Achieving a Secure and Resilient Cyber Ecosystem:

A Way Ahead

January 2016

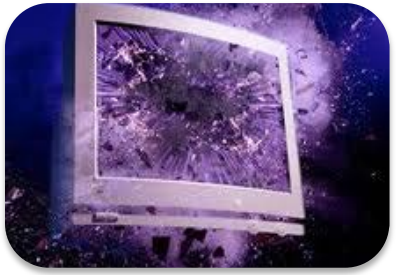
Continuing to strengthen the security and resilience of our nation's critical infrastructure in partnership with you…

Our Responsibilities

At CS&C, we have two complementary and related missions:

In the telecommunications arena, we support interoperability and continuity of communications needed in times of crisis.

In the cyber realm, we help the ***dot gov*** and ***dot com*** domains secure themselves, focusing on critical infrastructure.

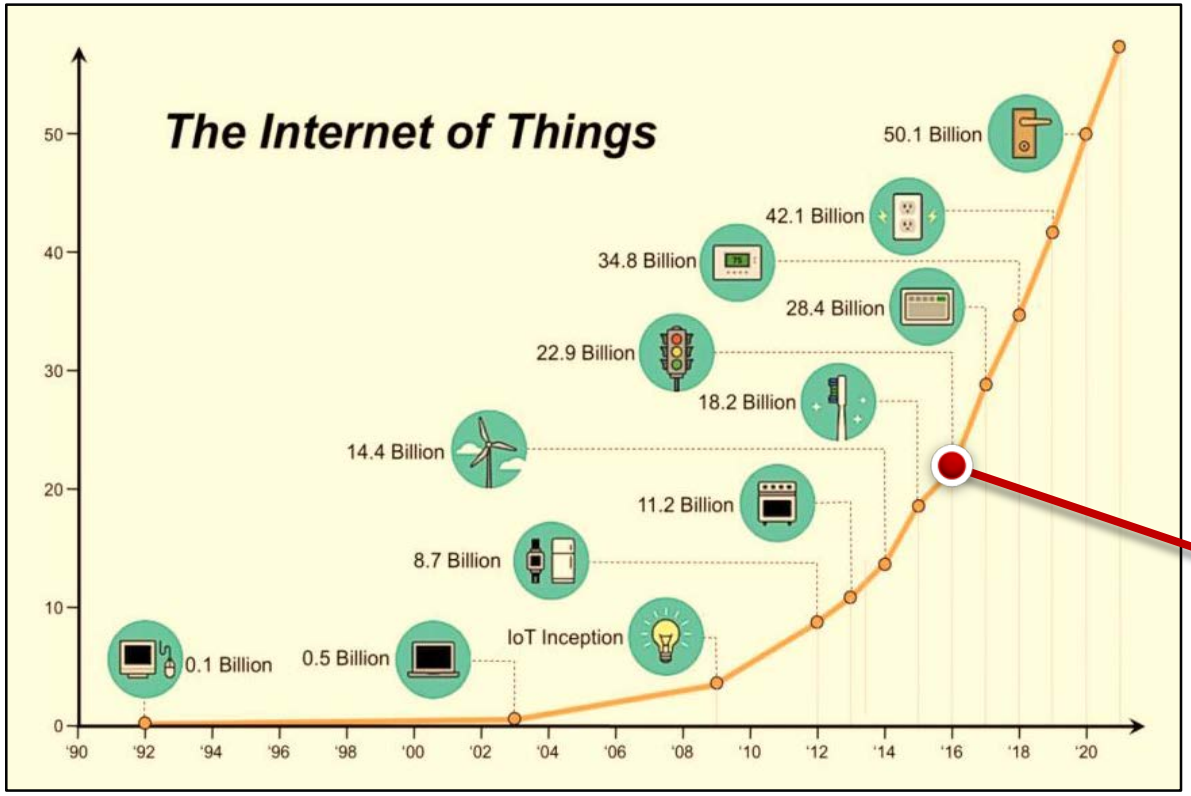


The *Cyber Ecosystem*

- **The cyber ecosystem is the foundation of our digital society. It consists of:**
  - Government and private sector information infrastructure, including international
  - The interacting persons, processes, data, information and communications technologies

- **It is expanding and under constant attacks**
  - The Internet of Things will enhance digital society, but it also increases attack surface
  - The attackers are nimble and inventive and constantly evolving their attack methods

Our Ecosystem Gets Bigger and More Complex



- Endpoint Explosion = Attack Surface Explosion
- Predicted to grow to 50B devices by 2020 [1]
- Increased user dependency
- BYOD with little regulation

2015: Auto manufacturers rush to secure next generation vehicles

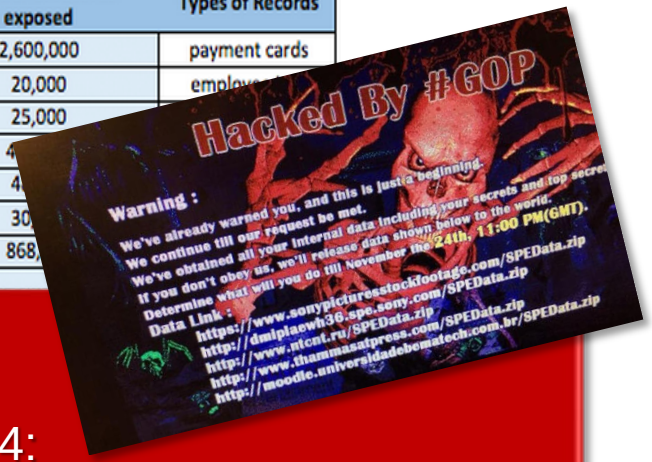
Social media scams flourish on mobile

Baby monitors and security cameras hacked

[1] D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco Report, April 2011

Attacks Are Continuously Expanding

Date	Company	Number of records exposed	Types of Records
1/25/2014	Michael's	2,600,000	payment cards
2/6/2014	Home Depot	20,000	
3/14/2014	Sally Beauty Supply	25,000	
4/17/2014	Aaron Brothers		
4/22/2014	Iowa State Univ.		
5/30/2014	Home Depot		
7/22/2014	Goodwill Industries	868,	
	Community Health		
11/10/2014	US Postal Service	800,000	personal data
11/18/2014	Staples	1,200,000	credit/debit card



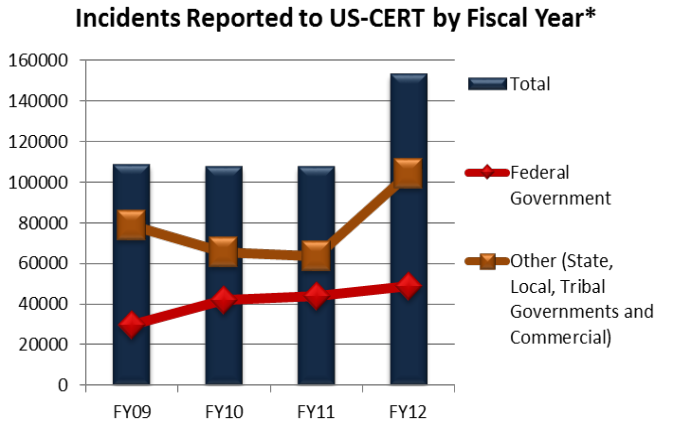
November 2014:
Sony hacked
December 17 2014:
Sony pulls public release of 'The Interview'

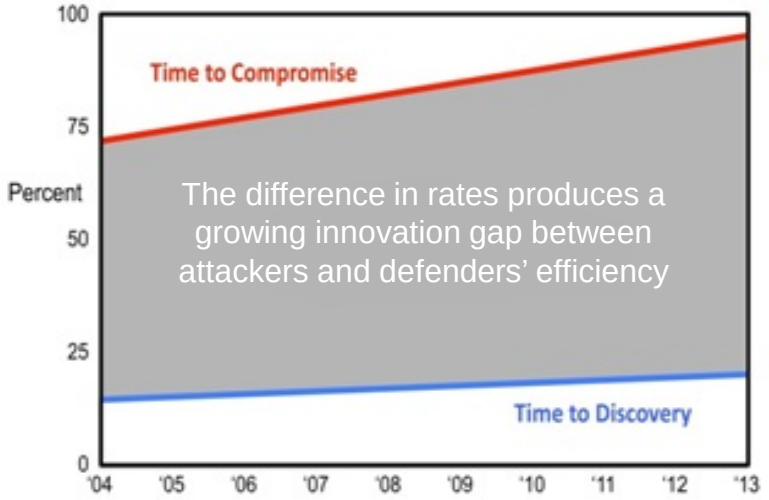
http://uk.appriver.com/resources/global_security_report/global_security_report_end-of-year-report-2014.aspx

January 2015:
80 Million affected by Anthem Data Breach

- Data breach attacks continue unabated
- Greater number of individuals and organizations impacted
- Business and policy decisions are affected
- Public trust is affected

Our Opponents Improve Faster than We Do





Derived from the 2014 Verizon Data Breach Investigations Report [3]

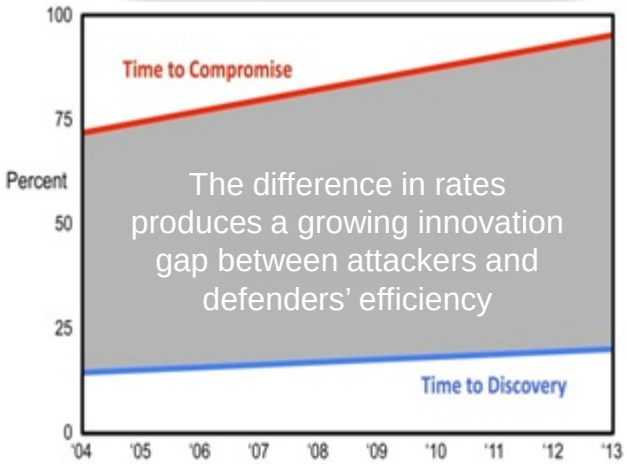
- Volume, sophistication of attacks go up while cost and risk to attackers decreases
- Attackers are always on the offensive
- Attackers can efficiently compromise a system 90% of time
- Defenders detect attacks only 20% over same period of time

The Cybersecurity Challenge

- Security analysts have incomplete knowledge and situational awareness of their enterprise and overall ecosystem security health
- Adversaries improving faster than defenders
- Insufficient security analysts to meet future requirements
- Ability to detect and respond to intrusions too slow
- Enormous growth of scope due to IoT
- Attackers rapidly innovating their attack methodologies
- Trust among organizations and with USG is not sufficient to automatically share and execute shared defensive courses of action
- There is no resilient infrastructure that would support assured communications

November 2014:
Sony hacked.
December 17, Sony pulls public release of The Interview

January 2015:
80 Million affected by Anthem Data Breach



Derived from the 2014 Verizon Data Breach Investigations Report [3]

How to Address the Challenges

Challenges	Proposed Solutions
Disparate tools don't provide integrated toolset. Costly and time consuming to integrate new innovative technology.	***INTEROPERABILITY***
Adversaries improving faster than defenders. Insufficient security analysts to meet future requirements. Ability to detect and respond to intrusions too slow.	***AUTOMATION***
Limited automated authentication. Lack of organizational partnerships and relationships.	***TRUST***
Security analysts have incomplete knowledge and situational awareness of their enterprise and overall ecosystem security health. Experience of others cannot be leveraged.	***INFORMATION SHARING***
Communications infrastructure could be attacked.	***ASSURED COMMUNICATIONS***

Mechanisms to Achieve Solutions

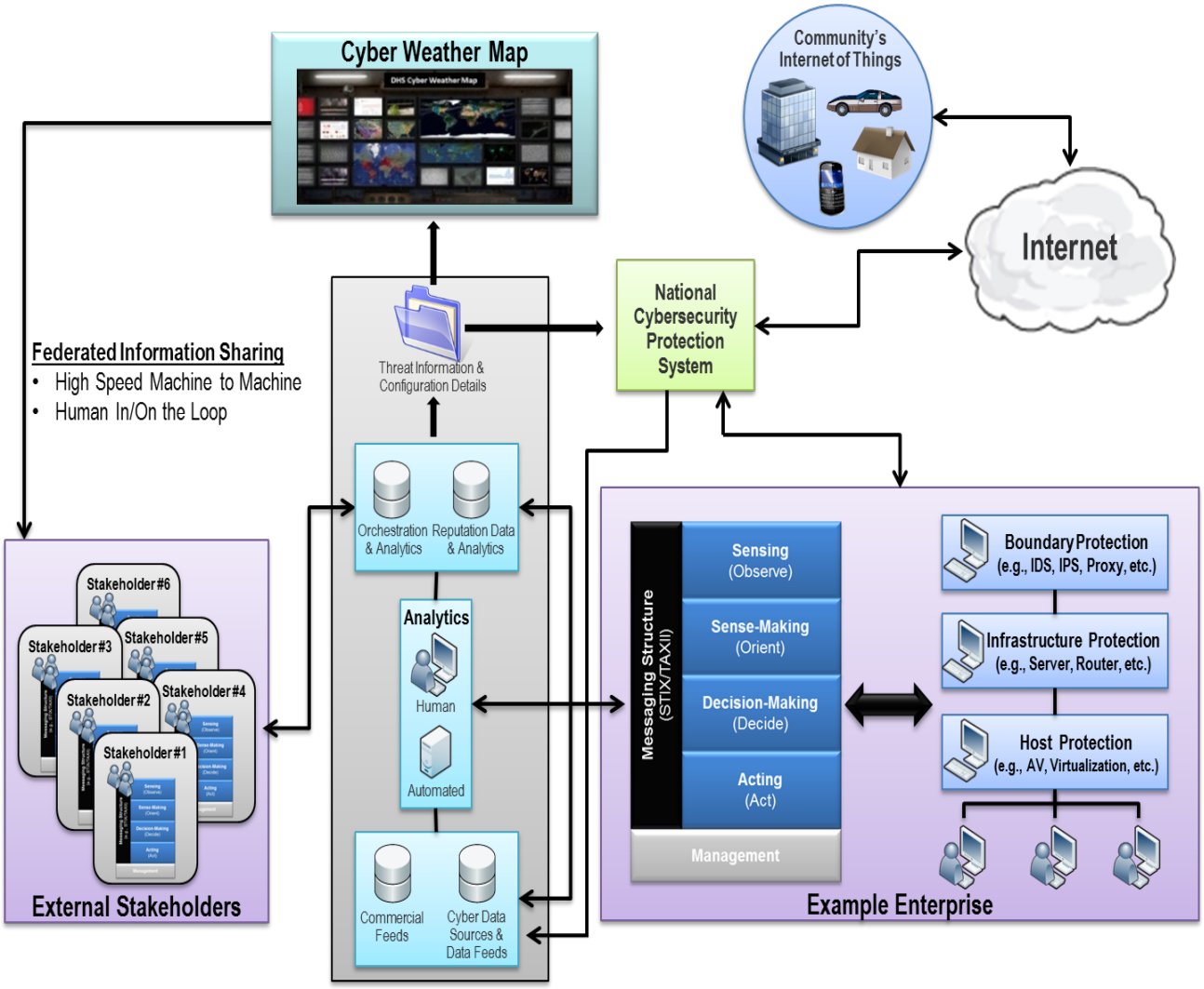
Challenges	Proposed Solutions	Mechanisms
Disparate tools don't provide integrated toolset. Costly and time consuming to integrate new innovative technology.	***INTEROPERABILITY***	Common Data Model Standards (data and transport) Open APIs, Frameworks, Control Planes Rapid Integration Acquisition
Adversaries improving faster than defenders. Insufficient security analysts to meet future requirements. Ability to detect and respond to intrusions too slow.	***AUTOMATION***	Common Data Model Orchestration Shared COAs
Limited automated authentication. Lack of organizational partnerships and relationships.	***TRUST***	Authentication Infrastructure Established partnerships
Security analysts have incomplete knowledge and situational awareness of their enterprise and overall ecosystem security health. Experience of others cannot be leveraged.	***INFORMATION SHARING***	Common Data Model Information Sharing & Authentication Infrastructure
Communications infrastructure could be attacked.	***ASSURED COMMUNICATIONS***	Resilient Communications Priority Services Interconnected Infrastructures

These mechanisms enable effective and efficient risk mitigation

Secure and Resilient Cyber Ecosystem Example Architecture

SRCE:

- Enterprise Automated Security Environment (EASE)
- Information Sharing Infrastructure
- Cyber Weather Map

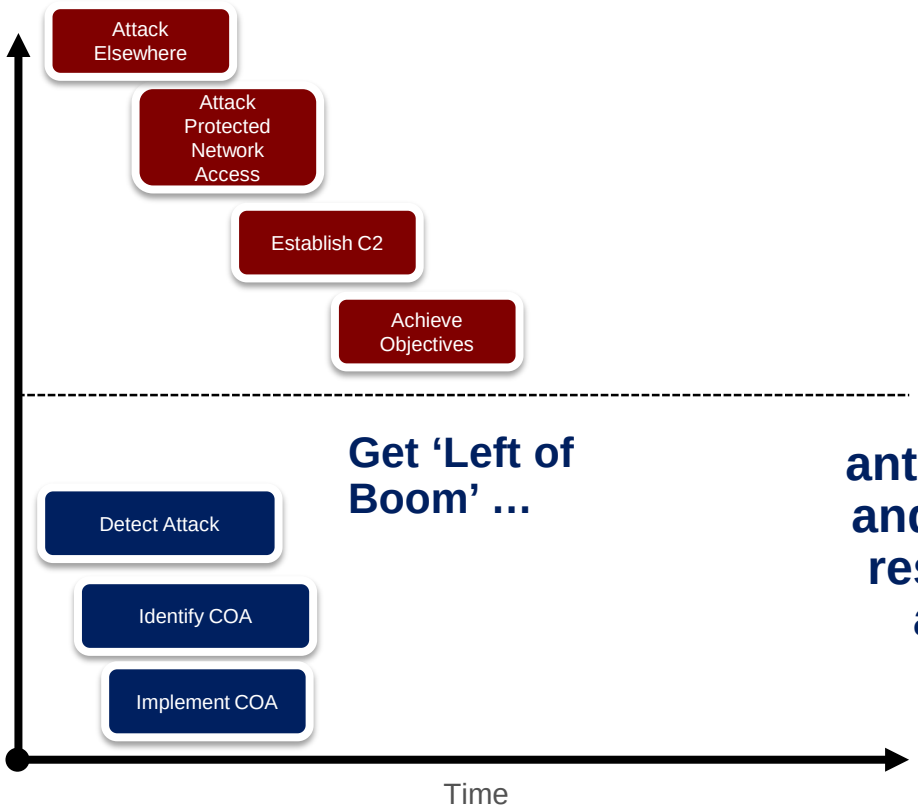


Establishing Collaboration to Achieve Way Ahead

- Government facilitates, but the private sector develops the solutions
- Solution providers:
  - Commercial sector,
  - National Labs/FFRDCs/UARCs,
  - Open source community
  - Academia

Can We Change Reality?

Attacker Actions

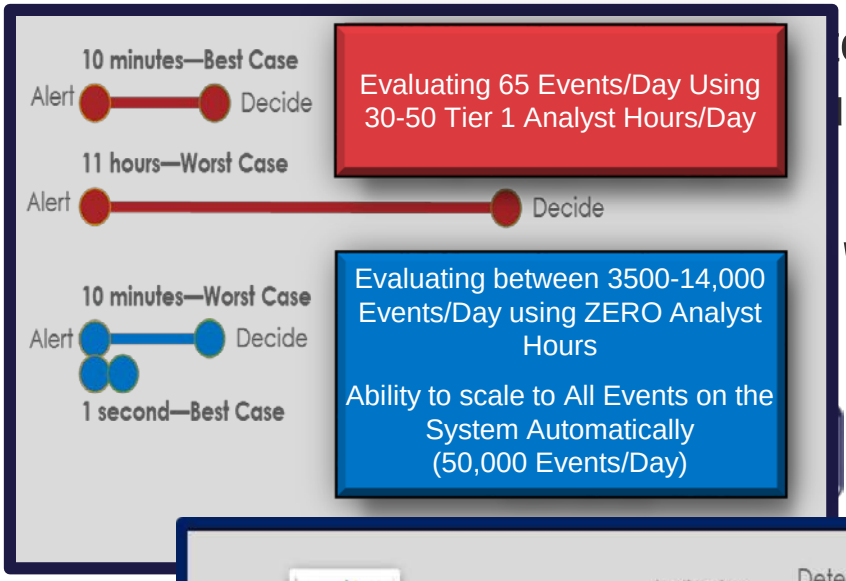


Defender Actions

Get 'Left of Boom' …

… and shift us to anticipation, prevention, and rapid detection and response ahead of the attacker's timeline

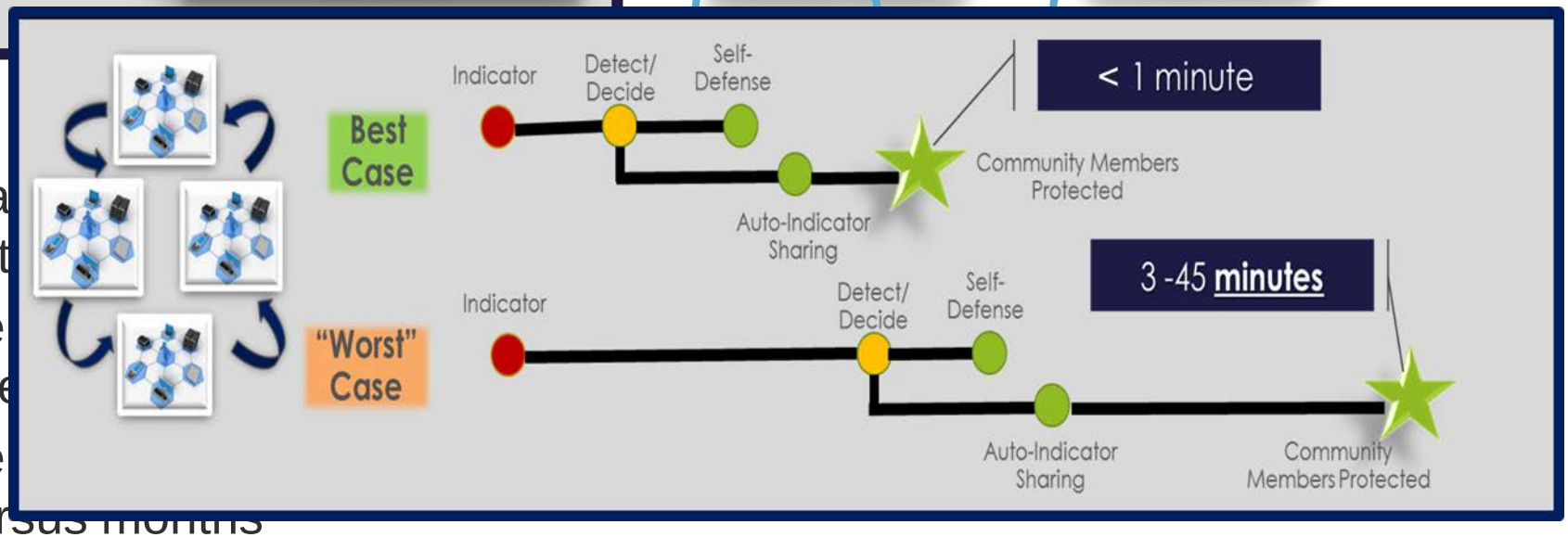
Early Accomplishments



ed 'common COAs' across multiple
rity environments

Virtualized Enterprises

for automated information sharing

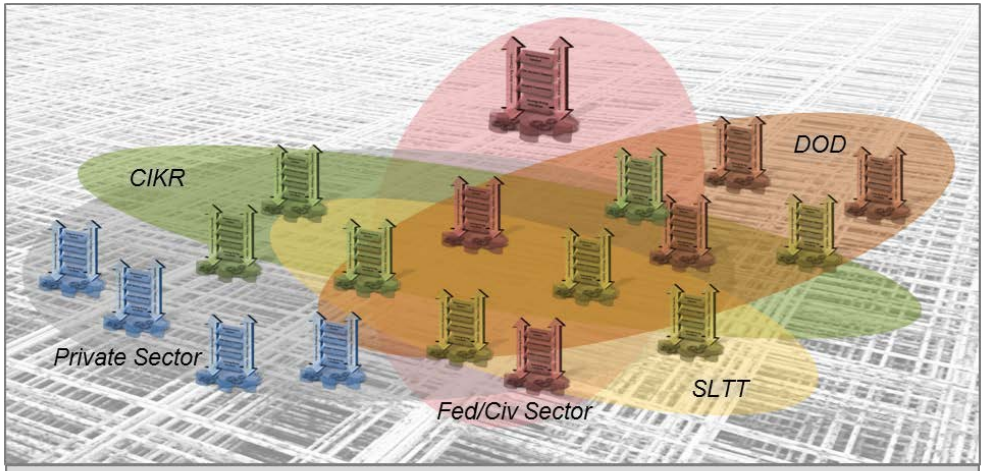


- Ma
  aut
- De
  ope
- De
  versus months

What Does Success Look Like?

Secure integration and automation across a diverse, changeable array of cyber defense capabilities

- Interoperable, flexible, extensible environment available across the cyber ecosystem
- Cyber defense operations are integrated and automated according to local capabilities, authorities, and mission needs
- Proactive cyber defense has evolved from
  months ➔ minutes ➔ milliseconds
- Operational and acquisition freedom exists to take advantage of diverse, changing, advanced solutions without wholesale changes to every system

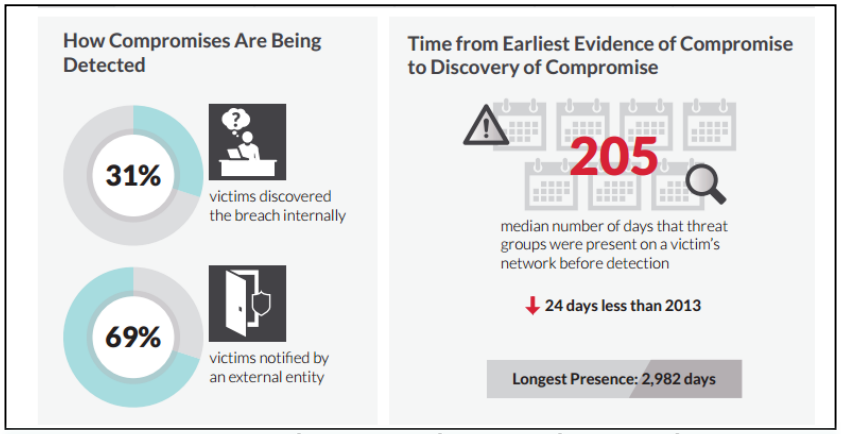


National	Coordinate National-level operations and support cross-enterprise cyber response
Regional	Enable collaborative, 'beyond-line-of-sight' defense
Local	Enable participants to defend themselves

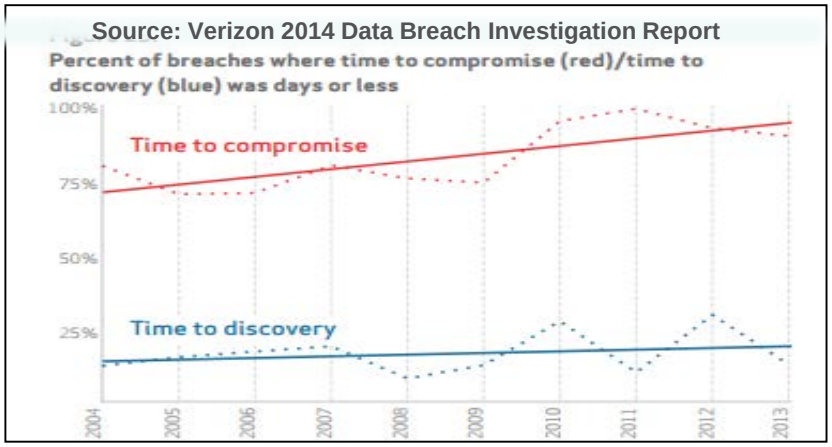
Cyber Ecosystem

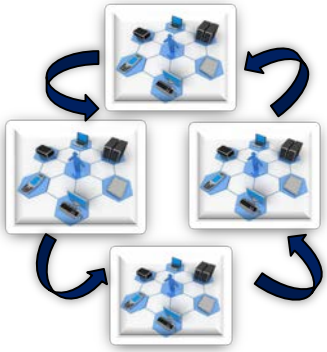
BACKUP

Spiral 1: Real-World Comparisons:
Auto-Indicator Sharing and Auto-Response Across Multiple Enterprises



Source: M-Trends 2015: A View From the Front Lines, FireEye/Mandiant





IACD Community of Trust

Best Case

Indicator → Detect/Decide → Self-Defense → **< 1 minute**

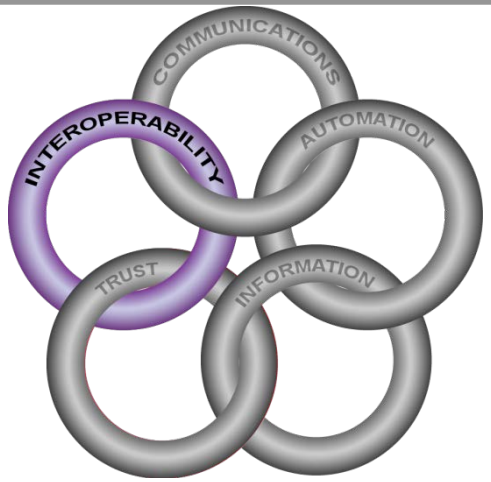
Indicator → Detect/Decide → Auto-Indicator Sharing → **< 2 minutes**

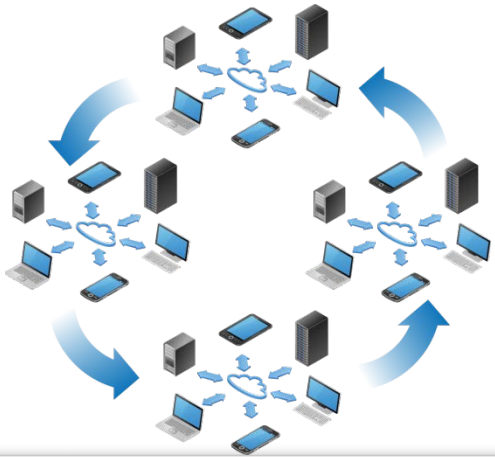
Worst Case

Indicator → Detect/Decide → Self-Defense → **8 minutes**

Indicator → Detect/Decide → Auto-Indicator Sharing → **9 minutes**

Interoperability





NOW

- Common Data Model
- Open APIs, Frameworks, Control Planes

SOON

- Open APIs, Frameworks, Control Planes
- Standards (data and transport)

FUTURE

- Standards (data and transport)
- Rapid Integration Acquisition
- Universal plug and play for the secure and resilient cyber ecosystem

With interoperability, the adversary is challenged to keep up with the pace of improvement

Automation

NOW

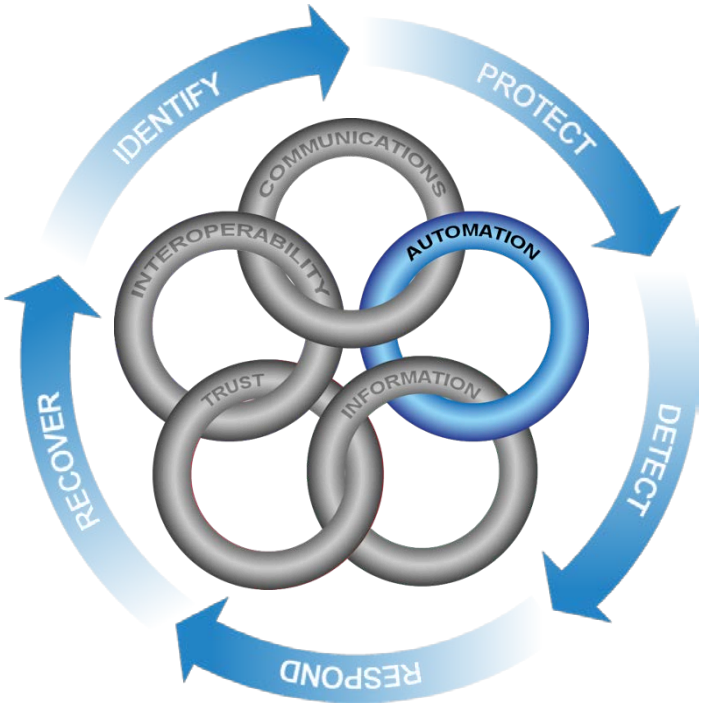
- Common Data Model
- Orchestration

SOON

- Shared COAs

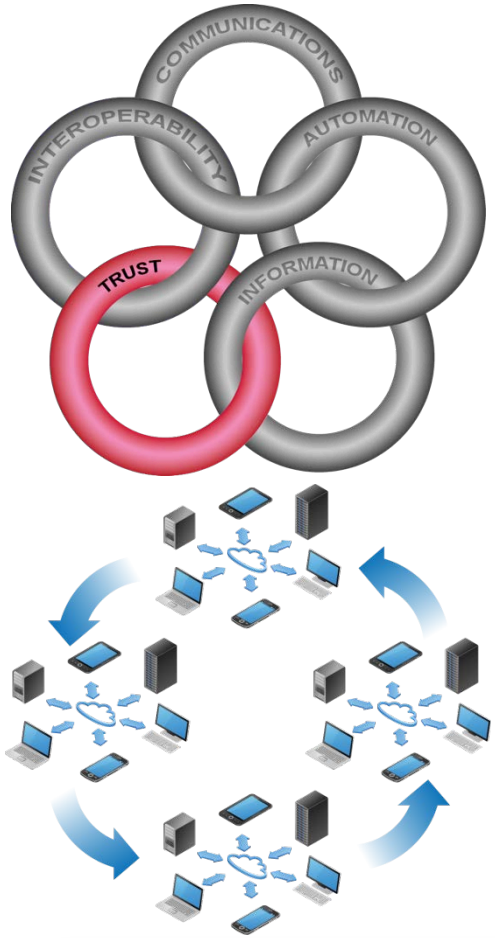
FUTURE

- Fully distributed autonomous response
- Humans controlling how aggressive automation should be (risk appetite)
- We can “undo” undesirable automated actions



With automation, we mitigate an intrusion before the adversary sees success

Trust



NOW

- Authentication Infrastructure
- Established partnerships

SOON

- We will provide a authentication/authorization infrastructure to provide trusted sources of information
- Will be able to act on information prior to validation

FUTURE

- We will trust the sources and methods of information automatically shared to drive automated response (shoot first and ask questions later)

With trust, we will be able to use authenticated information directly in our responses

Information Sharing

NOW

- Common Data Model
- Information Sharing & Authentication Infrastructure

SOON

- Shared data models will assure shared meaning of data
- Confidence will be associated with shared data
- Data will be actionable and able to be parsed automatically

FUTURE

- The right data will arrive just in time to take automated action
- Shared situational awareness will give all parties ground truth in what's happening

With information sharing, the right data at the right time will enable effective real-time response

Communications

NOW

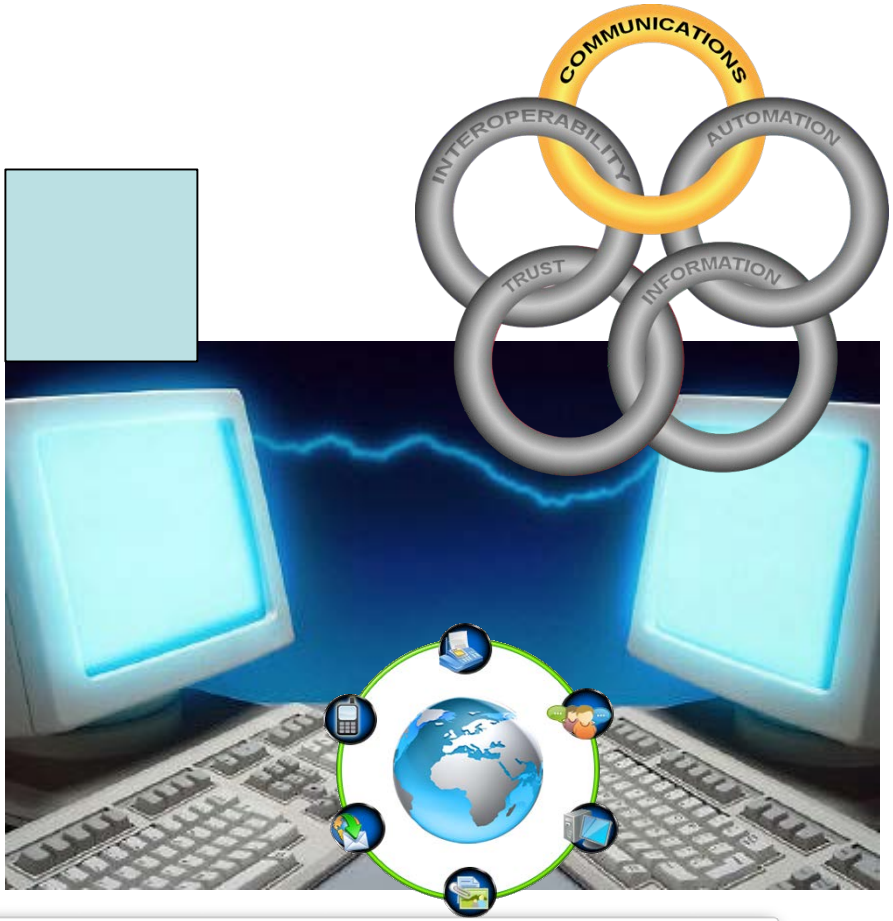
- Resilient Communications
- Priority Services
- Interconnected Infrastructures

SOON

- Full data redundant comms
- Multiple applications and vendors

FUTURE

- Resilient comms across the ecosystem



With assured communications, the adversary can't find a choke point to control