Integrated Cyber

May 2 and 3, 2019

Johns Hopkins University
Applied Physics Laboratory
Laurel, Maryland

The Evolution of Cyber Security Automation

// Welcome

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

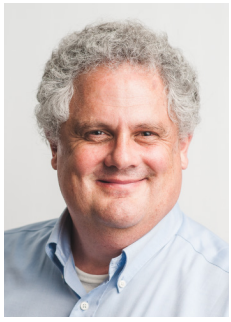
This event provides a forum for collaboration and technical exchange to support the adoption of integrated, automated cyber defense and information sharing. This day-and-a-half event showcases government, industry, operations, and critical infrastructure perspectives.

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

// Keynote Speaker Bios

Phil Reitinger, President and CEO, Global Cyber Alliance



Philip Reitinger has served as the President and CEO of the Global Cyber Alliance since December 2015. GCA is a nonprofit organization focused on eradicating cybersecurity risks—risk by risk. Formerly he filled senior cybersecurity roles at VisionSpear LLC, Sony, and Microsoft. In 2009 Mr. Reitinger was appointed as the Deputy Under Secretary for the National Protection and Programs Directorate at DHS. He also served as the first Executive Director of the DoD's Cyber Crime Center and as Deputy Chief of the Computer Crime and Intellectual Property Section at DOJ. Mr. Reitinger has been awarded the Secretary of Homeland Security's Distinguished Service Medal and the Attorney General's John Marshall Award.

Sue Gordon, Principal Deputy Director of National Intelligence

The Honorable Susan (Sue) M. Gordon was sworn in as the fifth Principal Deputy Director of National Intelligence (PDDNI) on August 7, 2017. As PDDNI, Ms. Gordon assists the DNI in leading the intelligence community (IC) and managing the ODNI. In particular, she focuses on advancing intelligence integration across the IC, expanding outreach and partnerships, and driving innovation across the community.

With nearly three decades of experience in the IC, Ms. Gordon has served in a variety of leadership roles spanning numerous intelligence organizations and disciplines. Most recently, Ms. Gordon served as the Deputy Director of the National Geospatial-Intelligence Agency (NGA) from 2015 to 2017. In this role, she helped the director lead the agency and manage the National System of Geospatial Intelligence. She drove NGA's transformation to meet the challenges of a 21st-century intelligence agency. She also championed agile governance, recruitment and retention of a diverse workforce, and expansion of geospatial intelligence services to the open marketplace. She is known for her commitment to diversity and inclusion and to the women and men of the IC.

Prior to her assignment with NGA, Ms. Gordon served for 27 years at the Central Intelligence Agency (CIA), rising to senior executive positions in each of the agency's four directorates: operations, analysis, science and technology, and support. She joined the CIA in 1980 as an analyst in the Office of Scientific and Weapons Research, and went on to serve as the Director of the Office of Advanced Analytic Tools, Director of Special Activities in the Directorate of Science and Technology, Director for Support, and ultimately in concurrent roles as Director of the Information Operations Center and the CIA Director's senior advisor on cyber. In 1998, she designed and drove the formation of In-Q-Tel, a private, nonprofit company whose primary purpose is to deliver innovative technology solutions for the agency and the IC. Ms. Gordon has been recognized for her creative executive leadership through numerous awards, including the Presidential Rank Award at the distinguished level.

Ms. Gordon holds a bachelor of science degree in zoology (biomechanics) from Duke University where she was the captain of the Duke Women's basketball team. She and her husband, Jim, live in Northern Virginia and have two adult children who have also chosen to serve their country.

George Barnes, Deputy Director, National Security Agency

Mr. George C. Barnes serves as the Deputy Director and senior civilian leader of the National Security Agency (NSA). In this capacity, he acts as the NSA's chief operating officer, responsible for guiding and directing operations, studies, and policy.

Having joined NSA in 1987, Mr. Barnes has held a number of critical technical and operational leadership roles throughout his career, including Deputy Chief of the SIGINT Development Strategy and Governance organization and Chief of Data Acquisition, NSA's SIGINT access, collection, and exploitation organization. Prior to his appointment as NSA's Deputy Director, Mr. Barnes held the position of NSA Director of the Workforce Support Activities Directorate where he was responsible for ensuring the effective operation and integration of enterprise-wide human capital management, education and training, security and counterintelligence, and installations and logistics.

Mr. Barnes is a certified cryptologic engineer with a bachelor of science in electrical engineering from the University of Maryland. His professional recognition has included the prestigious National Intelligence Medal of Achievement, a Meritorious Civilian Service Award, the NSA Ann Caracristi Award for Operations and Production Excellence, an Intelligence Community Leadership Collaboration Award, and Distinguished & Meritorious Executive Presidential Rank Awards.

// IC Community Groups

Our philosophy is simple: Do Something. Measure It.™

The Global Cyber Alliance (GCA) is an international, cross-sector effort dedicated to eradicating cyber risk and improving our connected world. We achieve our mission by:

- **Uniting Global Communities:** We must stand as a global community, across sectors and geography, if we are to effectively address cyber risks.
- **Implementing Concrete Solutions:** We build concrete solutions that reduce and eradicate cyber risk, and we make those solutions freely available for any organization or individual to use.
- **Measuring the Effect:** We believe in measuring effectiveness. We must measure to know we are doing the right things, and metrics drive action. We need to know what works and what does not.

https://www.globalcyberalliance.org/

The National Cyber Security Alliance (NCSA) builds strong public/private partnerships to create and implement broad-reaching education and awareness efforts to empower users at home, work and school with the information they need to keep themselves, their organizations, their systems and their sensitive information safe and secure online and encourage a culture of cybersecurity.

Vision: Realizing the full potential of our ever-evolving digital lives can only happen when a culture of cybersecurity and privacy is the foundation of:

- Free-flowing content
- Multiple methods and platforms for communication
- Trustworthy commerce
- Widely available and highly reliable connectivity

Mission: To educate and empower our global digital society to use the internet safely and securely.

Underlying Value: Securing our online lives is a shared responsibility.

https://staysafeonline.org

The Incident Response Consortium (IRC) is a non-profit, educational community, driven to change the landscape of today's lack of knowledge of incident response policies and procedures. The IRC is the First and Only Incident Response Community laser-focused on Incident Response, Security Operations and Remediation Processes concentrating on Best Practices, Playbooks, Runbooks and Product Connectors. In building the Community, the IRC is aimed to provide, design, share and contribute to the development of open source playbooks, runbooks and response plans for the industry community to use. These playbooks or recipes can be in the form of flowcharts, diagrams, sequences, scripts, orchestration platform playbooks, and product integration connectors. The collaborative community created by the IRC is driven to advance and address the ever-present and painful realities of today's cybersecurity industry.

Through its free-to-attend conferences, and freely accessible online resources available at http://www.IncidentResponse.com, the IRC is working to offer resources to everyone looking to further their knowledge and work toward more effective and efficient incident response. The IRC's next upcoming, free-to-attend event is its Incident Response Conference, "IR19," held September 4th and 5th, 2019 in the Washington, DC area at the Arlington Renaissance Capital View Hotel in Arlington, Virginia.

https://www.incidentresponse.com/

OASIS is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society.

OASIS promotes industry consensus and produces worldwide standards for security, Internet of Things, cloud computing, energy, content technologies, emergency management, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology.

OASIS members broadly represent the marketplace of public and private sector technology leaders, users and influencers. The consortium has more than 5,000 participants representing over 600 organizations and individual members in more than 65 countries.

OASIS is distinguished by its transparent governance and operating procedures. Members themselves set the OASIS technical agenda, using a lightweight process expressly designed to promote industry consensus and unite disparate efforts. Completed work is ratified by open ballot. Governance is accountable and unrestricted. Officers of both the OASIS Board of Directors and Technical Advisory Board are chosen by democratic election to serve two-year terms. Consortium leadership is based on individual merit and is not tied to financial contribution, corporate standing, or special appointment.

https://www.oasis-open.org//

Sector-based Information Sharing and Analysis Centers (ISACs) collaborate and coordinate with each other via the National Council of ISACs (NCI). Formed in 2003, the NCI today comprises 24 organizations designated by their sectors as their information sharing and operational arms.

The NCI is a true cross-sector partnership, providing a forum for sharing cyber and physical threats and mitigation strategies among ISACs and with government and private sector partners during both steady-state conditions and incidents requiring cross-sector response. Sharing and coordination is accomplished through daily and weekly calls between ISAC operations centers, daily reports, requests-for-information, monthly meetings, exercises, and other activities as situations require. The NCI also organizes its own drills and exercises and participates in national exercises.

Council members are present on the National Cybersecurity and Communications Integration Center (NCCIC) watch floor, and NCI representatives can embed with National Infrastructure Coordinating Center (NICC) during significant national incidents. The Council and individual members also collaborate with other agencies of the federal government, fusion centers, the State and Local Tribal Territorial Government Coordinating Council (SLTTGCC), the Regional Consortium Coordinating Council (RCCC), the Partnership for Critical Infrastructure Security (PCIS) – the Cross-Sector Council, and international partners.

The Council welcomes membership from organizations that have been designated by their sector leadership as their official forum for sharing threat information. Critical Infrastructure sectors and subsectors that have not yet established a method for sharing across their sectors are encouraged to contact the NCI to discuss how they can collaborate with the Council and participate in its activities.

https://www.nationalisacs.org/

// IC Community Groups

The IACI promotes information sharing through guidance, by assuring awareness of threats and providing management services supporting Government and Industry reduction of cyber risks. This coordinated development of partnerships allows all entities across the world the opportunity to become cyber resilient. IACI will continue to lead the way.

Under Executive Order (EO) 13691: Promoting Private Sector Information Sharing, the Secretary of Homeland Security was called on to strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs). ISAOs, like ISACs, are entities formed to share cyber threat information with its community of trust. However, whereas ISACs are sector based, ISAOs may be formed based on region, sector, subsector, or any affinity of interest. As part of the EO, DHS was to enter into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization (SO).

The International Association of Certified ISAOs (IACI) is a 501(c)6 non-profit with offices at Kennedy Space Center, Titusville, Florida, USA and Vienna, Austria. IACI was founded by the Defense Industrial Base Information Sharing and Analysis Center, Webster University, and the Global Institute for Cyber Security Research.

https://www.certifiedisao.org/

CIS® (Center for Internet Security, Inc.) is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.

The CIS Controls™ and CIS Benchmarks™ are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals.

Our CIS Hardened Images™ are virtual machine emulations preconfigured to provide secure, on-demand, and scalable computing environments in the cloud.

CIS is home to both the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC™), which supports the cybersecurity needs of U.S. State, Local and Territorial elections offices.

The CIS Vision:

Leading the global community to secure our connected world

The CIS Mission:

- Identify, develop, validate, promote, and sustain best practice solutions for cyber defense
- Build and lead communities to enable an environment of trust in cyberspace

https://www.cisecurity.org/

// A Huge Thank You to Our Sponsors!

// Upcoming Event

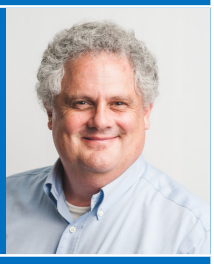
IACD and OASIS will deliver a three-day Borderless Cyber program October 8–10, 2019, in Washington, DC, addressing advances in automation and autonomous systems for network defense. Cyber threat intelligence experts and thought leaders from industry, government, and academia will share knowledge and experiences through a mixture of interactive panel discussions and presentations featuring proactive/reactive threat intelligence automation options, emerging exchange standards for automating cyber threat data, managing threats with AI and automation, and more. Debate and collaborate on strategies, tactics, and practices that accelerate the speed and scale of cyber defense. Thought leaders will also provide information on some of the new players in defense development and technology in waiting.

BC will be in parallel to CyberNext Summit 2019.
Registration and Call for Papers is open now.

https://www.kuppingercole.com/events/cns2019

BC BORDERLESS CYBER

// Agenda

Integrated Cyber Day 1 – Thursday, May 2	
8:00–8:45	Registration and Refreshments
8:45–9:00	Welcome
9:00–9:45	**Keynote** Phil Reitinger, Global Cyber Alliance 
9:45–10:30	**Integrated Cyber: The Evolution of IACD** Harley Parkes, JHU/APL
10:30–10:45	Break
10:45–11:45	Breakout Session 1
11:45–1:15	Lunch, with Community Networking
1:15–2:15	Breakout Session 2
2:15–2:30	Break
2:30–3:15	**Keynote** Sue Gordon, Principal Deputy Director of National Intelligence 
3:15–3:30	Break
3:30–4:30	Breakout Session 3
4:30–6:30	Networking Social/Community Speed Dating

Integrated Cyber Day 2 – Friday, May 3	
8:00–8:45	Registration and Refreshments
8:45–9:00	Welcome
9:00–9:45	**Keynote** George Barnes, Deputy Director, National Security Agency 
9:45–10:00	Break
10:00–11:00	Breakout Session 4
11:00–11:15	Break
11:15–12:15	Breakout Session 5
12:15–1:45	Networking Lunch with Community Members (free)

Please take advantage of our networking opportunities to visit the Community Groups (pages 4–6 of the program). The first 20 people to complete their Community Passport and return it to the registration desk will receive an IACD coffee mug.

You can visit the tables for the groups on the Mezzanine level throughout Integrated Cyber, but both lunches and the social will provide intentional opportunities to chat with them about how they are supporting the IACD tenets.

// Day 1 Breakout Session 1 Details

Session 1 10:45–11:45

Modern AI Expert Systems for Active Defense

Auditorium

This talk will focus on "knowledge engineering-derived AI" that is used to create an expert system for active defense. Whereas "data science-derived AI" focuses on how the data set is applied to tell us about the patterns in that data silo for prediction, classification, and clustering, knowledge engineering-derived AI expert systems focus on mimicking the abilities, knowledge, skills, and tasks of domain-specific human experts.

We'll also look at hard topics in artificial intelligence such as explainability, reproducibility, and use in zero-trust architectures to include how we're addressing these hard topics square on with knowledge engineering-derived AI expert systems.

Hear lessons learned from the front lines of an MSSP focused on adversary pursuit, Root9B, where they are using DarkLight, a modern expert system, as a differentiator in their automation strategy. This talk will interweave lessons learned by Root9B's operational testing and deployment.

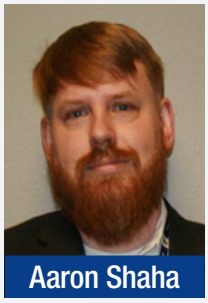
Presenters:

Shawn Riley, Chief Visionary Officer, DarkLight Cyber

Aaron Shaha, Director of Network Defense Operations (NDO) & Data Science , root9b

Michael Forgione, Network Defense Operator, root9b


Shawn Riley


Aaron Shaha


Michael Forgione

Future Innovations

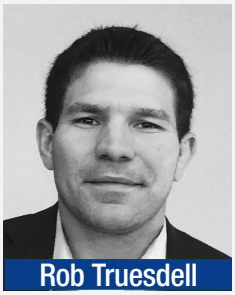
SOARing Across the Maturity Curve

K-3 and K-4

The SOAR market has grown significantly over the last 3 years, with organizations increasingly relying on automation in the SOC. Join this session to understand how organizations of varying levels of maturity are adopting SOAR, as well as hear a viewpoint on how this important technology may continue to evolve while driving efficiency and effectiveness in the SOC. We'll also share our assessment of 10 critical capabilities security teams must consider when optimizing their security workflows in the future.

Presenter:

Rob Truesdell, Director of Product Management, Automation and Orchestration, Splunk


Rob Truesdell

New Normal

Using Endpoint Security: Control Real Cyber Threats to IT/OT Convergent Infrastructure

K-5 and K-6

This session discusses the technical role and effectiveness of end-/any-point solutions, strategic use cases, telemetry/log/config contributions for context, and closing the loop early between DETECTION and REMEDIATION. Attendees can expect to address:

- Summary of IT/OT/IOT cyber threats, related scenarios, and defining concrete use cases for targeted risk and vulnerability management
- The anatomy of a solid end-point solution, including threat remediation and multimodal telemetry/log acquisition for context
- Assessing asset risk and behaviors and applying them to future end-point technologies
- Lessons learned when deploying OT first security solutions that enable linear convergence with IT-esque features

Presenter:

Ron Brash, Director of Cybersecurity Insights, Verve


Ron Brash

Advanced Applications

Shareable Workflows

K-7 and K-8

With an array of cyber Security Orchestration Automation and Response (SOAR) platforms available for IT organizations, there needs to be a common visual and data format that would share workflows across these tools. Sharable Workflows is that way. It utilizes the Business Process Model & Notation (BPMN) open standard to increase adoption of cyber SOAR platform tools by having repositories of workflows libraries. Additional benefits are secure repositories, sharing of workflows across the community, reduced time and financial capital to implement and maintain orchestration, and operational ease of transition between SOAR platforms.

Common Sharable Workflows allow greater adoption of SOAR platforms throughout the cyber community. BPMN Visual and Data XML-based format allows graphical representation of the workflow with multiple third-party editors (most free and interoperable) to revise, modify, and edit. Reference Sharable Workflows repositories can host libraries of reference workflow standards that can be used as-is or modified to suit the IT organization's policies and procedures. Workflows can be uploaded to repositories, then validated and verified, before being shared by the end user cyber community.


Paul Laskowski


Triton Pitassi

Presenters:

Paul Laskowski, Cyber Engineer, JHU/APL

Triton Pitassi, Software Engineer, JHU/APL

New Normal

// Day 1 Breakout Session 2 Details

Session 2 1:15–2:15

Stuck in the Upside Down: Crisis Management Automation @Netflix

Auditorium

The Netflix Security Incident and Response Team (SIRT) has grown out of the unique Netflix culture and technology stacks. As Netflix continues to grow its business and operations, SIRT continues to evolve to meet the needs. With the growth, we recognize the need to invest in automation and engineering to have more impact with the same resources. In the talk, we will show how the team automated the security incident response workflow using a SOAR solution. We will discuss how the investment decreased the cognitive load on the responder and enabled faster resolution times. The talk will highlight how we are enabling other teams within the organization to perform crisis management in their domains using the tooling and will also share our future automation roadmap. The goal is to grow our response capabilities through engineering efforts and new approaches as opposed to large multitiered SOCs with linear staffing requirements.

Presenter:

Swathi Joshi, Senior Technical Program Manager, Incident Response, Netflix

Swathi Joshi

New Normal

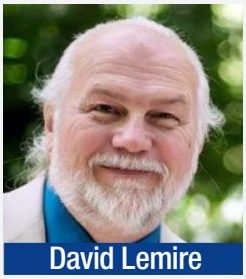
OpenC2 Integration Framework (OIF): A Reference Implementation for OpenC2

K-3 and K-4

Open Command and Control (OpenC2) is a concise and extensible language to enable machine-to-machine communications for purposes of command and control of cyber defense components, subsystems, and/or systems in a manner that is agnostic of the underlying products, technologies, transport mechanisms, or other aspects of the implementation. OpenC2 is being standardized under the auspices of OASIS. The OpenC2 Integration Framework is a prototype implementation demonstrating the creation and processing of OpenC2 Commands and Responses, and the use of multiple transfer protocols and serialization methods in transferring messages between OpenC2 Producers and Consumers.

Presenter:

David Lemire, Systems Engineer, Huntington Ingalls Industries



David Lemire

New Normal

Automate ATT&CK-Based Threat Intelligence to a Threat-Hunting Cycle

K-5 and K-6

The MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) framework has emerged as the most detailed and relevant knowledge repository for adversary techniques ever compiled. This session aims to demonstrate how we can mine threat intel data as well as build models of normal versus malicious behavior from a large malware sandbox data set, by using knowledge of these tactics and techniques. Furthermore we will demonstrate a systematic method to build a threat-hunting engine to operationalize such threat intelligence and models extracted from the sand box data set.

Presenter:

Kumar Saurabh, Founder, LogicHub


Kumar Saurabh

Advanced Applications

Best of Both Worlds—Machine Learning and Security Playbooks

K-7 and K-8

The power of machine learning to extract value from vast amounts of data is widely recognized in the industry. However, successfully integrating this powerful tool into security operations is not a trivial task.

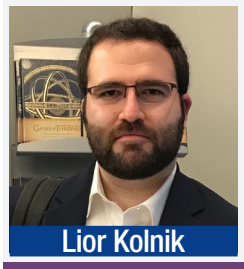
Meanwhile, security teams are shifting their approach to automation-first—aiming to increase efficiency and save valuable analyst time while reducing response time.

Some teams have adopted full SOAR platforms, while others have full automation teams maintaining their own systems and scripts in-house.

The question remains: How can we benefit from the power of machine learning while retaining our structured and powerful security playbooks built by experts?

In this talk we will give an overview of machine learning use cases for security operations and explore the relationship between machine learning and expert-built playbooks. We will review the limitations of machine learning in the context of orchestration and automation and how to successfully merge machine learning-based classifiers with the power of orchestration playbooks.

Finally, we will discuss the human's place in this solution and how these playbooks empower the security analyst and engage with multiple teams and stakeholders.


Lior Kolnik

Presenter:

Lior Kolnik, Head of Security Research, Demisto

Future Innovations

// Day 1 Breakout Session 3 Details

Session 3 3:30–4:30

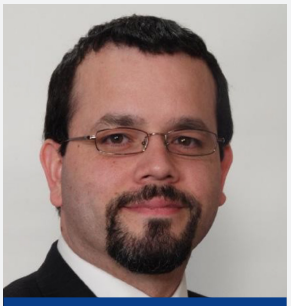
Symantec Integrated Cyber Defense eXchange (ICDX) and OpenC2 Implementation

Auditorium

This presentation will cover how Symantec went about implementing the OpenC2 language into Symantec Integrated Cyber Defense Exchange (ICDX) messaging bus. ICDX performs log collection of Symantec products and forwards to external log aggregation and orchestration platforms. The implementation will also show working examples of the OpenC2 inspired commands in ICDX.

Presenter:

Efrain Ortiz, Director, Office of the CTO, Symantec



Efrain Ortiz

New Normal

Brought Our Own Enterprise: Lessons Integrating the IACD Framework

K-3 and K-4

IACD strategies provide a strong reference framework for building cyber defense automation architectures. In practice, many technical and nontechnical challenges are uncovered. In this session, we will present our work establishing a threat response automation pipeline in a large-scale enterprise environment. Real-world implementation considerations include automated case management/change notification, orchestration in a heterogeneous landscape, and the inevitability of false positives. We will review architecture trade-offs, lessons learned, and recommendations for implementers considering a security automation pilot in their organization.

Presenters:

Michael Stair, Lead Member of Technical Staff, AT&T

Anthony Ramos, Lead – Technology Security, AT&T

Michael Stair

Anthony Ramos

New Normal

MOSAICS Spiral 0 Demo—MOre Situational Awareness for Industrial Control Systems

K-5 and K-6

MOSAICS leverages 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 demonstrate the early implementation of the IACD concepts into an industrial control system environment. This implementation represents the first step in the development of the MOSAICS concepts.

Presenter:

Harley Parkes, Director, IACD, JHU/APL

Harley Parkes

Advanced Applications

Embedded Contextual Analytics: Act on Data at the Point of Need

K-7 and K-8

Make analytics available where they are most useful. Embed real-time metrics and analysis tools into your end-user applications. Put contextual KPIs, visualizations, and analytics into your workflow development environment, into a human-in-the-loop decision step, into an auditor evaluation step, into a notification authoring step, and/or into many other end-user interfaces.

"*Data is only as valuable as your ability to act on it.*"
—Dalton Ruer (a.k.a., Qlik Dork)

This session will answer these questions: What are contextual analytics? Why embed contextual analytics into your end user applications? What are some examples of contextual analytics that would be useful in a cyber security application?

This session will show some example user interfaces that include contextual analytics, provide a brief summary of how to embed contextual analytics (technical) into your application, and discuss the build versus buy decision.

Presenter:

Michael Deane, Head of Contextual Analytics, Red Alpha

Michael Deane

Future Innovations

// Day 2 Breakout Session 4 Details

Session 4 10:00–11:00

Trust Panel

Auditorium

How do you identify and calibrate trust in automation? Studies of established pillars of safe and effective use of autonomous platforms have shown some hints. How will cloud and other future advances in cybersecurity impact trust?

Moderator:

Gill Brown, Human Systems Engineer, JHU/APL

Panelists:

Aubrey Merchant Dest, Federal CTO, Symantec

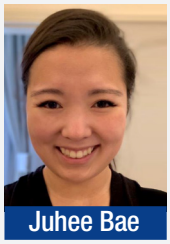
Juhee Bae, Product Manager, General Dynamics Mission Systems

Geoff Hancock, Chief Cybersecurity Executive, Advanced Cybersecurity Group

Jennifer Ockerman, Cognitive Systems Engineer, JHU/APL


Gill Brown


Aubrey Merchant Dest


Juhee Bae


Geoff Hancock


Jennifer Ockerman

Future Innovations

It's Not Just Play Books— Digging Deeper on Orchestration

K-3 and K-4

Providing musicians with sheet music that is arranged for their specific instrument results in the entire orchestra playing together in harmony. Delivering cybersecurity information should follow a similar approach. This talk will present different approaches to orchestrating, automating, and integrating both the technologies/security infrastructure and people/teams within companies that are too often siloed and disparate.

Companies are struggling to adopt new approaches, like the MITRE ATT&CK framework, which offers real-world knowledge of TTPs, detection, and mitigation. Orchestration has become as buzzy of a term as "cyber" itself, but it's no longer just the playbooks many think of. We will explore the concept of intel teams delivering their "product" to these desperate groups, and leveraging the work that the domain experts in each group performs to capture further context, thereby creating an intelligence refinement loop through machine to machine communication.

Presenter:

Ryan Trost, CTO and Co-Founder, ThreatQuotient


Ryan Trost

Advanced Applications

Making Sense of Unstructured Threat Data

K-5 and K-6

Over the last decade the cybersecurity community has made significant progress on collecting and aggregating intelligence that describes threat actors and campaigns, their tactics and techniques, and technical IOCs leveraged by them. However, tracking this intelligence as part of cybersecurity operations or applying it to analytical systems is difficult because it is generally unstructured. Knowledge bases like MITRE's ATT&CK are an excellent example of how useful intelligence can be once it is organized—getting to that end state is a huge challenge.

In this presentation we will show how recent advances in natural language processing (NLP) can help us organize this intelligence and add structure to make it actionable. We will demonstrate how to use Word2Vec: a shallow neural network that understands meanings and relationships between words and can therefore be used to organize the information these documents provide. This exercise trains a Word2Vec model on open-source intelligence and vulnerability reports such as EU-CERT and NIST and clusters them into "tactical and technical categories" that can be mapped to the MITRE ATT&CK framework.

Presenters:

Nicolas Kseib, Lead Data Scientist, TruSTAR Technology

Zainab Danish, Data Scientist, TruSTAR Technology


Nicolas Kseib


Zainab Danish

Advanced Applications

The Critical Role of Deception in Security Automation

K-7 and K-8

Deception has rapidly been adopted over the last couple of years as an enabler to accelerate detection and shrink dwell time. Today, security defenders utilize deception for its high-fidelity alerts via integration with SIEM systems, and just as important, playbooks, network, and EDR tools to react quickly to threats via automated and predefined response actions. As attacks become increasingly sophisticated and involve more automation, the defense must build and enable automated responses to counter new threats. This can only be accomplished through high-fidelity alerting systems with validated threat intelligence that directly integrate with existing security tools. During this session, we will discuss how deception systems are successfully countering advanced threats, including discussion about real-world use cases.

Presenters:

Tony Cole, Chief Technology Officer, Attivo Networks


Tony Cole

Advanced Applications

// Day 2 Breakout Session 5 Details

Session 5 11:15–12:15

The Evolution of Security Automation Technology and Its Future in the Modern Digital Enterprise

Auditorium

This moderated panel will explore the evolution and future of security automation as it continues to mature and become more widely adopted by modern digital enterprises. Topics covered will include applications of machine learning that accelerate positive security outcomes, the adoption and utility of risk-based decision models in the real world, the relevance of event-driven solutions for security automation to overarching modern digital transformation, and applicability of knowledge management to security automation's future.

Moderator:

JP Bourget, Founder and Chief Security Officer, Syncurity

Panelists:

Adam Vincent, CEO and Co-Founder, ThreatConnect

Bruce Potter, Chief Information Security Officer, Expel


JP Bourget


Adam Vincent


Bruce Potter

Future Innovations

Security Automation: Lessons Learned and the Path Forward

K-3 and K-4

In 2017, GuidePoint's managed services arm, vSOC, embarked on a large automation project to gain efficiencies for both infrastructure management and customer-facing security services. In this talk I will present some lessons learned from this journey, pitfalls and myths about automating operations, and our path moving forward. The audience will learn what tools and techniques worked as well as what failed miserably, and some tips for architecting security stack that will plug in seamlessly to their current infrastructure.

Presenter:

Patrick Orzechowski, Vice President, Research and Development, deepwatch


Patrick Orzechowski

New Normal

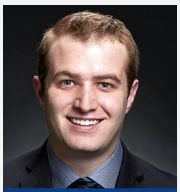
Beyond Indicators: Sharing Adversarial Behavior—An ATT&CK-Based Demo

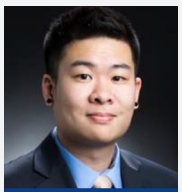
K-5 and K-6

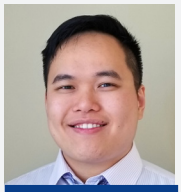
Cyber information sharing and response in the automation space revolves around indicators of compromise. This can be problematic because indicators can be changed by the adversary, leading to short shelf lives of usefulness. Additionally, TTPs (tactics, techniques, and procedures) being shared are often nebulous or not machine consumable. The IACD Integration Team has explored how parts of the industry share information and how adversary actions could be mapped to MITRE's ATT&CK framework to help facilitate automation. This session will include a proof-of-concept demonstration detailing a possible method to share adversarial behavior, including the accompanying concerns and challenges to take these slices of adversarial behavior to become the building blocks for machine-consumable TTPs.

Presenters:

Will Burger, Software Engineer, JHU/APL; Jason Mok, Cyber Engineer, JHU/APL; Keat Ly, Cyber Security Engineer, JHU/APL; Amar Paul, Software Engineer, JHU/APL


Will Burger


Jason Mok


Keat Ly


Amar Paul

Advanced Applications

Cybersecurity Data Science as a Process: Practitioner Insights and Best Practices

K-7 and K-8

Cybersecurity data science (CSDS) offers hope to organizations struggling with growing complexity, false positives, and data overload. CSDS brings to bear a range of methods to refine data into focused and effective alerts via analytical models. This presentation advocates a set of best practices derived from academic research, interviews with practitioners, and hands-on lessons from the field.

Lacking properly prepared data imbued with domain context, CSDS efforts flounder. The session aims to dig into areas where hype and failed projects have exposed gaps in CSDS efforts. A process-focused approach to integrated CSDS is framed.

The CSDS process encompasses data exploration to determine key features, preprocessing to impose structure, integrating distributed sources, deriving new measures, and establishing streamlined data pipelines. Model building and validation is thus situated in a larger frame. This presentation will be of interest to practitioners, experts, and planners alike.

Presenters:

Patrick Alcorn, Cybersecurity Data Scientist, SAS

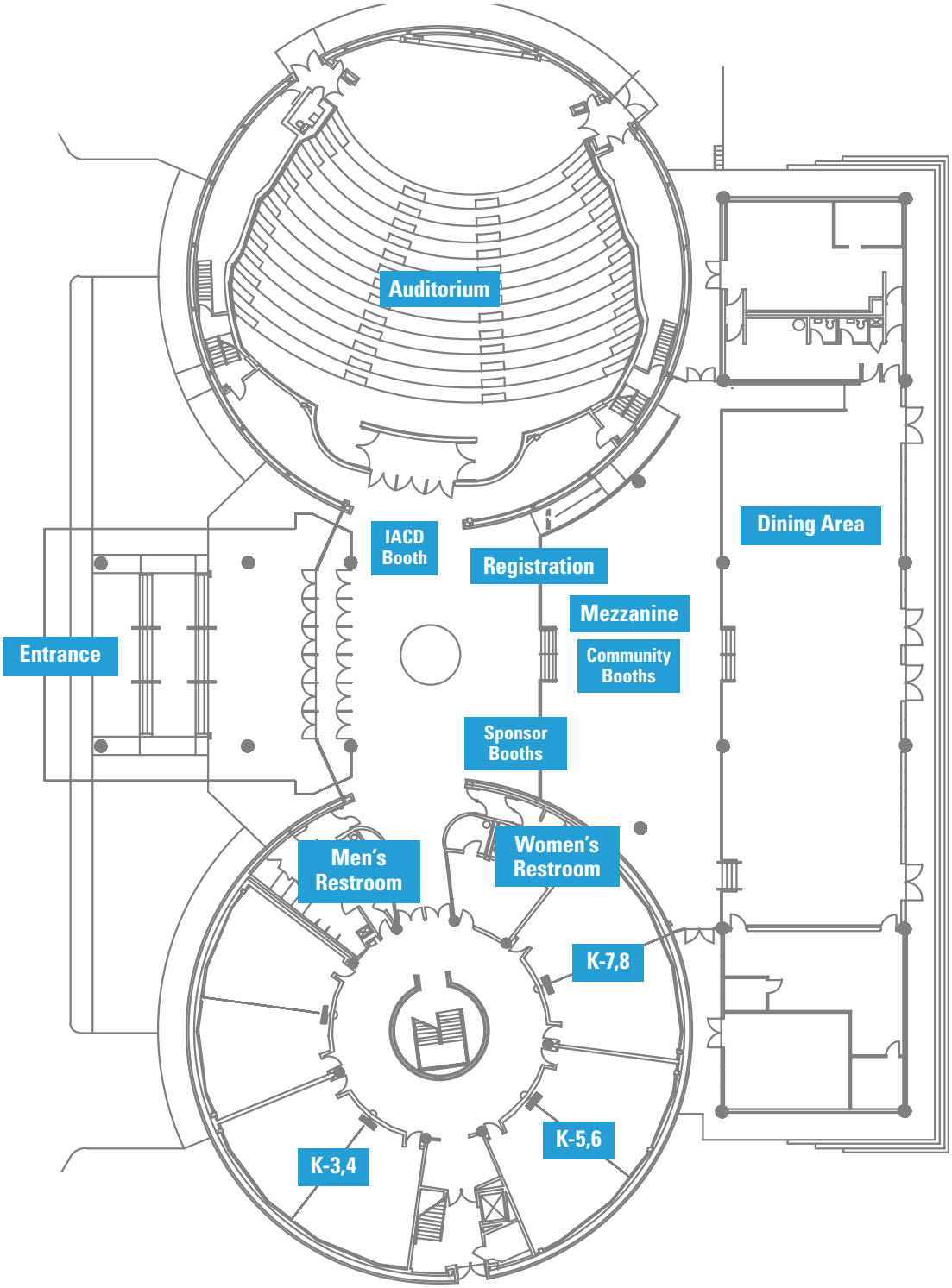
John Stultz, Analytic Platform Solutions Architect, SAS


Patrick Alcorn


John Stultz

Future Innovations

// Maps



1st Floor // Kossiakoff Center

// General Information

APL Guest Wi-Fi

Login: ICD

Password: IC2019

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.

Mothers Room

A mothers room is available in K-219, upstairs above the classrooms.

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

https://www.iacdautomate.org

FCC-6_19-01393