Automating the Defense: Really Taking Advantage of Automated Sharing

Michael Vermilye
The Johns Hopkins University Applied Physics Laboratory

© 2017 by The Johns Hopkins Applied Physics Laboratory.
Material is made available under the Creative Commons Attribution 4.0 International License.

Topics

- What is IACD?
- What is the big deal about automated information sharing?
- Laying the groundwork for an automated defense
  - Conversations
  - Selection – What to automate?
  - Go with the flow – the readiness framework
- Wrap up

What is IACD?

What Is IACD?

IACD defines a *strategy* and *framework* to adopt an extensible, adaptive, COTS-based approach

IACD is:

- The set of **orchestration services** and **commonly-understood information** needed to:
  - ***Integrate*** across multiple, disparate sources of information
  - ***Automate*** the determination of risk and the decision to act
  - ***Synchronize*** machine actions to align with business/ops priorities, as captured in **playbooks**
  - ***Inform*** communities of trust via **automated information sharing**

DHS-NSA Partnership to Leverage Resources and Talent

Integration Lab

Prototypes, Pilots, Partnerships

IACD Partnership

Interoperability Specifications

Research

Leverage existing and future investments to address common challenges

Enable enterprise owners/network operators to defend themselves

Harness innovation, energy, and momentum of private sector & commercial solutions

Automated Information Sharing – What is the big deal??

We share information!!!

Monthly cybersecurity magazine!

We have phone calls!!
We recently upgraded!!

LOTS of email with attachments!!

Conversations with people I trust

All important to exchange different types of information and gain differing levels of context and trust.

But not able to handle the speed and scale needed in the current environment.

Automated Sharing – Give me more!!!!

- We heard you! Here you go…
- Automated Indicator Sharing – Free indicator feed from DHS. More information at: https://www.us-cert.gov/ais
- Commercial threat feeds – A number of vendors provide automated threat feeds and supporting analysis services
- Your ISAC/ISAO – Information sharing organizations provide information feeds for their members. An advantage is a trust community and context for YOU

Sharing is the key, don't just receive information, send information!!

Give me more!! I want more!!

- We always wanted more, more, more information
- Be careful what you wish for…

- Now we are faced with the problem of automated flows of information from multiple sources. LOTS of fire hoses.

It's not volume that we need, we need to be sharing the right information at the right time for the defender and decision maker

Sharing Models

Separate core content from context, and make both available in an *automated* fashion

- Multiple sharing models
  - Each user wants different information for different reasons at different times
  - Bring Your Own Ecosystem still applies
- Core content drives initial action
- Context informs more advanced decision making

Actionable Information

Share information that drives local response

- Impact and risk tolerance are personal and local
  - Confidence scores are more actionable than risk scores
  - Most actionable information maps easily to local prioritization or defense processes
- Understand how consumers use the information you provide
  - Analysts vs. Defenders
  - Do they want your knowledge, perspective, or opinion?

Trust

Trust is derived from transparency and validation

- I am willing to trust a process I understand and agree with
- I am willing to trust peers I already have a relationship with
- I can develop trust in you through monitoring and oversight
- If you mislead me too often in the beginning, I may not make any effort to trust you

How valuable is automated information sharing without trust?

- The answer is not much
  - Speed in transmission fed into a manual process does not give you a lot of value
  - Defensive measures sent automatically lose much of their value if you have to “verify” the measure in a manual manner

- **Being able to fully take advantage of all facets of automation requires multiple layers of trust**
  - **Source and integrity of information**
  - **Accurate assessment**
  - ***My* environment**
  - **Automated execution** *“Trust but Verify”*
  - **Information you provide will be used and disseminated correctly**

Are you Ready?

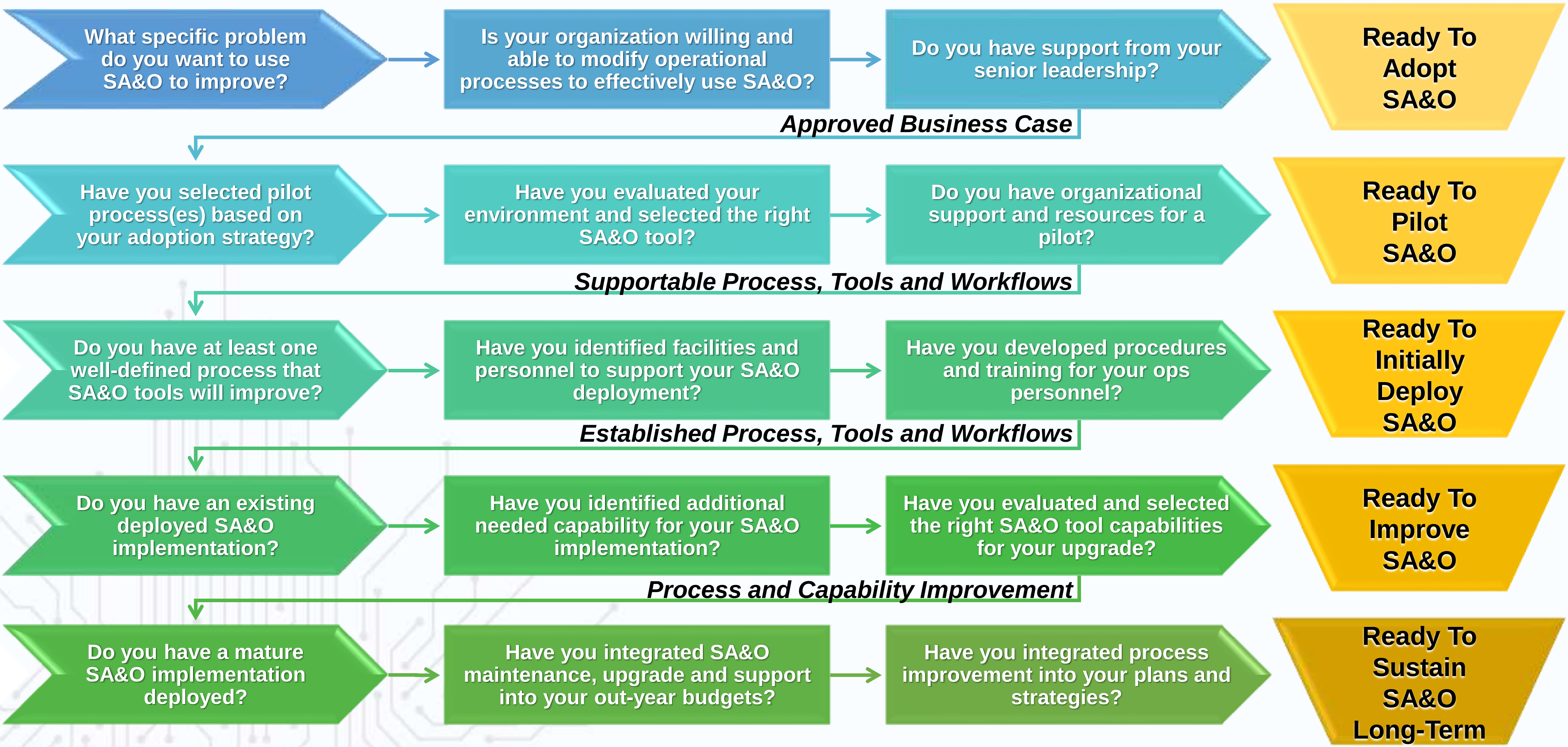
Readiness Assessment

You will need this..

It takes more than just purchasing an orchestration product or platform to implement cybersecurity automation.

You need to understand your organization’s cultural, procedural, and technical readiness to adopt Security Automation & Orchestration.

Adoption Preparation: IACD Readiness Framework



What specific problem do you want to use SA&O to improve?

Is your organization willing and able to modify operational processes to effectively use SA&O?

Do you have support from your senior leadership?

Ready To Adopt SA&O

Approved Business Case

Have you selected pilot process(es) based on your adoption strategy?

Have you evaluated your environment and selected the right SA&O tool?

Do you have organizational support and resources for a pilot?

Ready To Pilot SA&O

Supportable Process, Tools and Workflows

Do you have at least one well-defined process that SA&O tools will improve?

Have you identified facilities and personnel to support your SA&O deployment?

Have you developed procedures and training for your ops personnel?

Ready To Initially Deploy SA&O

Established Process, Tools and Workflows

Do you have an existing deployed SA&O implementation?

Have you identified additional needed capability for your SA&O implementation?

Have you evaluated and selected the right SA&O tool capabilities for your upgrade?

Ready To Improve SA&O

Process and Capability Improvement

Do you have a mature SA&O implementation deployed?

Have you integrated SA&O maintenance, upgrade and support into your out-year budgets?

Have you integrated process improvement into your plans and strategies?

Ready To Sustain SA&O Long-Term

What are you like?

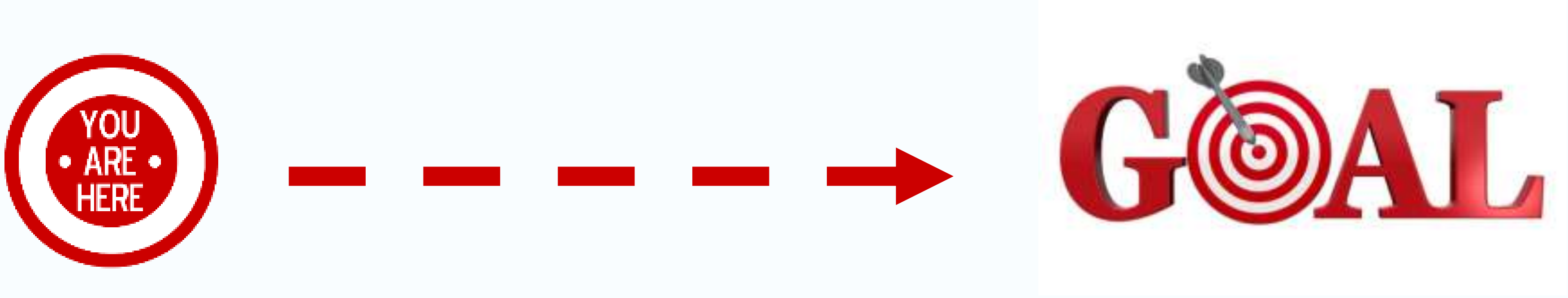
- What sector are you in? Are you federal, civilian, defense/intelligence, state/local, commercial, educational/research, healthcare, financial, law enforcement? Any special rules that you have to follow when it comes to doing automation? (…think regulations, laws, policies, directives, controls, governances, …)
- Are you geographically co-located or dispersed? Are you global, international, national, regional, local?
- Do you have a fairly large, well-resourced Security Operations Center (SOC) with tens of people working around the clock?
- Are you a smaller organization that is unlikely to buy an industrial-strength SA&O/SOAR solution, but still needs some degree of automation to better use the tools you have? ***Outsourcing may be your answer. You don’t need to buy the components, just the service.***
- Do you outsource some or all of your security services and need to better interface with your suppliers?

Get those ducks in a row

The 3 most critical elements of a successful SA&O/SOAR deployment are:

1. Visible Support for Automation at all levels of the organization
2. Willingness to Define and Modify Processes to gain efficiencies
3. Purchasing products and applications with Interoperability in Mind

Getting Started



- What is in your realm of possibility ***now,*** based on your current suite of network management and security products? And what types of capabilities do you want to add?
- Do you want to…
  - Automate some existing processes?
  - Restructure and improve your overall OPS Center?
  - Consult community members, collaborate on solutions, learn effective strategies, find out about adoption resources?

Successful implementations are designed to automate high return on investment (ROI), low-risk activities first, and then incrementally build to accommodate more complex decisions and processes.

Things that make sense to automate

1. Repetitive tasks -> Common processes
   - Account maintenance
   - Enrichment of received indicators
   - Log analysis
2. Reduce false positives -> Prioritize for analysis -> Post-analysis action/reporting
   - Using the information at machine speed that you are receiving at machine speed
3. Actions based on well-defined decisions -> Periodic implementation of previously authorized actions -> Event-based response actions

WHY MEASURE & WHICH METRICS?

Recognize & Evaluate

- Benefits
- Where SA&O can provide value
- Confidence achieving intended effects
- Troubleshooting & Tuning

Collect metrics on your existing processes *prior* to automation!

PLANNING

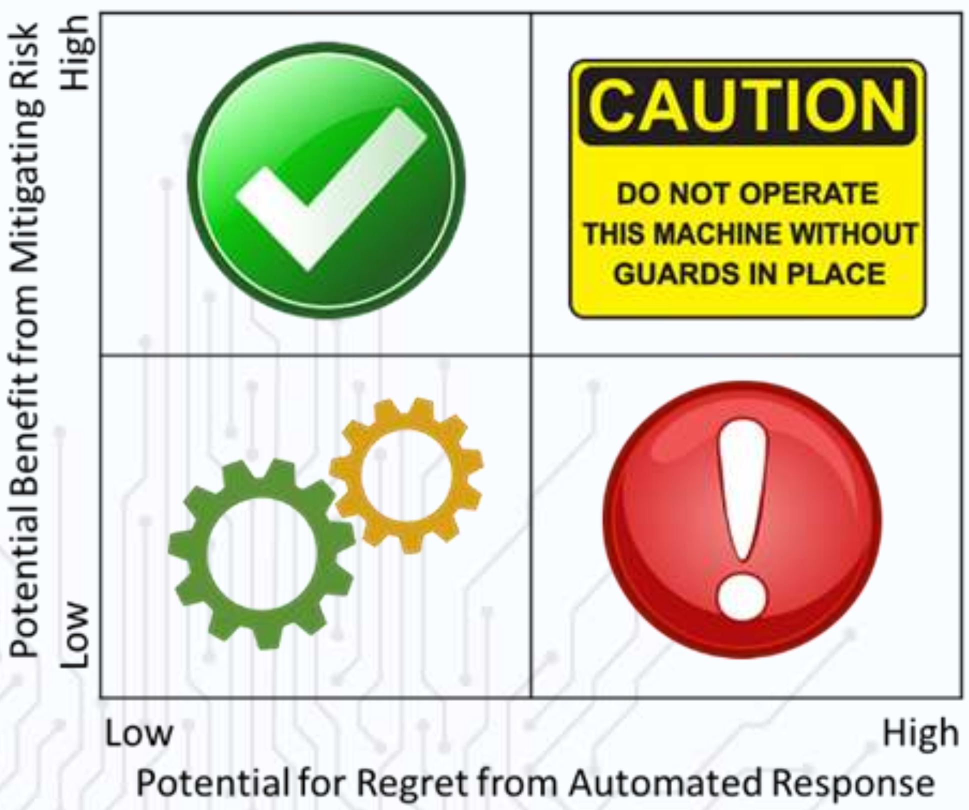
- **Why?** ***(Understand, Evaluate, Provide or Predict)***
- **Which metrics & measures?**
- **Who will take action?**
- **How should they be provided?**
- **How to interpret the results?**
- **What information is needed?**

DESIGN & IMPLEMENTATION

- **Supporting organizations?**
- **Which data sources?**
- **Data periodicity?**
- **Can you get to the data?**
- **Collection method?**
- **Reporting mechanism?**

Automated Response Actions

Focus on identification and execution of high-reward / low-regret response actions

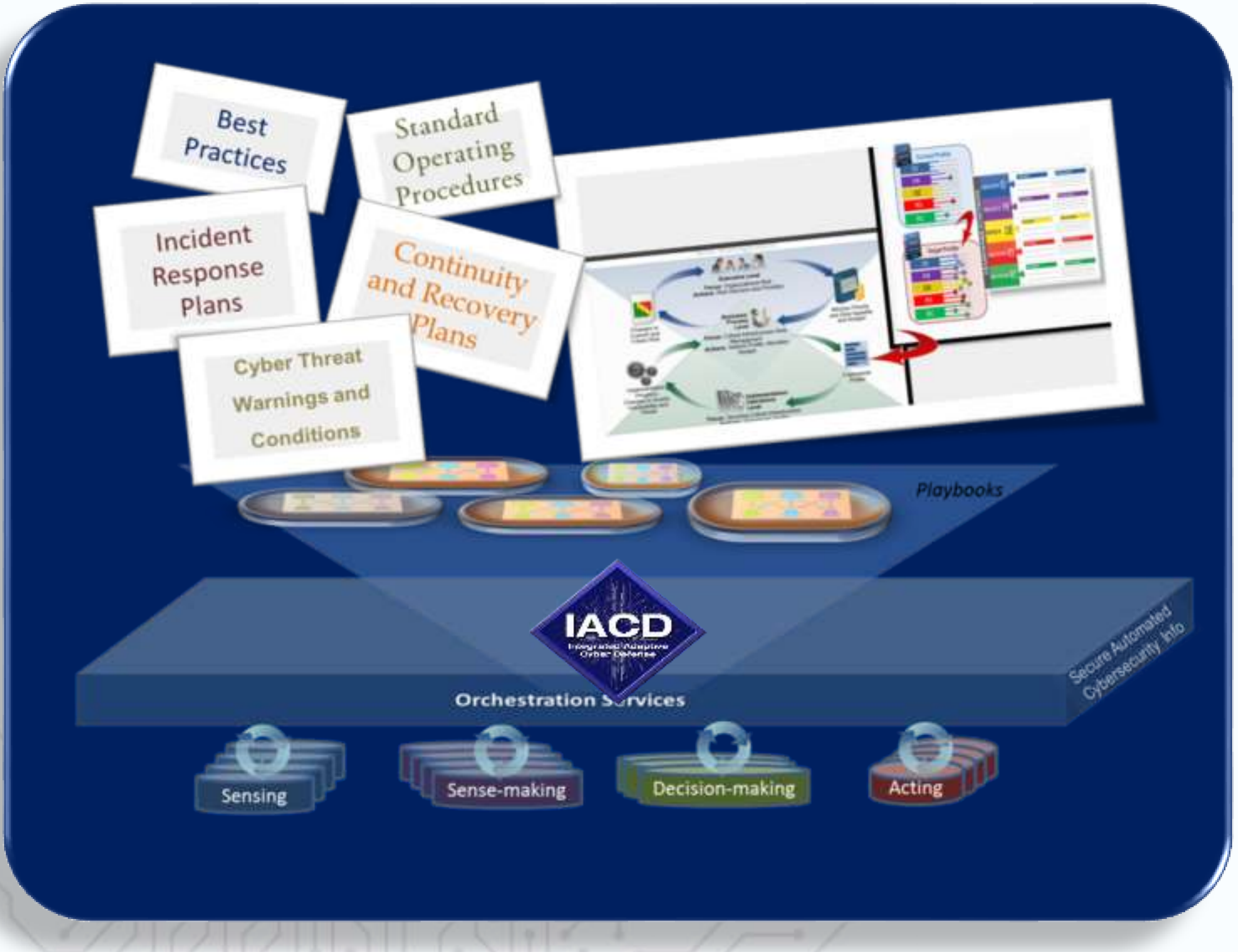


Automated Response Action Benefit vs. Regret Matrix

Potential Benefit from Mitigating Risk
High
Low
CAUTION
DO NOT OPERATE THIS MACHINE WITHOUT GUARDS IN PLACE
Low
High
Potential for Regret from Automated Response

- ✓ High-Reward/Low-Regret: Where Automation is Focused Today
- ⚙ Low-Reward/Low-Regret: Best Place to Add Automated Response Actions
- ⚠ High-Reward/High-Regret: Risk Posture Defines Automation Opportunities
- ❗ Low-Reward/High-Regret: Move it to Another Quadrant

Adoption: IACD Playbooks


Best Practices
Standard Operating Procedures
Incident Response Plans
Continuity and Recovery Plans
Cyber Threat Warnings and Conditions
Playbooks
IACD
Integrated Adaptive Cyber Defense
Orchestration Services
Secure Automated Cybersecurity Info
Sensing
Sense-making
Decision-making
Acting

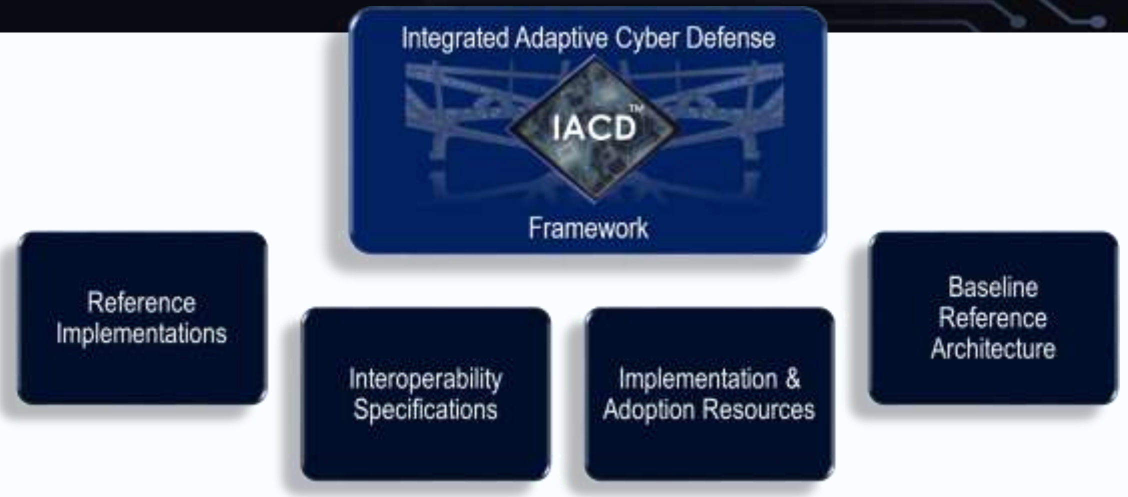
- Capture business- and operations-driven objectives, processes, and controls
- Can 'dial-ably' be translated and applied as automated implementations
- Map-able to NIST Framework, CIS Controls, regulatory requirements, etc.

© 2017 by The Johns Hopkins Applied Physics Laboratory. Material is made available under the Creative Commons Attribution 4.0 International License.

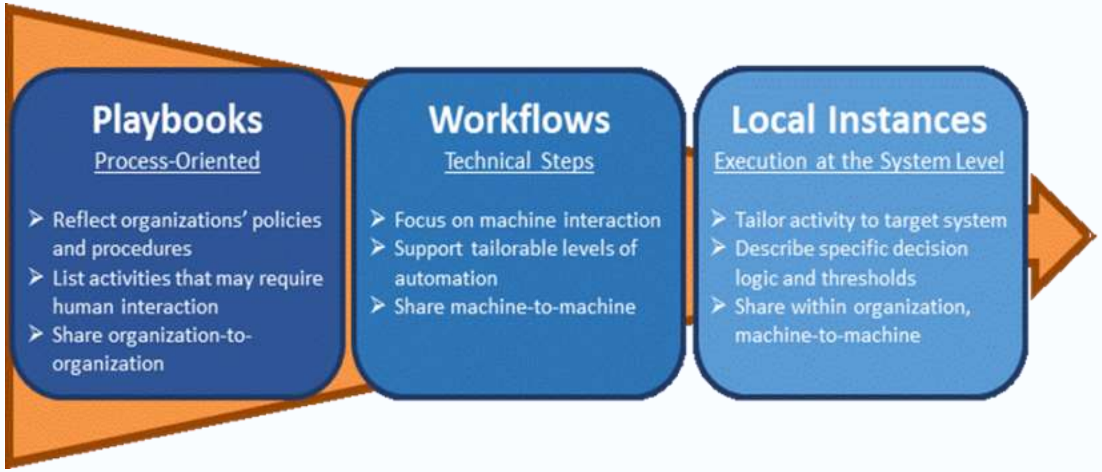
IACD Playbooks

- IACD framework defines specification for Playbooks, as well as guides to create, manage, and employ Playbooks.

- Playbooks are the most abstract in a series increasingly-specific representations of security actions
  - ***Playbooks*** **to represent their processes at a level independent of the decision to automate**
  - ***Workflows*** **capture a technology-specific view of the same process, focusing on machine interaction, with options for human input**
  - ***Local instances*** **of workflows tailor the implementation to the specific targeted systems and allow for local variations in policy, decision criteria, etc.**



Integrated Adaptive Cyber Defense
IACD™
Framework
Reference Implementations
Interoperability Specifications
Implementation & Adoption Resources
Baseline Reference Architecture



Playbooks

Process-Oriented

- Reflect organizations' policies and procedures
- List activities that may require human interaction
- Share organization-to-organization

Workflows

Technical Steps

- Focus on machine interaction
- Support tailorable levels of automation
- Share machine-to-machine

Local Instances

Execution at the System Level

- Tailor activity to target system
- Describe specific decision logic and thresholds
- Share within organization, machine-to-machine

Adoption: Current IACD Playbook Initiatives

- **CIS Critical Security Controls**
  - ➢Existing community
  - ➢Large extended community with ties to education, training, and thought leaders
  - ➢Integrated Cyber sessions to generate interest, community buy in, and ownership

- **FS-ISAC Insider Threat Working Group**
  - ➢Existing governance community
  - ➢Closely aligned with CSCs and Cyber Audit requirements
  - ➢Will be used to define and procure capability needs for financial sector

© 2017 by The Johns Hopkins Applied Physics Laboratory. Material is made available under the Creative Commons Attribution 4.0 International License.

Selection Process

Choosing wisely involves more than you realize

Process Selection

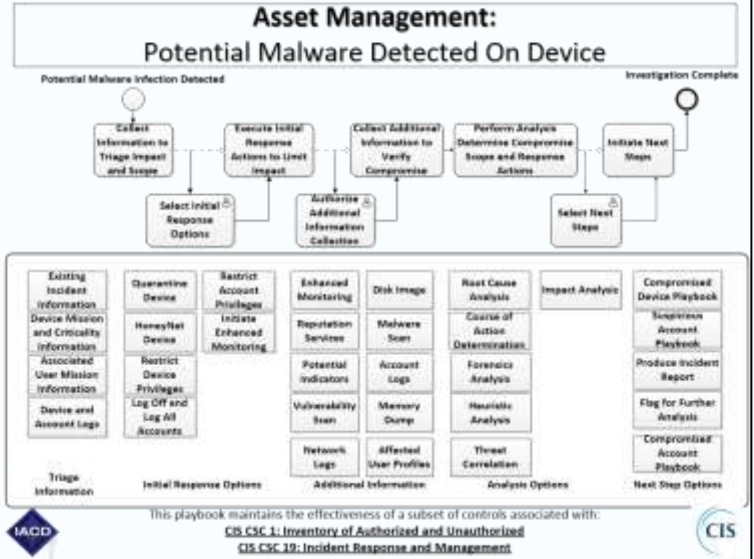
- **Use a process that is well-known**
  - May change for most effective automation
  - Should include human interaction (monitoring, control)
  - Needs well-defined decision criteria, too
- **Match the process to the available resources**
  - Inputs, integration with other tools, personnel availability
- **Going straight to full automation is probably a mistake**
  - Need steps for humans to check and monitor—these can be fully automated later!

Tool Selection

- **Know product and licensing limitations**
  - Verify functionality available via APIs
  - Identify any restrictions on number of actions
  - Understand task or query constraints
- **Be sure to consider tool certification for your network and your data**
  - Pilot environment AND operational environment
  - SA&O tool + integrated tools
- **Don't forget monitoring and reporting**
  - Current status and performance
  - Faults, failures and alerts
  - Troubleshooting

Adoption Preparation: Process and Tool Selection Guidance

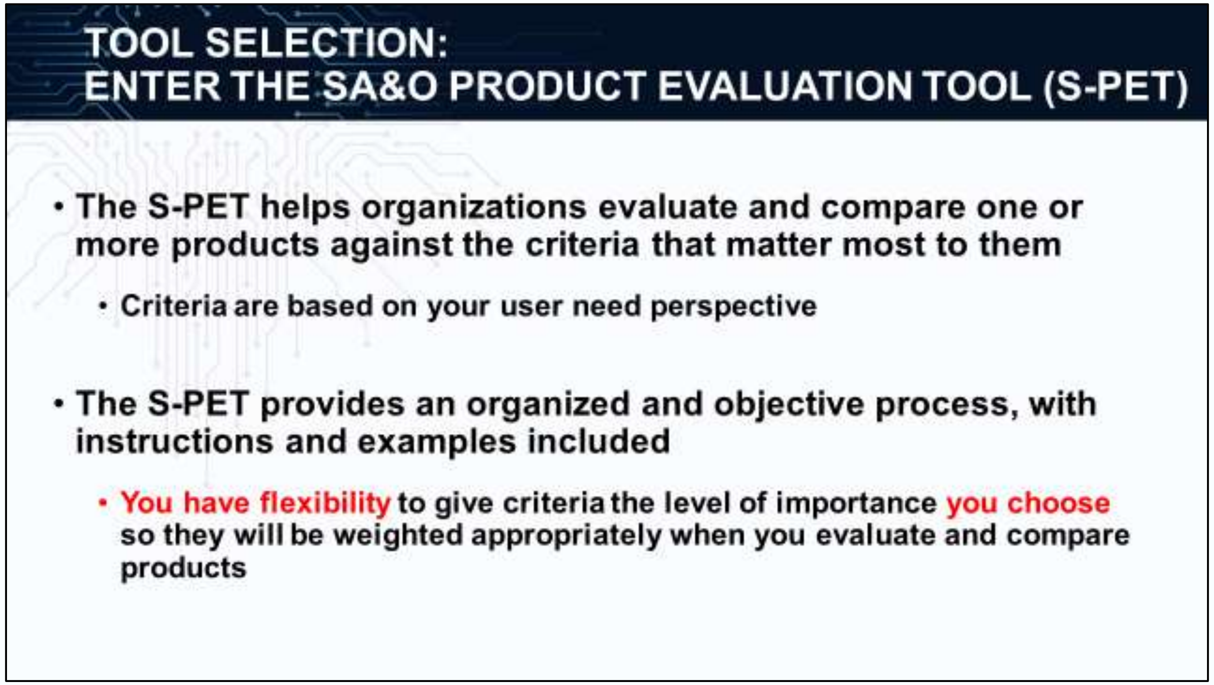
- **Support adoption strategy**
- **Remember that “well-defined” isn’t always well-defined**
- **Think about future evolution**
- **Watch out for scope creep**



Asset Management:
Potential Malware Detected On Device

Potential Malware Infection Detected
Collect Information to Triage Impact and Scope
Select Initial Response Options
Execute Initial Response Actions to Limit Impact
Authorize Additional Information Collection
Collect Additional Information to Verify Compromise
Perform Analysis Determine Compromise Scope and Response Actions
Select Next Steps
Initiate Next Steps
Investigation Complete
Existing Incident Information
Device Mission and Criticality Information
Associated User Mission Information
Device and Account Logs
Triage Information
Quarantine Device
HoneyNet Device
Restrict Device Privileges
Log Off and Log All Accounts
Restrict Account Privileges
Initiate Enhanced Monitoring
Initial Response Options
Enhanced Monitoring
Reputation Services
Potential Indicators
Vulnerability Scan
Network Logs
Disk Image
Malware Scan
Account Logs
Memory Dump
Affected User Profiles
Additional Information
Root Cause Analysis
Course of Action Determination
Forensics Analysis
Heuristic Analysis
Threat Correlation
Impact Analysis
Analysis Options
Compromised Device Playbook
Suspicious Account Playbook
Produce Incident Report
Flag for Further Analysis
Compromised Account Playbook
Next Step Options
IACD
CIS

This playbook maintains the effectiveness of a subset of controls associated with:
CIS CSC 1: Inventory of Authorized and Unauthorized
CIS CSC 19: Incident Response and Management



TOOL SELECTION:
ENTER THE SA&O PRODUCT EVALUATION TOOL (S-PET)

- **The S-PET helps organizations evaluate and compare one or more products against the criteria that matter most to them**
  - **Criteria are based on your user need perspective**
- **The S-PET provides an organized and objective process, with instructions and examples included**
  - **You have flexibility to give criteria the level of importance you choose so they will be weighted appropriately when you evaluate and compare products**

Technical Lessons Learned

Interoperability

Robust, open APIs remain the single most important criteria for current and future integration

- Implications for selection of products and services
- The **right** functionality **must** be exposed through the API to
  - Gain efficiencies via automation
  - Enable increased capabilities via integration
  - More readily leverage new functionality in existing operations

Security Considerations

Orchestration platforms have different models for security – make sure the one you buy meets your needs

- Authentication of human and non-human entities
- Secure access/usage of credentials
- Integration with native or third-party security services

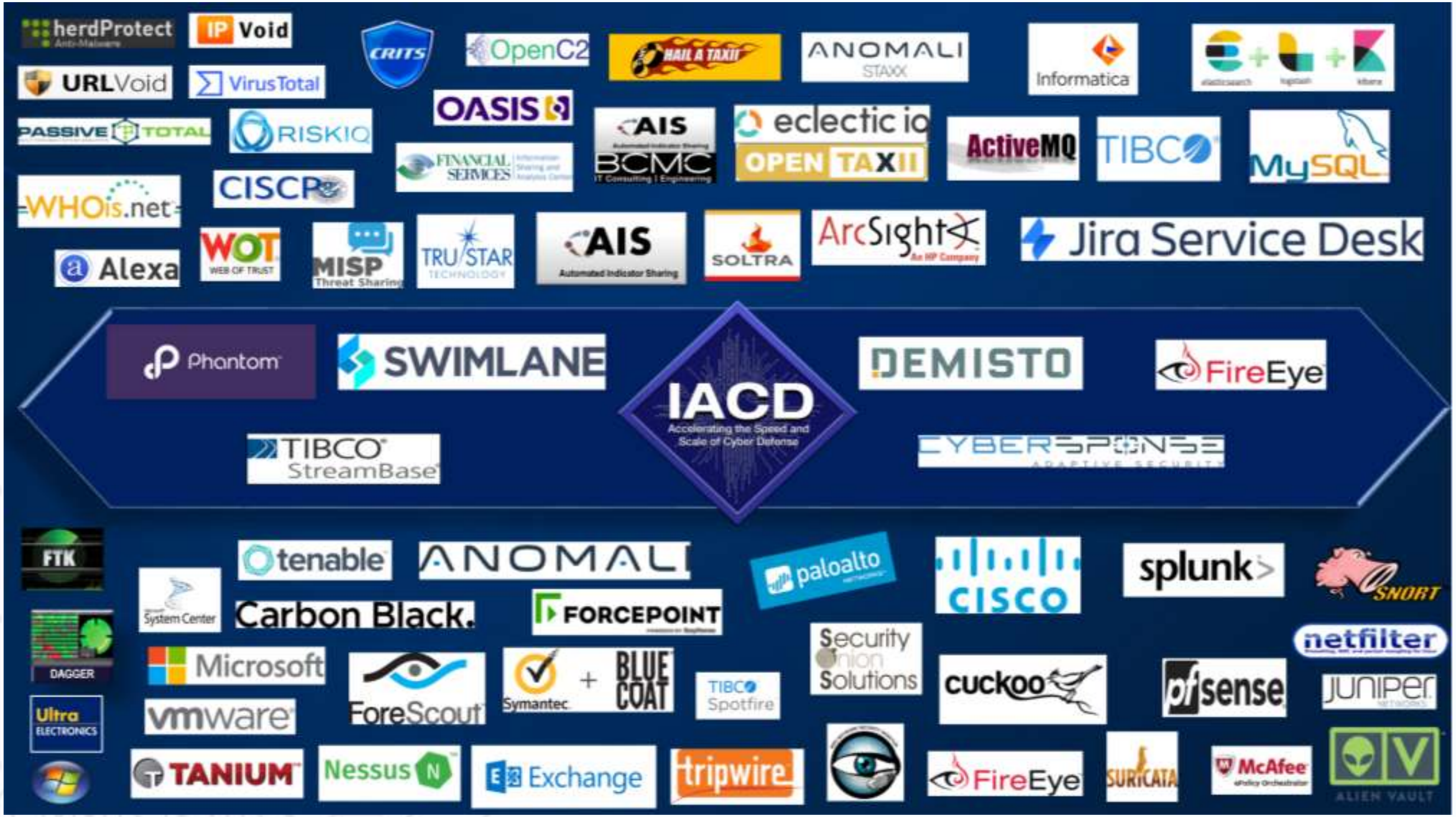
- Some vendors off-load security functions to integrated products or the network
- Sometimes your end products and services do not support secure integration

Changing your Infrastructure to Automate

Make industry your partner

- Buy differently
  - Demand support for interoperability with what you are keeping
  - Think about future interfaces with your facility and back office information systems
  - Demand robust APIs
  - Ask how something new improves what you already have
  - Ask for references of current installations that you can contact
  - Work with those vendors that will help support the deployment with resources, not just FAQs

Integrations Thus Far



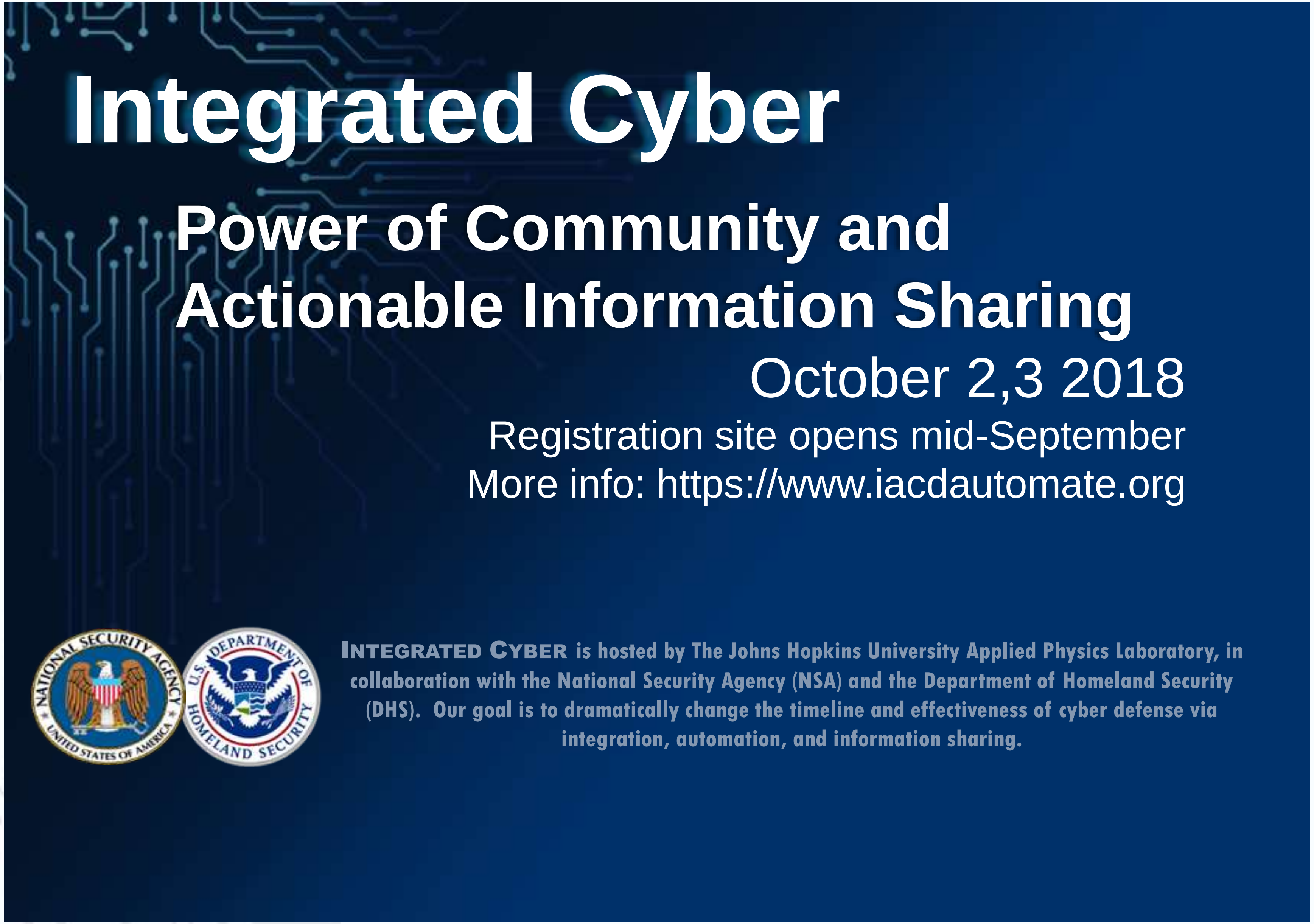
References

- **https://www.iacdautomate.org/**
  - Wealth of information
  - Products to help you assess your enterprise's readiness to automate
  - Material from previous IACD Integrated Cyber events
  - Ways to get involved

- For the social among you:
  - LinkedIn: **https://www.linkedin.com/groups/8608114**
  - Twitter: **@IACD_automate**

- Yes we do email: **icd@jhuapl.edu**

Questions anyone?



Integrated Cyber

Power of Community and Actionable Information Sharing

October 2,3 2018

Registration site opens mid-September
More info: https://www.iacdautomate.org

Integrated Cyber is hosted by The Johns Hopkins University Applied Physics Laboratory, in collaboration with the National Security Agency (NSA) and the Department of Homeland Security (DHS). Our goal is to dramatically change the timeline and effectiveness of cyber defense via integration, automation, and information sharing.

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

https://www.iacdautomate.org	@IACD_automate
https://www.linkedin.com/groups/8608114	icd@jhuapl.edu