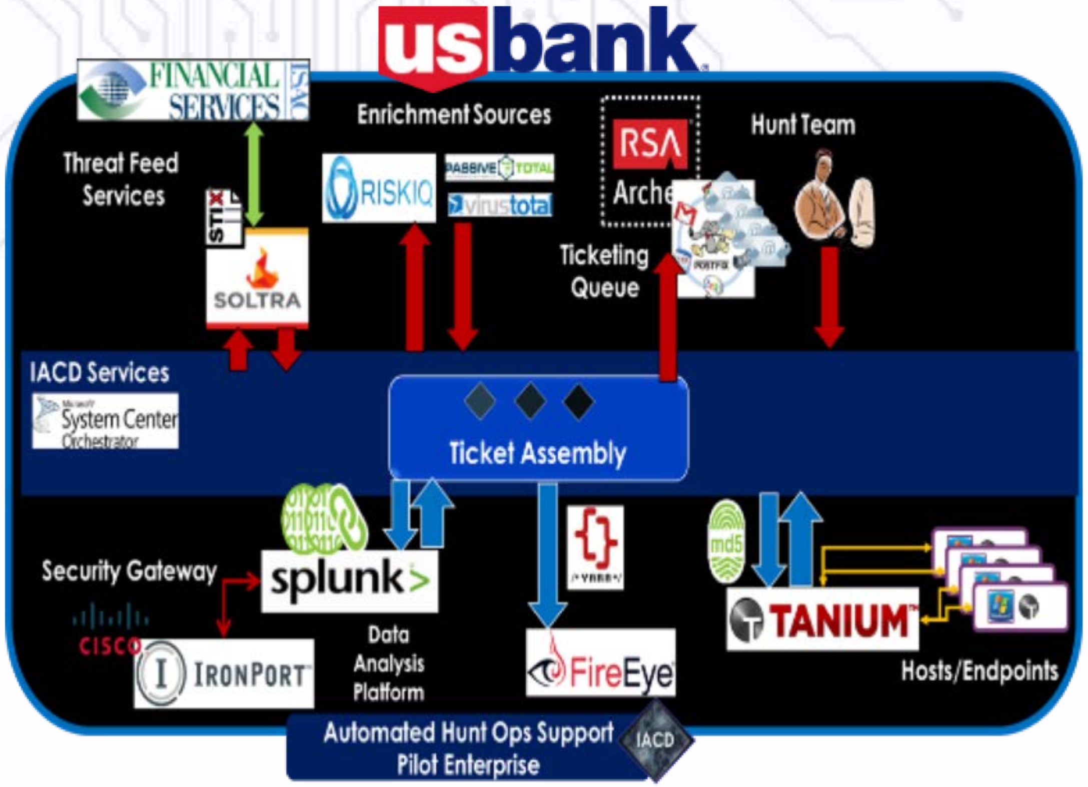
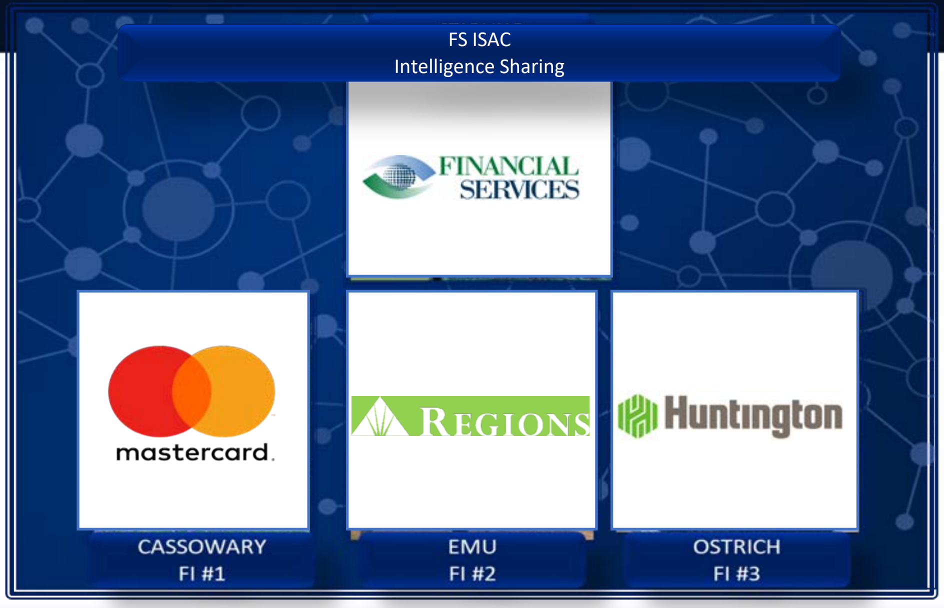
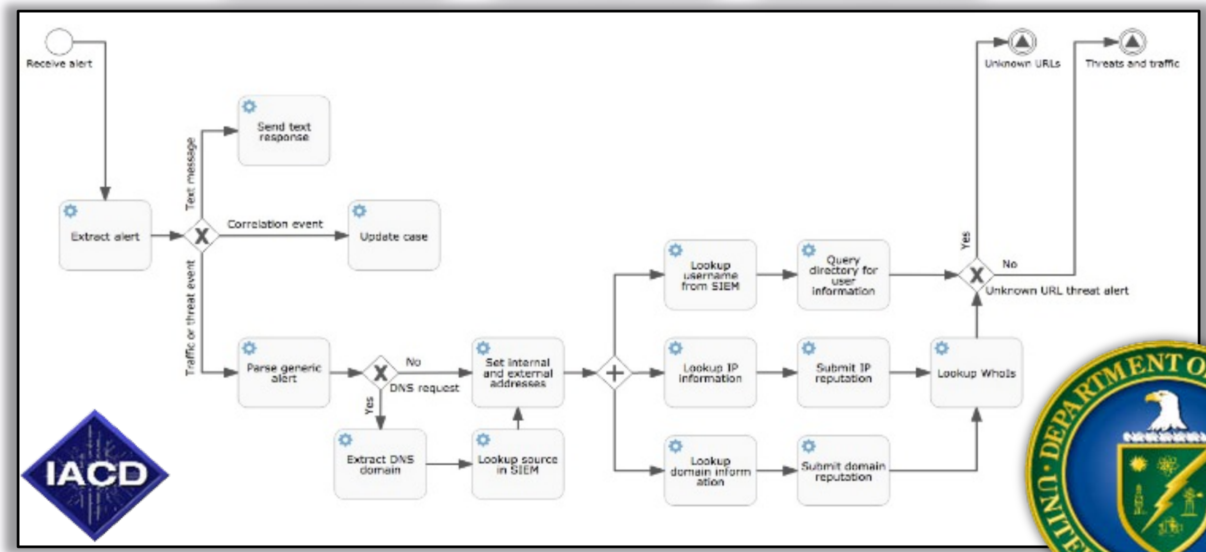
Integrated Adaptive Cyber Defense
Operationalization Lessons Learned

Harley Parkes
The Johns Hopkins University Applied Physics Laboratory

Multi-pronged Pilot Efforts







Organizational Lessons Learned

Organizational Culture

Security Automation and Orchestration (SAO) is a different way of doing business, not a technology upgrade

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

Visible Support for Automation at all levels of the organization

Willingness to Define and Modify Processes to gain efficiencies

Purchasing products and applications with Interoperability in Mind

Operational Readiness

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

Scalable processes – What if it executes 2000x a day instead of 20?

SAO skill sets - Do you have the expertise to design workflows? Integrate products and data sources? Implement security controls?

Evolving SOPs – How does the job change when analysts are freed from manual tasks? When they are expected to process more or different alerts/events?

Deployment Scope

Define the critical elements of success (and failure) before you start

- Define success and exit criteria
  - What must be achieved? When are you done? How will you know?
  - What must never happen? What if you need to de-scope?
- Identify key roles and responsibilities
  - Who are the stakeholders? Who needs to be included in the planning? What support is required?
- **Manage risk through proper planning**
  - **What are the test and evaluation requirements? How do you verify workflows fail safe? What happens if you need to go back to the current manual process?**

Metrics and Measures

Make sure to make your point – not just any point that can be made

- Why are you deploying a new capability? What does it take to demonstrate value to different stakeholders?
- Capture baseline measurements or metrics for comparison!
- Forethought = success

Communications

Transparency and consistent messaging are critical to success

- Open communications is key
  - Leverage modern technology
  - Maintain a shared understanding of goals and objectives
  - Needs to be a concerted, organized, deliberate effort by leadership
  - Establish a *single*, well-understood location for everyone to find *finished* products and materials

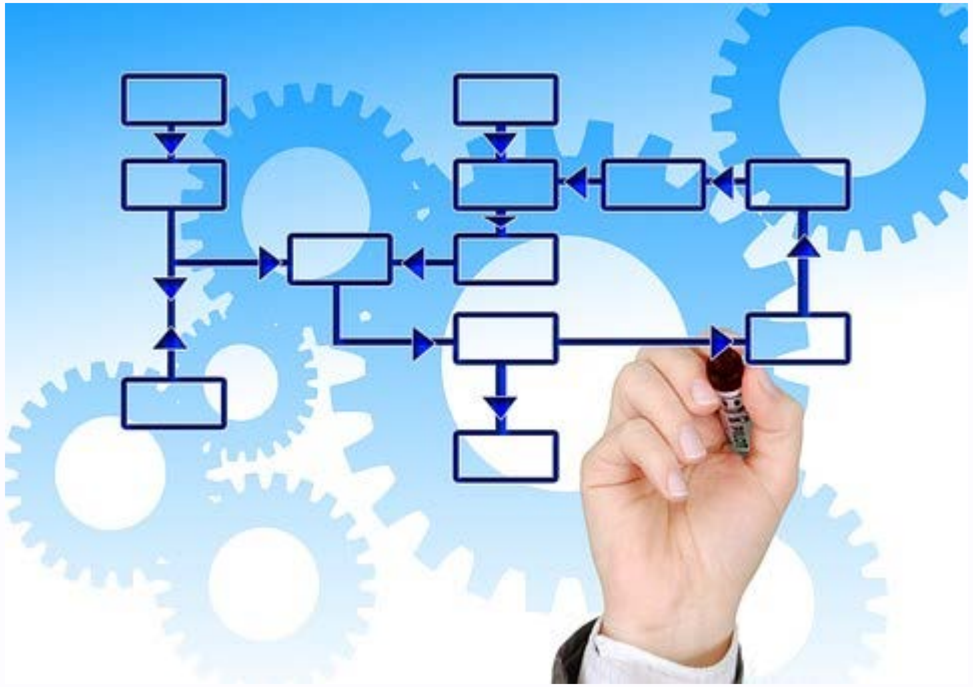
Technical Lessons Learned

Interoperability

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

- Implications for selection of products and services

- The **<u>right</u>** functionality **<u>must</u>** 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

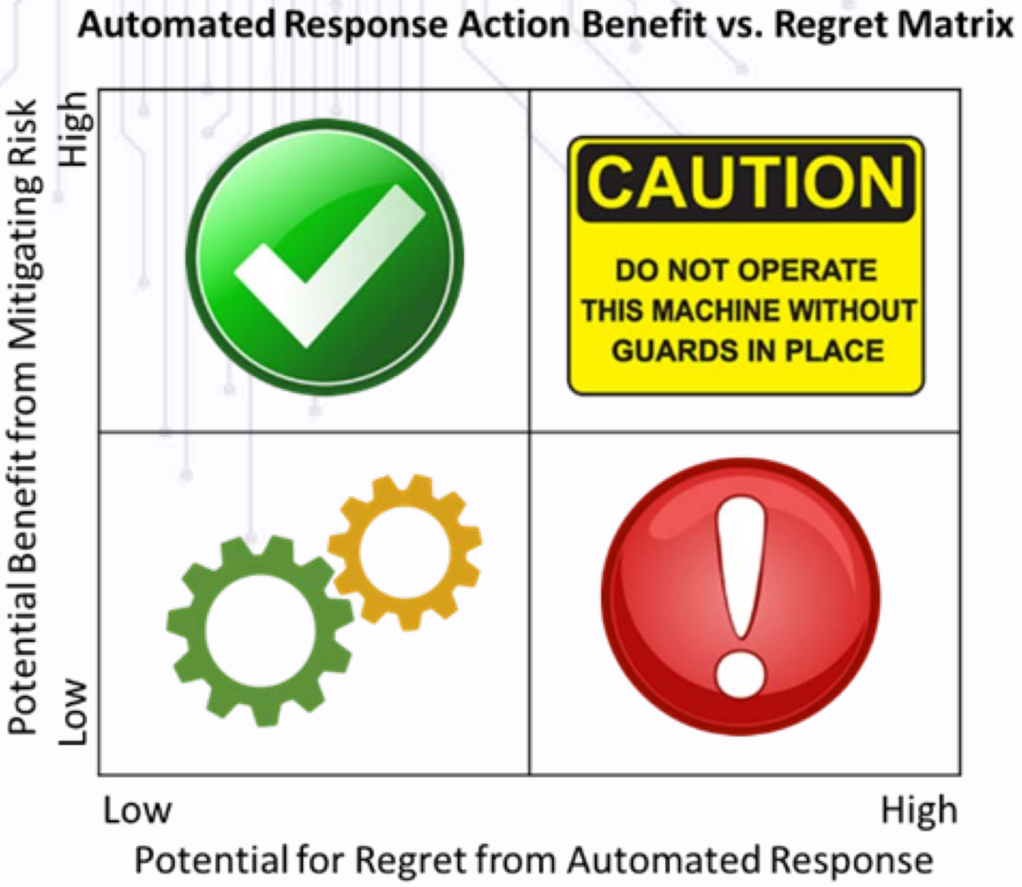
Orchestration platforms have different models for security – make sure the one you buy meets your needs

- 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**

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

Actionable Information

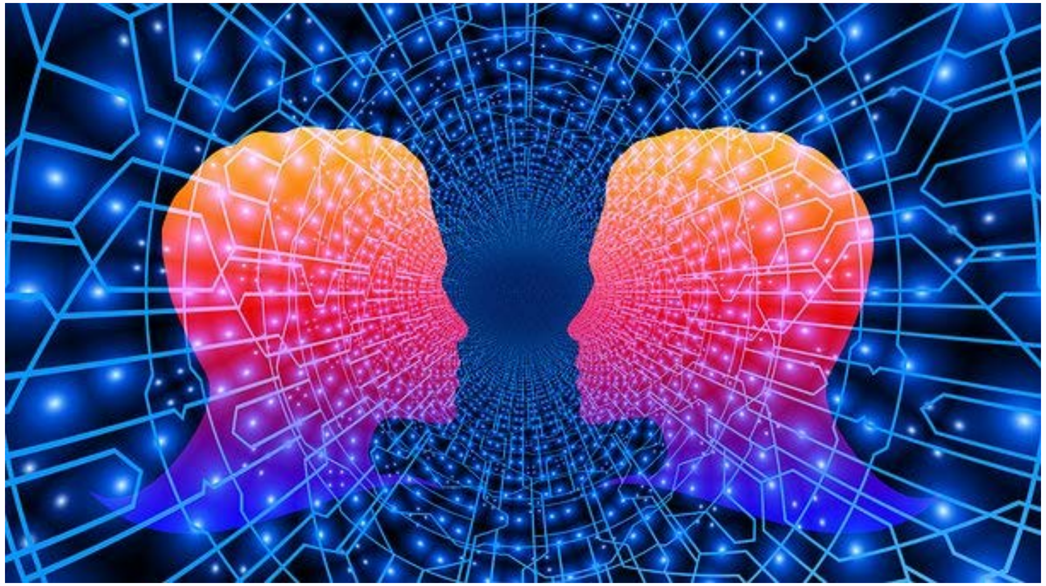
Share information that drives local response

- 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?

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**



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

Influencing Industry

Make industry your partner, not your competitor

- Let industry be your innovator and scaling function
  - COTS is a given in every ecosystem
  - Transfer knowledge, not technology
  - Affordable sustainment

- Buy differently
  - Demand support for interoperability
  - Demand robust APIs
  - Ask how something new improves what you already have

Actionable Information Sharing

"The real key is about translation"

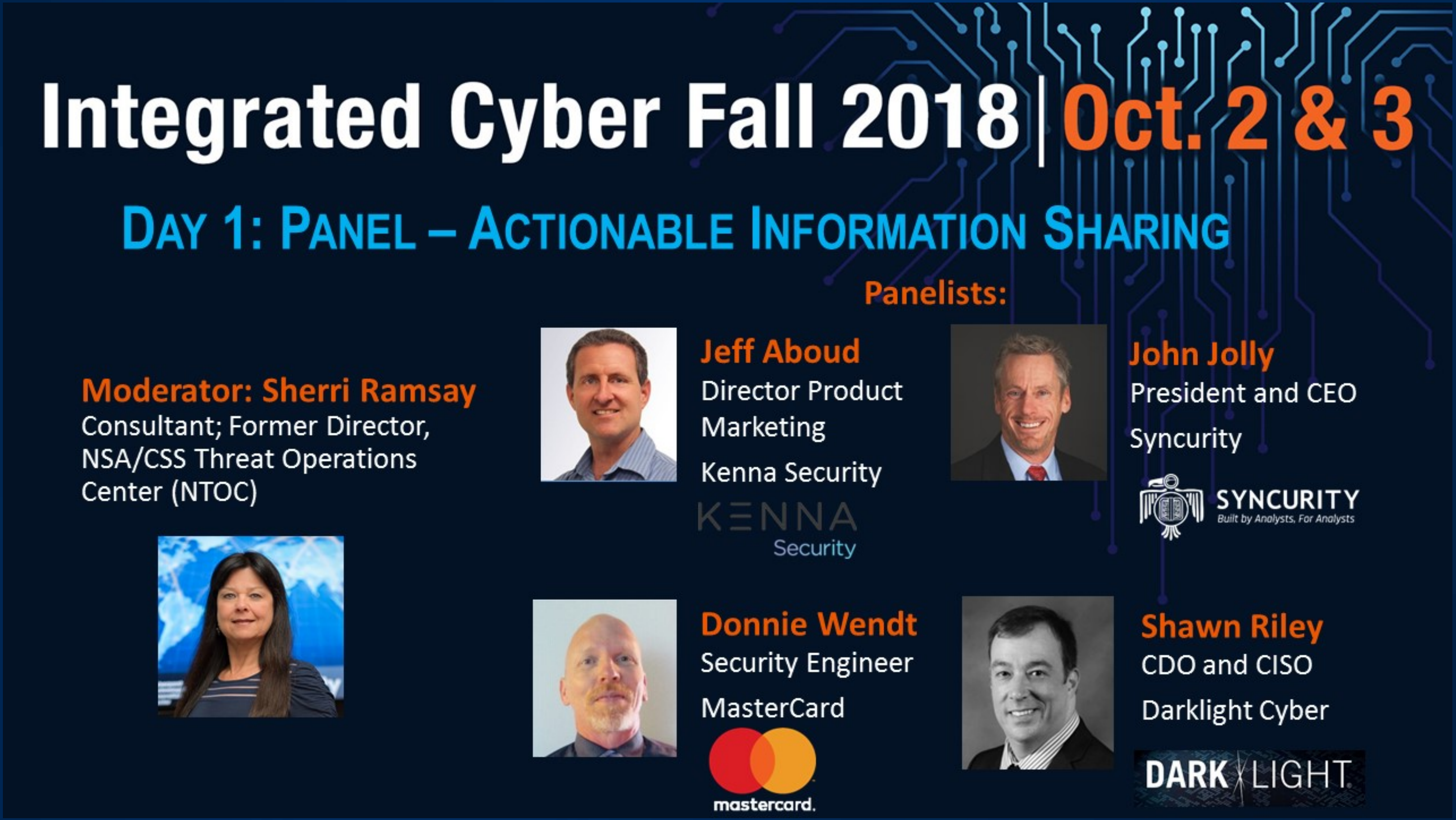
Integrated Cyber | Oct 2 & 3

Power of Community and Actionable Information Sharing

Keynote Speaker:

Ms. Sherri Ramsay

Consultant; Former Director NSA/CSS Threat Operations Center (NTOC)



Integrated Cyber Fall 2018 | Oct. 2 & 3

Day 1: Panel – Actionable Information Sharing

Moderator: Sherri Ramsay
Consultant; Former Director, NSA/CSS Threat Operations Center (NTOC)

Panelists:

Jeff Aboud
Director Product Marketing
Kenna Security

KENNA Security

John Jolly
President and CEO
Syncurity

SYNCURITY
Built by Analysts, For Analysts

Donnie Wendt
Security Engineer
MasterCard

mastercard.

Shawn Riley
CDO and CISO
Darklight Cyber

DARK LIGHT

Shareable Workflows: Spreading and adoption of cyber workflows through reuse and sharing throughout the community

Paul Laskowski
Senior Systems Engineer
JHU/APL

APL Johns Hopkins
Applied Physics Laboratory

Bharathram Krishnan
Solutions Architect
CyberSponse

CYBERSPONSE
ADAPTIVE SECURITY

Adversary Playbooks

Mike Harbison
Unit 42 Threat Researcher
Palo Alto Networks

paloalto NETWORKS

Taking a Modern Approach to Security: What You've Always Done Isn't Sufficient Anymore

Jeff Aboud
Director, Product Marketing
Kenna Security

KENNA Security

STOP Chasing Indicators

Josh Day
Senior Threat Hunter
Accenture

accenture

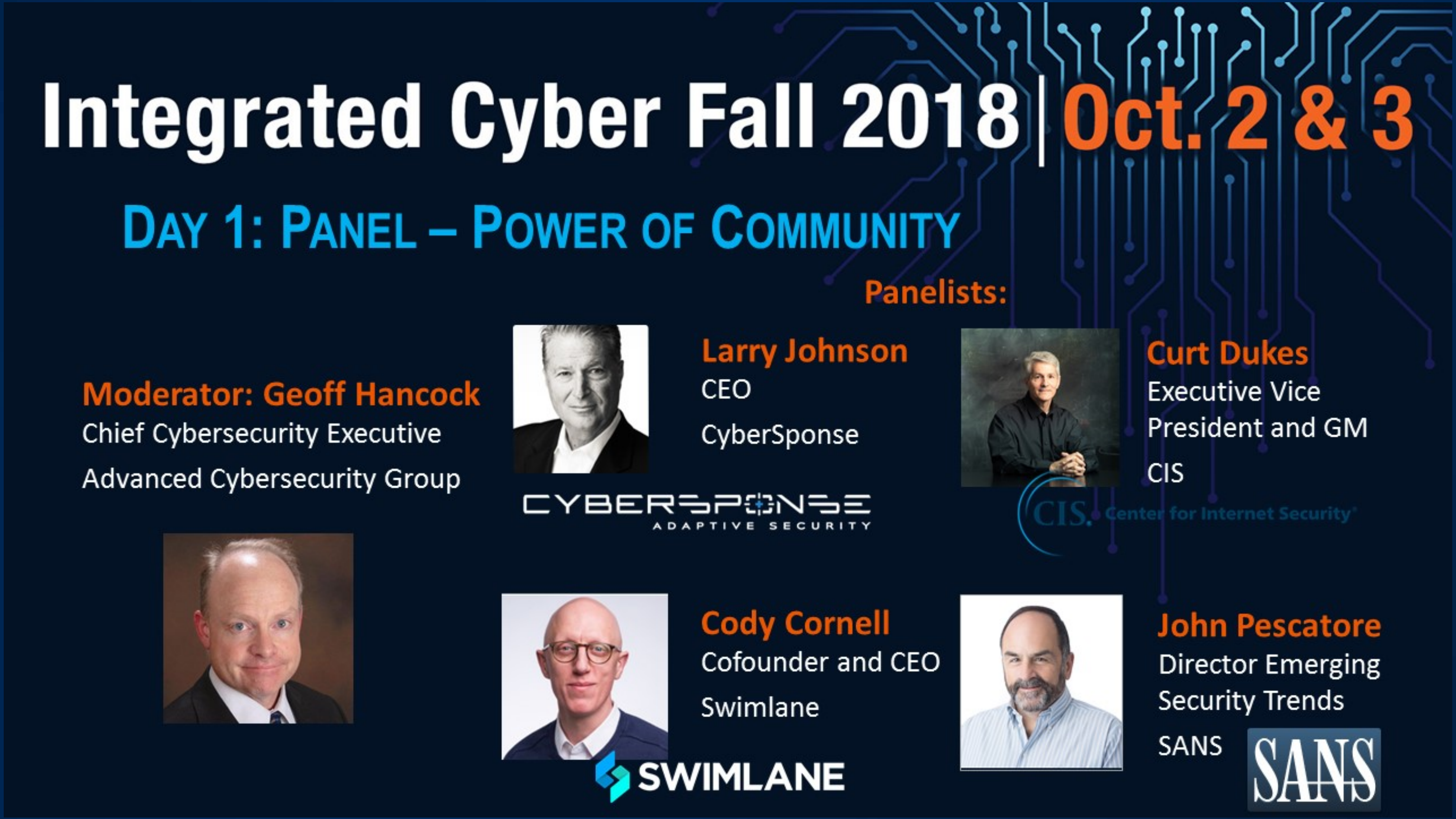
Brad Rhodes
Senior Threat Hunter
Accenture

accenture

Power of Community

We are committed to trust and collaboration across

public and private sectors



Integrated Cyber Fall 2018 | Oct. 2 & 3

Day 1: Panel – Power of Community

Moderator: Geoff Hancock
Chief Cybersecurity Executive
Advanced Cybersecurity Group

Panelists:

Larry Johnson
CEO
CyberSponse

CYBERSPONSE
ADAPTIVE SECURITY

Curt Dukes
Executive Vice President and GM
CIS

CIS. Center for Internet Security®

Cody Cornell
Cofounder and CEO
Swimlane

SWIMLANE

John Pescatore
Director Emerging Security Trends
SANS

SANS

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

Host: Cory Huyssoon

Systems Engineer

JHU/APL

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Presenter: Tim Schaad

Executive Director, Advanced Cyber Range Environment and Cyber Range Services

ManTech

AETNA Entitlement, Identity, and Risk System (AEIRS)

Jon Backus

Product Manager for AEIRS

AETNA

aetna

Power of Communities for the Evolution of Security Capabilities

Lior Kolnik

Head of Security Research

Demisto

DEMISTO

Reducing Healthcare Cyber Risk Using a Co
SOAR-enabled Healthcare Community H-SOC

Eric Eder

Founder & President

Sequris Group

sequris
VENTURE BEYOND RISK

John Jolly

President and CEO

Syncurity

SYNCURITY
Built by Analysts, For Analysts

ational Awareness for ICS (MOSAICS), Functional Requirements Update

Rich Scalco

Engineer

SPAWAR Systems Center Atlantic

SPAWAR

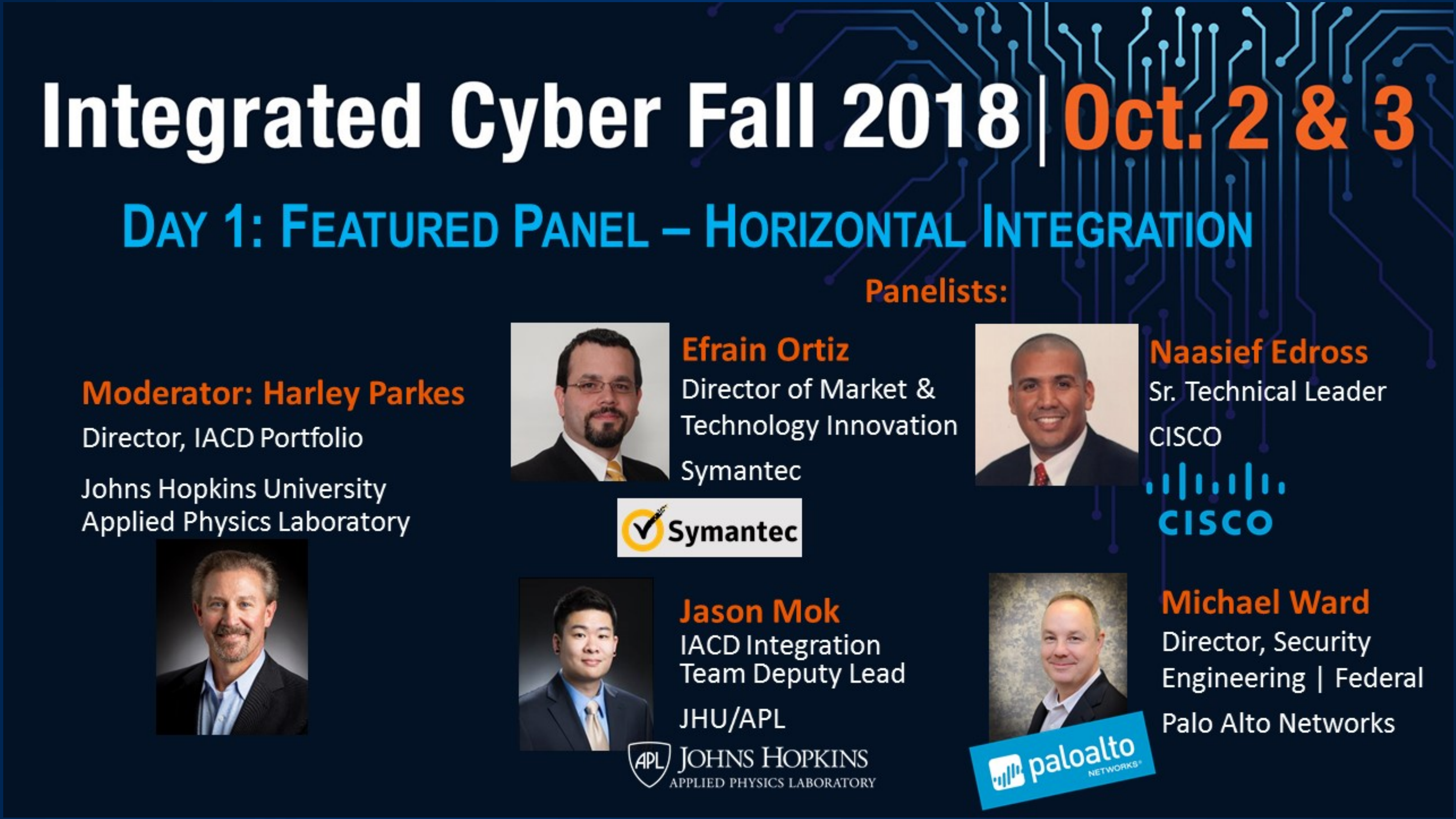
Larry Cox

Engineer

USPACOM (AECOM)

Operationalization

- Scale it
- Transfer it
- Make it adoptable and sustainable



Integrated Cyber Fall 2018 | Oct. 2 & 3

Day 1: Featured Panel – Horizontal Integration

Moderator: Harley Parkes

Director, IACD Portfolio

Johns Hopkins University
Applied Physics Laboratory

Panelists:

Efrain Ortiz

Director of Market & Technology Innovation

Symantec

Naasief Edross

Sr. Technical Leader

CISCO

Jason Mok

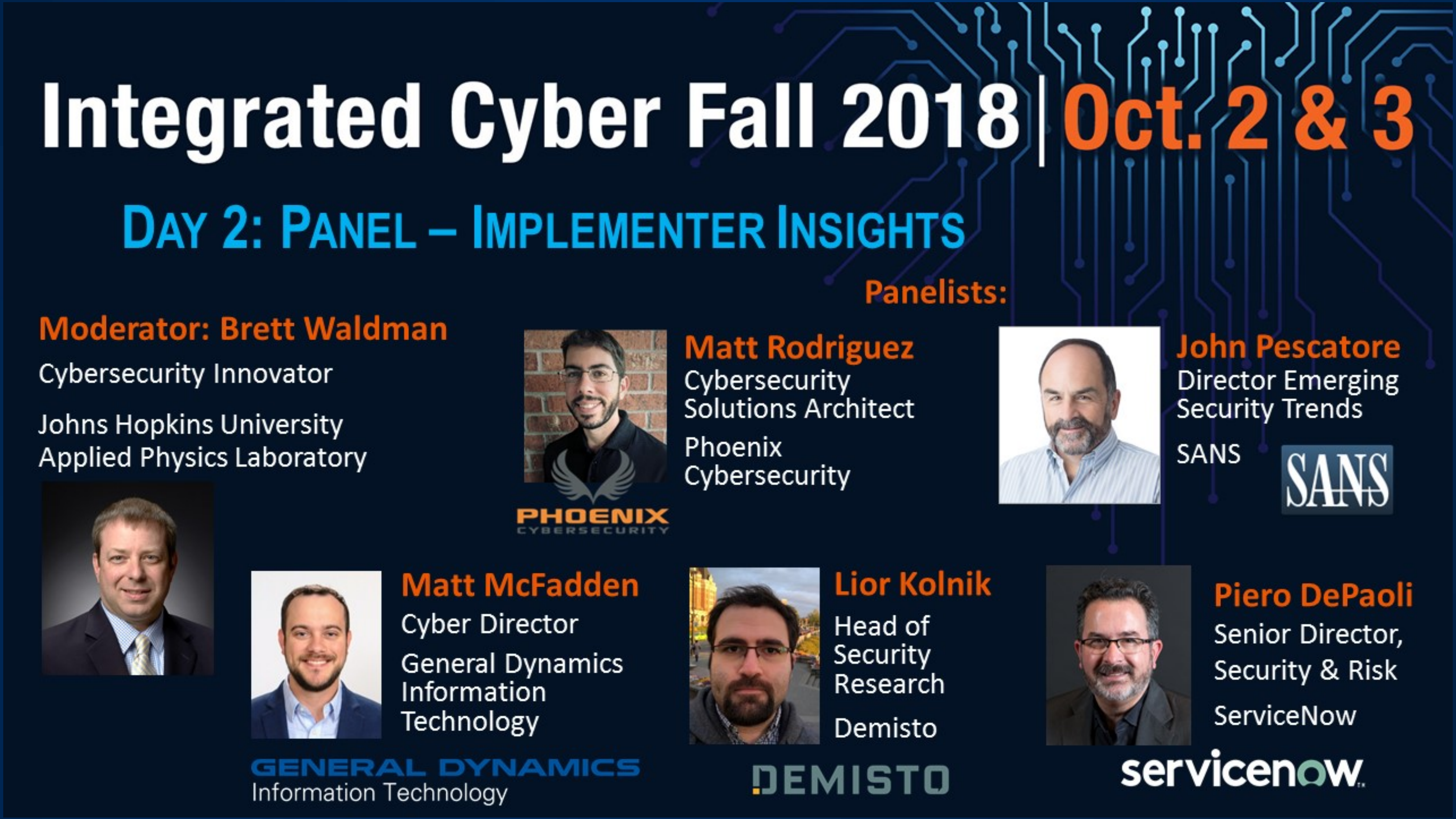
IACD Integration
Team Deputy Lead

JHU/APL

Michael Ward

Director, Security Engineering | Federal

Palo Alto Networks



Integrated Cyber Fall 2018 | Oct. 2 & 3

Day 2: Panel – Implementer Insights

Moderator: Brett Waldman
Cybersecurity Innovator

Johns Hopkins University
Applied Physics Laboratory

Panelists:

Matt Rodriguez
Cybersecurity
Solutions Architect

Phoenix
Cybersecurity

PHOENIX
CYBERSECURITY

John Pescatore
Director Emerging
Security Trends

SANS

SANS

Matt McFadden
Cyber Director

General Dynamics
Information
Technology

GENERAL DYNAMICS
Information Technology

Lior Kolnik
Head of
Security
Research

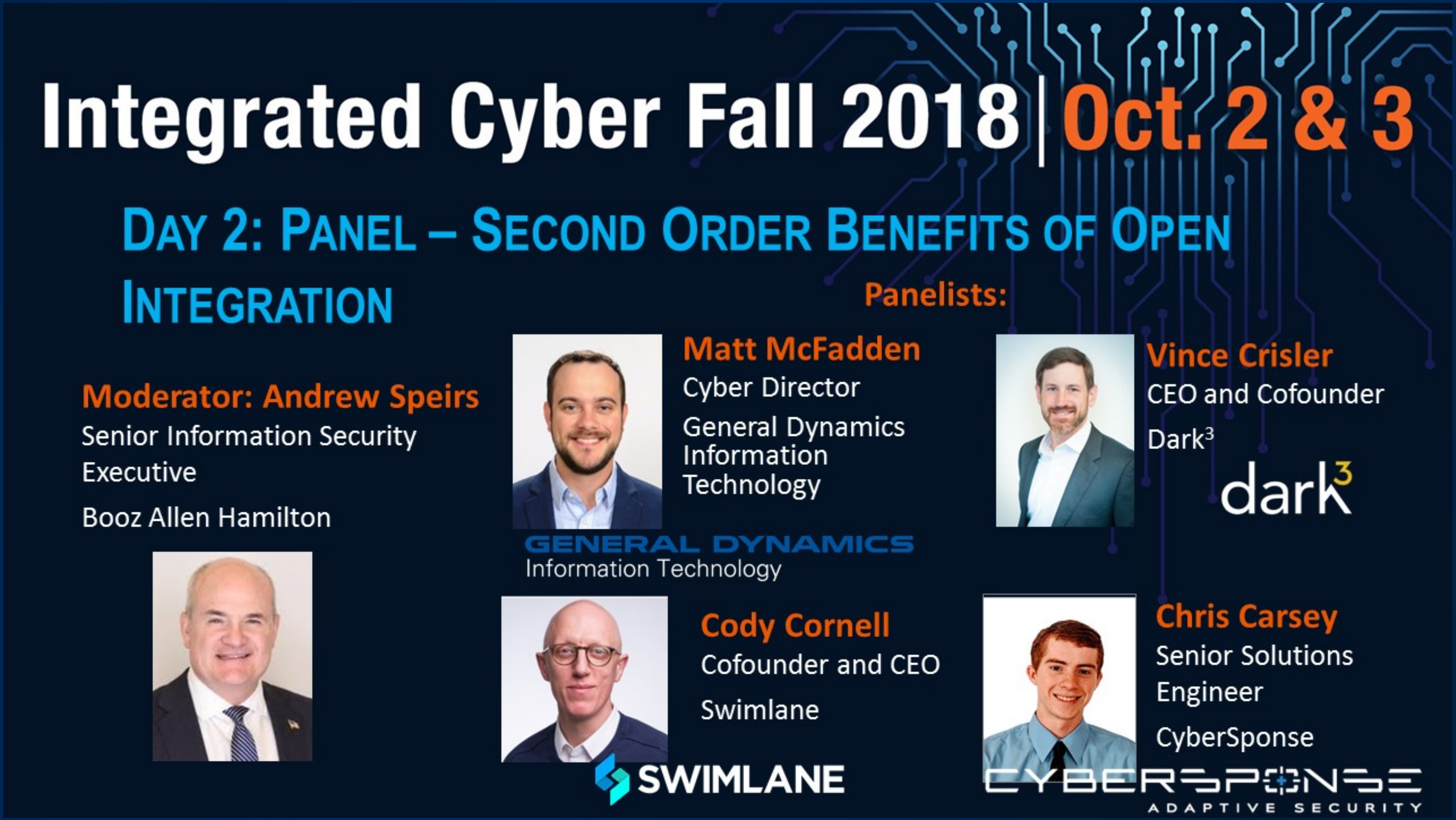
Demisto

DEMISTO

Piero DePaoli
Senior Director,
Security & Risk

ServiceNow

servicenow



Integrated Cyber Fall 2018 | Oct. 2 & 3

Day 2: Panel – Second Order Benefits of Open Integration

Moderator: Andrew Speirs

Senior Information Security Executive

Booz Allen Hamilton

Panelists:

Matt McFadden

Cyber Director

General Dynamics Information Technology

GENERAL DYNAMICS
Information Technology

Vince Crisler

CEO and Cofounder

Dark^3

dark^3

Cody Cornell

Cofounder and CEO

Swimlane

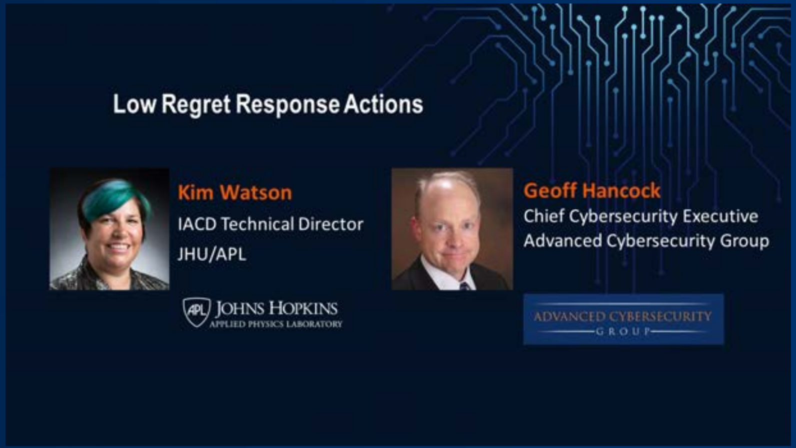
SWIMLANE

Chris Carsey

Senior Solutions Engineer

CyberSponse

CYBERSPONSE
ADAPTIVE SECURITY



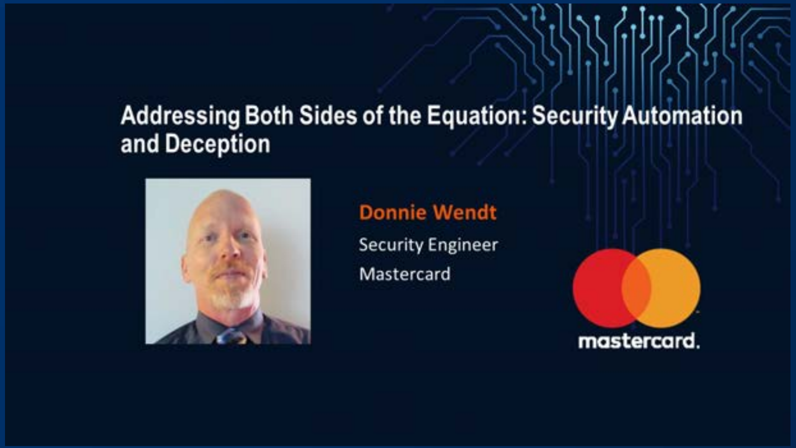
Low Regret Response Actions

Kim Watson
IACD Technical Director
JHU/APL

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Geoff Hancock
Chief Cybersecurity Executive
Advanced Cybersecurity Group

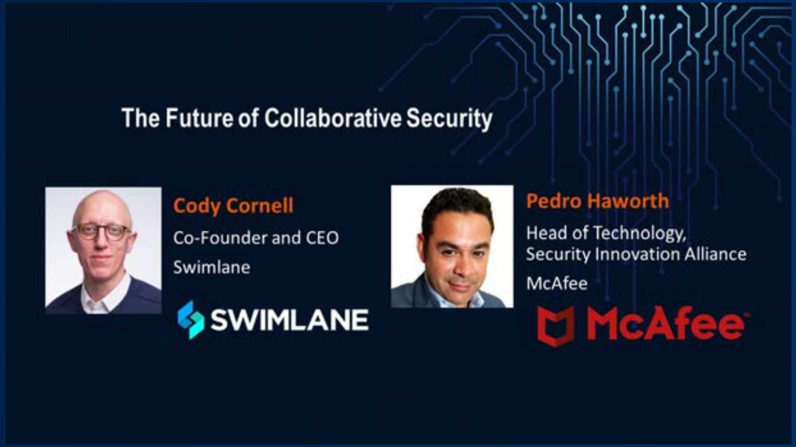
ADVANCED CYBERSECURITY
GROUP



Addressing Both Sides of the Equation: Security Automation and Deception

Donnie Wendt
Security Engineer
Mastercard

mastercard.



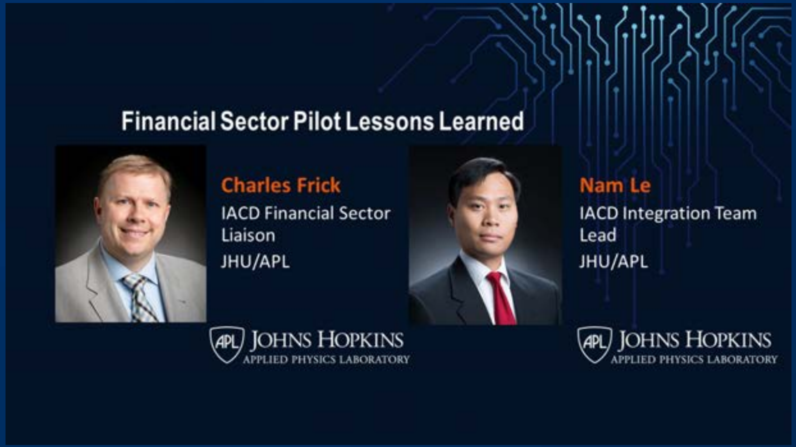
The Future of Collaborative Security

Cody Cornell
Co-Founder and CEO
Swimlane

SWIMLANE

Pedro Haworth
Head of Technology,
Security Innovation Alliance
McAfee

McAfee



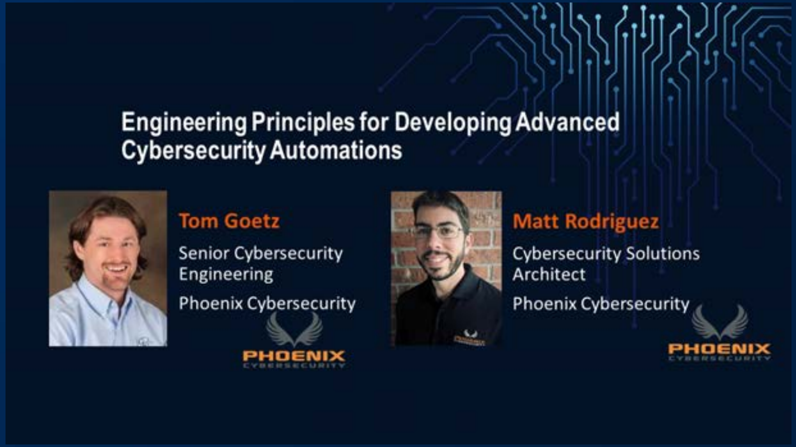
Financial Sector Pilot Lessons Learned

Charles Frick
IACD Financial Sector Liaison
JHU/APL

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Nam Le
IACD Integration Team Lead
JHU/APL

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY



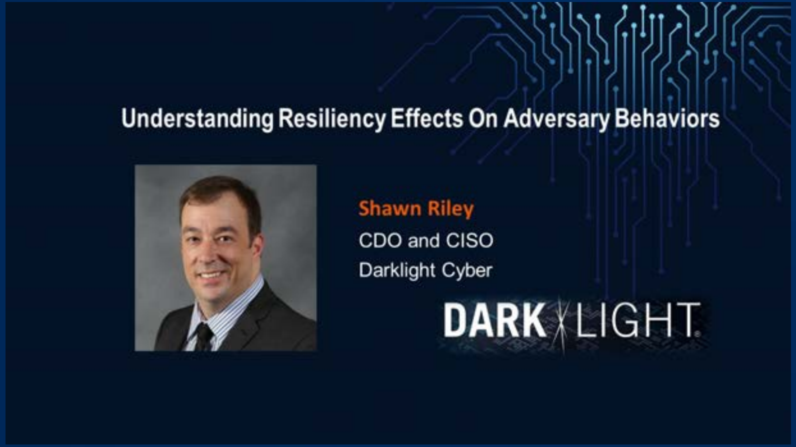
Engineering Principles for Developing Advanced Cybersecurity Automations

Tom Goetz
Senior Cybersecurity Engineering
Phoenix Cybersecurity

PHOENIX
CYBERSECURITY

Matt Rodriguez
Cybersecurity Solutions Architect
Phoenix Cybersecurity

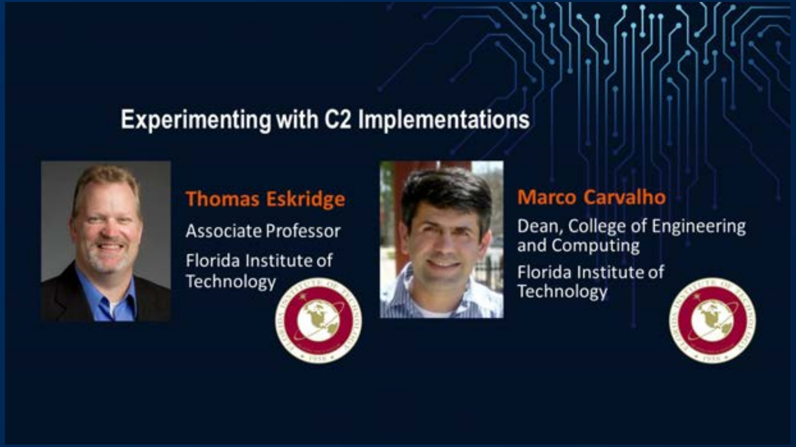
PHOENIX
CYBERSECURITY



Understanding Resiliency Effects On Adversary Behaviors

Shawn Riley
CDO and CISO
Darklight Cyber

DARK LIGHT



Experimenting with C2 Implementations

Thomas Eskridge
Associate Professor
Florida Institute of Technology

Marco Carvalho
Dean, College of Engineering and Computing
Florida Institute of Technology

AIS Automated Indicator Sharing
ANOMALI
EclecticIQ
FINANCIAL SERVICES ISAC
MISP Threat Sharing
RISKIQ
SOLTRA
TRUSTAR

Alexa
DOMAINTOOLS
herdProtect Anti-Malware Scanner
IP Void
MX TOOLBOX
ThreatMiner Data Mining for Threat Intelligence
URLVoid
virustotal
WHOis.net

CISCO
JUNIPER NETWORKS
netfilter firewalling, NAT, and packet mangling for linux
paloalto NETWORKS
pf Sense
Ultra ELECTRONICS 3eTI
tenable

DEMISTO
splunk> phantom
FireEye

IACD

SWIMLANE
CYBERSPONSE ADAPTIVE SECURITY
VERVE INDUSTRIAL PROTECTION

cuckoo
SURICATA
Indegy
NOZOMI NETWORKS
SECURITY MATTERS
Security Onion
SNORT

Carbon Black.
FORCEPOINT
ForeScout
McAfee
Microsoft
Symantec
TANIUM
tripwire

ALIEN VAULT
ArcSight An HP Company
elastic
splunk>
ATLASSIAN
BEST PRACTICAL Request Tracker
servicenow
Apache ACTIVEMQ
informatica
TIBCO
STIX
TAXII
OpenC2
COBALT STRIKE ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

IACD Community Partners

U.S. DEPARTMENT OF HOMELAND SECURITY
NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA
SPAWAR
bpi BANK POLICY INSTITUTE
DEPARTMENT OF ENERGY UNITED STATES OF AMERICA
SANS
IACD
FINANCIAL SERVICES ISAC
INCIDENT RESPONSE CONSORTIUM
GLOBAL CYBER ALLIANCE
CIS Center for Internet Security
OASIS
Huntington
mastercard
REGIONS

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://secwww.jhuapl.edu/iacd

@IACD_automate

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

icd@jhuapl.edu