RSAConference2015
Singapore | 22-24 July | Marina Bay Sands

CHANGE
Challenge today's security thinking

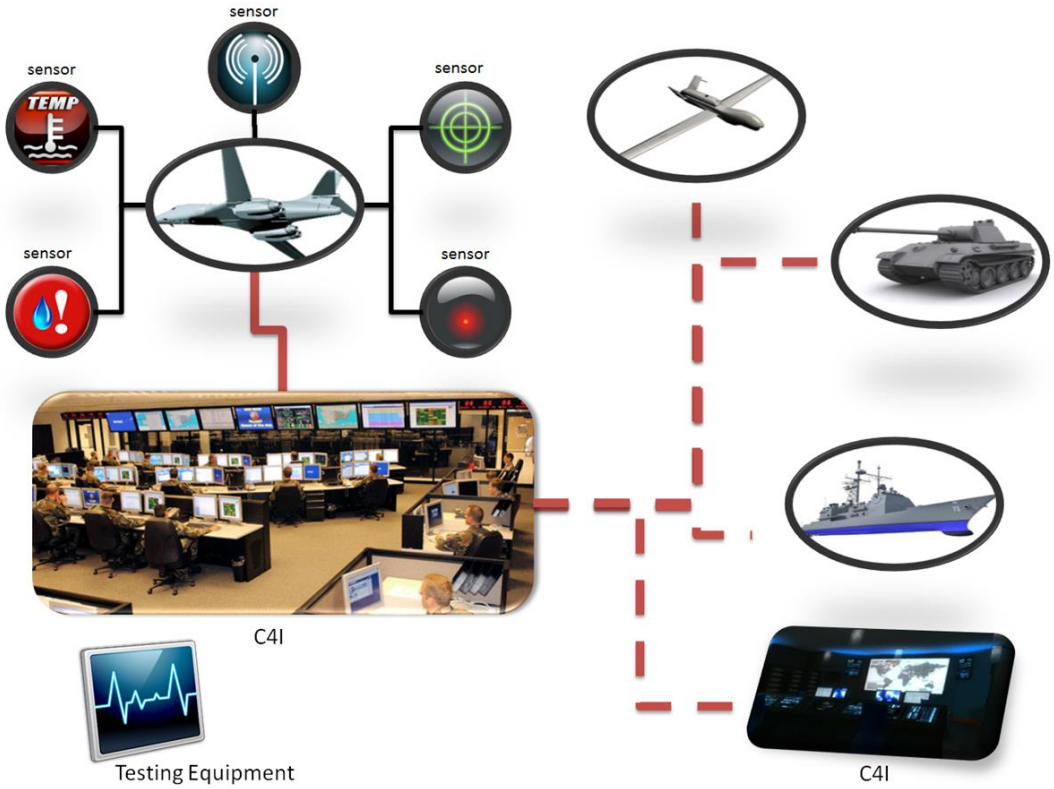
SESSION ID: CLE-F02

Building Blocks of Operational Systems' Cyber Worthiness

Esti Peshin

Director, Cyber Programs
Israel Aerospace Industries (IAI)

Mission Critical Systems (MCS)



4 December 2011: RQ-170 downed by Cyber?

US Officials initially deny a cyber attack and claim the UAV was “shot down”

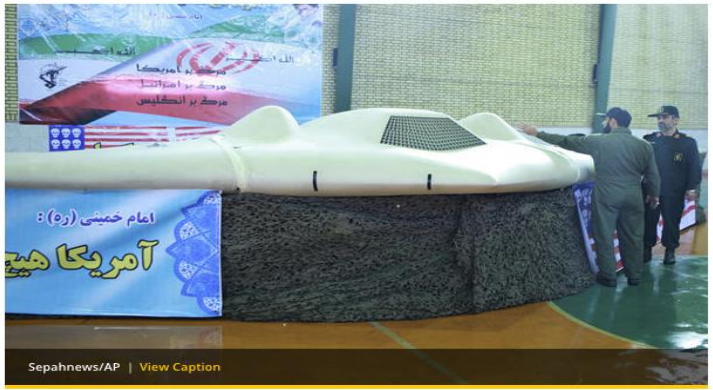
The Christian Science Monitor

WORLD | MIDDLE EAST

Exclusive: Iran hijacked US drone, says Iranian engineer (Video)

In an exclusive interview, an engineer working to unlock the secrets of the captured RQ-170 Sentinel says they exploited a known vulnerability and tricked the US drone into landing in Iran.

By Scott Peterson, Staff writer | Payam Faramarzi*, Correspondent | DECEMBER 15, 2011



Sepahnews/AP | View Caption

ISTANBUL, TURKEY — Iran guided the CIA's "lost" stealth drone to an intact landing inside hostile territory by exploiting a navigational weakness long-known to the US military, according to an Iranian engineer now working on

http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer

November 2014: Test flight of replica UAV

An Iranian copy of a US reconnaissance drone captured in 2011 has carried out its first flight

Iran test-flies 1st US drone replica

Published time: November 10, 2014 15:26 Get short URL

Iranian made drone "Epic" (AFP Photo/ISNA News)

3

An Iranian copy of a US reconnaissance drone captured in 2011 has carried out its first flight, and the Revolutionary Guards have declared the test a success.

Tags
Drones, Intelligence, Iran, SciTech, Security

http://rt.com/news/204043-iran-drone-copy-spy/

Can it be done ?

There is a proliferation of information on cyber vulnerabilities in UAVs

On the Requirements for Successful GPS Spoofing Attacks

Nils Ole Tippenhauer
Dept. of Computer Science
ETH Zurich, Switzerland
tinils@inf.ethz.ch

Christina Pöpper
Dept. of Computer Science
ETH Zurich, Switzerland
poepperc@inf.ethz.ch

Kasper B. Rasmussen
Computer Science Dept.
UCI, Irvine, CA
kbrasmus@ics.uci.edu

Srdjan Čapkun
Dept. of Computer Science
ETH Zurich, Switzerland
capkuns@inf.ethz.ch

We will show, for example, that any number of receivers can easily be spoofed to one arbitrary location; however, the attacker is restricted to only few transmission locations when spoofing a group of receivers while preserving their constellation.

In addition, we investigate the practical aspects of a satellite-lock takeover, in which a victim receives spoofed signals after first being locked on to legitimate GPS signals. Using a civilian GPS signal generator, we perform a set of experiments and find the minimal precision of the attacker's spoofing signals required for covert satellite-lock takeover.

October 2011: Academic researchers publish a research on GPS spoofing

http://www.syssec.ethz.ch/research/ccs139-tippenhauer.pdf

Can it be done ?

There is a proliferation of information on cyber vulnerabilities in UAVs

BBC News Sport Weather Earth Future Shop

NEWS TECHNOLOGY

Home UK Africa Asia Australia Europe Latin America Mid-East US & Canada Business Health

29 June 2012 Last updated at 10:54 GMT

Share

Researchers use spoofing to 'hack' into a flying drone

American researchers took control of a flying drone by "hacking" into its GPS system - acting on a $1,000 (£640) dare from the US Department of Homeland Security (DHS).

A University of Texas at Austin team used "spoofing" - a technique where the drone mistakes the signal from hackers for the one sent from GPS satellites.

The same method may have been used to bring down a US drone in Iran in 2011.

Analysts say that the demo shows the potential danger of using drones.

Drones are mostly used for military operations

Related Stories

Tests begin on

June 2012: Researchers demonstrate a GPS spoofing attack, following a dare by US DHS

http://www.bbc.com/news/technology-18643134

Can it be done ?

There is a proliferation of information on cyber vulnerabilities in UAVs

DIY DRONES
The Leading Community for Personal UAVs

3D ROBOTICS

How to spoof GPS to (potentially) take over a drone

Posted by Chris Anderson on July 1, 2012 at 1:16pm View Blog

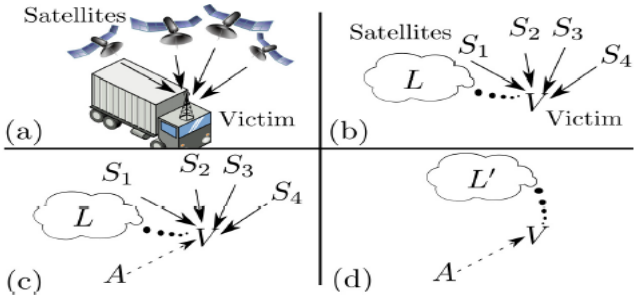


Figure 2: Basic attack scenario. (a) Visualization of the setup. The victim uses a GPS-based localization system and is synchronized to the legitimate satellites. (b) Abstract representation of the scene. (c) The attacker starts sending own spoofing and jamming signals. (d) The victim synchronizes to the attacker's signals.

July 2012: Popular blogs publish extracts of the landmark academic article

http://diydrones.com/profiles/blogs/how-to-spoof-gps-to-potentially-take-over-a-drone

IAI

Can it be done ?

There is a proliferation of information on cyber vulnerabilities in UAVs

2013 5th International Conference on Cyber Conflict
K. Podins, J. Stinissen, M. Maybaum (Eds.)
2013 © NATO CCD COE Publications, Tallinn

The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment

Kim Hartmann
Institute of Electronics, Signal Processing and Communication
Otto-von-Guericke-University
Magdeburg, Germany
kim.hartmann@ovgu.de

Christoph Steup
Department of Distributed Systems
Otto-von-Guericke-University
Magdeburg, Germany
steup@ovgu.de

June 2013: NATO Center of Excellence publishes a detailed cyber risk analysis for UAVs

Table II. Risk assessment results for commonly used communication links

Link type	Integrity	Confidentiality	Availability
K_u-band	0.1	0.1	0.1
C-Band	0.1	0.5	0.5
WiFi a	0.1	0.9	0.9
WiFi b	0.1	0.9	1
WiFi g	0.1	0.9	1
WiFi n	0.1	0.9	0.9
No encryption	0	0.9	0
No signature	0.9	0	0

http://ccdcoe.org/publications/2013proceedings/d3r2s2_hartmann.pdf

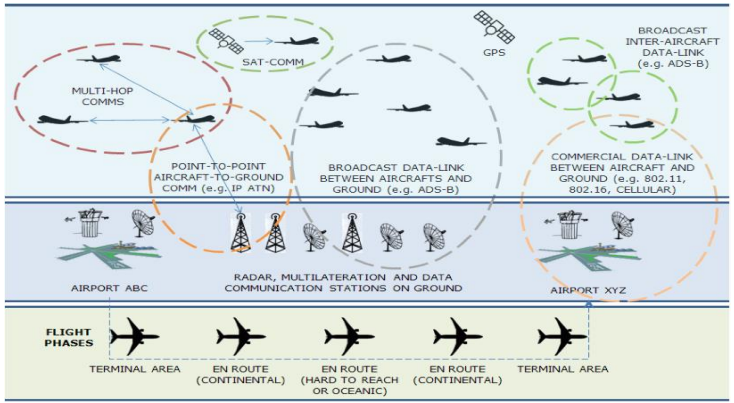
MCS Hardening - Challenges

- Proprietary and varying protocols & systems, which:
  - Do not include patch management, advanced authentications, etc.
  - Do not include built in security measures as part of their design
  - Lack documentation
- Challenging topology: Autonomous/field systems, Remote maintenance
- Challenging hardening process:
  - Extensive functionality and regression testing required
  - Real Time
  - Lack of domain knowledge to harden proprietary systems & protocols
- Proliferation of “how to” information on hacking MCS

Commercial Aviation at Risk

Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices

Andrei Costin, Aurélien Francillon
Network and Security Department
EURECOM
Sophia-Antipolis, France
Email: andrei.costin@eurecom.fr, aurelien.francillon@eurecom.fr



August 2012: Researcher demonstrates cyber vulnerabilities in ADS-B (Automatic Dependent Surveillance Broadcast) devices

http://www.s3.eurecom.fr/docs/bh12us_costin.pdf
http://www.s3.eurecom.fr/slides/bh12us_costin.slides.pdf

Commercial Aviation at Risk

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS **SECURITY** BUSINESS HARDWARE SCIENCE BOOTNOTES VIDEO

Researcher hacks aircraft controls with Android smartphone

This may give the TSA some ideas

11 Apr 2013 at 01:12, Iain Thomson 124

A presentation at the Hack In The Box security summit in Amsterdam has demonstrated that it's possible to take control of aircraft flight systems and communications using an Android smartphone and some specialized attack code.

Hugo Teso, a security researcher at N.Runs and a commercial airline pilot, spent three years developing the code, buying second-hand commercial flight system software and hardware online and finding vulnerabilities within it. His presentation will cause a few sleepless nights among those with an interest in aircraft security.

Teso's attack code, dubbed SIMON, along with an Android app called PlaneSploit, can take full control of flight systems and the pilot's displays. The hacked aircraft could even be controlled using a smartphone's accelerometer to vary its course and speed by moving the handset about.

April 2013: Researcher demonstrates aircraft hack via Android Smartphone

http://www.theregister.co.uk/2013/04/11/hacking_aircraft_with_android_handset/

Commercial Aviation at Risk

IOActive™
Comprehensive Information Security

August 2014: Vulnerabilities in Satellite Communication devices

http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

Commercial Aviation at Risk

TECH TIMES

Hacker claims commercial flights at risk for cyberattacks

By **Mark Hawver**, Tech Times | August 4, 4:04 PM

SHARE(10) TWEET(14) 0 COMMENTS

A cybersecurity researcher has found exploitable flaws in satellite communications equipment that could be hacked, possibly allowing disruptions and takeovers of navigation, communications and safety systems on commercial jets. Hackers could use a plane's Wi-Fi or inflight entertainment systems to exploit these flaws.
(Photo : Wiki Commons)

August 2014: WiFi flaws can impact aircraft controls (via SATCOM)

http://www.techtimes.com/articles/12057/20140804/hacker-claims-jet-flights-risk-cyber-attacks.htm

Commercial Aviation at Risk

Technology Secure + protect

Hacking planes - UK researchers developing plans to stop 'flight cyberjacking'

Theoretical vulnerabilities mean that a 'cyber bomb' could be possible, yet attacks are limited in their scope and extremely complex to carry out

Vulnerabilities in satellite and communications software theoretically mean that hackers could install malicious firmware under certain circumstances, a researcher has said Photograph: Julian Stratenschulte/EPA

November 2014: Researchers looking into flight "cyber-jacking" in the wake of MH-370 disappearance

http://www.theguardian.com/technology/2014/nov/04/hacking-planes-uk-researchers-developing-plans-to-stop-flight-cyberjacking

Commercial Aviation at Risk

United States Government Accountability Office

Report to Congressional Requesters

AIR TRAFFIC CONTROL

FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen

April 2015: GAO: NextGen IP-Based ATC systems introduce inherent cyber risks !

http://www.gao.gov/assets/670/669627.pdf

Commercial Aviation at Risk

- GAO Findings: As the agency transitions to the Next Generation Air Transportation System (NextGen), the Federal Aviation Administration (FAA) faces cybersecurity challenges in at least three areas:
  - Protecting air-traffic control (ATC) information systems,
  - Protecting aircraft avionics used to operate and guide aircraft (also due to internet connection)
  - Clarifying cybersecurity roles and responsibilities among multiple FAA offices

Commercial Aviation at Risk

theguardian
Winner of the Pulitzer prize 2014

United Airlines bars security researcher from flight after tweet about hacking

Chris Roberts was prevented from boarding flight from Colorado to San Francisco following joking post that said he could get oxygen masks to deploy

April 2014: Hacker removed from a flight after joking about hacking into the plane systems

http://www.theguardian.com/business/2015/apr/19/united-airlines-security-researcher-chris-roberts-hacking

Commercial Aviation at Risk

FBI: Hacker claimed to have taken over flight's engine controls

By Evan Perez, CNN Updated 0219 GMT (0919 HKT) May 19, 2015

Man claims entertainment system helped him hack plane 02:09

May 2014: Hacker admitted hacking into on board entertainment, overwriting codes, and issuing commands !

http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/

Commercial Aviation at Risk

USA TODAY
A GANNETT COMPANY

Cyber attack targets LOT airline; CEO warns 'it can happen to anyone'

TODAY IN THE SKY

Ben Mutzabaugh, USA TODAY 11:32 a.m. EDT June 22, 2015

(Photo: Czarek Sokolowski, AP)

25 CONNECT | 46 TWEET | 36 LINKEDIN | COMMENT | EMAIL | MORE

An apparent hack attack forced Polish carrier LOT had to cancel about 10 flights Sunday, grounding about 1,400 passengers.

LOT spokesman Adrian Kubicki tells The Associated Press hackers temporarily paralyzed the company's

June 2014: Hack paralyzed airline's computers, flight plans could not be generated

http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/

Interim Conclusions

- There is a proliferation of “how to” information
  - Academic researches
  - Popular blogs
  - Reports of experiments
- Essentially – a “blue print” for hackers
- Cyber hardening of Mission Critical Systems is a MUST !

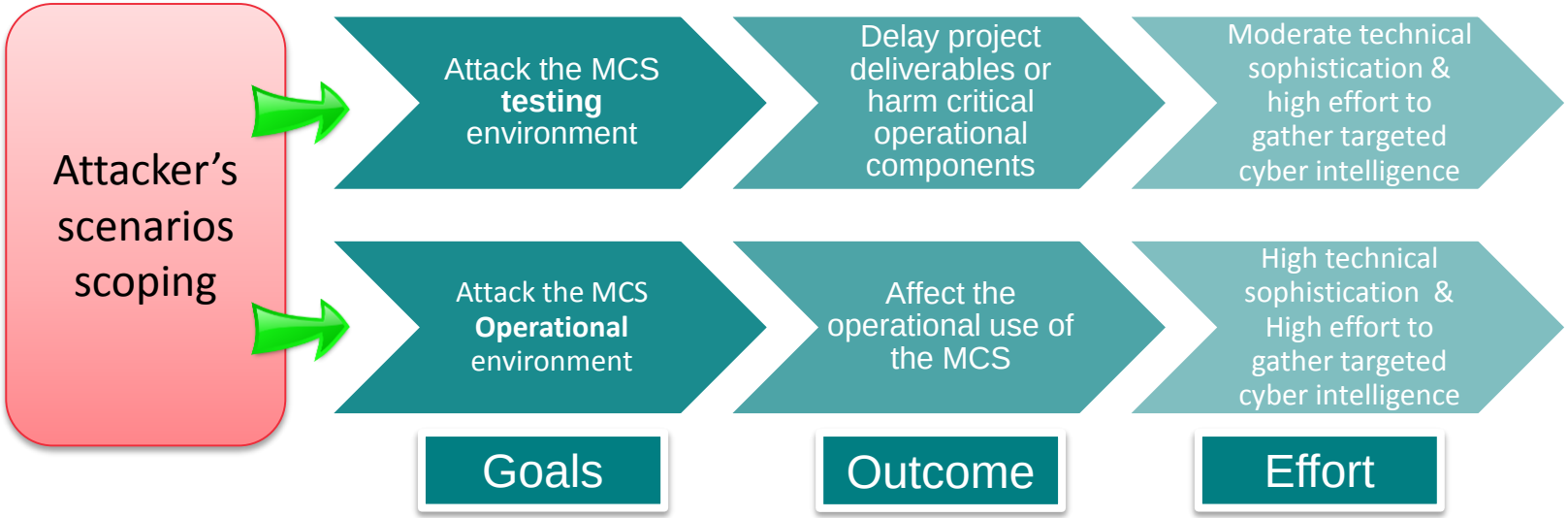
RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

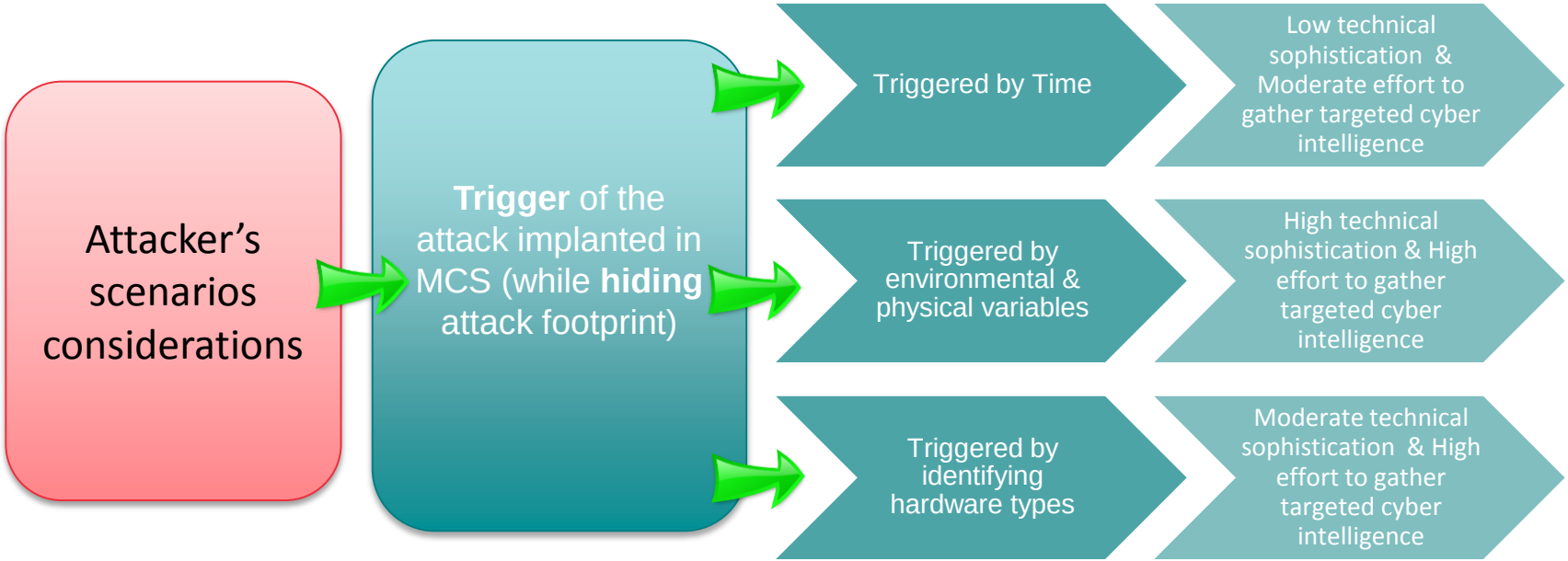
Mission Critical Systems (MCS) – Understanding the Attacker's Point of View

#RSAC

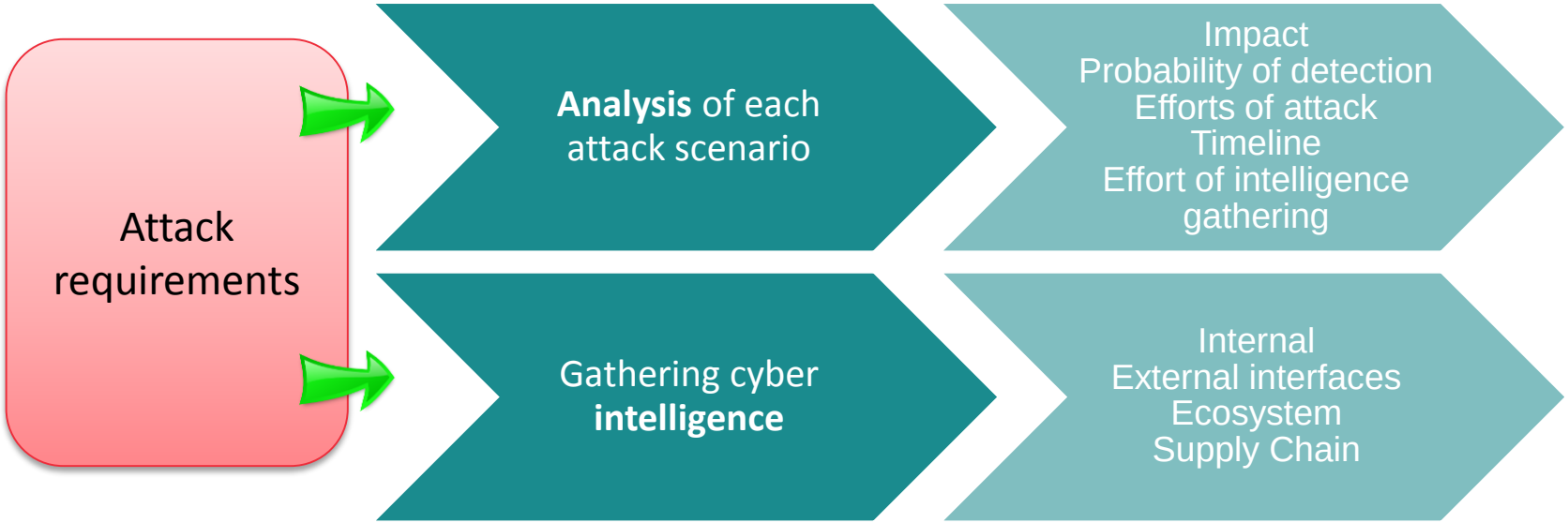
Understanding the Attacker's Point Of View



Understanding the Attacker's Point Of View



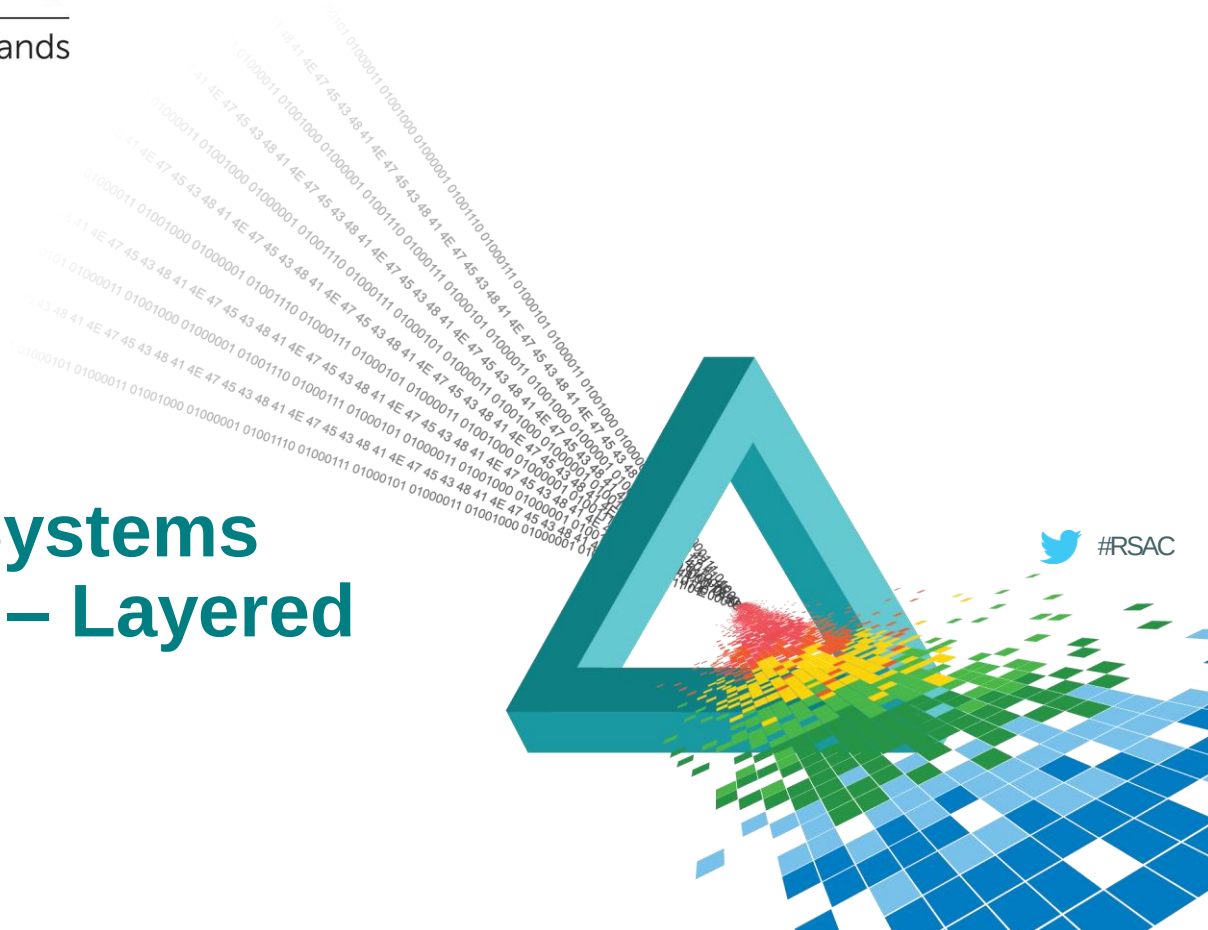
Understanding the Attacker's Point Of View



RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Mission Critical Systems (MCS) Hardening – Layered Approach



#RSAC

MCS Hardening – A Layered Approach

MCS Hardening – Phased Implementation

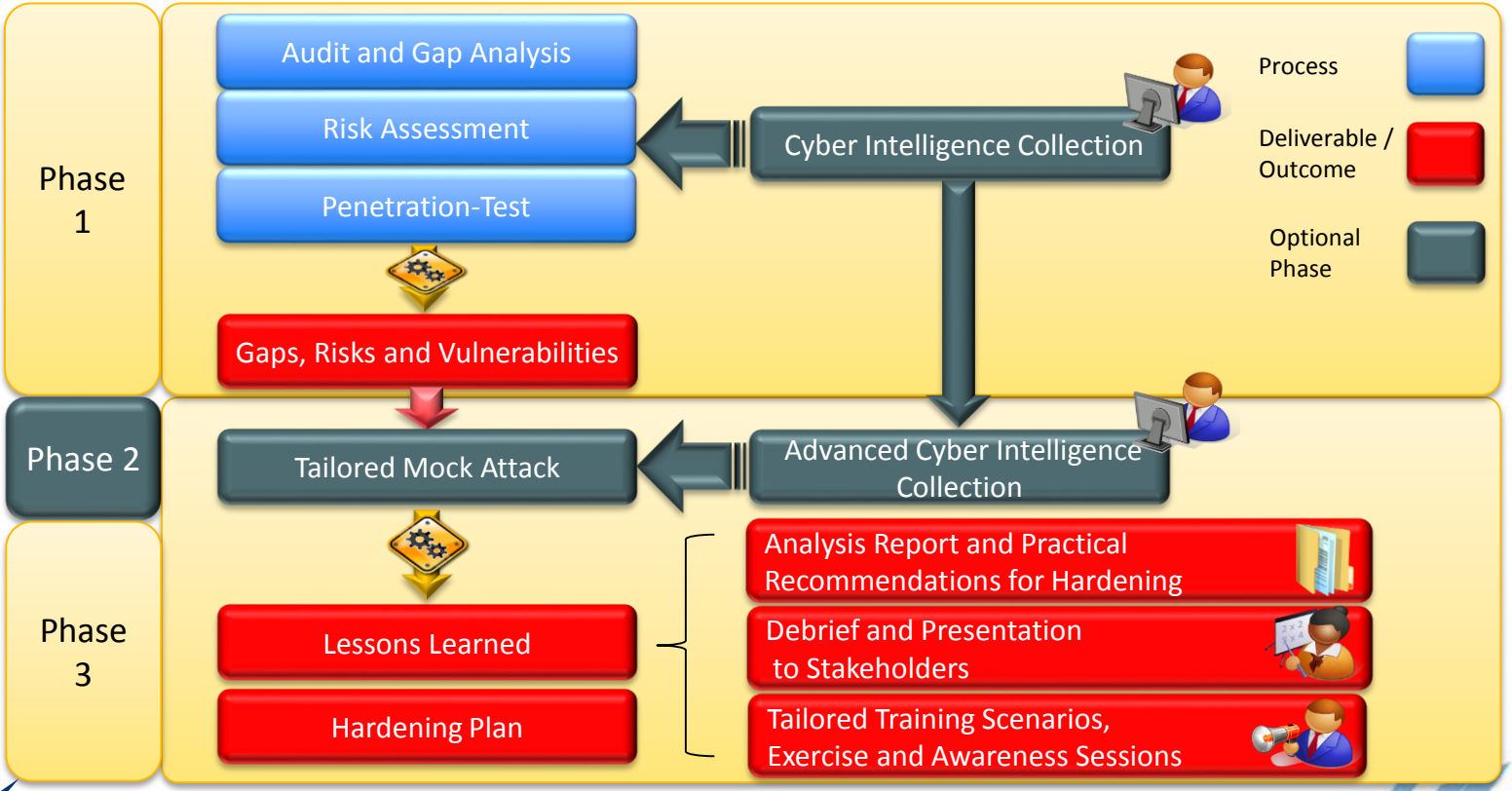
Holistic Coverage

- Component Level
- System Level
- Eco System

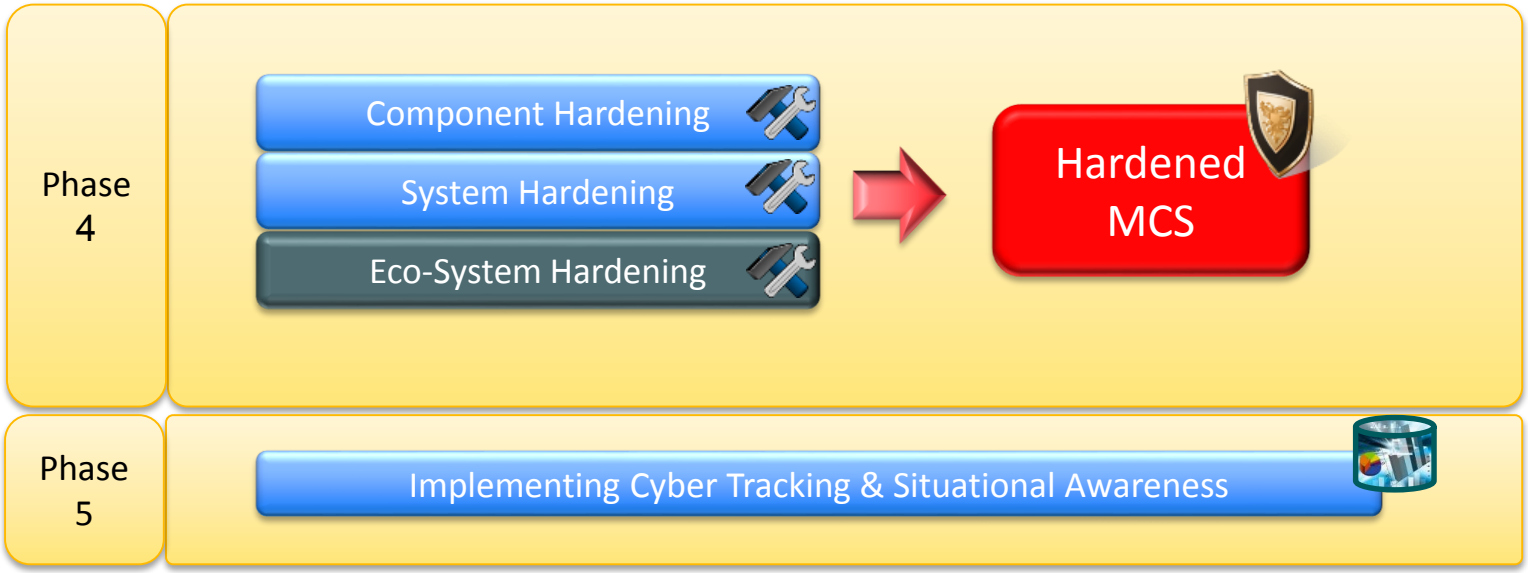
Phased Approach

- Phase 1 – System Level Analysis
- Phase 2 – Eco System Modelling
  - Analysis of critical components
  - Supply Chain vulnerabilities
  - OSINT analysis of eco-system
- Phase 3 – Customized Hardening

MCS Hardening - Approach Overview



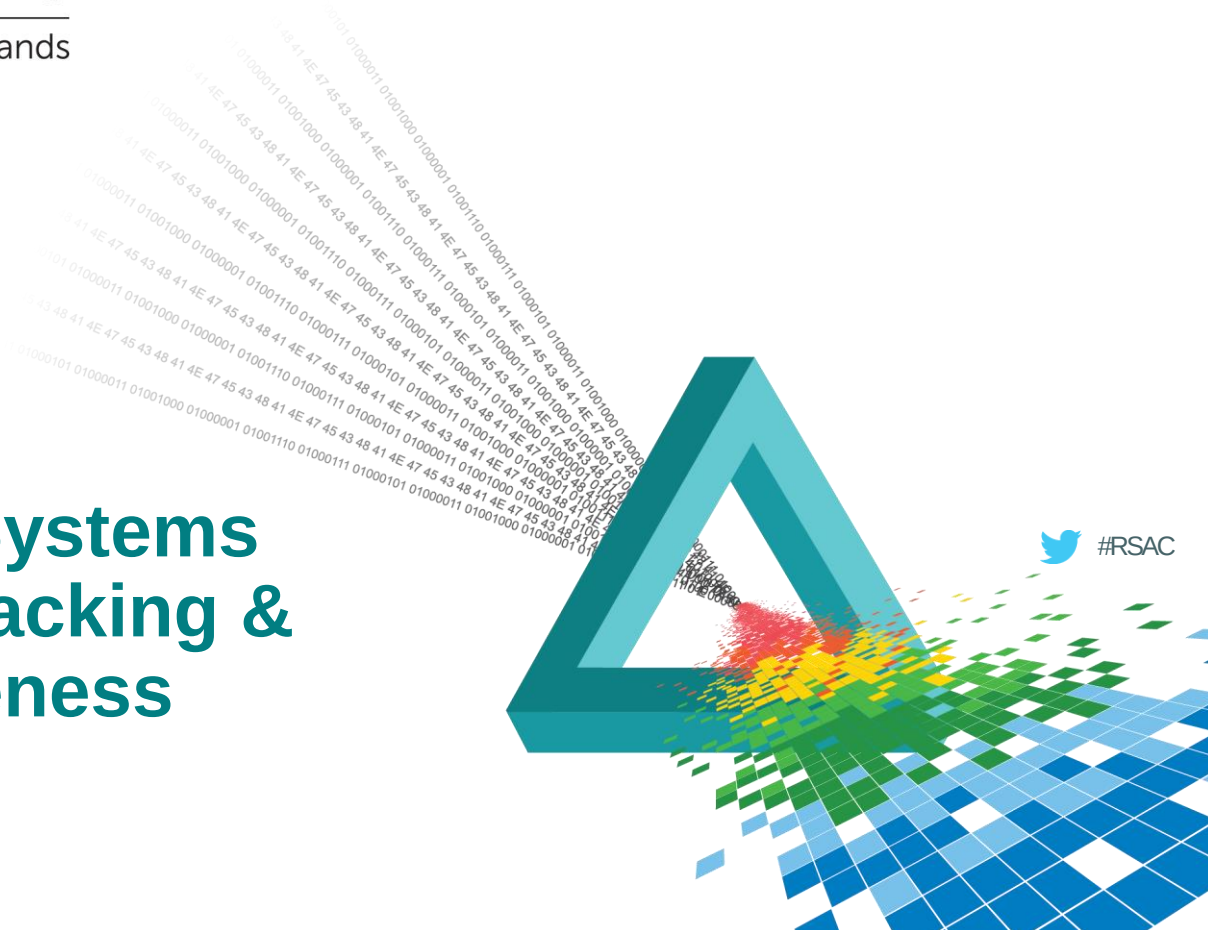
MCS Hardening - Approach Overview



RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

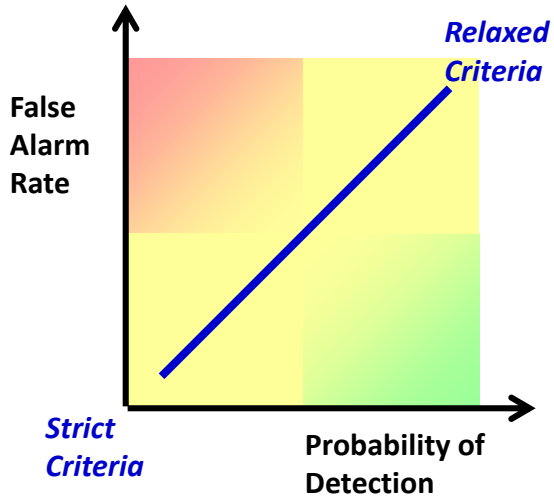
Mission Critical Systems (MCS) – Cyber Tracking & Situational Awareness



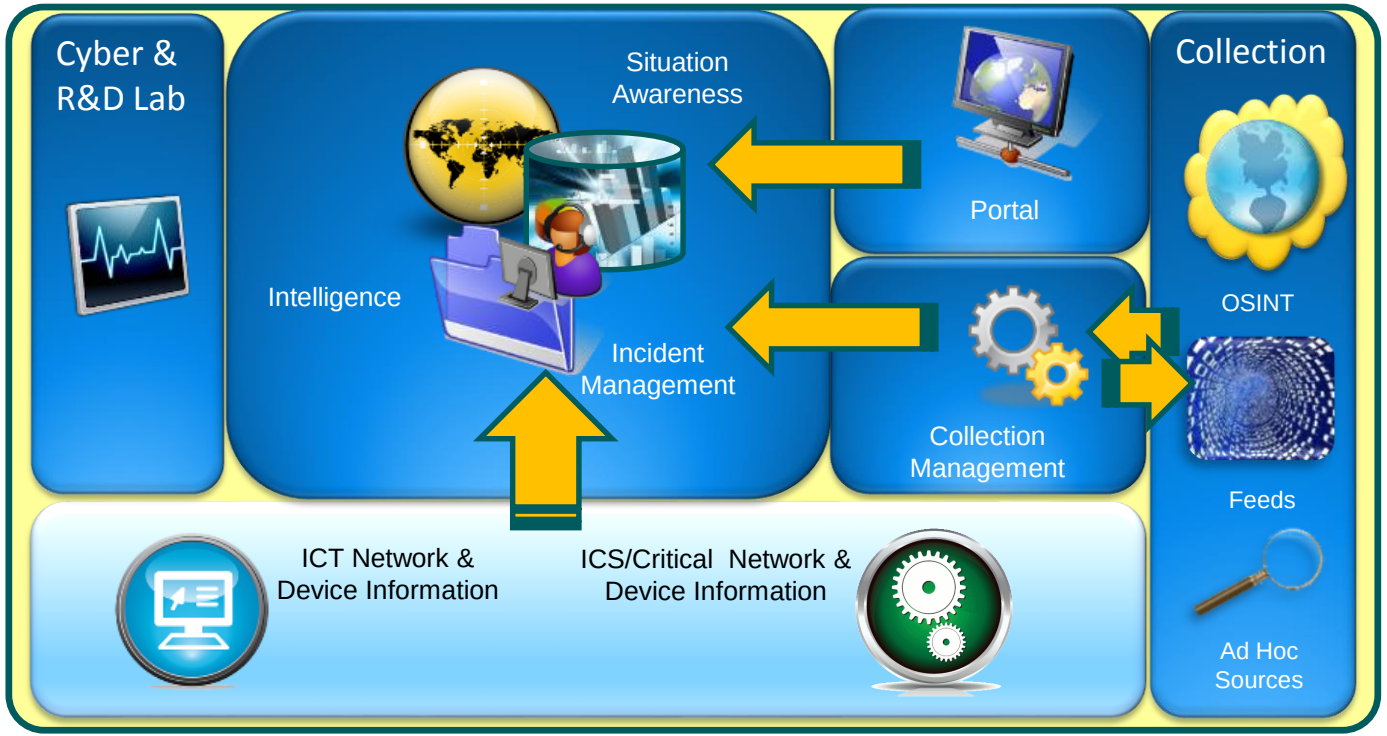
#RSAC

How effective is Cyber Situational Awareness ?

- Huge & diverse amounts of data
  - Maintaining effective coverage
  - Deriving effective insight
- Attacker/defender asymmetry
  - Proliferation of attack capabilities
  - Multiple and bogus identities
- Identifying subtle activities
  - Sophisticated attacks
- **Many false positives !**



Achieving Cyber Situational Awareness



Cyber Multi-Hypothesis Analysis (MHA)

- Multi-Hypothesis Analysis (MHA)
  - A method for handling complex & dynamic data
  - which is collected with various sources/sensors
  - which involves many entities,
  - whose information is partial and/or ambiguous as well as dynamically changing
- MHA can be applicable to **Cyber Situation Awareness**
  - Integrating various security tools & techniques
  - Integrating different processing & analysis engines
- **Multi-Hypothesis Analysis (MHA)** is a powerful method **to handle the uncertainty**

Cyber Tracking

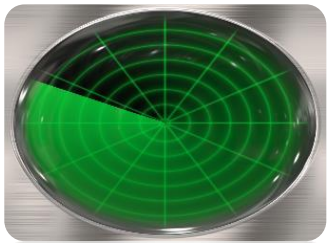
- **Tracking is** the process of **associating events** (data) including past events
- Generating a logical track of events enables
  - **Verification** of data consistency
  - **Identifying** the past origin of the track
  - **Predicting** the future evolution of the track

Multi Hypothesis Tracking (MHT)

Backward ← t → **Forward**

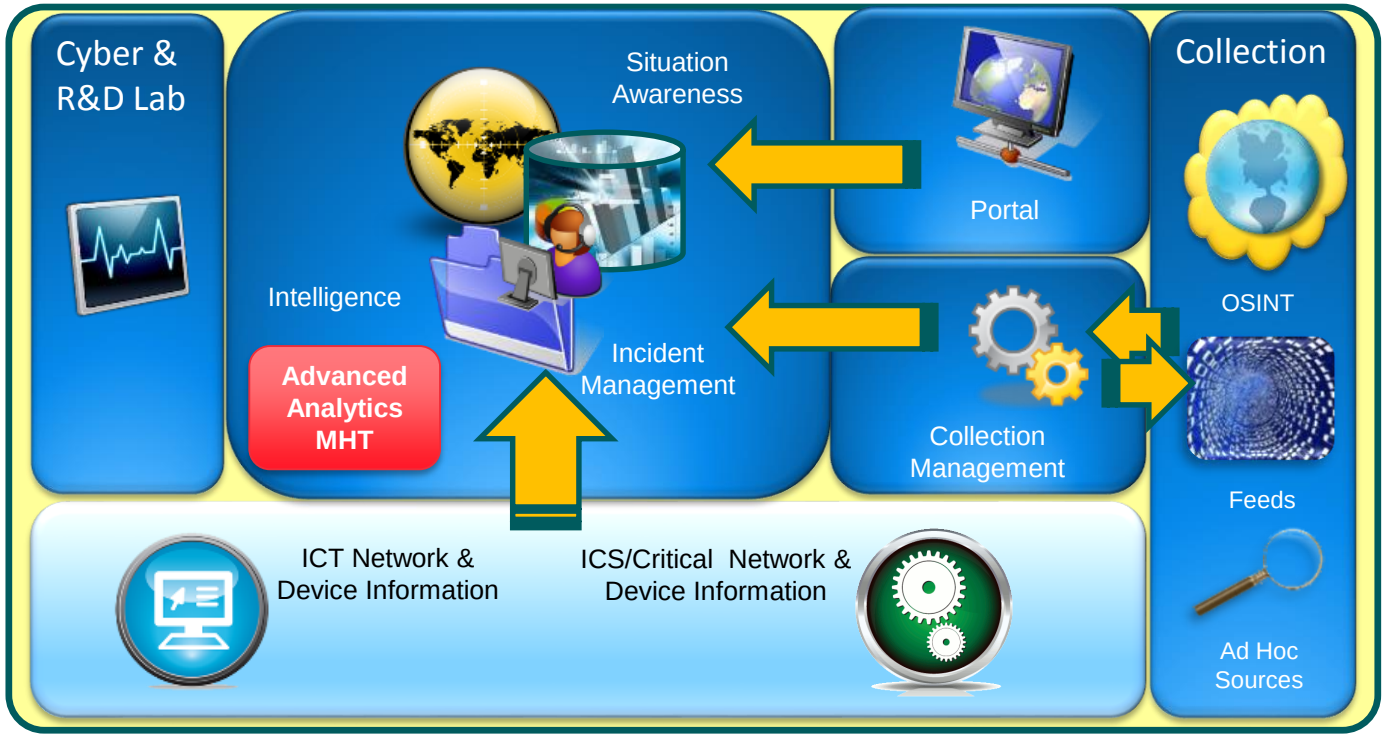
- Confirm information consistency
- Investigate overlooked or dropped events
- Look for actor trend & behavior

- Predict expected information
- Guide monitoring to suspicious paths
- Project situation evolution to assess impact



Situational Awareness

Effective Cyber Situational Awareness



Two Complementary Approaches

- Layered Approach
  - Protection & Prevention
  - Predication & Detection (via Situational Awareness)
  - Result: Mitigation & Action
- Cyber Tracking & Situational Awareness
  - Activity monitored (also) via info from Layered Defense
  - Predication, Detection, Intentions, Context & Impact
  - Result: Situational Awareness

Apply What You Have Learned Today

- Next week you should:
  - Identify Mission Critical System within your organization
- In the first three months following this presentation you should:
  - Identify a trusted consultant, with proven experience in the MCS & cyber hardening domains
  - Conduct a system-level analysis
  - Potentially, conduct an eco-system modeling

Apply What You Have Learned Today

- Within six months you should:
  - Establish an operational process/method for hardening MCS
  - Initiate the deployment of a Cyber & R&D Lab
  - Initiate an implementation project to close hardening gaps
  - Initiate an implementation project for situational awareness