

RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: STR-T06

Future-Proof Cybersecurity Strategy

Timothy Lee

Chief Information Security Officer
City of Los Angeles
@tswleej316



#RSAC

*"Strategy without tactics is
the slowest route to victory.*

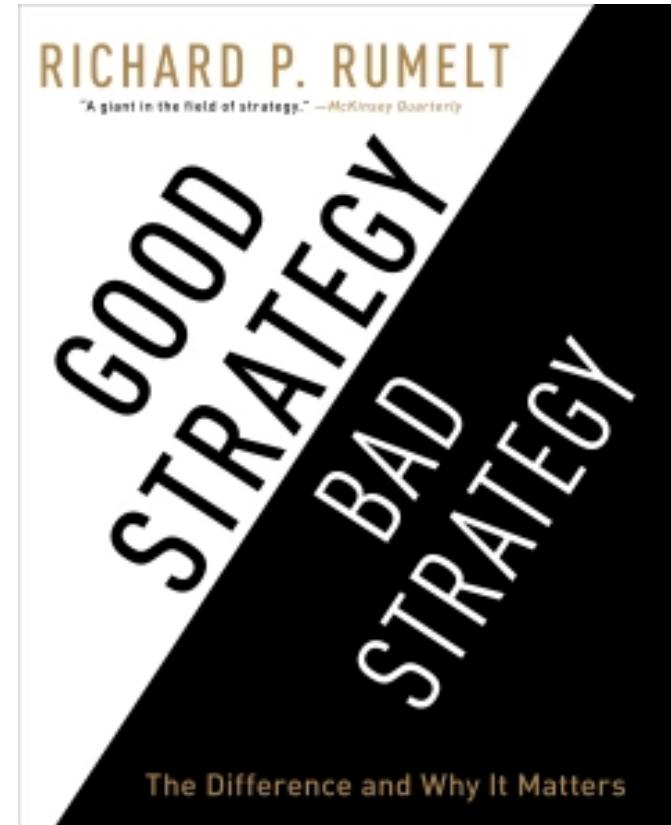
*Tactics without Strategy is
the noise before defeat."*

Sun Tzu



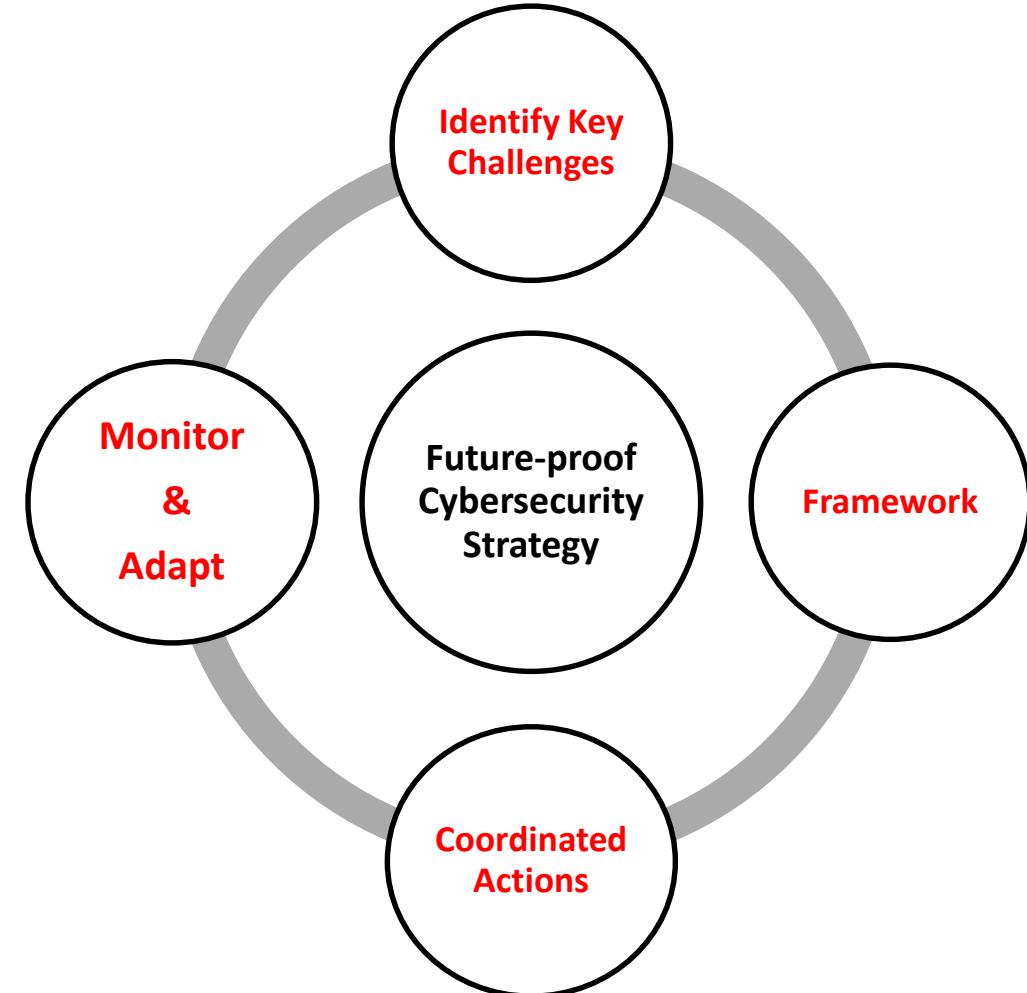
What is Good Strategy?

- **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



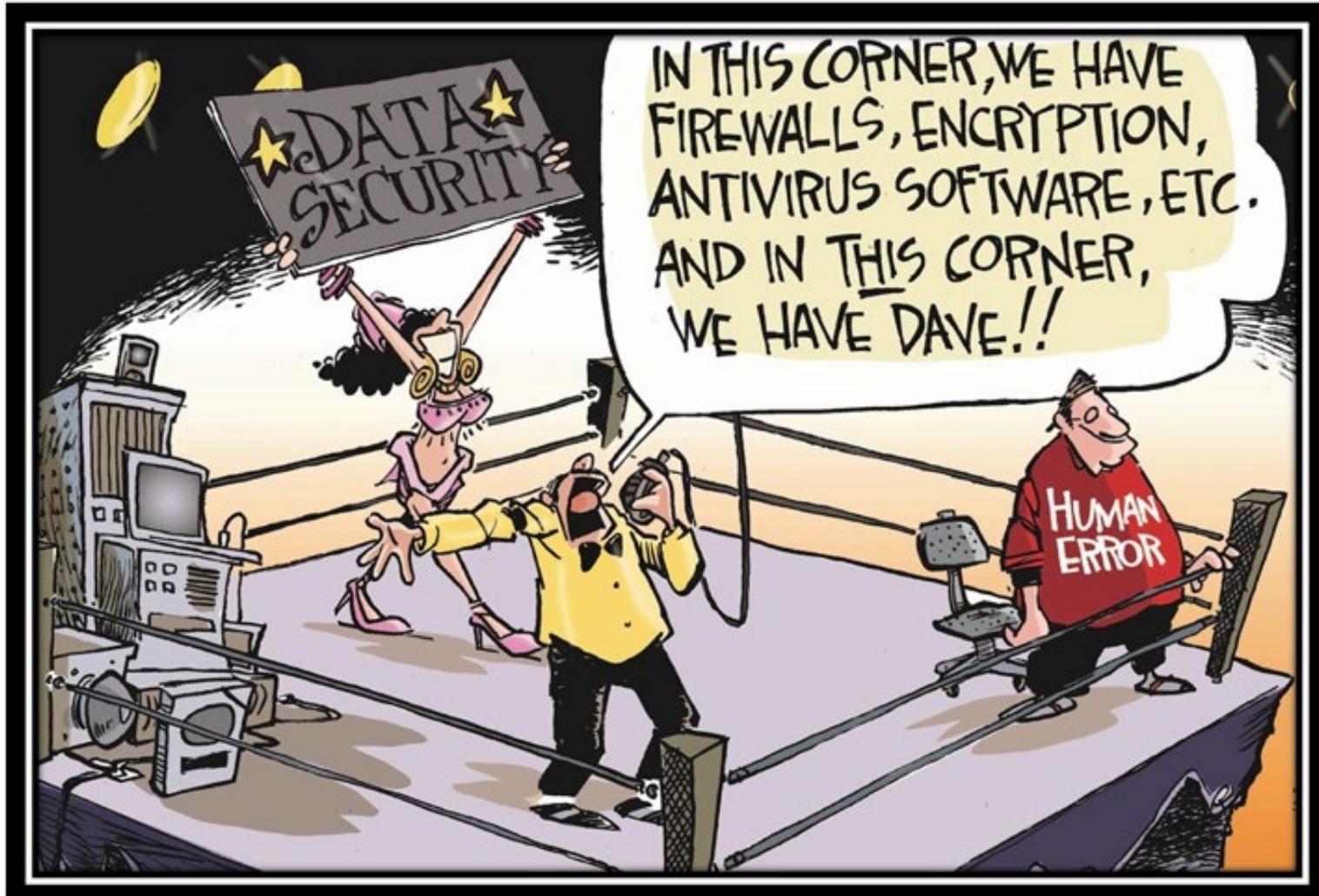
RSA®Conference2019

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

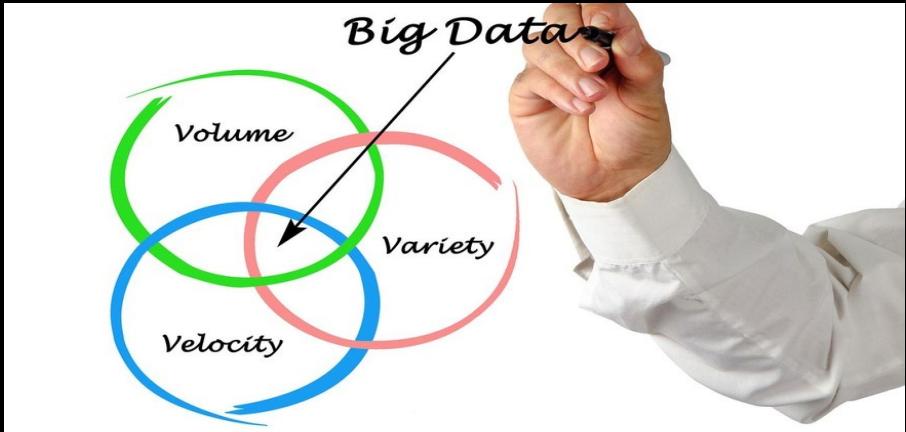
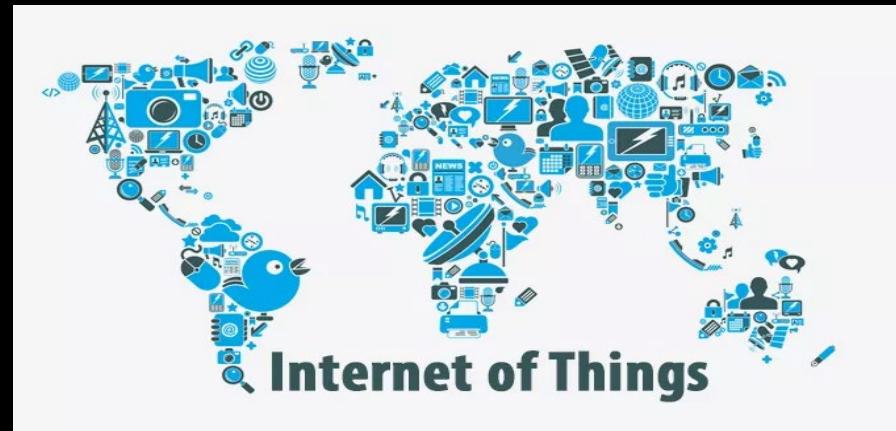


Connected



Persistent

#3 – Expansion of Attack Surface



#4 – Big Data (3V)



#5 - Business vs Cybersecurity Needs

Challenge Categories



1 Humans

2 Machines
(Things)



3 Data

RSA®Conference2019

Framework – the big picture

CITY OF LOS ANGELES

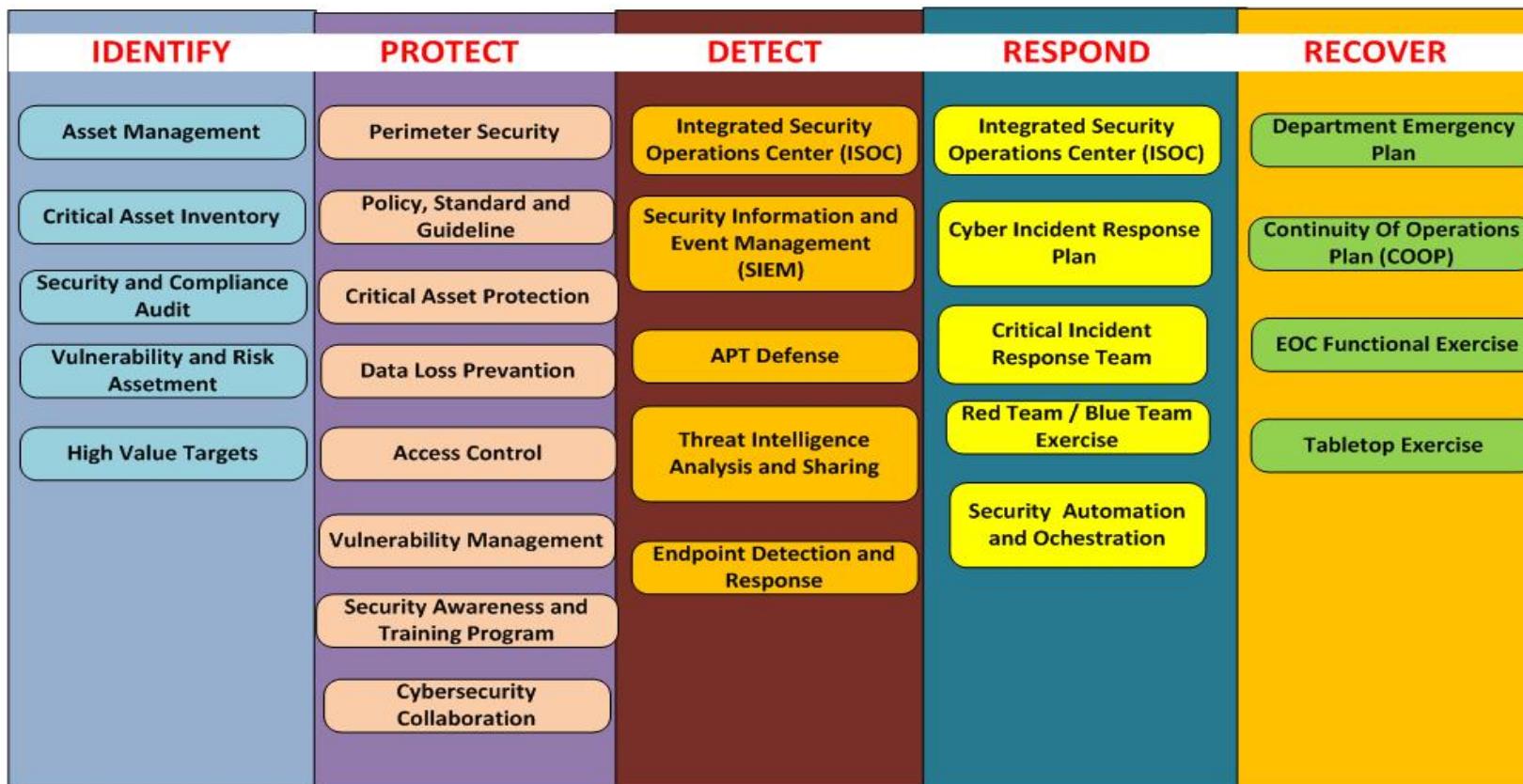
CYBERSECURITY STRATEGY IMPLEMENTATION ROADMAP

Confidentiality

Integrity

Availability

Privacy & Safety



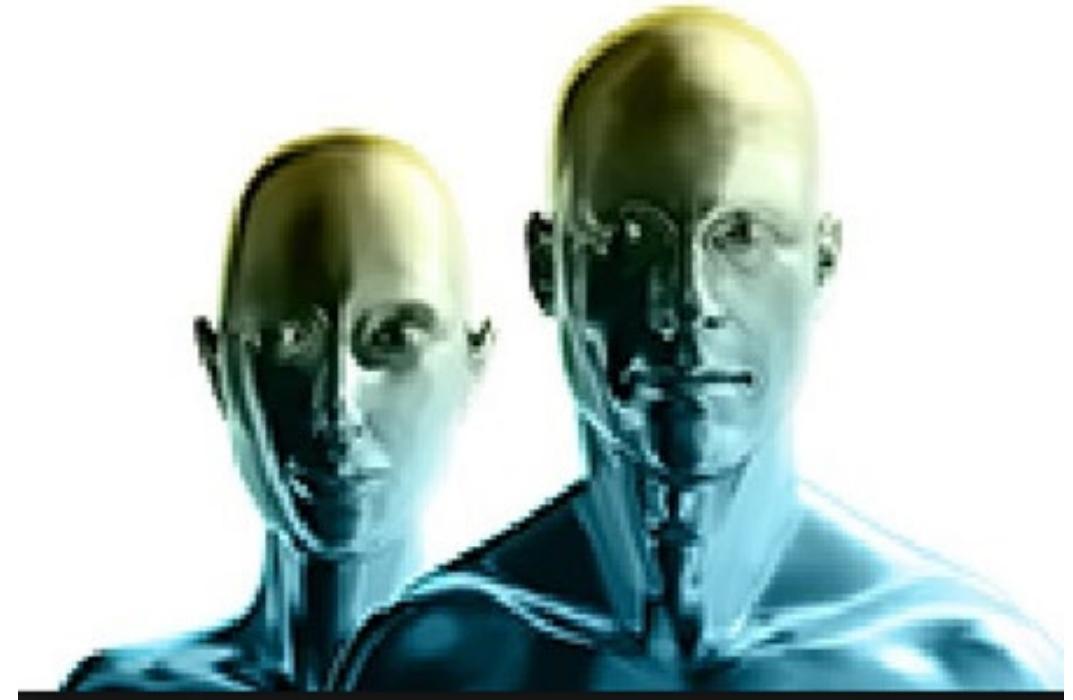
Use for

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

RSA®Conference2019

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

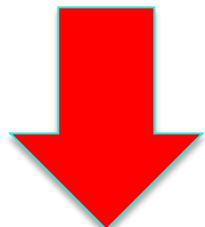
Intentional

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

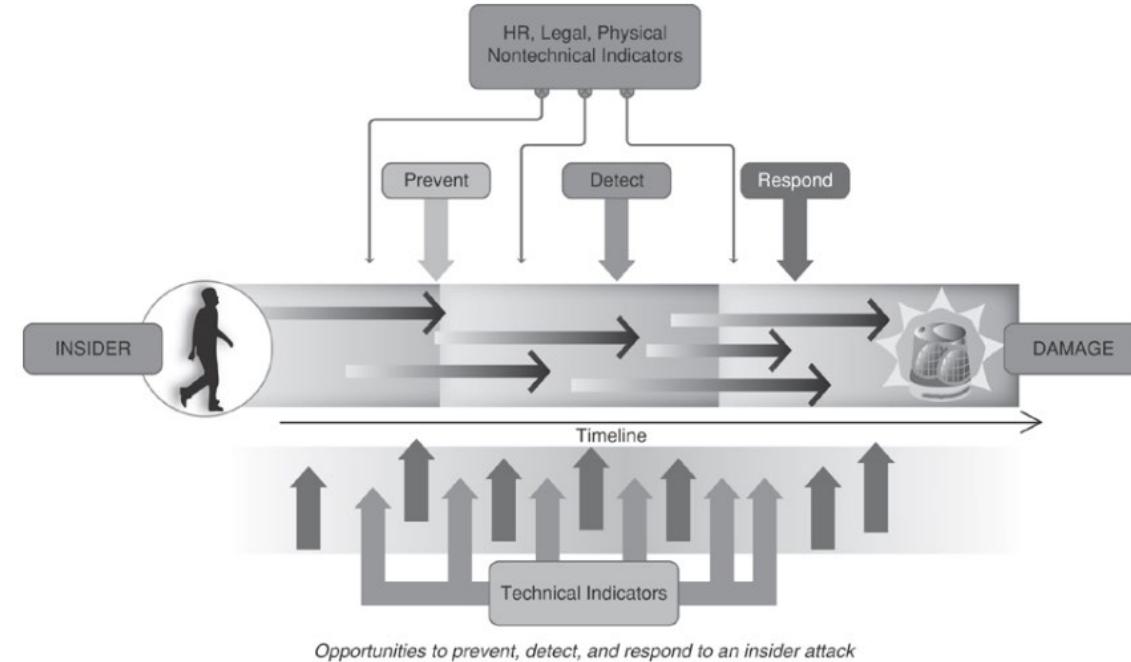


III. Implement tools and processes to prevent and detect insider threats

- 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



The CERT Insider Threat Center



#2 Situational Awareness & Intelligence-Driven Defense



The Art Of

War

Know Your
Enemy And Know
Yourself And
You Will Always
Be Victorious.

“Sun Tzu”



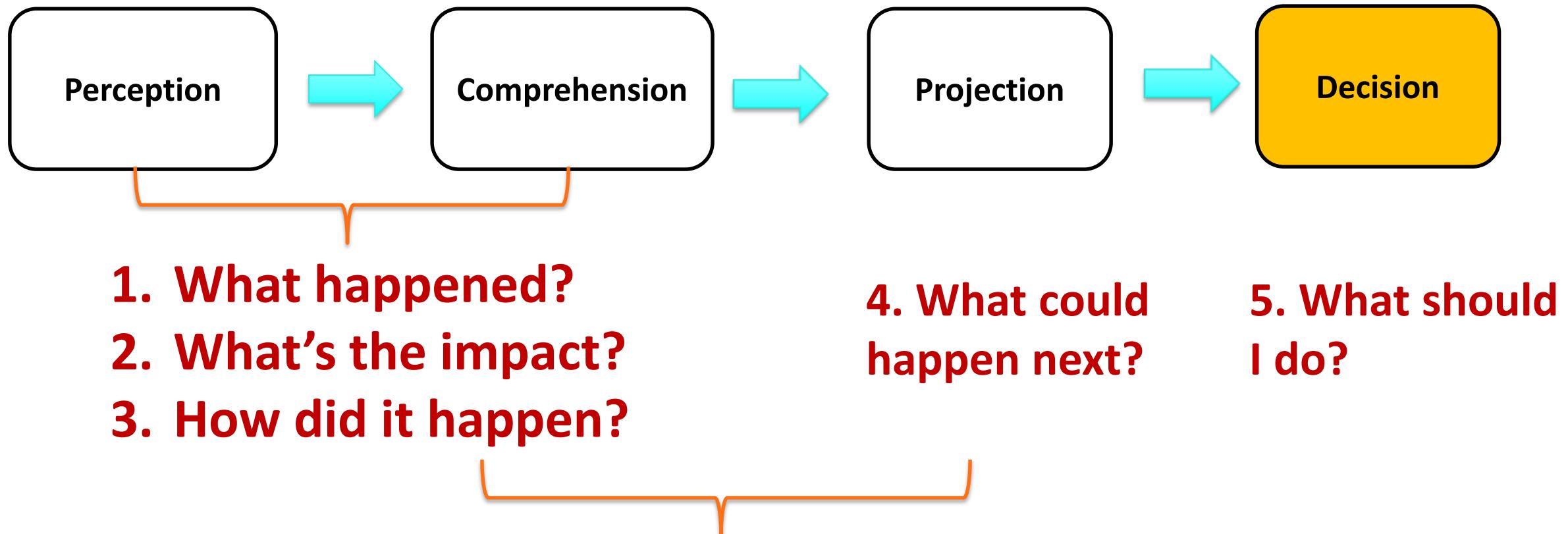
Cybersecurity

Situational Awareness
&
Threat Intelligence



Cyber Situation Awareness Process (Know Yourself)

Mica Endsley SA Model



Cyber SA

RSA Conference 2019

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

Attackers by Country (7 Days)
Data Source: FW, IPS

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

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

Firewall Traffic Analysis (1h)
OPSEC & Fortigate

75,000

Total Firewall Events (past 24 hours)
Data Source: FW, IPS

index	count
firewall	41166312
main	11086890

Threat Activity Details (1h)
Data From ES

_time	src	threat_match_value	sourcetype	threat_key
2012-08-22T12:00:00Z	192.168.1.1	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.2	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.3	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.4	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.5	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.6	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.7	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.8	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.9	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.10	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.11	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.12	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.13	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.14	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.15	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.16	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.17	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.18	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.19	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.20	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.21	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.22	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.23	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.24	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.25	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.26	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.27	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.28	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.29	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.30	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.31	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.32	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.33	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.34	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.35	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.36	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.37	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.38	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.39	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.40	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.41	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.42	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.43	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.44	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.45	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.46	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.47	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.48	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.49	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.50	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.51	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.52	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.53	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.54	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.55	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.56	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.57	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.58	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.59	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.60	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.61	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.62	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.63	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.64	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.65	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.66	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.67	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.68	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.69	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.70	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.71	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.72	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.73	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.74	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.75	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.76	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.77	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.78	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.79	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.80	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.81	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.82	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.83	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.84	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.85	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.86	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.87	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.88	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.89	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.90	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.91	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.92	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.93	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.94	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.95	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.96	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.97	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.98	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.99	malicious	file	malware
2012-08-22T12:00:00Z	192.168.1.100	malicious	file	malware

Total SIEM Events (past 24 hours)
All Data Sources

613,579,443
Total Event Count

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

CAP Asset Threats (ES, CB)

24h vs. 48h

0 -3

CAP Assets Reporting

24h vs. 48h

76 0

No results found.

Example 2: CISO Daily Trend

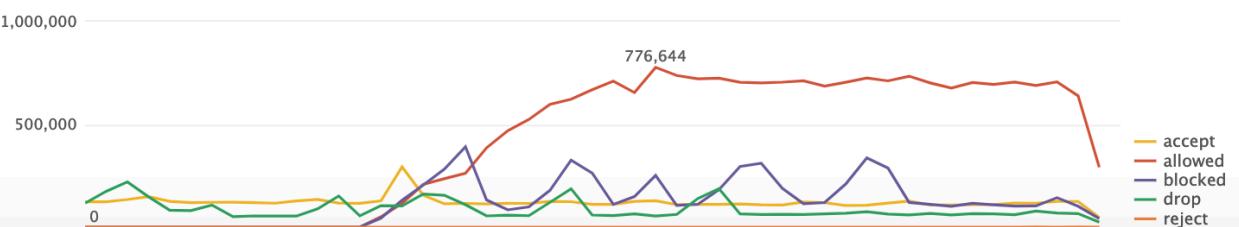
FW Connections Blocked

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
ITA	10.26.4.83	ESS	1
ITA	10.26.4.84	ESS	1
ITA	10.32.86.189	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?

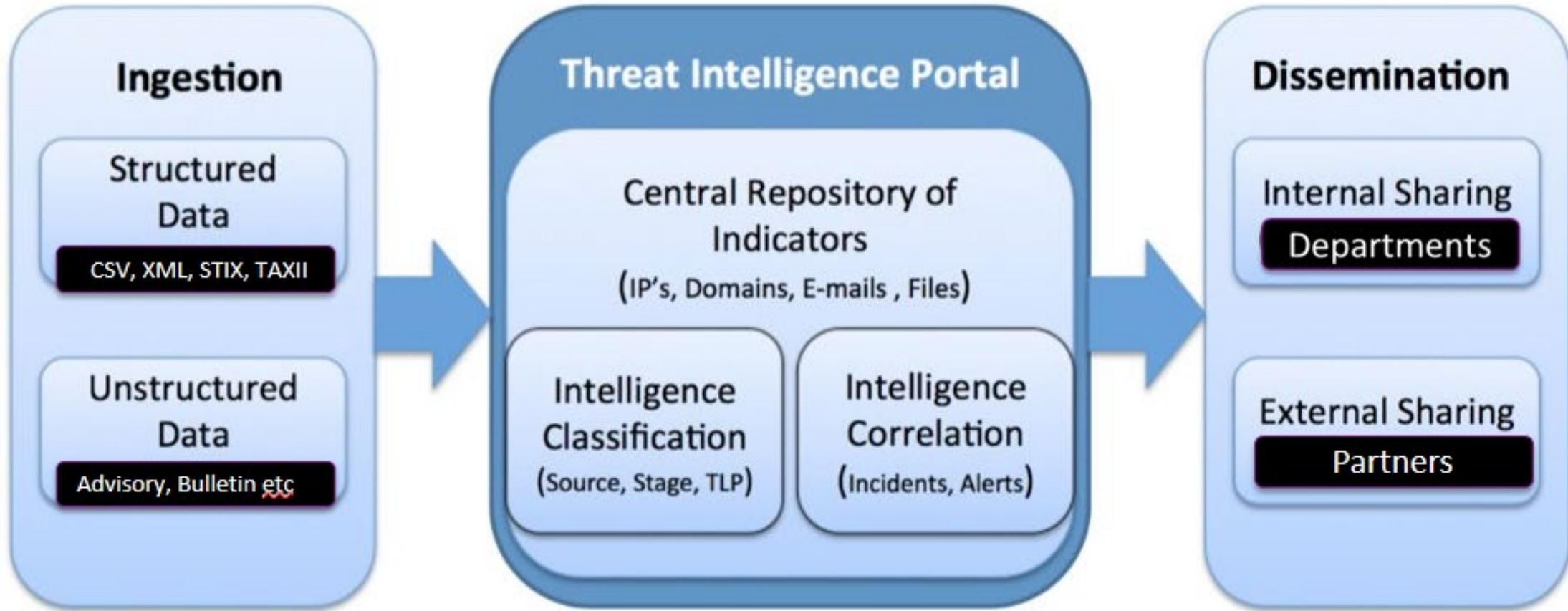
= **Threat Intelligence**

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

Threats Combined

Edit Export ...

Last 24 hours

SRC IP Threats Matched

12,675

Dest IP Threats Matched

4,927

Malware Callback Threat

0

CAP Asset Threats Matched

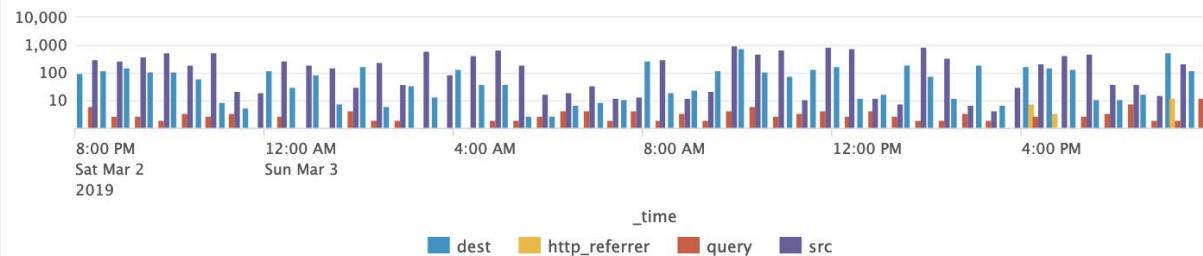
3

Targeted Campaign Monitoring

TA17-117 Chinese Malicious Cyber Activity

0

Threats Matched Field Over Time



Threats Matched by Intel Source

threat_key	count
AIS	16171
sans	1339
iblocklist_spyware	100
malware_domains	99
iblocklist_tor	19
ita_domains	4
iblocklist_web_attacker	2
edge:Package-042b1404-dab5-4636-a631-2be9a2936baa hailate ... AXI ... preDynamic_Host ... F00 ... APU ... 00.xml	1

City of LA Integrated SOC Threat Intelligence

CAP Asset Threats Matched by Dept (24hr)

Threat Match = Source IP

	Country	dest	src	
1	Seychelles	161.149.57.98	80.82.77.33	
2	United States	161.149.57.100	216.243.31.2	
3	United States	161.149.57.101	216.243.31.2	
4	United States	161.149.57.103	216.243.31.2	
5	United States	161.149.57.104	216.243.31.2	

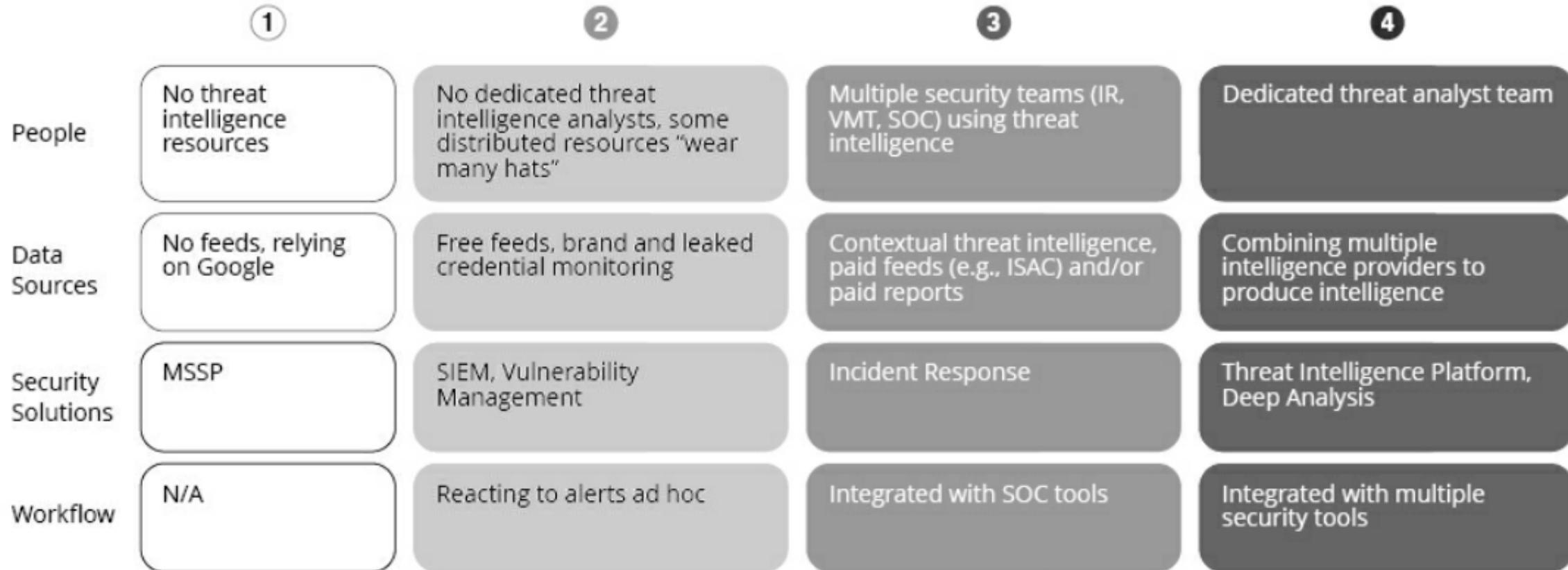
Threat Match = Destination

	Country	dest	src	count
1	Ireland	23.92.127.42	161.149.50.203	
2	United Arab Emirates	185.128.26.20	161.149.50.203	
3	Czechia	89.238.186.230	161.149.50.203	
4	United Kingdom	77.243.191.27	161.149.50.203	
5	Denmark	20.207.22.22	161.149.50.203	

CAP Asset Threats Matched by Dept (24hr)

Dashboard

Threat Intelligence Maturity Stages



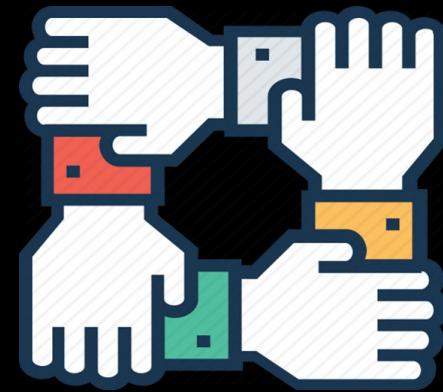
The Threat Intelligence Handbook – Chris Pace



#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

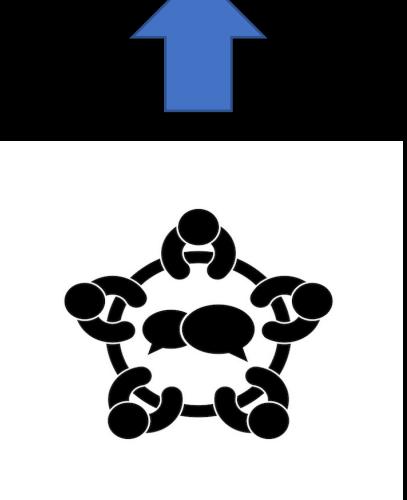
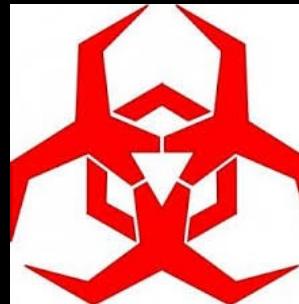
1. Research



2. Infiltration



3. Execution



\$\$\$ Ecosystem

5. Exfiltration



4. Command & Control



Collaborative Defense against Collaborative Attack



Government



Academia



A Public-Private Partnership
Benefits All



Business



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.



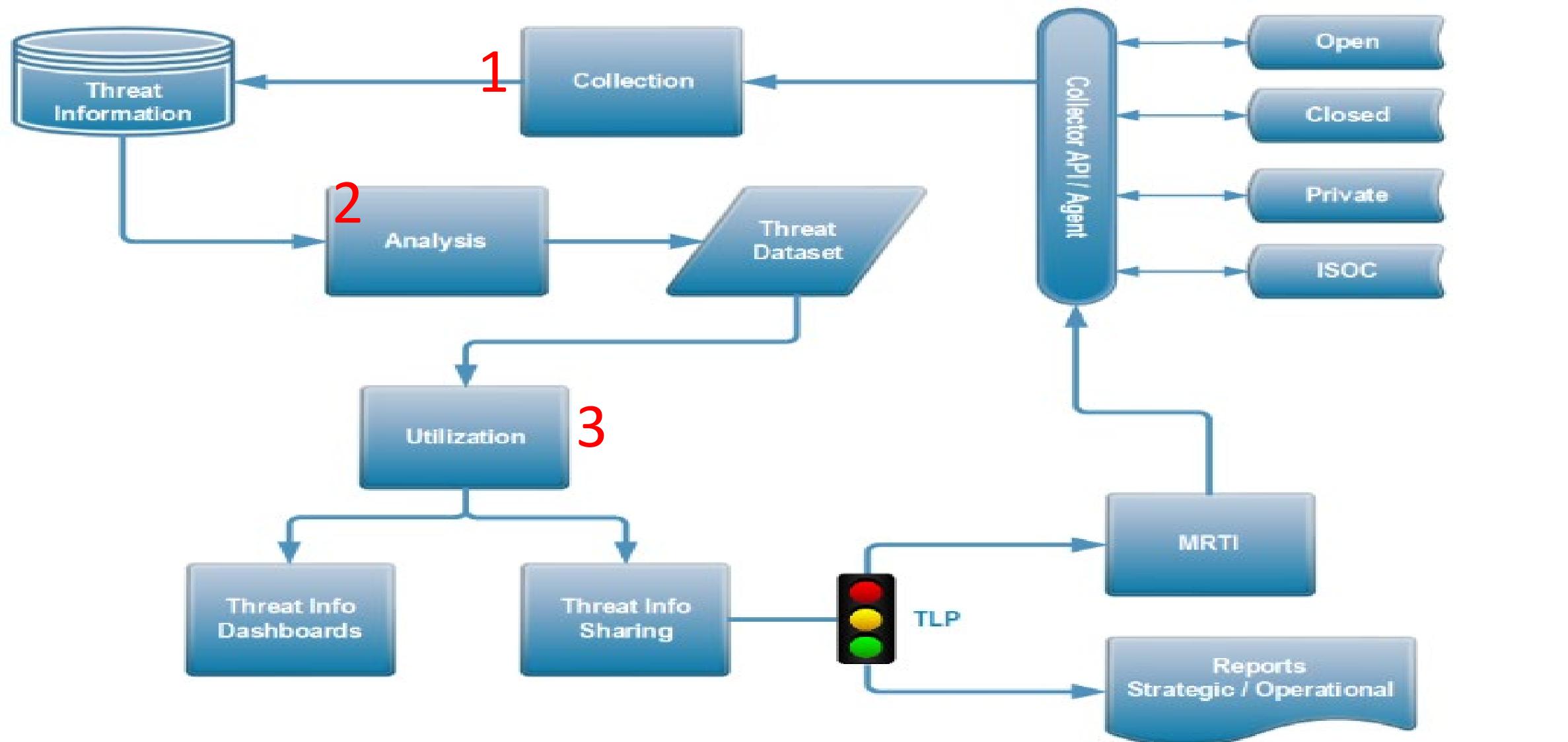
By [Jason Shueh](#)

AUGUST 16, 2017 9:23 AM



Los Angeles Cyber Lab

Threat Intelligence Analysis & Sharing Platform



Recommendations

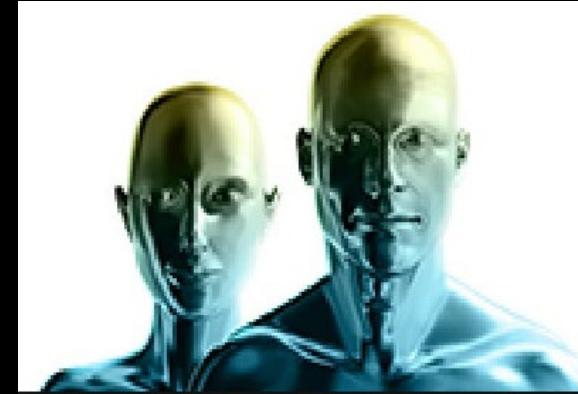
- Identify existing internal sources of CTI
- Develop Intelligence-driven use cases
- Establish information sharing platform, rules and agreements
- Join and participate in information sharing efforts
- Follow the TLP and protect the security of the shared information

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



RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: STR-T06

Thank you!

Timothy Lee

Chief Information Security Officer
City of Los Angeles
@tswleej316

#RSAC