Strengthening the Cyber Ecosystem

Dr. Peter M. Fonash
Chief Technology Officer
Office of Cybersecurity & Communications

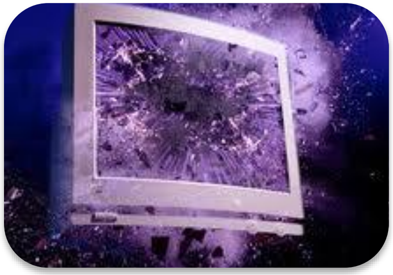
September 8, 2016

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.

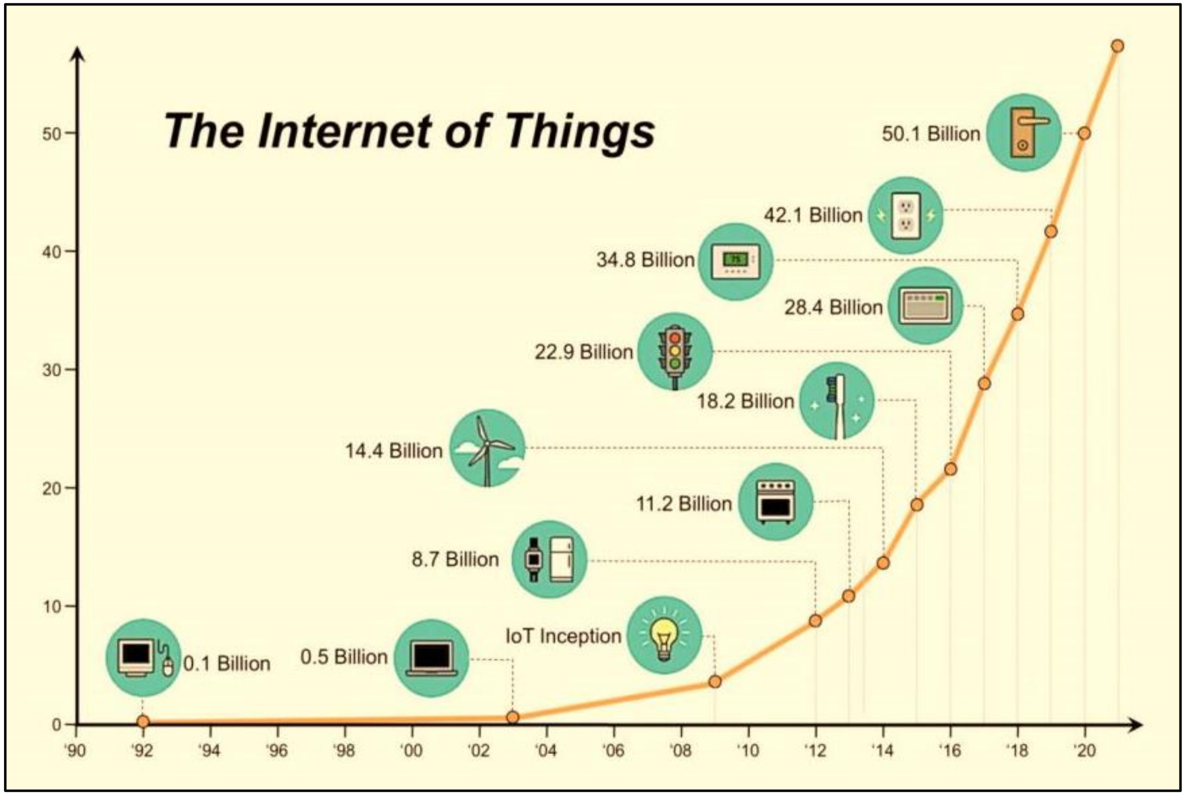
In the cyber realm, we help the ***dot gov*** and ***dot com*** domains secure themselves, focusing on critical infrastructure.



Our Challenges Grow Bigger and More Complex

We are members of a vast and expanding cyber ecosystem which consists of:

- Government and private sector information infrastructure, including international
- The interacting persons, processes, data, information and communications technologies



The cybersecurity challenge is growing every year

- The ecosystem is predicted to grow to 50B devices by 2020 [1]
- We are Increasingly reliant on cyber technologies
- The explosion in endpoints leads to an explosion in the number of opportunities for attackers

[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
2/2/2015	Boston Baskin Cancer Foundation	56,694	Patient Records
2/5/2015			
2/24/2015			
2/27/2015			
3/16/2015			
3/17/2015			
5/20/2015			
5/26/2015	IRS	700,000	F
6/4/2015	OPM	21,500,000	P
7/17/2015	UCLA Health System	4,500,000	
7/19/2015	Ashley Madison	37,000,000	Finan
9/10/2015	Excellus Blue Cross Blue Shield	10,000,000	F
10/1/2015	Scottrade	4,600,000	Name resses
10/1/2015	Experian	15,000,000	Personal data
11/9/2015	Comcast	590,000	email/passw ords
11/30/2015	Vtech	4,800,000 parents 6,400,000 children	Personal data
1/4/2016	Regional Income Tax Agency	50,000	
1			
1			
2			
2			
2/10/2016	IRS	101,000	Social Security Numbers
3/4/2016	21st Century Oncology	2,200,000	Patient Records

Reported June 2015:
18 Million Detailed Federal
Employee Records
Compromised

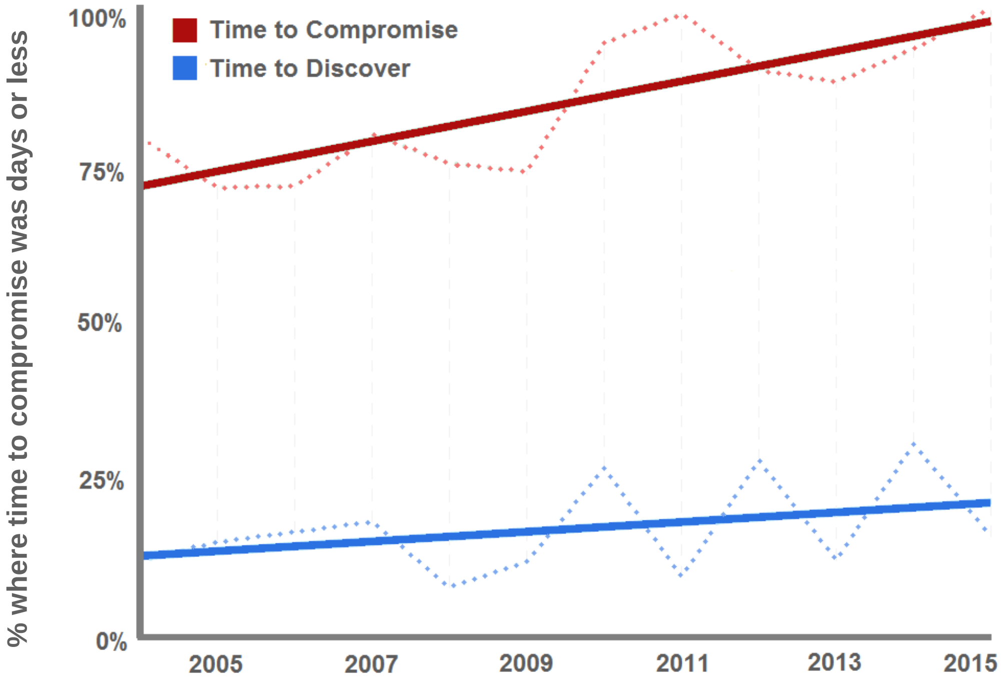
March 2016:
MedStar Hospitals
Struck by Ransomware

MedStar Georgetown University Hospital
HACKERS PARALYZED HOSPITAL CHAIN
This is a Tobacco-Free Campus

Privacy Rights Clearinghouse - http://www.privacyrights.org/data-breach
Credit Union Times - http://www.cutimes.com/2016/01/07/10-biggest-data-breaches-of-2015

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

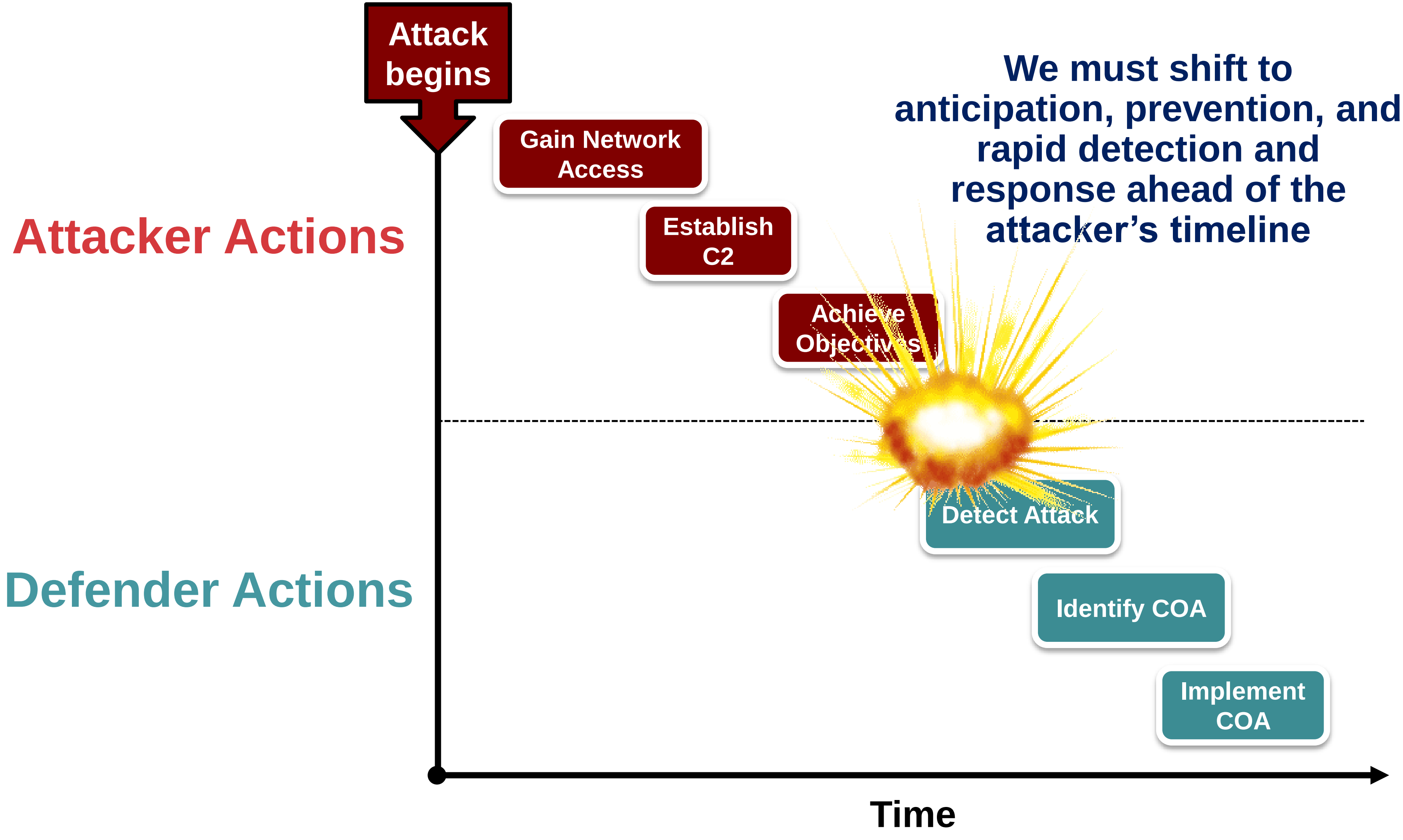
Our Opponents Improve Faster than We Do



Adapted from the 2016 Verizon Data Breach Investigations Report [3]

- Volume, sophistication of attacks go up while cost and risk to attackers decreases
- Attackers continue to improve their methods faster than defenders can adapt

Our Detection and Mitigation is Too Slow



We must shift to anticipation, prevention, and rapid detection and response ahead of the attacker’s timeline

The Way Forward: Enabling Effective and Efficient Risk Mitigation

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 innovating faster than defenders can adapt. IoT greatly expands the attack surface. Insufficient security analysts to meet future requirements. Defender ability to detect and respond to intrusions too slow.	*AUTOMATION*	Common Data Model Orchestration Shared COAs Security Architecture
Limited automated authentication. Lack of organizational partnerships and relationships. Insufficient trust to share and execute defensive courses of action.	*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 is vulnerable to attack. There is no resilient infrastructure to support assured communications.	*ASSURED COMMUNICATIONS*	Resilient Communications Priority Services Interconnected Infrastructures

Investigating the Concepts

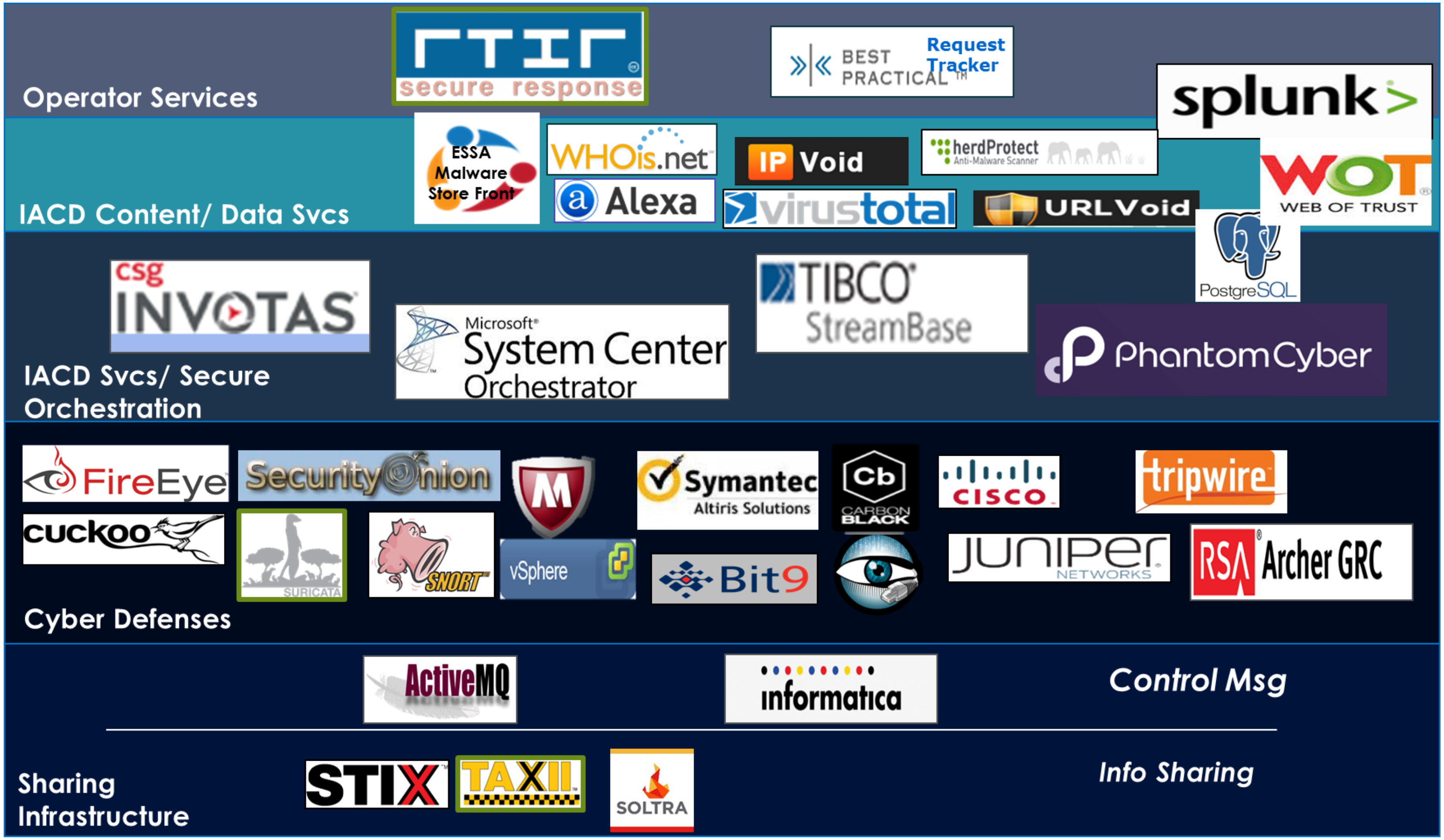
To demonstrate capabilities to meet the challenges we tested our ability to integrate and automate security operations using diverse commercial off-the-shelf products investigated via middleware and controlled by orchestration.

	Triage Capacity	Alert to Decide	
		Best	Worst
No automation or integrated tools	65 events/day	10 mins	11 hours
Automation and integration	6,500 events/day	1 second	10 minutes

- Automated indicator sharing via STIX achieved in seconds
- COAs shared in seconds to minutes

Integrating Across a Diverse Tool Set

We showed It is possible to automate off-the-shelf cybersecurity products from a range of vendors. Products from the companies below were successfully integrated in our investigations.



Operator Services

IACD Content/ Data Svcs

IACD Svcs/ Secure Orchestration

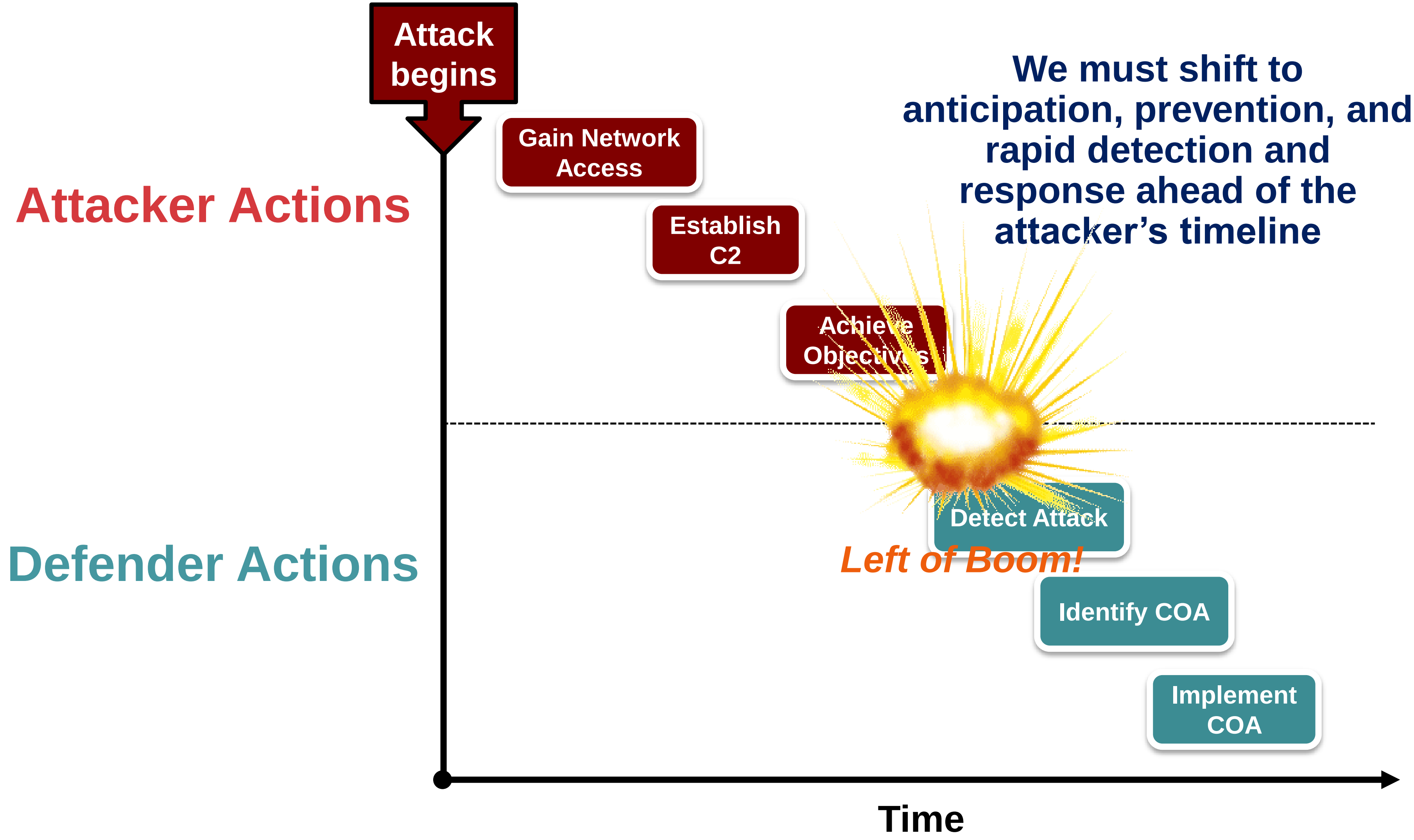
Cyber Defenses

Control Msg

Info Sharing

Sharing Infrastructure

We Can Accelerate Detection and Mitigation

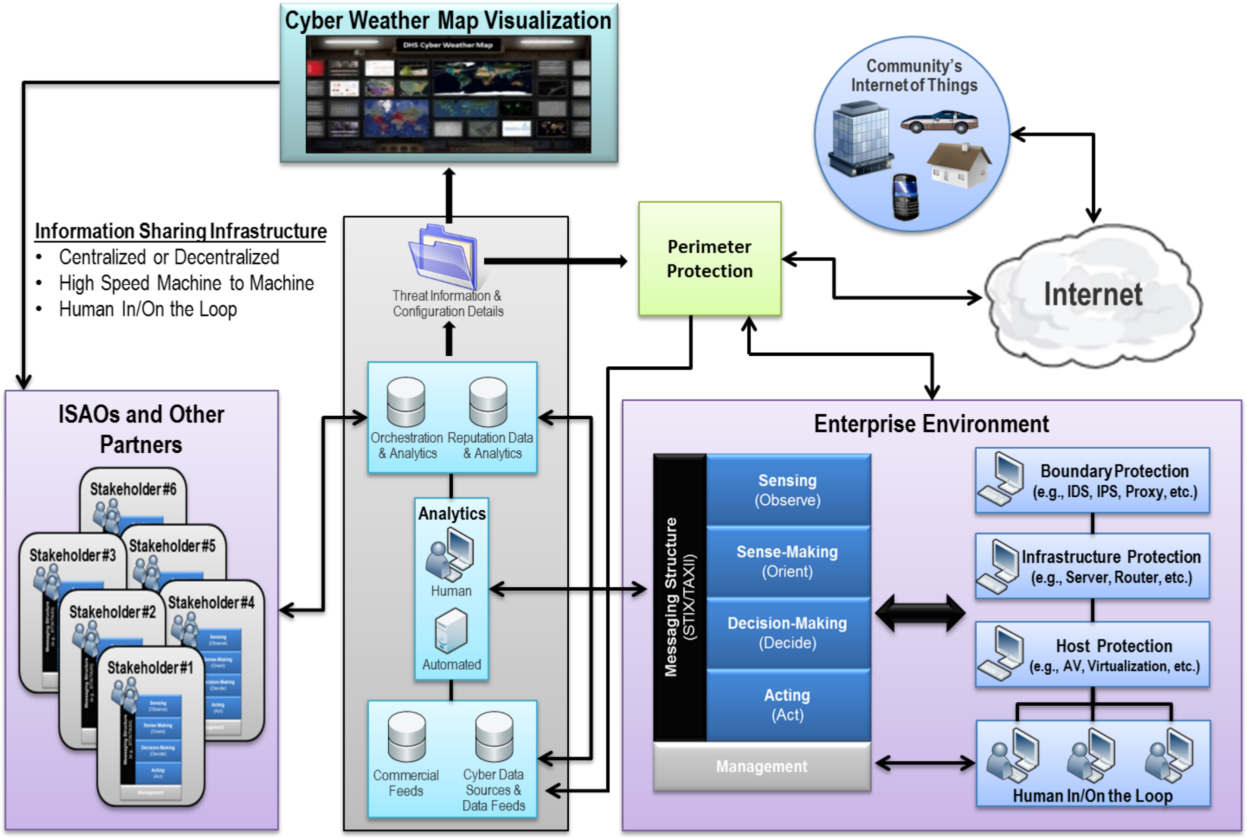


We must shift to anticipation, prevention, and rapid detection and response ahead of the attacker's timeline

Cyber Ecosystem Example Architecture

Components

- *Enterprise Environment*
- *Cyber Weather Map*
- *Information Sharing Infrastructure*


Cyber Weather Map Visualization
DHS Cyber Weather Map
Community's Internet of Things
Information Sharing Infrastructure
• Centralized or Decentralized
• High Speed Machine to Machine
• Human In/On the Loop
Threat Information & Configuration Details
Perimeter Protection
Internet
Orchestration & Analytics
Reputation Data & Analytics
Analytics
Human
Automated
Commercial Feeds
Cyber Data Sources & Data Feeds
ISAOs and Other Partners
Stakeholder #6
Stakeholder #5
Stakeholder #4
Stakeholder #3
Stakeholder #2
Stakeholder #1
Enterprise Environment
Messaging Structure (STIX/TAXII)
Sensing (Observe)
Sense-Making (Orient)
Decision-Making (Decide)
Acting (Act)
Management
Boundary Protection (e.g., IDS, IPS, Proxy, etc.)
Infrastructure Protection (e.g., Server, Router, etc.)
Host Protection (e.g., AV, Virtualization, etc.)
Human In/On the Loop

Accomplishments and Ongoing Efforts to Date

- RFI on Enterprise Automated Security Environment
- Thought Leaders Roundtable on Enterprise Automated Security Environment Vision
- Workshop on Interoperability, Automation, Information Sharing, and Architectures
- Courses of Action Working Group – OpenC2
- Formation of a Focus Group to discuss a common message fabric
- Public release of the white paper titled: “Enabling Adaptive and Interoperable Cyber Defense: Message Fabric Integration and Standardization”
- In the process of bringing together Interagency partners and private sector stakeholders to develop common message fabric specifications

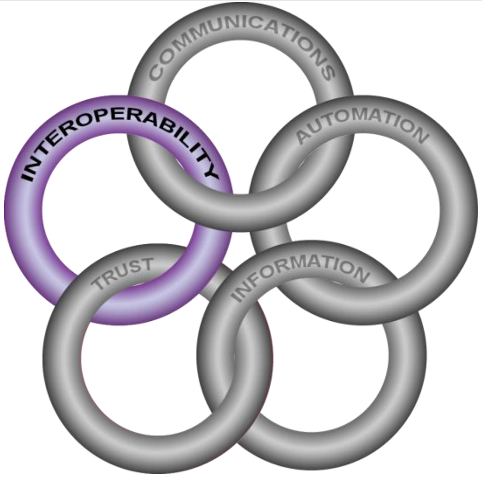
Where We Want to Go

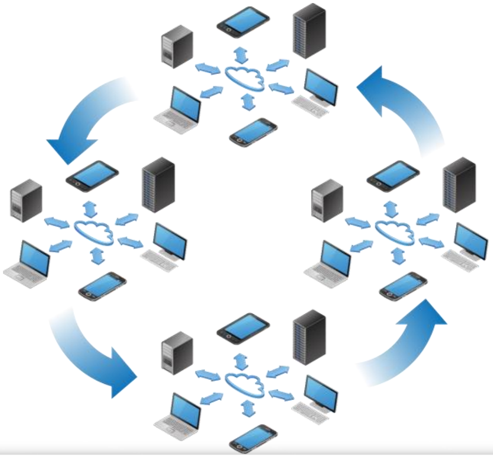
***Secure* integration and automation across a diverse, changeable array of cyber defense capabilities**

- Secure 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
- Security operations processes and procedures are codified
- Provide operational and acquisition freedom to take advantage of diverse, changing, advanced solutions without wholesale changes to every system

BACKUP

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

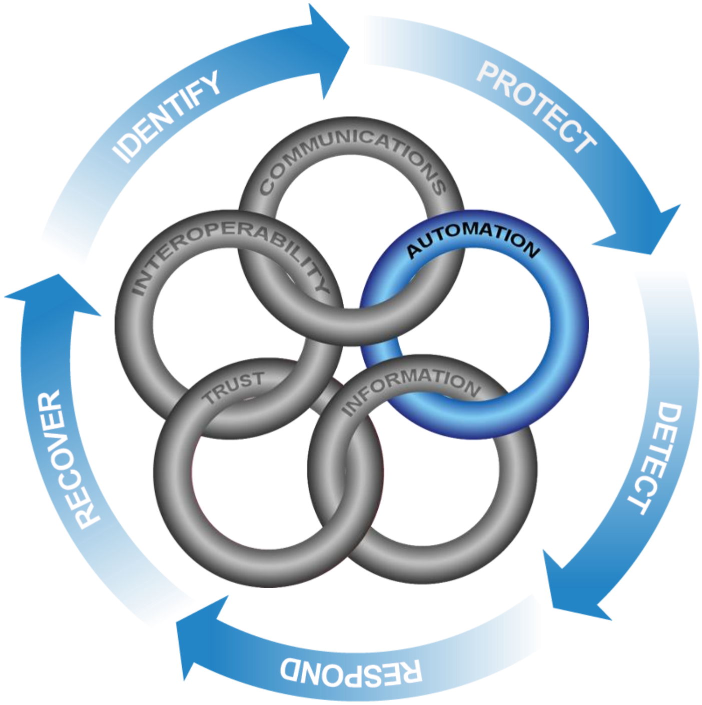
- Common Data Model
- Orchestration

SOON

- Shared COAs

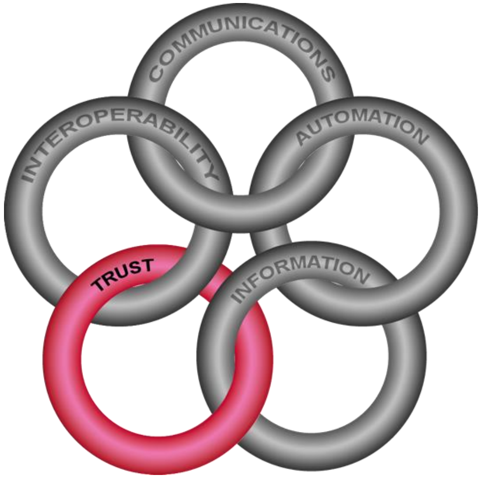
FUTURE

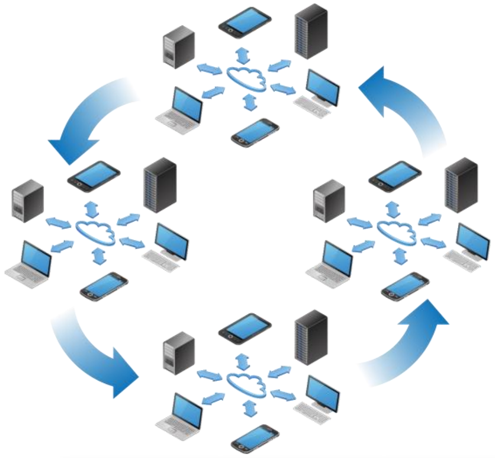
- Fully distributed autonomous response
- Humans controlling how aggressive automation should be (risk appetite)
- We can "undo" undesirable automated actions



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

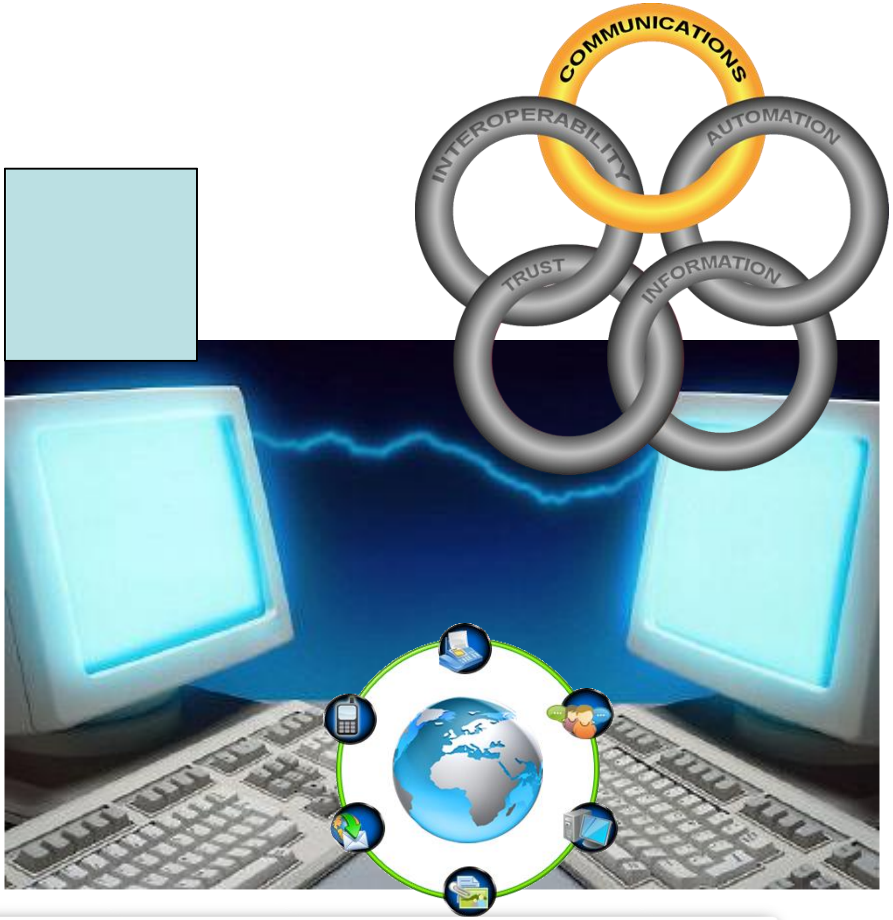
- Resilient Communications
- Priority Services
- Interconnected Infrastructures

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