

Integrated Cyber

DAY TWO

COMMUNITY CENTRAL:

IACD Integrator Community of Interest

Harley Parkes & Cory Huyssoon, JHU/APL ICD



Featuring:

Hugh Pyle, IBM Resilient

Richard Shok, US Bank



IBM Resilient



Integrator Community of Interest

Integrated Cyber
Johns Hopkins University Applied Physics Laboratory
Laurel Maryland, May 1-2, 2018

<https://secwww.jhuapl.edu/iacd>



Agenda

- **Integrator Community of Interest (COI) Overview**
- **Community Presentation – IBM Resilient**
- **Community Presentation – US Bank**
- **Website Presentation**
- **Next Steps**
 - **Community Actions**
 - **Next Integrator COI**

Purpose and Goals

Purpose



To advance the adoption of IACD concepts across a broad range of customer operational environments

Goals



Establish or grow core competency of entities providing IACD services.



Expand IACD solution reach to meet growing demand.



Understand needs of the integration community.

Overall Plan

- **Engage Integrators of IACD capabilities**
 - Critical infrastructure sectors
 - Technical areas
- **Meet as a community quarterly to advance adoption of IACD concepts**
 - New technology trends
 - Technical details deploying IACD framework
 - Challenges and lessons adopting IACD in various environments
- **Promote growing a body of knowledge**
 - Core competencies and best practices of IACD services
 - Needs of both user and integrator communities
 - Share and capture measures and metrics for IACD

Opportunities

- **Connect with parties looking for assistance in deploying IACD concepts**
- **Access to IACD innovations available to business pursuits**
- **Opportunity to collaborate on technical challenges or solutions**
- **Influence over new or evolving specifications and standards**
- **Access to a community of industry partners determined to demonstrate the value and opportunities to advance IACD**

Topics/Themes for 2018

- **Jan 2018 (Virtual)**
 - Department of Energy Pilot
 - Financial Sector Pilot Initiative
- **May 2018 (Integrated Cyber)**
 - IBM Resilient
 - US Bank
 - IACD Website – integrator profiles
- **Jul 2018 (Virtual)**
 - Operational Deployment Lessons Learned
- **Oct 2018 (Integrated Cyber)**
 - Common Integrator Challenges and Needs



Community Presentation – IBM Resilient

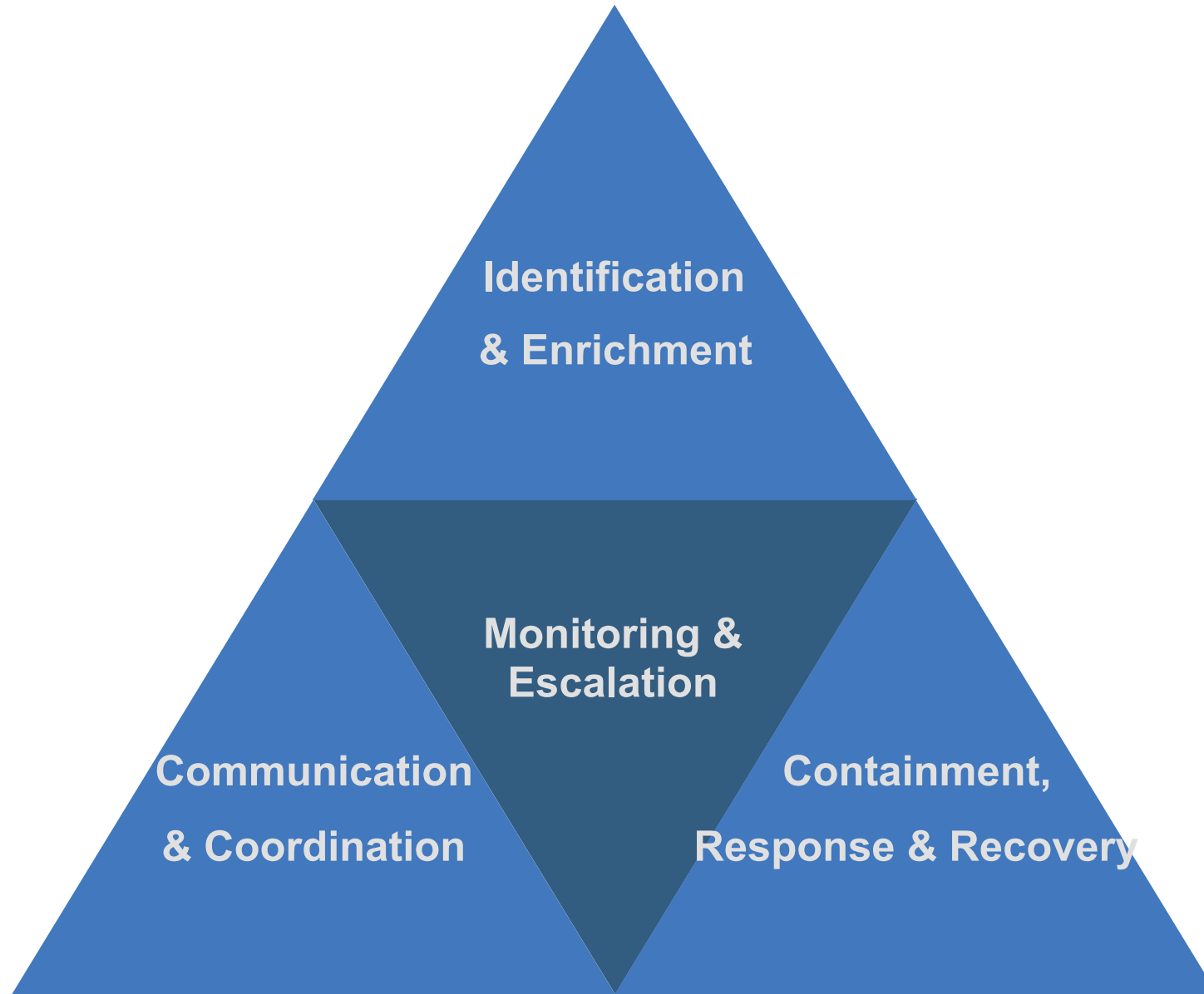
Orchestration & Automation for Incident Response

2018-05-02 IACD


Hugh Pyle

Product Manager, IBM Resilient

hpyle@us.ibm.com



Automation for Monitoring and Escalation

Details

Save Cancel

Owner

Due Date

Date Closed

Name

Phase

Creator Hugh Pyle

Date Initiated 03/18/2018 19:28

Instructions

Sans Serif Normal B I U

Review the Initial Alert (ex: SIEM, AntiVirus, Email, Firewall, IPS, IDS, Proxy) and Identify the following:

- Review any existing **Events** and or **Related Incidents** to assist with Triage and Analysis (Found in the Summary Section on the left-hand side of the Ticket).
- Collect any Indicators of Compromise (IOCs) and relevant information to support an Event/Incident Determination and any Response and Recovery actions (ex: Logs, Hashes, signatures, IP Addresses, ports, PCAPs, Vulnerability Scans, External Input, CMDB entries). Add these IOCs as **Artifacts** in the Artifacts Tab, and as Field Values as appropriate.
- Update the **Detection Sources** Field to add any new Alert sources discovered or referenced during the Initial Triage. Capture any specific Alert strings, Rule, Event and Offense values triggered in the **Detection Information** Field.
- Identify **Attack Vectors** if applicable.
- Identify affected **Endpoints/System Affected, Users/Employees Involved, and Data Compromised**.

Indicators of Compromise (IoCs) are any **Artifacts** of information observed on a system or network that can help an organization Identify, Protect, Detect, Respond and Recover to cyber threats. Examples of cyber threat information include IoCs, attacker Techniques, Tactics and Protocols (TTPs), security alerts, Threat Intelligence reports, and recommended security tool configurations.

For a comprehensive list of IoCs, Data Sources and Cyber Threat Information, Refer to Table 3-1 of the NIST Special Publication 800-150 - Guide to Cyber Threat Information Sharing:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>

Incident Fields

Detection Sources

Detection Information

Attack Vectors

Endpoints/Systems Affected

Search...

Name	Type	Operating System	Owner/Group	Data Encrypted	Location	IP Address	MAC Address	Critical Asset	Backup Created	Lost / Stolen / Mishandled	Notes
There is no data for this table											

Showing 0 to 0 of 0 entries

Automation for Monitoring and Escalation

What happened?

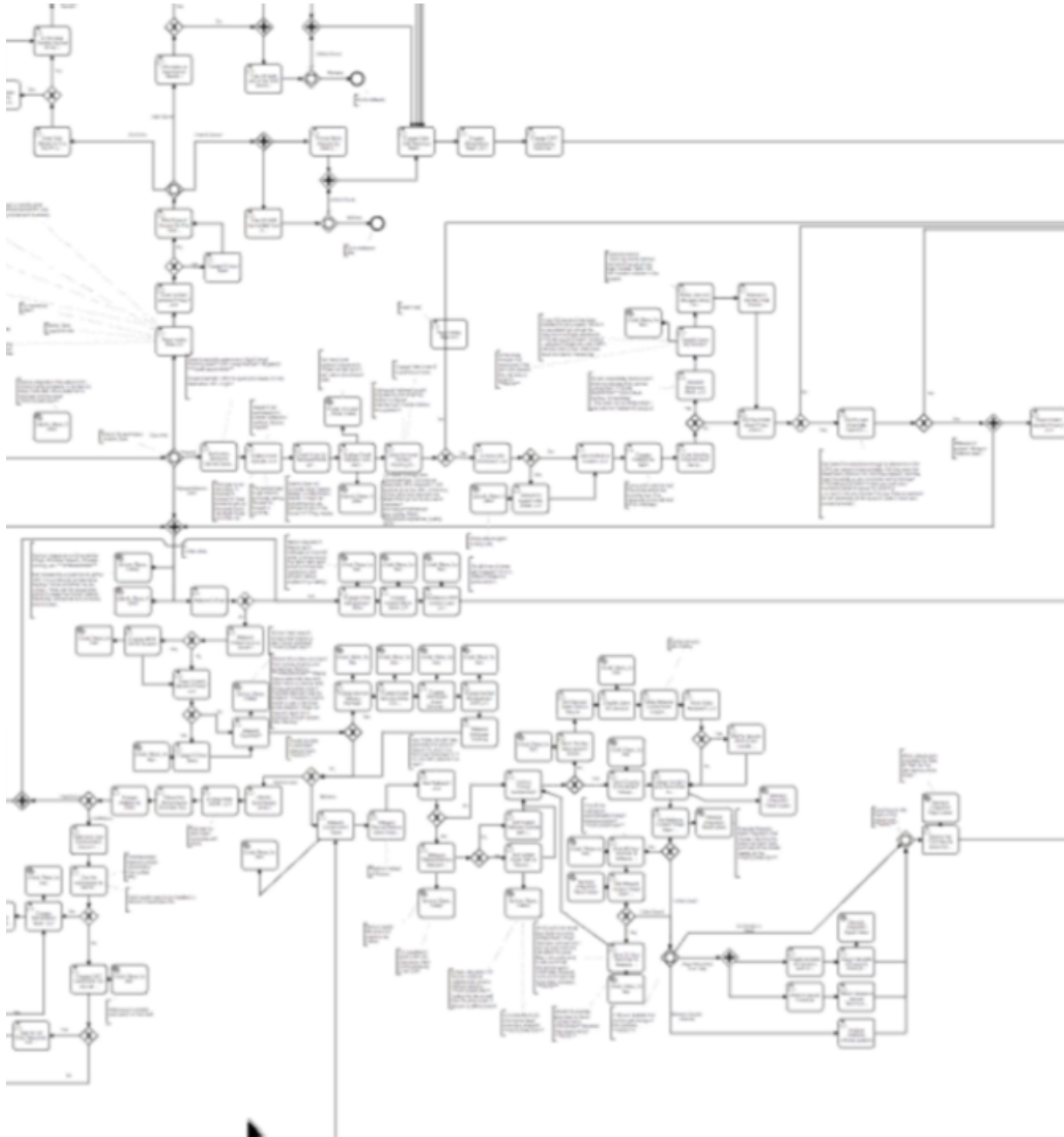
- Network activity
- File activity
- Email activity
- User activity
- SIEM and correlated alerts
- Other incoming

Automation for Monitoring and Escalation

- Use an incident response platform
- Escalate manually from noisy sources
- Escalate automatically if rare or reliable
- Monitor a mailbox

- **Examples:**
 - QRadar plugin
 - Splunk plugin
 - Symantec DLP, FireEye, CrowdStrike, etc.
- Data: Quality over quantity
- Volume of incidents creates your next problem!

Automation for Identification and Enrichment





Automation for Identification

Extract URLs/IPs from content

Extract URLs/IPs from behavior

Send observables to threat lookup

Send files to sandbox

- Threat Intel
- External Context

Automation for Enrichment

When else was this observed?

How did that get there?

How long has that been there?



























Who else hit these URLs?

Whose database server is that?

- Asset Intel
- Internal context

- Queries to directory, logs, databases, endpoints
- Pivot can be highly interactive

Automation for Containment, Eradication, and Recovery

☰ Containment  			
Task Name	Associated Rules		
☰ Select Containment Measures	(A) SI - General Security Incident	Disable	
☰ Disconnect Compromised/Affected Sys...	(A) SI - Host Investigation (A) SI - Lost/Stolen - Digital Assets More...	Disable	
☰ Sandbox Malware-Infected Endpoints	(A) SI - Malicious Code (A) SI - Ransomware	Disable	
☰ Gather Additional Forensics	(A) SI - Host Investigation (A) SI - Lost/Stolen - Digital Assets More...	Disable	
☰ Determine Remote Lock/Wipe Actions	(A) SI - Lost/Stolen - Digital Assets	Disable	
☰ Change Device/Application Passwords...	(A) SI - Host Investigation (A) SI - Lost/Stolen - Digital Assets More...	Disable	
☰ Update, Patch and Remediate Vulnera...	(A) SI - Host Investigation (A) SI - Lost/Stolen - Digital Assets More...	Disable	
☰ Block, Kill and Remove - Malicious ...	(A) SI - Malicious Code (A) SI - Ransomware	Disable	
☰ Stop Additional Data Loss	(A) PI - General Privacy Incident	Disable	
☰ Block IP Addresses & URLs Associate...	(A) SI - General Security Incident	Disable	
☰ Throttle or Block DoS Traffic	(A) SI - Denial of Service	Disable	
☰ Limit Propagation/Execution of the ...	(A) SI - Email Investigation (A) SI - Phishing (A) SI - Ransomware	Disable	
☰ Isolate Backup Media From Network	(A) SI - Ransomware	Disable	
☰ Contact Your Contracted ISP	(A) SI - General Security Incident	Disable	
☰ Notify Carrier/Service Provider	(A) SI - Lost/Stolen - Digital Assets	Disable	
☰ Contact Endpoint/System Owners	(A) SI - Denial of Service	Disable	
☰ Switch to Alternate Sites/Networks	(A) SI - Denial of Service	Disable	
☰ Notify System Owners of Attack	(A) SI - Email Investigation (A) SI - Phishing (A) SI - Ransomware	Disable	
☰ Notify Human Resources	(A) Situation - User/Employee Involved	Disable	
☰ Notify Legal Counsel of Criminal/Il...	(A) Situation - Criminal/Illegal Activity	Disable	
☰ Notify Public Relations Department	(A) Situation - Executive/VIP Involvement - High Severity	Disable	
☰ Secure Physical Location and Logica...	(A) PI - General Privacy Incident	Disable	
☰ Notify External Parties as Appropri...	(A) SI - General Security Incident	Disable	
☰ Notify Law Enforcement	(A) SI - Lost/Stolen - Digital Assets (A) Situation - Criminal/Illegal Activity	Disable	

Automation for Containment

- Capture and Isolate
- Block egress to these URLs
- Isolate this environment
- Deploy forensic tools
- Capture traffic, memory, activity
- Quarantine this email
- Quarantine this executable

Restore and Validate Baseline Operation:

- Remove Infection
- Re-image, restore, and rebuild
- Harden, patch, perform vulnerability assessments
- Review policies

Automation for Communication and Coordination

Breach Details

Exposure Resolved ⓘ	No
Data Breach Type ⓘ	Confidential Information (CI) Personally identifiable information (PII)
Detection Sources ⓘ	—
Negative PR ⓘ	No
Criminal/Illegal Activity ⓘ	No

Data Types

Contact Information

- First name
- First initial
- Middle name
- Last name
- Address
- Phone number
- Email address

Personal Information

- Date of birth
- Driver's license number
- Marital status
- Occupation
- Passport number
- SSN or SIN

Identification Data

- State ID number
- Tax ID number
- Personal identification
- Tribal ID number
- Employee ID number
- Military ID number

Financial Information

- Account password / access code (financial)
- Bank account number
- Bank routing number
- Brokerage account data
- Financial account number
- Online username (financial)
- Payment card mag strip data

Medical Information

- Medical history
- Medical treatment
- Diagnostic information
- Mental condition
- Organ donor information

Health-Related Information

- Personal Health Record (electronic)
- Health insurance policy number
- Health insurer ID
- Healthcare payment, eligibility or entitlement information
- Substitute decision maker
- Medicare number
- Medical registration information
- Healthcare provider

Other Data

- Account password / access code (non-financial)
- Biometric data
- CPNI/Communications Data
- Digitized / electronic signature
- Educational records
- Fingerprint
- Genetic information
- Insurance policy number (non-health)
- License information and status
- License plate information
- Online username (non-financial)
- Parent's legal surname prior to marriage
- Security question and answer
- Work-related evaluations

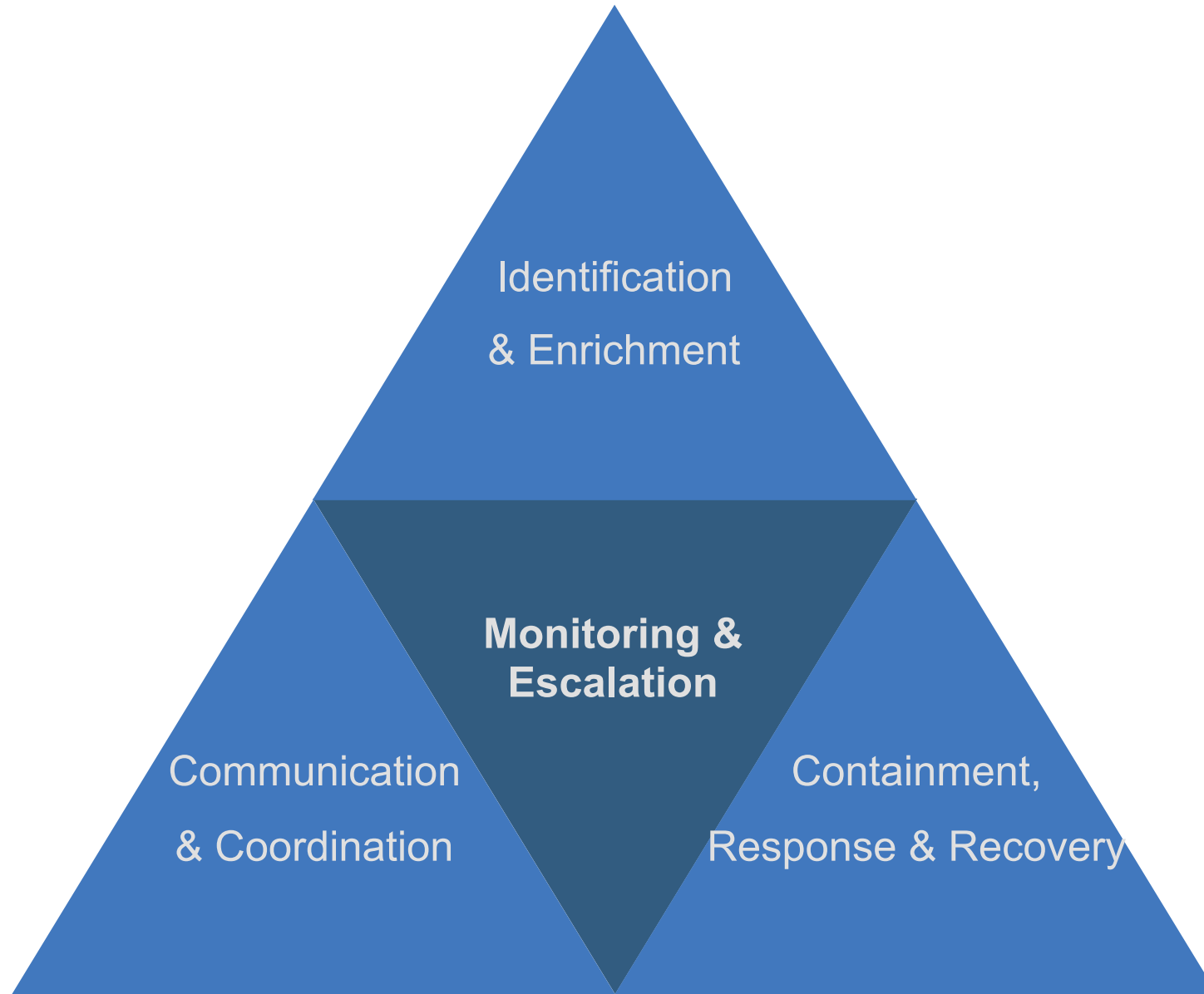
Automation for Communication and Coordination

Who needs to be notified?

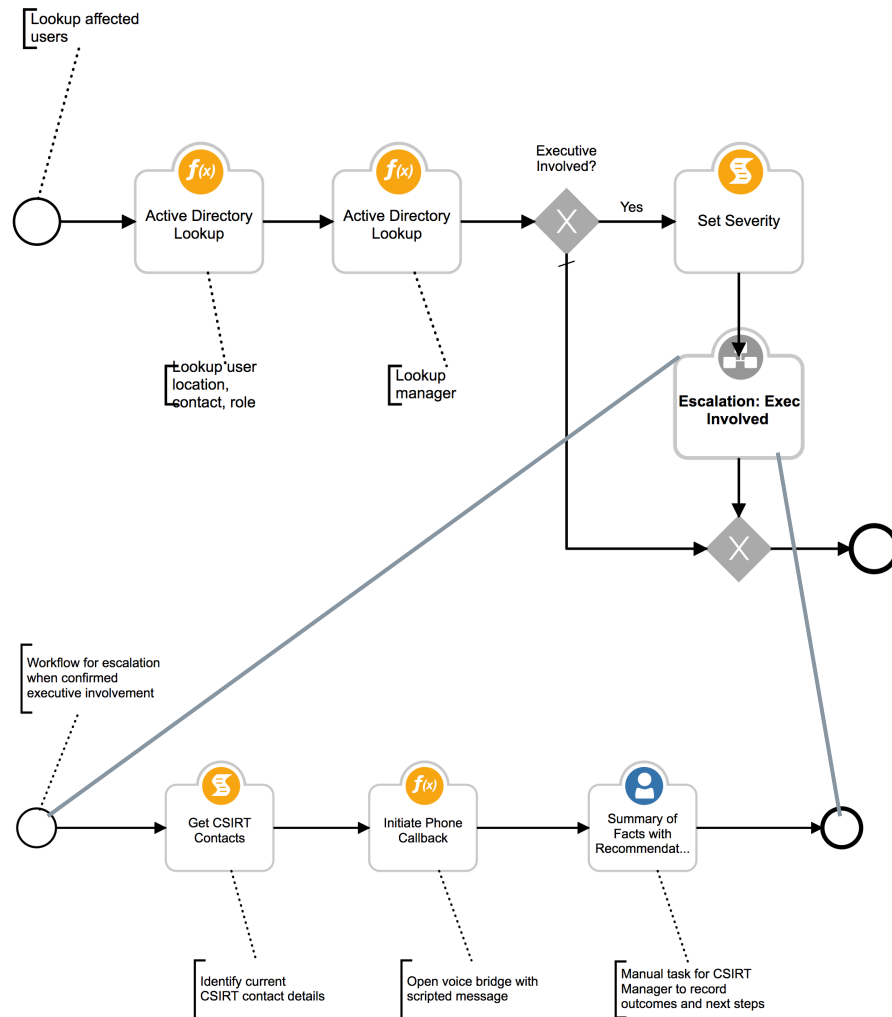
- Affected users
- Business owners and stakeholders

Other tasks:

- Measure and prioritize team activity
- Assign tasks outside the SOC
- Coordinate fusion workgroups
- Request and track resources
- Track investigation and remediation in other teams





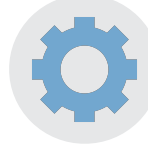
Dynamically Modify the Playbook as an Incident Evolves



- Identification changes the game
- Malware variants with special handling
- Additional tasks when an executive is involved
- High-severity incidents and CSIRT
- Tier 1 application impact
- Data loss with PII

The Response Playbook is More Than Automation Workflows



-  Preparation, analysis, recovery, post-incident activities
-  Data capture, metrics, and reports
-  Involves many people – coordination across activities and systems
-  SLAs and regulatory requirements
-  People, process, and technology

Organizations have Practical Constraints

- Insurance Company
 - Small security operations & IR team
 - Some Python skills – can “Assemble” and “Build”
 - Focus on endpoints
- Internet Provider
 - Very diverse organization, many different practices, but some overlap
 - High volume user reports, email, phishing
 - Complex & historical data for customer accounts
- Manufacturer
 - Software products deployed into global customer sites
 - Managed services for “traditional IT” threat monitoring L1/L2
 - ITSM (Remedy) as ticketing for network operations, desktops, etc.



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2017. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.



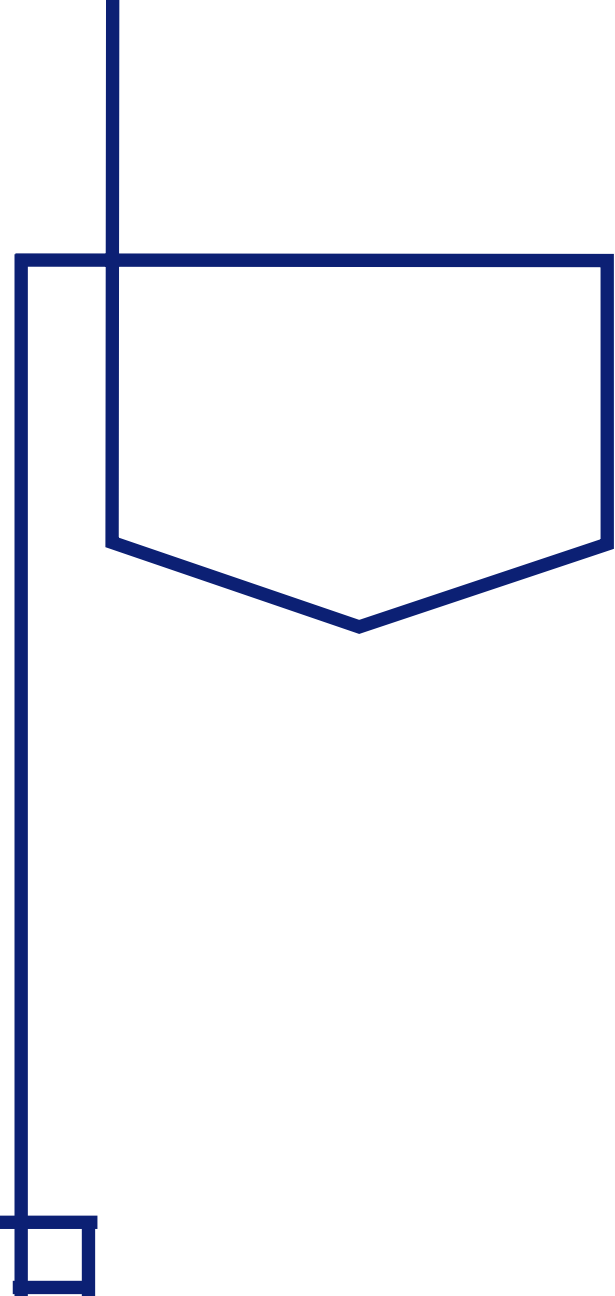
Community Presentation – US Bank

Cyber Defense: Protect and Defend

Integrated Adaptive Cyber Defense(IACD)
Threat Intelligence Automation

Rich Shok

May 2018



IACD Overview

IACD Automation is an on-going effort to replicate and expand upon the work initially done by Johns Hopkins University Applied Physics Lab (JHU/APL) collaborating with U.S. Bank.

Timeline of work:

- Initial collaboration with JHU/APL
- Implementation of playbook using Microsoft System Center Orchestrator(SCORCH)
- Switch to Security Automation and Orchestration Platforms(SA&O) for evaluation/PoC
- Stand up of chosen platform in production environment



Proof of Concept Approach

Three platforms brought in to evaluate in PoC environment. Platforms evaluated by development, infrastructure and various threat platform teams.

Considerations:

- Orchestration capabilities – Passing data from one task to next, playbook engineering, error reporting
- Out of the box integrations – Set up, calling in playbook, effectiveness
- Playbook/artifact capability
- Additional capabilities beyond orchestration
- Ease of use across development, admin and end users



Proof of Concept Considerations

Some helpful tips and items that may facilitate your PoC work.

- Clear, well defined processes for use to orchestrate
- Identify threat platforms needing integration for playbooks being built
- Gather test credentials ahead of time
- Identify a missing integration to possibly implement during PoC
- If evaluating multiple vendors, use same playbook(s) to compare/contrast
- Save work often and back up data/playbooks
- Allocate dedicated resources and time to adequately evaluate



Operational Considerations

What should we consider as we move into production?

- Security
 - End user vs admin vs engineer
 - Managing credential store within platform
- Artifact Handling across environments
 - Code for integrations
 - Playbooks and underlying code to use objects in the platform
 - Record Layout
 - Dashboard/Reporting



Operational Considerations(Cont)

What should we consider as we move into production?

- Governance
 - Which workflows are accessing what systems
 - What credentials are used in what integrations
 - Insuring workflow/code in repository matches what is being run in production
- Playbook Engineering
 - Managing of integrations/re-usable objects – Inputs/outputs
 - Who is allowed to engineer playbooks – Centralized or open to the organization?
- Health Monitoring



Considerations for Orchestration

Implementation points and things to consider to be successful.

- Automation goes more smoothly when working with clearly defined procedures and processes.
- Leverage APIs where available from internal as well as third party vendors.
- For platforms that don't offer APIs, push those vendors to offer them.
- Work iteratively as you develop your automation and orchestration.
- Consider how you want to manage your building blocks and workflows.



Demisto – April 20 - 27 2018

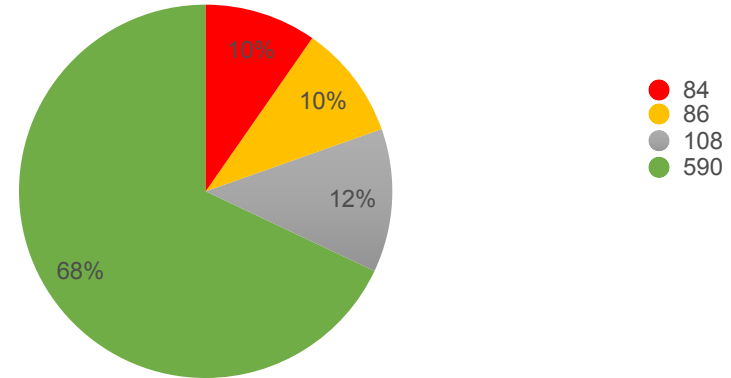
Highlights

- Phishing/SPAM playbook enabled in production 4-18-18
- Playbook in use only for emails without attachments sent to CSIRT Shared
- 868 emails forwarded to Demisto for orchestration/ automation during last 7 days
- 784 emails were auto closed by Demisto without any analyst interaction during last 7 days
- Original email sender auto responded to via tool notifying them if email was malicious or not along with reference case number
- Average time to closure for cases NOT requiring analyst interaction is 59.6 minutes
- Volume of auto closed cases in 1 week frees up 6 analysts time for entire month!

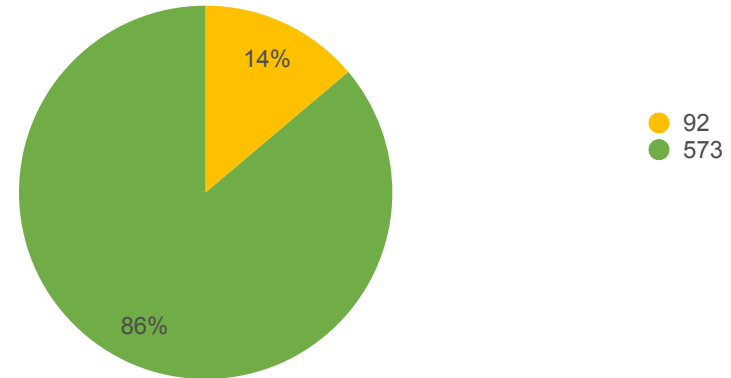
Average Time to Closure	
Hours	0.99
Minutes	59.6
Seconds	3576

Number of Analyst Time Saved	
Auto Closed	784
Tier 1 Avg/ mo	130
Analysts Saved	6.03

Case Severity



Proxy Hits



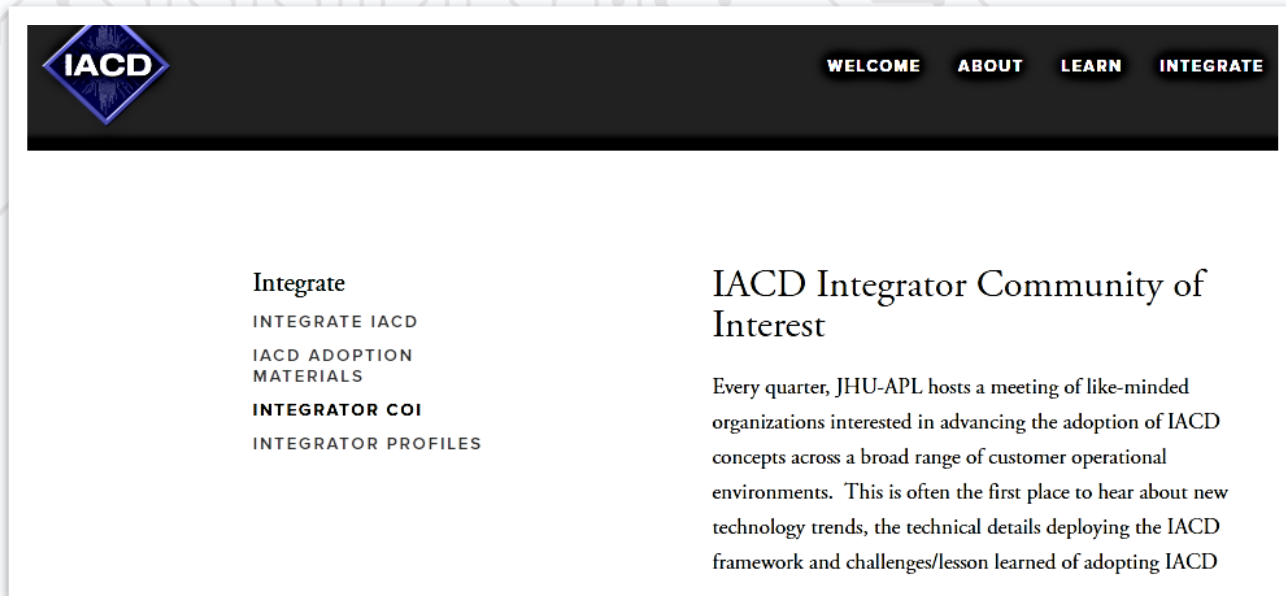
- Tool integration for emails with attachment sandbox not yet complete. Will come in a later phase
- Tier 1 average based on March 2018 numbers & used for comparison only
- Proxy hits DO NOT = malicious but rather that a URL forwarded in an email has been seen before on the bank proxies



Integrator COI Web Pages

Integrator COI Web Registration

<https://www.iacdautomate.org/integrator-coi/>



The screenshot shows the top navigation bar with the IACD logo and links for WELCOME, ABOUT, LEARN, and INTEGRATE. The main content area is divided into two columns. The left column lists navigation options: Integrate, INTEGRATE IACD, IACD ADOPTION MATERIALS, INTEGRATOR COI, and INTEGRATOR PROFILES. The right column features the heading 'IACD Integrator Community of Interest' and a paragraph describing quarterly meetings at JHU-APL for organizations interested in advancing IACD adoption.

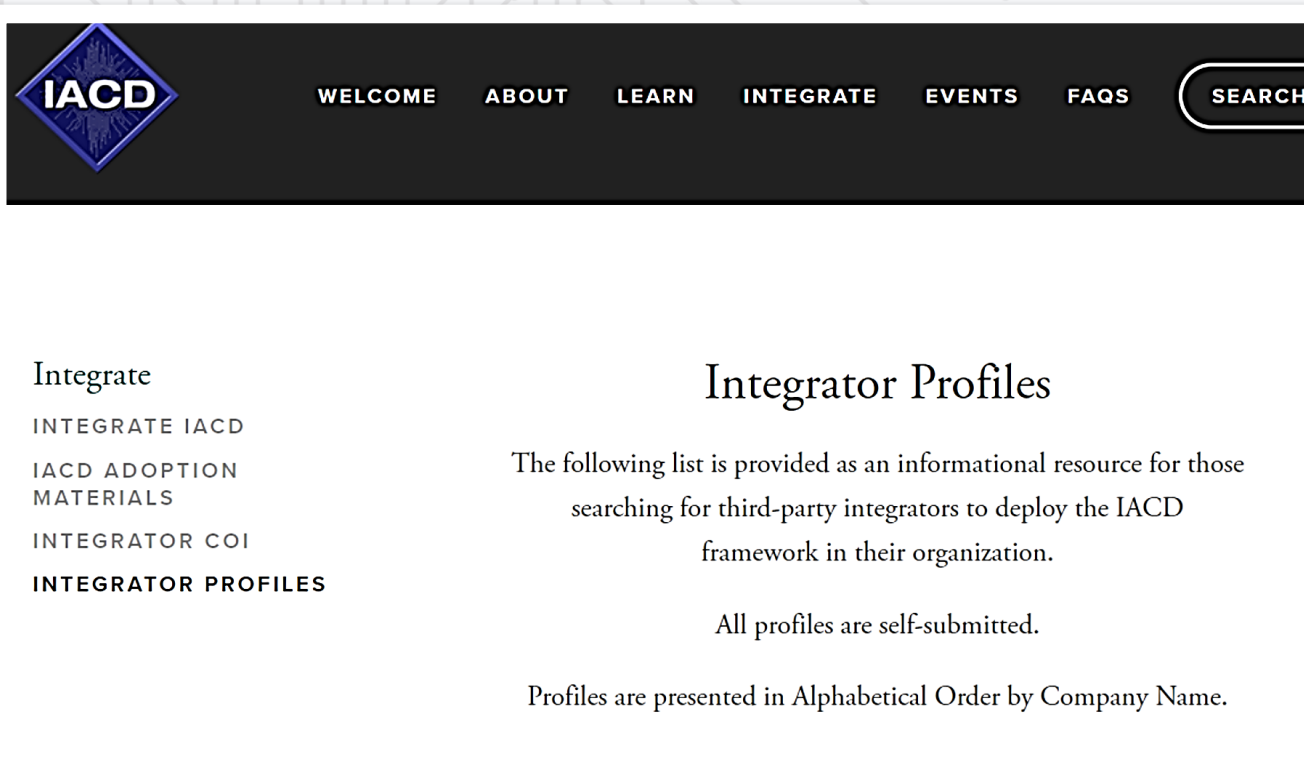
JOIN OUR INTEGRATOR COI

If you would like to join this COI and be included in invitations to these events, please provide the following information.

- **Join the Integrator COI**
 - Name
 - POC
 - Email
- **What do you hope to discover?**
- **Opportunities to contribute**
 - Success stories
 - Exploring and Demonstrating Automation

Integrator Profiles

<https://www.iacdautomate.org/integrator-profiles/>



The screenshot shows the IACD website's navigation bar with the IACD logo and menu items: WELCOME, ABOUT, LEARN, INTEGRATE, EVENTS, FAQs, and a SEARCH button. Below the navigation bar, the page title is "Integrator Profiles". The main content area contains the following text:

Integrate
INTEGRATE IACD
IACD ADOPTION MATERIALS
INTEGRATOR COI
INTEGRATOR PROFILES

Integrator Profiles

The following list is provided as an informational resource for those searching for third-party integrators to deploy the IACD framework in their organization.

All profiles are self-submitted.

Profiles are presented in Alphabetical Order by Company Name.

Asking Integrators to submit profiles for their organization

- **Contact Info and Web URL**
- **Technology Environments**
- **User Domain Experience**
- **Implemented Operational Processes**
- **Critical Infrastructure Areas**

Profiles are strictly provided to help interested parties identify organizations that have self-selected themselves to be listed as integrators.

Integrator Engagement

• Questions for Integrators

- Where are you actively engaged?
- What barriers to adoption do you need community to help overcome?
- What are some lessons learned?
- What are potential partnerships?

Examples of ongoing and near term engagement

Current Engagement	Potential Near Term Engagement	Future Engagement Desired
		State, Local, Tribal, Territorial Governments
		Election Infrastructure
		Maritime
		SLTT
		Defense
Critical Infrastructure Defined in PPD-21		
Chemical	Commercial Facilities	
Communications	Critical Manufacturing	
Dams	Defense Base Industrial Base and Supply Chain	
Emergency Services	Energy	
Financial Services	Food and Agriculture	
Government Facilities	Healthcare and Public Health	
Information Technology	Nuclear Reactors, material and waste	
Transportation Systems	Water and Wastewater Systems	

Community Actions

- **Identify points of contact for integration representatives to broaden the community by engaging more sectors and technology areas**
- **Identify areas of challenges and lessons learned within your organizations to support progress of key initiatives**
- **Complete Integrator Profiles on IACD Web**
<https://www.iacdautomate.org/integrator-profiles/>

Next Integrator COI

- **Date and Time: 11 July 2018, 1300 EST**
- **Location: Virtual WEBEX**
- **Theme: Operational Deployment Lessons Learned**

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.



 <https://secwww.jhuapl.edu/iacd>

 @IACD_automate

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

 icd@jhuapl.edu