



# Program





---

## **HACK 2021: Everyone is a Link in the Chain of Security**

Hosted by the Office of the Chief Information Officer

**Tuesday, May 11, 2021 | Virtual Only**

[Visit the Virtual Exhibit Hall!](#) [Register for the Escape Room!](#)

---

<b>8:45am</b>	<b>Virtual Exhibits Open</b>
<b>9:00am</b>	<b>Welcome</b> <a href="#">Dave Nelson</a>   <a href="#">NRC</a>   <a href="#">Michael Mangefrida</a>   <a href="#">NRC</a>
<b>9:15am</b>	<b>CISA's Efforts to Help Strengthen Global Supply Chains</b> <a href="#">Noel Kyle</a>   <a href="#">Cybersecurity and Infrastructure Security Agency's (CISA)</a> <b>Zero Trust Security: Securing Federal Assets</b> <a href="#">Helen Patton</a>   <a href="#">Duo Security at Cisco</a>
<b>10:00am</b>	<b>Break</b> <a href="#">Virtual Exhibits Open</a>
<b>10:10am</b>	<b>Cybersecurity: The Nuclear Effect an Attack Can Have if You're Not Prepared</b> <a href="#">Meredith Griffanti</a>   <a href="#">FTI Consulting</a>   <a href="#">Kate Rosenthal</a>   <a href="#">FTI Consulting</a> <b>Securing the Software Supply Chain: Understanding How Secure Containers Can Make the Difference</b> <a href="#">Jeremy Valance</a>   <a href="#">Anchore</a>
<b>10:55am</b>	<b>Break</b> <a href="#">Virtual Exhibits Open</a>
<b>11:05am</b>	<b>BIG Cyber-Cyber Operations Response</b> <a href="#">Michael Jenks</a>   <a href="#">STAHL Channels</a>   <a href="#">Adapt Forward, LLC</a> <b>Identity Crimes, Data Breaches, &amp; Cyberattacks - How the convergence of these events resulted in the toughest privacy laws in the United States</b> <a href="#">James E. Lee</a>   <a href="#">Identity Theft Resource Center (ITRC)</a>
<b>11:50am</b>	<b>Break</b> <a href="#">Virtual Exhibits Open</a>
<b>12:00pm</b>	<b>Protecting Nuclear Regulatory Commission Device Security</b> <a href="#">John Loucaides</a>   <a href="#">Eclipsium</a> <b>NRC Panel Discussion: Linking Together NRC's Initiatives and Tools to Support Data Protection</b> <a href="#">An NRC Panel Discussion</a>   <a href="#">NRC Subject Matter Experts</a>
<b>12:30pm</b>	<b>Closing Remarks</b> <a href="#">Virtual Exhibits Open</a>
<b>12:35pm</b>	<b>Escape Room 1 and 2</b> <a href="#">Sponsored By: Capitol Technology University</a>



---

### **Michael Mangefrida, IT Specialist (INFOSEC), Nuclear Regulatory Commission**

Michael Mangefrida began as a contractor for the Office of the Chief Information Officer (OCIO) at the Nuclear Regulatory Commission in 1999. In May of 2004 he became an employee, tasked with managing, maintaining, and developing sensitive systems for the agency with the Office of Nuclear Security and Incident Response (NSIR). While with NSIR Mr. Mangefrida worked alongside other offices and regions to assist with sensitive system, provided support for Licensee cyber inspections, was a member of the NRC team liaising with foreign partners as part of the international Pentapartite Working Group where he served as Chair for the Information Security sub working group. Mr. Mangefrida joined the Computer Security Office (CSO) that would become part of OCIO to serve as the cybersecurity point-of-contact for a various systems and is the agency's liaison for the Federal Risk and Authorization Management Program. He is also the lead for the NRC's Cybersecurity Training and Awareness program that brings to the agency events such as Helpful Applied Cyber Knowledge (HACK), the Information System Security Officer Forum, and Lunch Bytes.

### **Noel Kyle, Supply Chain Risk Management Initiative Lead, National Risk Management Center, CISA**

Ms. Noel Kyle is the Supply Chain Risk Management Initiative Lead within the National Risk Management Center (NRMCC) at the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Ms. Kyle oversees a wide-ranging CISA-wide program intended to provide supply chain support and recommendations to partners and stakeholders across the federal government and private industry. Supply chain risk management, with a focus on Information Communications Technology (ICT), is a top CISA priority.

To help identify and address the risks presented by vulnerabilities within the supply chain, Ms. Kyle's team provides the program management support behind the ICT Supply Chain Risk Management Task Force, a collection of 40 industry and 20 United States Government members tackling key strategic questions in the supply chain risk management space.

### **Helen Patton, Advisory CISO, Duo Security at Cisco**

With more years working in the Security, Risk, Privacy and Resiliency professions than she cares to say, Helen Patton advocates using information risk, security and privacy to enable the mission of organizations and to support society at large. Helen is an Advisory CISO at Duo Security (now Cisco), where she shares security strategies with the security community. Previously she was the CISO at The Ohio State University where she was awarded the ISE North American Academic/Public Sector Executive of the Year, and an Executive Director at JPMorganChase. Helen actively encourages collaboration across and within industries, to enable better information security and privacy practices. She believes in improving diversity and inclusion in the workforce, and mentors people interested in pursuing careers in security, privacy, and risk management. Helen has a master's degree in Public Policy and has earned Certified Information Systems Auditor and Certified in Risk and Systems Control certifications from ISACA. She serves on the State of Ohio Cybersecurity Advisory Board and is a founding board member of the National Technology Security Coalition.

### **Meredith Griffanti, Managing Director, Strategic Communications, FTI Consulting**

Meredith Griffanti is a Managing Director in the Strategic Communications segment at FTI Consulting and is based in Washington, DC. She leads the firm's Cybersecurity & Data Privacy Communications practice and specializes in crisis and high-stakes litigation communications, with a focus on complex cybersecurity attacks and data privacy investigations. She provides counsel to clients on both cybersecurity preparedness and incident response matters involving PII, PHI, IP and other sensitive data across a wide range of industries. Meredith has worked on some of the most high-profile and highly sensitive data breaches around the world and has successfully navigated responses to complex incidents such as business email compromise, phishing and spear phishing, DDoS, credential stuffing, nation-state and major, double-extortion ransomware attacks. She was named a 2020 Person of the Year for Crisis Management by PR News and received a Cybersecurity Excellence Award for being the 2021 Cybersecurity PR Professional of the Year.



---

**Kate Rosenthal, Director, Strategic Communications, FTI Consulting**

Kate Rosenthal is a Director in the Strategic Communications segment at FTI Consulting and is based in New York. She is part of the firm's Crisis & Issues Management and Cybersecurity & Data Privacy Communications specialty practices, where she advises clients in both the private and public sector in preparing for, responding to, and recovering from threats to business continuity, license to operate, and reputation. Ms. Rosenthal has particular expertise navigating the risks and challenges associated with operational disruptions and safety threats, including cybersecurity incidents and ransomware attacks, threats to public health, security, and safety, supply chain and manufacturing disruptions, and the business impacts of technological and natural disasters.

**Michael Jenks, Chief Operating Officer, Adapt Forward, LLC**

Michael Jenks is a proven leader within the InfoSec space and Inc5000 entrepreneur. His career spans 22 years with 15 focused primarily on offensive and defensive cyber operations. Co-Founder of Adapt Forward, a cyber security services company, and Room40 Labs an enterprise security optimization software solution.

**James Lee, Chief Operating Officer (COO), Identity Theft Resource Center (ITRC)**

James E. Lee is the Chief Operating Officer of the ITRC. A data protection and technology veteran, James is the former EVP & Company Secretary of Irish application security company Waratek and former SVP & Chief Marketing Officer for Atlanta-based data pioneer ChoicePoint (now LexisNexis). He also chaired two working groups for the American National Standards Institute (ANSI) on identity management and privacy. Prior to joining ChoicePoint, James served as a global public affairs and communication executive at International Paper Company (NYSE: IP). He holds academic credentials from the University of Texas School of Information – Center for Identity, the Wharton School at the University of Pennsylvania, and the University of Arkansas.

**John Loucaides, VP of Research and Development, Eclypsium**

John Loucaides is the VP of Research and Development at Eclypsium, the comprehensive cloud-based device security platform that protects enterprise devices all the way down to the firmware and hardware level. Headquartered in Portland, Oregon, the company was named to Fast Company's annual list of the World's Most innovative Security Companies for 2020, the CNBC Upstart 100 list, and Gartner's Cool Vendor list for Security Operations and Threat Intelligence. John has extensive history in hardware and firmware threats from experience at Intel Corporation and the United States government. At Intel he served as the Director of Advanced Threat Research, Platform Armoring and Resiliency, PSIRT, and was a CHIPSEC maintainer. Prior to this, he was Technical Team Lead for Specialized Platforms for the federal government.





**Containers** are an easy way to package and deliver software

**BUT** also a potential source of security risks

# LEARN HOW TO PROTECT YOUR SOFTWARE SUPPLY CHAIN.

anchore

Shift Security Left  
for Cloud-Native  
Applications

Find out more at  
[www.anchore.com/shift-security-left](https://www.anchore.com/shift-security-left)



#### **Anchore**

Angela Siefkes  
Jeremy Valance  
(512) 786-7057  
angela.siefkes@anchore.com



#### Anchore's Website

*Anchore accelerates the development of secure and compliant cloud-native applications. Our suite of container security solutions seamlessly embeds in the DevOps lifecycle with continuous security and compliance checks early in the software development process. From sourcing to CI/CD pipelines to production, Anchore's solutions protect the software supply chain and prevent container security risks from reaching production. Using Anchore as part of the DevSecOps toolchain creates a reliable way to detect issues earlier, save developers time and lower the cost to fix vulnerabilities. Built with an open source foundation, Anchore solutions provide transparency into source code and the benefit of peer reviews.*

**Session Sponsor**

#### **Capitol Technology University**

Iris Lieberman  
11301 Springfield Road  
Laurel, MD 20708  
(301) 655-2119



ialieberman@captechu.edu

#### Capitol Technology University's Website

*The mission of Capitol Technology University, for almost 100 years, has been to educate individuals for professional opportunities in engineering, computer and information sciences, and business. We provide relevant learning experiences that lead to success in the evolving global community.*

**Escape Room Sponsor**



**SECURE YOUR**

**FUTURE IN TECH**

*Move your career forward.*



# Ready To **Decode** Your Cyber Career?



**Gain the skills you  
need to build a  
career in the  
cybersecurity  
industry**

Cybersecurity Youth Apprenticeship Initiative (CYAI) connects top talent youth aged 16-21 with employers and training providers in your region. Earn money as you complete a combination of job-related instruction and hands-on training.

**CYAI is completely free.**

Visit us at [CYAI2024.org](https://CYAI2024.org) for more information and to enroll today.

Pursuant to the National Apprenticeship Act, the Department of Labor works to expand opportunities related to apprenticeship programs. This project has been funded, either wholly or in part, with Federal funds from the Department of Labor, Employment & Training Administration under the contract number/work order DOL-OPS-16-A-0012/1605DC-18-F-00060. The contents of this publication do not necessarily reflect the views or policies of the Department of Labor, nor does mention of trade names, commercial products, or organizations imply endorsement of same by the U.S. Government.



@CYAI2024



@CYAI2024



[CYAI2024.org](https://CYAI2024.org)



[CYAI2024@icf.com](mailto:CYAI2024@icf.com)



## Cybersecurity Youth Apprenticeship Initiative (CYAI)

Ed Trumbull  
William.Trumbull@icf.com  
CYAI2024@icf.com  
[CYAI's Website](#)



*Cybersecurity Youth Apprenticeship Initiative (CYAI) is funded by the U.S. Department of Labor's (DOL) Employment and Training Administration (ETA) Office of Apprenticeship (OA). CYAI promotes sustainable development of cybersecurity apprenticeship programs for youth aged 16-21 and is administered by ICF. The goal of the initiative is to create at least 900 new cybersecurity apprenticeships for youth by 2024.*

**Event Supporter**

## Duo Security at Cisco

Ash Mathew | Lauren Dillon  
123 N Ashley St.  
Ann Arbor, MI  
(866) 760-4247  
[ash247@cisco.com](mailto:ash247@cisco.com) | [laudillo@cisco.com](mailto:laudillo@cisco.com)



### Duo Security at Cisco's Website

*Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo is a trusted partner to more than 25,000 customers globally, including Bird, Facebook, Lyft, University of Michigan, Yelp, Zillow and more. Try it for free at [duo.com](https://duo.com).*

**Session Sponsor**

TASKED WITH  
PLANNING A

**TRAINING EVENT,  
SYMPOSIUM,  
OR  
WORKSHOP**

FOR YOUR AGENCY?



## WE'RE YOUR ANSWER!

FBC is a professional organization providing meeting and conference support for the DoD, Intelligence Community, and Federal Civilian Agencies since 1976.

The Federal Business Council (FBC) has established a proven track record of excellence in coordinating military events. We are experienced in every level of program advisement and specialize in the unique needs that our military partners encounter. Work with FBC on your next event through GSA Schedule 47QRAA20D0014 and use the "No Cost Option" available to all DoD, Civilian, and Intelligence Agencies. Whether you are coordinating training for your company or leading a base wide specialty event, FBC can support your program with web design/ hosting, attendee registration, name badges and staff that will ensure that your event is a success.

To view a list of our  
current events,  
visit our website at  
**[www.fbcinc.com](http://www.fbcinc.com)**

For questions about contracting  
an event, please contact  
Dave Johnson at  
(800) 878-2940, ext. 209  
or [djohnson@fbcinc.com](mailto:djohnson@fbcinc.com)





# Protect Citizen Data With Strong MFA

Secure your agency to minimize risk  
and meet compliance.

**LEARN MORE ►**



#### **Eclypsium**

920 SW Sixth Avenue, Suite 375  
Portland, OR 97204  
info@eclypsium.com  
+1(833) FIRMSEC



#### Eclypsium's Website

*Eclypsium helps government agencies manage and defend their computing infrastructure with the only comprehensive device security platform that protects laptops, servers and networking gear down to the firmware and hardware level.*

**Session Sponsor**

#### **Illumio**

Mark Sincevich  
920 De Guigne Drive  
Sunnyvale, CA 94085  
(301) 908-8876  
mark.sincevich@illumio.com



#### Illumio's Website

*Illumio is a cybersecurity software company enabling end to end Zero Trust in DCOs. Illumio prevents attacker lateral movement by protecting critical applications, HVAs & workloads through real time application dependency mapping, coupled with host based micro segmentation. Illumio is FIPS 140 2 and NIAP Common Criteria Protection Profile Certified.*

**Marketing Sponsor**



## **End-to End Zero Trust Through Host-Based Micro-Segmentation**

Improve your cybersecurity posture and your mission

- Provide real-time visibility
- Reduces the dynamic attack surface
- Enables faster implementation
- Stops the lateral movement of malware

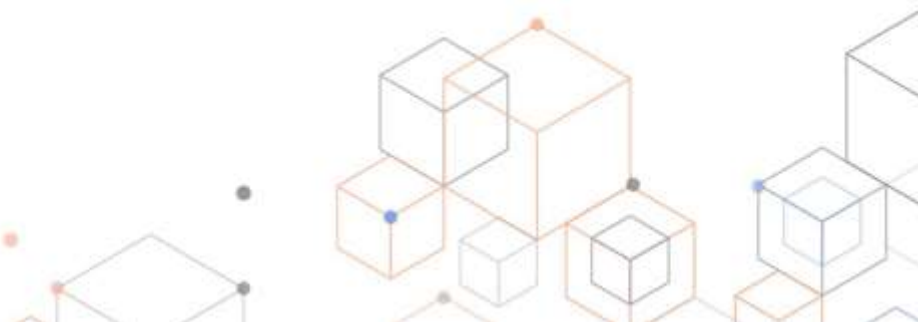


#### **PROTECTION PROFILE**

- NIAP Common Criteria, Protection Profile: Enterprise Security Management
- FIPS 140-2
- DHS CDM APL Phase 4
- Maps to NIST 800-207
- Maps to NIST 800-53

**SEE WHY ILLUMIO IS A LEADER IN  
THE FORRESTER ZERO TRUST WAVE**

[www.illumio.com/federal](http://www.illumio.com/federal)







# BIG Cyber - Cyber Operations Response

Customer Focused \* Mission Critical \* Performance Based

*"Our goal is to operationalize Executive Order 13800 'Strengthening the Cybersecurity Framework for Improving Critical Infrastructure' and the supporting 'Framework for Improving Critical Infrastructure Cybersecurity' by leveraging the MITRE ATT&CK® framework for the Nuclear Regulatory Commission"*

## Team Vista consists of two, expert companies:

**Vista Defense Technologies**, an Alaska Native Corporation (ANC), SBA Certified 8(a) Program Participant, a wholly owned subsidiary of Bristol Bay Native Corporation (BBNC), a **\$1.68 Billion** holding company with global interests across numerous economic sectors that include Information Assurance/Cyber Security, Data Science, Information Management, Technical Services, R&D and more. ISO 9001:2015; ISO/IEC 20000; ISO/IEC 27001:2013; ISO/IEC 27013:2015

### Solid Capabilities, Capital, and Commitment

Vista has access to **\$250M** in Reserve Capital specifically set-aside for contract start-ups!

**Adapt Forward**, a **Veteran Owned Small Business** founded in 2014. Adapt Forward's key leadership has performed Cyber Security for the Federal Government since 1998, specifically in support of the U.S. Department of Defense and Intelligence Community. They have **Unique expertise** building and certifying Computer Network Defense (CND) / Cybersecurity Service Provider (CSSP) and Cyber Red Team capabilities. Adapt Forward has **redefined how computer network defense is performed** throughout the DoD. By blending offensive and defensive skillsets, we have created a Purple Team hunt capability that results in a proven defensive security posture that continually enhances itself.

*"Former Employees of Vista and Adopt Forward are intertwined between the companies; the culture and performances are enhanced because of the Team's history and closeness."*

Team Vista has addressed cybersecurity customers who use disconnected point tools by consolidating and integrating the security tools they use, building security technology architectures (SOAPA), i.e., security operations and analytics platform architecture, that improve security efficiency and reduce operational overhead.



## Cybersecurity Results

2012 Cyber Red Team Assessment resulted in our evolution and maturity milestones:

- 2013 MITRE ATT&CK® framework introduced
- 2015 Cyber Red Team Assessment resulted in detection within an hour of initial compromise
- 2018 Cyber Red Team Assessment resulted in detection of the initial pivot attack point

### Key Benefits:

- \* Analysts: Detect Advanced Persistent Threat (APT) activity
- \* Analysts spend more time performing analysis threats, instead of gathering data
- \* Leverage integrated Incident workflows for expedited communication & response Focus on telemetry that matters
- \* Leadership: Better understand true risk posture Informed decisions on investments, rationalization, and procurement





## Resecurity, Inc.

Gene Yoo  
445 S. Figueroa Street, Suite 3100  
Los Angeles, CA 90071  
(888) 273-8276  
contact@resecurity.com

### Resecurity, Inc.'s Website

*Founded in 2016, Resecurity, Inc. has been globally recognized as one of the world's most innovative cybersecurity companies with the sole mission of protecting enterprises globally from evolving cyber threats through intelligence. Resecurity, Inc. has developed a global reputation for providing best of breed data-driven intelligence solutions.*

### Event Supporter

## SolarWinds

Miles Herbst  
7171 Southwest Parkway Boulevard, Suite 400  
Austin TX, 78735  
(703) 386-2670  
Miles.Herbst@solarwinds.com

### SolarWinds' Website

*SolarWinds® provides powerful and affordable IT management software to customers worldwide from enterprises of all sizes to virtually every civilian agency and branch of the US Military. We focus exclusively on IT Pros and strive to eliminate the complexity that they have been forced to accept. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use and maintain while providing the power to address any IT management problem.*

### Virtual Exhibitor

## STAHL Consulting Inc.

Charles Shillingburg  
Director, Business Development  
21010 S. Bankstreet, Suite 705  
Sterling, VA 20165  
(703) 558-9059  
charles.shillingburg@stahl-companies.com

### STAHL Consulting Inc.'s Website

### ***BIG Cyber-Cyber Operations Response***

*Learn how **Team Vista** has **redefined how computer network defense is performed** throughout the DoD. By blending offensive and defensive skillsets, **Team Vista** has created a Purple Team hunt capability that results in a proven defensive security posture that continually enhances itself. Team Vista's MITRE ATT&CK Framework:*

- *Presents a "kill chain" framework to guide targeted capability investments, measure effective coverage, overall effectiveness, and portfolio rationalization*
- *Informs decisions on Capability necessity, suitability, adequacy, priority, and identifies unnecessary overlaps*

***Team Vista** has performed cybersecurity for the Federal Government since **1998**, specifically in support of the U.S. Department of Defense and Intelligence Community. We have **unique expertise** in building and certifying Computer Network Defense (CND) / Cybersecurity Service Provider (CSSP) and Cyber Red Team capabilities.*

### Session Sponsor



This event has been professionally produced by the Federal Business Council.

For more information visit [www.fbcinc.com](http://www.fbcinc.com)



Federal Business Council

9800 Patuxent Woods Drive, Suite H

Columbia, MD 21046

Phone: (800) 878-2940

Website: [www.fbcinc.com](http://www.fbcinc.com)

E-mail: [sales@fbcinc.com](mailto:sales@fbcinc.com)

GSA Schedule #47QRAA20D0014



@FBCinc



@FederalBusinessCouncil



@FederalBusinessCouncil



@Federal-Business-Council