RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: STR-T06

Future-Proof Cybersecurity Strategy

Timothy Lee

Chief Information Security Officer
City of Los Angeles
@tswleej316

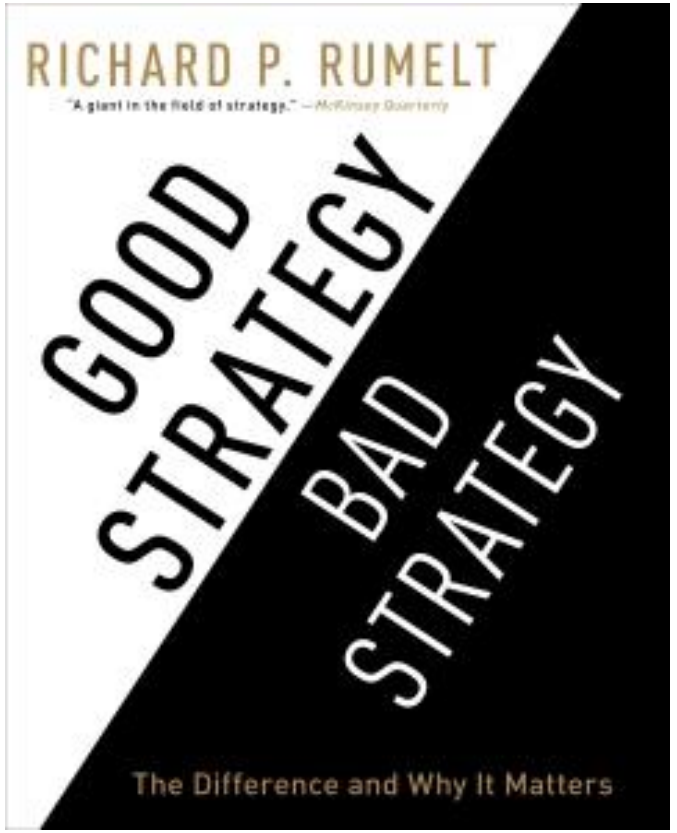
"Strategy without tactics is the slowest route to victory.

Tactics without Strategy is the noise before defeat."

Sun Tzu

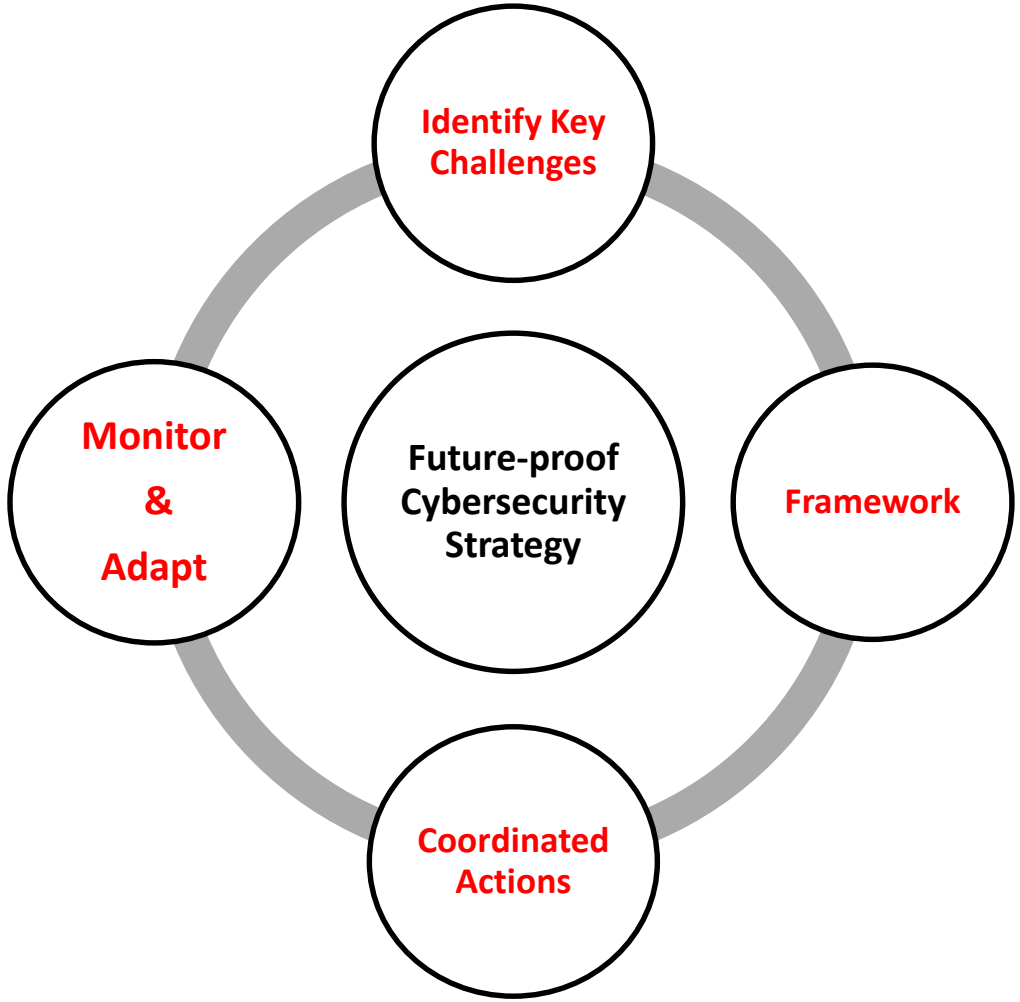
What is Good Strategy?

- **Diagnosis:** defines key challenges to overcome
- **Guiding Policy:** the overall approach
- **Coherent Actions:** Set of coherent actions or coordinated steps



What is good (future-proof) cybersecurity strategy?

- ***Identify key challenges***
- ***A framework or roadmap – the big picture***
- ***Coordinated actions to address challenges***
- ***Continuous monitoring and adaptation***



AGENDA

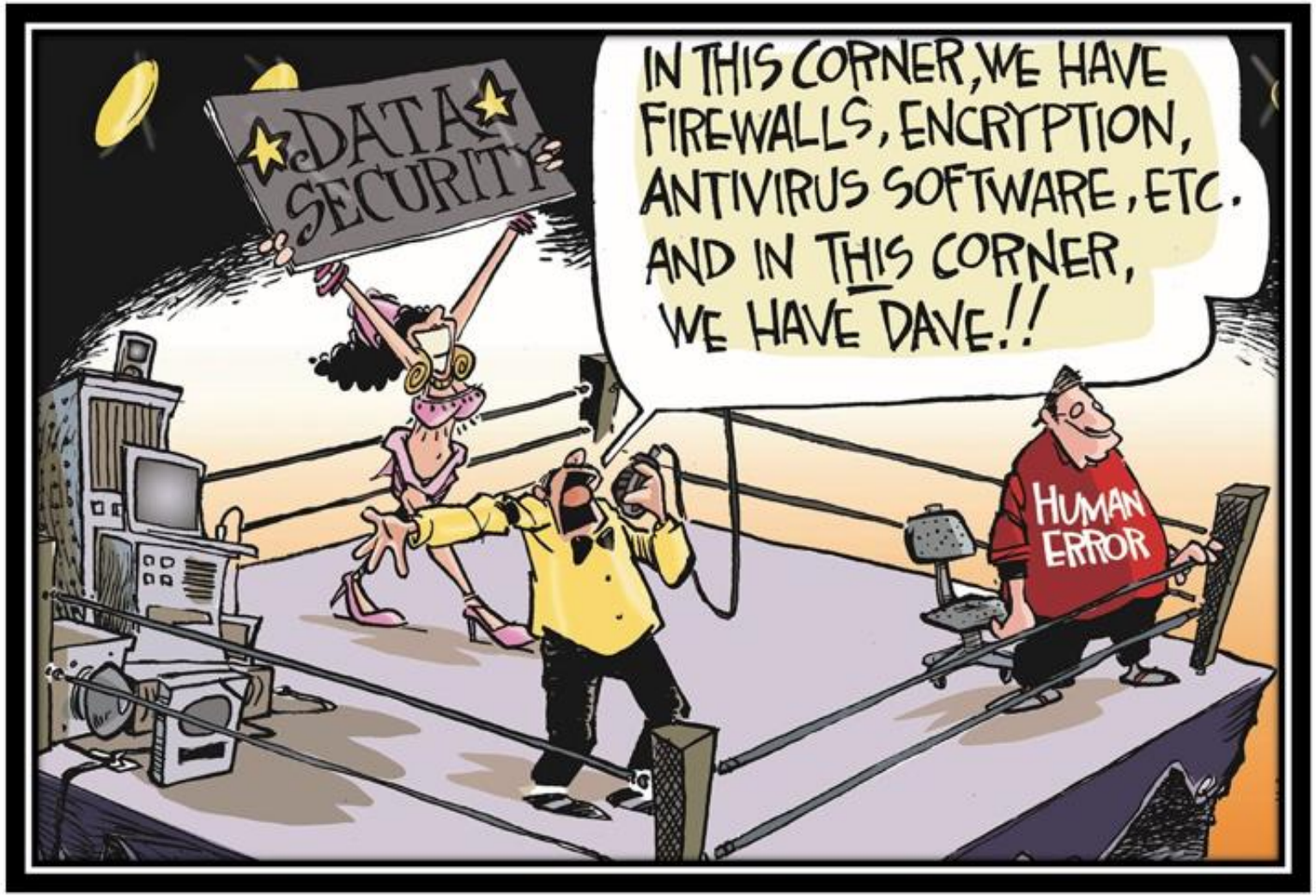
- 5 Key Cybersecurity Challenges
- A framework or roadmap
- 3 must-haves to future-proof cyber strategy

RSAConference2019

5 Key Cybersecurity Challenges

#1 Humans are (still) the weakest link in Cybersecurity

“Companies spend millions of dollars on firewalls, encryption, and secure access devices …… none of these measures address the weakest link in the security chain: the **people**..” ***Kevin Mitnick***



#2 – The Evolving Threat Landscape

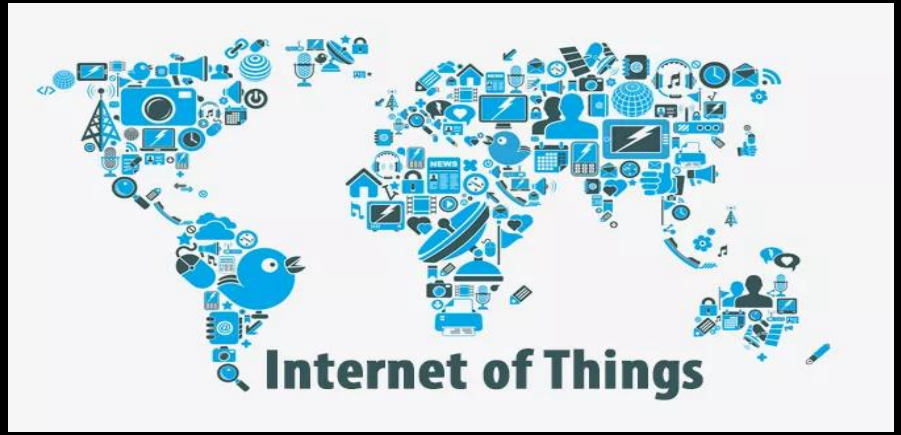
Unpredictable

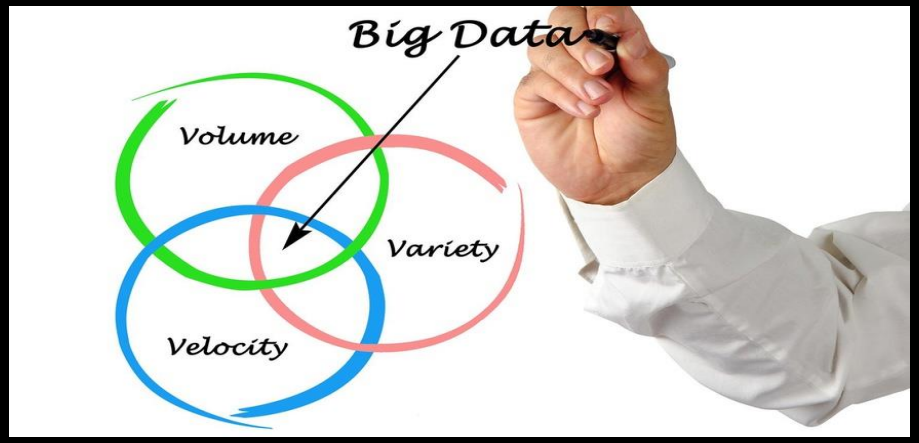
Organized

Connected

Persistent

#3 – Expansion of Attack Surface





#4 – Big Data (3V)

#5 - Business vs Cybersecurity Needs

Challenge Categories

1 Humans

2 Machines (Things)

3 Data

RSAConference2019

Framework – the big picture

CITY OF LOS ANGELES

CYBERSECURITY STRATEGY IMPLEMENTATION ROADMAP

Confidentiality | **Integrity** | **Availability** | **Privacy & Safety**

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Perimeter Security	Integrated Security Operations Center (ISOC)	Integrated Security Operations Center (ISOC)	Department Emergency Plan
Critical Asset Inventory	Policy, Standard and Guideline	Security Information and Event Management (SIEM)	Cyber Incident Response Plan	Continuity Of Operations Plan (COOP)
Security and Compliance Audit	Critical Asset Protection	APT Defense	Critical Incident Response Team	EOC Functional Exercise
Vulnerability and Risk Assetment	Data Loss Prevantion	Threat Intelligence Analysis and Sharing	Red Team / Blue Team Exercise	Tabletop Exercise
High Value Targets	Access Control	Endpoint Detection and Response	Security Automation and Ochestration	
	Vulnerability Management			
	Security Awareness and Training Program			
	Cybersecurity Collaboration			

Use for

- ✓ **Gap assessment**
- ✓ **Resource planning**
- ✓ **Implementation roadmap**
- ✓ **Strategy communication**

RSAConference2019

3 must-haves to future-proof cybersecurity strategy

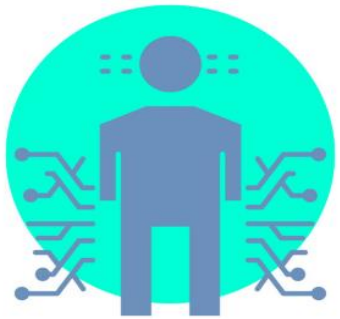
#1 Secure the Human

Roles of humans in cybersecurity

User

Defender

Attacker



Info provider (sensor)

Human Error & Misbehavior
Insider Threat

Unintentional

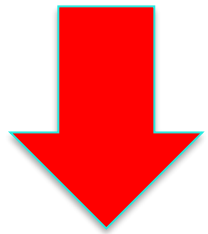
Ignorance
Negligence
Lack of awareness and knowledge

Intentional

Sabotage
Theft of IP
Espionage
Insider Fraud

Reduce risk by managing human factors

RISK = Threat x
Vulnerability x
Consequence



I. Identify High-Value Targets

- Risk = Threat x Vulnerability x **Consequence**

- Executives / Executive assistants
- Accounting / Finance / HR
- Public safety / Elected Officials
- System Admins / DBA / Privileged users
- IT network and security team

II. Targeted and Persistent Security Awareness Program

- Risk = Threat x **Vulnerability** x **Consequence**

  - Risk priorities / topics / target groups matrix

Human Risks/Topics	Probability (Per SOC)	Probability (Per HelpDesk)	Impact	Risk Score	**Target Groups** [Employees, Executives, IT Professionals, Security Professionals, ALL]
Dangerous Attachments	5	5	5	25	Employees, Executives, IT Professionals
Dangerous Links	5	5	5	25	Employees, Executives, IT Professionals
Fraudulent URLs	5	5	5	25	Employees, Executives, IT Professionals
Passwords	5	5	5	25	Employees, Executives, IT Professionals
Password Policy Compliance	5	5	5	25	Employees, Executives, IT Professionals
PCI-DSS	5	4	5	22.5	Office of Finance / Dept Accounting
PII	4	4	5	20	HR / City Clark / LACERS / LAFPP
Executive Security	4	4	5	20	Executives / Admin team
Spear Phishing	4	3	5	17.5	Employees
Security Beyond the Office	4	4	4	16	Employees
Social Engineering	4	4	4	16	Employees

Delivering methods

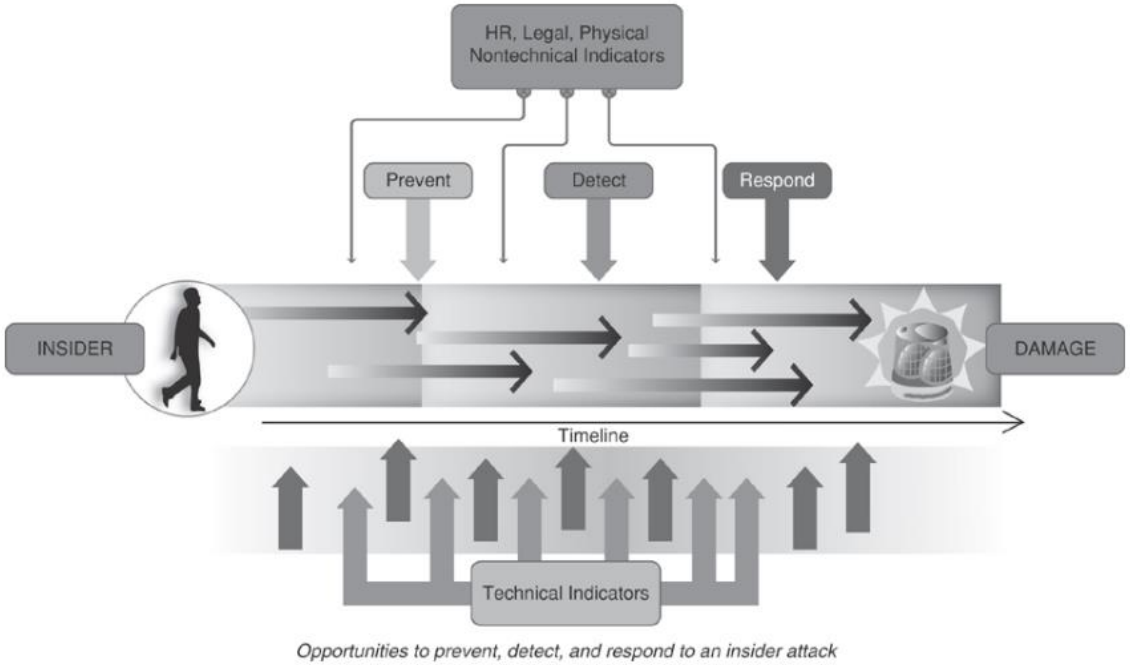
Newsletters, posters, Security events, CBT, workshops, instructor-led training, phishing simulation, bug bounty program

III. Implement tools and processes to prevent and detect insider threats

- Risk = **Threat** x **Vulnerability** x **Consequence**

Layered approach defense

- Email security, web security, perimeter security, sandboxing
- Security Awareness and training, Policy and standards
- EDR, UBA, SIEM, DLP, CASB



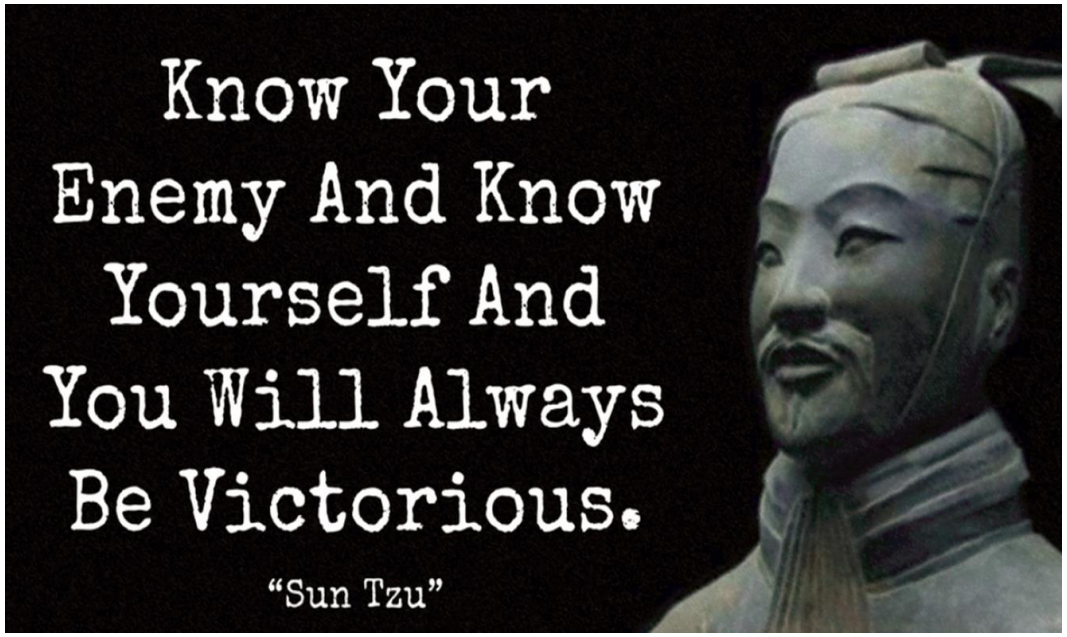
Opportunities to prevent, detect, and respond to an insider attack

The CERT Insider Threat Center

#2 Situational Awareness & Intelligence-Driven Defense

The Art Of

War

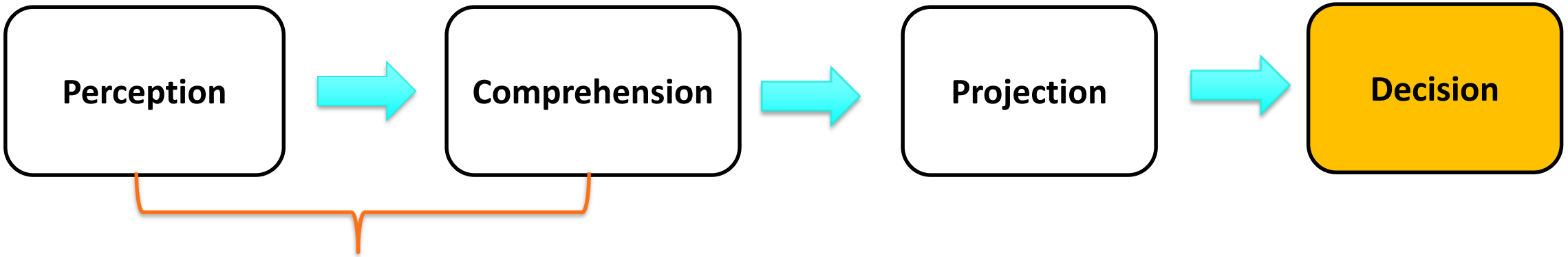


Cybersecurity

Situational Awareness
&
Threat Intelligence

Cyber Situation Awareness Process (Know Yourself)

Mica Endsley SA Model



1. What happened?
2. What's the impact?
3. How did it happen?

4. What could happen next?

5. What should I do?

Cyber SA

5 Enemies of Cyber Situational Awareness

- Attentional Tunneling (lock in on certain data sources, tools and dashboards)
- Data overload (excessive alert noise)
- Errant Mental Models (incorrectly interprets or ignore relevant alarms)
- Misplaced Salience (ineffective data visualization)
- Out-of-the-loop Syndrome (rely heavily on process and response automation)

Recommendations

- Use S.M.A.R.T dashboards (*Simple, Meaningful, Accurate, Relevant and Timely)*
- Use workflows to simplify detect/respond process
- Develop your SOC team on problem-solving skills, not just technical expertise
- Promote team collaboration
- Conduct Simulation Exercise regularly

Example 1: Executive Dashboard

Search | Datasets | Reports | Alerts | Dashboards

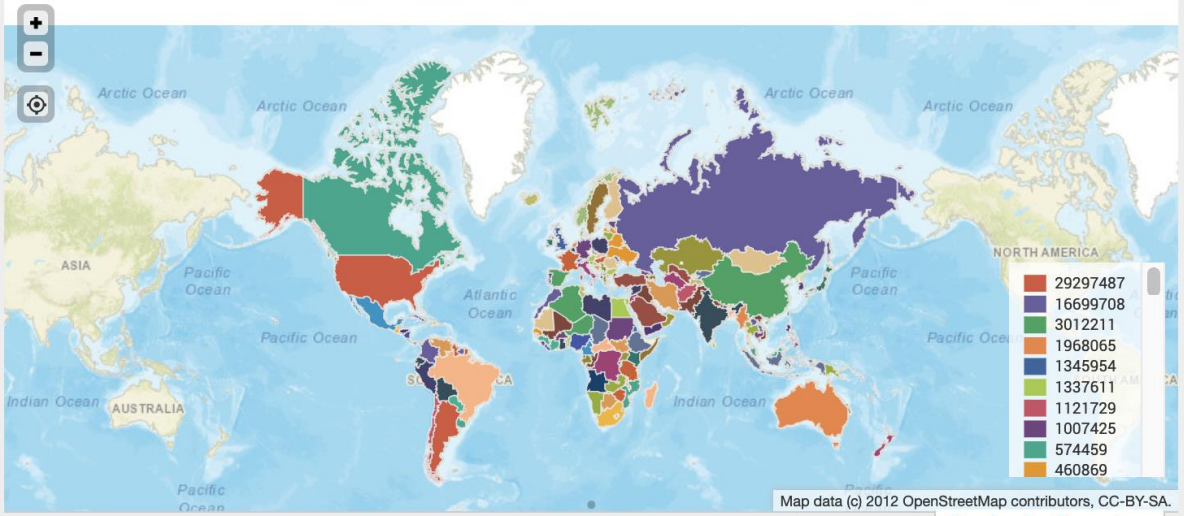
Executive Dashboard

Limited drill down navigation

Edit

Attacker by Country (7 Days)

Data Source: FW, IPS



Top 15 Attacking Countries (7 Days)

Data Source: FW, IPS

Country
United States
Russia
China
Netherlands
United Kingdom
Bulgaria
Seychelles
Germany
Canada
Ukraine
Japan
Brazil
Italy
Thailand
Hong Kong

Total Firewall Blocked (past 24 hours)

Data Source: FW, IPS

12,568,204

Total Firewall Events (past 24 hours)

Data Source: FW, IPS

index	count
firewall	41166312
main	11086890

Total SIEM Events (past 24 hours)

All Data Sources

613,579,443

Total Event Count

Firewall Traffic Analysis (1h)

OPSEC & Fortigate

75,000

Threat Activity Details (1h)

Data From ES

_time	src	threat_match_value	sourcetype	threat_key

CISO Daily - Trend

24h vs. 48h

Edit Export ...

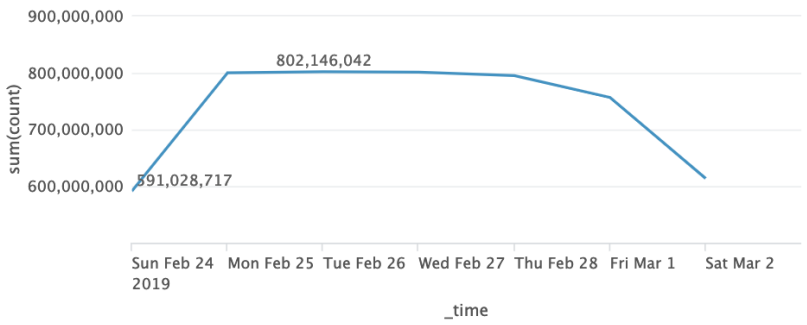
Total Events Ingested by SIEM

Midnight to Midnight

613,579,443 -142,909,092

Total Events Ingested by SIEM

Last 7 days



Critical SEP Alerts

Past 24h

CIDS_Signature_String	count
Web Attack: IIS Server CVE-2017-7269	3
Web Attack: Masscan Scanner Request	3
Attack: Apache Struts CVE-2017-5638	1
Web Attack: Malicious OGNL Expression Upload	1
Web Attack: Malicious Script Redirection 15	1

Targeted Campaign Monitoring

24h - Lookup: Threat_Threats

No results found.

CAP Asset Threats (ES, CB)

24h vs. 48h

0 -3

CAP Assets Reporting

24h vs. 48h

76 0

Example 2: CISO Daily Trend

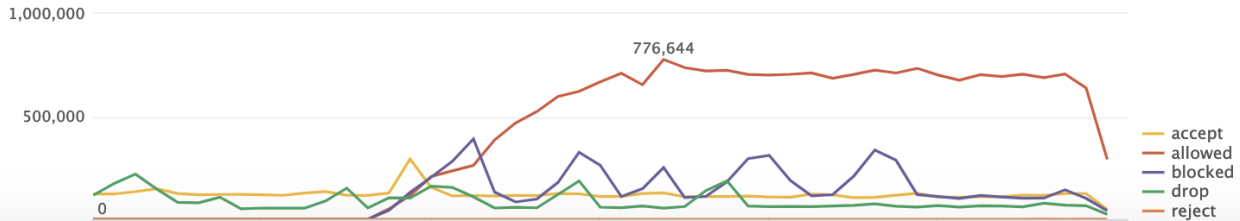
FW Connections Blocked

24h vs. 48h

12,553,723 -1,305,227

FW Connections by Action

past 24h

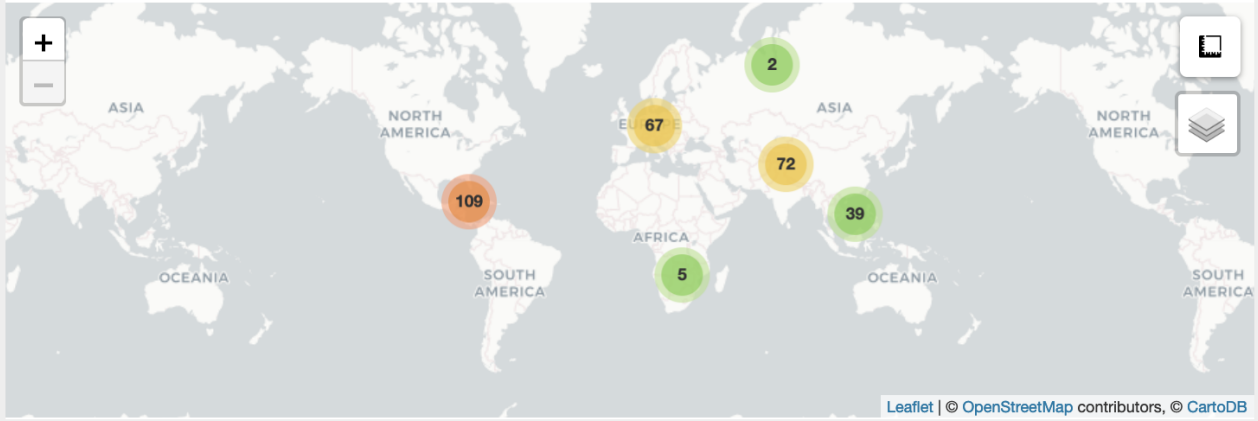


Critical Asset Protection - Security

Edit Export ...

CAP Attackers by Country (24hr)

Data Source: FW, IPS



Top Attacking Countries (24hr)

Data Source: FW, IPS

Country	count
United States	2094
Russia	1382
China	272
United Kingdom	204
Seychelles	166

« prev 1 2 3 next »

Total Hosts Reporting (1hr)

Critical Assets Monitored

74 -2

Total Identified Threats (24hr)

Data Source: ES, FireEye

3

<1m ago

ES Alerts by Dept (24hr)

Data Source: FW, IPS

department	ip_address	it_contact	count
[redacted]		ESS	1
		ESS	1
		ESS	1

FireEye Alerts (24 hr)

FireEye Alerts

No results found.

Example 3: Critical Asset Protection

Total Connections Allowed (past 5d)

Data Source: FW, IPS

12,638 -4,147

Total Intrusions Blocked (past 5d)

Data Source: FW, IPS

2,126 -8,496

Threat Intelligence (Know Your Enemy)

+

+

+

Actor

who are they?

Intent

What are they trying to achieve?

Capability

What is their ability to achieve the intended goals?

Opportunity

How much do they know about my environment and vulnerabilities?

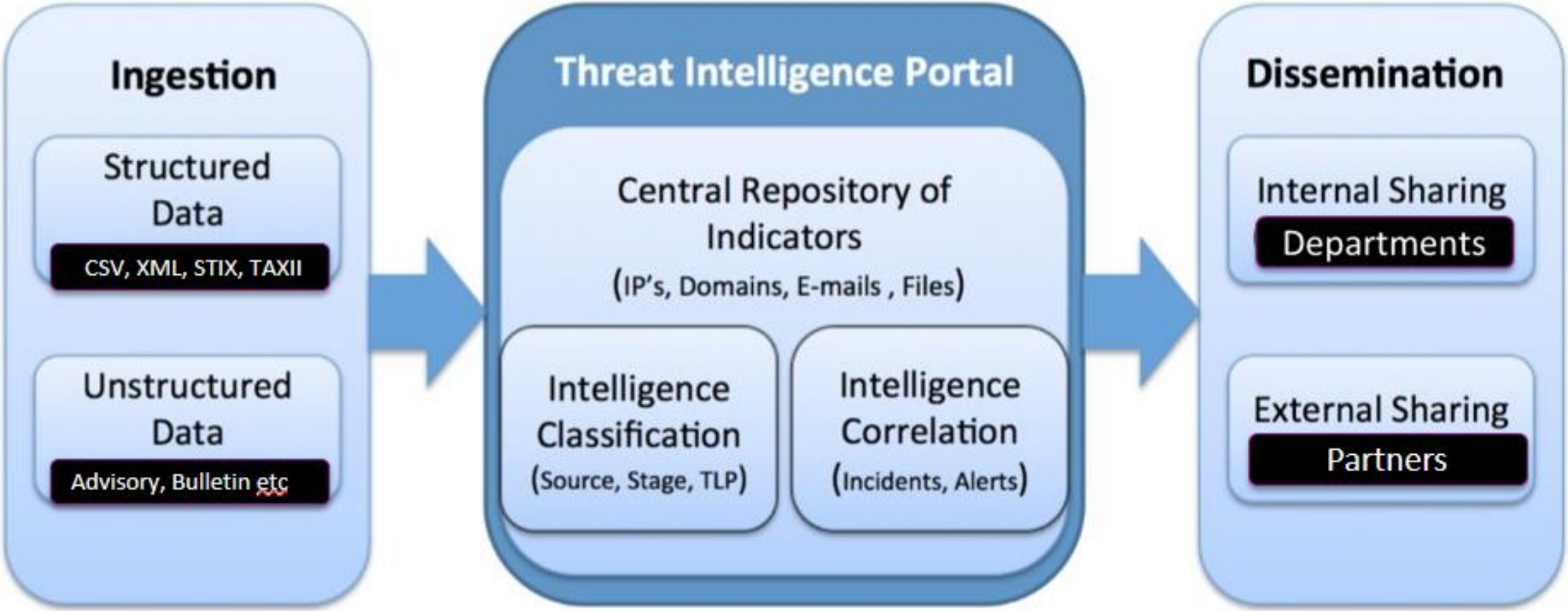
= Threat Intelligence

Cyber Threat Intelligence Types

- Indicators
- Threat Actors and Tactics, Techniques, and Procedures (TTPs)
- Security alerts / Incidents
- Course of action (security advisories, CVEs etc)
- Threat intelligence reports (example: Novetta’s Operation Blockbuster)

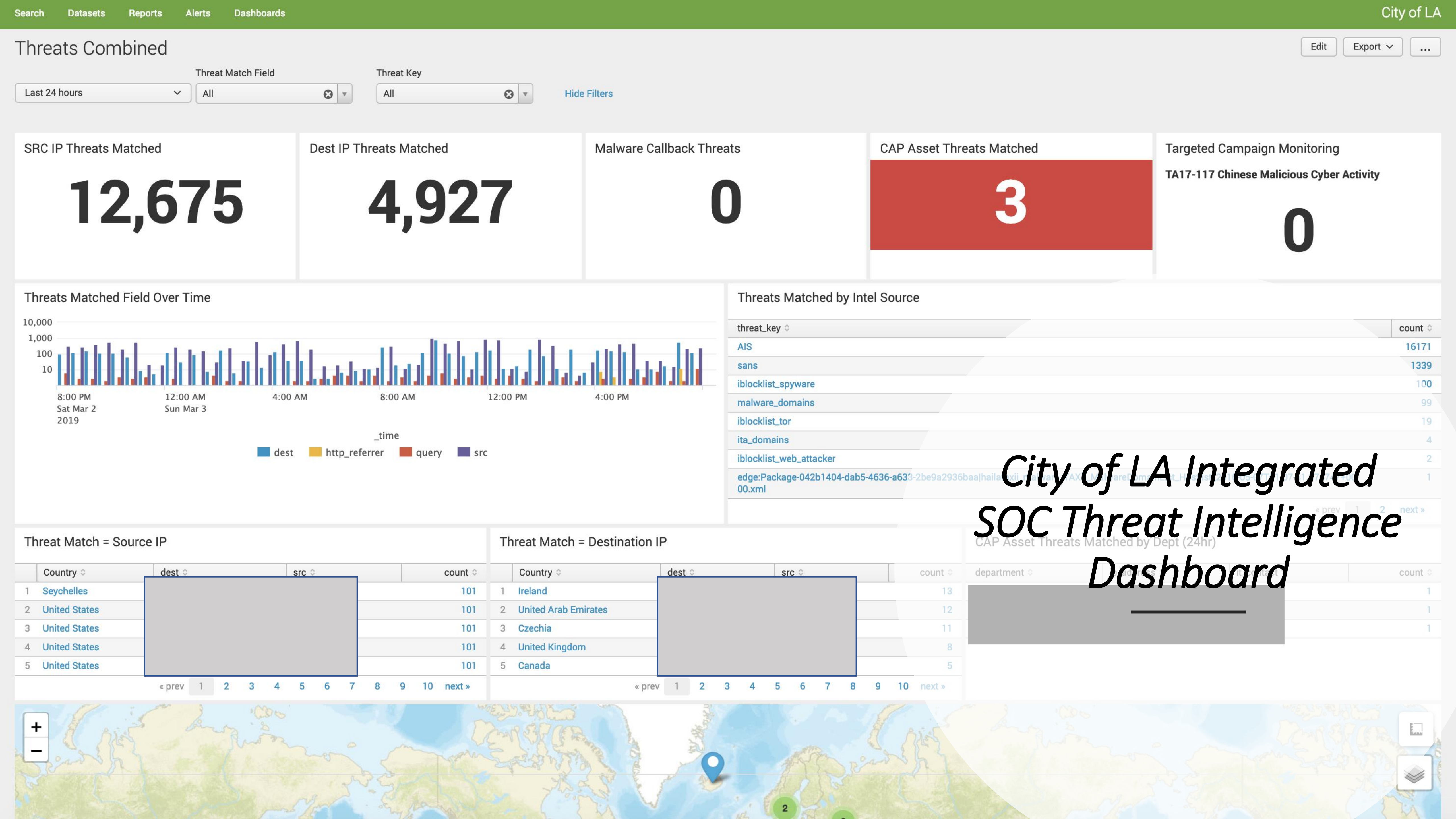
Threat Intelligence Lifecycle

1. Intelligence goals
2. Collection
3. Data enrichment and analysis
4. Utilization (Cyber SA, Detection, Prevention, and Dissemination)



City of LA Integrated SOC Threat Intelligence Platform

City of LA Integrated SOC Threat Intelligence Dashboard



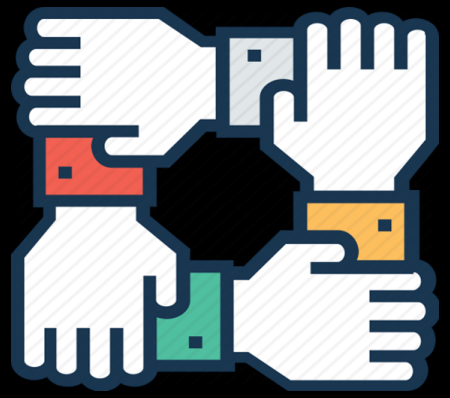
Threat Intelligence Maturity Stages

	1	2	3	4
People	No threat intelligence resources	No dedicated threat intelligence analysts, some distributed resources "wear many hats"	Multiple security teams (IR, VMT, SOC) using threat intelligence	Dedicated threat analyst team
Data Sources	No feeds, relying on Google	Free feeds, brand and leaked credential monitoring	Contextual threat intelligence, paid feeds (e.g., ISAC) and/or paid reports	Combining multiple intelligence providers to produce intelligence
Security Solutions	MSSP	SIEM, Vulnerability Management	Incident Response	Threat Intelligence Platform, Deep Analysis
Workflow	N/A	Reacting to alerts ad hoc	Integrated with SOC tools	Integrated with multiple security tools

The Threat Intelligence Handbook – Chris Pace

#3 Collaboration

Why Collaboration?



Average time to detect a breach **191 days**

Average time from discovery to containment **66 days**

Ponemon Institute 2017

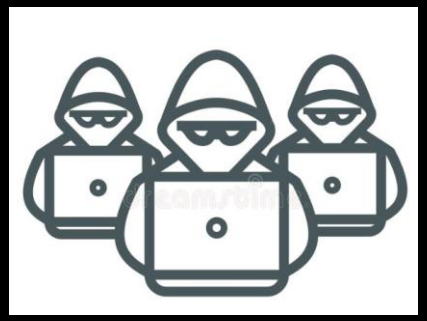
How long does it take to breach a network? **< 15 Hours**

Nuix Report 2018

Bad guys are collaborating

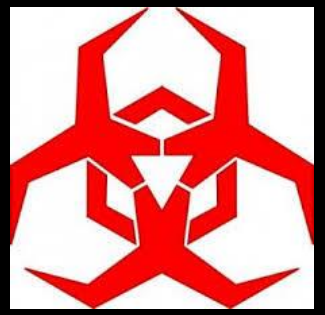
We must do the same

1. Research



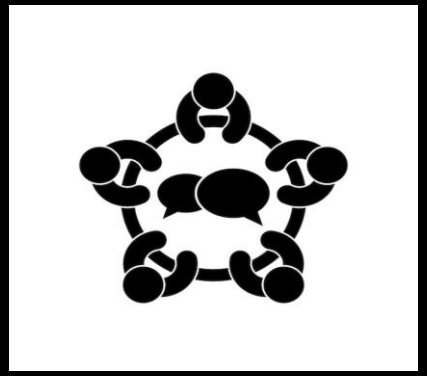
2. Infiltration

3. Execution



4. Command & Control

5. Exfiltration



$$$ Ecosystem

Collaborative Defense against Collaborative Attack

LA CYBER LAB

LA launches CyberLab to share more threat information with region's businesses

The new tech platform and public-private partnership aims to protect critical IT infrastructure and aid businesses to fight cyberattacks in real time.

By *Jason Shueh*

AUGUST 16, 2017 9:23 AM

BIO

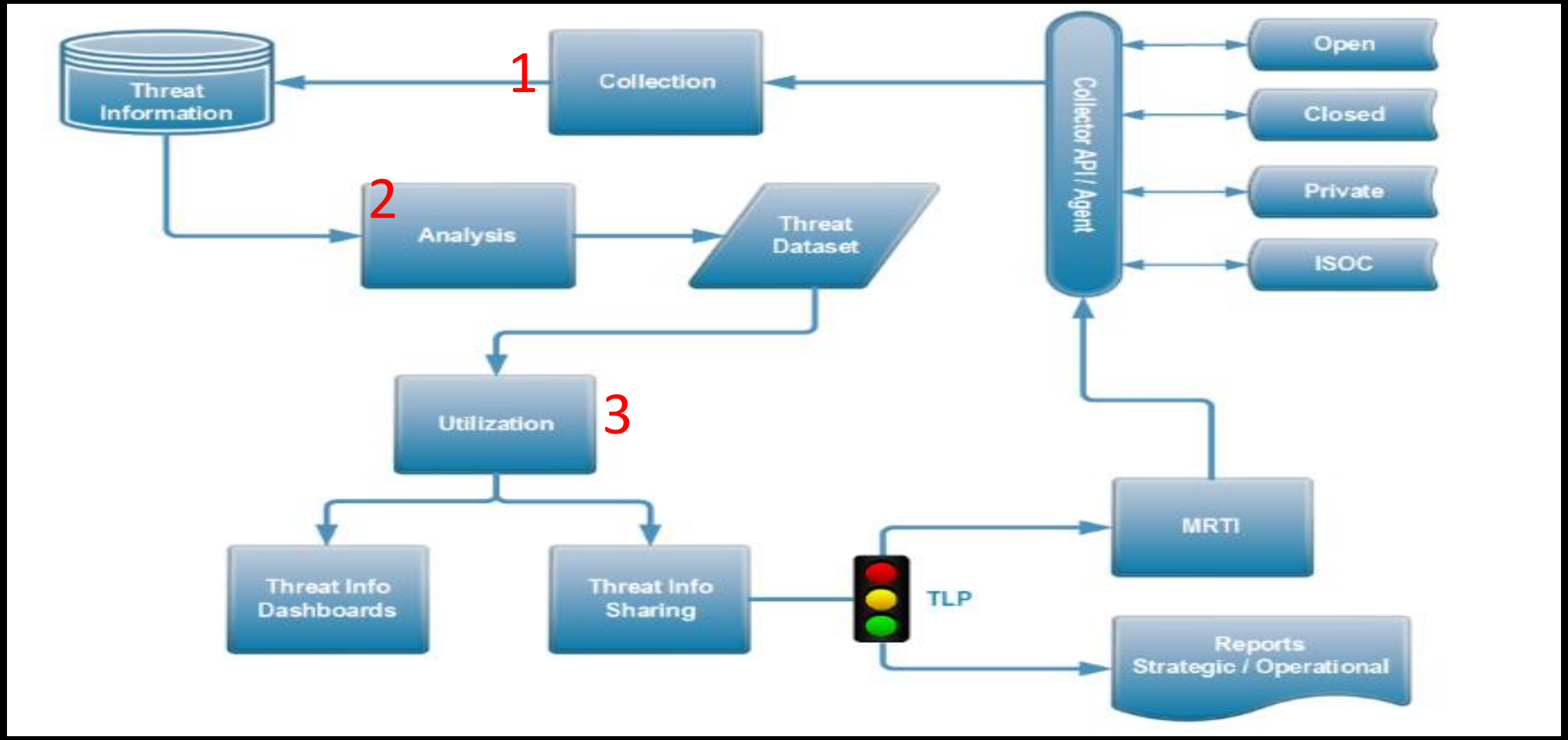
Government

Academia

Business

A Public-Private Partnership Benefits All

Los Angeles Cyber Lab
Threat Intelligence Analysis & Sharing Platform



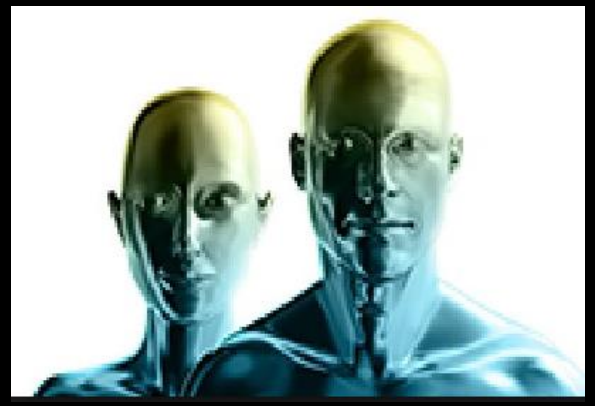
Recommendations

- Identify existing internal sources of CTI
- Develop Intelligence-driven use cases
- Establish information sharing platform, rules and agreements
- Join and participate in information sharing efforts
- Follow the TLP and protect the security of the shared information

IN CASE YOU MISSED IT

3 Must-haves To Future-proof Your Cyber Strategy

#1 Secure the Human



#2 Situational Awareness
& Threat Intelligence

#3 Collaboration

Resources (Secure the Human)

- The CERT Guide to Insider Threats
- NIST 800-50, 800-16
- SANS Security Awareness MGT433
- CHEAT: An updated approach for incorporating human factors in cyber-security assessments - *Amanda Widdowson*

Resources (Cyber SA & Threat Intelligence)

- Theory and Models for Cyber Situation Awareness *(Peng Liu, Sushil Jajodia, Cliff Wang)*
- The Threat Intelligence Handbook *(Chris Pace)*
- Unlocking User-centered Design Methods for building Cyber Security Visualizations *(Sean McKenna, Diane Staheli, Miriah Meyer)*
- Designing for Situation Awareness (*Mica Endsley, Betty Bolte and Debra Jones)*

Resources (Collaboration)

- Collaborative Cyber Threat Intelligence (*Florian Skopik)*
- Collaborative Attack vs Collaborative Defense (*Shouhuai Xu*)
- NIST SP 800-150

RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: STR-T06

Thank you!

Timothy Lee

Chief Information Security Officer
City of Los Angeles
@tswleej316