NETITUDE

EXCELLENCE AS STANDARD

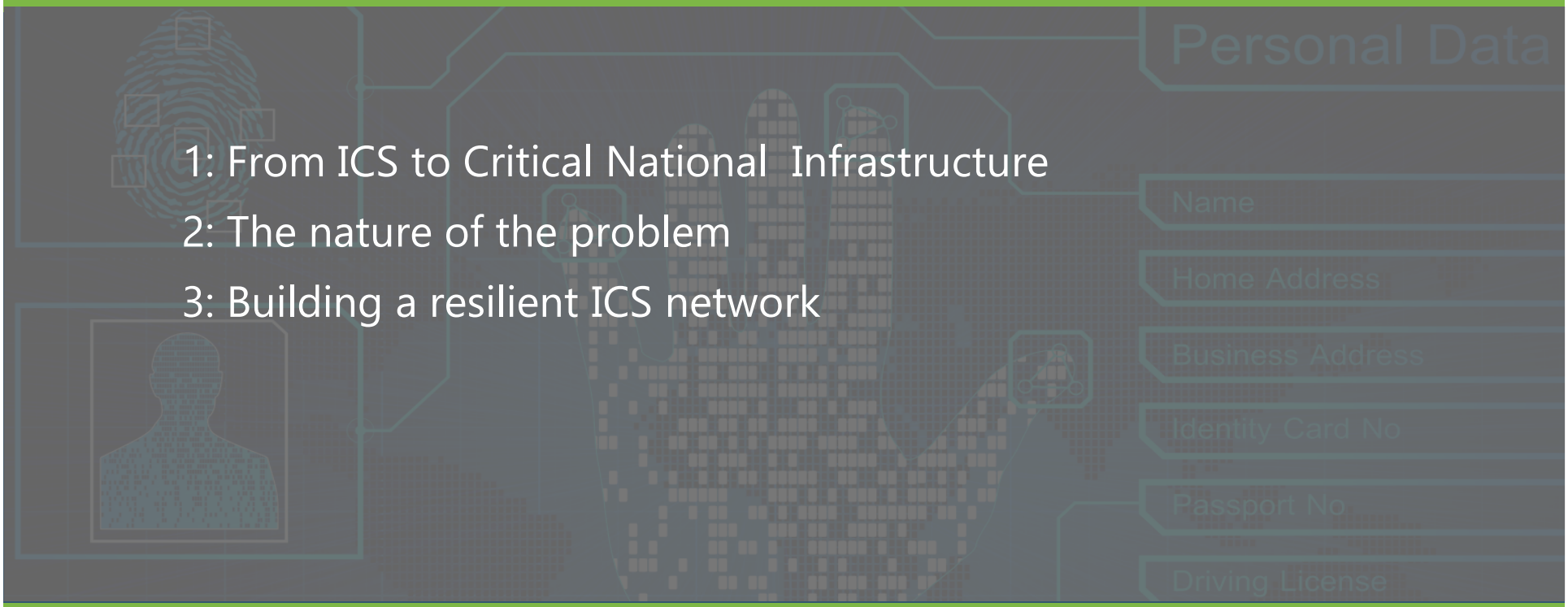
Building a resilient ICS

By Dr Jules Pagna Disso, @julesdisso

NETTITUDE

EXCELLENCE AS STANDARD

Building a resilient Industrial Control System (ICS)



1: From ICS to Critical National Infrastructure

2: The nature of the problem

3: Building a resilient ICS network

1: From ICS to Critical National Infrastructure

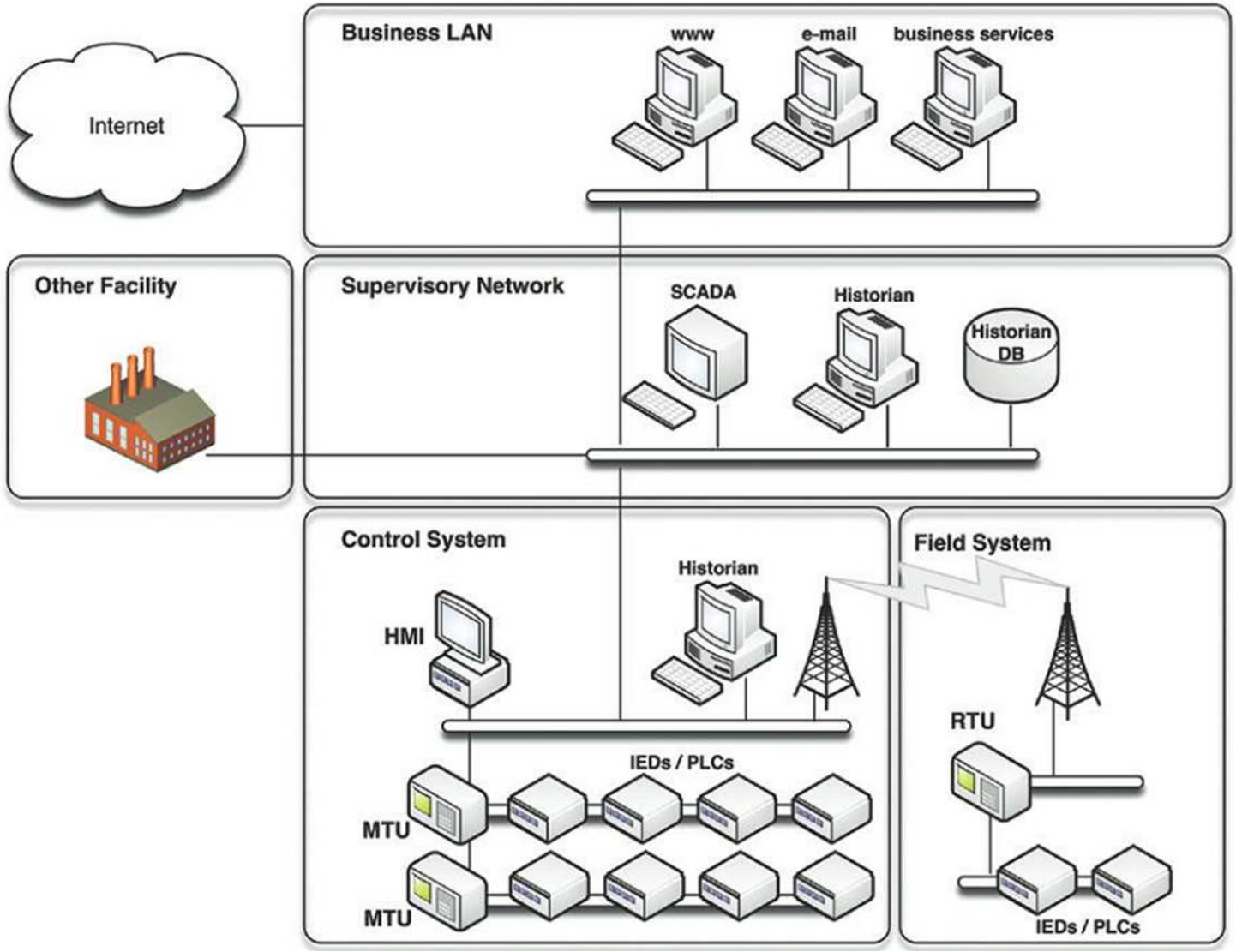
"To know your enemy, you must become your enemy."
— Sun Tzu

NETTITUDE

:: A critical view of ICS – important definitions

- The buzz word: SCADA security
- Industrial Control Systems are often referred to in the media as “SCADA,” which is both inaccurate and misleading
- Industrial network is most typically made up of several distinct areas:
  - Business network or enterprise
  - Business operations
  - A supervisory network
  - Process and control networks
- SCADA or Supervisory Control and Data Acquisition is one piece of the Supervisory Network
- Industrial Network is any network operating some sort of automated control system that communicates digitally over a network

:: A critical view of ICS - Typical ICS Infrastructure



:: A critical view of ICS - Main Components

- PLC: Programmable Logic Controller
- Digital embedded computer used for automating the function of electromechanical processes such as controlling factory assembly lines
- PLC are designed for multiple inputs and outputs arrangements.
- Programs are generally stored in non volatile memory
- Automation or automatic control
- Use of control system to control equipment, processes in factorys, boilers and heat treating ovens, aircraft and other applications with minimal or reduced human intervention

:: A critical view of ICS - RTU

- RTU: Remote Terminal Unit

- Purpose-built controller designed for specific applications
  - Water Quality Analyser
  - Flow Calculators
  - Pipeline Leak Detectors
  - Tank Gas Emission Control
  - Boiler Control
  - Gas Quality Analysers
  - Etc.
- Pre-configured for specific purposes. Generally performs limited control function

:: A critical view of ICS - IEDs

- IED: Intelligent Electronic Devices
- Specific controllers that are used in the Electric Power industry, can sense variations in voltage, current, or frequency
- They can raise or lower voltage levels in order to maintain the desired level or signal disconnect switches to break open the line to save the rest of the grid due to a surge or large swing in voltage, current, or frequency
- Main Functions
  - Protection
  - Control
  - Monitoring
  - Metering
  - Communication

:: A critical view of ICS - Data Historian

- Architected to efficiently gather and disseminate plant data (typically temperature, pressure, level, flows) from a variety of plant systems (dcs, plc, scada, etc.) to form a complete context of manufacturing situation.

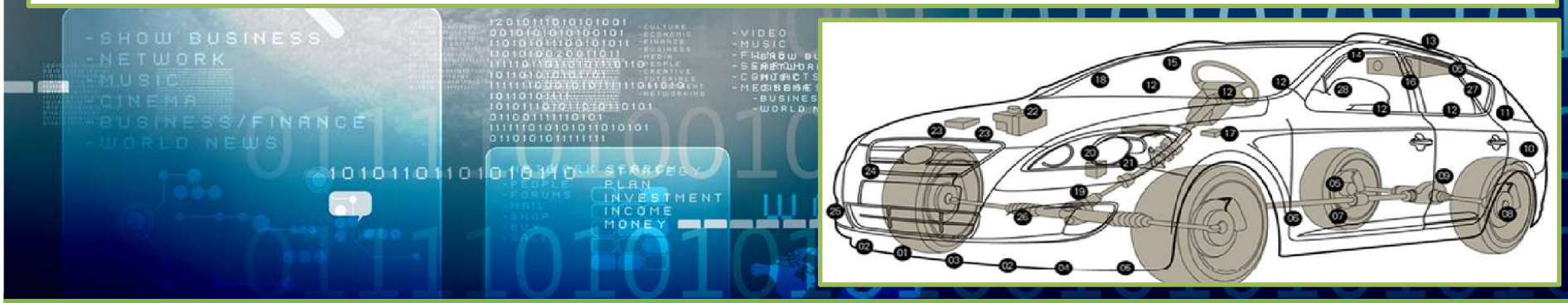
- Due to their excellent analytical capability, historians can be used for the short term, but excel at managing over a longer time horizon

- Wide range of capabilities including finding patterns in the data for root cause analysis. Can easily download information into spreadsheets for further analysis

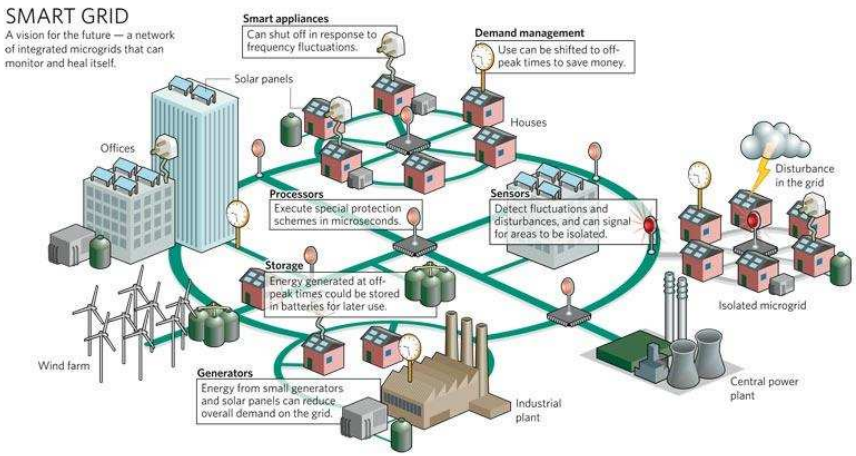
- Historians can be used as a standalone plant system or function across the entire company to easily enable enterprise-wide benchmarking

:: A critical view of ICS – IoT

1. Road condition sensor
2. Magnetic sensor
3. Vehicle distance sensor
4. Forward obstacle sensor
5. Blind spot monitoring camera
6. Drive recorder
7. Side obstacle sensor
8. Air pressure sensor
9. Inside door lock/unlock
10. Rear obstacle sensor
11. GPS sensor
12. Airbag
13. Road-to-Vehicle/Vehicle-to-Vehicle communication system
14. Rear view camera
15. Water repelling windshield
16. Seatbelt pretensioner
17. Driver monitoring sensor
18. Heads-up display
19. Steering angle sensor
20. Electronic control throttle
21. Electronic control brake
22. Fire detection sensor
23. Vehicle speed, acceleration sensor
24. Collision detection sensor
25. Pedestrian collision injury reduction structure
26. Electronic control steering
27. Message display system
28. Hands-free system

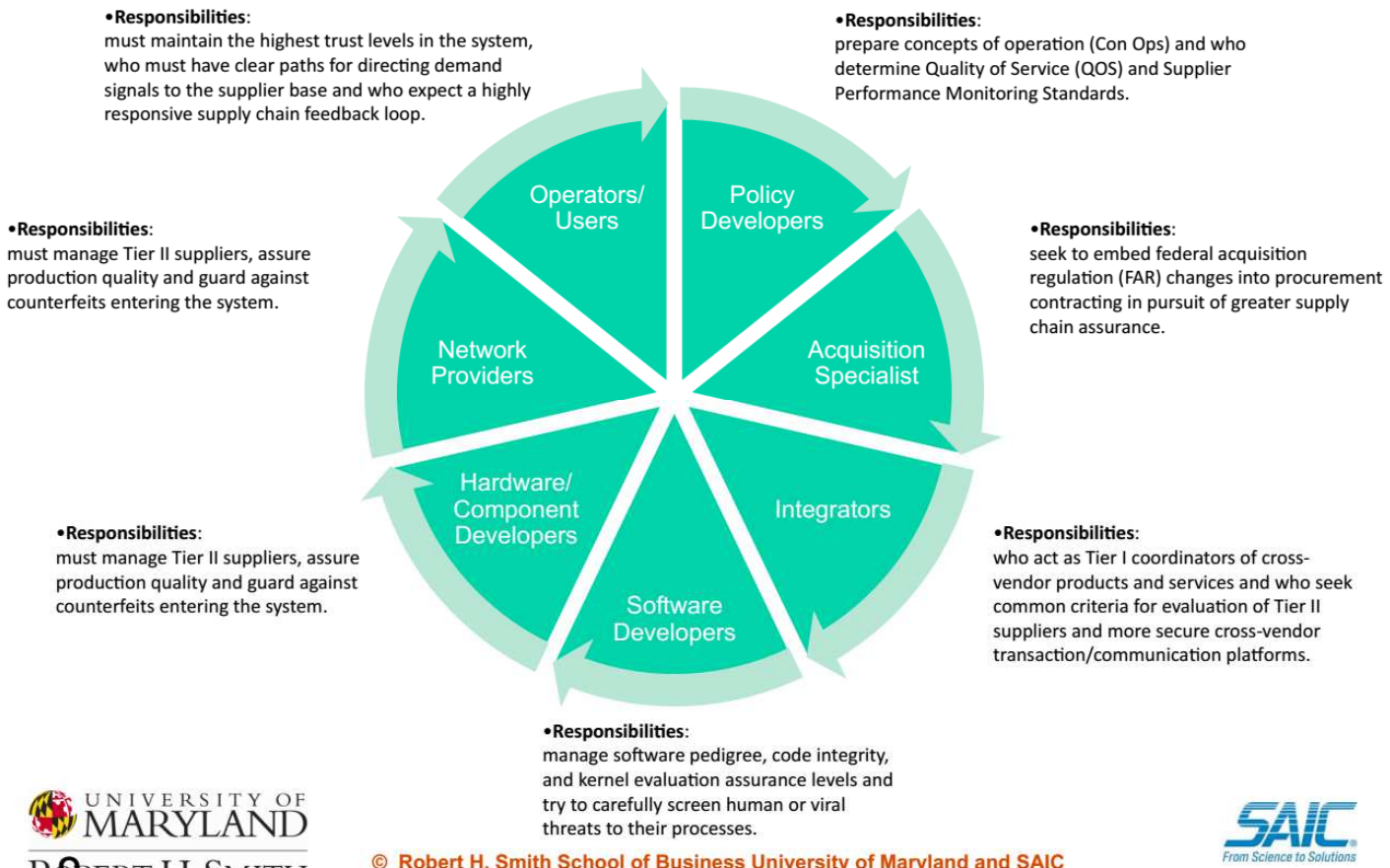


:: A critical view of ICS – From components to National Infrastructure



:: A critical view of ICS – Who do we blame?

Cyber Supply Chain Actors



© Robert H. Smith School of Business University of Maryland and SAIC

UNIVERSITY OF MARYLAND
ROBERT H. SMITH SCHOOL OF BUSINESS

SAIC From Science to Solutions

NETTITUDE

EXCELLENCE AS STANDARD

Building a resilient Industrial Control System (ICS)

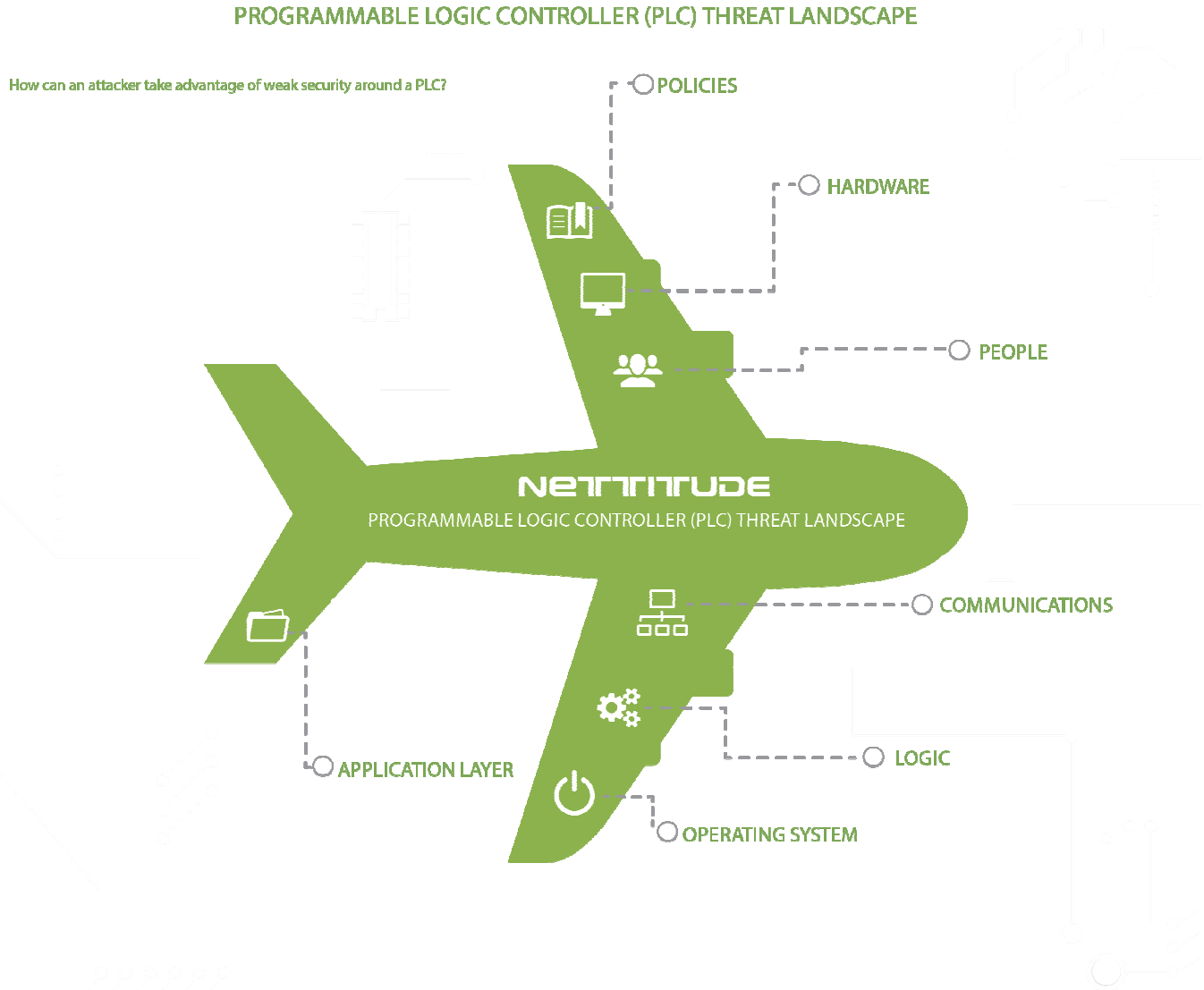
1: From ICS to Critical National Infrastructure

2: The nature of the problem

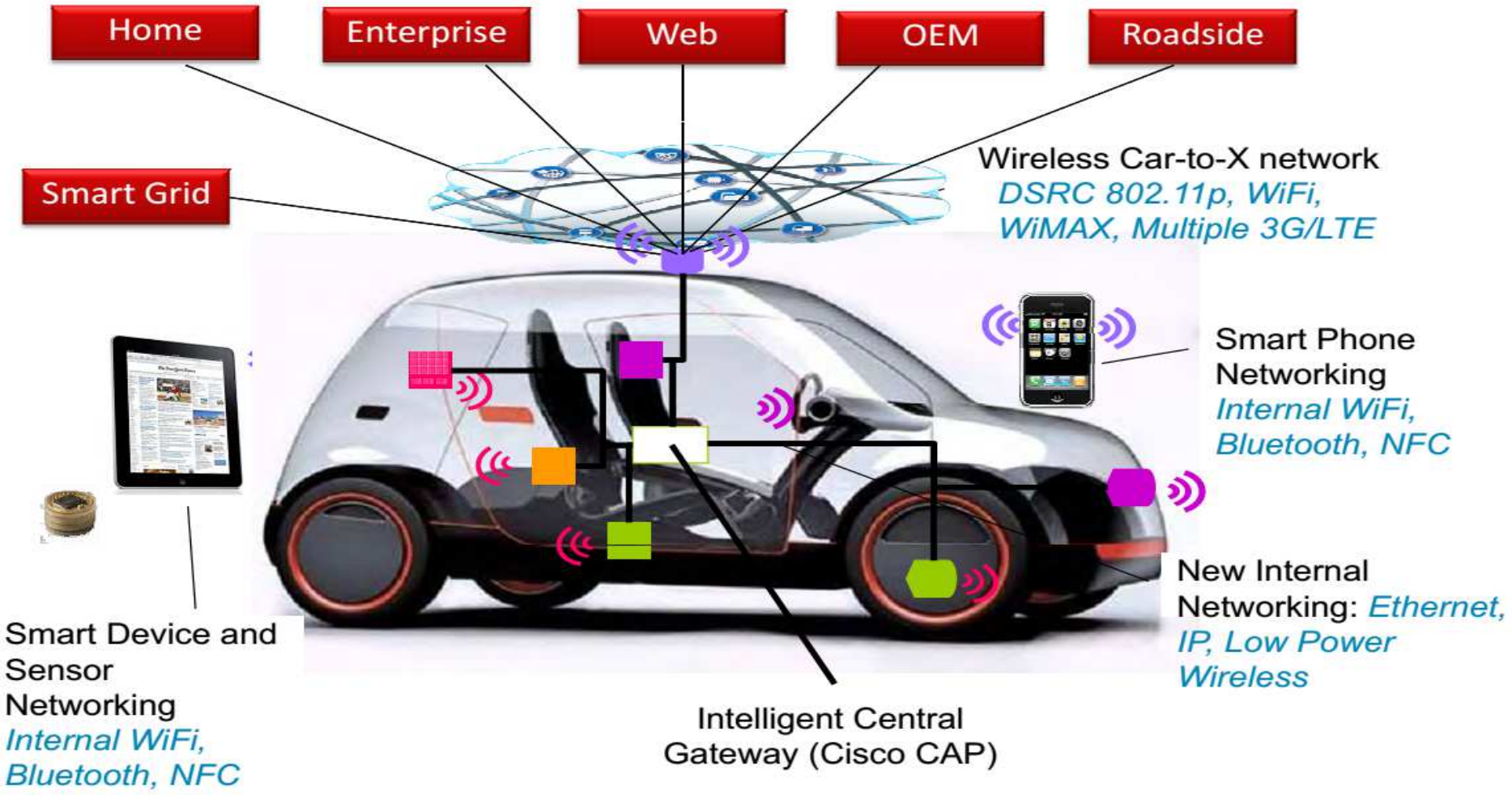
3: Building a resilient ICS network

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Sun Tzu

:: Threat landscape



:: Threat landscape



© 2010 Cisco and/or its affiliates. All rights reserved. Cisco Public

:: Can we build resilient ICS?

Looking back:

- Between 2001 -2014, 80-90% of attacks originated from external sources
- In 60% of cases attackers are able to compromise an organisation within minutes.
- 75% of attacks spread from Victim-A to Victim-B within one day (24 hours).
- In the 2013 DBiR by Verizon, phishing was associated with over 95% of incidents attributed to state sponsored actors
- For two years running, more than two-thirds of incidents that comprise the Cyber-Espionage pattern have featured phishing

65.5 days
Malicious insider attacks

49.8 days
Malicious code attacks

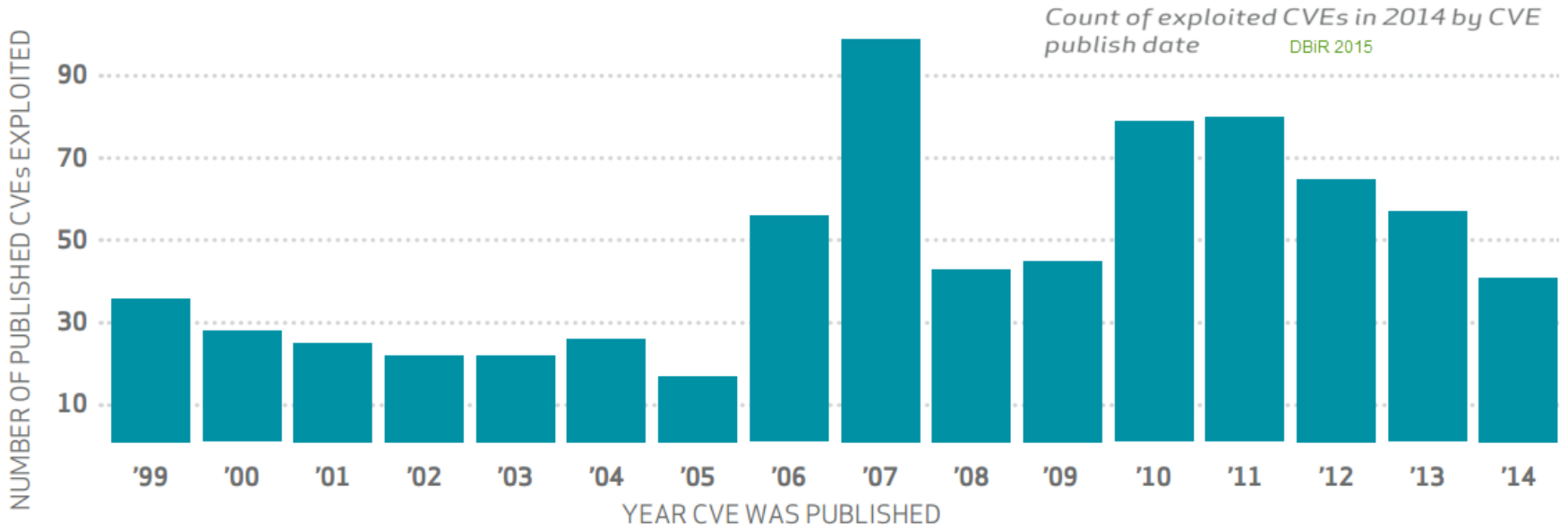
45.1 days
Web-based attacks (hackers)

SOURCE: Ponemon, p. 14

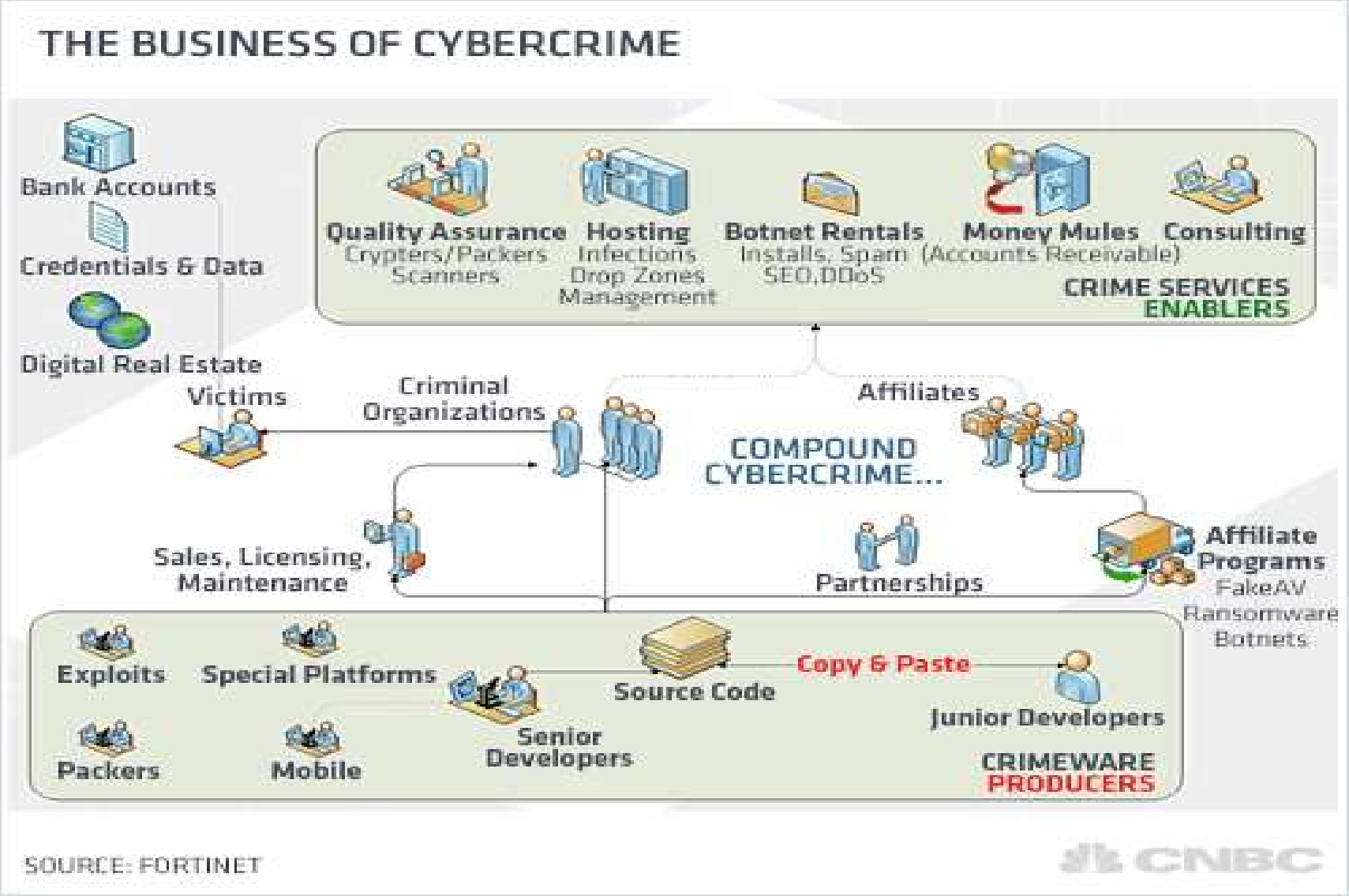
:: Can we build resilient ICS?

Looking back…

- 99.9% of the exploited vulnerabilities were compromised more than a year after the CVE was published
- 70–90% of malware samples are unique to a single organization
- 84% of criminal activities are related to botnets



:: Who is the adversary?



:: Who is the adversary?

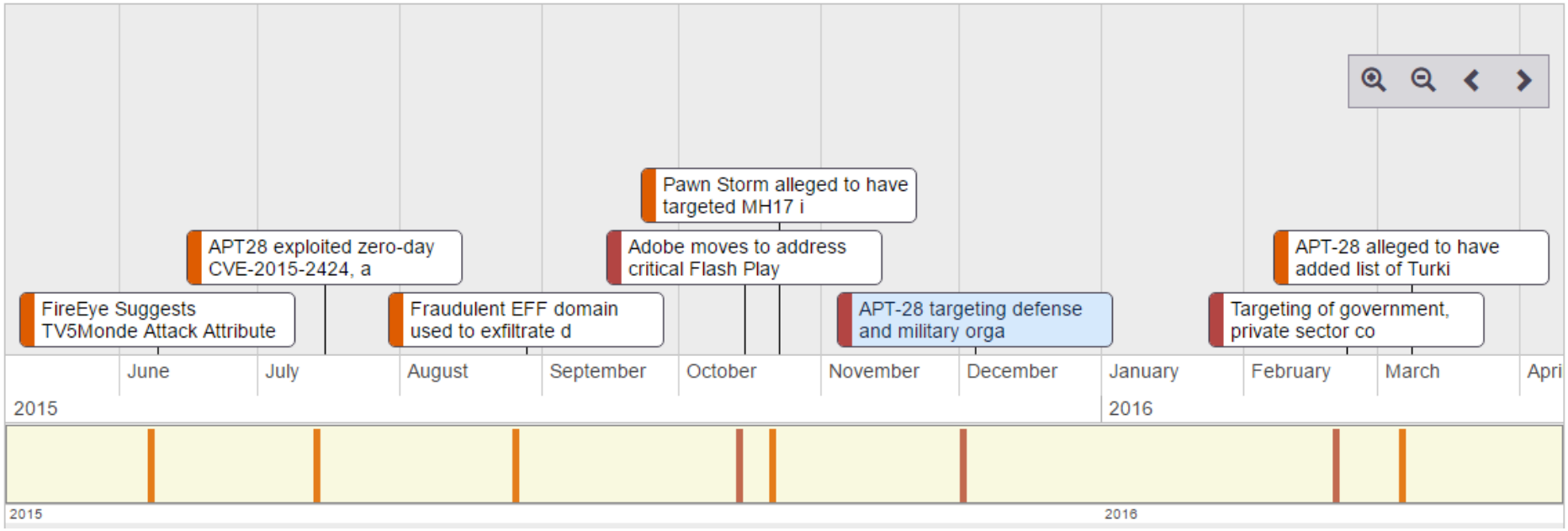
APT-28 targeting defense and military organizations with updated tools

> Sofacy (also known as "Fancy Bear", "Sednit", "STRONTIUM" and "APT28") is an advanced threat group that has been active since around 2008, targeting mostly military and government entities worldwide, with a focus on NATO countries. More recently, we have also seen an increase in activity targeting Ukraine.

APT-28

ACTIVE | Threat Level: High | BIO | Timeline | Associations | Incidents

A timeline of incidents linked to 'APT-28'. Click and hold the timeline to scroll, mouse wheel can be used to zoom in/out. Click an incident to view more details below.



NETTITUDE

EXCELLENCE AS STANDARD

Building a resilient Industrial Control System (ICS)

1: From ICS to Critical National Infrastructure

2: The nature of the problem

3: Building a resilient ICS network

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Sun Tzu

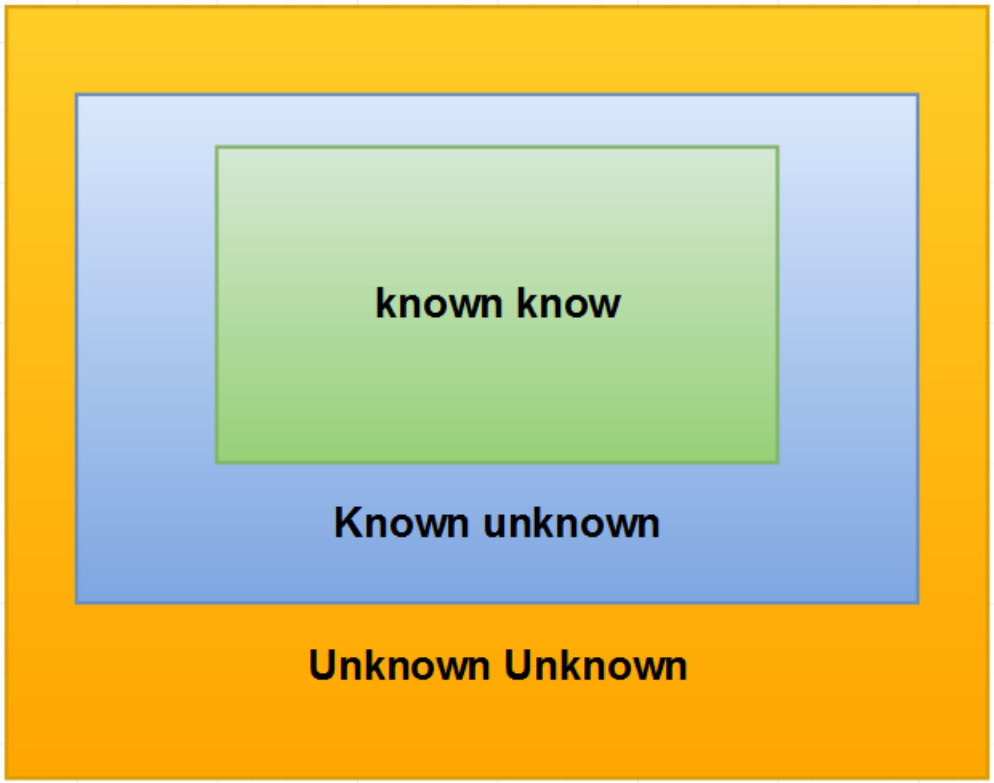
:: 3 – Building resilient ICS

Definition:

- The business understands the impact of a potential cyber-attack
- The business knows the steps required to prevent, survive and recover from such an attack
- The business understand its real threat model
- It's bringing people, technologies and policies together to prevent cyber attack disrupting the course of operations
- It's the ability for a business to recover after a successful attack whilst keeping the impact of such an attack to the minimum

:: 3 – Building resilient ICS

Which one do we care about?



:: Holistic Cyber Security

360 Degree Cyber Security

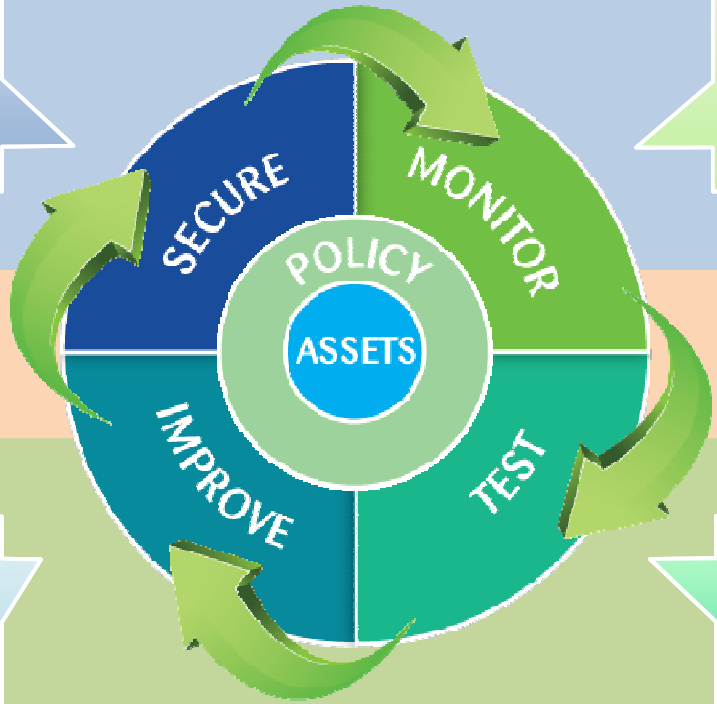
Managed Security Services (MSS)

Defend

Network Operations Centre (NOC), Managed Security Technology & Support

Detect & Respond

Security Operations Centre (SOC), N-CERT, Incident Response, HoneyTraps



Research & Development

Innovation

Define

Threat Intelligence, Governance, Risk Management, Compliance, Assessment, Measurement, Training

Assurance

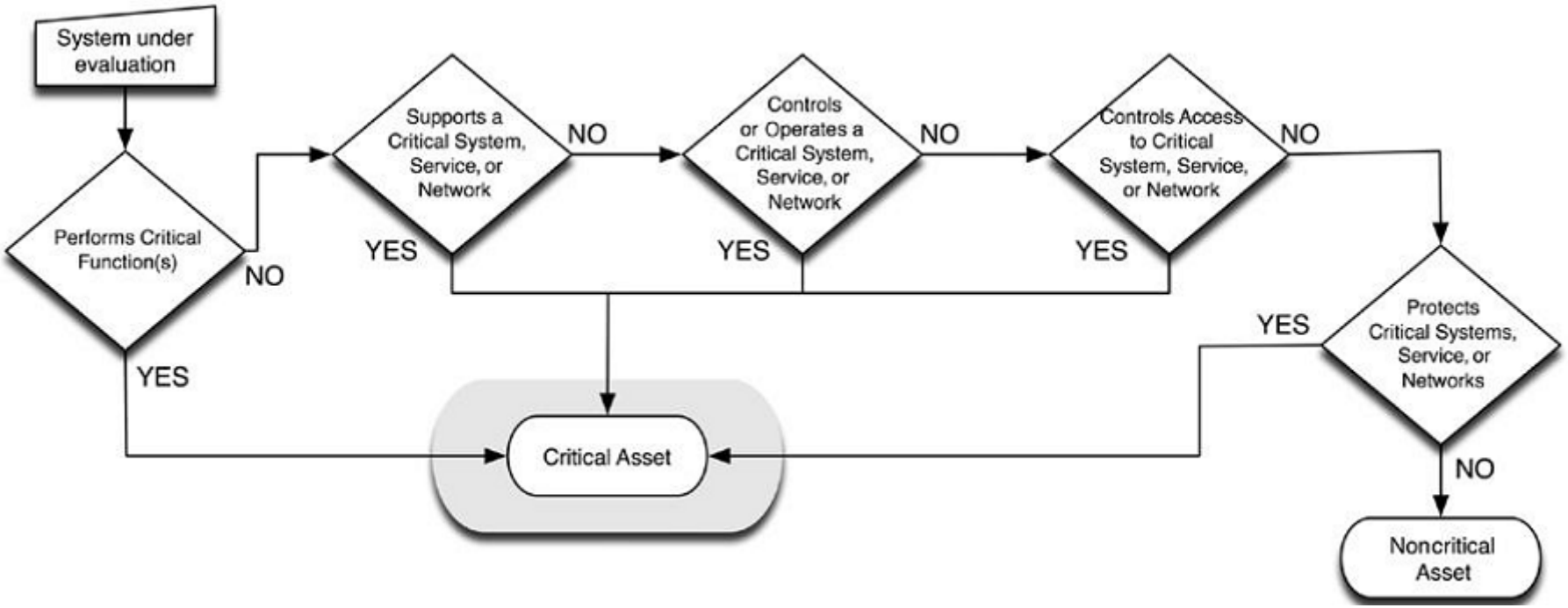
Identify vulnerabilities in People, Process and Technology, Guidance on Risk

Professional Services

:: Resilient ICS – Define

The ASSET

- Physical components
- The people
- The processes



:: Resilient ICS: Define

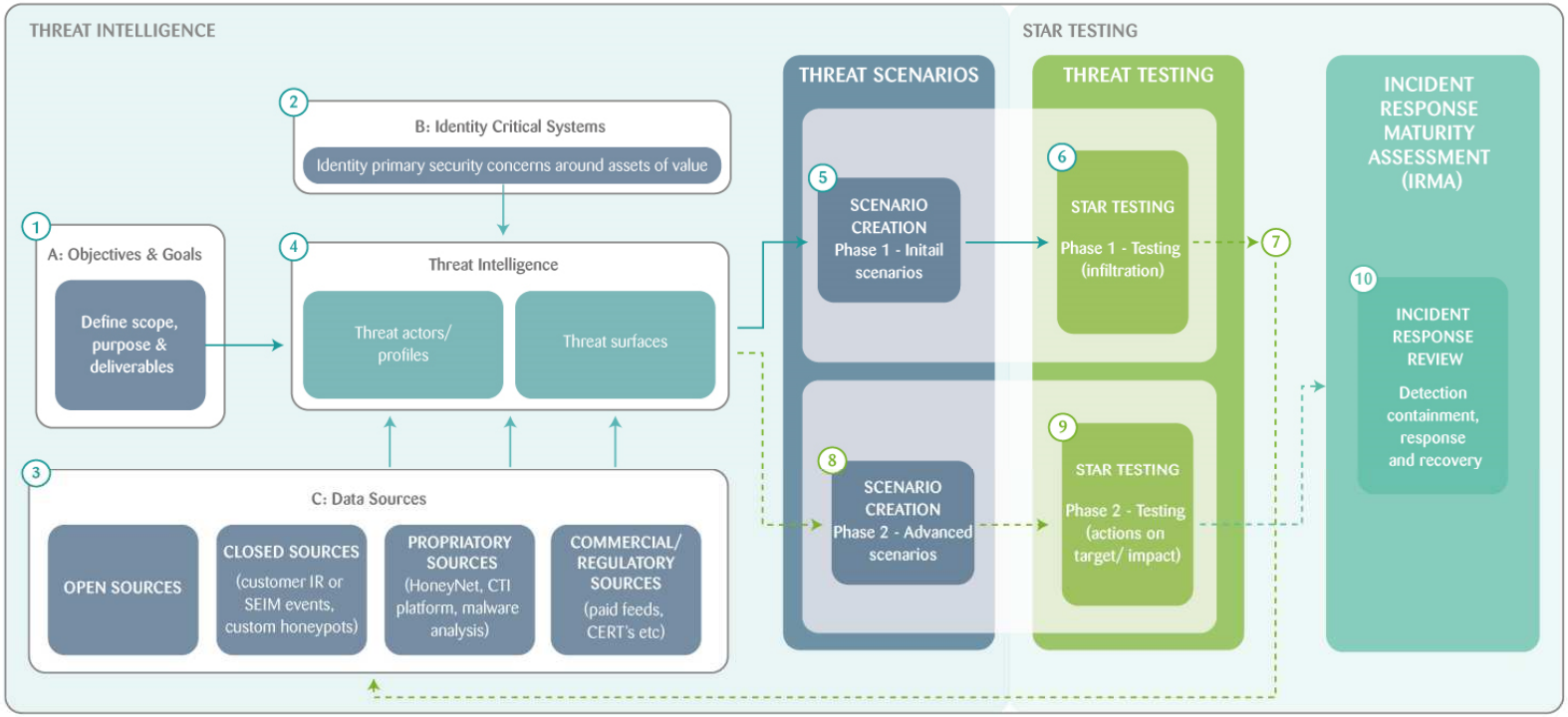
Managing your asset:

- Asset and network discovery and mapping
- Understanding your cyber risk posture
- Know your real threat landscape
- Mapping assets to vendor relationships

- Know your external threat landscape and understanding how to recognise if you are being targeted through comprehensive
- Global threat intelligence, correlation, and analysis capabilities
- Educate users
- Reduce the impact of attacks
- Have a business continuity model fully tested and implemented

:: Threat Intelligence

NETTITUDE'S ADVANCED CTI PROCESS FLOW



KEY AND PROCESS DESCRIPTION

PHASE 1

1 – Define the objectives & goals for the threat intelligence work
2 – Identify & score the assets of value
3 – Determine the appropriate & relevant data sources to use
4 – Identify & model the threat actors and threat surfaces
5 – Create & build scenarios for Initial Entry into the target organization/network/3rd parties/people
6– Conduct STAR simulated scenario testing and continue to gather inside intelligence

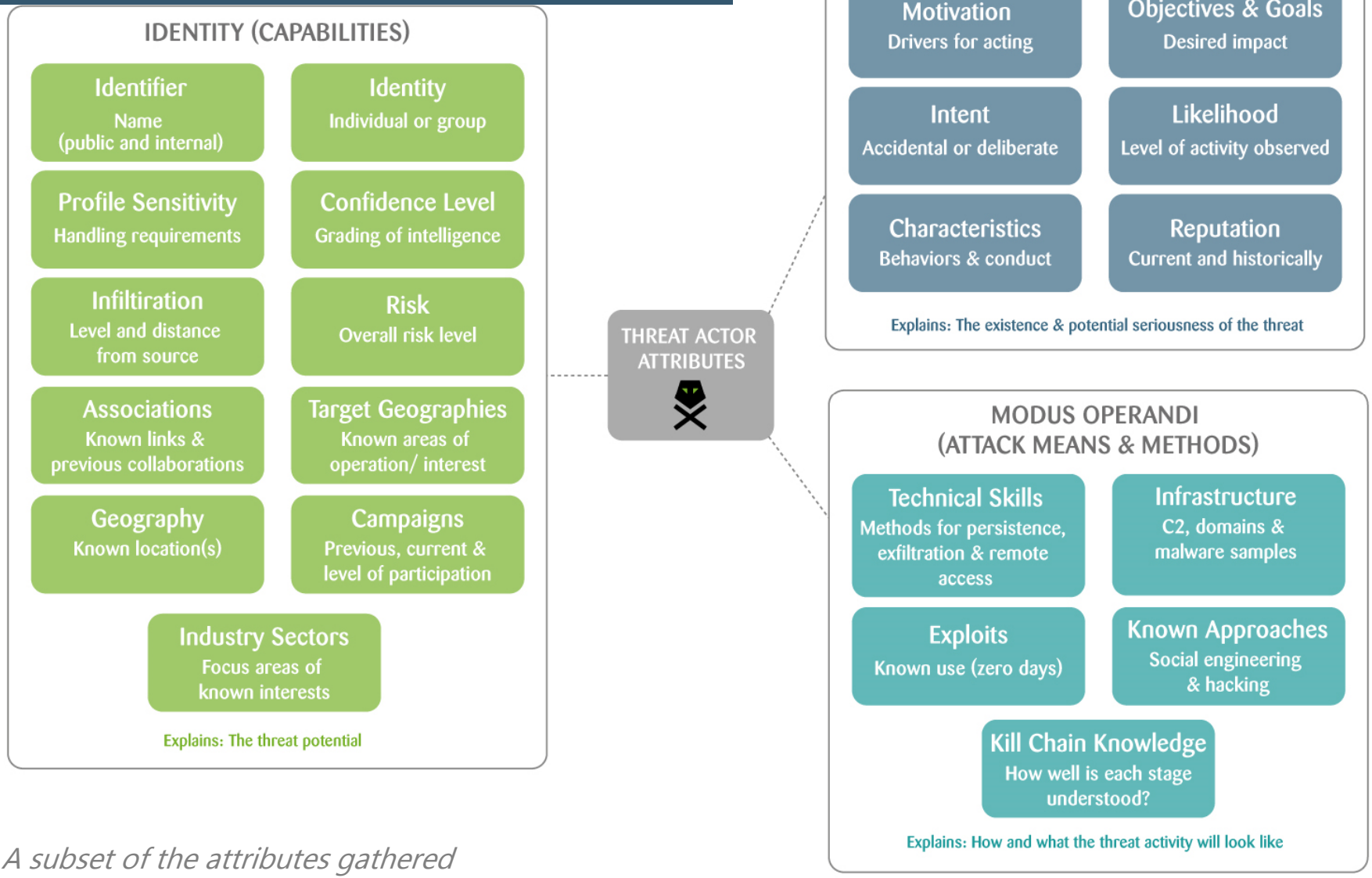
PHASE 2

7 – Use the inside intelligence to update the threat actor capabilities, infrastructure and technology knowledge
8 – Re-evaluate & update the scenario's created
9 – Perform the 2nd stage simulated attack against the main objectives within the organization targeted

PHASE 3

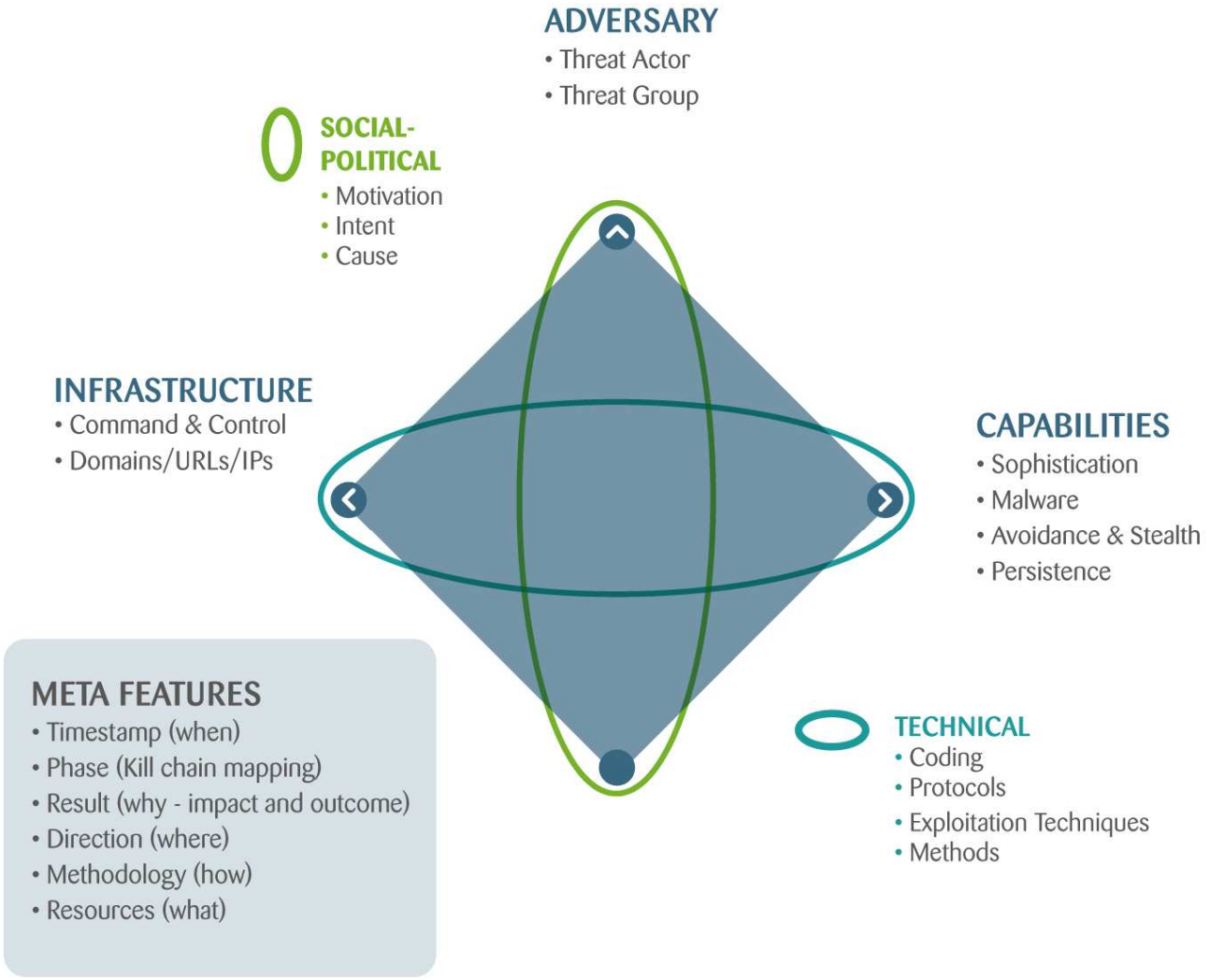
10 – Conduct Incident Response Maturity Assessment (IRMA)

:: 3 – Threat actors!



- *A subset of the attributes gathered*

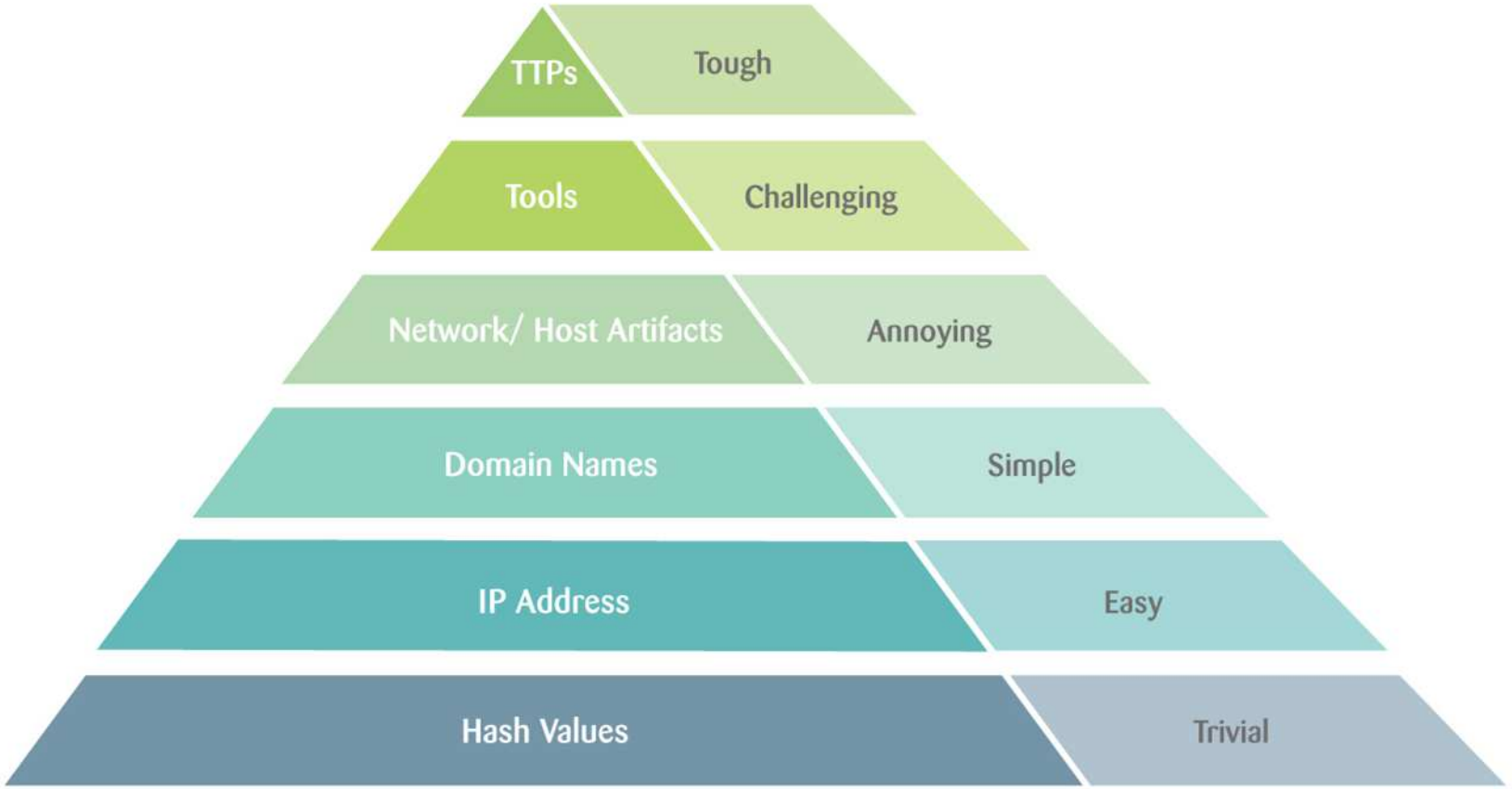
:: 3 – Understanding your threat actors!



:: Detect and Respond

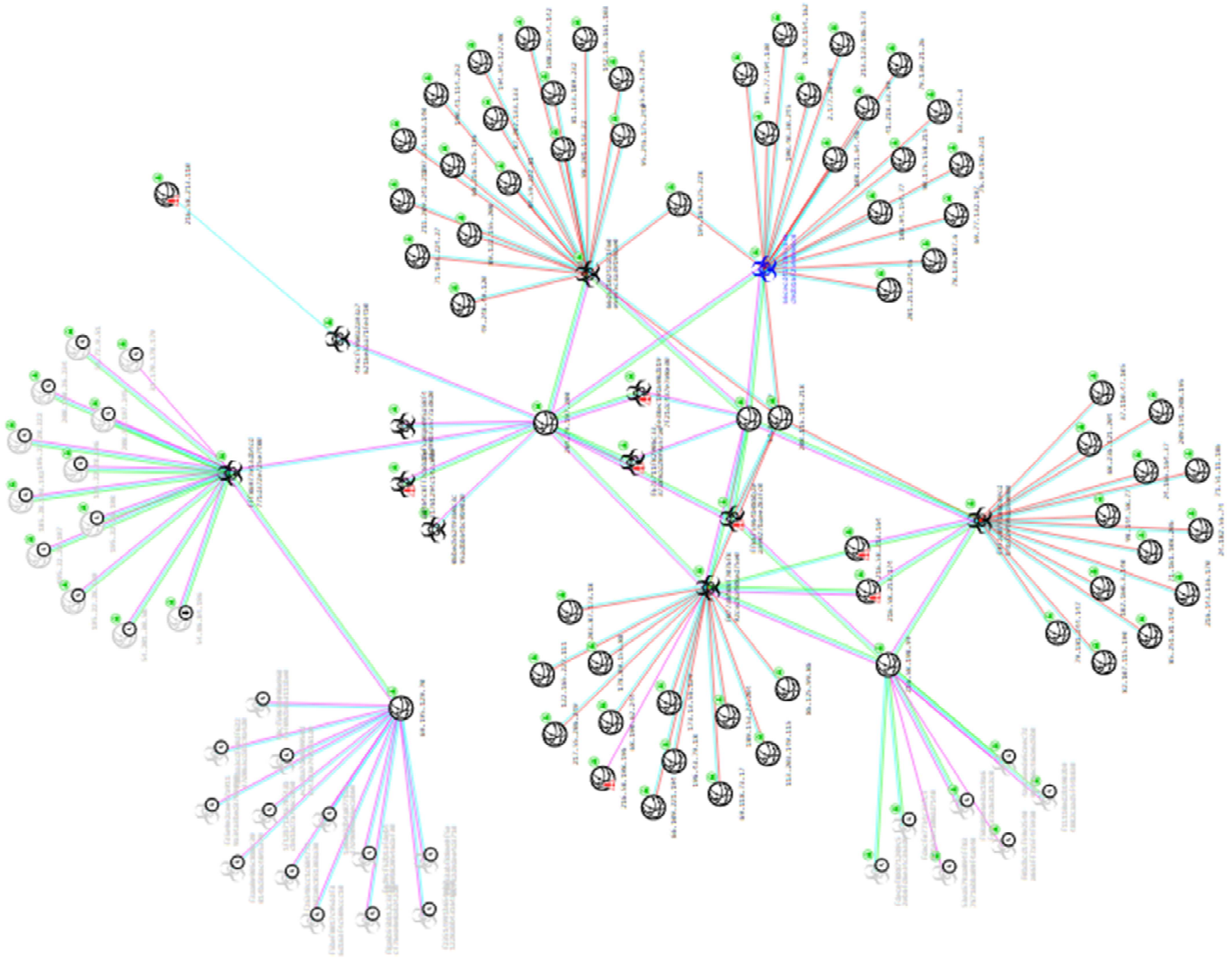
PYRAMID OF PAIN

Understanding the disruption caused when technical attributes are actively defended



SOURCE: DAVID J. BIANCO, PERSONAL BLOG

:: 3 – Needle in a haystack – data analysis



:: Defend!

Prioritise!

- Protecting all assets is not always possible
- Buying the right product is very important
- Address your threat
- Work with specialist groups

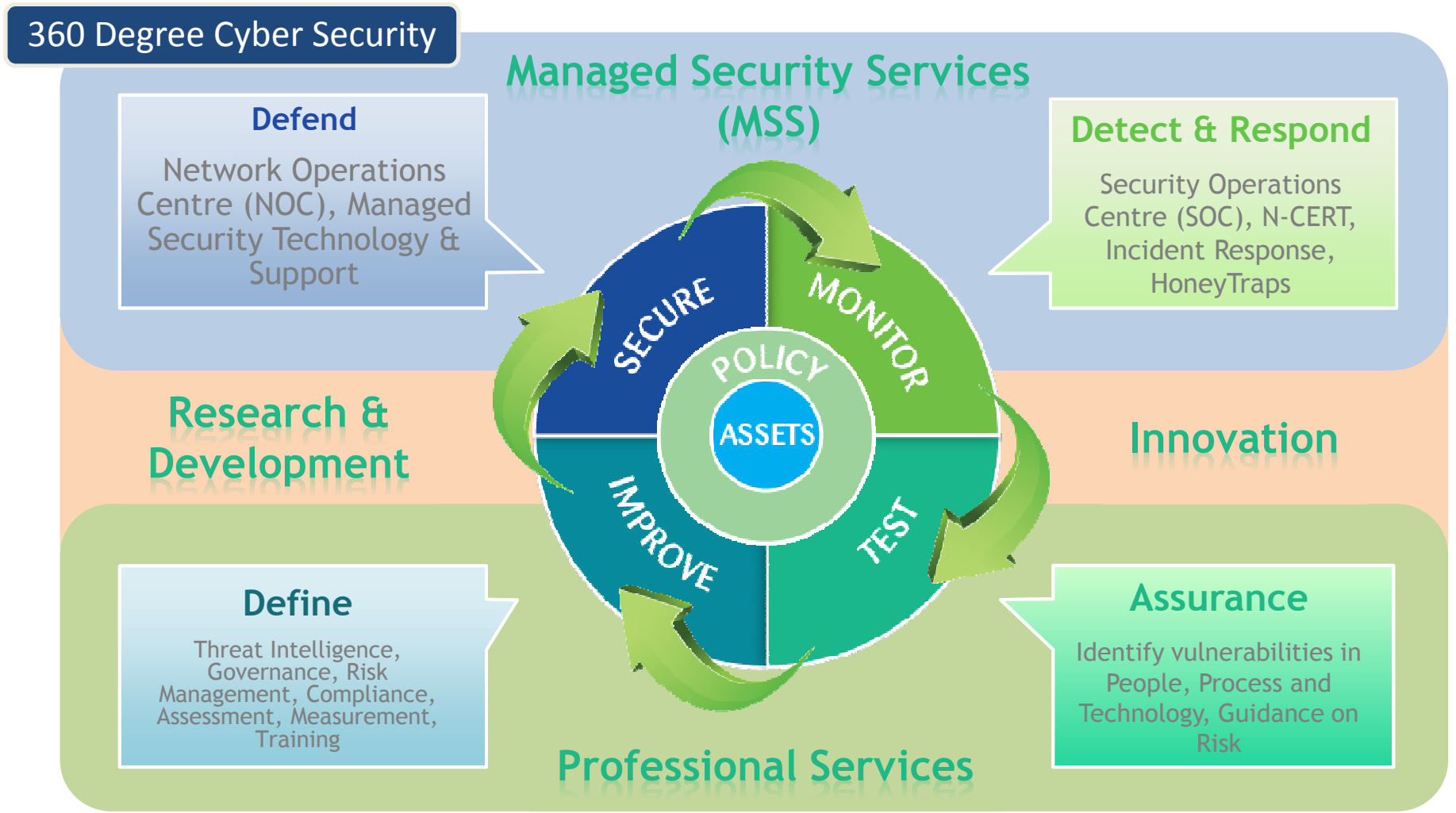
End point protection	P1	P2	P3	P n..
Signature based detection				
Scan every email and check any associated link				
Keep a hash for known file and sandbox any other file				
CPU inspection level				
Allow known files to run and block unknown files				

:: Assurance

Validate your security and assess your response maturity level

- Traditional penetration testing is quite focussed:
  - Restricted to a particular system and methodology
  - Based on the target organisations internal security concerns
- The STAR approach aims to address a lot of these weaknesses:
  - Includes TI, PT and IR
  - Any system is potentially in scope
  - The methodology is based on real world scenarios gleaned from TI
  - Addresses actual threats, based on TI, rather than perceived threats
  - Importantly – IR is ‘baked in’ and measured
- STAR testing aims to be more advanced, more inclusive and more realistic

:: Holistic Cyber Security



NETTITUDE

EXCELLENCE AS STANDARD

Thank You

0345-5200085 | jpagnadisso@nettitude.com | www.nettitude.co.uk

Partner with the best….