Sunday, April 30

3:00 p.m. – 5:00 p.m.

Registration Desk Open

Grand Ballroom Foyer, Second Floor

Session Type:

Delivery Format: Service Desk

Track:

Monday, May 1

7:30 a.m. – 8:00 a.m.

Continental Breakfast for Preconference Workshop Participants

Grand Ballroom Foyer, Second Floor

Session Type: Meal

Delivery Format: Meal

Track:

Join colleagues for a light breakfast and network informally.

Menu (subject to change):
Juices: Pineapple, Orange, Kombucha
Sliced Seasonal Fruit: Honeydew, Cantaloupe, Pineapple (Vn, GF, DF)
Whole Fruit: Bananas, Honeycrisp Apples, Seasonal Fruit (Vn, GF, DF)
House Baked Fresh Bakeries: Croissants, Banana Muffin with Macadamia Streusel, Seasonal Bakery (V, G, D, E, S, N)
Grains: Steel Cut Oatmeal with Brown Sugar, Honey, Toasted Almonds (N, V, DF, GF)
Infused Water: Orange-Mint
Fresh Coffee and Tazo Hot Tea

V-Vegetarian, Vn-Vegan, G-contains gluten, D-contains dairy, E-contains egg, S-contains soy, N-contains nuts
GF-gluten free, DF-dairy free

7:30 a.m. – 5:30 p.m.

Registration Desk Open

Grand Ballroom Foyer, Second Floor

Session Type: Service Desk

Delivery Format: Service Desk

Track:

For the most up-to-date information please use the EDUCAUSE Events mobile app.

8:00 a.m. – 11:30 a.m.

An Introduction to Cloud Security Assessments Using HECVAT (Separate Registration Is Required)

Grand Ballroom C, Second Floor

Session Type: Additional Fee Program

Delivery Format: Preconference Workshop

Track:

Charles Escue, *Information Security Manager, Indiana University*
Nick Lewis, *Program Manager, Security and Identity, Internet2*
Joshua Callahan, *Information Security Officer and CTO, Humboldt State University*

As more people join the higher education information security community or start new responsibilities around cloud security for SaaS services or cloud vendor risk management, they need an introduction to how to assess the security of SaaS cloud services. A key part of this assessment is HECVAT. This workshop will be an introduction to using HECVAT across your campus to manage risk around SaaS cloud services. We'll discuss tactical and strategic aspects to include in these efforts.

This year, we'll do breakouts based on institution size to help you work with the group to identify the next strategic and tactical steps for developing your cloud security assessments program, using HECVAT as a standard assessment tool in your campus process. We'll scale the discussion from one-person security offices to larger programs! We'll have an additional exercise focusing on choosing a specific area of cloud vendor risk management to improve on your campus. We'll ask for questions in advance of the workshop to frame the discussion.

Crafting Effective Tabletop Exercises (Separate Registration Is Required)

Cedar Ballroom, Second Floor

Session Type: Additional Fee Program

Delivery Format: Preconference Workshop

Track:

Stephen Safranek, *Chief Information Security Officer, West Chester University of Pennsylvania*

Join fellow higher education community members for a hands-on workshop to learn the basics of tabletop exercise (TTX) design and delivery. Participants will be exposed to general principals and best practices of TTX and will be given access to resources available to security professionals to help in the planning and delivery of their own campus exercises. Participants will also leave understanding how to capture data during an exercise and effectively implement remediations to the gaps discovered.

Join the Hunt: A Hands-on Approach to Cyber Threat Hunting (Separate Registration Is Required)

Grand Ballroom A, Second Floor

Session Type: Industry Led

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Delivery Format: Preconference Workshop

Track:

Keatron Evans, *Principal Cybersecurity Advisor, Infosec, part of Cengage Group*

For Institutional Attendees Only

Have you ever wondered what cyber threat hunting is actually like and how it's done? It's safe to assume that some security controls implemented in your institution have failed at least once, opening the door of your environment to a threat actor or group. Come learn what hypothesis-based, proactive threat hunting is all about and how eye-opening it can be. You'll experience a series of live demos and hands-on exercises of notoriously hard-to-detect adversarial behaviors like memory-only malware and living-off-the-land techniques. And you'll walk away with the essential skills and tools used to detect and mitigate adversarial behaviors. We look forward to active participant engagement in the workshop. This will be a fun hunt!

Who Should Attend

Any IT professional, developer, cybersecurity professional or technology professional interested in taking a test drive behind the wheel of tracking a threat/hacker in a live environment should attend. This session will spend the first 10 minutes with an overview of what threat hunting is and what it is not. The rest of the time will be 100 percent hands-on, detailed walkthroughs of tracking a threat. We will go from intro- to intermediate-level threat hunting, so cybersecurity practitioners who already have some knowledge but want to add some additional real-world, hands-on skills are encouraged to attend.

Prerequisites

Attendees should be familiar with Windows and Linux command line at a basic level (e.g., open command prompt and ping google.com). If you can do this or figure it out quickly, you meet the prerequisites. There will be a lab environment provided with already configured online virtual machines with incident response, forensics and threat-hunting tools. Just bring a laptop, and you'll be ready to go.

Note: All attendees will receive free access to the Infosec Skill cyber ranges needed for this exercise.

Learning Objectives

You will walk away with repeatable skills that you will likely be able to use in your environment immediately, whether in a complex enterprise network or at home. We will be using all open-source tools to make sure attendees can recreate the environment and exercises at home without spending money. **After attending this workshop, you will:**

1. Understand how to find threat actors once they've made it into your environment undetected.

2. Understand how to conduct proper network and memory forensics in a way unique to hunting for threats that typically go undetected.

3. Understand the procedures for developing a hypothesis based on industry threat intelligence and executing a hunt based on the same.

Instructor: *Keatron Evans, Principal Cybersecurity Advisor, Infosec Institute*

8:00 a.m. – 4:00 p.m.

Advanced System Security Plan Workshop (Separate Registration Is Required)

Regency Ballroom A-C, Second Floor

Session Type: Additional Fee Program

Delivery Format: Preconference Workshop

Track:

Damon Armour, *Director of Information Security, Risk & Assurance, North Carolina State University*

Laura Raderman, *Policy and Compliance Coordinator, Carnegie Mellon University*

Erik Deumens, *Director UF Research Computing, University of Florida*

Carolyn A. Ellis, *CMMC Program Manager, University of California San Diego*

Louis Daher, *Data Security Analyst, University of Michigan-Ann Arbor*

Jay Gallman, *Risk Advisor, Duke University*

One of the prevalent challenges faced by institutions engaged in regulated research is determining alignment of their interpretation of controls with those of other institutions engaged in similar activities. Given the sensitive nature of implementation decisions and the varied resources available to institutions, the primary means of addressing this challenge is traditionally through internal teams or external consulting efforts. However, when teams have been heavily involved in the development and implementation of a System Security Plan, they may inadvertently overlook crucial details or divulge excessive information in their solutions.

This advanced, full-day workshop will focus on the creation of a NIST 800-171 / CMMC Level 2 System Security Plan (SSP) through collaboration and expert input. Participants will learn whether their peers use similar implementation strategies, and they will contribute to building a framework for possible implementation strategies at a depth of information that can be generally shared. This workshop will produce a novel resource achieved from national security and compliance experts finding consensus of implementation strategies and determining best practices. Regulated Research Community of Practice (RRCoP) will provide scholarships as a sponsor. For more information: https://www.regulatedresearch.org/cppcworkshop23

Agenda: The full-day workshop will begin with the development of an enclave architecture in a collaborative setting, which will serve as the foundation for the rest of the day's activities. The morning will be dedicated to discussing implementation strategies for NIST SP 800-171 controls, with small-group consensus building and presentations for feedback from peers. In the afternoon, the focus will shift to addressing more challenging controls through small-group discussions and peer feedback. The workshop will conclude with a summary of the day's accomplishments and closing remarks.

Workshop Output: This workshop will create a portion of a SSP, developed through consensus with peer experts and documentation of a select group of controls. By focusing on the mechanics of key controls found in an 800-171 compliance SSP, institutions will have a reference document as they approach a CMMC assessment. All participants will have access to the newly created SSP and it will be available on www.regulatedresearch.org with the participants' attribution.

Participants: Participants are expected to have significant knowledge and experience with writing or owning an SSP or implementing NIST 800-171 / CMMC Level 2 controls. To improve diversity, participation from an institution will be limited, thus allowing participation from many institutions.

<u>**Schedule**</u>

Morning (3 hours)

- Introduction
- Scoping Exercise
- Controls in Small Groups
- Debrief & Discussion

Afternoon (3 hours)

- Complex controls in Small Groups
- Debrief & Discussion
- Closing & Actions to Continue

REN-ISAC 2023 Member Meeting: Blazing a Path to the Future (Registration limited to REN-ISAC members)

Regency Ballroom D-G, Second Floor

Session Type: Additional Fee Program

Delivery Format: Preconference Workshop

Track:

Charles Conner-Rondot, *Chief of Engagement REN-ISAC, Indiana University*
Susan Coleman Snyder, *Assessment Program Manager, Indiana University Bloomington*
Shane Albright, *Principal Security Engineer, REN-ISAC, Indiana University*

Registration for REN-ISAC Members Only

With a foundation of 20 years of helping members identify, analyze, and mitigate cyberthreats, the REN-ISAC is poised to launch an increasingly complex future partnership with current and new members. Join our first in-person meeting in several years to celebrate our 20th anniversary and look to the future. Network with REN-ISAC experts and fellow members, learn about enhanced membership services, get an update on our plans, hear from other members, and sit in on a very special session by Microsoft.

9:30 a.m. – 10:00 a.m.

Refreshment Break for Preconference Workshop Participants

Foyers, Second Floor

Session Type: Break

Delivery Format: Break

Track:

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Menu (subject to change):
Regular Coffee, Decaffeinated Coffee, Tazo Hot Tea
Assorted soft drinks
Chia Seed Pudding with Fresh Berries (GF, DF, Vn)
Fresh Mini Bakeries:
- Chocolate Croissants (G, D, E, V)
- Assorted Mini Danishes (G, D, E, N, V)
- House Made Orange Doughnut (G, D, E, V)

Whole Seasonal Fruits
V-Vegetarian, Vn-Vegan, G-contains gluten, D-contains dairy, E-contains egg, S-contains soy, N-contains nuts
GF-gluten free, DF-dairy free

11:30 a.m. – 12:30 p.m.

Lunch for Preconference Workshop Participants

Grand Ballroom E-K, Second Floor

Session Type: Meal

Delivery Format: Meal

Track:

Lunch is provided for all preconference workshop attendees. *Lunch ticket is required.*

Menu (subject to change):
Vegetable Barley Soup (GF, DF, Vn)
Frisee And Romaine, Roasted Summer Squash, Shaved Radish, Fresh Blackberries, Toasted Walnuts And White Balsamic Vinaigrette (N, Vn, DF, GF)
Baby Mizuna Greens, Roasted Pears, Grape Tomatoes. Shaved Beecher's Cheese. Candied Hazelnuts And Orange-Tarragon Vinaigrette (GF, D, N)
Voodoo Spice Marinade Steelhead, With Charred Oranges (GF, DF)
Grilled Flank Steak, Fried Pearl Onion Relish With Demi (GF, DF)
Charred Green Zucchini, Yellow Peppers And Baby Spinach (Vn)
Wild Rice Pilaf With Dried Apricots And Chopped Herbs (Vn, GF, DF)
Mini Key Lime Pie With Meringue (D, G, E)
White Chocolate Mousse With Sea Salt Caramel Sauce (GF, D, E)
Fresh Coffee and Tazo Tea
Iced Tea

V-Vegetarian, Vn-Vegan, G-contains gluten, D-contains dairy, E-contains egg, S-contains soy, N-contains nuts
GF-gluten free, DF-dairy free

12:30 p.m. – 4:00 p.m.

Advanced Cloud Security Assessments on Campuses (Separate Registration Is Required)

Grand Ballroom C, Second Floor

Session Type: Additional Fee Program

Delivery Format: Preconference Workshop

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Track:

Nick Lewis, *Program Manager, Security and Identity, Internet2*
Joshua Callahan, *Information Security Officer and CTO, Humboldt State University*
Charles Escue, *Information Security Manager, Indiana University*

You've figured out how to use HECVAT through trial and error. You're already using HECVAT 3.0. What next? Where do you need to drive your campus to more effectively manage cloud security assessments or cloud vendor risk management for SaaS services across your campus? What do you need to do to scale your usage of HECVAT to assess every cloud service on your campus? We'll address these questions during the workshop.

This year, we'll do breakouts based on institution size to help you work with the group to identify the next strategic and tactical steps for your campus processes. We'll scale the discussion from one-person security offices to larger programs! We'll have an additional exercise focusing on choosing a specific area of cloud vendor risk management to improve on your campus. We'll also have sufficient time to get into the details and decision support in HECVAT. We'll ask for questions in advance of the workshop to frame the discussion.

Attack Surface Management for Higher Education Institutions on a Budget (Separate Registration Is Required)

Cedar Ballroom, Second Floor

Session Type: Additional Fee Program

Delivery Format: Preconference Workshop

Track:

Kevin Shivers, *Deputy Chief Information Security Officer, University of Maryland*
Brian Markham, *Chief Information Security Officer, EAB*

Institutions of higher education have the biggest, most unusual attack surfaces and generally lack the resources to buy expensive commercial ASM tools. Having managed very large attack surfaces ourselves, we've experienced this firsthand. What institutions lack in budget can be made up for with creativity and DIY elbow grease. In this half-day workshop, we'll cover building out an attack surface management program at your university and identify vulnerable assets before bad guys can take advantage of them.

Cisco SAFE: Risk Assessment Security Workshop (Separate Registration Is Required)

Grand Ballroom A, Second Floor

Session Type: Industry Led

Delivery Format: Preconference Workshop

Track:

William Clay, B, *Technical Security Architect, Cisco Systems, Inc.*

For Institutional Attendees Only

For the most up-to-date information please use the EDUCAUSE Events mobile app.

In this session, you will first learn about common risk assessment techniques and the value they bring to teams planning security architectures. Second, you will be guided through a qualitative risk assessment and a vendor-agnostic security control gap analysis. You will have the opportunity to gain familiarity with the report that is generated using new Cisco security design tools made available during these live sessions. This report provides two outputs: a security project roadmap prioritized by risk mitigation and a visualization of critical flows and their alignment to Cisco validated security architectures. After this session, you will be able to articulate the value of security within your organization and make informed design decisions by aligning security investment to risk.

2:00 p.m. – 2:30 p.m.

Refreshment Break for Preconference Workshop Participants

Foyers, Second Floor

Session Type: Break

Delivery Format: Break

Track:

Menu (subject to change):
Regular Coffee, Decaffeinated Coffee, Tazo Hot Tea
Assorted soft drinks
Home Style Cookies:
- Double Chocolate (G, D, E, S, V)
- Lemon Crinkle (G, D, E, S, V)
- Fruity Pebble (G, D, E, V)
- Chocolate Chip, Marshmallow, Corn Flakes (G, D, E, V)
- French Macarons (D, E, S, V, N)
Blue Corn Tortilla Chips, Warm Artichoke and Spinach Dip (D, V, GF)
Whole Seasonal Fruits

V-Vegetarian, Vn-Vegan, G-contains gluten, D-contains dairy, E-contains egg, S-contains soy, N-contains nuts
GF-gluten free, DF-dairy free

3:00 p.m. – 4:00 p.m.

Higher Education Information Security Council (HEISC) Advisory Committee Meeting (by invitation only)

Larch, Third Floor

Session Type:

Delivery Format: Meeting

Track:

4:45 p.m. – 5:15 p.m.

Cybersecurity and Privacy Community Welcome

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Regency Ballroom A-C, Second Floor

Session Type:

Delivery Format: Meeting

Track:

Join us for a welcome networking event, where you can meet other attendees, learn about EDUCAUSE Community Groups, and other ways to get involved after the conference.

5:30 p.m. – 6:45 p.m.

Happy Hour Meet-Up Reception

Grand Ballroom A, Second Floor

Session Type: Industry Led

Delivery Format: Industry Led

Track:

Tuesday, May 2

7:15 a.m. – 8:00 a.m.

Continental Breakfast - Sponsored by Fortinet

Regency Ballroom Foyer, Second Floor

Session Type: Meal

Delivery Format: Meal

Track:

Join colleagues for a light breakfast and network informally.

[Click here](#) *for a message from Fortinet, the sponsor of this function.*

Menu (subject to change):
Juices: Grapefruit, Orange, Carrot
Sliced Seasonal Fruit: Honeydew, Pineapple, Watermelon (Vn, GF, DF)
Whole Fruit: Bananas, Valencia Oranges, Seasonal Fruit (Vn, GF, DF)
House Baked Fresh Bakeries: Croissants, Strawberry with White Chocolate Chip Muffin, Assorted Mini Danish (V, G, D, E)
Grains: Buckwheat Porridge –Toasted Coconut Flakes, Cinnamon, Vanilla, Maple Syrup, Almond Milk (Vn, GF, DF, N)
Infused Water: Lemon-Basil
Breakfast Burrito: Cage Free Eggs, Italian Sausage, Pepper Jack Cheese, Pepper & Onions, Salsa, Sour Cream
Fresh Coffee and Tazo Hot Tea Selection

V-Vegetarian, Vn-Vegan, G-contains gluten, D-contains dairy, E-contains egg, S-contains soy, N-contains nuts
GF-gluten free, DF-dairy free

For the most up-to-date information please use the EDUCAUSE Events mobile app.

7:15 a.m. – 5:00 p.m.

Registration Desk Open

Grand Ballroom Foyer, Second Floor

Session Type: Service Desk

Delivery Format: Service Desk

Track:

8:00 a.m. – 9:00 a.m.

Opening General Session

Grand Ballroom E-K, Second Floor

Session Type: General Session

Delivery Format: General Session

Track:

Join us as we kick off the Cybersecurity and Privacy Professionals Conference with opening general session speaker, Melissa Agnes. Creator of the Crisis Ready Model and author of *Crisis Ready: Building an Invincible Brand in an Uncertain World*, Melissa Agnes is a recognized leading authority on crisis preparedness, reputation management, and brand protection. Agnes is a coveted speaker, commentator, and advisor to some of today's leading organizations faced with the greatest risks.

[Click here](#) for a message from Cisco Secure, Platinum Partner, the sponsor of this session.

9:00 a.m. – 6:00 p.m.

Corporate Displays

Grand Ballroom Foyer, Second Floor

Session Type: Industry Led

Delivery Format: Industry Led

Track:

Companies will be showcasing security technology solutions for higher education with dedicated visiting time scheduled during the morning and afternoon breaks. Stop by to learn more about their solutions and interact with company representatives.

Armis

Armis is the global leader in cyber asset security. Organizations trust our real-time, comprehensive asset visibility and intelligence platform for automated enforcement across every connected asset and environment? IT, cloud, IoT, IoMT, OT,

For the most up-to-date information please use the EDUCAUSE Events mobile app.

BYOD, and edge. Armis helps organizations across any industry continuously secure their entire cyber-asset attack surface.

Bravura Security

Bravura Security is an analyst-recognized industry leader delivering best-in-class identity, privileged access, password, and password-less solutions with the power of one platform. Over the last two decades, Bravura Security has helped higher education institutions protect their organizations against increasing cybersecurity threats.

CampusGuard

Founded in 2009, CampusGuard provides cybersecurity and compliance services for campus and community-based organizations, including higher education, health care, state and local government and agencies, financial services firms, and SaaS/tech companies, among others. CampusGuard's success in serving their customers can be attributed to the experience, education, and commitment of their certified professionals and their in-depth understanding of the unique needs of the markets they serve. For more information, visit *www.campusguard.com*.

Cisco Secure, Platinum Partner

Cisco Secure drives security resilience, enabling organizations to protect the integrity of their business amidst unpredictable threats or change and emerge stronger. With the Cisco Security Cloud, organizations see across the multi-cloud environments, anticipate what's next, take the right action, close security gaps, and get better every day to support the success of institutional-wide resilience investments.

Cloudflare

Cloudflare is the security, performance, and reliability company on a mission to help build a better internet. Today, it runs one of the world's largest networks that powers anything connected to the internet. Its services are used by everyone from educational institutions to Global 2000 companies and top government organizations.

Fortinet

Fortinet makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing devices, data, applications, and connections from the data center to the cloud.

Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures.

Imperva

Imperva is the comprehensive digital security leader on a mission to help organizations protect their data and all paths to it. Customers around the world trust Imperva's integrated approach combining edge, application, and data security to protect their applications, data, and websites from cyberattacks.

Infosec, part of Cengage Group

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at *infosecinstitute.com*.

Indiana University OmniSOC

For the most up-to-date information please use the EDUCAUSE Events mobile app.

OmniSOC is the shared security operations center for higher education and research. OmniSOC rapidly delivers only critical, actionable, high-quality alerts 24/7, allowing cybersecurity staff to focus on what's important—at substantial cost savings—from a trusted leader in the higher education cybersecurity community and supported by the formidable capabilities of Indiana University's GlobalNOC.

Microsoft Corporation, Platinum Partner

Reimagined for a new era of digital learning, Microsoft Education helps to unlock student potential with powerful tools to learn, collaborate, and create all in a secure and trusted environment. The solution also promotes diversity and inclusion with a commitment to expand accessibility for all, and to bridge the gap in education by providing access to technology for those around the world with disabilities.

Moran Technology Consulting, Gold Partner

At Moran Technology Consulting, we enable our clients to build mature identity and access management (IAM) programs and identity-focused cybersecurity solutions that have transformational impact on digital experience, DEI initiatives, and institutional risk management. Our expert consultants perform assessments, strategic planning, roadmaps, platform evaluations, and solution design and implementations.

Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. We're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

Rapid7

Rapid7's industry-leading security solutions and strategic expertise empower you to stay ahead of attackers, ahead of the competition, and future-ready for what's next.

Salty Cloud

Isora GRC from SaltyCloud is the Lightweight Governance, Risk, and Compliance (GRC) Assessment Platform that helps teams unlock new dimensions of risk for more efficient mitigation, improved regulatory compliance, and robust resilience without the hassle of legacy solutions. Ready to build a GRC program you can trust?

SANS Institute

Launched in 1989 as a cooperative for information security thought leadership, the SANS mission is to empower cybersecurity professionals with the practical skills and knowledge they need to make our world a safer place. Visit our display and learn more about our SANS training products and educational institution discount programs.

SecureW2

SecureW2 helps universities deploy password-less security via digital certificates to provide more secure Wi-Fi and application access. Improve connection experience to networks with fewer disconnects and faster Wi-Fi roaming. Talk to us about how you can leverage certificates to securely connect users to on-prem and cloud apps without MFA fatigue.

SecurityZones

SecurityZones is a commercial partner and distributor of Spamhaus Technologies. Spamhaus is the trusted authority on IP and domain reputation, providing industry-leading, real-time datasets to safeguard against malware, phishing, botnets, spam, and more. With 25 years of experience, Spamhaus not only protects, but provides insight, across networks and email worldwide.

Splunk

Splunk helps make organizations more resilient. Leading organizations use our unified security and observability platform to keep their digital systems secure and reliable. Organizations trust Splunk to prevent security, infrastructure, and application issues from becoming major incidents; absorb shocks from digital disruptions; and accelerate transformation.

Yakabod

Built for higher education, Yakabod Cyber Incident Manager (CISOBox) delivers efficient, secure, automated incident handling through intelligence agency technology. Universities use CISOBox to isolate and secure sensitive incident data, documentation, and communication; generate critical metrics/reports for leadership; and gain NIST 800-61r2 compliance. Integrated with ServiceNow, Active Directory, Teams, Slack, and more.

Zscaler

Zscaler accelerates digital transformation so that customers can be more agile and secure. The Zscaler Zero Trust Exchange, a SASE-based platform, is the world's largest inline cloud security platform, protecting thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications over any network.

9:15 a.m. – 10:00 a.m.

Designing and Replicating Controlled Unclassified Information (CUI) Training That Was Due Yesterday!

Grand Ballroom BC, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

Kira Dunn, *Senior Risk and Compliance Analyst, University of California San Diego*
Lillian Maestas, *Project Manager, University of California San Diego*

Imagine discovering that your staff requires training to meet an urgent compliance deadline, but the training does not yet exist! Learn how one organization rose to the challenge and follow their demanding journey to craft training to meet looming deadlines while providing accessibility, tracking, and transparency. When funding is a challenge, hiring outside training consultants and voice talent may not be feasible; look within your organization for utility and talent. If no dedicated team exists, consider leveraging your internal staff! Avoid "reinventing the wheel" by researching and gathering information from established, trusted sources on the web. The organization in focus was required to adhere closely to Department of Defense (DoD) regulatory standards, but your requirements may be less stringent. Take lessons from one organization's struggle and increase the chances of a smoother path for yours!

Let's Talk! NSPM-33 Research Security Compliance Programs

Regency Ballroom D-G, Second Floor

Session Type: Breakout Session

Delivery Format: Facilitated Discussion

Track: Risk, Compliance, and Policy

Carolyn A. Ellis, *CMMC Program Manager, University of California San Diego*
Joanna Lyn Grama, *Vice President, Vantage Technology Consulting Group*

For the most up-to-date information please use the EDUCAUSE Events mobile app.

There's a new research data protection initiative on the block. Unlike previous initiatives targeting specialized sensitive research, National Security Presidential Memorandum 33 (NSPM-33) addresses any federally funded U.S. research and development activity, even fundamental research. NSPM-33 will soon require many research institutions to establish and operate a research security program. In this facilitated discussion, you'll collaborate with peers and share ideas on how to implement your NSPM-33 research security compliance program. We'll work through individual NSPM-33 controls in small groups to understand implementation approaches. At the end of the session, we will hold a large group discussion to discuss differing approaches and build an institutional "next steps" action list.

PrivSec: The New Frontier

Grand Ballroom A, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Privacy

Michael Tran Duff, *Chief Information Security and Data Privacy Officer (CISDPO), Harvard University*

At Harvard University, we're taking the progressive approach of fully integrating privacy and infosec into a single program that we're calling "PrivSec." We'll discuss our rationale for combining the two and our strategy for the program. Our PrivSec journey is just beginning. Is this grand experiment destined to fail, or will it become the new standard?

Second-Semester Security Professionals

Regency Ballroom A-C, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Technologies and Operations

Robert Wilson, *Director of Security Operations and IR, University of South Carolina*
Alexander Galloway, *Security Engineer, University of South Carolina*

At the University of South Carolina, we've undertaken a multiyear project to include students in all aspects of our security services. In this talk, we'll cover how we're using technology to rapidly teach concepts to students, get them working on real-world alerting in their first week, and raise the bar for what's possible as a "tier one" analyst in a Security Operations Center. We'll touch on developing SOAR processes to act as a technical mentor through enrichment, measuring where you need to measure, and teaching people how to think as analysts.

Widening the Net: Innovative Ideas for Hiring Diverse and Successful Teams

Cedar Ballroom, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Leadership and Professional Development

JoAnna Parker Martin, *Security Analyst, Rice University*

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Learn how Rice University has implemented out-of-the box ways to improve on the hiring challenges within our industry. Topics presented will include not only a primer on how to implement an apprenticeship program but other strategies and ways of thinking about hiring that can help you bridge your team's gaps. This will also include discussion of how hiring for diversity improves team success.

10:00 a.m. – 10:45 a.m.

Refreshment Break and Corporate Displays

Grand Ballroom Foyer, Second Floor

Session Type: Break

Delivery Format: Break

Track:

Menu (subject to change):
Regular Coffee, Decaffeinated Coffee, Tazo Hot Tea
Assorted soft drinks
Yogurt Parfaits:
- Zoi Honey Greek Yogurt (D, V)
- House-Made Seasonal Fruit Compote (Vn, GF, DF)
- House-Made Granola (G, N, V)
Sweet & Savory Muffins (D, G, E, S):
- Blueberry
- Chocolate Chi
- Lemon Poppyseed
- Jalapeno and Cheddar Cheese
- Bacon & Cheese
Whole Seasonal Fruits
V-Vegetarian, Vn-Vegan, G-contains gluten, D-contains dairy, E-contains egg, S-contains soy, N-contains nuts
GF-gluten free, DF-dairy free

10:45 a.m. – 11:30 a.m.

Beyond FERPA: Higher Ed's Guide to Privacy Laws and Regs

Grand Ballroom A, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Privacy

Pegah K. Parsi, *Chief Privacy Officer, University of California San Diego*

This is a survey of key privacy legislation that impacts higher education, covering personal information in records related to students, finances, HR, research participants, and patients. We will cover the intersectionality of FERPA, GLBA, HIPAA, and the Common Rule, as well as state and foreign laws. We will also cover key privacy principles that are instrumental in compliance with all of these laws.

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Faculty, Staff, and Students, Oh My! Reducing Risk by Expanding Security Awareness to Everyone

Grand Ballroom BC, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

Amanda Griffith, *Assistant Director Governance, Risk, & Compliance/Privacy Officer, West Virginia University*

Alison E Murray, *Senior Information Security Specialist, University of Massachusetts Boston*

Reducing human risk and building a collective mindset of cybersecurity as everyone's responsibility requires a security awareness and training program that intentionally veers from one-size-fits-all education and communications. Yet developing role-appropriate training for staff, faculty, or students takes planning, collaboration, and even a touch of creativity. Security and compliance professionals at UMass Boston and West Virginia University discuss and compare strategies from their security awareness training playbooks for different learner audiences. Discover what's working for them, important lessons learned, and adaptations they've made (and continue to make) to strengthen their institutions' security consciousness, build enduring security habits, and ultimately contribute to lowering their risk profiles.

Lasso the Moon: Achieving Federated Cyber Risk Management in Higher Education

Regency Ballroom D-G, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Risk, Compliance, and Policy

Teresa E. Banks, *Manager, Information Security & Compliance Programs, The University of Arizona*

Steven Hicks, *Principal Information Security Architect, The University of Arizona*

The University of Arizona (UArizona) Information Security Office has pioneered the development and implementation of a federated information security risk management program that successfully identifies risk to the university and its academic and research mission and provides units with achievable risk mitigation goals. Attendees will learn how UArizona has built a successful program through the following: training and team-building exercises for unit risk managers; consultations with information security experts; a new, automated federated cyber-risk management platform; gamification of the annual risk management cycle that incentivizes security plan completion and recognizes achievements of units and their risk managers; and providing campus leadership with an annual report, tracking institutional security posture and progress.

One Giant Leap: A Modern Approach to Transforming Security Strategies and Stopping Breaches

Regency Ballroom A-C, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Technologies and Operations

John Virden, *AVP, Chief Information Security Officer, Miami University*

Tina Thorstenson, *VP, Industry Business Unit, CrowdStrike*

Jeremy Rosenberg, *Chief Information Security Officer, Yale University*

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Today's cyberattacks constantly target academia, but these can be thwarted by embracing modern enterprise visibility, cloud security, and identity protection. Join us in a collaborative discussion, including Jeremy Rosenberg, CISO of Yale; John Virden, CISO of Miami University; and Tina Thorstenson, former CISO of Arizona State University, as they share insights on designing and implementing transformative security strategies designed to stop breaches. They will discuss successes and lessons learned, plus share how they leveraged partnerships, including CrowdStrike, as an extension of their in-house security team to strengthen their security posture.

Our Team is Our Most Important Asset

Cedar Ballroom, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Leadership and Professional Development

Ping Wei, *Sr. Director of ISO Operations, Stanford University*

There is a significant shortage in the information security workforce globally. In this highly competitive job market, how do we successfully build and retain a team of professionals with high performance, high engagement, and high motivation? What "secret sauce" keeps a team loving its job and doing it exceptionally well, especially in the higher education environment? Why is staff development critical, and how do we do a better job of it? What are the common challenges that teams face in staff development? How do we develop leadership and provide opportunities when the promotion pipeline in a higher education environment is slow? How do we efficiently recruit with diversity and inclusion? What are the practical tips? What are the essential qualifications needed to succeed in infosec? How does the increase in the remote workforce help the situation, while at the same time bringing new challenges?

11:45 a.m. – 12:30 p.m.

Bridging the Gap: Gender Identity and Privacy

Grand Ballroom A, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Privacy

Mike Olsen, *CEO, Proctorio*

Stanna Michelle Slater shares her journey as a transgender woman and discusses the difficulties for members of the LGBTQ community to claim their identity in education and beyond and to protect their privacy in an increasingly surveilled world.

How To Win Friends and Influence University Leaders

Grand Ballroom BC, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Track: Leadership and Professional Development

Ian Douglas Washburn, *Director of Information Security, University of Notre Dame*
Paul Drake, *IT Risk Program Manager, University of Notre Dame*

Support from university leadership is the most critical component of an information security program. This session is about how to get that support to meet the rising challenges of securing our operations and data. With specific and detailed steps, we share our principles and strategies for ensuring that leaders invest their confidence and priorities in your security program. We will lay out our experience developing and validating our roadmap, demonstrating value, and growing our team.

Strategic Leadership to Implement Zero Trust

Cedar Ballroom, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Leadership and Professional Development

Albert Veysel ERDAG, *Chief Information Security Officer, University of Arkansas, Little Rock*

Implementing Zero Trust requires not only technical and architectural changes but also cultural changes. Security leaders need to show strong leadership skills to implement Zero Trust successfully. Strategic management and strategic leadership practices will be the most effective methods that can be used to design and implement a successful Zero Trust solution. Research has shown that a Human-Centered Approach and Leadership Alignment and Accountability are critical elements to implement Zero Trust successfully. In this session, security and IT leaders will get details about strategic leadership behaviors and practices. The session will also give examples and cases to understand the strategic leadership practices. Communication and cultural change are important and critical components of Zero Trust implementation, and strategic leadership skills should be used.

Web Application Security: Building an Offensive Testing Program with Cybersecurity Graduate Students

Regency Ballroom D-G, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Technologies and Operations

Charron Andrus, *Associate Chief Information Security Officer, University of California, Berkeley*
Josh Kwan, *IT Security Analyst, University of California, Berkeley*
Allison Kay Henry, *Chief Information Security Officer, University of California, Berkeley*

According to the 2022 Verizon Data Breach Investigations Report, 40% of all data breaches involved a web application attack. At the same time, hands-on web application security testing is resource-intensive and out of reach for many institutions on tight budgets, leaving many critical applications vulnerable to attack. Come learn about UC Berkeley's innovative solution to this challenge, a partnership between the Information Security Office and the School of Information's Master of Information and Cybersecurity (MICS) Program, to provide offensive web application security testing services for campus business applications. Through their coursework, MICS students are authorized to launch attacks against real-world campus web applications. This invaluable learning strategy prepares them for cybersecurity careers while lowering

For the most up-to-date information please use the EDUCAUSE Events mobile app.

our campus risk profile by providing actionable reports to campus application developers. During this session, we'll cover all aspects of this program from inception to management and give you ideas for implementing a similar program at your institution.

HECVAT 2023 Updates

Regency Ballroom A-C, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Risk, Compliance, and Policy

Susan Coleman Snyder, *Assessment Program Manager, Indiana University Bloomington*
Joshua Callahan, *Information Security Officer and CTO, Humboldt State University*
Charles Escue, *Information Security Manager, Indiana University*
Nick Lewis, *Program Manager, Security and Identity, Internet2*

The higher education information security community, the HECVAT working group, and others have collaborated for over seven years to build the successful HECVAT with over 150 campuses using it. Our session this year will review the HECVAT futures survey from 2022, future plans, scope creep discussion, and ask for your input into where to develop HECVAT in the future to benefit the higher education community. For example, we heard from the survey that 40% don't use the scoring, so we want to see what you think about it! We also have heard clearly that more training and documentation are needed. We want to hear your thoughts on what is needed and how HECVAT could be developed or enhanced. We'll also go over where we need you to get involved to build more resources for the community and the service providers that support us.

Lunch - Sponsored by Cloudflare

Grand Ballroom E-K, Second Floor

Session Type: Meal

Delivery Format: Meal

Track:

Join colleagues to eat lunch and network informally.

[**Click here**](#) **for a message from Cloudflare, the sponsor of this function.**

Menu (subject to change):
Chicken and Black Bean Tortilla Soup (GF, DF)
Baby Spinach, Cotija Cheese, Roasted Corn, Roasted Baby Peppers, Pepitas And Cilantro Lime Vinaigrette (D, GF, V)
Black Bean & Quinoa Salad, Shaved Red Onion, Cilantro, Chorizo, Shaved Jamaica And Avocado Vinaigrette (GF, DF)
Grilled Marinade Chicken Adobo with Charred Lemon and Chives (GF, DF)
Slow Braised Beef Machaca with Pickled Baby Peppers and Cilantro (GF, DF)
Flour Tortillas – Corn Tortilla on request (Vn)

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Charred Baby Carrots with Sauteed Mushrooms (Vn, GF)
Spanish rice with Grilled Green Onions (Vn, GF)
Fresh Coffee and Tazo Tea
Iced Tea

V-Vegetarian, Vn-Vegan, G-contains gluten, D-contains dairy, E-contains egg, S-contains soy, N-contains nuts
GF-gluten free, DF-dairy free

1:45 p.m. – 2:30 p.m.

IAM Program Strategies for Delivering Continuous Improvement and Transformational Value

Regency Ballroom A-C, Second Floor

Session Type: Industry Led

Delivery Format: Presentation/Panel Session

Track: Technologies and Operations

Brandon Kendall, *Sr. Consultant, Moran Technology Consulting*

Scott Weyandt, *Vice President, Information Security , Moran Technology Consulting*

Sureyya Tuncel, *Manager, Identity and Access Management, University of California, Riverside*

Dewight Kramer, *CISO, University of California, Riverside*

Too often, IAM efforts focus on selecting and deploying technology. However, a transformational IAM program must be capable of making continued, strategic improvements (i.e., delivering real, sustained value). The University of California Riverside began a multiyear, multiphase initiative to build an IAM Program able to reduce risk and also transform its academic digital experience. We explore UCR's experience (wins, lessons, and plans) to identify key elements of an effective IAM Program.

Overview of Updates to the Chief Privacy Officer (CPO) Primer

Cedar Ballroom, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Privacy

Susan Bouregy, *Chief Privacy Officer, Yale University*

Jeff Gassaway, *Information Security & Privacy Officer, University of New Mexico*

This session is ideal for privacy officers who are new to their roles, privacy professionals who are seeking to move into privacy officer positions, or those building a new program. In this session, we will share details of the resource-rich updated primer and how the primer can help privacy officers identify approaches to success at their institutions, wherever their institutions are in their privacy journeys.

Partnering for Next-Gen Cybersecurity in a Growing and Complex Risk Landscape

Grand Ballroom A, Second Floor

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Session Type: Industry Led

Delivery Format: Presentation/Panel Session

Track: Technologies and Operations

Hunter Ely, *Higher Education Strategist, Palo Alto Networks*
Bruce Hembree, *Field Chief Technology Officer, Cortex, Palo Alto Networks*
Leo Howell, *Chief Information Security Officer, Georgia Institute of Technology*

Join us for a panel discussion with Palo Alto Networks, CDW, and Georgia Tech in which they will discuss key issues such as how to build and run a SOC, prioritize and respond to threats, and collaborate with other organizations to enhance cybersecurity. The panelists will also delve into the critical role of partnerships between the education and cybersecurity communities, focusing on modern cybersecurity capabilities that can be leveraged to share intelligence and prevent threats.

Third-Party Risk Management: Higher Education's Shield Against Third-Party Cyber Threats

Grand Ballroom BC, Second Floor

Session Type: Industry Led

Delivery Format: Presentation/Panel Session

Track: Risk, Compliance, and Policy

Sandra Taylor, *Director of Information Security Governance, Risk and Compliance, University of Southern California*
Jeff Welch, *Senior Manager, Deloitte & Touche LLP*

Third-party cyber threats are on the rise, prompting institutions of all sizes to take an enhanced security stance as cyber attacks continue to increase in both scale and frequency. This session will provide an overview of third-party cyber risk management, including leading practices, recent trends and emerging risks, and insights into navigating college and university structures. Participants will find out how other institutions are structuring their programs and prioritizing risk.

2:30 p.m. – 3:15 p.m.

Dessert, Refreshment Break, and Corporate Displays

Grand Ballroom Foyer, Second Floor

Session Type: Break

Delivery Format: Break

Track:

Menu (subject to change):
Regular Coffee, Decaffeinated Coffee, Tazo Hot Tea
Assorted soft drinks
Fresas Con Crema (GF, D)
Dulce de Leche Cake Bite (D, G, E)
Warm Pretzel Bites (G, D), Smoked Cheddar Cheese Sauce (GF, D), Honey Whole Grain Mustard (V, GF)
Whole Seasonal Fruits

For the most up-to-date information please use the EDUCAUSE Events mobile app.

V-Vegetarian, Vn-Vegan, G-contains gluten, D-contains dairy, E-contains egg, S-contains soy, N-contains nuts
GF-gluten free, DF-dairy free

3:15 p.m. – 4:00 p.m.

Identity Makeover: Transforming a Campus IAM System

Grand Ballroom A, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Technologies and Operations

Bryan Meeker, *IAM Architect, University of California, Riverside*

Sureyya Tuncel, *Manager, Identity and Access Management, University of California, Riverside*

This presentation will focus on a multiyear journey to review and revamp the identity and access management (IAM) technology stack at an educational institution. Like many organizations, the IAM technology stack had grown in an organic way, leading to various challenges related to identity management. The presentation will share the lessons learned during more than two years of moving away from the organic technology stack and toward an enterprise solution. The speakers will discuss how this new set of tools improves the end-user experience as well as the security posture of the campus. Attendees will gain insights into the process of modernizing an IAM technology stack and the benefits that can be achieved through the implementation of an enterprise solution.

Putting the Spotlight on Web Privacy

Cedar Ballroom, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Privacy

Christopher Billick, *Director of Digital Strategy, University of Michigan-Ann Arbor*

Klare Savka, *IT Policy, Privacy, and Governance Analyst, University of Michigan-Ann Arbor*

In 2022, the University of Michigan Privacy Office decided to put the university's commitment to respecting and protecting the privacy of our community members and guests to the test on U-M websites. We scanned 80 of the university's most visited and prominent sites. In this presentation, we will share our findings, demonstrate the improvements we have pursued, and share the best practices we have identified for strengthening privacy considerations in the U-M web environment.

REN-ISAC Cybersecurity Peer Assessment Service: Findings over Five Years

Regency Ballroom D-G, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Technologies and Operations

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Susan Coleman Snyder, Assessment Program Manager, Indiana University Bloomington

The REN-ISAC offers cybersecurity assessments of research and educational organizations completed by higher educational cybersecurity professionals. With experience from dozens of assessments, there are many learnings that can be applied to all organizations. This session reviews collective trends, recommendations, and priorities discovered by REN-ISAC's assessors and focuses on practical advice to help improve cybersecurity programs.

The Cyber Bowl: Exploiting School Rivalries to Enhance Security Awareness

Grand Ballroom BC, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

Avi Baumstein, Cybersecurity Manager, University of Florida
Philip Kraemer, Information Security Training Coordinator, Florida State University

Hut, hut, hike! Play the Cyber Bowl! It's time to take the field and start tackling cyberthreats! Get your ticket to the game to learn how we utilized the rivalry between Florida State University and University of Florida to increase participation during Cybersecurity Awareness Month in October 2022.

The Power of Circles: Build a Support Network, Grow Your Career, AND Stay Sane

Regency Ballroom A-C, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Leadership and Professional Development

Mary McKee, Senior Director of Engineering, Cirrus Identity, Inc.
Han Thazin Tun, Security Operations Engineer, Amazon Web Services
Emily K. Adams, Principal Security Analyst, Indiana University
Amy Starzynski Coddens, Strategic Security Manager , University of Wisconsin System Administration

Building on personal experiences and lessons learned, this panel of four women cybersecurity professionals will explore the friendly alternative to formal mentorship by cultivating a strong team of peer advisors held as an inner circle. We will dive into how mentorship and peer advising can supplement each other, how to cultivate an awesome peer advisor team, and explore when and how to lean on your circle for both support and levity during professional challenges and opportunities.

4:15 p.m. – 5:00 p.m.

Put The Hammer Down! Leadership for an Integrated Organization

Grand Ballroom BC, Second Floor

Session Type: Breakout Session

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Delivery Format: Presentation/Panel Session

Track: Leadership and Professional Development

Ryan MacTaggart, *Associate Director, Professional Learning, EDUCAUSE*

Ever feel like a hammer looking for nails? Cybersecurity leaders often feel like they need to be a proverbial hammer, ever aware of the nails that are true and impactful threats. However, being and developing leaders who put the hammer down helps to open communication, enable creativity, and create an integrated culture much more likely to lead to positive outcomes. It can even lead to more effective hammering when it's time to pick up the hammer again. Let's discover why an integrated approach is better and explore when and how to loosen our grip.

Securing the Cloud: A University's Adventure

Grand Ballroom A, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Technologies and Operations

John Ives, *Senior Security Analyst, University of California, Berkeley*

As many institutions move infrastructure and systems to public clouds, they are challenged to keep up with the security of those systems. While many turn to using the provider's native tools, UC Berkeley decided that would not be a sustainable model with their staffing, so they set out to find a way. This talk will cover why they took the approach they did, their adoption process, the choice they made, and some of the hidden surprises they found along the way.

The Last SOC Student Employee: Using a Capture-the-Flag Competition to Engage Potential Student Employees

Cedar Ballroom, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Leadership and Professional Development

Andrew McClurg, *IT Analyst - Security, Syracuse University*

How do you identify student employees who have an interest in security and the ability to problem-solve in areas outside of their experience? Resumes and short interviews and can only tell you so much. Through a free platform, Syracuse University hosted a capture-the-flag (CTF) competition to engage students interested in security and help identify students to recruit as future SOC employees. Unlike traditional employment assessments, CTFs provide a way for security departments to evaluate a wide range of skills in a real-world, hands-on setting. While CTF competitions are not a stand-alone employment assessment solution, when used in conjunction with other methods of evaluating candidates they can provide a deeper understanding of a student's interest in the security field.

Vendor Risk Management in Privacy and Security: Mastering the Balance between Efficient and Effective

Regency Ballroom A-C, Second Floor

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Risk, Compliance, and Policy

Laurie Neal, *Information Security Awareness Specialist, University of Connecticut*
Donald W Babcock, *Application Security Analyst II, University of Connecticut*

Every day, institutions rely on third parties to perform services on our behalf. Operating a Vendor Risk Management (VRM) program is necessary to identify and mitigate risks and to make informed business decisions. With limited resources and competing priorities, however, finding where efficiency meets effectiveness is a challenge. This session will help security and privacy professionals consider VRM strategies when assessing university vendors.

Zero Trust: Ease of Use and Flexibility Restored to Regulated Research

Regency Ballroom D-G, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Risk, Compliance, and Policy

Veronica Wilkinson, *Director of IT Services, CEC, University of South Carolina*
Marshall Hollis, *System Architect, University of South Carolina*

Just prior to the COVID-19 pandemic, our college launched the Carolina Enclave for Secure Research to provide its researchers with a self-contained environment for Department of Defense projects. The requirements for our regulated research enclave were simple: researchers needed a NIST SP 800-171 compliant environment to edit Controlled Unclassified Information (CUI) documents and collect data. With the sudden pivot to work from home during the pandemic, we had to find a way to enable those working on regulated research projects to safely browse the web, use collaborative SaaS tools like Office 365 and Teams, and access resources. Post-pandemic, our regulated research users needed flexibility. Researchers work out of different locations: on site at a college lab or office, at home, or when traveling to conferences. We started redesigning the regulated research environment with these new requirements and along the way realized we were implementing a Zero Trust Architecture. This talk describes our journey and uses the new NIST Special Publication 800-207 (Zero Trust Architecture) to demystify and sort out the elements of Zero Trust from the marketing buzzwords. We identify the roadblocks we experienced along the way, as well as the benefits of Zero Trust. The Zero Trust paradigm has taken our CMMC/NIST SP 800-171 implementation and restored much of the flexibility and ease of use that our users expect, allowing the users to concentrate on the research and not the environment.

5:00 p.m. – 6:00 p.m.

Networking Reception

Grand Ballroom Foyer, Second Floor

Session Type: Reception

Delivery Format: Reception

Track:

For the most up-to-date information please use the EDUCAUSE Events mobile app.

One of the most valuable aspects of this conference is the opportunity to connect face-to-face with fellow attendees. Join us for the reception, where you can relax over food and drink and get to know your colleagues. A cash bar will be available; each attendee will receive one drink ticket.

NOTE: Please wear your name badge for admittance.

Menu (subject to change):
Wine
Premium and Import Beer
Domestic Beer & Hard Seltzer
Mineral Water/Juices/Soft Drinks
Vegetable Crudité Display
Artisanal Cheese Display
- Handcrafted Northwest Cheese Selection including Beecher's and Cascadia Creamery (D)
- Dried Fruits and Toasted Nuts (N)
- Local Honey, Fig Jam, Citrus Mostarda
- Local breads and Crackers (G)

Local Meats Display
- Artisanal Locally Cured meats to include Salt Blade, Olympia Provisions, and Salumi
- Dried Fruits and Toasted Nuts (N)
- Peach Lemon Mostarda, Quince Paste, Fig Jam
- Local Breads and Crackers (G)

Passed Appetizers:
- Malibu Coconut Fried Shrimp (DF, G, Contains Shellfish)
- Seared Beef, Lemon Ricotta, Crostini, Red Chimichurri Drizzle (D, G)
- Dungeness Crab Cakes with Red Pepper Aioli (G, DF, Contains shellfish)
- Chili and Chicken Skewers with Balsamic Glaze (GF, DF)
- Short Rib in Bacon, Ancho BBQ Sauce (GF, DF)
- Sundried Tomatoes and Mushrooms Puff Pastry (G, D)

V-Vegetarian, Vn-Vegan, G-contains gluten, D-contains dairy, E-contains egg, S-contains soy, N-contains nuts
GF-gluten free, DF-dairy free

8:00 p.m. – 11:59 p.m.

Get Your Game On! - Sponsored by Menlo Security

Regency Ballroom A-C, Second Floor

Session Type:

Delivery Format: Activity

Track:

Join us for the ninth annual Cybersecurity and Privacy Professionals Conference game night! This is a great way to get to know your fellow conference-goers in a relaxed atmosphere. No experience necessary; we invite attendees to bring along their favorite game, from casual party games to serious board games. Games will startup throughout the evening so come by whenever you like. Grab a chair and get your game on!

[Click here](#) *for a message from Menlo Security, the sponsor of this function.*

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Wednesday, May 3

7:15 a.m. – 8:00 a.m.

2023 Program Committee Breakfast (by invitation only)

Larch, Third Floor

Session Type: Meal

Delivery Format: Meal

Track:

Menu (subject to change):
Juices: Pomegranate, Orange, Tomato
Sliced Seasonal Fruit: Honeydew, Cantaloupe, Pineapple (Vn, GF, DF)
Whole Fruit: Bananas, Anjou Pears, Seasonal Fruit (Vn, GF, DF)
House Baked Fresh Bakeries: Croissants, Mango Muffin with Toasted Coconut, Seasonal Bakery (V, G, D, E, S, N)
Grains: Quinoa Porridge with Coconut Milk– Toasted Pecans, Dried Cherries, Fresh Berries, Soy Milk (GF, DF, Vn)
Infused Water: Cucumber-Tarragon
Locally made Breakfast Turnovers:
- Bacon, Egg, and Cheese (G, D, E, S)
- Mushroom, Leeks and Egg (G, D, E, S)

Fresh Coffee and Tazo Hot Tea
V-Vegetarian, Vn-Vegan, G-contains gluten, D-contains dairy, E-contains egg, S-contains soy, N-contains nuts
GF-gluten free, DF-dairy free

Continental Breakfast - Sponsored by Okta

Grand Ballroom Foyer, Second Floor

Session Type: Meal

Delivery Format: Meal

Track:

Join colleagues for a light breakfast and network informally.

[Click here](#) for a message from Okta, the sponsor of this function.

Menu (subject to change):
Juices: Pomegranate, Orange, Tomato
Sliced Seasonal Fruit: Honeydew, Cantaloupe, Pineapple (Vn, GF, DF)
Whole Fruit: Bananas, Anjou Pears, Seasonal Fruit (Vn, GF, DF)
House Baked Fresh Bakeries: Croissants, Mango Muffin with Toasted Coconut, Seasonal Bakery (V, G, D, E, S, N)
Grains: Quinoa Porridge with Coconut Milk– Toasted Pecans, Dried Cherries, Fresh Berries, Soy Milk (GF, DF, Vn)
Infused Water: Cucumber-Tarragon
Locally made Breakfast Turnovers:
- Bacon, Egg, and Cheese (G, D, E, S)
- Mushroom, Leeks and Egg (G, D, E, S)

Fresh Coffee and Tazo Hot Tea

For the most up-to-date information please use the EDUCAUSE Events mobile app.

V-Vegetarian, Vn-Vegan, G-contains gluten, D-contains dairy, E-contains egg, S-contains soy, N-contains nuts
GF-gluten free, DF-dairy free

7:15 a.m. – 11:30 a.m.

Registration Desk Open

Grand Ballroom Foyer, Second Floor

Session Type: Service Desk

Delivery Format: Service Desk

Track:

8:00 a.m. – 8:45 a.m.

Building and Implementing a CMMC Program: An Overview

Regency Ballroom A-C, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Risk, Compliance, and Policy

Michael Corn, *CISO, University of California San Diego*

Jason E. Pufahl, *Vice President Security Services, Vancord*

Amy Starzynski Coddens, *Strategic Security Manager , University of Wisconsin System Administration*

CMMC is an evolving regulatory requirement that will impact any industry that has a working relationship with the Department of Defense. Since the original "Dear Colleague" letter in 2016, higher education has been wrestling with making sense of the requirements, identifying potential scope, and implementing the framework in what is often a complex, distributed, and shared ecosystem. This session will provide an overview of CMMC, explore the current status of the CMMC program, discuss practical strategies to help universities and colleges determine how to comply, and discuss why the Gramm-Leach-Bliley Act and Federal Student Aid create an additional business case for NIST 800-171.

Expanding Annual Cybersecurity Assessments on an Obstreperously Decentralized Campus

Regency Ballroom D-G, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Risk, Compliance, and Policy

Gabriel McElwain, *IT Risk Analyst, University of Chicago*

Cornelia Ann Bailey, *Director, Information Assurance, University of Chicago*

David Mendez, *Risk Analyst, University of Chicago*

Jessica Abra Sandy, *Governance, Risk, and Compliance Manager, University of Chicago*

For the most up-to-date information please use the EDUCAUSE Events mobile app.

We will share lessons we learned from completing the first cycle of the University of Chicago's cybersecurity assessment program, the feedback we received from participants (and auditors), and the revisions we have made for our second assessment cycle. We will describe the ways in which we created, revised, and delivered reports for leadership and participants; solicited and analyzed feedback from participants; leveraged internal auditors to review our approach; expanded the scope of the program; revised the assessment process, structure, and language; built infrastructure to support tracking, communications, and change management; and planned for the future of our assessment program.

Junior Security Operations Center Analyst Badging Program for Student Employees

Cedar Ballroom, Second Floor

Session Type: Breakout Session

Delivery Format: Demonstration

Track: Leadership and Professional Development

Douglas Lomsdalen, *Information Security Officer, California Polytechnic State University, San Luis Obispo*

In 2019, the California Polytechnic State University Information Security Office established a Learning Security Operations Center (SOC), where a team of security analysts works together to proactively monitor the university's ability to operate securely. The students learn Tier 1 SOC duties (e.g., proactive monitoring, remediation, compliance, and communication skills). In this very competitive job market and the industry's desire for cybersecurity "unicorns," we wanted to give our students a leg up in the job hunt. In 2021, we created a homegrown three-tier (entry-level, intermediate, and advanced) badging program to recognize our student employee accomplishments while they work in the Learning SOC as Junior SOC Analysts. The badge is a visual representation of the student's achievements and skills learned while working in the SOC. These badges are shareable through social media platforms like LinkedIn via their profiles. We've developed a rubric to identify the qualifications for each badge; a link to the associated metadata is also viewable through the social media platform. Along the way, they must meet four SOC Key Competencies: SIEM, Procedures, Monitor, and Collaborate.

Launching Cybersecurity Training at a Big Ten: Lessons Learned

Grand Ballroom BC, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

Isaac Galvan, *Lead Cybersecurity Training Specialist, University of Illinois at Urbana-Champaign*
Cynthia McKendall, *Senior Cybersecurity Training Specialist, University of Illinois at Urbana-Champaign*
Sandra Bone, *Cybersecurity Training Specialist, University of Illinois at Urbana-Champaign*

Managing human risk with a high-quality cybersecurity training and awareness program can make a measurable difference in how faculty, staff, and students approach their own security, building more secure habits that benefit themselves and the institution. In 2021, the Cybersecurity Training and Awareness team at the University of Illinois Urbana-Champaign launched required cybersecurity training for campus employees. Find out how our team laid the groundwork for a successful launch and how the training and awareness program continues to grow to address human risk. We will discuss how the cybersecurity training and awareness program at the University of Illinois yields positive results, as well as lessons learned along the way.

8:30 a.m. – 10:30 a.m.

Corporate Displays

Grand Ballroom Foyer, Second Floor

Session Type: Industry Led

Delivery Format: Industry Led

Track:

This is your last opportunity to meet with companies showcasing security technology solutions for higher education with dedicated visiting time scheduled during the morning break. Stop by to learn more about their solutions and interact with company representatives.

Armis

Armis is the global leader in cyber asset security. Organizations trust our real-time, comprehensive asset visibility and intelligence platform for automated enforcement across every connected asset and environment? IT, cloud, IoT, IoMT, OT, BYOD, and edge. Armis helps organizations across any industry continuously secure their entire cyber-asset attack surface.

Bravura Security

Bravura Security is an analyst-recognized industry leader delivering best-in-class identity, privileged access, password, and password-less solutions with the power of one platform. Over the last two decades, Bravura Security has helped higher education institutions protect their organizations against increasing cybersecurity threats.

CampusGuard

Founded in 2009, CampusGuard provides cybersecurity and compliance services for campus and community-based organizations, including higher education, health care, state and local government and agencies, financial services firms, and SaaS/tech companies, among others. CampusGuard's success in serving their customers can be attributed to the experience, education, and commitment of their certified professionals and their in-depth understanding of the unique needs of the markets they serve. For more information, visit *www.campusguard.com*.

Cisco Secure, Platinum Partner

Cisco Secure drives security resilience, enabling organizations to protect the integrity of their business amidst unpredictable threats or change and emerge stronger. With the Cisco Security Cloud, organizations see across the multi-cloud environments, anticipate what's next, take the right action, close security gaps, and get better every day to support the success of institutional-wide resilience investments.

Cloudflare

Cloudflare is the security, performance, and reliability company on a mission to help build a better internet. Today, it runs one of the world's largest networks that powers anything connected to the internet. Its services are used by everyone from educational institutions to Global 2000 companies and top government organizations.

Fortinet

Fortinet makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere. The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing devices, data, applications, and connections from the data center to the cloud.

Gigamon

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures.

Imperva

Imperva is the comprehensive digital security leader on a mission to help organizations protect their data and all paths to it. Customers around the world trust Imperva's integrated approach combining edge, application, and data security to protect their applications, data, and websites from cyberattacks.

Infosec, part of Cengage Group

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at *infosecinstitute.com*.

Indiana University OmniSOC

OmniSOC is the shared security operations center for higher education and research. OmniSOC rapidly delivers only critical, actionable, high-quality alerts 24/7, allowing cybersecurity staff to focus on what's important—at substantial cost savings—from a trusted leader in the higher education cybersecurity community and supported by the formidable capabilities of Indiana University's GlobalNOC.

Microsoft Corporation, Platinum Partner

Reimagined for a new era of digital learning, Microsoft Education helps to unlock student potential with powerful tools to learn, collaborate, and create all in a secure and trusted environment. The solution also promotes diversity and inclusion with a commitment to expand accessibility for all, and to bridge the gap in education by providing access to technology for those around the world with disabilities.

Moran Technology Consulting, Gold Partner

At Moran Technology Consulting, we enable our clients to build mature identity and access management (IAM) programs and identity-focused cybersecurity solutions that have transformational impact on digital experience, DEI initiatives, and institutional risk management. Our expert consultants perform assessments, strategic planning, roadmaps, platform evaluations, and solution design and implementations.

Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. We're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

Rapid7

Rapid7's industry-leading security solutions and strategic expertise empower you to stay ahead of attackers, ahead of the competition, and future-ready for what's next.

Salty Cloud

Isora GRC from SaltyCloud is the Lightweight Governance, Risk, and Compliance (GRC) Assessment Platform that helps teams unlock new dimensions of risk for more efficient mitigation, improved regulatory compliance, and robust resilience without the hassle of legacy solutions. Ready to build a GRC program you can trust?

SANS Institute

For the most up-to-date information please use the EDUCAUSE Events mobile app.

Launched in 1989 as a cooperative for information security thought leadership, the SANS mission is to empower cybersecurity professionals with the practical skills and knowledge they need to make our world a safer place. Visit our display and learn more about our SANS training products and educational institution discount programs.

SecureW2

SecureW2 helps universities deploy password-less security via digital certificates to provide more secure Wi-Fi and application access. Improve connection experience to networks with fewer disconnects and faster Wi-Fi roaming. Talk to us about how you can leverage certificates to securely connect users to on-prem and cloud apps without MFA fatigue.

SecurityZones

SecurityZones is a commercial partner and distributor of Spamhaus Technologies. Spamhaus is the trusted authority on IP and domain reputation, providing industry-leading, real-time datasets to safeguard against malware, phishing, botnets, spam, and more. With 25 years of experience, Spamhaus not only protects, but provides insight, across networks and email worldwide.

Splunk

Splunk helps make organizations more resilient. Leading organizations use our unified security and observability platform to keep their digital systems secure and reliable. Organizations trust Splunk to prevent security, infrastructure, and application issues from becoming major incidents; absorb shocks from digital disruptions; and accelerate transformation.

Yakabod

Built for higher education, Yakabod Cyber Incident Manager (CISOBox) delivers efficient, secure, automated incident handling through intelligence agency technology. Universities use CISOBox to isolate and secure sensitive incident data, documentation, and communication; generate critical metrics/reports for leadership; and gain NIST 800-61r2 compliance. Integrated with ServiceNow, Active Directory, Teams, Slack, and more.

Zscaler

Zscaler accelerates digital transformation so that customers can be more agile and secure. The Zscaler Zero Trust Exchange, a SASE-based platform, is the world's largest inline cloud security platform, protecting thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications over any network.

9:00 a.m. – 9:45 a.m.

Information Security Approval Matrix: Bringing Order to Complexity

Regency Ballroom D-G, Second Floor

Session Type: Breakout Session

Delivery Format: Demonstration

Track: Risk, Compliance, and Policy

Tony Kinne, *Security Engineer, Miami University*

Jacob Harrison, *Security Analyst, Miami University*

Approval authority can be extremely complex. Information security offices are asked daily to view, gather, investigate, retrieve, export, forward, disable, enable, provision, de-provision, delegate, create, remove, block, allow, playback, hide, or redact all kinds of information, accounts, devices, networks, files, applications, email, calendars, video, phones, and door access. The office of authority to approve these actions varies based on the type and sensitivity of the data involved. Approval can be at a department or division level. It may be the data owner, human resources, student affairs, academic

For the most up-to-date information please use the EDUCAUSE Events mobile app.

integrity, the provost, law enforcement, or even the legal office. In some cases, approval is dictated by compliance requirements. This session introduces and shares a convenient and simple tool that provides direction on the execution of Miami University's Information Security Approval Matrix (ISAM). The ISAM is based on common or expected cyber-related events or messaging in a clear, concise, and consistent fashion.

Privacy in Higher Education's Legal Landscape (with Guest Appearances from Ethics and History)

Grand Ballroom BC, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Privacy

Abe Bender, *Senior Privacy Analyst, University of Washington*

This session will provide a 70,000-foot view of privacy history, ethics, and law as they affect U.S. higher education.

The Last Line of Defense: How to Improve Recovery by Leveraging the Cloud

Grand Ballroom A, Second Floor

Session Type: Breakout Session

Delivery Format: Demonstration

Track: Technologies and Operations

Mark Kawasaki, *Assoc. Director, Disaster Recovery, Emory University*

Recovery is a critical but often neglected cybersecurity function, the last line of defense against cyberattacks and other threats. This session will provide an overview of how Emory University has been able to leverage the power of the cloud and automation to improve its cybersecurity recovery efforts with increased scalability, flexibility, and cost-effectiveness. Emory will share lessons learned and benefits gained and discuss various cloud-based recovery strategies and best practices they have adopted.

The Sky's the Limit: How Privacy and Security Awareness Enable Data-Enhanced Decision-Making

Regency Ballroom A-C, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

Joseph Gridley, *Chief Data Privacy Officer, University of Maryland*
Jonathan Engelberg, *Research Analyst, University of Maryland*
Mark A Werling, *Chief Privacy Officer, Indiana University*

As student and learning analytics become more reliant on large data sets, machine learning, and predictive modeling, institutions must be careful not to alienate the student populations they are trying to support. Panelists will discuss the

For the most up-to-date information please use the EDUCAUSE Events mobile app.

security and privacy sections of the 2022 EDUCAUSE student survey, what those results tell the community, and how to use those results to establish trust and enable data-informed student support.

Zero Trust: The Critical Role of Identity

Cedar Ballroom, Second Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

Emily Longman, *Lead Security Analyst, Oregon State University*

Marjorie McLagan, *Deputy Chief Information Security Officer , Oregon State University*

As part of our Zero Trust program, Oregon State University completed an RFP, purchased a commercial IGA (Identity Governance and Access) system, and hired an implementation partner. We plan to replace our Shibboleth IDP with Azure SSO and deploy the Cirrus Bridge; redesign our account lifecycles to better reflect real-world scenarios; design enterprise roles for automated access; implement a workflow-based access request process for exceptional access; and create periodic access recertification campaigns. We are early in our journey for replacing OSU Identities and will approach the next phase of this project during the time of this conference (May 2023). We can discuss various aspects such as our reasons for choosing commercial software over open source (TAP), how we will continue to participate in the InCommon Federation, and applying Zero Trust principles in higher education.

9:45 a.m. – 10:30 a.m.

Refreshment Break and Corporate Displays

Grand Ballroom Foyer, Second Floor

Session Type: Break

Delivery Format: Break

Track:

Menu (subject to change):
Regular Coffee, Decaffeinated Coffee, Tazo Hot Tea
Assorted soft drinks
Washington Trails: Assorted Nuts, Dried Cherries, Banana Chips, Mini M&M's, Mini Pretzels, Yogurt Covered Raisins (N, V)
Individual Yogurts (D, V)
Bagel Bites (G, Vn)
Assorted Doughnuts (D, E, G)
Whole Seasonal Fruits

V-Vegetarian, Vn-Vegan, G-contains gluten, D-contains dairy, E-contains egg, S-contains soy, N-contains nuts
GF-gluten free, DF-dairy free

10:30 a.m. – 11:30 a.m.

For the most up-to-date information please use the EDUCAUSE Events mobile app.

FBI, REN-ISAC, and CISA Threat Briefing

Grand Ballroom E-K, Second Floor

Session Type: General Session

Delivery Format: General Session

Track:

The 2023 conference wraps up a memorable week with the ever-popular closing General Session featuring representatives from the FBI, REN-ISAC, and CISA.

The threat landscape may seem like more of the same, but new threats are constantly emerging and old exploits are being used in new ways. This session will provide you the freshest information REN-ISAC, FBI and CISA can share. We will discuss threats, trends, and ideas and you'll leave with a better understanding of specific cyberthreats from around the globe, as well as some insight into the malicious actors' methods, motives, and potential targets in the research and education community.