Integrated Adaptive Cyber Defense

The Evolution of IACD

Harley Parkes

The Johns Hopkins University Applied Physics Laboratory

IACD Experimentation: The Beginning

0 **Make it Real**

July '14 **0**

Make it Real
Quickly establish the ability to automate and integrate

IACD Spiral Efforts to Inform Framework

0	Make it Real
1	Scalability and Automated Indicator Sharing
2	Risk- and Mission-based COA Selection
3	Anomalous Behavior Mitigation & COA Sharing
4	Message Fabric Interoperability/ Interchangeability
5	Response Action Interoperability, Automated Hunt Operations Support
6	Secure Orchestration, Expanded Response Action Interoperability
7	Multi-orchestration Integration, IT/OT Integration, Workflow Integrity
8	Automated Restoration After Destructive Malware
9	Autoimmunity in Information Sharing
10	Reversibility

IACD

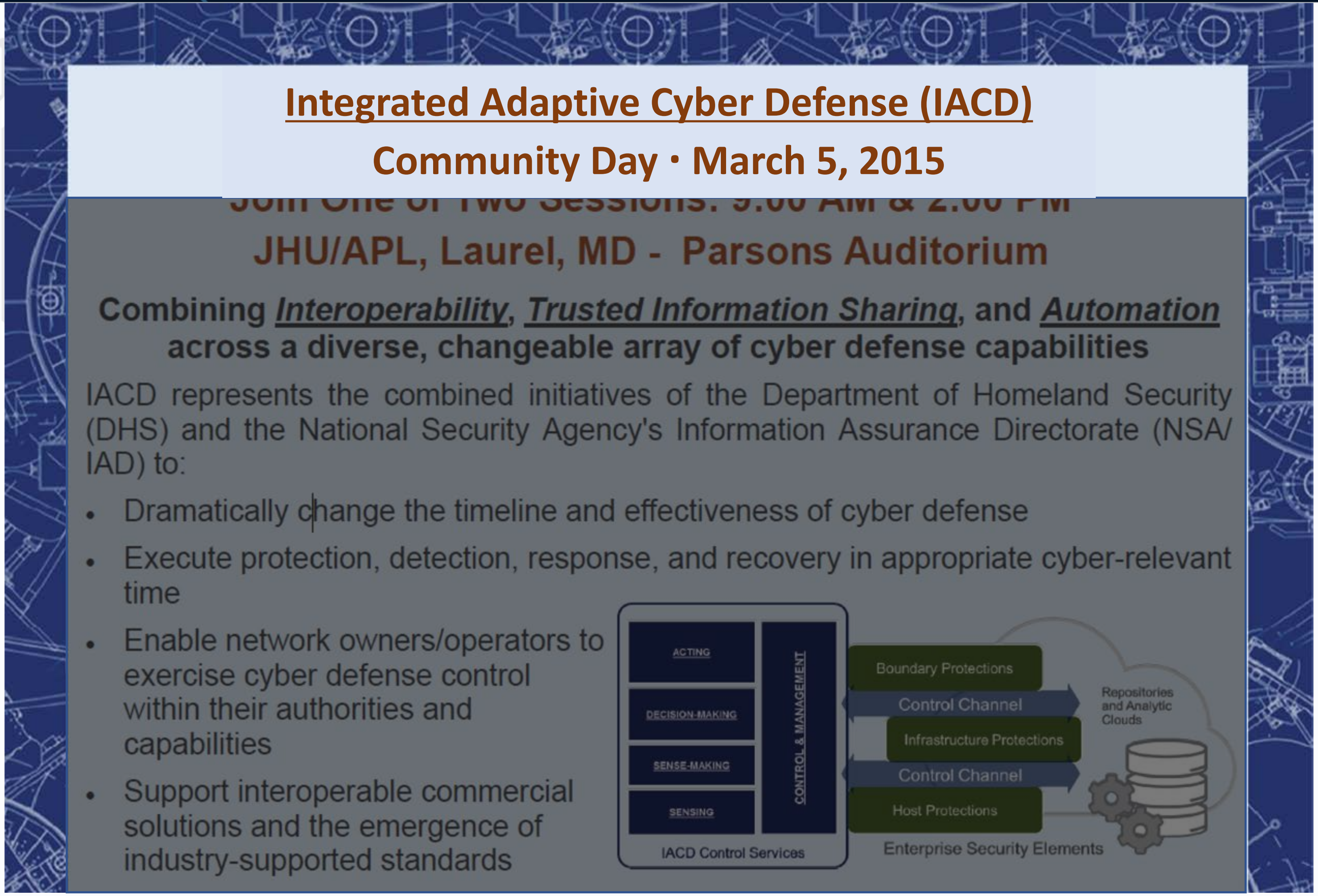
Accelerating the Speed and Scale of Cyber Defense

Integrated Adaptive Cyber Defense
IACD
Accelerating the Speed and Scale of Cyber Defense
Framework

Published IACD Framework Includes:

- IACD Baseline reference architecture
- Orchestration Services Specification
- Playbook Specification
- Orchestration Services key considerations for security, selection, and operational use
- IACD Reference Playbooks

First IACD Community Day



Integrated Adaptive Cyber Defense (IACD)

Community Day · March 5, 2015

Join One of Two Sessions: 9:00 AM & 2:00 PM

JHU/APL, Laurel, MD - Parsons Auditorium

Combining *Interoperability*, *Trusted Information Sharing*, and *Automation* across a diverse, changeable array of cyber defense capabilities

IACD represents the combined initiatives of the Department of Homeland Security (DHS) and the National Security Agency's Information Assurance Directorate (NSA/IAD) to:

- Dramatically change the timeline and effectiveness of cyber defense
- Execute protection, detection, response, and recovery in appropriate cyber-relevant time
- Enable network owners/operators to exercise cyber defense control within their authorities and capabilities
- Support interoperable commercial solutions and the emergence of industry-supported standards

First IACD Community Day - Agenda

Focused on APL Content

DHS CS&C & NSA IAD

- Welcome

JHU/APL IACD Team

- ACD/IACD Background
- IACD Activities & Approach
- Federated Innovation, Integration & Research Environment (FIIRE)
- Spiral 0: Making It Real – Summary & Results
- Spiral 1: Scalability & Automated Indicator Sharing - Demonstration
- Spiral 2: Risk- and Mission-based Decision Complexity – Looking Ahead

All

- Discussion/Questions/Feedback – Parsons Auditorium & Barton Room

Final Community Day Agenda

Integrated Adaptive Cyber Defense (IACD) Community Day – March 23, 2017

0830 – 0840	**Welcome**
0840 – 0915	**IACD Overview and the IACD Framework**
0915 – 1000	**Spirals 6 & 7: IACD Implementations and Findings**
1000-1015	**Break – Poster Sessions on Mezzanine**
1015 – 1130	**External IACD-associated Demonstrations and Presentations**
1015-1040:	Anomali/STAXX - Modularization of Information Sharing
1040-1105:	Symantec - OpenC2 Proxy Prototype
1105 – 1130:	WWT - Look Ma – No Hands!
1130-1140	**Overview of Breakout Sessions/Afternoon Logistics**
1140-1215	**Lunch – Networking, Poster Sessions**
1220 – 1335	**Breakout Sessions by Community**
1340 - 1400	**Reconvene – Discussions, Q&A, Close out**

Integrated Cyber

Accelerating the Speed and Scale of Cyber Defense

Johns Hopkins University Applied Physics Laboratory
Laurel, Maryland, 16-17 October, 2017

https://secwww.jhuapl.edu/iacd

Welcome:

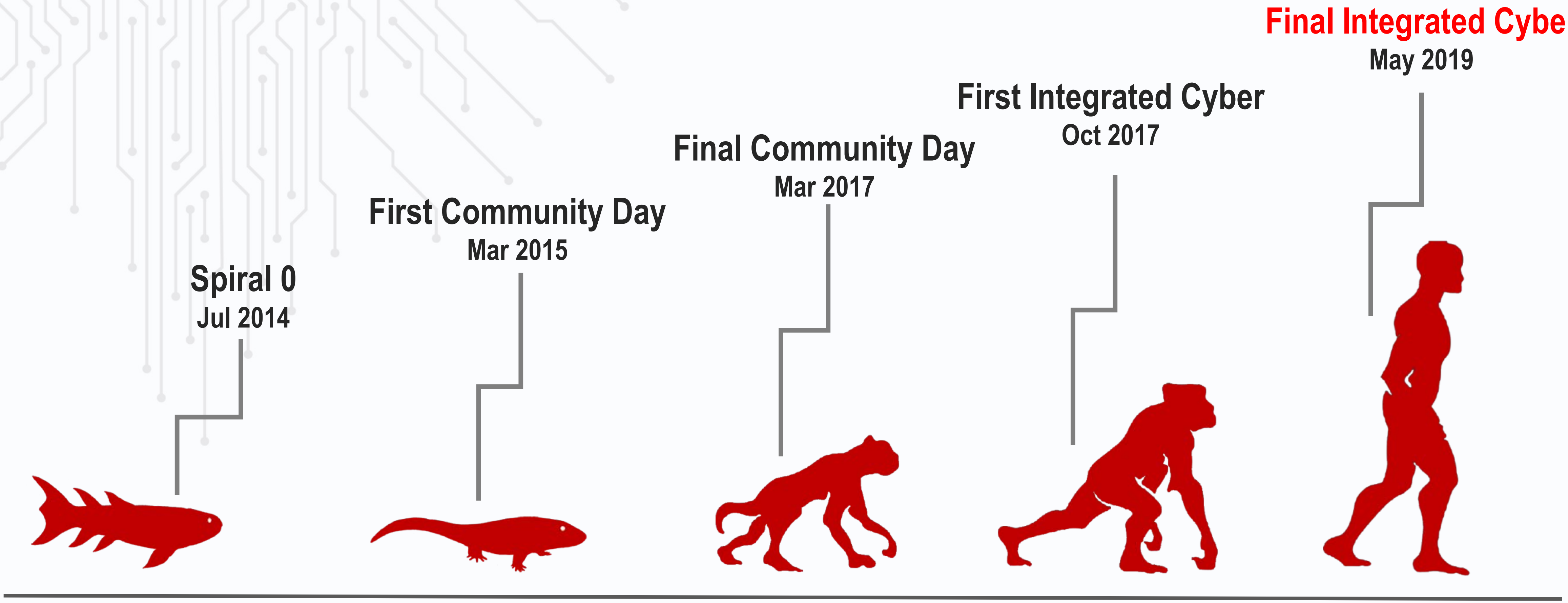
Integrated Cyber Fall 2017

IACD
Integrated Adaptive
Cyber Defense

- 500+ Registrants
- 240+ Organizations
- 60+ Speakers
- 4 Keynotes
- 6 Panels
- 6 Tech Talks/Deep Dives
- 6 Community Central Sessions
- 3 Integrated Cyber 101 Sessions
- 2 Lunch Networking Sessions
- 1 Networking Social

AIS
Automated Indicator Sharing

THE Evolution of Integrated Cyber



Spiral 0
Jul 2014

First Community Day
Mar 2015

Final Community Day
Mar 2017

First Integrated Cyber
Oct 2017

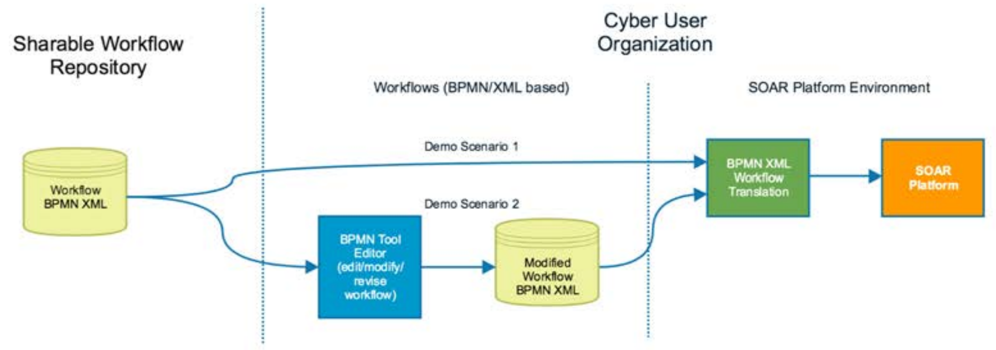
Final Integrated Cyber
May 2019

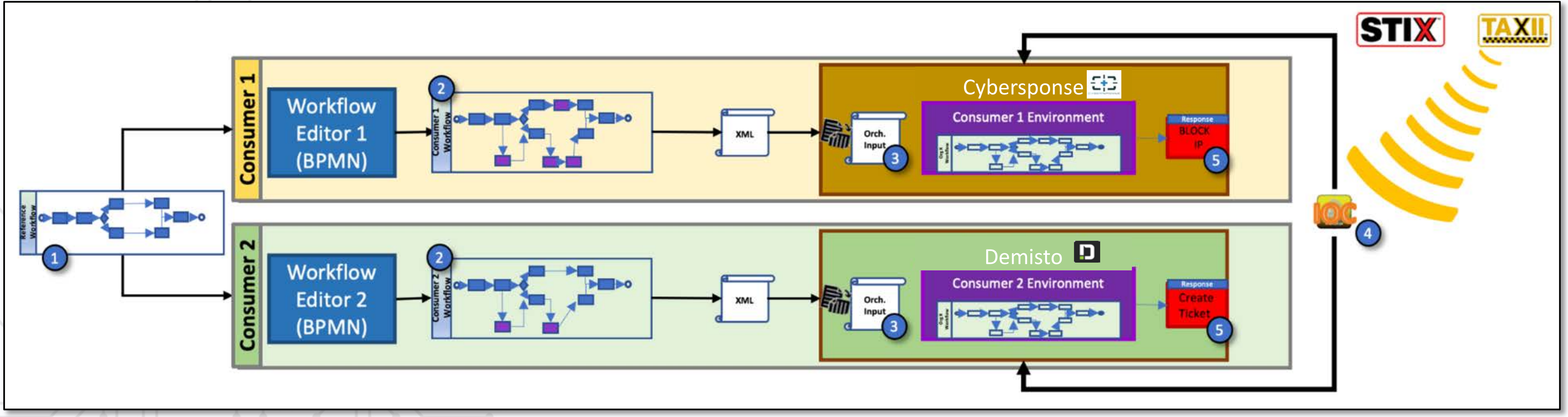
…defense at cyber-relevant speed…

IACD Community

Shareable Workflows Concept

- Uses established ISO open standard, BPMN/XML.
- Workflows ingestible into any BPMN tool
- Tailor to specific organization's local policies and business rules
- Automatic translation into SOAR-specific formats
- 2 SOARs have actively participated in this demonstration
- IOCs & TTorPs are "triggers" for shared workflows
- Can lead to organization-specific actions based on Risk Profile

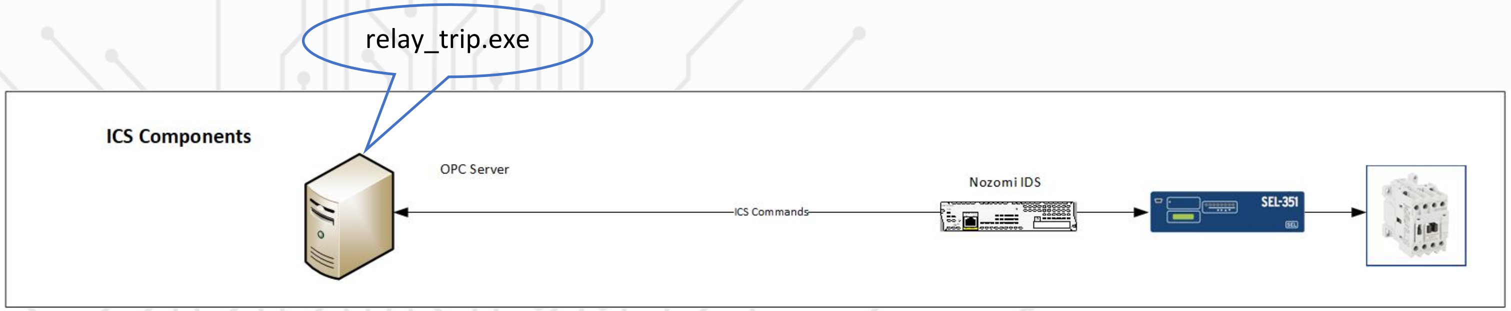

Sharable Workflow Repository
Cyber User Organization
Workflows (BPMN/XML based)
SOAR Platform Environment
Workflow BPMN XML
Demo Scenario 1
Demo Scenario 2
BPMN Tool Editor (edit/modify/ revise workflow)
Modified Workflow BPMN XML
BPMN XML Workflow Translation
SOAR Platform

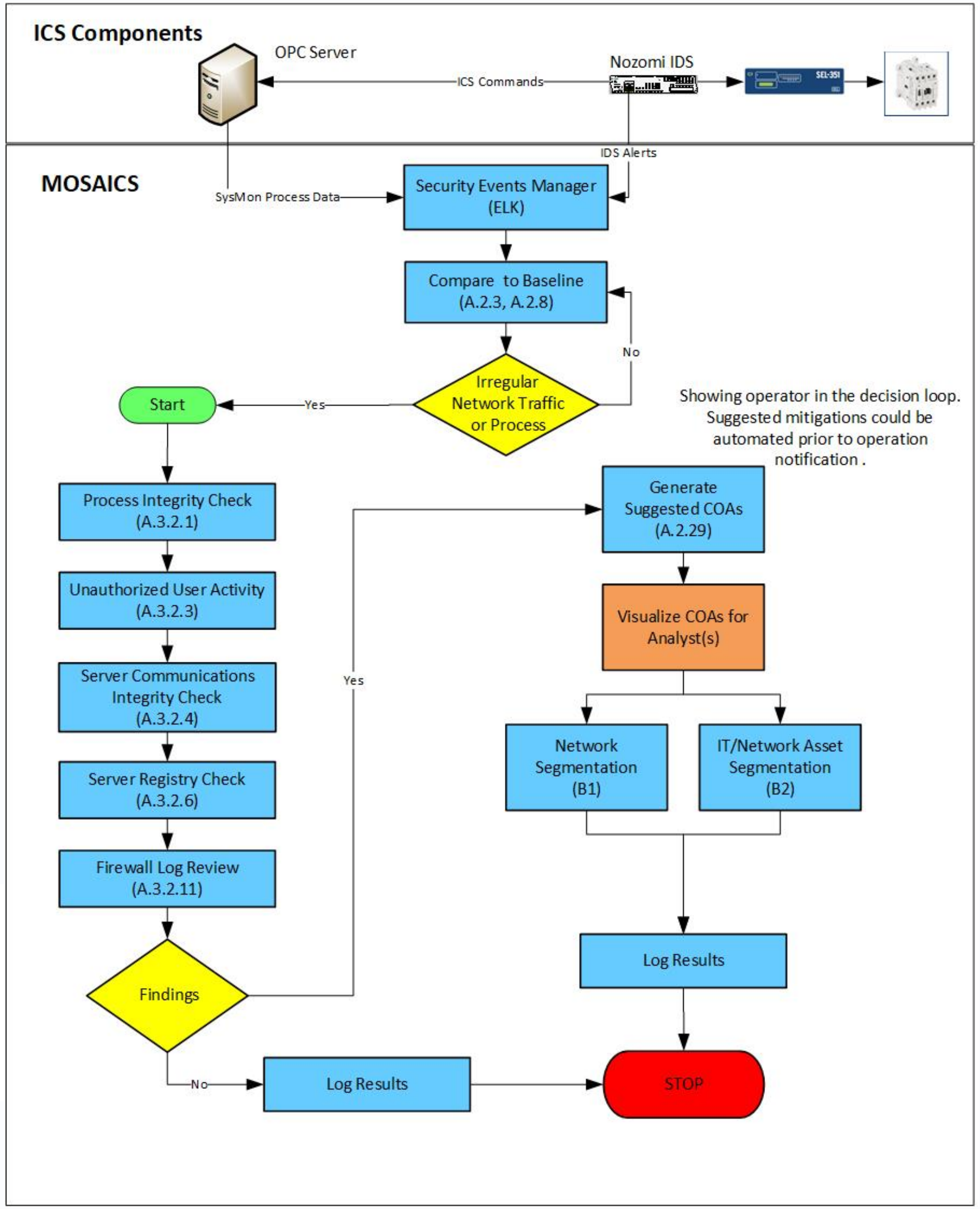


MOSAICS Spiral 0 Reference Implementation

Industrial Control Systems (ICS)

Attack Scenario - Malicious Process Detection and Response




ICS Components
OPC Server
ICS Commands
Nozomi IDS
SEL-351
IDS Alerts
MOSAICS
SysMon Process Data
Security Events Manager (ELK)
Compare to Baseline (A.2.3, A.2.8)
No
Irregular Network Traffic or Process
Yes
Start
Process Integrity Check (A.3.2.1)
Unauthorized User Activity (A.3.2.3)
Server Communications Integrity Check (A.3.2.4)
Server Registry Check (A.3.2.6)
Firewall Log Review (A.3.2.11)
Findings
Yes
No
Log Results
Generate Suggested COAs (A.2.29)
Visualize COAs for Analyst(s)
Network Segmentation (B1)
IT/Network Asset Segmentation (B2)
Log Results
STOP

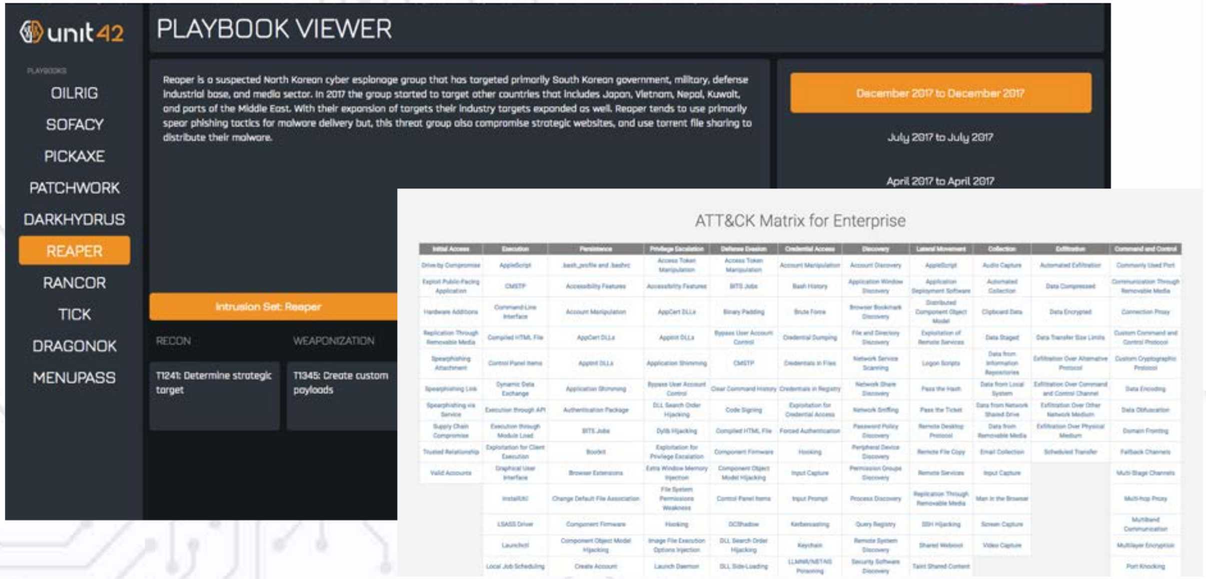
Showing operator in the decision loop. Suggested mitigations could be automated prior to operation notification .

Beyond Indicators: Scalable Network Defense

- **Current research on sharing Tactics, Techniques, or Procedures**

- **Utilization of Palo Alto's Adversary Playbooks and MITRE's ATT&CK**

- **Identification of triggers for automation workflows within adversary playbook**



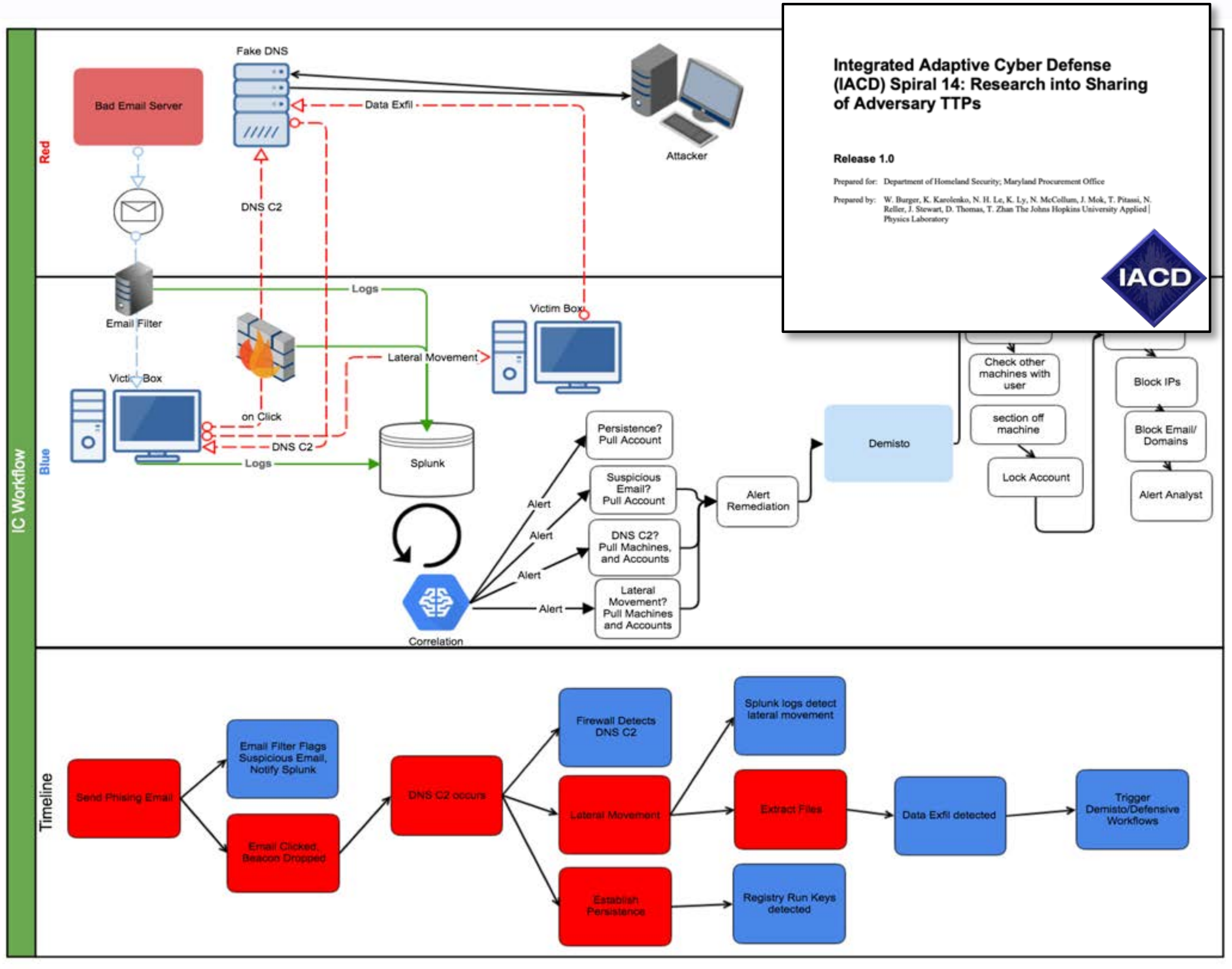
Reaper is a suspected North Korean cyber esplonage group that has targeted primarily South Korean government, military, defense industrial base, and media sector. In 2017 the group started to target other countries that includes Japan, Vietnam, Nepal, Kuwait, and parts of the Middle East. With their expansion of targets their industry targets expanded as well. Reaper tends to use primarily spear phishing tactics for malware delivery but, this threat group also compromise strategic websites, and use torrent file sharing to distribute their malware.

T1241: Determine strategic target

T1345: Create custom payloads

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking	Screen Capture		Multiband Communication
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Keychain	Remote System Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Local Job Scheduling	Create Account	Launch Daemon	DLL Side-Loading	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking



Integrated Adaptive Cyber Defense (IACD) Spiral 14: Research into Sharing of Adversary TTPs

Release 1.0

Prepared for: Department of Homeland Security; Maryland Procurement Office

Prepared by: W. Burger, K. Karolenko, N. H. Le, K. Ly, N. McCollum, J. Mok, T. Pitassi, N. Reller, J. Stewart, D. Thomas, T. Zhan The Johns Hopkins University Applied | Physics Laboratory

IACD Roadmap - What's Next?

Improving Information Sharing participation

- Eliciting Trust: indicator scoring, provenance/source
- Incentivizing information sharing
- Identifying the most useful types of information to share (e.g., tactics vice indicators)
- Design/Implement the next generation architecture for Cyber Information Sharing

Leveraging Artificial Intelligence

- Sense-making analytics
- Decision Support (Orchestration workflow design and testing)
- Automating support to equity review and classification determination

Evolve to Fit Emerging Cybersecurity Landscape

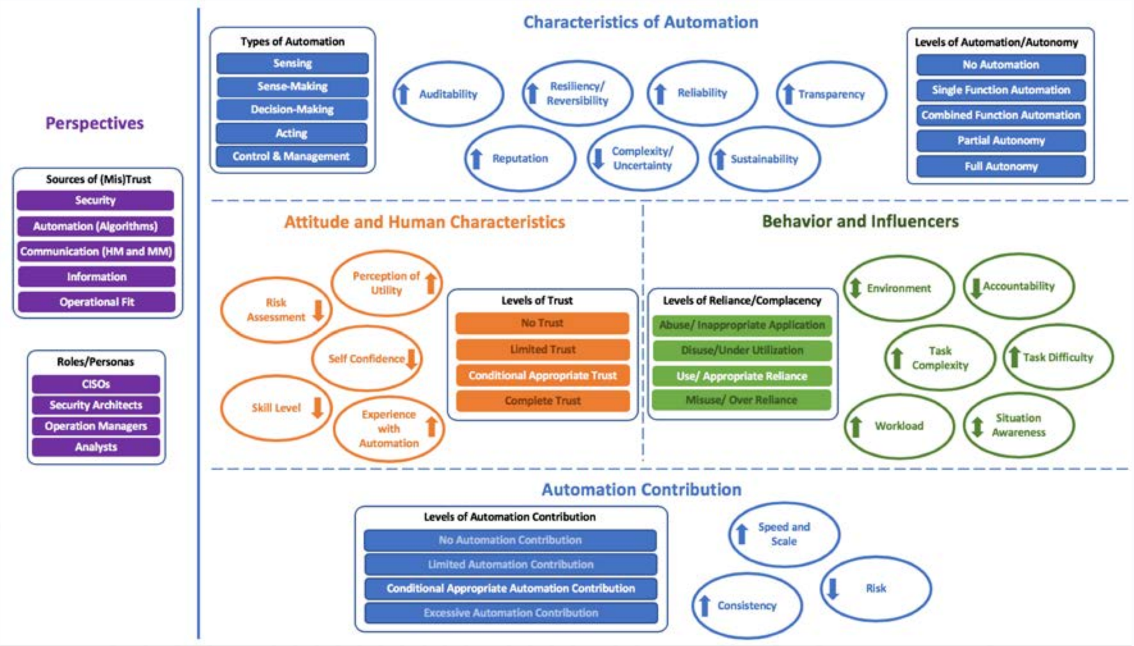
- Incorporating Shared Services
- Moving from Boundary Protection to Information Protection
- Moving from Centralized to Decentralized Information Sharing
- Holistic approach to security and operations
- Impact driven—not just event or threat driven

Automation Security

- Orchestrator Hardening
- Secure Credential Access/Storage
- Trusted M2M Authentication
- Protection Profile

Improve the Security of Automation

As we increasingly automate our cybersecurity operations, automated systems become lucrative targets. We need to ensure those systems have a security level commensurate with their criticality.



Perspectives

Sources of (Mis)Trust
- Security
- Automation (Algorithms)
- Communication (HM and MM)
- Information
- Operational Fit

Roles/Personas
- CISOs
- Security Architects
- Operation Managers
- Analysts

Characteristics of Automation

Types of Automation
- Sensing
- Sense-Making
- Decision-Making
- Acting
- Control & Management

↑ Auditability

↑ Resiliency/ Reversibility

↑ Reliability

↑ Transparency

↑ Reputation

↓ Complexity/ Uncertainty

↑ Sustainability

Levels of Automation/Autonomy
- No Automation
- Single Function Automation
- Combined Function Automation
- Partial Autonomy
- Full Autonomy

Attitude and Human Characteristics

Risk Assessment ↓

Perception of Utility ↑

Self Confidence ↓

Skill Level ↓

Experience with Automation ↑

Levels of Trust
- No Trust
- Limited Trust
- Conditional Appropriate Trust
- Complete Trust

Behavior and Influencers

Levels of Reliance/Complacency
- Abuse/ Inappropriate Application
- Disuse/Under Utilization
- Use/ Appropriate Reliance
- Misuse/ Over Reliance

↕ Environment

↓ Accountability

↑ Task Complexity

↑ Task Difficulty

↑ Workload

↕ Situation Awareness

Automation Contribution

Levels of Automation Contribution
- No Automation Contribution
- Limited Automation Contribution
- Conditional Appropriate Automation Contribution
- Excessive Automation Contribution

↑ Speed and Scale

↑ Consistency

↓ Risk

- *Harden orchestrators* – Security orchestrators are at the core of security automation. We need to investigate designs that ensure their security against compromise.
- *Design secure credential access/storage* – The ability of the orchestrator to authenticate itself to security capabilities and services makes a strong case for a secure and available credentialing infrastructure to support needed automated operations.
- *Implement trusted M2M authentication* – The ability for services to authenticate to each other at machine speed (as opposed to relying on person-based credentials) is critical for security automation. We need to ensure trust mechanisms for those machine-to-machine credentials.
- *Establish an orchestration Protection Profile* – Formalize the considerations for evaluating orchestrator security.
- *Architect playbook provenance* – Establish the mechanisms for understanding the origins of playbooks in order to evaluate their trustworthiness and applicability to a given context.

Integrated Cyber May 2 & 3, 2019

Trust in Automation and Autonomy

Aubrey Merchant-Dest

Federal CTO

Symantec

Geoff Hancock

Chief Cybersecurity Executive

ADVANCED CYBERSECURITY GROUP

Juhee Bae

Product Manager

GENERAL DYNAMICS Mission Systems

Jennifer Ockerman

Cognitive Systems Engineer

APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY

IACD

The Evolution of Cyber Security

Leveraging Artificial Intelligence

Artificial intelligence and machine learning hold the promise of substantially improving portions of sensing, sense-making, decision-making, and even evaluating the efficacy of actions that have been taken. How do we leverage the progress being make in this area to speed information sharing and increase automated response actions?

- *Implement shareable, sense-making analytics* – Address the critical need to rapidly assess and utilize the information that is flowing in from multiple sources at the speed and scale needed to anticipate and respond to changing situations; and share the 'how to' with others.
- *Advance Automated Decision Support* – Accelerate progress to rapidly assess potential response actions and provide suggested responses for humans 'in the loop', and accurately determine and implement high-benefit/low-regret responses for humans 'on the loop.'
- *Automate support to equity review, analytic review, and classification determination* – Every information provider has equity concerns about the information they share. At the same time, the value of cyber information decays rapidly over time. This addresses moving these manual processes to the speed of relevance. We need to speed the ability to make accurate equity and classification determinations while the information has greatest value.

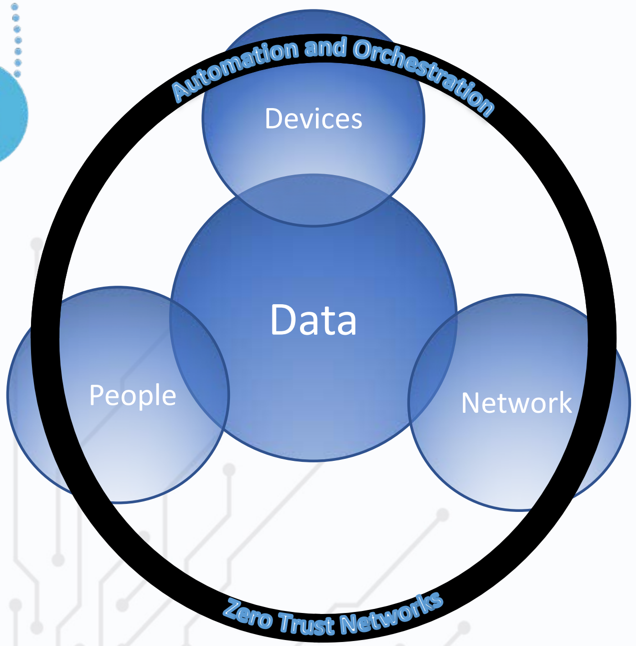
Evolve to Fit the Emerging Cybersecurity Landscape

Cloud services are playing an increasingly important role. Further, there is an increasing understanding of the need to have information-focused, rather than system-focused security.

ICS Protection

Facilities Engineer

Cyber Defender



- *Incorporate Shared Services* – Determine how best to apply the principles of security automation, interoperability, and information sharing in the context of cloud services.
- *Expand Beyond Boundary Protection to Information Protection* – With the decline in firm boundaries, determine how best to exercise fine-grained control and protection for information.
- *Include Both Centralized and Decentralized Information Sharing* – Moving beyond only a hub and spoke information sharing model, to one that enables and fosters peer-to-peer sharing of information and defensive actions within and among communities of trust.
- *Unify the approach to security and operations* – There is an emerging need to fully integrate cybersecurity systems and processes with the operational/mission portions of the enterprise. Determine how that affects the content and processes for sharing cybersecurity information.
- *Impact driven—not just event or threat driven* – Move from a severity model that only considers threats and events, to one that also considers impacts and risks.

IACD

Integrated Cyber
Spring 2019

The Evolution of Cyber Security

May 2 & 3, 2019

Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road, Laurel, MD 20723

www.iacdautomate.org

Integrated Adaptive Cyber Defense is sponsored by the Department of Homeland Security and the National Security Agency in collaboration with The Johns Hopkins University Applied Physics Laboratory.

Our goal is to dramatically change the timeline and effectiveness of cyber defense via integration, automation, and information sharing.

IACD
Accelerating the Speed and Scale of Cyber Defense

http:// https://iacdautomate.org

@IACD_automate

https://www.linkedin.com/groups/8608114

icd@jhuapl.edu