Integrated Cyber Fall 2018 | Oct. 2 & 3

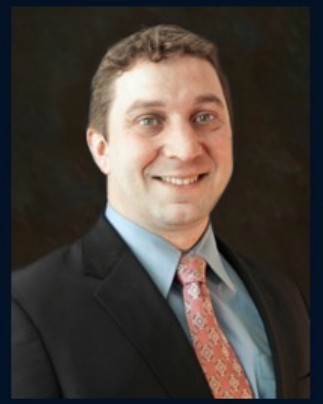
Day 1 - Tech Talk – Integrator COI

Integrator COI Technical Talk - Tales from the Trenches: Use of a Cyber Range to overcome obstacles to SOAR/IACD Adoption

Host:

Cory Huyssoon,
JHU/APL

APL Johns Hopkins Applied Physics Laboratory



Presenter:

Tim Schaad,
Executive Director, Advanced Cyber Range Environment and Cyber Range Services,
ManTech

ManTech

Integrator Community of Interest

Integrated Cyber
Johns Hopkins University Applied Physics Laboratory
Laurel Maryland, October 2-3, 2018

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

IACD
Integrated Adaptive Cyber Defense

APL JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Agenda

- Integrator Community of Interest (COI) Overview
- Community Presentation – ManTech
- Integration Engagement
- 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

Community Presentation – ManTech

ManTech

Securing the Future

Overcoming IACD Adoption Challenges with Cyber Range Techniques

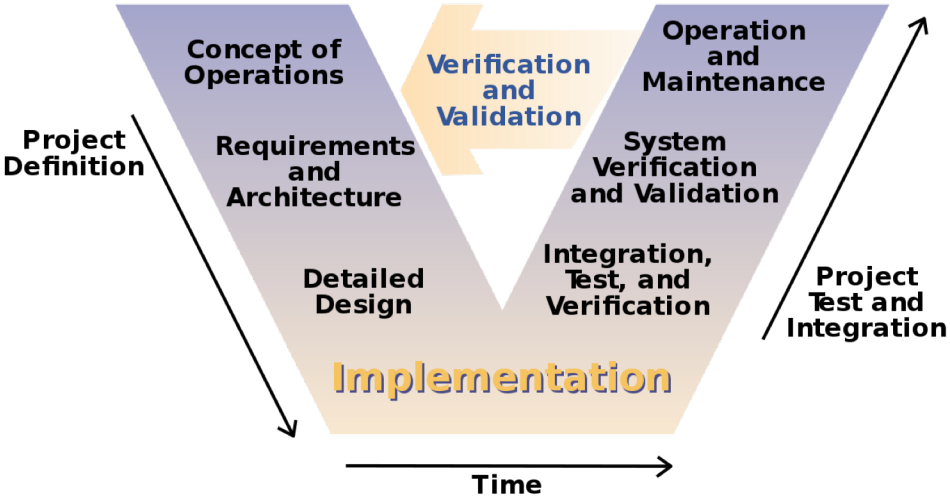
October 2, 2018

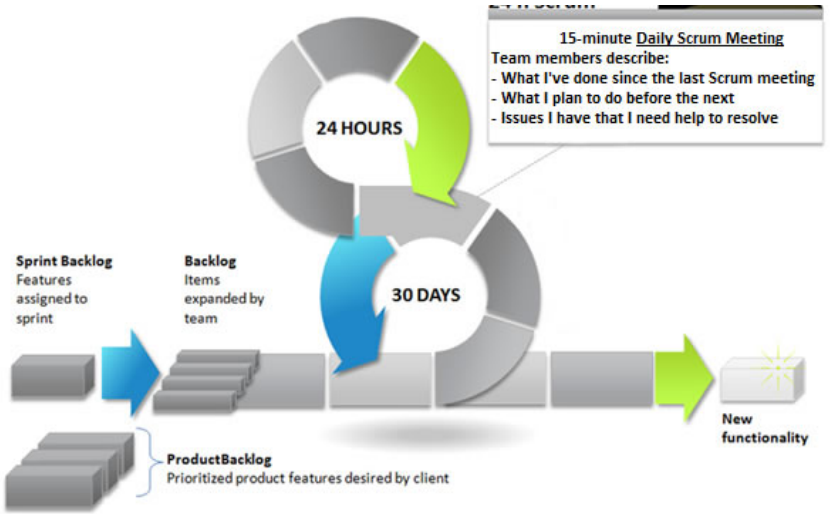
The Promise of IACD

- Traditional cyber defense operates at human speed
- Cyber offense operates at machine speed
- IACD can even the odds

Implementation Approach

- Crawl, walk, run
- Deploy “safely”
  - Limited Pilot
  - Out of band
  - Monitor-only
- Develop automations
- Turn them on**





Real-world IACD Adoption Challenges

- Confidence in Process
- Confidence in Data
- Confidence in Analytics
- Confidence in Technology

Lack of Confidence in Technology

- We've been able to automate incident response for a long time through APIs and SDKs
  - Lots of time and effort
  - Extensive testing
  - Difficult to maintain
- SOAR/IACD technologies are normalizing and simplifying the process
  - Technology is still maturing
  - Extensive testing is still necessary

Lack of Confidence in Data & Analytics

- Quantity vs. Quality
  - Data quantity isn't a problem
  - Curating data into quality (actionable) information is
  - What are the most trustworthy data sources?
- Good rules are hard
  - How do you avoid false positives?
  - How good is good enough?
  - When rules go bad, how do you fix it?
- AI/ML has a play
  - But these are new as well

Lack of Confidence in Process

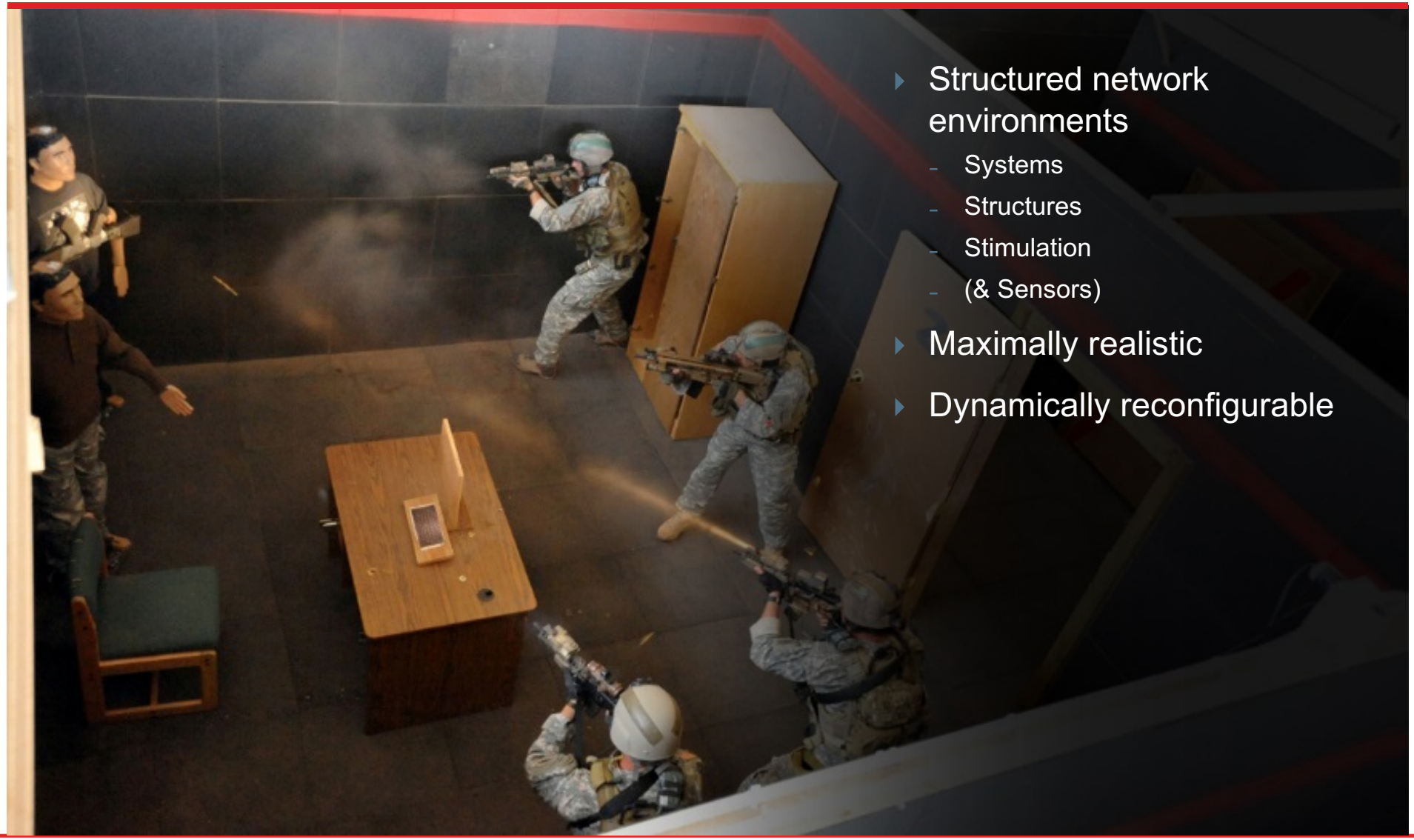
- Automating a bad process gets you bad results fast
- What actions & sequences are correlated to metrics of defensive success?
- What are the Legal and Risk Management implications?

Building Confidence

- **Test** technology
- **Train** personnel
- **Exercise** the whole system

This is what a Cyber Range is for!

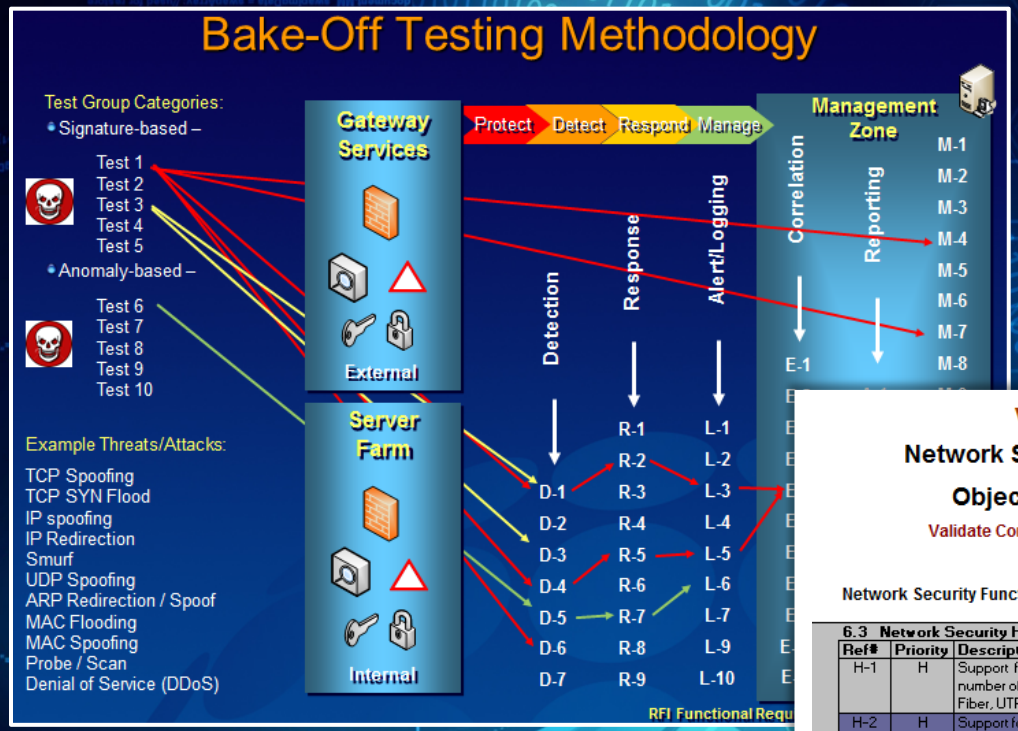
A Working Definition of Cyber Range

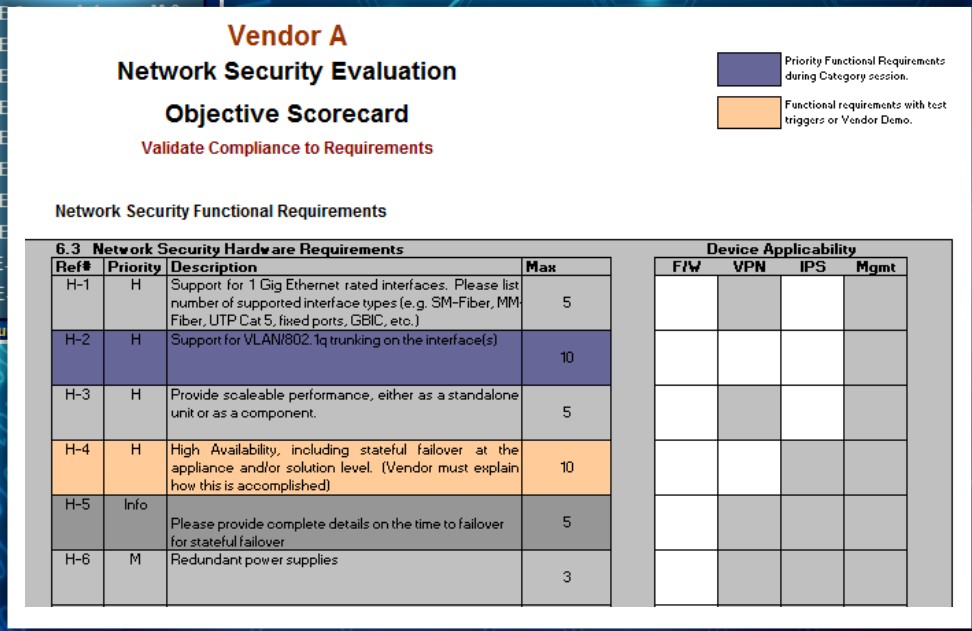


- Structured network environments
  - Systems
  - Structures
  - Stimulation
  - (& Sensors)
- Maximally realistic
- Dynamically reconfigurable

Safe for unsafe behavior

Maximally realistic testing





Vendor A

Network Security Evaluation

Objective Scorecard

Validate Compliance to Requirements

Priority Functional Requirements during Category session.

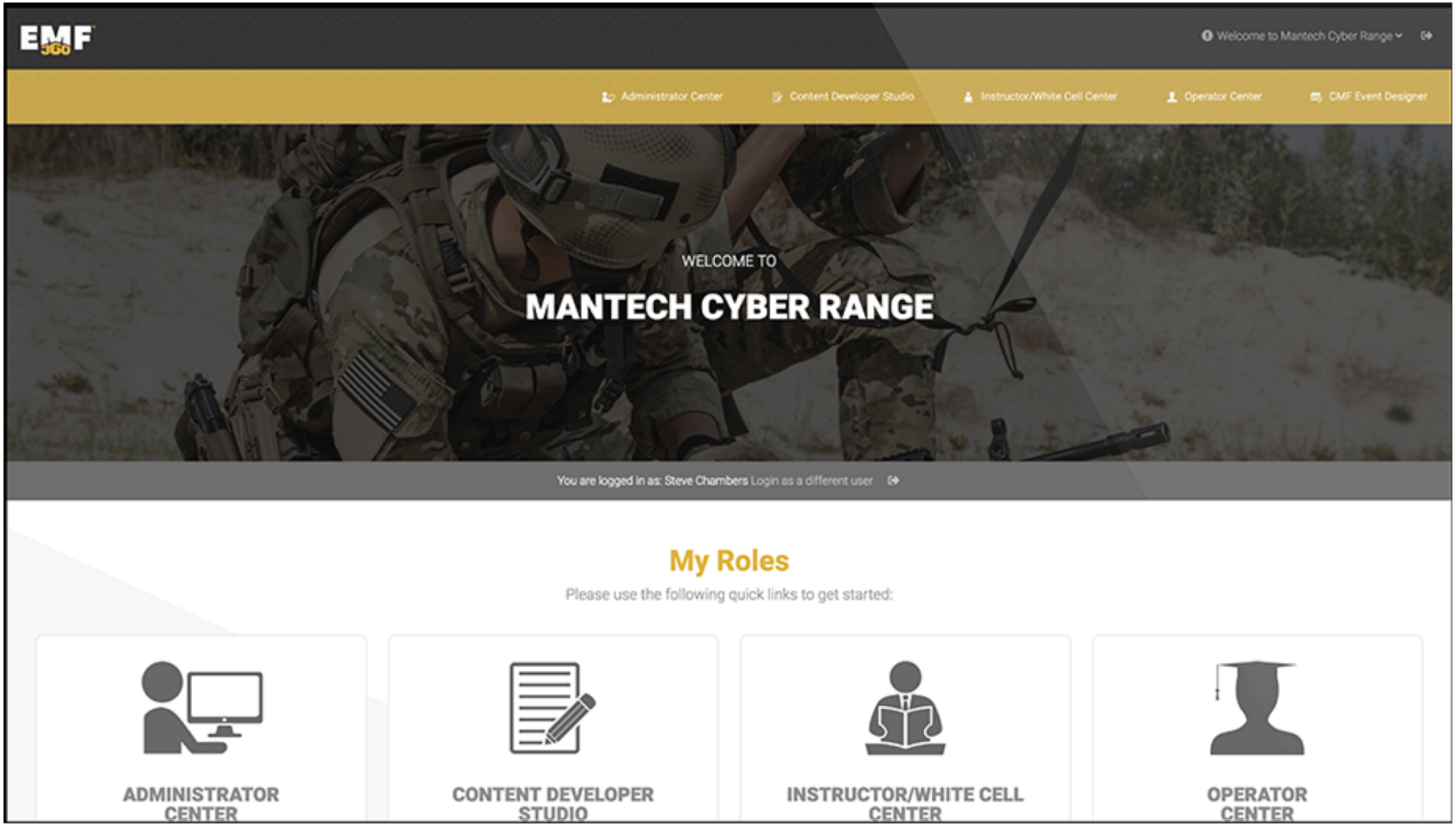
Functional requirements with test triggers or Vendor Demo.

Network Security Functional Requirements

6.3 Network Security Hardware Requirements

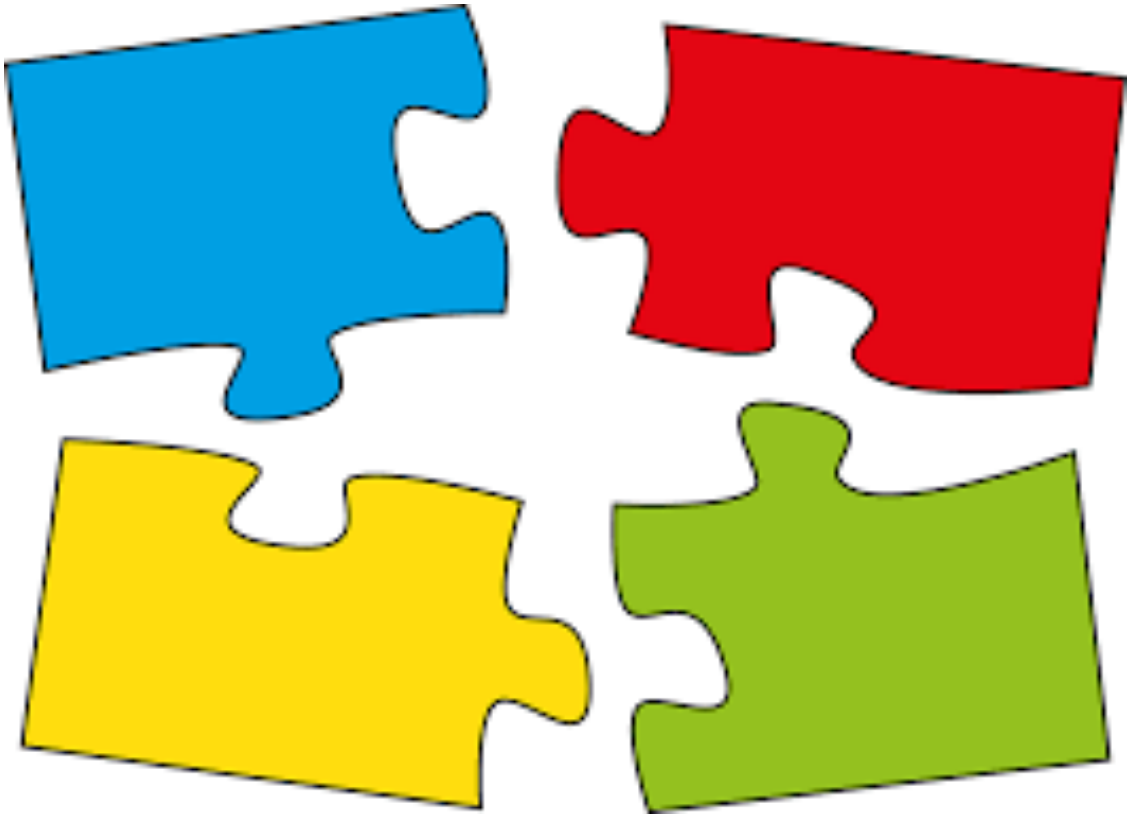
Ref#	Priority	Description	Max	Device Applicability F/W	VPN	IPS	Mgmt
H-1	H	Support for 1 Gig Ethernet rated interfaces. Please list number of supported interface types (e.g. SM-Fiber, MM-Fiber, UTP Cat 5, fixed ports, GBIC, etc.)	5				
H-2	H	Support for VLAN/802.1q trunking on the interface(s)	10				
H-3	H	Provide scaleable performance, either as a standalone unit or as a component.	5				
H-4	H	High Availability, including stateful failover at the appliance and/or solution level. (Vendor must explain how this is accomplished)	10				
H-5	Info	Please provide complete details on the time to failover for stateful failover	5				
H-6	M	Redundant power supplies	3				

Individual & Collective Training



Exercise

- Pull the pieces together
- Discover unknown-unknowns
- Adjust and try again



ManTech

QUESTIONS

Mark Shaw *Senior Executive Director, Cyber Solutions*
EMAIL: Mark.Shaw@ManTech.com **PHONE:** 703-388-2126

Tim Schaad *Executive Director, Cyber Solutions*
EMAIL: Timothy.Schaad@ManTech.com **PHONE:** 703-674-2773

Miguel Rosario *Executive Director, Cyber Solutions Architect*
EMAIL: Miguel.Rosario@ManTech.com **PHONE:** 202-389-2441

Integration Engagement

Integrator Engagement

- **Questions for Integrators**
  - **Would you be willing to participate in demonstrations or showcases involving testing of large scale automated capabilities?**
  - **Would potential of working together to fill gaps in large scale experimentation of IACD capabilities be beneficial for you?**
  - **Would inclusion of various vendors to promote communication and feedback be useful in this kind of forum?**
  - **How would bringing in different kinds of federal, civil, and private users across different operational environments be helpful in understanding integration needs and challenges?**
  - **What growing technical trends or disruptive challenges are barriers to your implementation and integration of automated capabilities?**

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: 16 January 2019, 1300 EST**
- **Location: Virtual WEBEX**
- **Theme: TBA**

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://www.iacdautomate.org

@IACD_automate

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

icd@jhuapl.edu