Astrikos Consulting™

PROACTIVE, INTELLIGENCE BASED CYBERSECURITY FRAMEWORK IN THE COGNITIVE & OPEN ERA

SMART CITIES AND SMART INFRA

Dr. Chinmay Hegde
ASTRIKOS CONSULTING

Astrikos Consulting™

STRATEGIZE – ELUCIDATE – DELIVER - ENHANCE

ISO

ISO/IEC 21823-1:2019 | ISO/IEC 20000-1:2011 | ISO/IEC 27001-1:2013 | ISO 9001:2015

www.astrikosconsulting.com

OVERVIEW

The cyberspace isn't any longer a closed mesh, it has eventually become open.

"Citizens are becoming netizens" - Computers or Mobile phones or any handheld devices.

New Challenge - "upkeeping cyber security when connected";

More and more challenging for the governing and regulating bodies, a.k.a. Cyber police or cyber cops. More the cyberspace technologies update, updated are the attackers too.

Recent types of attacks include following

- Ransomwares on computers and IoT devices
- Social Media hate attacks
- Phishing, Smishing and Vishing based financial frauds
- IP/DNS spoofing and poisoning
- Distributed Denial of Service attacks
- Brand Vandalism attacks and … many more !

OBJECTIVES

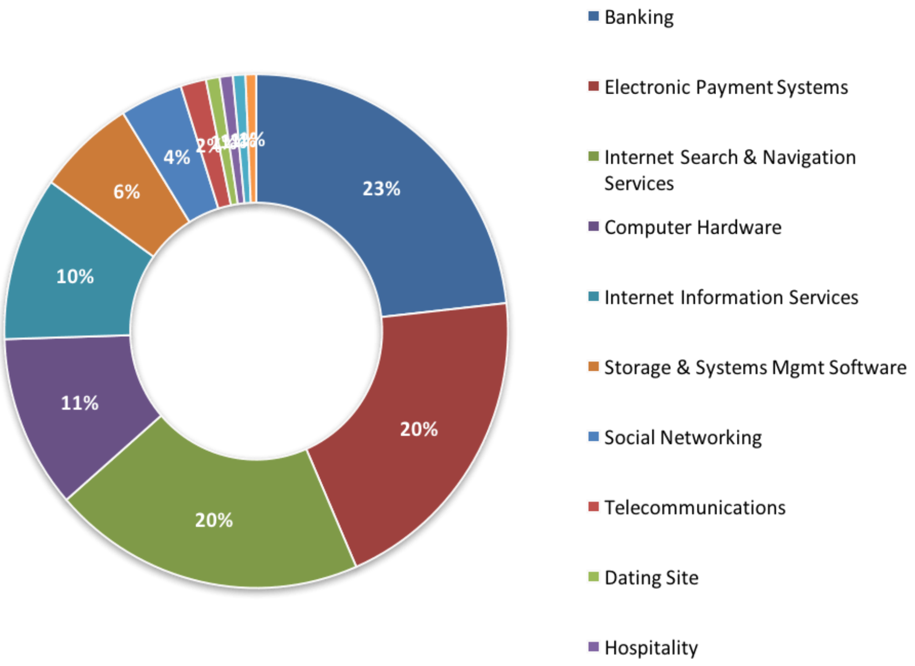
- Artificial Intelligence driven Cyber Security Analytical System
- Targeting the 'zero-day' detection of the potential threats
- Proactive prevention of possible incidents
- Detect possible "Hate Attacks" with

  Threat Intelligence driven **Heuristic Analysis**
- **CUSTOMIZED ATTACK DEFINITION –**

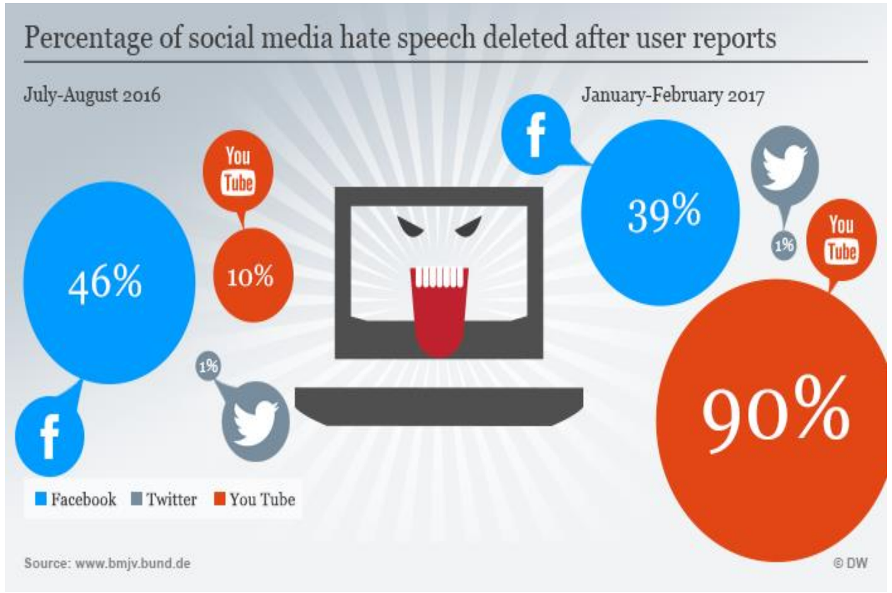
  "What you define as not an attack can be attack for me !"
- Attack forensics and Repository Systems

ATTACK DIASPORA

ATTACK TARGETS

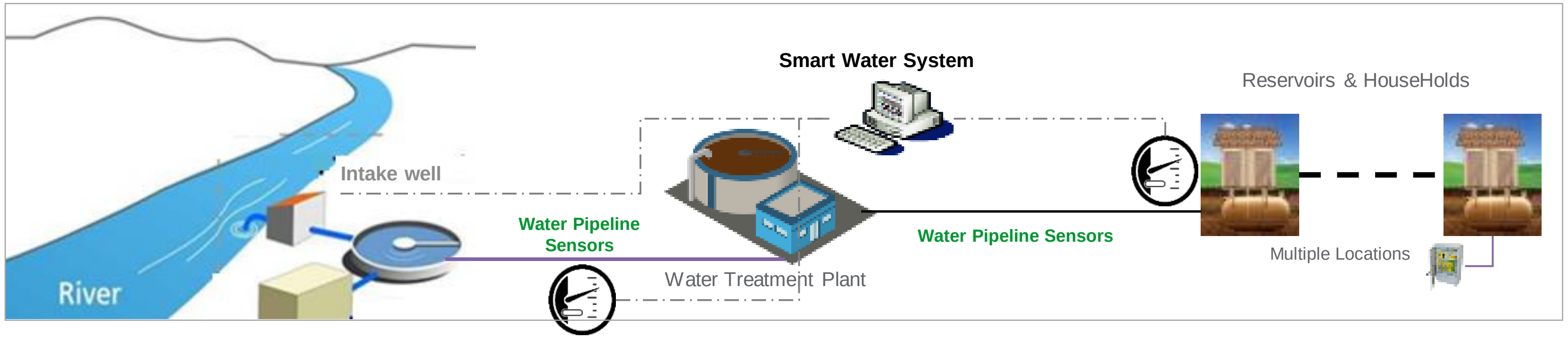


ARE THESE ONLY ATTACKS ?? NO


Percentage of social media hate speech deleted after user reports

Source: www.bmjv.bund.de

"SOCIAL MEDIA HATE ATTACKS"



Smart Water System

Reservoirs & HouseHolds

Intake well

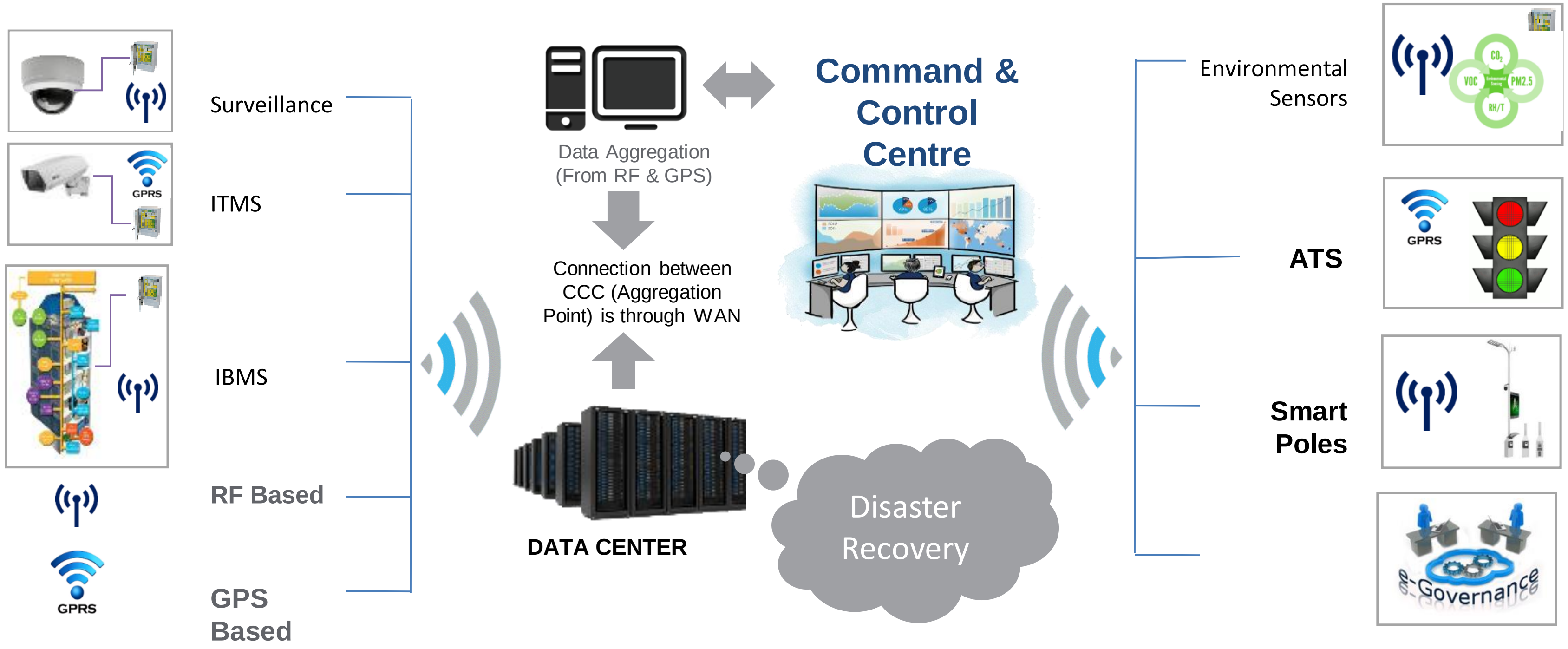
Water Pipeline Sensors

Water Pipeline Sensors

Multiple Locations

River

Water Treatment Plant



Surveillance

ITMS

IBMS

RF Based

GPS Based

Data Aggregation (From RF & GPS)

Connection between CCC (Aggregation Point) is through WAN

DATA CENTER

Command & Control Centre

Disaster Recovery

Environmental Sensors

ATS

Smart Poles

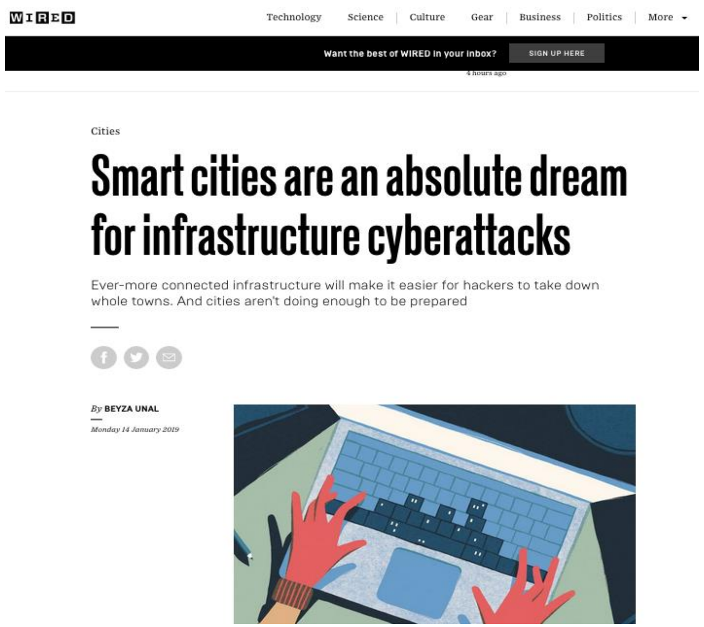
CYBER SECURITY CHALLENGE IN SMART INFRA

City network is an

“OPEN NETWORK”

- Wider Attack Surface
- Open Smart Elements installed in public places
- Open Data Flow and Exchange
- Collaborative cross-departmental integration –

“High chances of loose coupling and loopholes”



Want the best of WIRED in your inbox?

4 hours ago

Cities

Smart cities are an absolute dream for infrastructure cyberattacks

Ever-more connected infrastructure will make it easier for hackers to take down whole towns. And cities aren't doing enough to be prepared

By BEYZA UNAL

Monday 14 January 2019

What is needed

"A CUSTOMIZABLE SECURITY ANALYTICAL AND RESPONSE SYSTEM

THAT CAN ADAPT THE 'ZERO DAY DETECTION AND PREVENTION

TECHNIQUE' SCALABLE ACROSS MULTIPLE PROPRIETARY SOLUTIONS"

- **ONLY PROPRIETARY SECURITY SOLUTIONS CAN'T CATER TO THIS NEED**
- **NEED OF LEVERAGING OPEN SOURCE TECHNOLOGIES TOO**

"FOLLOW A - FRAMEWORK - APPROACH"

DETECTION

APPROACH AND METHODOLOGY

SMART CITY MISSION GUIDELINES

- MoHUA Guidelines – **What should be the part of Smart Cities?**
- MoHUA Guidelines – **ICT Enablement in Smart Cities**
- MoHUA Guidelines – **Citizen's Data Privacy and Cyber Security in Smart Cities**
- **Responsibilities of Stakeholders**

Generic Guidelines:

http://smartcities.gov.in/content/innerpage/guidelines.php

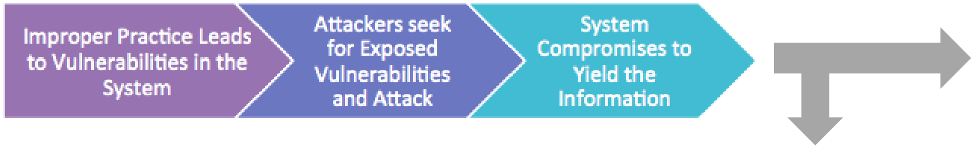
Data Privacy and Cyber Security:

http://smartcities.gov.in/upload/oms/5821b621a862dCyber_Securitypdf.pdf

Holistic Cyber and Information Security Model

Astrikos Consulting™

Vulnerability – Exploitation – Compromise


Improper Practice Leads to Vulnerabilities in the System

Attackers seek for Exposed Vulnerabilities and Attack

System Compromises to Yield the Information

"Old Method 4D's

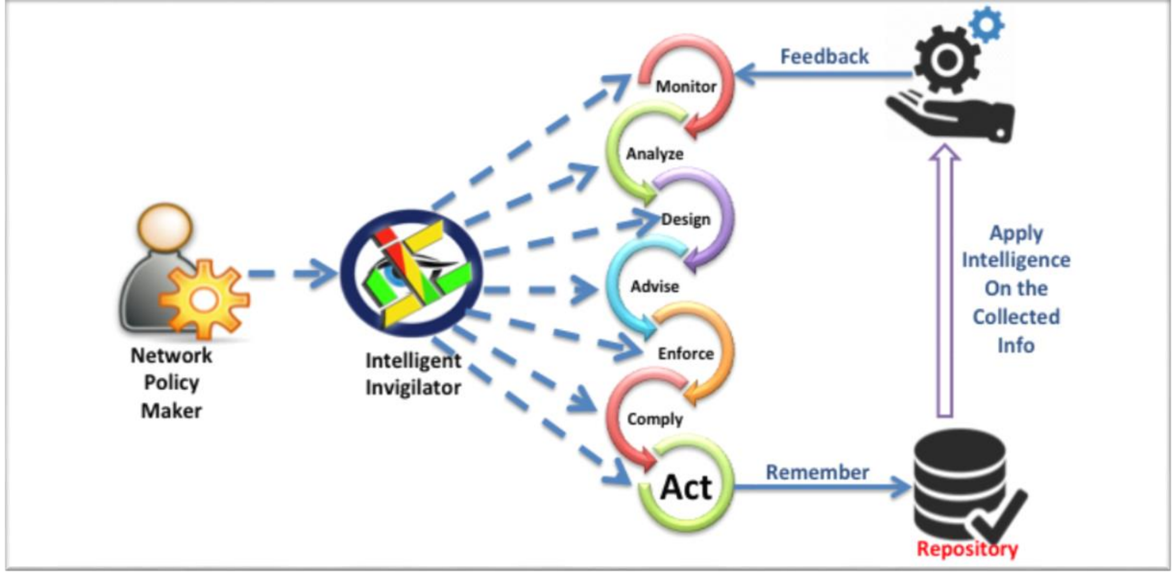
- Deter
- Delay
- Detect
- Deny

"OUTDATED TECHNIQUE"

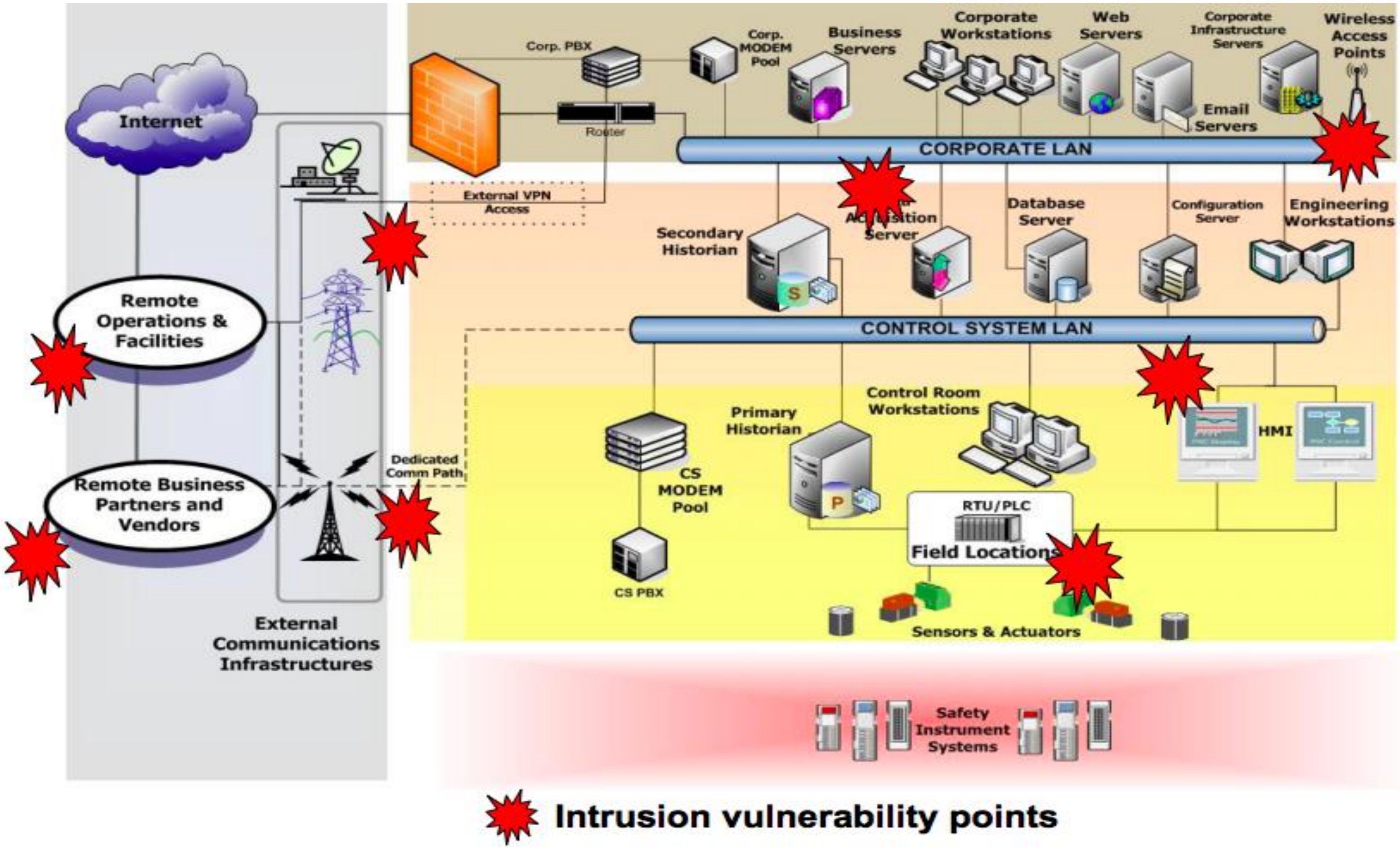
NEW GENERATION INFORMATION AND CYBER SECURITY FRAMEWORK

- Firewalls / IPS Appliances
- Web Application Firewall
- Advanced Persistent Threat Management
- Unified Threat Management
- VPN based restricted and eligible network access
- Holistic Security Information and Intelligence Management

Innovative Auto-Learning Threat Protection



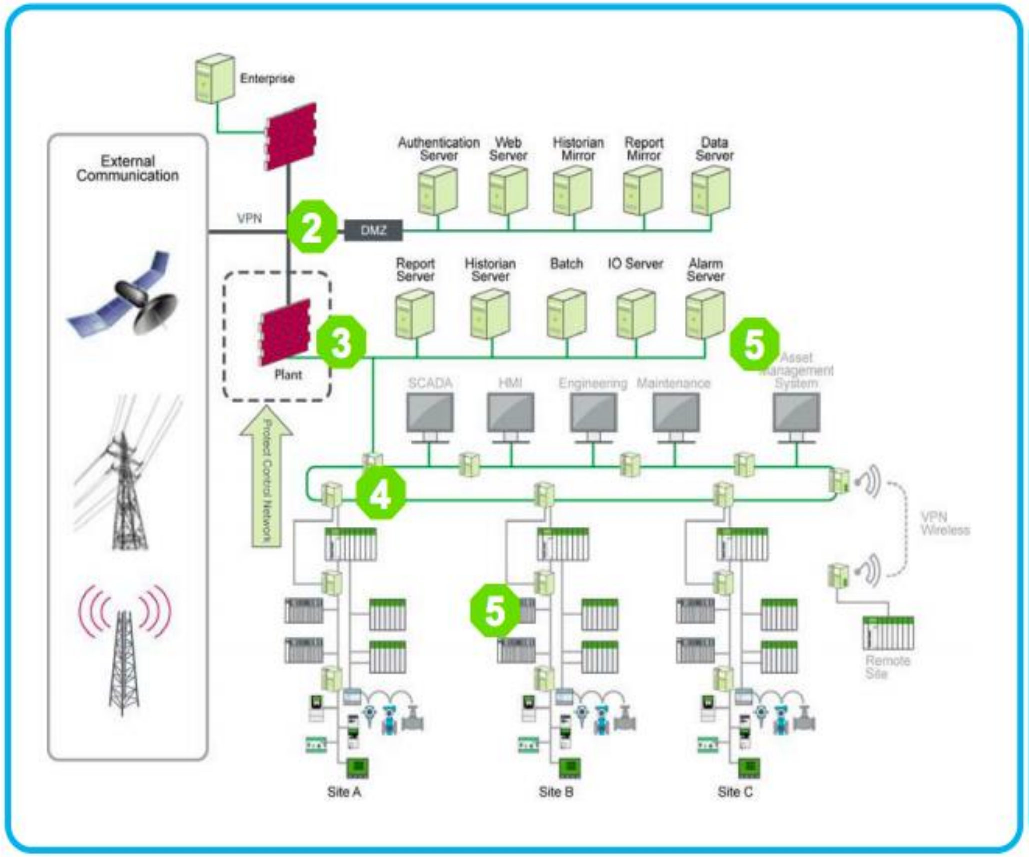
Holistic Cyber and Information Security Model



Multi-Layered Security Approach

- Technologies
- Architectures
- Policies
- Monitoring and Enforcement
- Compliance
- Training

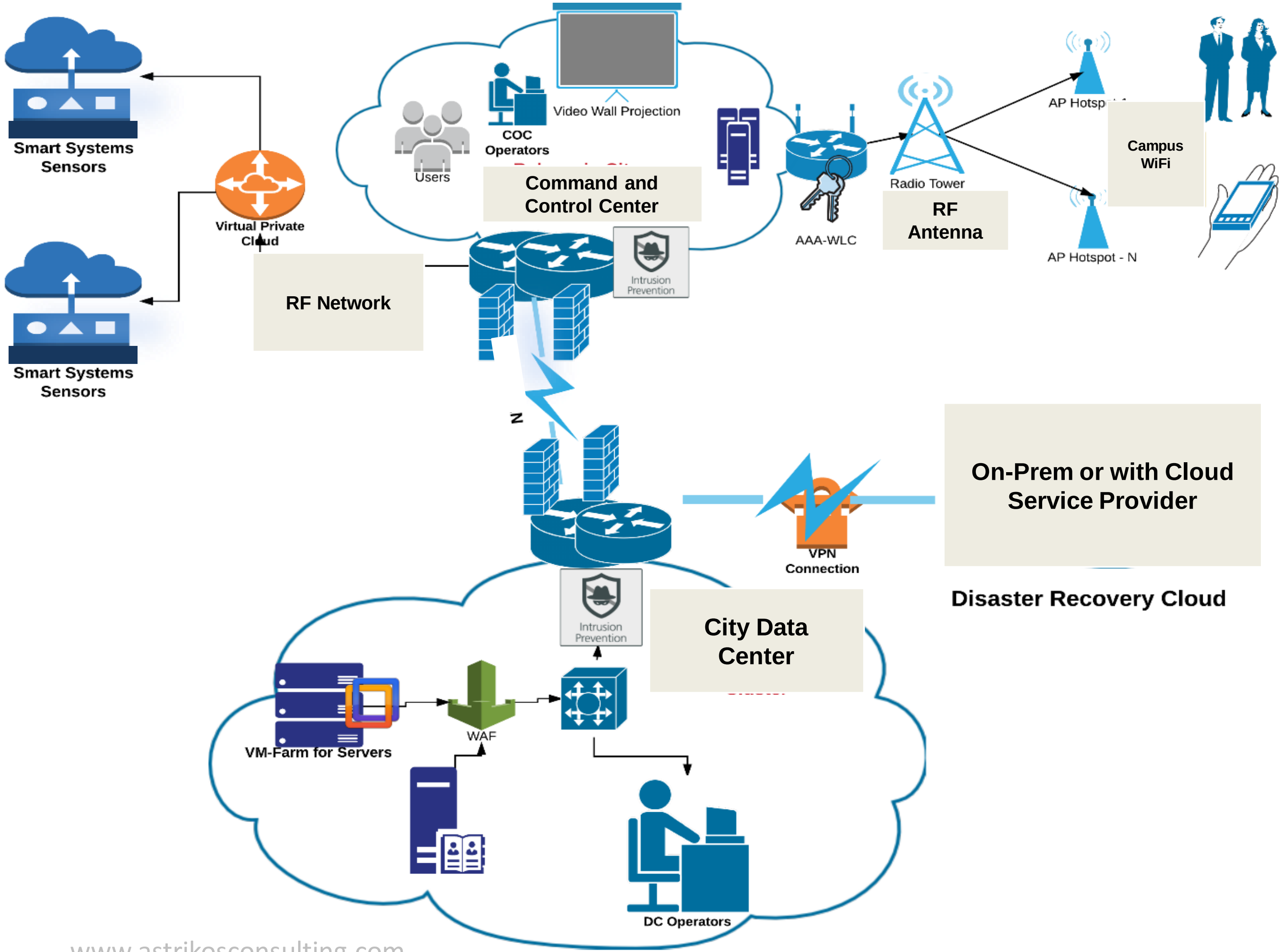
The “Defence in Depth” Approach (DiD)



6 key steps:

1. Security Plan
2. Network Separation
3. Perimeter Protection
4. Network Segmentation
5. Device Hardening
6. Monitoring & Update

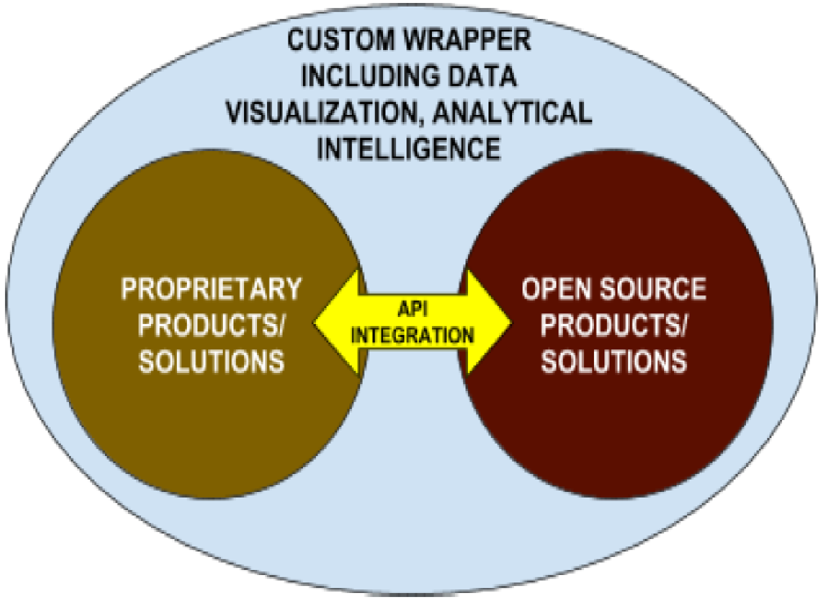
Reference Security & Network Architecture



- **Industrial** Data Centre
- **On-prem or Cloud** for DR
- **MAN/WAN** Linkbetween CCC & DC
- **RF** Based Campus Network & Aggregated Bandwidth
- **RF** Based Edge Things Network
- End-to-End AAA & Information Security

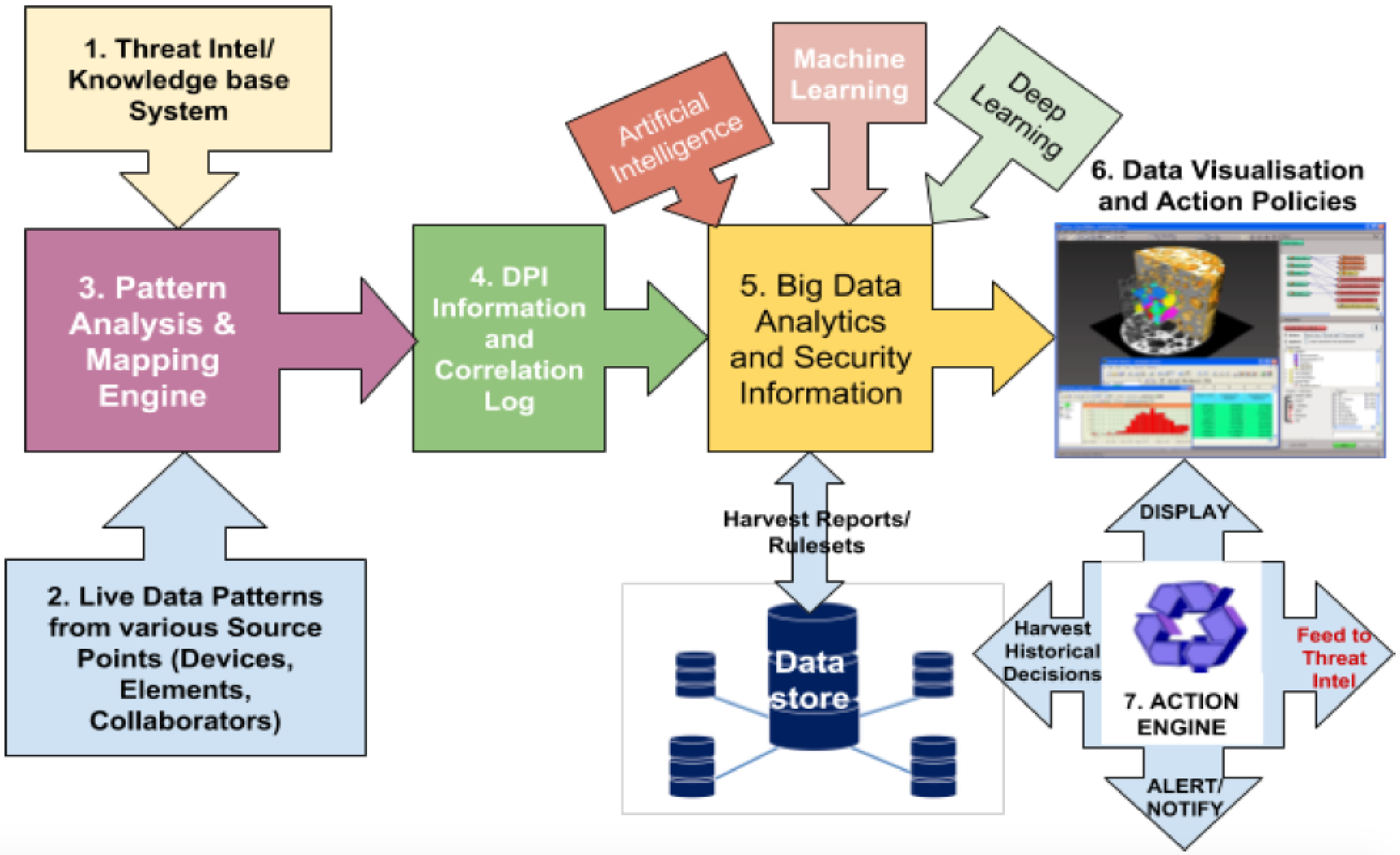
WHAT'S THE MAGIC COMBO?

- **PROPRIETARY SOLUTIONS:**
  - GATEWAY PROTECTION
  - IDENTITY MANAGEMENT
  - SIEM AND SECURITY INFORMATION SYSTEMS
  - ANTI PERSISTENT THREAT MANAGEMENT
  - ETC…
- **OPEN SOURCE SOLUTIONS:**
  - VA/PT
  - THREAT INTEL SOURCES
  - GLOBAL THREAT REPOSITORIES
  - SECURITY INTELLIGENCE SYSTEMS
  - ETC..
- **ANY OTHER CUSTOM SOURCES : CCTNS/eCourts DB or etc.,.**
- **DEVELOP A CUSTOM WRAPPER SYSTEM TO INTEGRATE AND BUILD A HOLISTIC SYSTEM**


CUSTOM WRAPPER INCLUDING DATA VISUALIZATION, ANALYTICAL INTELLIGENCE
PROPRIETARY PRODUCTS/ SOLUTIONS
API INTEGRATION
OPEN SOURCE PRODUCTS/ SOLUTIONS

Astrikos Consulting

APPROACH OF DETECTION



1. Threat Intel/ Knowledge base System

2. Live Data Patterns from various Source Points (Devices, Elements, Collaborators)

3. Pattern Analysis & Mapping Engine

4. DPI Information and Correlation Log

5. Big Data Analytics and Security Information

Artificial Intelligence

Machine Learning

Deep Learning

6. Data Visualisation and Action Policies

Harvest Reports/ Rulesets

Data store

DISPLAY

Harvest Historical Decisions

7. ACTION ENGINE

Feed to Threat Intel

ALERT/ NOTIFY

Thank You !

QUESTIONS AND QUERIES…?

Contact: Chinmay Hegde

Cell. +91 99028 25577 | Ph. +91 80 2667 5222

Email: chegde@astrikosconsulting.com / connect@astrikosconsulting.com

www.astrikosconsulting.com

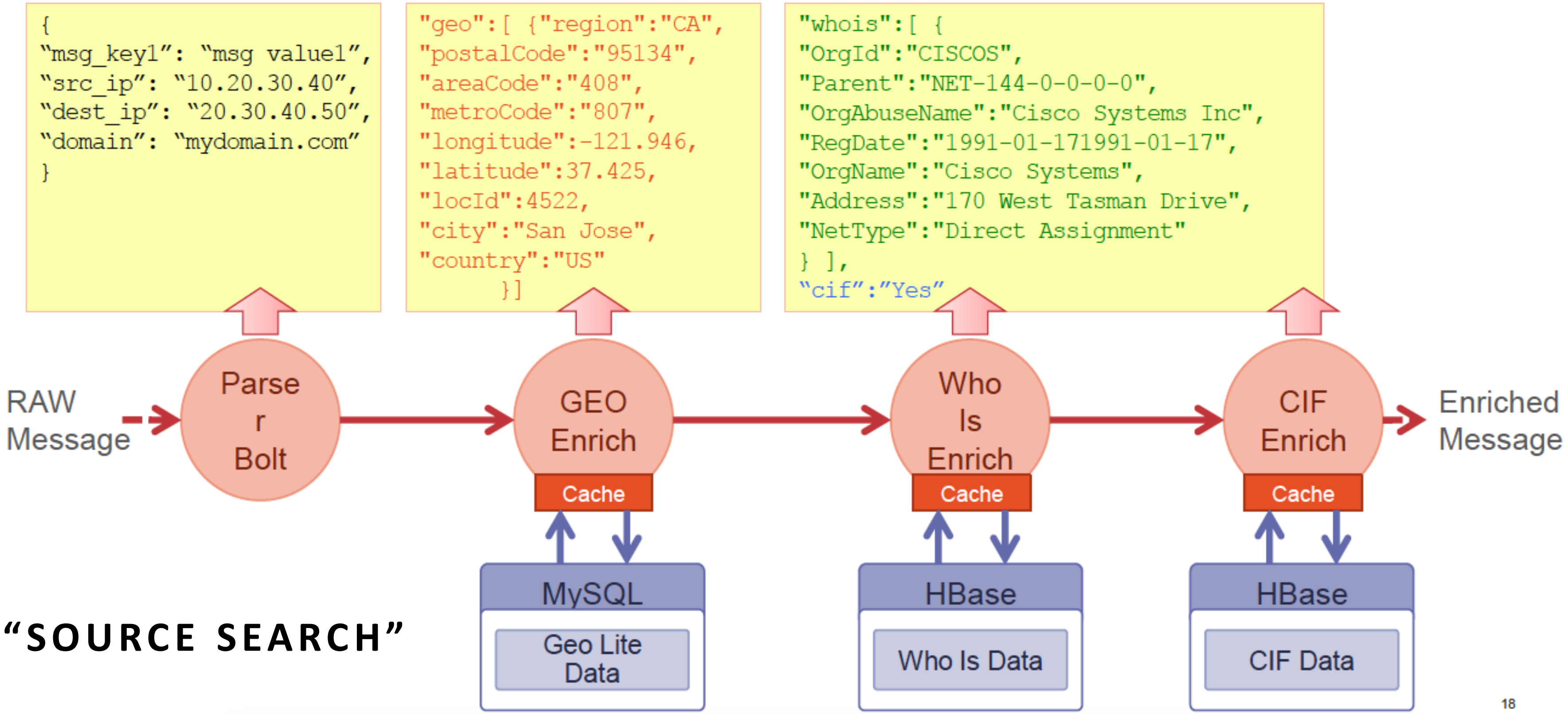
Smart Cities, Smart Villages, Smart Systems and Cyber Security

India: #129, K R Road, Basavangudi, Bengaluru– 560004
Singapore: #2 Corporation Road, 01-13, Corporation Place, Singapore – 618494

Astrikos Consulting™

BACKUP SLIDES

DETECTION - IN DEPTH OVERVIEW



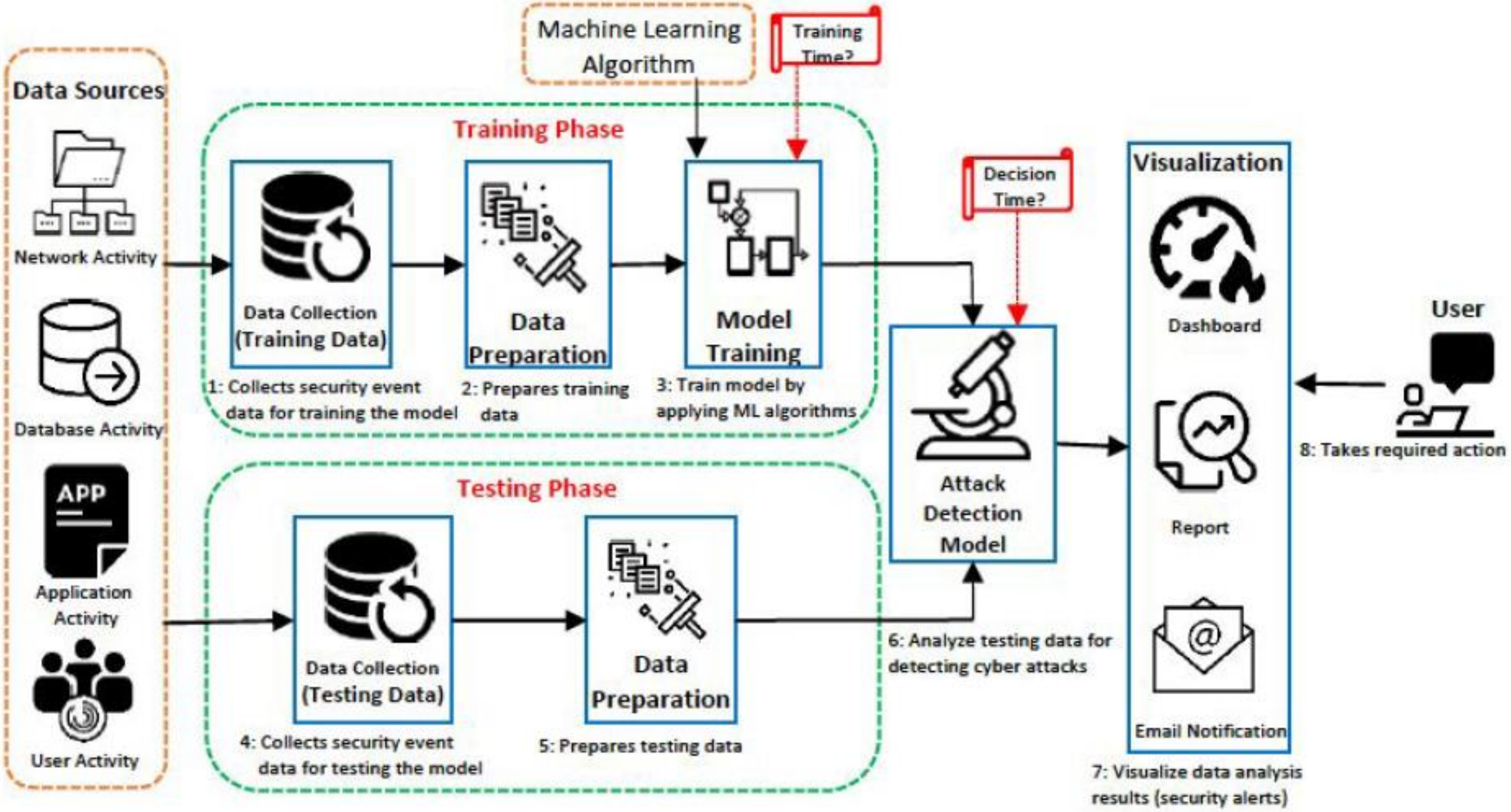
```
{
“msg_key1”: “msg value1”,
“src_ip”: “10.20.30.40”,
“dest_ip”: “20.30.40.50”,
“domain”: “mydomain.com”
}
```

```
"geo":[ {"region":"CA",
"postalCode":"95134",
"areaCode":"408",
"metroCode":"807",
"longitude":-121.946,
"latitude":37.425,
"locId":4522,
"city":"San Jose",
"country":"US"
      }]
```

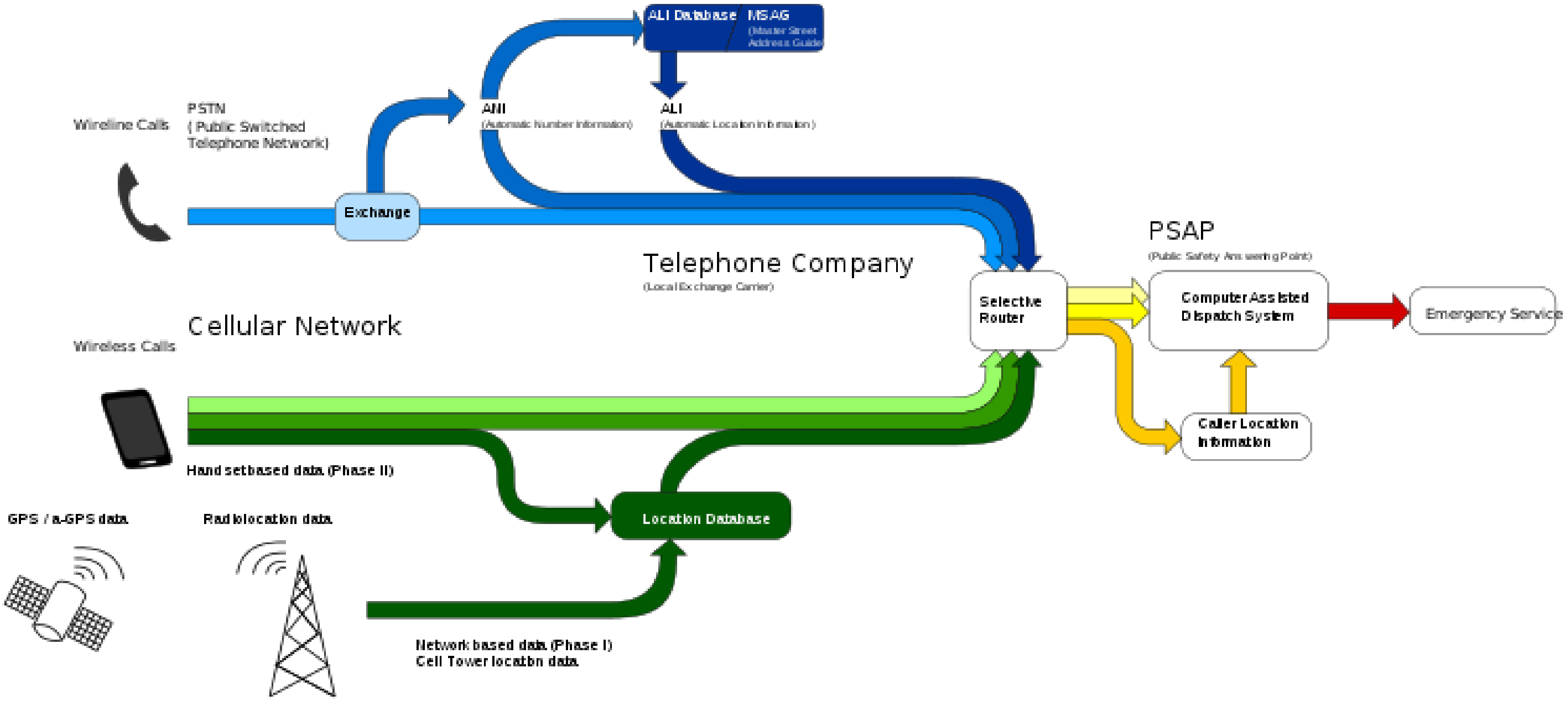
```
"whois":[ {
"OrgId":"CISCOS",
"Parent":"NET-144-0-0-0-0",
"OrgAbuseName":"Cisco Systems Inc",
"RegDate":"1991-01-171991-01-17",
"OrgName":"Cisco Systems",
"Address":"170 West Tasman Drive",
"NetType":"Direct Assignment"
} ],
“cif”:”Yes”
```

“SOURCE SEARCH”

TECHNICAL DATA FLOW DESIGN


Machine Learning Algorithm
Training Time?
Data Sources
Network Activity
Database Activity
APP
Application Activity
User Activity
Training Phase
Data Collection (Training Data)
Data Preparation
Model Training
1: Collects security event data for training the model
2: Prepares training data
3: Train model by applying ML algorithms
Testing Phase
Data Collection (Testing Data)
Data Preparation
4: Collects security event data for testing the model
5: Prepares testing data
Decision Time?
Attack Detection Model
6: Analyze testing data for detecting cyber attacks
Visualization
Dashboard
Report
Email Notification
7: Visualize data analysis results (security alerts)
User
8: Takes required action

DETECTION - CDR ANALYSIS


ALI Database
MSAG
(Master Street Address Guide)
Wireline Calls
PSTN
(Public Switched Telephone Network)
ANI
(Automatic Number Information)
ALI
(Automatic Location Information)
Exchange
Telephone Company
(Local Exchange Carrier)
PSAP
(Public Safety Answering Point)
Selective Router
Computer Assisted Dispatch System
Emergency Service
Cellular Network
Wireless Calls
Handset based data (Phase II)
Caller Location Information
GPS / a-GPS data
Radiolocation data
Location Database
Network based data (Phase I)
Cell Tower location data

GOALS

- DRIVE THE TIME TO DETECT & REACT
- CONTRIBUTE TO THE COMMUNITY

HOW

- ALERT/EVENT COLLECTION
- AUTOMATION
- COLLABORATION

WHAT (TOOLS)

MISP Threat Sharing

- CYBER THREAT INTELLIGENCE
- INCIDENT RESPONSE
- DIGITAL FORENSICS

WHAT (TAKE TWO)

- LIBRARIES
- SYNAPSE
- 'FEEDERS'

WHO

- THEHIVE CORE TEAM (6 MEMBERS)
- A LARGE COMMUNITY (SOC/CSIRT/CERT)

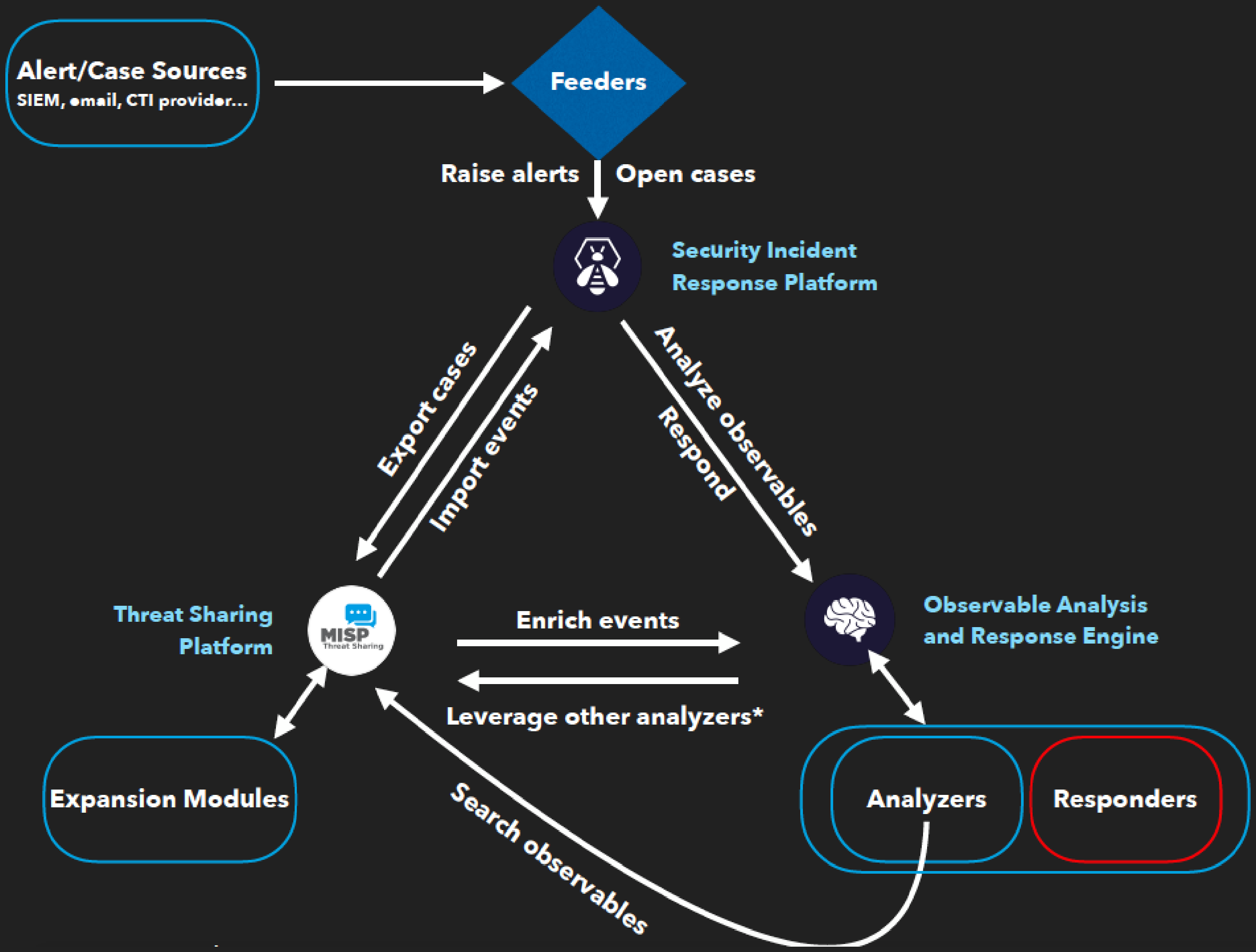
SINCE WHEN

AGPL V3

- OCT 2014 (PRIVATE VERSION)
- NOV 2016 (FLOSS)
- FEB 2017 (CORTEX)

SECURITY INTELLIGENCE

HOW THE SYSTEM WORKS??



Alert/Case Sources
SIEM, email, CTI provider…

Feeders

Raise alerts

Open cases

Security Incident Response Platform

Export cases

Import events

Analyze observables

Respond

Threat Sharing Platform

MISP Threat Sharing

Enrich events

Leverage other analyzers*

Observable Analysis and Response Engine

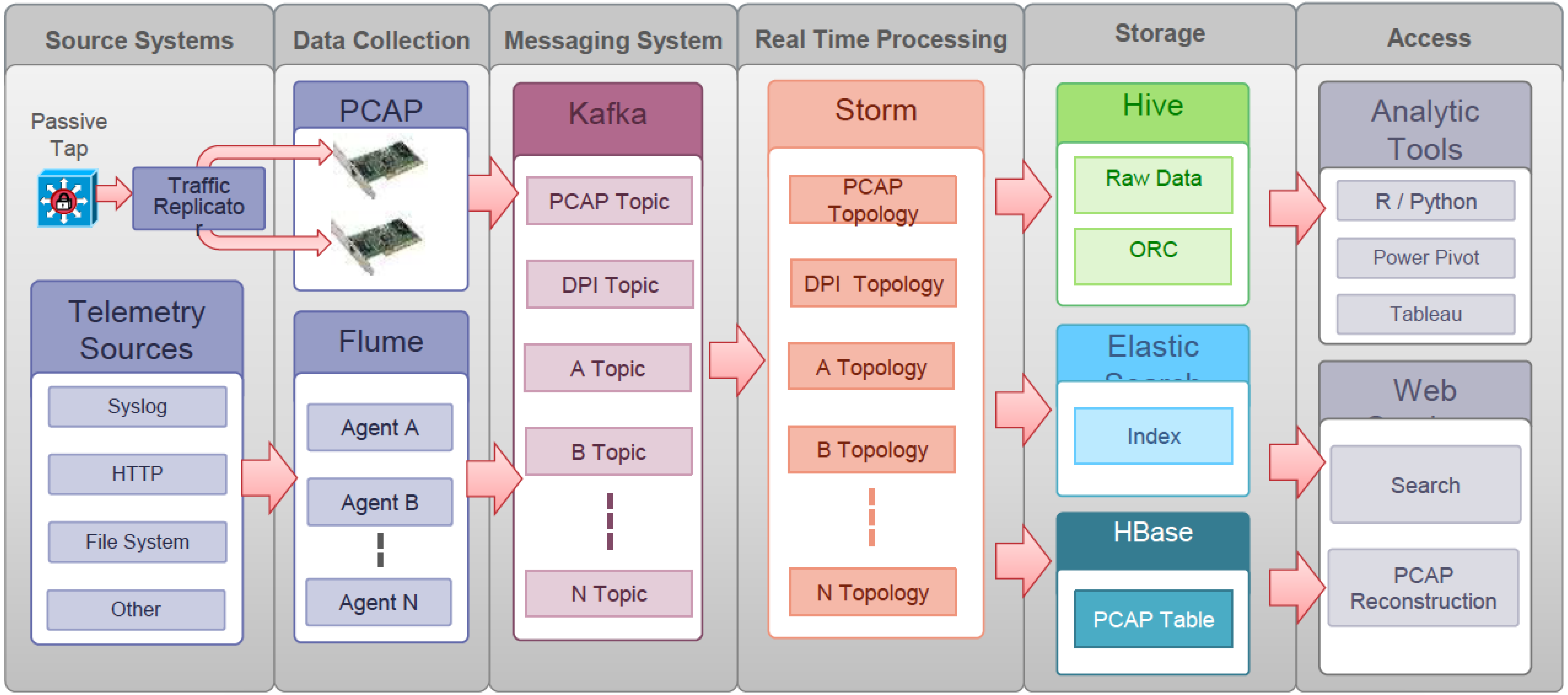
Expansion Modules

Search observables

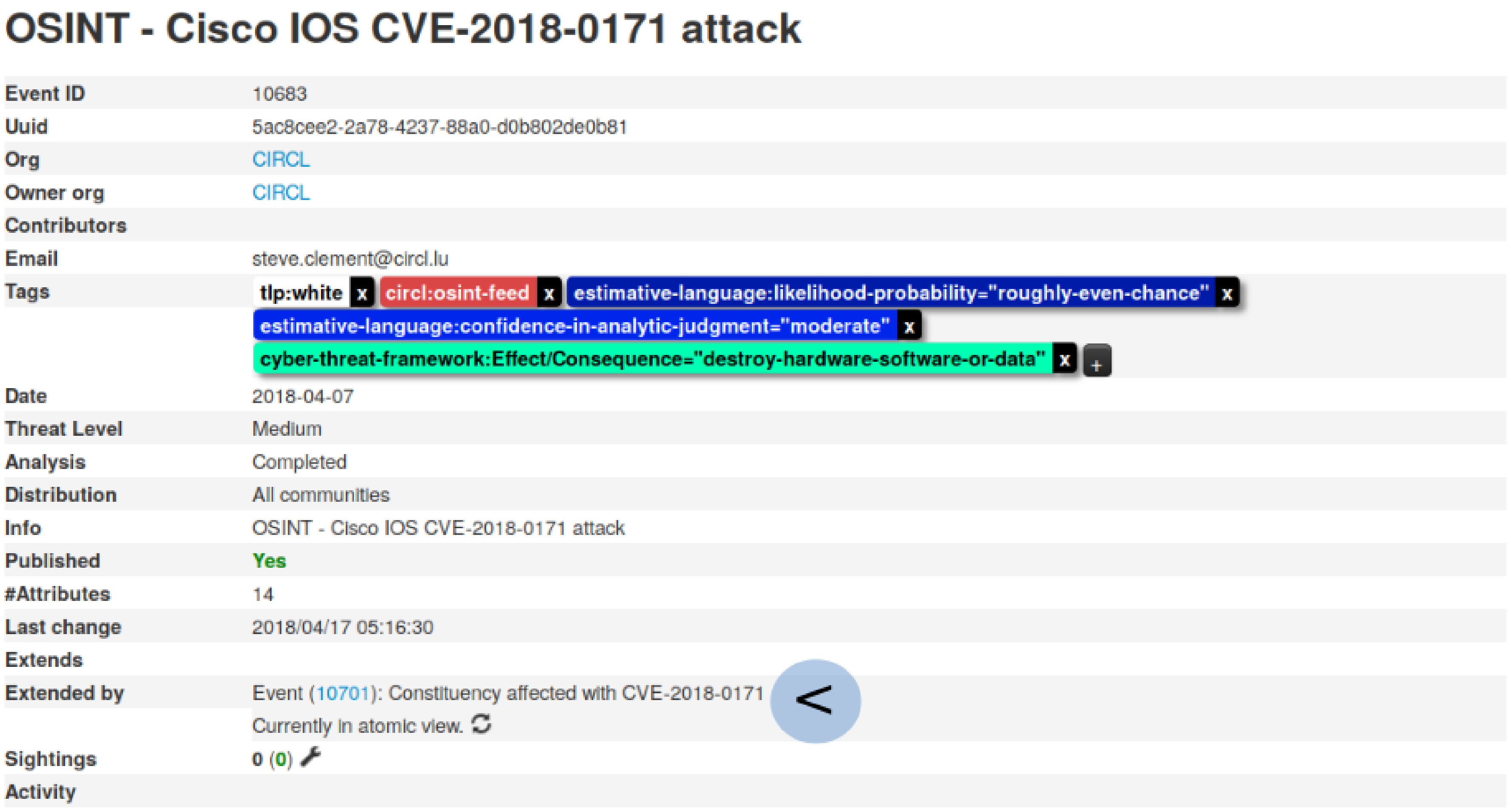
Analyzers

Responders

TECHNICAL OVERVIEW



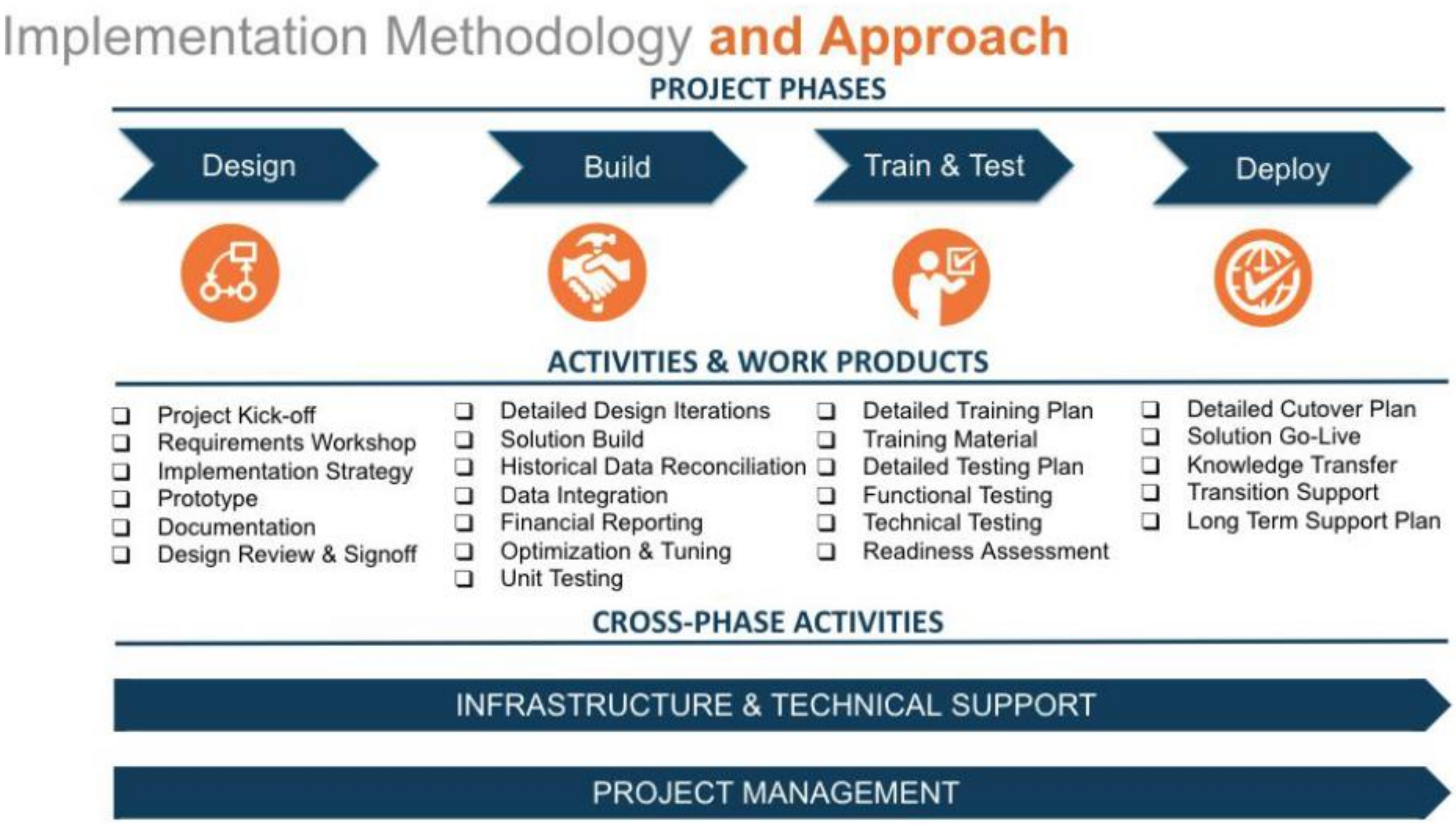
EVENT STRUCTURE - SAMPLE



OSINT - Cisco IOS CVE-2018-0171 attack

Event ID	10683
Uuid	5ac8cee2-2a78-4237-88a0-d0b802de0b81
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	steve.clement@circl.lu
Tags	tlp:white x circl:osint-feed x estimative-language:likelihood-probability="roughly-even-chance" x estimative-language:confidence-in-analytic-judgment="moderate" x cyber-threat-framework:Effect/Consequence="destroy-hardware-software-or-data" x +
Date	2018-04-07
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Info	OSINT - Cisco IOS CVE-2018-0171 attack
Published	Yes
#Attributes	14
Last change	2018/04/17 05:16:30
Extends	
Extended by	Event (10701): Constituency affected with CVE-2018-0171 Currently in atomic view.
Sightings	0 (0)
Activity	

DELIVERY MODEL



Implementation Methodology and Approach

PROJECT PHASES

Design → Build → Train & Test → Deploy

ACTIVITIES & WORK PRODUCTS

Design

- ❑ Project Kick-off
- ❑ Requirements Workshop
- ❑ Implementation Strategy
- ❑ Prototype
- ❑ Documentation
- ❑ Design Review & Signoff

Build

- ❑ Detailed Design Iterations
- ❑ Solution Build
- ❑ Historical Data Reconciliation
- ❑ Data Integration
- ❑ Financial Reporting
- ❑ Optimization & Tuning
- ❑ Unit Testing

Train & Test

- ❑ Detailed Training Plan
- ❑ Training Material
- ❑ Detailed Testing Plan
- ❑ Functional Testing
- ❑ Technical Testing
- ❑ Readiness Assessment

Deploy

- ❑ Detailed Cutover Plan
- ❑ Solution Go-Live
- ❑ Knowledge Transfer
- ❑ Transition Support
- ❑ Long Term Support Plan

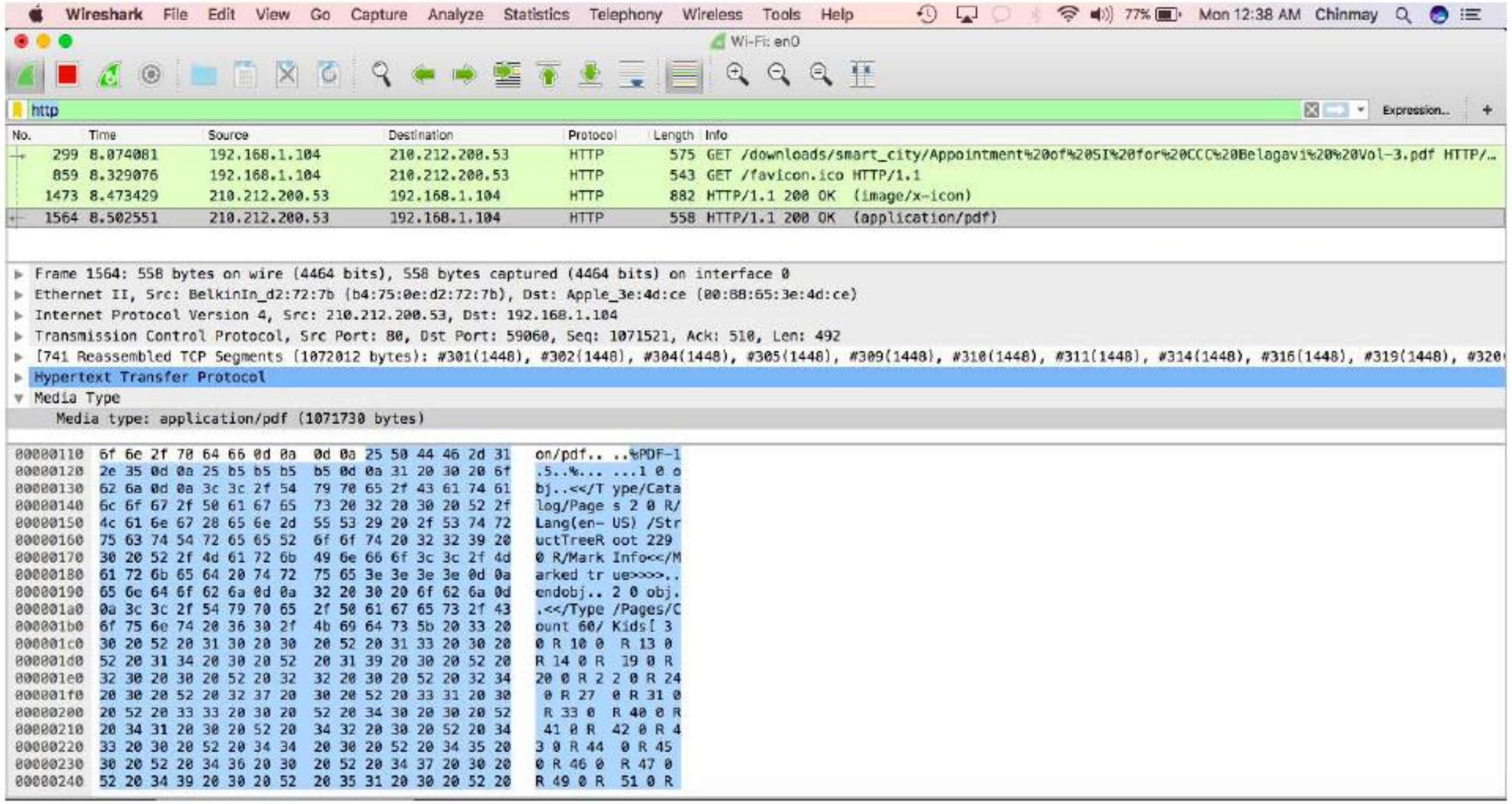
CROSS-PHASE ACTIVITIES

INFRASTRUCTURE & TECHNICAL SUPPORT

PROJECT MANAGEMENT

https://en.wikipedia.org/wiki/List_of_file_signatures

Here is an example in which a PDF file is downloaded from a web server that is serving HTTP protocol – captured using WireShark sniffing tool. PDF being a presentation layer protocol is encapsulated inside the HTTP response, which is application layer protocol. The third window in this picture shows the Hexadecimal signature code of PDF file – 25 50 44 46.



```
http
```

```
No.    Time      Source          Destination     Protocol  Length  Info
  299  8.074081  192.168.1.104   210.212.200.53  HTTP      575  GET /downloads/smart_city/Appointment%20of%20SI%20for%20CCC%20Belagavi%20%20Vol-3.pdf HTTP/…
  859  8.329076  192.168.1.104   210.212.200.53  HTTP      543  GET /favicon.ico HTTP/1.1
 1473  8.473429  210.212.200.53  192.168.1.104   HTTP      882  HTTP/1.1 200 OK  (image/x-icon)
 1564  8.502551  210.212.200.53  192.168.1.104   HTTP      558  HTTP/1.1 200 OK  (application/pdf)
```

```
▶ Frame 1564: 558 bytes on wire (4464 bits), 558 bytes captured (4464 bits) on interface 0
▶ Ethernet II, Src: BelkinIn_d2:72:7b (b4:75:0e:d2:72:7b), Dst: Apple_3e:4d:ce (00:88:65:3e:4d:ce)
▶ Internet Protocol Version 4, Src: 210.212.200.53, Dst: 192.168.1.104
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 59060, Seq: 1071521, Ack: 510, Len: 492
▶ [741 Reassembled TCP Segments (1072012 bytes): #301(1448), #302(1448), #304(1448), #305(1448), #309(1448), #310(1448), #311(1448), #314(1448), #316(1448), #319(1448), #320
▶ Hypertext Transfer Protocol
▼ Media Type
    Media type: application/pdf (1071730 bytes)
```

```
00000110  6f 6e 2f 70 64 66 0d 0a  0d 0a 25 50 44 46 2d 31   on/pdf.. ..%PDF-1
00000120  2e 35 0d 0a 25 b5 b5 b5  b5 0d 0a 31 20 30 20 6f   .5..%... ...1 0 o
00000130  62 6a 0d 0a 3c 3c 2f 54  79 70 65 2f 43 61 74 61   bj..<</T ype/Cata
00000140  6c 6f 67 2f 50 61 67 65  73 20 32 20 30 20 52 2f   log/Page s 2 0 R/
00000150  4c 61 6e 67 28 65 6e 2d  55 53 29 20 2f 53 74 72   Lang(en- US) /Str
00000160  75 63 74 54 72 65 65 52  6f 6f 74 20 32 32 39 20   uctTreeR oot 229 
00000170  30 20 52 2f 4d 61 72 6b  49 6e 66 6f 3c 3c 2f 4d   0 R/Mark Info<</M
00000180  61 72 6b 65 64 20 74 72  75 65 3e 3e 3e 3e 0d 0a   arked tr ue>>>>..
00000190  65 6e 64 6f 62 6a 0d 0a  32 20 30 20 6f 62 6a 0d   endobj.. 2 0 obj.
000001a0  0a 3c 3c 2f 54 79 70 65  2f 50 61 67 65 73 2f 43   .<</Type /Pages/C
000001b0  6f 75 6e 74 20 36 30 2f  4b 69 64 73 5b 20 33 20   ount 60/ Kids[ 3 
000001c0  30 20 52 20 31 30 20 30  20 52 20 31 33 20 30 20   0 R 10 0  R 13 0 
000001d0  52 20 31 34 20 30 20 52  20 31 39 20 30 20 52 20   R 14 0 R  19 0 R 
000001e0  32 30 20 30 20 52 20 32  32 20 30 20 52 20 32 34   20 0 R 2 2 0 R 24
000001f0  20 30 20 52 20 32 37 20  30 20 52 20 33 31 20 30    0 R 27  0 R 31 0
00000200  20 52 20 33 33 20 30 20  52 20 34 30 20 30 20 52    R 33 0  R 40 0 R
00000210  20 34 31 20 30 20 52 20  34 32 20 30 20 52 20 34    41 0 R  42 0 R 4
00000220  33 20 30 20 52 20 34 34  20 30 20 52 20 34 35 20   3 0 R 44  0 R 45 
00000230  30 20 52 20 34 36 20 30  20 52 20 34 37 20 30 20   0 R 46 0  R 47 0 
00000240  52 20 34 39 20 30 20 52  20 35 31 20 30 20 52 20   R 49 0 R  51 0 R 
```

Thank You !

QUESTIONS AND QUERIES…?

Contact: Chinmay Hegde

Cell. +91 99028 25577 | Ph. +91 80 2667 5222

Email: chegde@astrikosconsulting.com / connect@astrikosconsulting.com

www.astrikosconsulting.com

Smart Cities, Smart Villages, Smart Systems and Cyber Security

India: #129, K R Road, Basavangudi, Bangalore – 560004
Singapore: #2 Corporation Road, 01-13, Corporation Place, Singapore – 618494