IACD

Integrated Cyber

Oct 2 & 3, 2018

Johns Hopkins University
Applied Physics Laboratory
Laurel, Maryland

IACD

Power of Community

Actionable Information Sharing

Operationalization

// Welcome

Integrated Cyber is the premier cyber conference bringing together the Integrated Adaptive Cyber Defense (IACD), Automated Indicator Sharing (AIS), and Information-Sharing communities.

This event provides a forum for collaboration and technical exchange to support the adoption of integrated, automated cyber defense and information sharing. This two-day event showcases government, industry, operations, and critical infrastructure perspectives.

The conference is hosted by the Johns Hopkins University Applied Physics Laboratory (JHU/APL), 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.

// Contents

// Welcome 1

// Main Stage Speaker Bios 2

// Sponsor Thanks 5

// Agenda 6

// Featured Speakers Abstracts 8

// Featured Panel Abstract & Members 9

// Lunchtime Lectures Abstracts & Speakers 9

// **Day 1** Breakout Session 1 Details 10

// **Day 1** Breakout Session 2 Details 12

// **Day 2** Breakout Session 3 Details 14

// **Day 2** Breakout Session 4 Details 16

// **Day 2** Breakout Session 5 Details 18

// Maps 20

// General Information 21

// Main Stage Speaker Bios

Neal Ziring, Technical Director, Capabilities Directorate, National Security Agency

Neal Ziring is the Technical Director for the National Security Agency's Capabilities Directorate, serving as a technical advisor to the Capabilities Director, Deputy Director, and other senior leadership. Mr. Ziring is responsible for setting the technical direction across many parts of the capabilities mission space, including in cybersecurity. He tracks technical activities, promotes technical health of the staff, and acts as liaison to various industry, intelligence, academic, and government partners. Prior to the formation of the Capabilities Directorate, Mr. Ziring served 5 years as Technical Director of the Information Assurance Directorate.

His personal expertise areas include security automation, IPv6, cloud computing, cross domain information exchange, data access control, and cyber defense.

Prior to coming to NSA in 1988, Mr. Ziring worked at AT&T Bell Labs. He has B.S. degrees in computer science and electrical engineering and an M.S. degree in computer science, all from Washington University in St. Louis.

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

Sherri Ramsay is a consultant, engaged in strategy development and planning, partnership development, and marketing/development of security operations centers. She is on the Board of Advisors for Virginia Tech's Hume Research Center and for TruSTAR Technology.

Ms. Ramsay is the former director of NSA's Threat Operations Center (NTOC). She led discovery and characterization of threats to national security systems, provided situational awareness for those threats, and coordinated actionable information to counter those threats with the Department of Defense (DoD), Department of Homeland Security (DHS), and Federal Bureau of Investigation (FBI). She served as a senior leader in NSA's Signals Intelligence Directorate, Technology Directorate, and Information Assurance Directorate.

Ms. Ramsay has received the DoD Distinguished Civilian Service Award, the Exceptional Civilian Service Award, the NSA Meritorious Civilian Service Award twice, the Presidential Rank Award, the National Intelligence Meritorious Unit Citation, the Louis Tordella Award, and the Armed Forces Communications and Electronics Association (AFCEA) Meritorious Service to the Intelligence Community Award. She has also received the Women's Leadership Award from the congressional bipartisan SMART (Strengthening the Mid-Atlantic Region for Tomorrow) caucus.

Ms. Ramsay graduated magna cum laude (general honors) from the University of Georgia (B.S.). She graduated with honors from the Johns Hopkins University (M.S.). She graduated from the Industrial College of the Armed Forces (ICAF), National Defense University (M.S.). She received a Certificate in Leadership from the University of Virginia.

Rick Howard, Chief Security Officer, Palo Alto Networks

Rick Howard is Palo Alto Networks' Chief Security Officer, where he has overall responsibility for the company's internal security program, leads Palo Alto Networks Threat Intelligence Team (Unit 42), directs the company's efforts on the Cyber Threat Alliance Information Sharing nonprofit, hosts the Cybersecurity Canon Project, and provides thought leadership for the company and the cybersecurity community at large. Mr. Howard previously served as TASC Chief Information Security Officer, iDefense General Manager, Counterpane SOC Director, and Commander of the U.S. Army's Computer Emergency Response Team, where he coordinated network defense, network intelligence, and network attack operations for the Army's global network. He holds a master's degree in computer science from the Naval Postgraduate School and an engineering degree from the U.S. Military Academy. He also taught computer science at the Academy from 1993 to 1999.

Paul Kurtz, Cofounder and CEO, TruSTAR Technology

Paul Kurtz is an internationally recognized expert on cybersecurity and the cofounder and CEO of TruSTAR Technology. Mr. Kurtz began working on cybersecurity at the White House in the late 1990s. He served in senior positions relating to critical infrastructure and counterterrorism on the White House's National Security and Homeland Security Councils under Presidents Clinton and Bush.

Since leaving government, Mr. Kurtz has held numerous private sector cybersecurity positions, including founding the Cyber Security Industry Alliance (acquired by TechAmerica) and serving as Executive Director of SAFECode, as Managing Partner of Good Harbor Consulting in Abu Dhabi, and as Chief Information Security Officer of CyberPoint International.

Mr. Kurtz's work in intelligence analysis, counterterrorism, critical infrastructure protection, and nonproliferation of weapons of mass destruction influenced his approach to cybersecurity—specifically the need to build an exchange platform that addresses barriers to fusing cyber and physical intelligence in real time while addressing bureaucratic, legal, and market risk concerns.

// Main Stage Speaker Bios

Ben Miller, Director of Threat Operations, Dragos, Inc.

Ben Miller is Director of the Threat Operations Center at the industrial cybersecurity company Dragos, Inc., where he leads a team of analysts in performing active defense inside of ICS/SCADA networks. In this capacity, he is responsible for threat hunting, incident response, and malware analysis for the industrial community.

Prior to his role at Dragos, Inc., Mr. Miller was the Associate Director of the Electricity Information Sharing & Analysis Center (E-ISAC) and led cyber analysis for the sector. He and his team focused on leading-edge cyber activities as they relate to the North American bulk electric system. Mr. Miller was recognized as instrumental in building new capabilities surrounding information sharing and analytics in his 5 years at the E-ISAC. Before joining the E-ISAC, he built and led a nine-person team focused on network security monitoring, forensics, and incident response at a Fortune 150 energy firm. His team received numerous accolades from industry and law enforcement. During this time, he also worked on a CIP implementation project and various enterprise-wide mitigation programs. Mr. Miller has over 18 years of experience and currently holds the CISSP and GIAC GREM certifications. He has served in various roles, including both planner and player roles in GridEx I, II, and III. He served as a member of the NERC Cyber Attack Task Force, as an acknowledged contributor to NIST SP 800-150, as a panel member of the NBISE Advanced Defender panel, and as adviser on the CI Advanced Defender Training program. Mr. Miller is an accomplished speaker in various venues including SANS, ICSWJG, ShmooCon, and others. He was recognized by SANS as a 2017 Difference Maker Award Winner for his contributions to the electricity sector.

Karl Gumtow, Executive Director, Maryland Innovation & Security Institute

Mr. Karl R. Gumtow serves as Executive Director of the Maryland Innovation & Security Institute as well as the Chief Executive Officer of Cyber Point International, LLC. Mr. Gumtow served as Senior Vice President of RABA Technologies LLC and was responsible for managing innovation, pioneering new avenues of business development, and helping customers solve their most complex and intractable technology problems. He has more than 16 years of operational, professional, and technical experience and has dedicated his career to serving the federal and commercial technology sectors. His expertise in directing large engineering organizations, managing multi-million-dollar engineering programs, leading diverse technical teams, and developing innovative strategies to identify and win new business has allowed him to innovate, explore, and push boundaries of technology consulting. His commitment to excellence and best practices, as well as his passion for his work, is evident in the numerous achievements of his team. He holds a Master of Science in electrical engineering from the Johns Hopkins University and a Bachelor of Science in electrical engineering from the George Washington University. He is a part-time bush pilot for one of Alaska's most remote mountain ranges.

Thank You to Our Sponsors!

Integrated Cyber | Oct 2&3

Power of Community and Actionable Information

PLATINUM LEVEL SPONSOR:

GENERAL DYNAMICS
Information Technology

Integrated Cyber | Oct 2&3

Power of Community and Actionable Information

GOLD LEVEL SPONSOR:

DARK LIGHT.ai®
Active Defense Expert System

Integrate Automate Validate **Explain**

Integrated Cyber | Oct 2&3

Power of Community and Actionable Information

SILVER LEVEL SPONSOR:

SWIMLANE

Integrated Cyber | Oct 2&3

Power of Community and Actionable Information

SILVER LEVEL SPONSOR:

CYBERSPONSE
ADAPTIVE SECURITY

Nonprofit Partners:

CIS. Center for Internet Security®

GLOBAL CYBER ALLIANCE

INCIDENT RESPONSE CONSORTIUM

// Agenda

Integrated Cyber Day 1 – Tuesday, October 2

8:00–8:45	Registration and Refreshments
8:45–9:00	Welcome
9:00–9:45	**Keynote** Neal Ziring, Technical Director, NSA Capabilities Directorate
9:45–10:30	**Integrated Cyber: Automated Information Sharing and the Power of Community** Harley Parkes, JHU/APL
10:30–10:45	Break
10:45–11:30	**Keynote** Sherri Ramsay, Consultant; Former Director, NSA/CSS Threat Operations Center (NTOC)
11:30–12:00	**Featured Speaker** Paul Kurtz, CEO and Cofounder, TruSTAR
12:00–1:00	Lunch, with Lunchtime Lecture by Global Cyber Alliance starting at 12:30
1:00–2:00	Breakout Session 1
2:00–2:15	Break
2:15–3:15	Breakout Session 2
3:15–3:30	Break
3:30–4:30	**Featured Panel: Horizontal Integration** Moderator: Harley Parkes, JHU/APL Panelists: Palo Alto Networks, Symantec, Cisco, JHU/APL
4:30–6:30	Networking Social

Integrated Cyber Day 2 – Wednesday, October 3

8:00–8:45	Registration and Refreshments
8:45–9:00	Welcome
9:00–9:45	**Keynote** Rick Howard, Chief Security Officer, Palo Alto Networks
9:45–10:00	Break
10:00–11:00	Breakout Session 3
11:00–11:15	Break
11:15–12:00	**Featured Speaker** Ben Miller, Director of Threat Operations, Dragos, Inc.
12:00–1:00	Lunch, with Lunchtime Lecture by OpenC2 starting at 12:30
1:00–2:00	Breakout Session 4
2:00–2:15	Break
2:15–3:15	Breakout Session 5
3:15–3:30	Break
3:30–4:15	**Featured Speaker** Karl Gumtow, Executive Director, Maryland Innovation & Security Institute
4:15–4:30	Summary and Inspiration

// Featured Speakers Abstracts

Paul Kurtz (Day 1 at 11:30)
Power of Information Sharing with Lessons Learned in the Retail Sector

Information sharing can be a powerful strategy to security operations and beyond. Learn from real-life case studies on how a cyber intelligence exchange can transform your organization into a more secure, efficient machine.

Ben Miller (Day 2 at 11:15)
ICS Threat Operations: Responding to Industrial Intrusions

This presentation will offer thoughts on how to respond to industrial intrusions. One of our biggest challenges as a community is how we are largely untested in our ability to recognize and respond to an industrial intrusion. Making matters worse, the industrial environments often lack the level of logging needed to respond and understand an attack. We must quickly move to a “protection eventually fails” mindset and understand how to “live off the land” to gain the defender’s advantage. This talk will pragmatically step through how our engagements have shaped our thoughts and our technology.

Karl Gumtow (Day 2 at 3:30)
DreamPort: Innovation. Collaboration. Community Engagement

DreamPort is a cyber innovation, collaboration, and prototyping facility located in Columbia, Maryland. It was created by USCYBERCOM through a Partnership Intermediary Agreement awarded to the Maryland Innovation and Security Institute (MISI) in May 2018.

DreamPort is designed as an open facility that welcomes the public to tour, collaborate, and prototype in support of USCYBERCOM and its mission partners. Daily, monthly, and quarterly collaboration events will be announced through our website and via e-mail for those who register to participate in our DreamPort Partnership Network.

The use of Partnership Intermediaries is authorized by 15 U.S. Code 3715 and permits an intermediary to assist, counsel, advise, evaluate, or otherwise cooperate with small business firms, institutions of higher education, or educational institutions that need or can make demonstrably productive use of technology-related assistance.

// Featured Panel Abstract & Members

Horizontal Integration (Day 1 at 3:30)

As more and more vendors realize the importance of integrating within their product lines and with third-party vendors, many large market players are designing frameworks, platforms, and standards to make their products and product lines accessible. This panel will focus on the importance of horizontal integration across vendors, how it has become a driver for competition in the open market, and its importance for automation and speed of cyber defense.

The panel will explore the operational challenges with this type of integration across vendors/products as well as the various models being developed and how they can be used to address these challenges.

Moderator: Harley Parkes, Director, IACD Portfolio, JHU/APL

Panelists

Left to right: Efrain Ortiz, Director Market & Technology Innovation, Symantec; Naasief Edross, Senior Technical Leader, Cisco; Jason Mok, IACD Deputy Integration Team Lead, JHU/APL; and Michael Ward, Director, Security Engineering I Federal, Palo Alto Networks

// Lunchtime Lectures Abstracts & Speakers

Mary Rahmani, Global Partnership Officer, Global Cyber Alliance (Day 1 at 12:30)
Less Talk and More Action: How the Global Cyber Alliance Is Making a Difference and You Can Too

Global Cyber Alliance (GCA) is an international nonprofit focused on developing and deploying practical solutions, which we make freely available, that measurably improve our collective cybersecurity.

During this lecture, you'll learn about GCA's efforts to bring communities together to provide scalable solutions and how those resources can help you address systemic risk. We'll discuss GCA's efforts to tackle security challenges associated with IoT devices and technologies as well as a new initiative to help small and medium businesses confront cyber risk. Attendees will learn how they can access GCA's trusted and globally available resources and become part of a growing movement to eradicate cyber risk.

David Lemire, Secretary, OASIS OpenC2 Technical Committee (Day 2 at 12:30)
OpenC2 Update

A community update on OpenC2, to include highlights of this week's face-to-face meeting and information on how you can get involved.

// Day 1 Breakout Session 1 Details

Session 1 1:00–2:00

Actionable Information Sharing: Enabling Defenses

Auditorium

Sharing IOCs is necessary but not sufficient. We need to make processing/usage of IOCs as automated as possible, and we need to evolve what is being shared to be something that organizations can use to more appropriately protect and defend the network. This panel will discuss what makes threat information actionable for network defenders and what type of information (e.g., adversary TTPs) would be valuable to share.

Moderator:

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

Panelists:

Jeff Aboud, Director, Product Marketing, Kenna Security

John Jolly, President and CEO, Syncurity

Shawn Riley, CDO and CISO, DarkLight Cyber

Donnie Wendt, Security Engineer, Mastercard

Actionable Information Sharing

Integrator COI: Tales from the Trenches: Use of a Cyber Range to Overcome Obstacles to SOAR/IACD Adoption

K-3 and K-4

Cyber Ranges offer features that can be used reduce risk and measure performance of the adoption of SOAR/IACD capabilities. A Cyber Range has the ability to recreate “worst day” scenarios that “stress test” SOAR/IACD platforms beyond the ability of limited production pilots or laboratory testing to minimize risk during production implementation and operation. Cyber ranges have tools to instrument and measure system and human activities to model improvements in SOAR/IACD capabilities. A well-engineered Cyber Range allows for high-quality data collection, which increases confidence in automated decision processes and leads to improved response.

Host:

Cory Hoyssoon, Systems Engineer, JHU/APL

Presenter:

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

Community

Tuesday, Oct 2

Low-Regret Response Actions

K-5 and K-6

Instead of asking IF we should automate cyber defenses, how about if we asked WHEN we should automate? This talk presents a benefit versus regret matrix and discusses the concept of low-regret response actions.

Presenters:

Kim Watson, IACD Technical Director, JHU/APL

Geoff Hancock, Chief Cybersecurity Executive, Advanced Cybersecurity Group

Operationalization

Aetna Entitlement, Identity, and Risk System (AEIRS)

K-7 and K-8

Many organizations have adopted machine learning and data analytics to help them identify security anomalies. However, mere identification isn't good enough in a world where Petya and other modern attacks can take down 15,000 servers in a single organization in under two minutes. To combat these new types of malware, organizations need to be looking at Model Driven Security Orchestration where the security responses to emerging threats and attacks are automated and driven at machine speed. In this presentation, Aetna will provide an overview of our security orchestration program, including what worked, what didn't, and lessons learned.

Presenter:

Jon Backus, Product Manager for AEIRS, Aetna

Community

// Day 1 Breakout Session 2 Details

Session 2 2:15–3:15

Power of Community

Auditorium

Cybersecurity has very few absolutes, almost everything is a best practice, and the sharing of tools and techniques is critical to making best practices a reality. There is a lot of interest in building and participating in practitioner communities where you can find individuals like yourself that you relate to and trust. Such communities allow practitioners to learn from each other, share with one another, and generally advance their expertise. This panel discusses the power of community in improving cybersecurity and defining/advancing best practices.

Moderator:

Geoff Hancock, Chief Cybersecurity Executive, Advanced Cybersecurity Group

Panelists:

Larry Johnson, CEO, CyberSponse

Curt Dukes, Executive Vice President and General Manager, Center for Internet Security

Cody Cornell, Cofounder and CEO, Swimlane

John Pescatore, Director of Emerging Security Trends, SANS Institute

Community

Reducing Healthcare Cyber Risk Using a Cooperative SOAR-Enabled Healthcare Community H-SOC

K-3 and K-4

Healthcare remains the most exposed CI component and the most under-resourced. Many firms are recognizing the difficulties in keeping pace with the threats to their increasing attack surface (e.g., IoT medical devices, mobile and remote care delivery), meeting regulatory requirements, and finding/retaining qualified security personnel. However, traditional security third-party monitoring models fall short and aren't optimized to address the volume of alerts that require investigation. In addition, current approaches don't collectively share the granularity of data necessary to dramatically improve outcomes. As a result, a new, cooperative model is emerging in healthcare, which has been chartered by the State of Michigan and supported by Sequris Group. This session will provide an overview of this new model, highlight the differences from traditional MSS operations, and explain the critical role SOAR technology plays in delivering these services effectively and efficiently.

Presenter:

Eric Eder, Founder and President, Sequris Group

Ryan Winn, CISO and Director of IT, Munson Healthcare

John Jolly, President and CEO, Syncurity

Community

Tuesday, Oct 2

Addressing Both Sides of the Equation: Security Automation and Deception

K-5 and K-6

Security automation and intelligence sharing seek to speed the detection of and response to cyberattacks. Meanwhile, deception and moving-target defenses can slow the attacker by disrupting the attacker’s situational awareness. By addressing both sides of the equation—speeding the response and slowing the attack—we can narrow the gap between attackers’ time to compromise and our time to detect and respond. Security automation allows defenders to accelerate their observe–orient–decide–act (OODA) loop through continuous situational awareness and rapid response. Additionally, defenders can operate within the attacker’s OODA loop by using deception to disrupt the attacker’s situational awareness. This discussion will present the conceptual framework underlying research into the use of security automation and adaptive cyber defense in the financial services industry.

Presenter:

Donnie Wendt, Security Engineer, Mastercard

Operationalization

Shareable Workflows: Spreading and Adoption of Cyber Workflows through Reuse and Sharing throughout the Community

K-7 and K-8

Based on Sharable Workflow presentation and demonstration with CyberSponse. A complete life cycle of downloading a workflow, modifying it, exporting it, and importing into a Orchestration Tool will be discussed.

Presenters:

Paul Laskowski, Senior Systems Engineer, JHU/APL

Bharathram Krishnan, Solutions Architect, CyberSponse

Actionable Information Sharing

// Day 2 Breakout Session 3 Details

Session 3 10:00–11:00

Implementer Insights

Auditorium

An increasing number of organizations are exploring and integrating Security Automation & Orchestration (SA&O)/ Security Orchestration, Automation & Response (SOAR) strategies and platforms in cyber defense. During this panel, experienced organizations share SA&O, with information sharing, lessons learned, best practices, and recommendations.

Moderator:

Brett Waldman, IACD Adoption, JHU/APL

Panelists:

John Pescatore, Director of Emerging Security Trends, SANS Institute

Matt McFadden, Cyber Director, General Dynamics Information Technology

Matt Rodriguez, Cybersecurity Solutions Architect, Phoenix Cybersecurity

Lior Kolnik, Head of Security Research, Demisto

Piero DePaoli, Senior Director, Security & Risk, ServiceNow

Operationalization

Adversary Playbooks

K-3 and K-4

When your boss forwards you the latest intelligence report with an urgent flag set and the message reads: "What are we doing about this?" what do you say? To be confident in your answer, you need to understand how that adversary operates, or what's in their Playbook. In this session, we'll give you an in-depth report on OilRig, an adversary based in the Middle East that has launched a series of targeted attacks over the past 3 years. We'll show you how to analyze the threat to build a structured copy of their offensive plays, so you can better prepare your defensive line.

Presenter:

Mike Harbison, Unit 42 Threat Researcher, Palo Alto Networks

Actionable Information Sharing

Wednesday, Oct 3

Understanding Resiliency Effects on Adversary Behaviors

K-5 and K-6

This talk will explore the intersection of adversary tactics and techniques and defender resiliency effects to help defenders understand their resilience to attack within the context of the IACD observe–orient–decide–act (OODA) loop. This talk will leverage community knowledge from the NIST SP 800-160 Vol. 2 Cyber Resiliency Engineering Framework, the ODNI Cyber Threat Framework, and MITRE's ATT&CK to give concrete examples of resiliency techniques and approaches mapped to specific adversary objectives. We'll explore how defender resiliency effects on adversary behavior impact the defender's risk. We'll use the Cyber Effects Matrix to show defenders how to measure gaps, map response actions, and determine whether the desired effect on adversary behavior across the cyberattack life cycle has been achieved.

Presenter:

Shawn Riley, CDO and CISO, DarkLight Cyber

Operationalization

More Situational Awareness for ICS (MOSAICS), Functional Requirements Update

K-7 and K-8

This session will provide an overview of the DoD's MOSAICS concept demonstration with a focus on the functional requirements definition for the system. MOSAICS will leverage existing commercial technologies and, where applicable, developmental technologies from government laboratories and academia to address gaps in commercial offerings. Integration of these capabilities to automate key aspects of the Advanced Cyber ICS Tactics, Techniques, and Procedures (ACI TTP) will be the primary focus of this concept demonstration. This presentation will provide insights into the technical requirements for the MOSAICS system as decomposed from the ACI TTP and other sources.

Presenters:

Rich Scalco, Engineer, SPAWAR SYSCEN-ATLANTIC

Larry Cox, Engineer, USPACOM (AECOM)

Community

// Day 2 Breakout Session 4 Details

Session 4 1:00–2:00

Second Order Benefits of Open Integration

Auditorium

The evolution of the SOAR market has the potential to fundamentally change classic business models because of the open integration of products and services. If companies are opening up their APIs, what other support services and opportunities does this open to small/mid-sized business development approaches and integration approaches? Tools that used to be custom-developed for integration are now commercially available and supported. What is your organization's perspective on how a market of open integration changes for different business partners and operational activities?

Moderator:

Andy Speirs, Senior Information Security Executive, Booz Allen Hamilton

Panelists:

Christopher Carsey, Senior Solutions Engineer, CyberSponse

Cody Cornell, CEO and Cofounder, Swimlane

Vince Crisler, CEO and Cofounder, Dark^{3}

Matt McFadden, Cyber Director, General Dynamics Information Technology

Operationalization

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

K-3 and K-4

Security teams are overwhelmed and are increasingly becoming less effective. They're outnumbered and outgunned, and the problem isn't getting any better. But it doesn't have to be that way! Solving the problem and getting the upper hand against the bad guys isn't a question of how many more resources we need to add—it's a question of focusing what we already have on what really matters. Taking a modern approach to security means that we need to work smarter, not harder. This session will discuss a modern approach to security to help teams maximize the efficiency of their efforts to maximize their impact on the organization's risk.

Presenter:

Jeff Aboud, Director, Product Marketing, Kenna Security

Actionable Information Sharing

Experimenting with C2 Implementations

K-5 and K-6

FIT recently conducted a series of experiments comparing two different implementations of IACD C2 systems: The Systems Behavior Command and Control (SBC2) distributed C2 system based on the MIRA agent framework and a "conventional" C2 system using the Phantom orchestrator and apps connecting to sensors and actuators. The experiments were conducted on an emulated electrical smart grid testbed and focused on the identification and mitigation of attacks targeting the path from the smart meter to the utility data center. The experiments measured:

- Effectiveness – whether the C2 framework produces the desired result, and to what level of accuracy
- Efficiency – the computational resources (space, time, messages) required to compute the result
- Security – the level of security of the orchestration process throughout the communication events
- Usability – the degree of difficulty in the installation, deployment, and operation of the C2 system

Each of these measurements included several different experimental conditions that are reported, along with examples of the tests conducted.

Presenters:

Thomas Eskridge, Associate Professor, Florida Institute of Technology

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

Operationalization

Power of Communities for the Evolution of Security Capabilities

K-7 and K-8

In today's threat landscape, the only way to disrupt attackers and protect an organization is to unite systems and people, forming a collective defense. There are many opportunities for collaboration on shared goals, allowing security teams to stretch their resources further. This session will discuss the value in leveraging the power of community for the evolution of security capabilities.

Presenters:

Lior Kolnik, Head of Security Research, Demisto

Community

// Day 2 Breakout Session 5 Details

Session 5 2:15–3:15

Financial Sector Pilot Lessons Learned	Stop Chasing Indicators
Auditorium	K-3 and K-4
IACD and the FS ISAC have been partnering with Mastercard, Huntington National Bank, and Regions Bank for the last year on an integrated pilot for enhanced information sharing and decision support. This talk will present the initial results of that pilot. **Presenters:** Charlie Frick, IACD Financial Sector Liaison, JHU/APL Nam Le, IACD Integration Team Lead, Senior Systems Engineer, JHU/APL	Threat intelligence has grown out of a desire to better defend against known threats. Unfortunately, most threat intelligence today consists of a curated list of known malicious indicators. Using principles extracted from proactive threat-hunting methodologies, we propose a better way forward for threat intelligence. **Presenters:** Josh Day, Senior Threat Hunter, accenture Brad Rhodes, Senior Threat Hunter, accenture
Operationalization	Actionable Information Sharing

Wednesday, Oct 3

The Future of Collaborative Security

K-5 and K-6

Industry-wide, security teams are duplicating (and wasting) valuable time and resources to complete similar investigations, workflows, and threat responses. This is costly and unnecessary, especially when considering the ever-expanding threat landscape and global skilled staffing shortage. Imagine the alternative: Multiple organizations have investigation teams who agree to collaborate. One does an in-depth investigation, hunt, or mitigation and is able to share that process in real time with another organization. There are now multiple organizations and teams who are leveraging their skills and expertise to increase the efficacy of their collective SOCs. They are armed with the resources to prevent breaches and hunt for other threats while bolstering the security industry as a whole. Welcome to the future of collaborative security.

Presenters:

Cody Cornell, Cofounder and CEO, Swimlane

Pedro Haworth, Head of Technology, Security Innovation Alliance, McAfee

Operationalization

Engineering Principles for Developing Advanced Cybersecurity Automations

K-7 and K-8

Learn how adopting modular and decentralized design principles for automation scripts can help you keep up with the rapidly changing cyber landscape.

Creating cybersecurity automations that keep up with the rapidly changing cyber landscape is hard. You need to balance the desire to follow a proper development life cycle with the need for rapid turnaround. The solution is adopting modular and decentralized design principles for automation scripts.

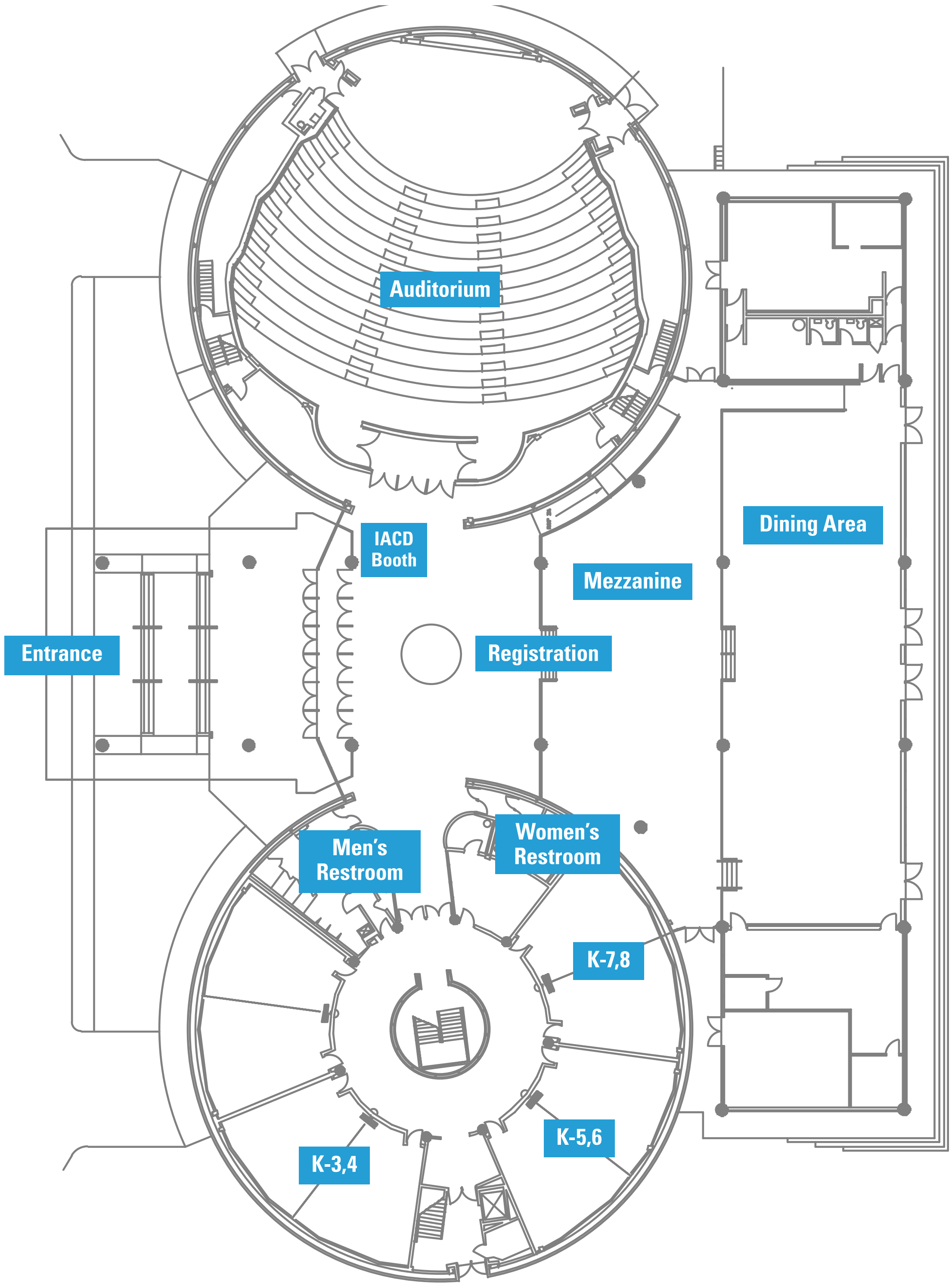
Presenters:

Matt Rodriguez, Cybersecurity Solutions Architect, Phoenix Cybersecurity

Tom Goetz, Senior Cybersecurity Engineer, Phoenix Cybersecurity

Operationalization

// Maps



1st Floor // Kossiakoff Center

// General Information

APL Guest Wi-Fi

Login: ICD

Password: IC2018

IACD Contacts

🌐	www.iacdautomate.org
✉	ICD@jhuapl.edu
Linkedin	https://www.linkedin.com/groups/8608114
▶ YouTube	goo.gl/5YiRAV
🐦	@IACD_automate

Material presented will be available on the IACD website.

Collaboration Space

Attendees are welcome to grab a seat at a table in the Mezzanine or Dining Area spaces to chat with each other.

Upcoming Integrated Cyber Events

Spring 2019 (dates to be announced)

September 4–5, 2019

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

https://www.iacdautomate.org