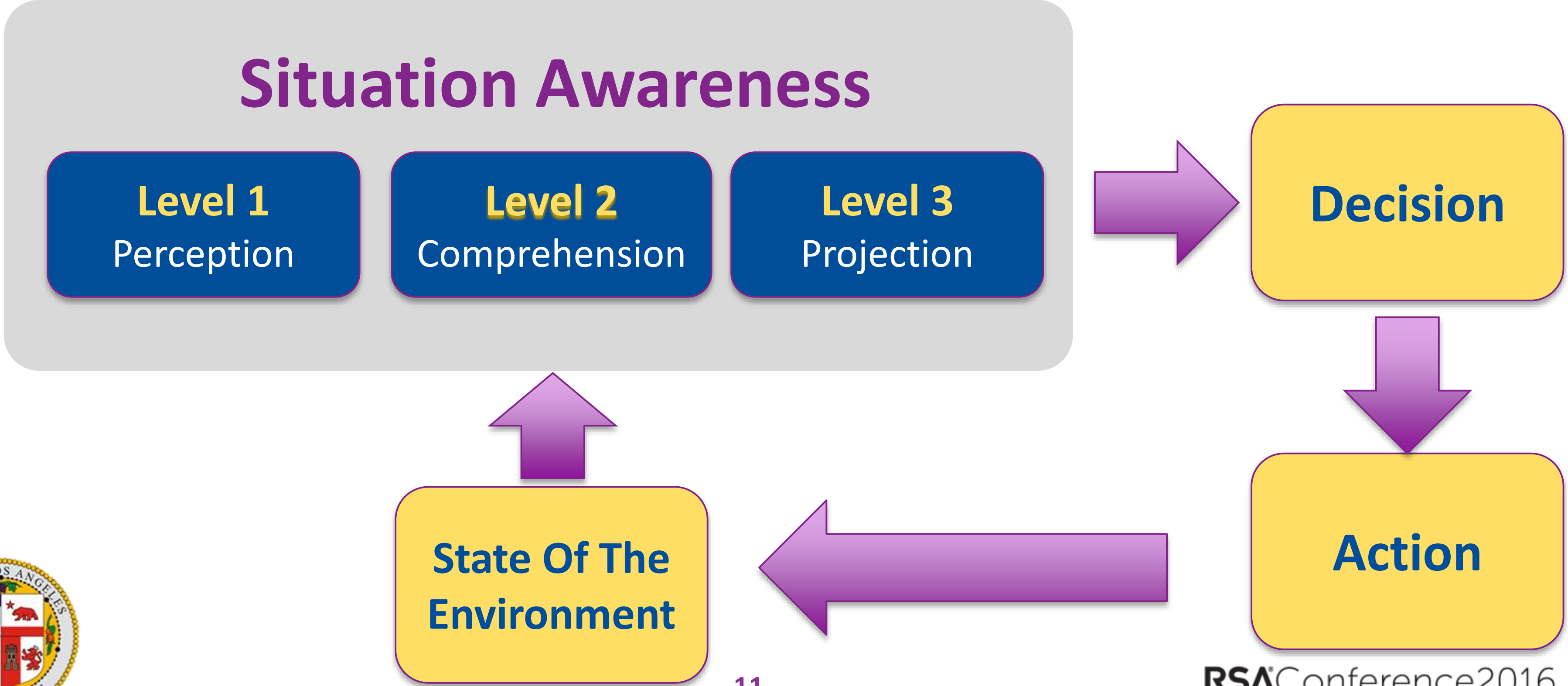
- ***Knowing What is going on***

What is Situation Awareness ?

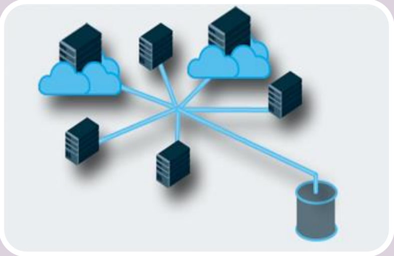
Situation Awareness (SA) is the ***perception*** of the elements in the environment within a volume of time and space, the ***comprehension*** of their meaning, and the ***projection*** of their status in the near future.

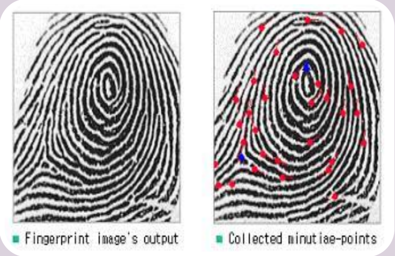
Mica Endsley, 1988

Endsley SA Model



Situation Awareness





PERCEPTION

- *Log Collection*
- *Threat Intel Feeds*
- *SOC Incident Feeds*
- *Security Posture Dashboard*

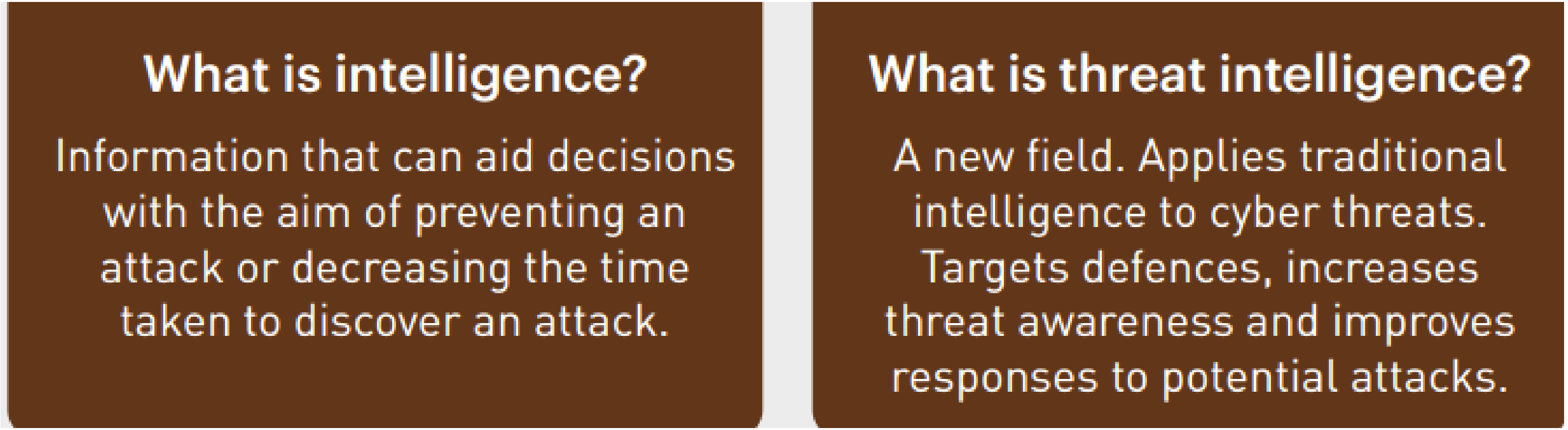
COMPREHENSION

- *Event Correlation and Analysis*
- *Threat Intelligence Analysis*

PROJETION

- *Pattern Matching*
- *Threat Forecast*

What Is Threat Intelligence (TI)?



What is intelligence?

Information that can aid decisions with the aim of preventing an attack or decreasing the time taken to discover an attack.

What is threat intelligence?

A new field. Applies traditional intelligence to cyber threats. Targets defences, increases threat awareness and improves responses to potential attacks.

Centre for the Protection of National Infrastructure cpni.gov.uk

What is Threat Intelligence?

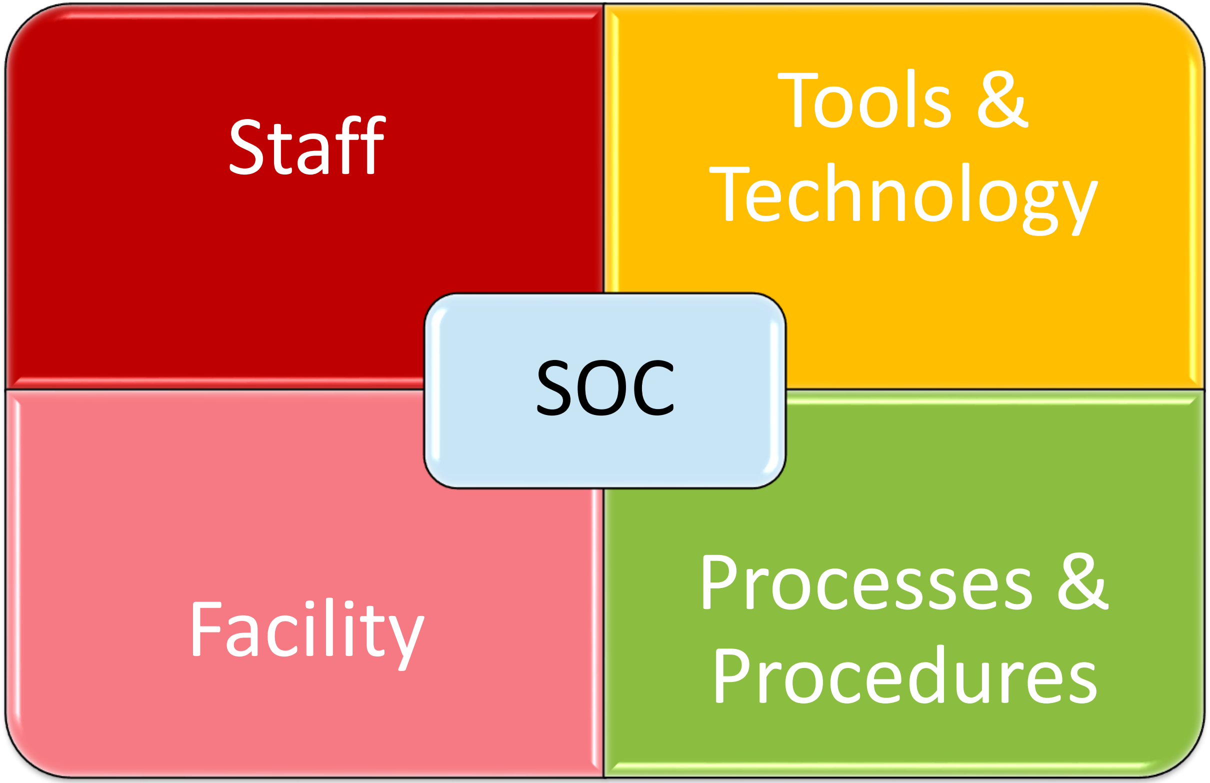
- Specific
- Meaningful
- Actionable
- Relevant
- Timely

Threat Intelligence Sharing

- Internal – SOCs, NOCs, Sysadmins, CIRTs
- External – Trusted partners, Law Enforcements, Vendors
- Standards – IODEF, YARA, OpenIOC, IF-MAP, STIX, TAXII, VERIS, CyBOX, TLP, OTX, CIF etc.

City of Los Angeles
Integrated Security Operations Center

Security Operations Center (SOC)



Staff

Tools & Technology

SOC

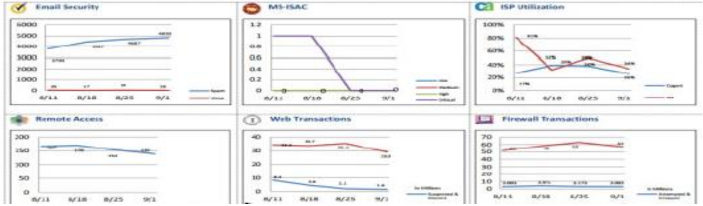
Facility

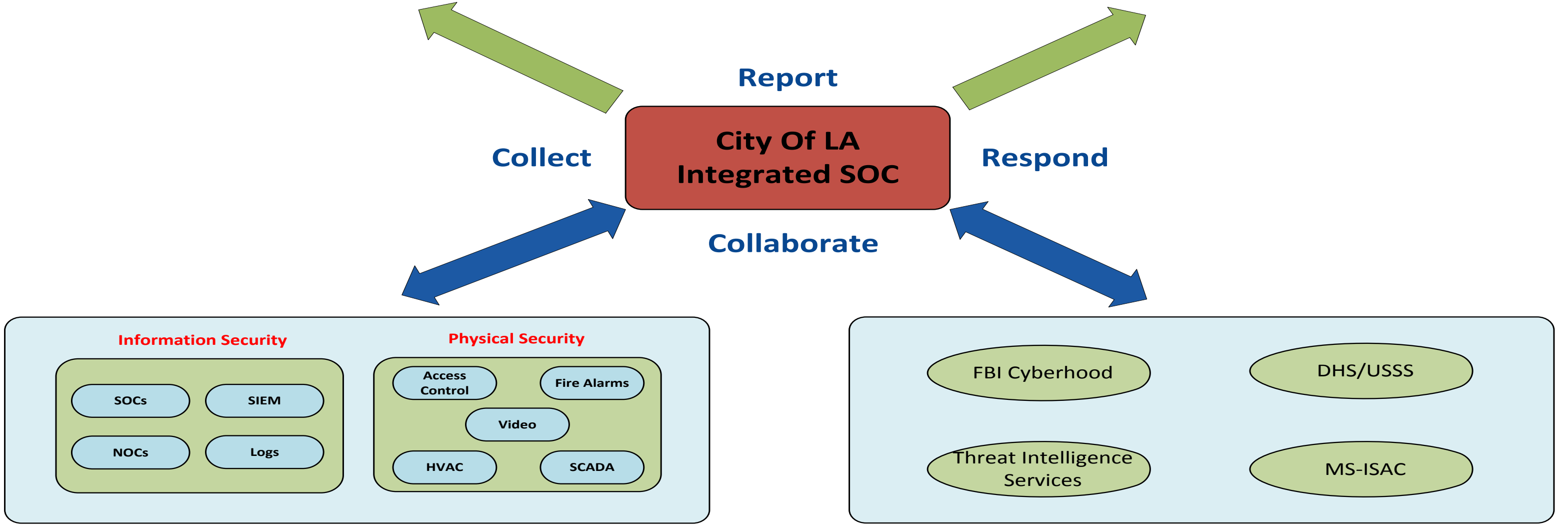
Processes & Procedures

Integrated Security Operations Center (ISOC)

Situational Awareness

Threat Intelligence





Report

Collect

City Of LA
Integrated SOC

Respond

Collaborate

Information Security

SOCs

SIEM

NOCs

Logs

Physical Security

Access Control

Fire Alarms

Video

HVAC

SCADA

FBI Cyberhood

DHS/USSS

Threat Intelligence Services

MS-ISAC

Internal

External

ISOC Components

- ISOC SITUATION AWARENESS
  - ➢ Operational Framework
  - ➢ SOC Integration
  - ➢ ISOC Access Control
  - ➢ Security Posture Dashboard
  - ➢ Threat Level Indicator
  - ➢ ISOC On-boarding Requirements

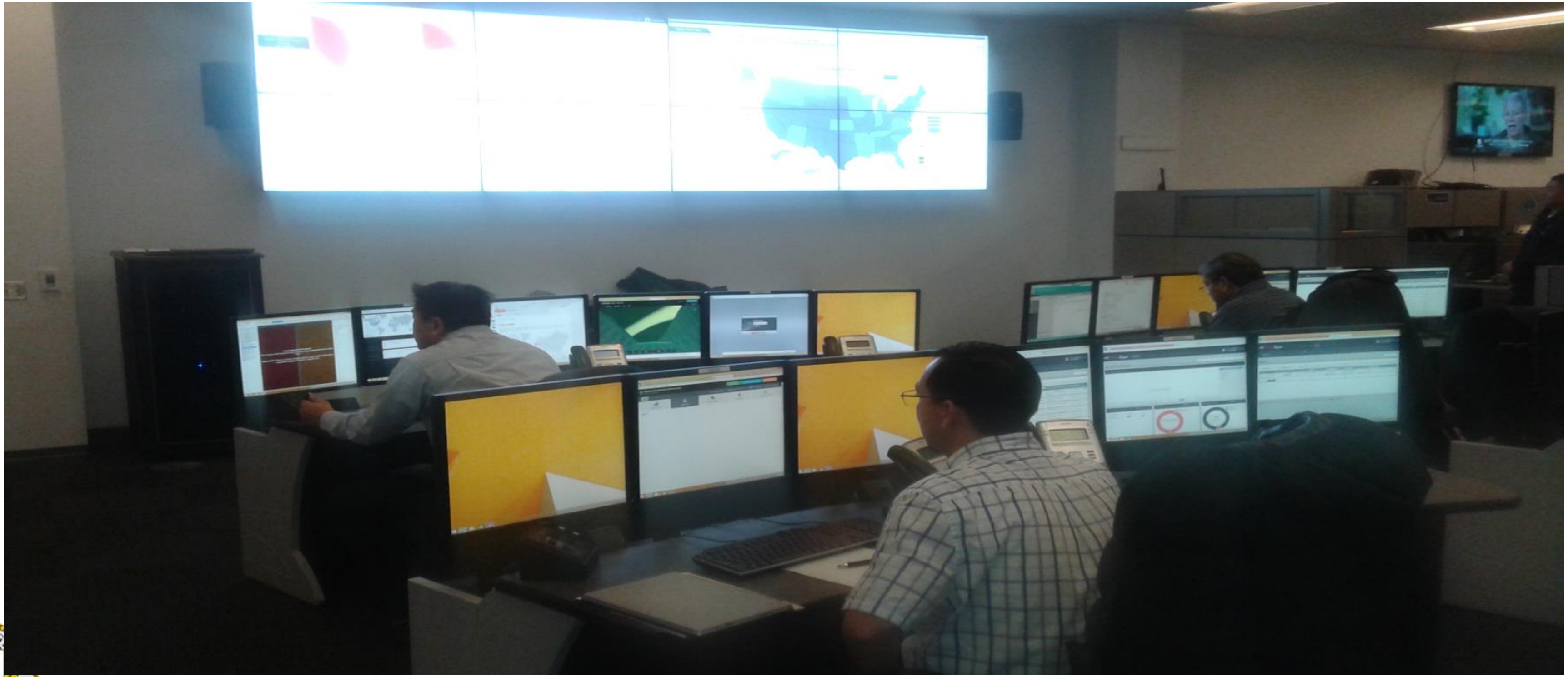
ISOC Components

- Threat Intelligence Portal (TIP)
  - Data Collection (Structured, Unstructured)
  - Data Sharing and Dissemination (Internal, External)
  - Data Integration
  - Classification
  - Alert Correlation
  - Access Control
  - Threat Map / Dashboard

ISOC Components

- Facility Design and Build
  - Display Wall
  - Display Wall Controller
  - Consoles
  - ISOC Dashboard Profiles

City of Los Angeles
Integrated Security Operations Center



Awards

- ***CENTER FOR DIGITAL GOVERNMENT'S 2015 CYBERSECURITY LEADERSHIP AND INNOVATION AWARD***
- ***PUBLIC TECHNOLOGY INSTITUTE 2016 TECHNOLOGY SOLUTIONS AWARD***

References

- Security Operation Center Concepts & Implementation – Renaud Bidou
- Building An Intelligence Driven Security Operations Center – RSA Technical Brief, June 2014
- Toward a Theory of Situation Awareness in Dynamic Systems – Mica R. Endsley, 1995
- Technology Overview for Threat Intelligence Platforms – Craig Lawson, Rob McMillan, December 2014

TIMOTHY LEE

Chief Information Security Officer

City of Los Angeles

timothy.lee@lacity.org