
# Back to the 'root' of Incident Response

Boston Park Plaza Hotel | June 22-27, 2014

# National-level Collaborative Multi-Lateral Defensive Framework based on Big Data Analytics Paradigm

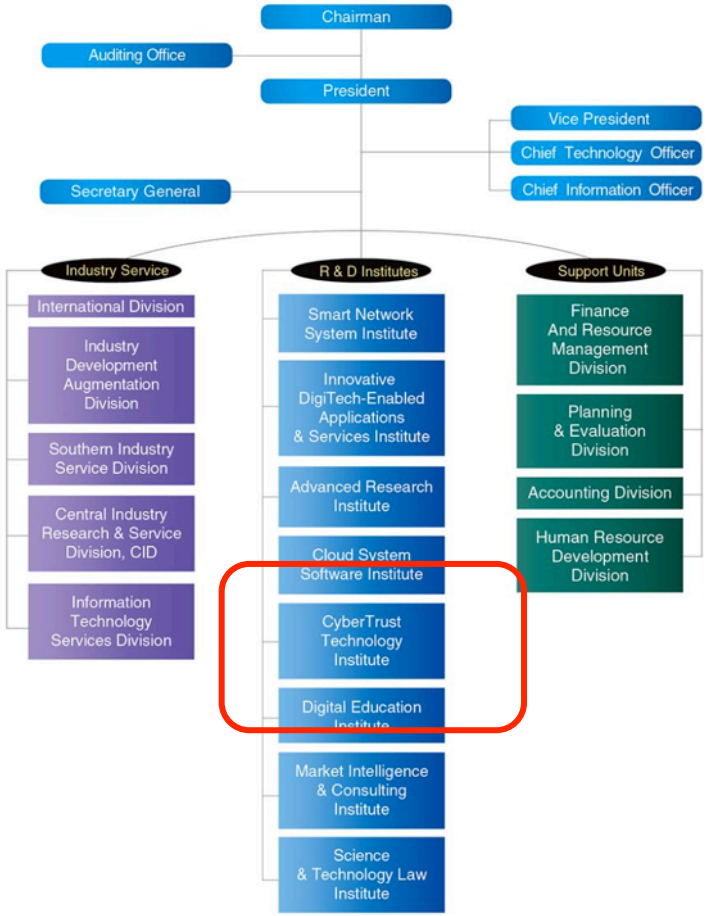
Ching-Hao, Eric, Mao Ph. D.
Institute for Information Industry / TWNCERT
chmao@iii.org.tw

# About Presenter


- Institute for Information Industry
- TWNCERT, GSOC Team Manager
- EDUCATIONS and EXPERIENCES
  - Ph. D., National Taiwan University of Science and Technology, Computer Science
  - Visiting scholar in Carnegie Mellon University, CyLab
  - Presentation: FIRST 2013/2014, CSA-APAC 2013, APCERT2014
- RESEARCH EXPERIENCES
  - big data analytics, network security, intrusion detection, mobile APP static analysis
  - more than 20+ academic journal and conferences papers

# About Institute for Information Industry

- To support the development/ applications of the information industry as well as the information society in Taiwan (NGO)
- CyberTrust Technology Institute (III) is running the Technology Service Center for the National Information and Communication Security Taskforce of the Executive Yuan



# Before the talk

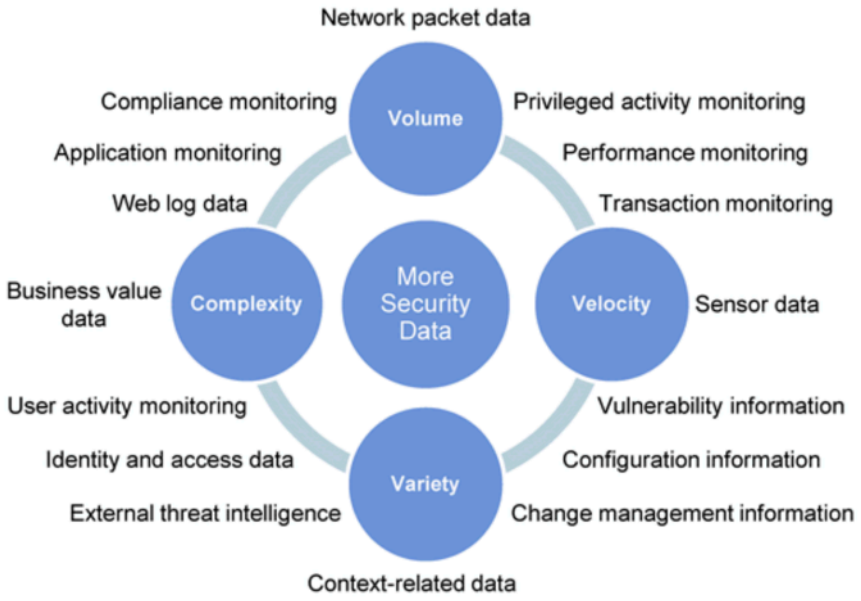
- This talk intents to share the experiences in how smoothly push the big data analytics combining different security operation centers data
- NOT represents Taiwan official government
- NOT drill down the sleepy detail of technology

# Outline

- Emergence Threats against to SOC
- Big Data Analytics in Security
- Security Analytics as a Service Framework
- Real Case 1: Taiwan Governments G-SOC in Big Data Analytics
- Real Case 2: Social Media Intelligence
- Conclusions

# SOC with Emergence Threats

- When an advanced targeted attack (APT) has bypassed traditional preventative security controls and has penetrated the organization




- Markets for security analytics platforms and for security patterns and algorithms providers will emerge
- A new role for a "security analytics analyst" or "security data scientist" will emerge

BIG DATA is emerging

# A Cute Definition

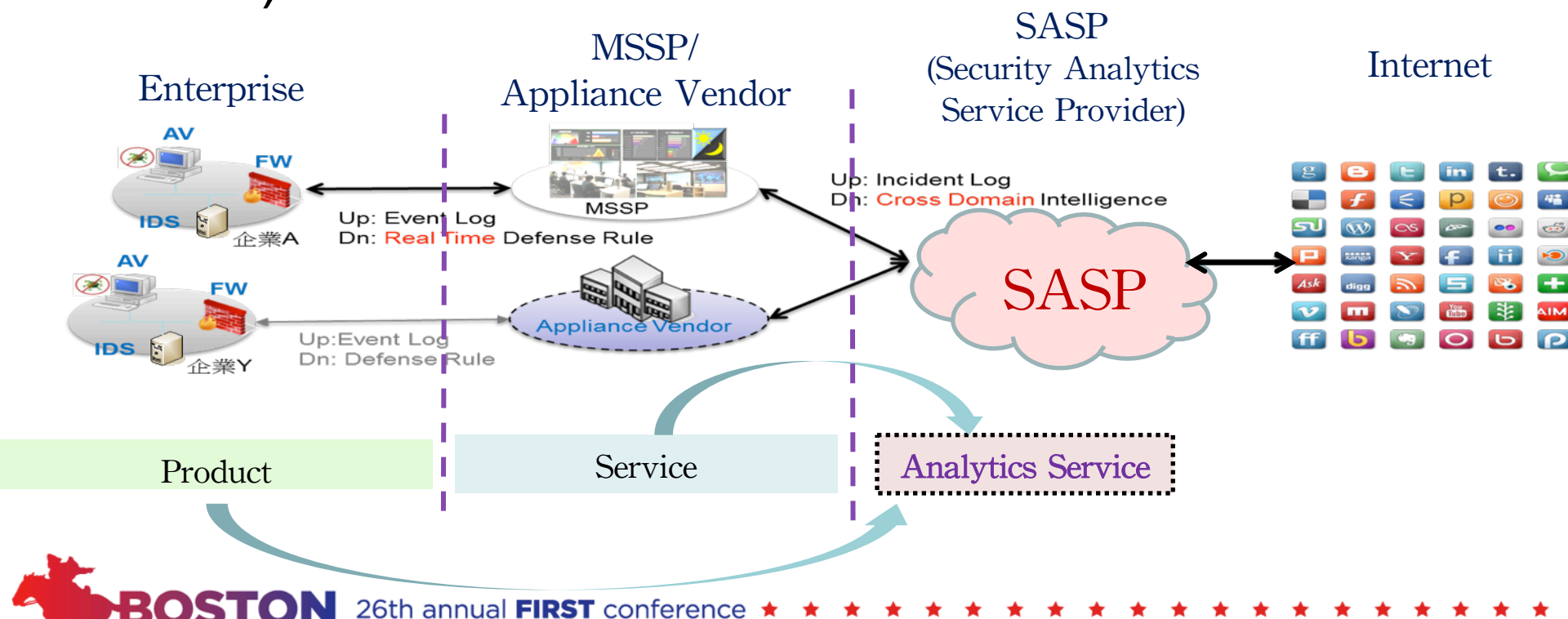
- “Big data is like teenage sex
  - everyone talks about it,
  - nobody really knows how to do it,
  - everyone thinks everyone else is doing it,
  - so everyone claims they are doing it...”


- Dan Ariely

Ref from: J. Pei: Being a Happy Dwarf in the Big Data Age PAKDD 2014 Keynote

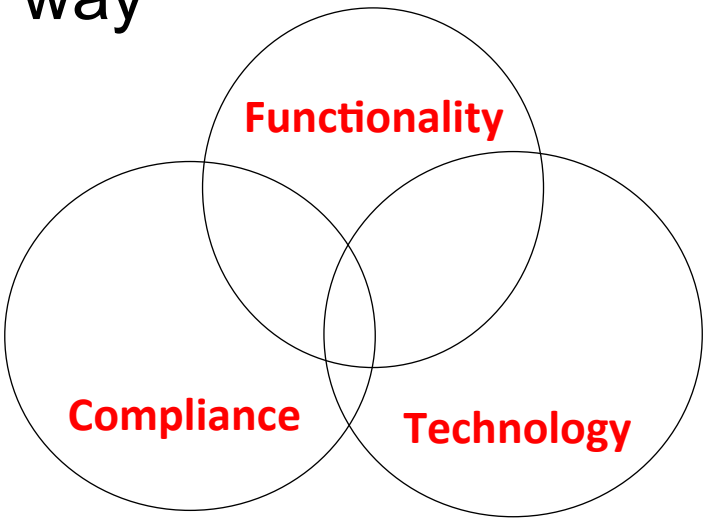
# Security Analytics as a Service

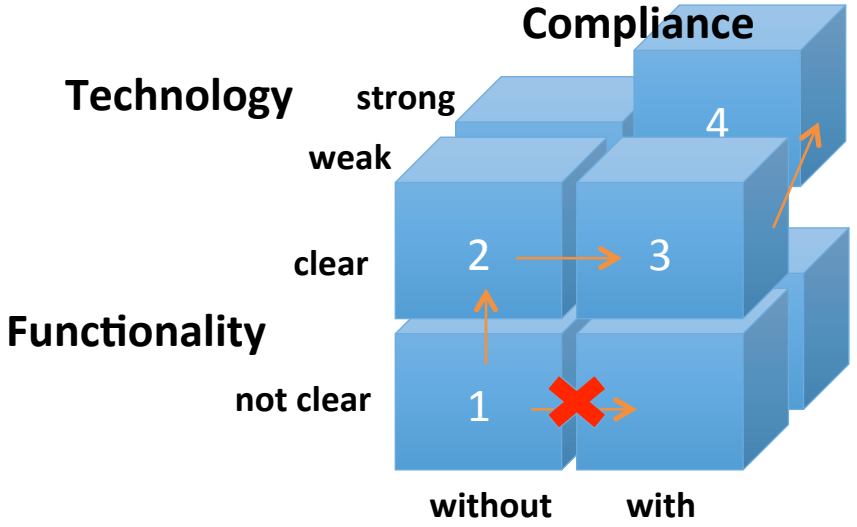
- Context-aware, risk-based view of IT, combining threat intelligence, vulnerability knowledge, compliance and business impact (from Gartner 2012)



# Key Considerations

- Difficult to achieve the expectation of strategy-level managers
- Difficult to convince the share of the data from business owner
- Difficult to adopt the big data solution in economic way



# Functionality (Scenario)

- Checking the material, understanding the scenario, making up a story and giving a imaginable results

- Careless configurations
- Non-techniques
- Context-aware required features

**STEP A:**
**Self-inspection**

- Estimating the baseline
- Building the multiple context-aware models
- Finding the patterns

**STEP B:**
**Threat Recognition**

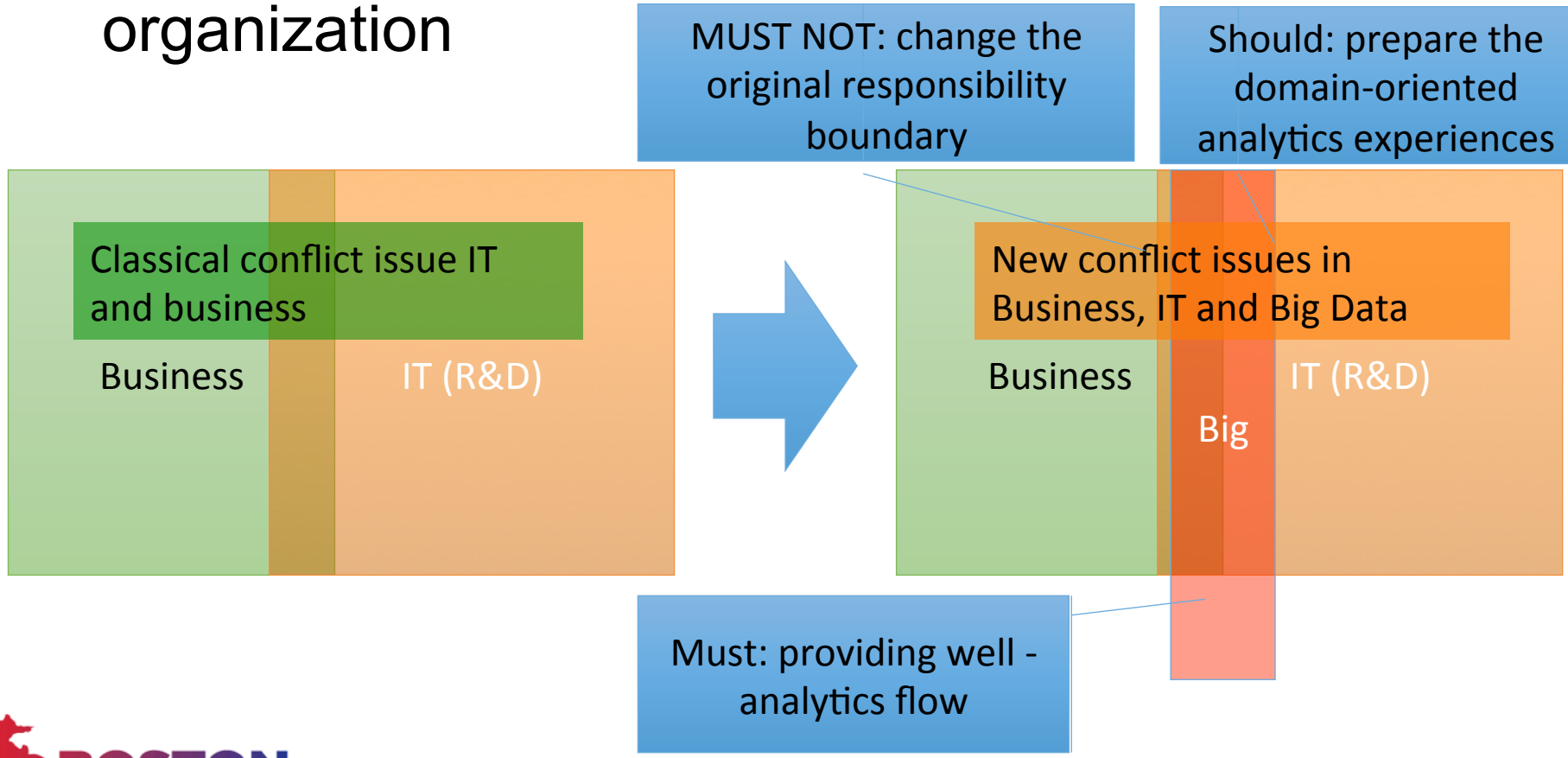
- Prioritizing candidate suspicious lists
- Correlating potential similar behavior lists

**STEP C:**
**Prioritization, Predictions and Decisions**

Without domain knowledge -> VERY GENERAL and NON-SENSE

# Compliance (Position)

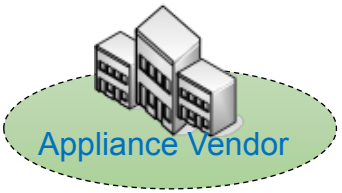
- As a big data analytics team, like third-party organization

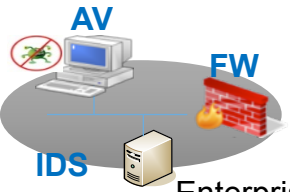


# Techniques (Cost Issue)

- If big data deployments are without key spirit, the commercial-solution advanced techniques just like slammers
- Compromise in OPEN-SOURCE and COMMERCIAL
- Data collection techniques
  - cost-sensitive consideration (depends on data values)
- Data warehouse and scalable computation
  - fast-indexing, scalable computation, distributed storages, NO-SQL
- ETL and Analytics mechanisms
  - domain-specific considerations, integration and modulation

# Security Analytics as a Service Architecture


conn

ArcSight

**Security Analytics Services and Visualization**

+ableau SOFTWARE

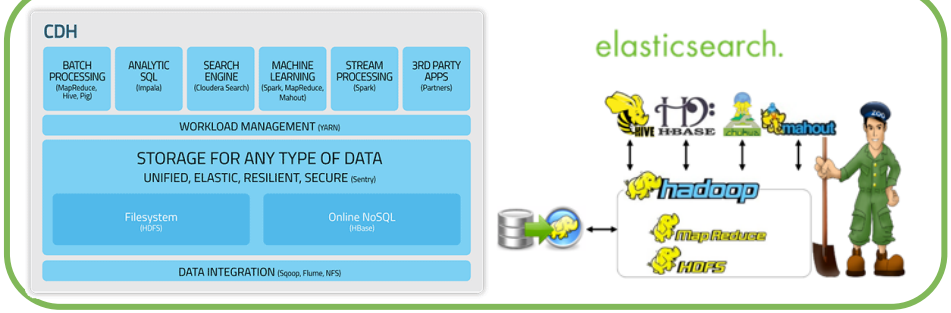
**Security-Specific Social and Logs ETL**

| Self-Inspection Modules | Threat Recognition Modules | Prioritization, Predictions Decisions Modules |
|---|---|---|

**Security-Specific Social and Logs ETL**

syncsort

conn

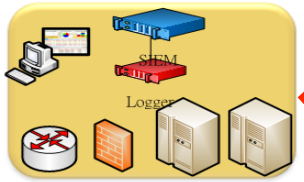



**Big data analytics platform**

Social Media
Threat Intelligenc

# REAL CASE 1: TAIWAN G-SOC

Gov. Inst.



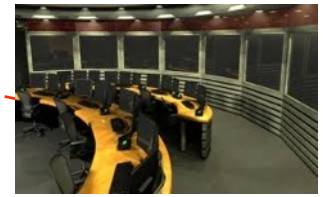

Outsourced
SOC Service

20,000 EPS * 60 (s) * 60 (m) *
365 (d) * 350K = 26.28 TB

Government
Chief of Security Officer

GOV Self-SOC

Academic SOC



Enterprise SOC

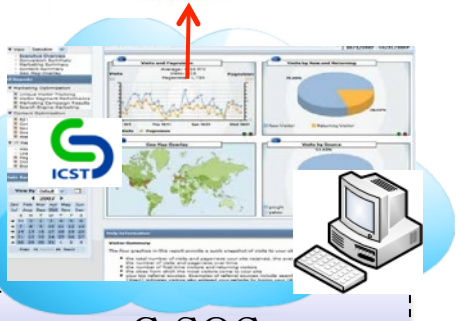
International
ISAC

acer eDC

TRADE-VAN 關貿網路

Information Security Service Digital United

HiNet 資安艦隊




G-SOC

GSN Backbone

Honeynet

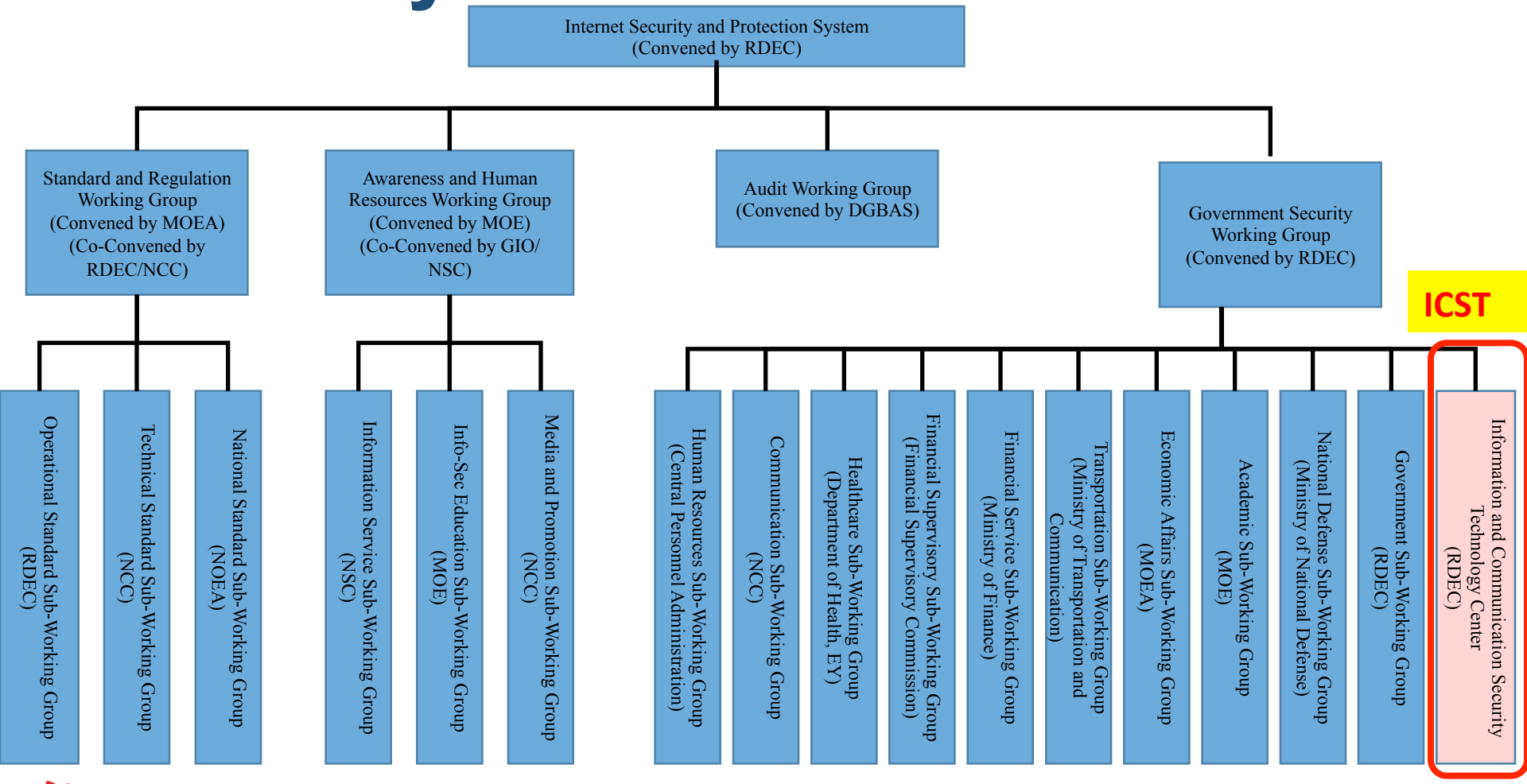
Tickets
Correlated Events
Raw Events

1:10:100

# SOC service in Taiwan Government

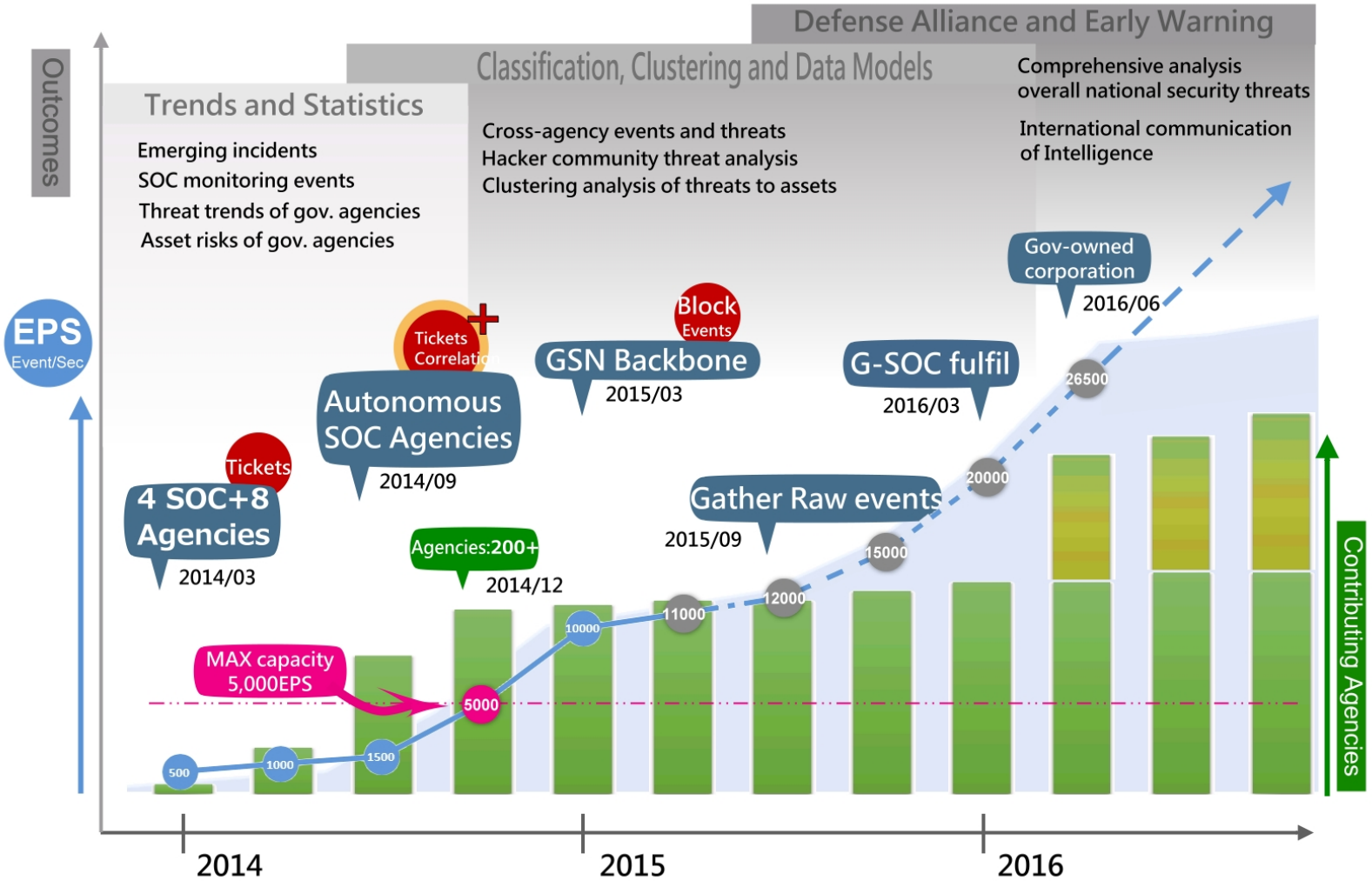
- Main service providers: Acer (Taiwan largest eDC), Chungwha Telcomm (Taiwan Largest ISP), ISSDU and TradeVan
  - Cover almost whole government institutes in Taiwan
  - Two Types:
    - Assist to build up the SOC but not operate
    - Assist to deploy the sensors to provide SOC 7x24 monitoring service


# Current National Info & Comm Security Taskforce




TWNCERT

# Milestone of G-SOC



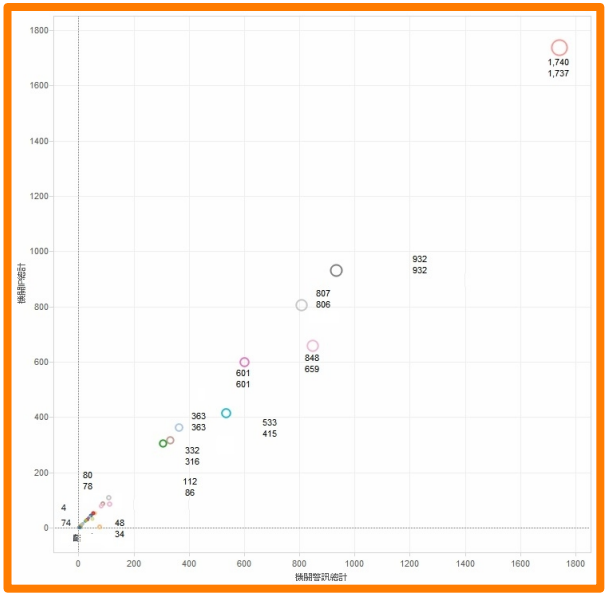
# Functionality (Scenario)

- Normalization -> Self-inspection

| | (1) System | (2) Policy | (3) Scan | (4) DDoS | (5) Malware | (6) Intrusion |
|---|---|---|---|---|---|---|
| Group A | 1 | 223 | 48 | 19 | 116 | 3,473 |
| Group B | 6 | 981 | 100 | 12 | 37 | 887 |
| Group C | 85 | 102 | 82 | 33 | 0 | 546 |
| Group D | 0 | 237 | 4 | 186 | 4 | 178 |
| Group E | 0 | 0 | 0 | 0 | 10 | 93 |
| Group G | 0 | 0 | 7 | 0 | 21 | 31 |
| Group H | 0 | 0 | 0 | 0 | 13 | 17 |
| Group I | 0 | | | | 17 | 16 |
| Group J | 0 | 0 | 0 | 0 | 0 | 4 |

1-99 100-499 500-999 1000-1999 2000↑

- ✓ Careless configurations
- ✓ Non-techniques
- ✓ Context-aware required features




Large-scale Graph Analysis

Statistic Analysis

**STEP A:**
**Self-inspection**

Data Mining Patterns Finding

**STEP B:**
**Threat Recognition**

**STEP C:**
**Prioritization, Predictions and Decisions**

# Not only compliances! collaboration is the key!

- Paradigm: Just like Verizon-Data Breach Investigations Report (DBIR)
- From the analytics view, we do not involve original functionality of each institutes
- Share and devote the inter-organization threat correlations

# Techniques

- Commercial solutions in first step
- Open source solutions in second step
- Continually integrate both

*SOC*

*Intelligence in the wild*

*Social media*

Connectors

## G-SOC Analysis

- Emergency Security event correlations
- Cross-organizations correlation and trend analysis
- Social media intelligence and threat trend analysis
- Assets and security events correlations

## G-SOC Platform

**Big Data Analytics**

**SIEM**

**Scalable data warehouse**

## Outcome

- Specified security event and intelligence report
- National information security threat intelligence report
- National threat intelligence exchange

SAN?
NAS?
Hadoop!

# REAL CASE 2:

- Social media is a path to enter big data
  - Data fulfills 4V
  - Implementation easily
  - Abundance of algorithms, mechanisms, open source toolkits
  - Application is interesting (involved human)
- However, how to evaluate the analysis result is still a “BIG” issue

# Break News from Social Media


This week I tried hard on Android (tools and os) by fuzzing and I found a **Android OS memory corruption bugs** and Android Debug Bridge (adb.exe) BOF.

Also announced his app on his blog, welcome everyone to test


ibrahim BALİÇ@ibrahimbalic 3/16
I'm now trying to publish that app on the google play store, so let see whats going to happin ( :

**Google (GOOG) Hacked Twice**

BY Tony Owusu | 03/17/14 - 04:36 PM EDT

Turkish Hacker Crashes Google Play Store Twice while testing vulnerability

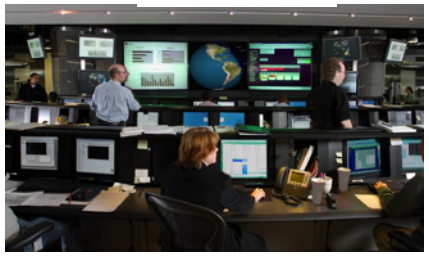
Tuesday, March 18, 2014 by Swati Khandelwal

**Android malformed APK DoS – Part II**

MARCH 18, 2014 | MAKALELER | NO COMMENTS |

# Social Media Intelligence

- PegAthena: emergence security threats recognition system

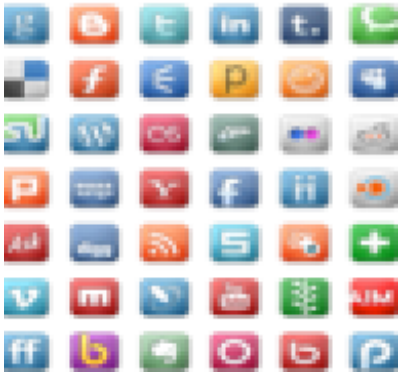



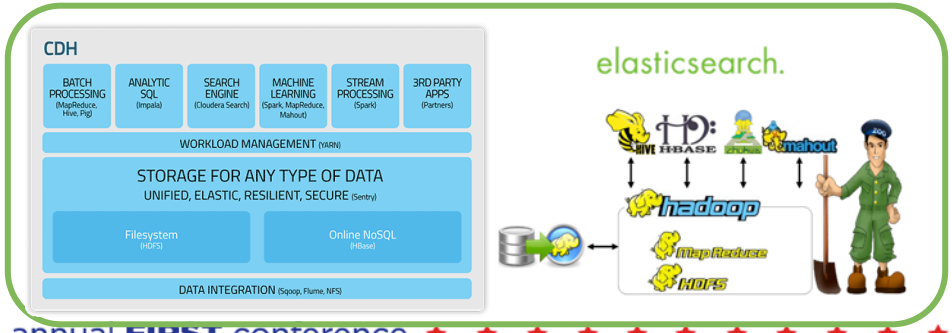
Service Management Interface

Emergence Threat Topic Finding

Social Media Connector

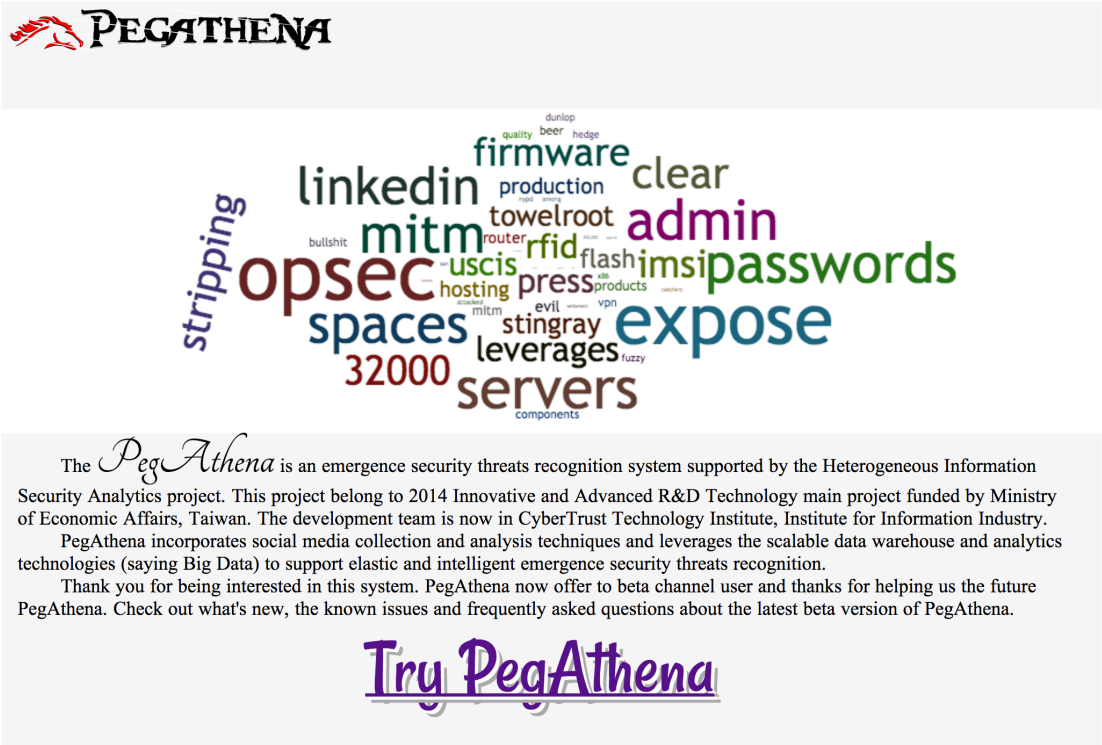
cve.mitre.org





# Pegathena

- http://pegathena.info/
- Welcome helping us to test

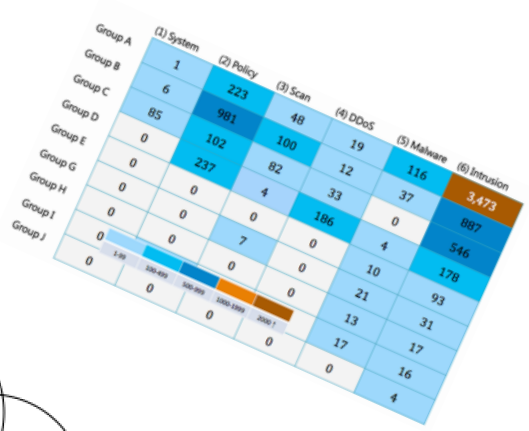


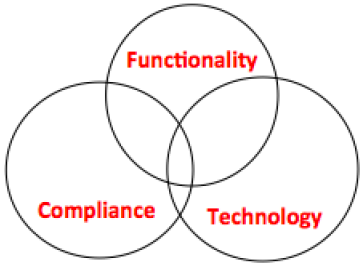
# Conclusions

- Three keys: Functionality, Compliance and Technology
  - Functionality- scenario with reality
  - Technology- open source and commercial solutions
  - Compliance- aware the positions
- Security Analytics as a Service as well as G-SOC Big Data Analytics plays a new role but not replaces the original roles

# Acknowledgement

and
Dr. Perry Liu,
Greg Wu,
Chih-Hung Lin
…





# Thanks & Questions

# Welcome to use: http://pegathena.info/