Sunday, May 12

3:00–5:00 p.m.

☕ Registration Desk Open

REGISTRATION DESK, SECOND FLOOR EVENT CENTRE

Monday, May 13

7:30 a.m.–5:30 p.m.

Registration Desk Open

REGISTRATION DESK, SECOND FLOOR EVENT CENTRE

7:30 a.m.–8:30 a.m.

☕ Continental Breakfast for Preconference Workshop Participants

FOYER, SECOND FLOOR EVENT CENTRE

8:30 a.m.–12:00 p.m.

MORNING WORKSHOPS

Note: Separate registration and fee are required

Cyberthreat Intelligence

STINGAR: Automated Detection, Sharing, and Mitigation of Network Threats

VEVEY 3, SECOND FLOOR EVENT CENTRE

Jesse Bowling, Security Architect and CSIRT Program Manager, and **Anthony Miracle**, IT Security Analyst, Duke University

Join this workshop to learn about the Shared Threat Intelligence for Network Gatekeeping and Automated Response (STINGAR) project and CommunityHoneyNetwork (CHN). We will provide an in-depth review of the project's overall goals and future directions, examine the architecture of the STINGAR ecosystem, and demo installation processes. In a final lab, you'll be given access to AWS virtual machines to deploy your own instances of CHN, which will be kept running during the conference; data summaries will be shared postconference. As time and interest allows, internals of the project development processes and future roadmap will be discussed. The goal of the STINGAR project led by Duke University (https://stingar.security.duke.edu/) is to enable low-friction generation of threat intelligence, data sharing, and action on threat intelligence for the higher ed community. Through the use of the CHN (https://communityhoneynetwork.readthedocs.io) honeypot system (a fork of Threatstream/Anomali Modern Honey Network), institutions are able to quickly deploy a central console and multiple honeypots to gather information about attacks on their networks. CHN also supports easy integration with CIF (Collective Intelligence Framework) to summarize and share this attack information with others in the community. Using CIF or CHN APIs, it is trivial to generate feeds of malicious IP addresses that can be loaded directly into an organization's protective or detective devices.

Outcomes: Understand the broad goals of the STINGAR project • Learn the key requirements for building an automated response capability based on threat intelligence • Learn how to deploy the CHN honeypot system and integrate with CIF • Influence future features of STINGAR technology

Security Architecture and Design

Integrated Cyberdefense: The Foundation for Innovation

ST. GALLEN 1, SECOND FLOOR EVENT CENTRE

Renault Ross, Chief Strategist, Symantec Corporation; **Seth Shestack**, Deputy CISO, Temple University

The accelerated adoption of cloud-based applications and services, along with the proliferation of PC, laptops, and other devices, has left many campuses increasingly vulnerable to a wide range of cyberthreats. Even if those applications and devices come with some cybersecurity features, the complexity of that environment can't be managed with a piecemeal cyberstrategy. Only an enterprise-wide integrated cyberdefense can provide a sustainable foundation for current and future innovation. In this session, we will dive into how Temple University is consolidating various disparate solutions into a wholistic approach—not only strengthening security but also improving efficiencies and lowering the total cost of ownership.

Outcomes: Understand the role of threat intelligence in assessing risks and implementing proactive controls • Identify a cohesive approach to managing security across cloud and on-premises systems environments • Evaluate enterprise licensing strategies for lowered costs and better management

Security Awareness, Communications, and Training

Using Capture the Flag for Cybersecurity Education and Training

ST. GALLEN 2–3, SECOND FLOOR EVENT CENTRE

David Raymond, Director, Virginia Cyber Range; Deputy Director, IT Security Laboratory, and **Thomas "Tweeks" Weeks**, Director of Future Technology and Communities, Virginia Tech

If done well, a capture-the-flag (CTF) competition is an educational experience disguised as a competition. It's hard not to get excited after teaching yourself a new skill, finding a flag, then being rewarded with CTF points. Bring your laptop! In this workshop, we will introduce different types of CTF competitions and describe how we have used them with students and IT professionals to drive interest and enhance learning in cybersecurity topics. And you'll get a head start on a CTF contest that will be available for the duration of the conference.

Outcomes: Learn about CTF competitions, how to host them, and how they can be leveraged in cybersecurity training and education • Participate in a live CTF competition and learn the tools and techniques used to approach different kinds of challenges • Have fun!

Strategic Leadership, Professional/Organizational Development, and Personnel Management

Creating/Rebooting Your Campus Information Security Program

VEVEY 4, SECOND FLOOR EVENT CENTRE

Alfred Barker, Assistant Vice Chancellor/Chief Information Security Officer, Board of Regents of the University System of Georgia; **Alan Bowen**, Chief Information Security Officer, Franklin & Marshall College; **Cathy Bates**, Associate Vice President, and **Joanna Lyn Grama**, Senior Consultant, Vantage Technology Consulting Group; **Lisa Warren**, Information Security Services, North Carolina A&T State University

Does digital transformation and disruptive innovation have your information security program in reactive mode? Do you feel like you're going in every direction at once, making it difficult to see what you're accomplishing overall? Chances are your campus feels this way too. Whether you need to create an information security program from scratch or reboot your current program, join this workshop to learn how to design a comprehensive security program that will scale to support transformation and innovation in all its many forms. You'll leave with a framework and plan to create an information security program with vision, governance, and a suite of services that form a cohesive and coordinated effort to support the mission of your institution in a way that is understood and leveraged by all users, from campus leaders to students.

Outcomes: Identify the information security elements that define a program versus a disjointed set of activities • Refresh, refine, or develop your information security governance model • Use a framework to define your program, services, and working relationships with campus

8:30 a.m.–4:30 p.m.

FULL-DAY WORKSHOPS

Note: Separate registration and fee are required

Governance, Risk, and Compliance (GRC)

Strategies for Streamlining Security Assessments Using the HECVAT

VEVEY 1–2, SECOND FLOOR EVENT CENTRE

Jon Allen, Chief Information Security Officer and Interim CIO, Baylor University; **Joshua Callahan**, Information Security Officer and CTO, Humboldt State University; **Susan Coleman**, Indiana University Bloomington; **Charles Escue**, Extended Information Security Manager, Indiana University; **Nick Lewis**, Program Manager, Security and Identity, Internet2

Cloud vendor security assessments continue to be a hot topic for information security, and the winds of change are only driving us to move faster than ever before. How are campuses managing the risk posed by these services? This workshop will focus on how information security teams can work with campus stakeholders to manage and assess the risks surrounding the use of cloud services.

Outcomes: Explore best practices for managing vendor risk • Learn what the HECVAT is and how it can save time in assessing the security of cloud services • Discover how institutions are using the HECVAT to improve their vendor assessments and procurement processes

Incident Management and Response

Incident Response and Analysis for First Responders

MONTREUX, SECOND FLOOR EVENT CENTRE

Duane Dunston, Assistant Professor of Information Security, Champlain College

First responders have a challenging task of determining whether a security incident has occurred. Learning to collect information from a suspected compromised computer and then analyzing it to determine if a compromise occurred is a valuable skill and could expedite the incident response process. You'll learn how to build a first-responder toolkit and how to use it to find simulated malware that mimics real malicious activity in a cloud-based virtual environment. You'll leave with a working first-response toolkit, the skills to analyze a computer system for malicious activity, and a tool to simulate malware for continuous learning.

Outcomes: Create a first-responders incident response toolkit • Analyze information collected with the toolkit to identify anomalous software • Learn to identify malicious software and its behavior to determine the potential scope of a compromise

Strategic Leadership, Professional/Organizational Development, and Personnel Management

Effective Leadership Seminar: Building Your InfoSec Leadership Style

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Cathy Hubbs, Chief Information Security Officer, American University; **David Seidl**, Vice President for Information Technology and CIO, Miami University

Leaders must leverage practices that inspire, engage, and empower others. Shifting from high-performing individual contributor to outstanding manager and leader can be challenging. You are no longer only responsible for yourself—you are responsible for a team of individuals. We'll focus on fundamental traits and characteristics effective leaders demonstrate including communication, building effective teams, emotional intelligence, and strategic thinking. We'll also explore why these skills are necessary, how to develop them, and what they mean for teams and organizations.

Outcomes: Identify traits that set successful leaders apart • Learn tools and techniques to recognize, build, and manage a synergistic team • Gain insight into key core competencies that will help you inspire, engage, and empower your staff

10:00–10:30 a.m.

☕ Refreshment Break for Preconference Workshop Participants

Sponsored by Attain

FOYER, SECOND FLOOR EVENT CENTRE

12:00–1:00 p.m.

☕ Lunch for Preconference Workshop Participants

ZURICH BALLROOM D-G, FIRST FLOOR EVENT CENTRE

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

1:00–4:30 p.m.

AFTERNOON WORKSHOPS

Note: Separate registration and fee are required

Cyberthreat Intelligence

Threat-Hunting Workshop

ST. GALLEN 1, SECOND FLOOR EVENT CENTRE

Mark Stanford, SE Manager, Public Sector | Canada | LATAM, Cisco Cloud Security

In the heat of a crisis, every keystroke count, and indecision could cost your organization millions. What separates security pros from security liabilities? A plan—and practice. Please bring your laptop to join Cisco's Advanced Threat Solutions Team for a hands-on workshop to develop your skills and test your abilities.

Outcomes: Uncover best practices for threat hunting • Learn how to incorporate threat hunting into your daily workflow • Execute real-world lab scenarios

Privacy

Fun with Certificates: A Deep Dive into Cryptography for All

VEVEY 3, SECOND FLOOR EVENT CENTRE

Brian Epstein, Manager, Network and Security, Institute for Advanced Study

In 2018, Transport Layer Security became a requirement for major browsers, and 87% of higher ed schools comply. We'll explore how this technology works, where it came from, and where it's going. You'll learn about symmetric and asymmetric cryptography an experience a hands-on walkthrough of RSA and Elliptic Curve cryptosystems. We'll also break apart certificates and talk about trust and deployment of certificates with the OpenSSL command-line tool. You'll leave with an in-depth model of how the technology works and hands-on experience of how to deploy it within your environment.

Outcomes: Discover how asymmetric cryptography works with RSA and ECC • Understand how the PKI trust model works with certificates • Learn how to use the OpenSSL tool to deploy certs in your environment

Security Architecture and Design

Securing and Supporting Research Projects: Facilitation Design Patterns

VEVEY 4, SECOND FLOOR EVENT CENTRE

Michael Corn, CISO, and **Cyd Burrows-Schilling**, Research Facilitator, University of California San Diego

This workshop will help prepare security professionals to support sponsored research projects. It provides an overview of how research operates within Universities; teaches facilitation skills for working with faculty; and provides guidance on how to develop a project specific security plan that meets the requirements of NSD, DoD, and other sponsoring organizations. Working with actual researchers, participants will learn to navigate the gap between the traditional top-down approach to security and the practicalities of everyday research lab infrastructures. This workshop is organized by the ResearchSOC project (researchsoc.iu.edu–NSF award 1840034). The ResearchSOC project is focused on bringing together the diverse information security and research communities by fostering the mutual understanding of perspectives.

Outcomes: Understand how research projects differ from classic enterprise administrative environments • Obtain facilitation skills for working with faculty and researchers • Learn how to use specific tools and templates designed for working with research projects

Security Awareness, Communications, and Training

Know Which Way the Wind Blows: Security Awareness that Soars

ST. GALLEN 2–3, SECOND FLOOR EVENT CENTRE

Tara Schaufler, Information Security Awareness and Training Program Manager, Princeton University; **Ben Woelk**, ISO Program Manager, Rochester Institute of Technology

Understanding the prevailing winds of technological and societal change helps us craft a security awareness program that is meaningful and prepares our user community for change. Creating a security awareness program that harnesses the changing winds is critical to ensuring that your community is ready for rapidly evolving threats and technologies. Join the presenters as they take you through the steps needed to create a strategic awareness program, drawing on a variety of engagement strategies that promote confidence in our user communities and equip them to recognize and respond to current and future threats.

Outcomes: Understand key elements and considerations in creating a security awareness plan • Complete a high-level plan and identify specific deliverables for selected topics • Identify appropriate metrics for evaluating effectiveness

2:30–3:00 p.m.

☕ Refreshment Break for Preconference Workshop Participants

Sponsored by Attain

FOYER, SECOND FLOOR EVENT CENTRE

4:45–5:30 p.m.

Welcome and Orientation for First-Time Attendees

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Jesse Bowling, Security Architect and CSIRT Program Manager, Duke University; **Jacqueline Pitter**, CISO/Senior Network Administrator, Reed College

The 2019 Security Professionals Conference Program Committee would like to welcome all first-time attendees (or anyone new to the higher ed information security community) to this short and informative orientation session. Learn how to navigate the conference program and take advantage of the many networking and community-building opportunities while you're in Chicago. You'll also discover how to become more involved in this ever-growing community of information security and privacy professionals. Bring your questions and leave prepared to get the most out of this conference!

5:30–6:45 p.m.

☕ Happy Hour Meet-Up Reception hosted by Deloitte, Silver Partner

MONTREUX, SECOND FLOOR EVENT CENTRE

Deloitte invites you for drinks, snacks, and conversation around many security topics that matter to you, such as the importance of identity and access management, compliance, and risk management at colleges and universities. Come and discuss these topics and more with specialists from our Higher Education practice.

☕ Happy Hour Meet-Up Reception hosted by Identity Automation

VEVEY 1–2, SECOND FLOOR EVENT CENTRE

Join Identity Automation to eat, drink, relax, and connect. With savory snacks and good company, it's the perfect way to wind down the day and discuss the most important topics to you with IAM experts in the field of higher education. We can't wait to see you here!

☕ Happy Hour Meet-Up Reception hosted by Tanium

ST. GALLEN, SECOND FLOOR EVENT CENTRE

Join Tanium and Palo Alto Networks in the Windy City for breezy beverages and light (and not so light) snacks. Network with industry leaders about your institution's security hygiene programs and protecting your faculty and student networks. Guests will have a chance to win a pair of Apple AirPods.

8:00–10:00 p.m.

Birds-of-a-Feather Sessions (BOFs)

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Join colleagues this evening to discuss hot topics in an informal setting. You'll be able to network and exchange ideas, insights, and experiences.

- **Edward Aractingi**, Associate Vice President for Information Technology and CIO, Marshall University
- **Sarah Bigham**, Lead Security Analyst, REN-ISAC
- **Jesse Bowling**, Security Architect and CSIRT Program Manager, Duke University
- **Dan Boyd**, Director of Information Security, Berry College
- **Mark Bruhn**, Peer Assessment Engagement Manager, Indiana University
- **Andrea Childress**, Executive Director ITS, University of Nebraska
- **Florence DiStefano Hudson**
- **Curtis J. Kappenman**, Security Compliance Officer, Anderson University
- **Carlos S. Lobato**, IT Compliance Officer, New Mexico State University
- **Helen Patton**, Chief Information Security Officer, The Ohio State University
- **Bryce Porter**, Chief Information Security Officer, University of North Carolina at Greensboro
- **Bill Rodriguez**, Senior IT Security Engineer, Rollins College
- **Stefan Wahe**, Deputy Chief Information Security Officer, University of Wisconsin–Madison

Blended-Threat Workshops (Sarah Bigham)

REN-ISAC is offering a series of blended-threat workshops for the higher education community. Participants from many areas of campus are encouraged to attend—from campus policy to IT to communicators and administrators. In this tabletop-like exercise, we'll create a final report to capture lessons learned.

Building Collaboration (Curt Kappenman)

Building a network of professionals who meet regularly to discuss threats, technological advancements, and successes and failures of methods to help protect our institutions is the first step in creating a collective of minds to help us as individuals and as a community to face the challenges that are yet ahead.

Cybersecurity Needs and Partnering with Researchers to Fill the Gaps (Florence Hudson, Helen Patton, Ed Aractingi)

The NSF Cybersecurity Center of Excellence at Indiana University—under the Cybersecurity Transition to Practice (TTP) program—will share cybersecurity needs identified by research, education and industry interviews in 2018. Attendees will be able to provide input and discuss the opportunity to leverage cybersecurity research to fill those gaps.

Funding Fun and Flaws (Stefan Wahe)

Join us to share and hear the tips, tricks, and pitfalls of acquiring the funding needed to secure your campus.

Governance, Risk, and Compliance (Andrea Childress)

We'll discuss GRC-specific areas of responsibility including policy, compliance, risk assessment, and program management. Learn how institutions are using GRC tools and partnering with stakeholders to develop and implement policy.

New/First Year CISO (Bryce Porter)

Are you a new CISO at your institution who is struggling to transform a program but not quite sure if your struggles are unique, or if you are employing the right strategies and choosing the right priorities? Let's meet BOF-style to share ideas and talk about our experiences thus far, including the common Information Security needs of our institutions. You'll be encouraged to share your unique perspectives on the challenges you're experiencing, the strategies you're pursuing, and the priorities you're setting as you seek to take your institution's information security program to the next level.

One-Person Information Security Departments (Dan Boyd, Bill Rodriguez)

Discuss strategies useful to single FTE InfoSec departments. Budgeting, responsibilities, operational vs. oversight/executive approach, and strategies for implementing change are all on the table.

Peer Assessment Services (Mark Bruhn)
In 2018 REN-ISAC introduced a peer assessment service available to all higher ed institutions (not just REN-ISAC members). Learn more about this cost-recovery service, which provides a highly professional review of IT security services, procedures, and/or policies of the institution's choosing, with assessments performed by peers within higher education.

Security vs. Privacy vs. Compliance (Carlos Lobato)
There appears to be overlap in responsibility among these functions. Working together could result in tremendous benefits to the institution. Is there a trend to merge all of these functions under either a CISO or CPO?

Threat Intelligence (Jesse Bowling)
We'll discuss the current state of threat intelligence sharing and use in higher education, including areas such as tooling, processes, metrics/outcomes, and more.

Tuesday, May 14

7:00 a.m.–5:00 p.m.

Registration Desk Open

REGISTRATION DESK, SECOND FLOOR EVENT CENTRE

7:15–8:00 a.m.

☕ Breakfast

Sponsored by Cirrus Identity
ZURICH BALLROOM D-G, FIRST FLOOR EVENT CENTRE
Join colleagues to eat breakfast and network informally.

8:00–9:00 a.m.

Cyberthreat Intelligence

Start Generating Threat Intelligence in 3 Easy Steps!

MONTREUX, SECOND FLOOR EVENT CENTRE
Jesse Bowling, Security Architect and CSIRT Program Manager, Duke University

Duke has embarked on a mission to help lower the bar on automated threat intelligence sharing across higher education institutions under the umbrella project STINGAR (Shared Threat Intelligence for Network Gatekeeping and Automated Response). The goals of STINGAR are to enable organizations (especially in higher education) across a wide range of technical, operational maturity, and budget resources to collect, analyze, action, and share threat intelligence. Given the types of challenges that face even a single organization in achieving these goals, our goals may appear lofty, but we believe we have developed a path to help organizations achieve them.

Outcomes: Understand the goals of the STINGAR project • Experience a live installation of STINGAR components • Learn how to start using intel at your institution

Governance, Risk, and Compliance (GRC)

Clearing Skies: Managing Risk in the Cloud

VEVEY 4, SECOND FLOOR EVENT CENTRE
Shelley Rossell, Network Security Officer, University of Chicago

We'll describe our experience in extending our security program, both nontechnical and technical, to IaaS cloud solutions, particularly to Amazon Web Services and, to some extent, GCP. We'll cover our central IT cloud IaaS strategy as well as how to manage the proliferation of this activity outside of central IT. Topics will include our challenges, solutions, lessons learned, and how risk is driving decisions on where to spend scarce resources to improve our IaaS cloud-security posture.

Outcomes: Learn how to adapt your on-premises security program to an IaaS solution like AWS • Examine a risk-based approach to managing the proliferation of IaaS outside of central IT • Explore methods of implementing some technical and nontechnical security controls within an IaaS environment

Identity and Access Management

Implementing Role-Based Access Control at Michigan

VEVEY 1–2, SECOND FLOOR EVENT CENTRE
DePriest Dockins, Director, Identity and Access Management, and **Aimee Lahann**, Intermediate Project Manager, University of Michigan–Ann Arbor

The University of Michigan is transforming how permissions in systems and access to data are granted, maintained, and revoked. Currently, access to resources is often managed manually on a service-by-service basis. By introducing automated provisioning, user accounts can be immediately created or modified with the correct permissions for an individual to perform a job. This change will improve compliance, reduce administrative costs, and improve the user experience. Join us for an interactive conversation and hear how we plan to implement role-based access control. Also, learn how an identity governance tool can be leveraged.

Outcomes: Explore a comprehensive process for acquiring an identity governance tool • Learn how business and technical roles are developed and maintained • Learn best practices for implementing in role-based access control in a university setting

Security Awareness, Communications, and Training

Before and After: Strategies for Increasing Engagement During Cybersecurity Training

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE
Louise Flinn, Trainer and Graphic Designer, North Carolina State University

Cybersecurity training for employees and students is essential, but our users often see it as perfunctory, boring, or irrelevant. NC State's Office of Information Technology is increasing engagement during cybersecurity training sessions by incorporating storytelling, statistics, and active learning exercises while covering topics like phishing, two-factor authentication, and other essentials. We'll demonstrate before-and-after examples that show the shift from a straight lecture to an active training session and easy-to-implement tactics. You'll have the opportunity to do a minimakeover of your own materials.

Outcomes: Experience the difference between a high-engagement and low-engagement delivery through before/after examples • Transform your own trainings to engage learners by applying specific strategies shared

Security Operations and Engineering

Is Weird Really Weird? Parsing weird.log to Build Healthier Network

ST. GALLEN, SECOND FLOOR EVENT CENTRE

Fatema Bannat Wala, Security Engineer, University of Delaware

Bro (now Zeek), an open-source network analysis framework, produces lots of interesting log files based on network activity. One of these logs is the "weird.log" file, in which Bro/Zeek logs interesting activity that is not categorized as normal according to the TCP/IP protocol standards. This talk will present the research done on different weird notices flagged in the network traffic at the University of Delaware, and whether those flags were really weird or just network misconfigurations. We used Bro/Zeek's weird.log file to do analysis/troubleshooting of the network, resulting in some weird classification as normal/interesting for our environment.

Outcomes: Learn how to analyze, classify, and possibly remediate weird activity • Understand the types and cause of weird activity in your network • Learn to use Bro IDS as a tool to identify and correct network problems, apart from the conventional IDS use

Strategic Leadership, Professional/Organizational Development, and Personnel Management

Evolving the Art of Recruiting and Hiring in Information Security

VEVEY 3, SECOND FLOOR EVENT CENTRE

Lanita Collette, Chief Information Security Officer, The University of Arizona; **Christian Hamer**, CISO, Harvard University; **Brad Judy**, Information Security Officer, University of Colorado System; **Helen Patton**, Chief Information Security Officer, The Ohio State University; **Stefan Wahe**, Deputy Chief Information Security Officer, University of Wisconsin–Madison

Do you face tough competition for talent? Are you trying to be inclusive in hiring practices? Building great teams through effective hiring practices is one of our most important responsibilities. This engaging panel session will build from five perspectives to provide a variety of actionable ideas to improve and optimize recruiting and hiring. Five schools come together in this panel to discuss their work to improve information security recruiting and hiring practices. We expect robust discussion and interaction, so bring your questions and challenges.

Outcomes: Explore how different goals drove different approaches • Learn techniques that can be immediately applied to recruiting and hiring practices • Engage panelists with your own hiring challenges and receive feedback and suggestions

9:15–10:15 a.m.

GENERAL SESSION

Analyzing the Chemistry of Data

Sponsored by Fischer Identity, Silver Partner

ZURICH BALLROOM D-G, FIRST FLOOR EVENT CENTRE

Wendy Nather, Head, Advisory CISOs, Duo Security

Security is difficult because data is not static. Even apart from its measurable qualities—format, content, length, and so on—it has meaning. Data can change its security requirements in the blink of an eye, as soon as a business decision is made with it or the minute it's combined with different data. And at this point in our society's evolution, data is becoming an increasingly dangerous, explosive mixture. In this talk, we'll explore the chemistry of data and what we must still discover about it if we want to use it safely.

10:15 a.m.–6:00 p.m.

Corporate Displays

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.

Corporate Displays

ZURICH BALLROOM FOYER, FIRST FLOOR EVENT CENTRE

Cyber Threat Intelligence

FireEye

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant consulting. FireEye eliminates the complexity and burden of cybersecurity for academic organizations struggling to prepare for, prevent, and respond to cyberattacks.

SpyCloud

SpyCloud is the leader in account takeover (ATO) prevention. We help institutions of all sizes mitigate account takeover by proactively remediating account exposures for students and faculty in an automated way. We accomplish this through our award-winning ATO prevention solutions powered by a world-class team of security researchers and technology.

Governance, Risk, and Compliance (GRC)

Deloitte, Silver Partner

Deloitte's Higher Education practice can help higher education institutions become more diligent and deliberate in being secure and resilient, focusing on policies and controls to prevent the compromise of their most risk-sensitive assets and operations. We can help achieve the fundamentals faster, by leveraging our engagement accelerators, extensive industry experience, and deep cyberrisk domain knowledge to safeguard risk-sensitive assets and operations. Learn more at www.deloitte.com/us/higher-ed-cyber-security.

Quest Software

No matter where—on premises, cloud, or hybrid—Quest is your go-to expert to help move, manage, and secure your most critical Microsoft platforms so you have more time to drive innovation forward.

Salty Cloud

Salty Cloud provides workflow automation solutions for security/risk teams and was created in the InfoSec trenches at UT Austin and Georgia Tech for real and acute pain points. Our products are for higher education, by higher education and include questionnaire-based security/risk assessments, asset classification, vendor assessments, credential management, antiphishing, and the popular Dorkbot service.

San Diego Supercomputer Center

SDSC Health Cyberinfrastructure Division's Sherlock Cloud platform was established to provide managed services to meet the secure computing and data management needs of our academic, government, and industry partners. It offers a multitude of high-touch, value-added turnkey solutions that span secure cloud computing, big data management, data science, and analytics.

WTC Consulting

Our information security assessment provides six key elements: (1) inventory of security services provided by the central IT organization, (2) assessment of central IT staffing levels, (3) identification of gaps and vulnerabilities in the IT security environment, (4) assessment of security policy and practices, (5) security and user awareness training recommendations, and (6) estimated costs.

Identity and Access Management

Fischer Identity, Silver Partner

The Fischer International Identity mission is simple: your success. We make identity governance and administration work for your organization, technically and financially. We never stop innovating or evolving. We are never satisfied because we know we can make IGA easier. Fischer Identity is the last IGA product you will ever need.

Identity Automation

Identity Automation helps organizations embrace security, increase business agility, and deliver an enhanced user experience with RapidIdentity, the most complete identity, access, governance, and administration platform available.

LastPass

LastPass provides secure password management to reduce the risk of breach and remove employee password frustration. With secure password sharing, customizable policies, and comprehensive user management, LastPass gives businesses of all sizes the tools to create an enterprise security posture. Founded in 2008, LastPass is a product of LogMeIn.

Moran Technology Consulting, Gold Partner

Moran Technology Consulting provides IT management and technology consulting to higher education clients, including IAM strategic planning, vendor selection, architecture, and implementation; Active Directory security assessments and secure (re)design; and IT security assessments and security program implementation.

Painless Security

Painless Security offers Jisc Liberate in North America. Liberate is a fully managed cloud solution that gives you access to the InCommon Federation, eduroam, and a Shibboleth-based web proxy in an easy-to-configure service. With Liberate, you can save time and money, reduce risk, and eliminate the need for specialized in-house expertise.

Incident Management and Response

Best Practical Solutions

Best Practical Solutions develops and maintains Request Tracker (RT) and Request Tracker for Incident Response (RTIR). RTIR was designed in collaboration with several global security organizations to enable security teams, CERTs, CSIRTS, and similar types of groups to manage and respond to network and security incidents for their organizations.

Corelight

Come to Corelight's table to learn why network security monitoring is your best next move and how it can dramatically accelerate your average incident response times and unlock new threat detection and threat hunting capabilities.

CrowdStrike

CrowdStrike is the leader in cloud-delivered endpoint protection, going beyond traditional antivirus to provide complete protection. Our cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed. CrowdStrike's ultimate goal is to help customers stop breaches immediately, with minimal time, effort, and impact on their processes.

EdgeWave

EdgeWave delivers unparalleled inbox protection from today's exploding messaging threats like phishing, spoofing, BEC, and more. At the core of our email security solutions is ThreatTest, an automated inbox detection and response solution that uses machine learning and expert human review to quickly catch, analyze, and resolve suspicious emails.

Rapid7

TBD Organizations around the globe rely on Rapid7 technology, services, and research to securely advance. The visibility, analytics, and automation delivered through our Insight cloud simplifies the complex and helps security teams reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Learn more at www.rapid7.com.

Yakabod

Built for higher ed, CISOBox delivers efficient, secure information security incident management through intelligence agency–accredited technology. Universities use CISOBox to isolate and secure sensitive incident data, documentation, and communication; generate critical metrics; and gain NIST 800-61r2 compliance. CISOBox's new security review management application offers efficient handling of vendor assessments, too.

Security Architecture and Design

Symantec Corporation

Symantec Corporation, the world's leading cybersecurity company, helps organizations, governments, and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, the cloud, and infrastructure. For more information, please visit www.symantec.com.

Security Operations and Engineering

Forescout Technologies

Forescout is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environments and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, 100% real-time and continuous discovery and classification.

Strategic Leadership, Professional/Organizational Development, and Personnel Management

TDI Security

Having experienced the challenges and complexities associated with managing cybersecurity for multiple organizations firsthand, we knew there had to be a better way. CnSight is an innovative and practical solution providing situational awareness for leaders to help them truly understand and improve the effectiveness of their cybersecurity.

Corporate Displays

FOYER, SECOND FLOOR EVENT CENTRE

Cyber Threat Intelligence

Cisco Systems, Gold Partner

Cisco Security enables organizations to gain more empowered security, so they focus on what they do best. With our integrated security portfolio, organizations stay safer and respond faster while teams do more, and resources go further. As enterprise IT pioneers, it is our job to secure IT, something we do better than anyone.

Fortinet

Fortinet provides top-rated network and content security, as well as secure access products that share intelligence and work together to form a cooperative fabric. Our unique Fortinet Security Fabric delivers broad protection and visibility to every network segment, device, and appliance, whether virtual, in the cloud, or on premises.

Governance, Risk, and Compliance (GRC)

Spirion

Spirion is the leader in the rapid discovery, accurate classification, and automated protection of sensitive data across your network and public cloud. Spirion provides enterprise data management software to help businesses reduce their sensitive data footprint and proactively minimize the risks, costs, and reputational damage of successful cyberattacks. Visit www.spirion.com.

Identity and Access Management

Splunk

Splunk turns machine data into answers. Organizations use market-leading Splunk solutions with machine learning to solve their toughest IT, Internet of Things, and security challenges. Join millions of passionate users and discover your aha moment with Splunk today: www.splunk.com.

10:15–11:00 a.m.

☕ Refreshment Break and Corporate Displays

ZURICH BALLROOM FOYER, FIRST FLOOR EVENT CENTRE, AND FOYER, SECOND FLOOR EVENT CENTRE

11:00 a.m.–12:00 p.m.

Cyberthreat Intelligence

FBI and REN-ISAC Threat Briefing

MONTREUX, SECOND FLOOR EVENT CENTRE

Naomi Latt, Computer Scientist, Federal Bureau of Investigation; **Kim Milford**, Executive Director, REN-ISAC, Indiana University

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 and the FBI can share. We will discuss threats, trends, and ideas that we can't even imagine at the time of this proposal. 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.

Outcomes: Understand the broader threat landscape and the impact on research and higher education • Direct your defense and response resources with clearer vision • Assess the current risks to your institution

Governance, Risk, and Compliance (GRC)

Recovering from a Class-Action Lawsuit: 7 Years Later

VEVEY 4, SECOND FLOOR EVENT CENTRE

Sandra K. Furuto, Director, Data Governance and Operations, University of Hawaii System Office; **Jodi-Ann Ito**, Chief Information Security Officer, University of Hawaii at Manoa

In 2011, the University of Hawaii System was served with a class-action lawsuit as a result of several data breaches on multiple campuses. Join the university's data governance director and CISO as they recount their journey over the last seven years building the institution's data governance and information security programs to intended to increase the university's security posture, heighten awareness, and reduce the risk of exposure of the institution's sensitive information and avoid another lawsuit. Bring your grit, fortitude, and focus and join the journey.

Outcomes: Review our lessons learned • Learn about the collaboration and partnerships that you need to achieve a robust data governance and information protection program • Develop your data governance and information security roadmap

Identity and Access Management

MFA Usage in Higher Education

VEVEY 1–2, SECOND FLOOR EVENT CENTRE

RuthAnne Bevier, Chief Information Security Officer, California Institute of Technology; **Alan Bowen**, Chief Information Security Officer, Franklin & Marshall College; **Shana Bumpas**, Director of Information Security, University of Richmond; **Nick Lewis**, Program Manager, Security and Identity, Internet2; **Roger Safian**, Lead Security Analyst, Northwestern University; **Doug Streit**, Director, IT Security and Planning, Old Dominion University

Gale force winds of change are pushing higher education to deploy multifactor authentication throughout their environments and the community. Higher education has reacted and deployed MFA across the campus community. This panel session will include speakers from campuses deploying MFA on their campuses. The panelists will talk about their campus deployments, populations affected, options used, integrations, and future plans for their campuses.

Outcomes: Understand MFA usage in higher education • Hear how institutions are using MFA to improve their information security programs

Security Awareness, Communications, and Training

Say Yes to Creative Cybersecurity: See, Say, and Do Together

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Erika Powell-Burson, CISO, Bentley University

Consider new possibilities for your role, your people, and your program by way of visualization, communication, and appropriate action to reduce risk and fulfill your purpose(s). There are several steps between you, risk reduction, and goal accomplishment. This session assumes that you know the cybersecurity best-practice basics. We will explore positive and colorful methods to visualize, connect, create, and ultimately protect your most valuable assets. Unlocking and developing creative thinking in you and others helps ensure interest in and commitment to protections.

Outcomes: Visualize your strengths and gaps in context of your program and university needs (see it) • Connect with supporters and advocates and move your program forward (say it) • Create campaigns and implement successful policies and controls collaboratively (do it)

Security Operations and Engineering

Ask Better Questions About Your Network with Nmap Scripting Engine

ST. GALLEN, SECOND FLOOR EVENT CENTRE

James Clark, Director of Information Security, University of Chicago

Nmap is a free and open-source tool used for network and service discovery, auditing, inventory, monitoring, and more. The Nmap Scripting Engine (NSE) is a framework allowing anyone to extend the built-in functionality by writing small but powerful scripts. This session will describe the range of possible uses of NSE, demonstrate how to use any of the many published scripts, and then demonstrate how to customize and write entirely new scripts. The ultimate goal is to show you how to translate sophisticated questions about your network into functional Nmap queries that provide immediate, actionable results.

Outcomes: Learn what types of questions you can ask using Nmap scripting engine • Learn how to use publicly available Nmap scripts and libraries • Learn how to write custom Nmap scripts

Strategic Leadership, Professional/Organizational Development, and Personnel Management

David and Goliath: Small and Large Institution Information Security Collaboration

VEVEY 3, SECOND FLOOR EVENT CENTRE

Lanita Collette, Chief Information Security Officer, and **Tina Thorstenson**, Assistant Vice President and Chief Information Security Officer, Arizona State University; **Sean Hagan**, Chief Information Security Officer, Yavapai College; **Michael W. Zimmer**, Director of Information Security, Northern Arizona University

Higher ed institutions often embrace collaboration and knowledge sharing, but does that extend to your information security program? Will you collaborate with institutions much larger or much smaller than your own? In this session, you'll learn how four schools of very different sizes and with very different resources work together, both directly and indirectly, to derive value and share unique institutional knowledge and capabilities for the collective benefit of all.

Outcomes: Identify requirements and key considerations for establishing a multi-institution working group • Evaluate different methods for information sharing • Discuss specific examples of beneficial information sharing • Consider other potential sharing partners and benefits

12:00–1:00 p.m.

Lunch

Sponsored by BerryDunn

ZURICH BALLROOM D-G, FIRST FLOOR EVENT CENTRE

Join colleagues to eat lunch and network informally.

1:00–2:00 p.m.

Cyberthreat Intelligence

Automating IT Security: Letting Security Analysts Be Analysts

MONTREUX, SECOND FLOOR EVENT CENTRE

Stephen Huff, Security Analyst, Virginia Tech

The tools and appliances available within the IT landscape have expanded the analysis and monitoring capabilities available to IT security personnel. However, these tools (FireEye, Nessus, Rapid7, Bro/Zeek and Kibana) rarely integrate with each other. We'll share how the Virginia Tech IT Security Office has developed several web applications that leverage the APIs of these security appliances, Google Drive, and ServiceNow to provide connective tissue and eliminate data entry and tedium whenever possible. Audience participation will be encouraged so that IT automation strategies, tips, and lessons can be shared and brainstormed.

Outcomes: Learn about the benefits of IT automation and integration between security appliances and incident response and notification systems • Hear from other universities and discuss strategies for automation and management buy-in • Deep dive into key API code examples, followed by a demonstration of how to integrate tools

Governance, Risk, and Compliance (GRC)

What the HECVAT! Driving the Winds of Change

VEVEY 4, SECOND FLOOR EVENT CENTRE

Jon Allen, Chief Information Security Officer and Interim CIO, Baylor University; **Joshua Callahan**, Information Security Officer and CTO, Humboldt State University; **Susan Coleman**, Indiana University Bloomington; **Nick Lewis**, Program Manager, Security and Identity, Internet2; **Charles Escue**, Extended Information Security Manager, Indiana University

Cloud vendor security assessments continue to be a hot topic for information security, and the winds of change are only driving us to move faster than ever before. The Shared Cloud Security Assessment Working Group updated the Higher Education Cloud Vendor Assessment Tool (HECVAT) and developed additional resources in 2018, based on community input. In 2018, an analyst report, summary report, and automated scoring were integrated into the HECVAT, supporting improved decision support. We'll go over the updates from 2018, community adoption, plans for 2019, and use cases and provide feedback to the working group.

Outcomes: Gain an understanding of the HECVAT and its advantages • Hear how institutions are using the HECVAT to improve their vendor assessments • Get a community update on the status of the working group

Identity and Access Management

Auditing and Deploying Next-Gen Campus Access, ID, and Payment Systems

VEVEY 1–2, SECOND FLOOR EVENT CENTRE

Barton Lawyer, Assistant Director, IT, and **Nicholas Tripp**, Senior Security Analyst, Duke University

What does it take to develop and secure a new format for ID systems on a large university campus? This session will provide a retrospective look at Duke's work with Apple and Blackboard to move student IDs to iOS and watchOS devices. We'll discuss performing security audits of Duke's existing ID systems and disclosing vulnerabilities discovered in those systems to campus leadership. We'll also cover the security architecture of the new Apple Wallet–based system while reviewing lessons learned from our deployment.

Outcomes: Understand the benefits of tokenized virtualized identification/access control/payment systems over traditional solutions in a university environment • Learn how to perform auditing of production systems on your campus • Identify important questions to ask when deploying a new campus card system

Security Awareness, Communications, and Training

Influencing a Security Culture: From Community College to Ivy League

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Patricia M Clay, Chief Information Officer, Hudson County Community College; **David Sherry**, Chief Information Security Officer, Princeton University

Oh no, not another awareness session! While the answer to that is yes, this will not be your typical session on security awareness. You'll hear ideas and solutions to engage your community, no matter your institution's size, Carnegie designation, or whether it's public or private. The presenters believe in this mission and have witnessed great success in their awareness journeys that will be of benefit to all. Sure, they are both from New Jersey, but don't hold that against them.

Outcomes: Learn a new method of outreach • Learn how to schedule a new event to engage with new university members • Plan a new awareness event to consider for the upcoming year

Security Operations and Engineering

After the Storm: Rebuilding and Strengthening Defenses

ST. GALLEN, SECOND FLOOR EVENT CENTRE

Michael Grinnell, Deputy CISO, University of Virginia

After weathering a security typhoon in 2015, the University of Virginia rebuilt core infrastructure and embarked on a three-year program with 36 projects and initiatives to improve information security. Learn from our successes and challenges in implementing multiple concurrent security products and changes in a decentralized university environment. We'll cover policies, MFA, server and endpoint security, log correlation, phishing simulations, user-awareness training, and network protections: there's something for everyone!

Outcomes: Learn successful strategies for implementing a multiyear security improvement program • Prioritize security technologies and approaches • Understand how to manage multiple simultaneous security changes affecting the entire institution

Strategic Leadership, Professional/Organizational Development, and Personnel Management

Women in Information Security: Where Are They?

VEVEY 3, SECOND FLOOR EVENT CENTRE

Sarah Braun, Assistant Information Security Officer, University of Colorado System; **Laura Heilman**, IT Security Analyst Specialist, University of Georgia

We all know that biases, barriers and cultural norms affect recruiting and retaining women in Information Security. Change has to happen to create an inclusive community of practice. Using their own experiences as a basis, two women share their perceptions of what we all need to do to support and encourage women to choose a career in Information Security. Learn about common barriers and explore strategies that any Information Security professional can use to respectfully initiate beneficial cultural change.

Outcomes: Identify challenges that may impact women in information security at your institution • Describe how these challenges to women can affect your institution • Discuss possible strategies to overcome those challenges

2:00–2:45 p.m.

☕ Dessert, Refreshment Break, and Corporate Displays

ZURICH BALLROOM FOYER, FIRST FLOOR EVENT CENTRE

2:45–3:45 p.m.

Governance, Risk, and Compliance (GRC)

Questionnaire-Based Risk Assessments at Scale

MONTREUX, SECOND FLOOR EVENT CENTRE

Cam Beasley, Chief Information Security Officer, University of Texas at Austin; **Andrew Scheifele**, Co-Founder and CEO, Salty Cloud

Collecting and managing risk-related information across a federated university environment can involve hundreds of separate org units and thousands of end users, not to mention third-party vendors. Spreadsheets are not a sustainable solution at scale, and most GRC solutions are not flexible enough to efficiently collect information needed. UT Austin leverages technology for end-to-end workflow management for questionnaire-based assessments: they collate questions, send notifications, collect and analyze responses, and generate reports. ISORA allows UT Austin to quantify their risk and measure continuous improvement of their overall security posture over time, assessing on-campus and vendor risk.

Outcomes: Understand risk-assessment needs across a large university campus • Discuss workflow automation solutions that more efficiently collect, collate, and analyze risk information • Learn about streamlined third-party vendor risk-assessment collection and analysis

Incident Management and Response

Endpoint Protection: When, How, and Why to Evaluate New Solutions

VEVEY 1–2, SECOND FLOOR EVENT CENTRE

Mark DeDomenic, Assistant Information Security Officer for Security Operations, Old Dominion University; **Kelly Housman**, Senior Sales Engineer, CrowdStrike

Determining the best practices in software evaluation can be difficult in a constantly evolving market. In this session, we'll discuss the various steps Old Dominion University took to ensure they chose the best solution for their situation, address industry trends, and answer your questions about the next steps you can take to stop breaches.

Outcomes: Identify when to evaluate new endpoint protection solutions • Navigate the current solutions market • Learn more about solutions for higher ed institutions

Security Operations and Engineering

Connecting the Dots with Zeek (Bro)

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Vincent Stoffer, Senior Director, Product Management, Corelight; **Nicholas Turley**, Security Architect, Brigham Young University

The ability to connect the dots when responding to security incidents and threat hunting is vital to the success of cybersecurity teams. We face challenges of security tools failing to integrate, failing to correlate, and failing to tell the story. University systems are rich with security data but are often underutilized due to difficulties in integrating and conducting analytics. BYU is tackling this challenge by building an event-driven microservices architecture with a focus on orchestration, rapid integrations, and contextual enrichment. We will focus on how data-rich network security platforms such as Zeek and Corelight can be used to connect the dots, tell the story, and massively reduce the time to incident resolution and threat detection.

Outcomes: Learn about unique ways Zeek can be used as more than just an intrusion-detection system • Understand the purpose of event-driven microservices architectures in SecOps • Learn about the importance of contextual enrichment and correlation in operational threat hunting

Securing the Connected Campus

ST. GALLEN, SECOND FLOOR EVENT CENTRE

Kenneth Compres, CISO, Hillsborough Community College; **Chris Dullea**, Engineering Manager, Forescout Technologies

This session will address how Hillsborough Community College deployed an enterprise-wide network device visibility and control platform to offer users secure wired and wireless network access with minimal disruption while mitigating risk and meeting compliance requirements. Hear how HCC is able to continuously identify and secure all devices on campus networks on connection without the need of an agent to ensure device compliance. In addition, learn how Hillsborough has been able to realize more value out of existing security investments through orchestration with the device visibility and control platform.

Outcomes: Learn how to reduce risk of security incidents and breaches • Learn how to ensure security compliance • Learn how to improve security operations productivity through automation and orchestration

Vulnerability Management: Myths and Solutions

VEVEY 3, SECOND FLOOR EVENT CENTRE

Jason Edelstein, IT Risk and Compliance Program Manager, University of Chicago; **Sherif Hassabo**, Information Security Engineer, University of Chicago; **Eric Reiners**, CIO, Rapid7

Vulnerability management: a never-ending slog or a mainstay of modern information security? When time is precious, budgets are tight, and priorities are shifting, is vulnerability management the right investment? What kind of vulnerability management should you do? Authenticated scans, threat prioritization, sysadmins with questions, firewall rules, and a thousand other concerns loom behind a simple yes-or-no question. Join Rapid7 and the University of Chicago as we open the door wide on our partnership and confront the myths we dispelled, the discussions we had, and the choices we made for UChicago on how to build a sustainable program.

Outcomes: Clearly outline the principles of an enterprise-grade vulnerability management program • Get actionable insight on how to prioritize vulnerabilities, including metrics from across higher education • Discuss challenges to vulnerability management in a decentralized environment from a technical perspective, including firewall rules, credential management, and vulnerability classifications

4:00–5:00 p.m.

Tornado Talks in Ten

VEVEY 1–2, SECOND FLOOR EVENT CENTRE

Winston Armstrong, Chief Information Security Officer, San Diego Supercomputer Center; **Brandon Bailey**, Data Security Analyst, and **Ross Geerlings**, Senior Data Security Analyst, University of Michigan–Ann Arbor; **Craig Drake**, Information Security Engineer, University of Chicago; **Apurva Goenka**, Student Assistant, and **Daniel Quach**, Security Analyst, University of California San Diego; **Chris Gregg**, Associate Vice President of Information Security/CISO, and **Melinda Mattox**, Director of Security Operations, University of St. Thomas; **Sarah Noell**, Associate Director, Outreach, Communications, and Consulting, North Carolina State University

Talk 1: Cost-Effective Sensitive Data Discovery at Scale

Brandon Bailey and **Ross Geerlings**, University of Michigan–Ann Arbor

Sensitive data discovery is vital to organizations with regulated sensitive data. Unfortunately, leading commercial products are generally very pricey for a university budget, and existing free solutions by themselves are inadequate. The University of Michigan has built a solution to these common sensitive data discovery challenges that leverages a combination of custom, in-house developed, and inexpensive solutions.

Outcomes: Learn from the experiences of our team interacting with users across many different campus units • Gain an understanding of how to implement effective, inexpensive sensitive data discovery for your campus

Talk 2: RAEngine: Scoring, Prioritizing, and Automating Your Vulnerability Risk Assessment

Winston Armstrong, **Apurva Goenka**, and **Daniel Quach**, University of California San Diego

IT organizations and universities alike are dealing with risks and compromises on an ongoing basis. Unpatched vulnerabilities are one of the chief culprits causing compromise of systems. Sherlock’s standardized and automated approach to vulnerability risk management focuses equally on minimizing system downtime, maintaining customer satisfaction, and keeping systems secure.

Outcomes: Learn how to assess and score risks associated with vulnerabilities • Learn how to prioritize patches • Learn how to automate vulnerability risk assessment

Talk 3: Something You Have: A Microsoft MFA Success Story

Chris Gregg and **Melinda Mattox**, University of St. Thomas

We’ll describe how we deployed Microsoft’s multifactor authentication solution as a response to continuous phishing attacks at the University of St. Thomas. Since we were already licensed for Microsoft MFA through the existing campus agreement, we forged ahead. Using a combination of communication strategies and focusing on user experience, our campus-wide MFA implementation to over 28,000 accounts in eight months has led to a 99% reduction in compromised email accounts and a dramatic decrease in phishing and spam emails on campus.

Outcomes: Understand the nuances of how Microsoft MFA can be deployed at your university • Learn ways you can reduce phishing risks and still maintain user experience through an MFA deployment • Understand how to use data to demonstrate need for and track the eventual success of an MFA initiative

Talk 4: Reading SMTP Headers

Craig Drake , University of Chicago

Participants will learn to read the key elements of SMTP header information related to investigating phish, spam, and other email related security incidents. Beyond the standard header From, Recipient, Subject, etc., we will look at envelope details. You’ll learn to investigate the true origination of an email message and routing through SMTP servers on the way to its final destination. We will also touch on SMTP authentication details (i.e., SPF, DKIM, and DMARC), as well as additional header details added my email security filtering applications.

Outcomes: Be able to identify important header elements of an SMTP message • Follow the routing of an SMTP message • Read details like envelope information and email authentication

Talk 5: Taming the Wild West of Third-Party Apps in G Suite

Sarah Noell , North Carolina State University

Join us for a quick overview on how the Google Service Team at NC State is working to get a handle on the myriad of third-party apps currently in use in our G Suite domain. We’ll go over our approach and the processes we’ll be using to review/re-review these apps, including the partnerships with our Software Licensing and Security unit.

Outcomes: Understand what third-party apps are in Google • Identify risky permissions asked by third parties • Understand the potential impact of loose permissions and how to stay safer online

Governance, Risk, and Compliance (GRC)

Controlled Unclassified Information: It’s Not Just an IT Problem

VEVEY 4, SECOND FLOOR EVENT CENTRE

Doug Dodson, Research Data Security and Compliance Analyst, Office of the Vice President for Research, The Pennsylvania State University
Benjamin Rogers, Director of Research Services, The University of Iowa; **Preston Smith**, Director of Research Computing Services, Purdue University

During this session, panelists will discuss the “other” challenges with supporting controlled unclassified information (CUI) or other regulated research that are not the IT challenges—security controls, technology, or regulations. Topics will include the use of research facilitators dedicated to regulated research, building relationships between campus IT organizations, appropriate compliance offices, research administration, IRBs, and export control offices, as well as improving institutional processes. Ultimately the goal is to create a systematic approach that results in rapid flow from contracts to actionable technical requirements to implementation to approval, so that research data can begin in the minimum possible time frame.

Outcomes: Understand the different roles involved in a systemic CUI environment • Learn best practices to build a CUI ecosystem • Identify training opportunities by various administrative and IT roles associated with CUI handling

How an Audit Led to an Opportunity for Partnership

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Angela Neria, Chief Information Officer, Pittsburg State University; **Amanda Williams**, Information Security Officer, Pittsburg State University

You know those IT security audits that every state randomly performs on-site at state agencies each year? Well, Pittsburg State University in Pittsburg, Kansas, had the pleasure of enduring one of those last spring. What began as a routine audit was soon seen by our IT security officer and IT leadership as an opportunity to move the university in the right direction and not be the villain in the process.

Outcomes: Create an effective action plan to meet needed IT security improvements cited by an auditing body • Create an effective communication plan for campus IT team members, administration, and clients • Develop a culture of client partnerships versus policing

Incident Management and Response

It Just Got Real at Stanford! Tabletop Exercise to Live Response

MONTREUX, SECOND FLOOR EVENT CENTRE

Stacy Lee, Information Security Operations Specialist, and **Jeremy Tavan**, Information Security Systems Specialist, Stanford University

It's time to take your tabletop exercise to the next level and make it a live response exercise. We recently created an incident based on real-world cyberthreats that generated actual artifacts in our detection tools. We brought in 20 people from our ISO and IT orgs to investigate what happened by leveraging the actual tools we use in real incident response. Learn how to level up your teams by running them through analysis of real incidents, where everyone brings their own unique skills to bear on the challenge and has fun doing it.

Outcomes: Plan and create a hands-on live response exercise • Teach your ISO team to use existing tools and how to stay focused on objectives • Learn how to use the kill chain to guide your investigation

Security Operations and Engineering

SecOps Journey: From Use Cases Toward Automation

ST. GALLEN, SECOND FLOOR EVENT CENTRE

Eric Barnes, Associate Director, Information Security, and **Lorna Koppel**, CISO/Director of Information Security, Tufts University

Tufts has been on a journey to transform security operations that focuses on detection of and response to threats and on having the ability to conduct necessary research for a variety of situations. This talk will cover our lessons learned so far on the journey of mapping use cases to log sources, codifying operational processes, assessing the potential for automation and the SIEM tools and ecosystem to make this possible. We will also discuss transforming our team into our own internal SecDevOps model.

Outcomes: Learn an approach to develop value-added security operations through use cases • Explore rarely discussed concepts for a hybrid SIEM ecosystem and aligning use cases to necessary data sources • Identify key concepts for staffing, skills, internal SecDevOps, and potential sources of efficiency improvements using automation

Strategic Leadership, Professional/Organizational Development, and Personnel Management

Peer Cybersecurity Assessments: For and by Higher Education

VEVEY 3, SECOND FLOOR EVENT CENTRE

Mark Bruhn, Peer Assessment Engagement Manager, Indiana University; **Ryan Knutson**, Assistant Vice President for Technology, South Dakota State University

The REN-ISAC Peer Cybersecurity Assessment service is now active and has already provided three campuses with extensive objective advice from experienced peers. While managed by REN-ISAC, assessments are performed by teams of highly experienced CIOs and/or CISOs from various universities and colleges. Assigned assessors are seasoned professionals who have dealt with most if not all of what you are working through and can add objective advice to your efforts in the form of discussion, narratives, and actionable recommendations. Ryan Knutson (SDSU) will join Mark Bruhn (REN-ISAC) to discuss how the program works, SDSU's assessment experience, and answer questions.

Outcomes: Explore the REN-ISAC assessment service as a possible valuable component of a security strategy • Understand the benefits derived by one university that made use of the service • Hear an overview of some of the common specific problem areas seen across campus assessments

5:00–6:00 p.m.

☕ Reception

ZURICH BALLROOM FOYER, FIRST FLOOR EVENT CENTRE

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.*

6:00–7:00 p.m.

PGP Key Signing

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Don Becker, Senior Information Security Engineer, Adelphi University; **Ken Connelly**, Director, Information Security, University of Northern Iowa; **Brian Epstein**, Manager, Network and Security, Institute for Advanced Study

The annual PGP Key signing activity is open to all interested conference attendees. Additional information is available on the REN-ISAC website. Questions about this event should be directed to the presenters.

8:00–10:00 p.m.

Cybersecurity Awareness Escape Rooms—Join the Fun!

ZURICH BALLROOM D-G, FIRST FLOOR EVENT CENTRE

Linda Ludwig, Information Security Awareness Specialist, Grinnell College

Do you have what it takes to crack codes, discover clues, and solve puzzles? Escape rooms are a chance to share cybersecurity principles in a fun, engaging environment with students, faculty, and staff. During this session, groups of 4 to 10 participants can try to solve one of two escape rooms that were created for Grinnell College's 2017 and 2018 National Cybersecurity Awareness Month activities." So you want to be a spy" focuses on phishing, dangers of USB drives, and building strong passwords. “Can you hack it?” focuses on social engineering. You will have 40 minutes to solve your choice of either escape room. If time permits, you are free to tackle both!

8:00–11:59 p.m.

Get Your Game On!

Sponsored by Akamai Technologies

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Don Becker, Senior Information Security Engineer, Adelphi University; **Brian Smith-Sweeney**, Chief Information Security Officer, Columbia University

Join us for the seventh annual Security Professionals Conference game night! This is a great way to kick off the conference and help you get to know your fellow conference-goers in a relaxed atmosphere. No experience necessary; we’ll be sure to have something for everyone, 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!

8:00–11:59 p.m.

Lock Picking for InfoSec

ZURICH BALLROOM D-G, FIRST FLOOR EVENT CENTRE

Nathan Heald, Senior Security Consultant, and **John Michael Stitt**, Senior Security Consultant, Fraternal Order of Lock Sport

Keeping bad guys out of your network is important. So is keeping them out of your data center. Come learn how to evaluate the physical security of locks by picking them! The Fraternal Order of Lock Sport (http://www.bloomingtonfools.org) will teach you how to pick locks so you can decide for yourself what is and is not secure. It’s a fun learning environment reinforced with games and prizes!

Wednesday, May 15

7:15 a.m.–1:00 p.m.

Registration Desk Open

REGISTRATION DESK, SECOND FLOOR EVENT CENTRE

7:15–8:00 a.m.

☕ 2020 Program Committee Breakfast

By invitation only

CURRENTS, CONCOURSE LEVEL

7:15–8:00 a.m.

☕ Breakfast

Sponsored by Quest Software

ZURICH BALLROOM D-G, FIRST FLOOR EVENT CENTRE

Join colleagues to eat breakfast and network informally.

8:00–9:00 a.m.

Governance, Risk, and Compliance (GRC)

Cybersecurity Metrics: Leaders and Laggards

VEVEY 4, SECOND FLOOR EVENT CENTRE

Leo F. Howell, Chief Information Security Officer, University of Oregon

Kelvin said, “When you can measure what you are speaking about, and express it in numbers, you know something about it.” This presentation will serve as a stimulus to help us do just that— express cybersecurity in numbers—so that we can demonstrate that we know what we are talking about. We will explore some business drivers for cybersecurity metrics, as well as some old and new metrics that can help us tell the cybersecurity story. Metrics will be presented to help to demonstrate the effectiveness of a cybersecurity program, at all levels.

Outcomes: Learn the difference and impact of leading vs. trailing metrics • Identify value, community, operational, and advancement metrics for use on your campus • Obtain a framework and useful metrics for including in your own cybersecurity metrics program

Incident Management and Response

Threat Intel and IR Tools for Dummies: Real-Life Use Cases

MONTREUX, SECOND FLOOR EVENT CENTRE

Kevin Cheek, University Incident Response Lead, and **Matthew Coons**, Incident Responder and Threat Analyst, University of Michigan–Ann Arbor

Sometimes the hardest part of using a new tool is just getting started. We’ll walk you through our own experiences trying out and using some free and open-source threat intelligence, incident response, and forensics tools to detect and respond to real incidents that otherwise would have been much more difficult to handle. We’ll share our failures and wins, including how we’ve successfully leveraged open-source tools to exponentially increase our effectiveness as an IR team.

Outcomes: Learn how to automate threat intelligence, IR, and forensics tools • Understand how to leverage free tools that can be deployed easily by resource constrained teams • Learn how to implement threat intel, IR, and forensics tools in diverse situations, including cloud and decentralized environments

Security Architecture and Design

Going Passwordless at Stanford (Part II)

VEVEY 1–2, SECOND FLOOR EVENT CENTRE

Michael Duff, Chief Information Security Officer, Stanford University

Realizing our long-term vision of strong user authentication coupled with endpoint security posture enforcement at Stanford, last year we deployed the final component: client certificates that strongly authenticate both the user and the device. We'll describe the underlying systems and key design decisions while highlighting lessons we learned along our six-year journey. Join us to hear this rare story of dramatically improving security and user experience simultaneously and learn how you can replicate this success with a fraction of the resources. This is a continuation of last year's talk, with a focus on our deployment over the past year.

Outcomes: Understand the benefits of identity-aware, application layer endpoint security posture enforcement coupled with client certificate-based authentication • Learn how to architect the systems necessary to implement your own version of Stanford's Cardinal Key service • Explore the keys to a successful implementation and rollout along with the potential pitfalls

Security Awareness, Communications, and Training

FSU Cyber Bowl Cybersecurity Campaign: Don't Fumble Your Password!

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Philip Kraemer, Security Training Coordinator, Florida State University

Hut, hut, hike! Play the Cyber Bowl—it's time to take the field and start tackling cyberthreats. Learn about the touchdowns and fumbles of FSU's 2018 cybersecurity awareness campaign and how your school can create an engaging program that people want to listen to, teaches them more, and ultimately changes behaviors. We'll explain how we engaged and communicated on an emotional level with students, staff, and faculty. Key points will include marketing, defining culture, and developing an engagement strategy and communication methods.

Outcomes: Develop ideas to leverage campus organizations and improve cybersecurity awareness in a large university • Design successful marketing and communications strategies to educate your campus on common cybersecurity threats and best practices for protecting confidential information • Learn how to overcome challenges associated with engaging students, faculty, and staff

Security Operations and Engineering

Stop Worrying About Compromised Accounts: O365 Enhanced Security Tools

ST. GALLEN, SECOND FLOOR EVENT CENTRE

Thomas Conley, Information Security Officer, **Rachel Schlueter**, IT Systems Administrator, **Greg Williams**, Director of Operations, and **Kevin Wolf**, Director of Application Development and Support, University of Colorado Springs

At UCCS, we have seen a 90% drop in compromised account incidents without any major impact to help desk operations, while increasing end-user satisfaction. Previously, we used a variety of homegrown and third-party security tools to manage password resets, account activity, and email. When physical systems needed to be replaced, we adopted a new approach to security tools, using EOP, AAD, ADFS, MFA, and SSPR, over a year-long period. Processes and change management were the most critical parts of the entire project.

Outcomes: Learn how to effect large changes to your security architecture with limited disruption • Explore O365 security offerings • Learn how to configure O365 security offerings

Strategic Leadership, Professional/Organizational Development, and Personnel Management

Women in Security (Not Insecurity)

VEVEY 3, SECOND FLOOR EVENT CENTRE

Andrea Childress, Executive Director ITS, University of Nebraska; **Leilani Lauger**, Chief Information Security Officer, University of Chicago; **Cheryl O'Dell**, Security Awareness and Incident Response Manager, University of Nebraska–Lincoln; **Renee Peters**, Director of Technology Risk and Service Management, Northeast Community College

According to a 2017 global information security workforce study white paper from Frost & Sullivan, women represent only 14% of the cybersecurity workforce in North America. What is even more disappointing is that the percentage has not changed in four years. Come hear from four women who decided on a career in cybersecurity and helped stir the winds of change for security teams. They'll discuss how they got where they are, the importance of being a woman in security and bringing diversity to the IT team as a whole, and some struggles and opportunities they experienced.

Outcomes: Understand how to attract more women into your security team • Learn about some common struggles women in security face • Identify reasons why diversity in security is necessary

9:00 a.m.–2:20 p.m.

Corporate Displays

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.

Corporate Displays

ZURICH BALLROOM FOYER, FIRST FLOOR EVENT CENTRE

Cyber Threat Intelligence

FireEye

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant consulting. FireEye eliminates the complexity and burden of cybersecurity for academic organizations struggling to prepare for, prevent, and respond to cyberattacks.

SpyCloud

SpyCloud is the leader in account takeover (ATO) prevention. We help institutions of all sizes mitigate account takeover by proactively remediating account exposures for students and faculty in an automated way. We accomplish this through our award-winning ATO prevention solutions powered by a world-class team of security researchers and technology.

Governance, Risk, and Compliance (GRC)

Deloitte, Silver Partner

Deloitte's Higher Education practice can help higher education institutions become more diligent and deliberate in being secure and resilient, focusing on policies and controls to prevent the compromise of their most risk-sensitive assets and operations. We can help achieve the fundamentals faster, by leveraging our engagement accelerators, extensive industry experience, and deep cyberrisk domain knowledge to safeguard risk-sensitive assets and operations. Learn more at: www.deloitte.com/us/higher-ed-cyber-security.

Quest Software

No matter where—on premises, cloud, or hybrid—Quest is your go-to expert to help move, manage, and secure your most critical Microsoft platforms so you have more time to drive innovation forward.

Salty Cloud

Salty Cloud provides workflow automation solutions for security/risk teams and was created in the InfoSec trenches at UT Austin and Georgia Tech for real and acute pain points. Our products are for higher education, by higher education and include questionnaire-based security/risk assessments, asset classification, vendor assessments, credential management, antiphishing, and the popular Dorkbot service.

San Diego Supercomputer Center

SDSC Health Cyberinfrastructure Division's Sherlock Cloud platform was established to provide managed services to meet the secure computing and data management needs of our academic, government, and industry partners. It offers a multitude of high-touch, value-added turnkey solutions that span secure cloud computing, big data management, data science, and analytics.

WTC Consulting

Our information security assessment provides six key elements: (1) inventory of security services provided by the central IT organization, (2) assessment of central IT staffing levels, (3) identification of gaps and vulnerabilities in the IT security environment, (4) assessment of security policy and practices, (5) security and user awareness training recommendations, and (6) estimated costs.

Identity and Access Management

Fischer Identity, Silver Partner

The Fischer International Identity mission is simple: your success. We make identity governance and administration work for your organization, technically and financially. We never stop innovating or evolving. We are never satisfied because we know we can make IGA easier. Fischer Identity is the last IGA product you will ever need.

Identity Automation

Identity Automation helps organizations embrace security, increase business agility, and deliver an enhanced user experience with RapidIdentity, the most complete identity, access, governance, and administration platform available.

LastPass

LastPass provides secure password management to reduce the risk of breach and remove employee password frustration. With secure password sharing, customizable policies, and comprehensive user management, LastPass gives businesses of all sizes the tools to create an enterprise security posture. Founded in 2008, LastPass is a product of LogMeIn.

Moran Technology Consulting, Gold Partner

Moran Technology Consulting provides IT management and technology consulting to higher education clients, including IAM strategic planning, vendor selection, architecture, and implementation; Active Directory security assessments and secure (re)design; and IT security assessments and security program implementation.

Painless Security

Painless Security offers Jisc Liberate in North America. Liberate is a fully managed cloud solution that gives you access to the InCommon Federation, eduroam, and a Shibboleth-based web proxy in an easy-to-configure service. With Liberate, you can save time and money, reduce risk, and eliminate the need for specialized in-house expertise.

Incident Management and Response

Best Practical Solutions

Best Practical Solutions develops and maintains Request Tracker (RT) and Request Tracker for Incident Response (RTIR). RTIR was designed in collaboration with several global security organizations to enable security teams, CERTs, CSIRTS, and similar types of groups to manage and respond to network and security incidents for their organizations.

Corelight

Come to Corelight's table to learn why network security monitoring is your best next move and how it can dramatically accelerate your average incident response times and unlock new threat detection and threat hunting capabilities.

CrowdStrike

CrowdStrike is the leader in cloud-delivered endpoint protection, going beyond traditional antivirus to provide complete protection. Our cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed. CrowdStrike's ultimate goal is to help customers stop breaches immediately, with minimal time, effort, and impact on their processes.

EdgeWave

EdgeWave delivers unparalleled inbox protection from today's exploding messaging threats like phishing, spoofing, BEC, and more. At the core of our email security solutions is ThreatTest, an automated inbox detection and response solution that uses machine learning and expert human review to quickly catch, analyze, and resolve suspicious emails.

Rapid7

TBD Organizations around the globe rely on Rapid7 technology, services, and research to securely advance. The visibility, analytics, and automation delivered through our Insight cloud simplifies the complex and helps security teams reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Learn more at www.rapid7.com.

Yakabod

Built for higher ed, CISOBox delivers efficient, secure information security incident management through intelligence agency–accredited technology. Universities use CISOBox to isolate and secure sensitive incident data, documentation, and communication; generate critical metrics; and gain NIST 800-61r2 compliance. CISOBox's new security review management application offers efficient handling of vendor assessments, too.

Security Architecture and Design

Symantec Corporation

Symantec Corporation, the world's leading cybersecurity company, helps organizations, governments, and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, the cloud, and infrastructure. For more information, please visit www.symantec.com.

Security Operations and Engineering

Forescout Technologies

Forescout is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environments and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, 100% real-time and continuous discovery and classification.

Strategic Leadership, Professional/Organizational Development, and Personnel Management

TDI Security

Having experienced the challenges and complexities associated with managing cybersecurity for multiple organizations firsthand, we knew there had to be a better way. CnSight is an innovative and practical solution providing situational awareness for leaders to help them truly understand and improve the effectiveness of their cybersecurity.

Corporate Displays

FOYER, SECOND FLOOR EVENT CENTRE

Cyber Threat Intelligence

Cisco Systems, Gold Partner

Cisco Security enables organizations to gain more empowered security, so they focus on what they do best. With our integrated security portfolio, organizations stay safer and respond faster while teams do more, and resources go further. As enterprise IT pioneers, it is our job to secure IT, something we do better than anyone.

Fortinet

Fortinet provides top-rated network and content security, as well as secure access products that share intelligence and work together to form a co-operative fabric. Our unique Fortinet Security Fabric delivers broad protection and visibility to every network segment, device, and appliance, whether virtual, in the cloud, or on premises.

Governance, Risk, and Compliance (GRC)

Spirion

Spirion is the leader in the rapid discovery, accurate classification, and automated protection of sensitive data across your network and public cloud. Spirion provides enterprise data management software to help businesses reduce their sensitive data footprint and proactively minimize the risks, costs, and reputational damage of successful cyberattacks. Visit www.spirion.com.

Identity and Access Management

Splunk

Splunk turns machine data into answers. Organizations use market-leading Splunk solutions with machine learning to solve their toughest IT, Internet of Things, and security challenges. Join millions of passionate users and discover your aha moment with Splunk today: www.splunk.com.

9:15–10:15 a.m.

Governance, Risk, and Compliance (GRC)

We've Already Changed the Game: UC's Security Policy Architecture

VEVEY 4, SECOND FLOOR EVENT CENTRE

Robert Smith, Systemwide IT Policy Director, Security Director, University of California, Office of the President

Effective security policy architecture allows for adaptations and creates a culture of compliance. Policy is about more than just what to do and what not to do. Its architecture—or the framework that helps it adapt to changes and the needs of an organization—is part of what makes it work well. At UC, it was on observing the cultural shift in conversations about security compliance that we realized the effectiveness of our policy architecture. As the adoption process started, people were talking about a plan for compliance. A cultural shift accompanied our policy change because of our policy architecture.

Outcomes: Learn about popular approaches to security policy and about the experience of a large R1 university's experience developing and implementing a new approach • Find out more about our adoption process

Incident Management and Response

Extended Information Security: Improving Incident Response Beyond the Security Office

MONTREUX, SECOND FLOOR EVENT CENTRE

Charles Escue, Extended Information Security Manager, Indiana University; **Ian Douglas Washburn**, Systems Risk Mitigation Manager, Indiana University Bloomington

To address increasing cyberrisk at IU, we created a new team within our security office, Extended Information Security (EIS), with the goal of reducing incident remediation times and better handling imminent threats. By building a collaborative relationship with security professionals outside the security office, the EIS program seeks to leverage their talents, improve communication between the enterprise and the edge, and increase security office capacity without additional cost. Join this session to learn more about this endeavor and to share your similar efforts with the community.

Outcomes: Learn how to build trust with units outside the security office • Explore how you can improve incident response capabilities leveraging existing resources • Learn how you can match central and edge capabilities using the NIST Cybersecurity Framework

Security Architecture and Design

Machine Learning for Security Operations: A Gentle Introduction

VEVEY 1–2, SECOND FLOOR EVENT CENTRE

Louw Smith, Senior Security Analyst, Boston College

No doubt by now everyone has encountered machine learning in some way or another. Your vendor probably mentioned it, your SIEM may be doing it, and your colleagues might even have experimented with a classifier or two. Maybe you even have a few ideas yourself. This talk aims to give a sober-minded overview without the hype and give practitioners enough resources to launch their own machine learning projects specifically in the information security domain.

Outcomes: Become familiar with machine learning methodology • Gain exposure to existing tools, methods, and free data resources • Have enough training to either launch your own machine learning initiative or at least critically assess proposed initiatives

Security Awareness, Communications, and Training

Cybersecurity Woke: Effecting Positive Change Through Outreach and Education

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Stephen Cobb, Senior Security Researcher, ESET; **Kelvin Coleman**, Executive Director, NCSA; **Robert Jorgensen**, Cybersecurity Program Director/Assistant Professor, Utah Valley University; **Robert Arthur Turner**, Chief Information Security Officer, University of Wisconsin–Madison

Cybersecurity awareness training is important, of course, but getting people to care and actually change behavior is difficult. We will discuss two recently initiatives that helped motivate students and staff and effected positive cyberchange on campus. We'll also provide practical tips on how to bring in partners and effectively communicate program ideas and initiatives to garner buy-in and support. The panel will also discuss current free cybereducation tools and programs that IT administrators can start using today to help staff and students become more "cyberwoke."

Outcomes: Understand why creating cybereducation programming can help reduce risk and promote engagement • Identify how to effectively build partnerships that support cybereducation programming and communicate with key stakeholders • Obtain resources that can help promote staff and student cyberawareness

Security Operations and Engineering

SIEM Usage in Higher Education

ST. GALLEN, SECOND FLOOR EVENT CENTRE

Richard Biever, CISO, Duke University; **Nick Lewis**, Program Manager, Security and Identity, Internet2; **Stacy Lee**, Information Security Operations Specialist, **Jeremy Tavan**, Information Security Systems Specialist, and **Kevin Wilcox**, Information Security Specialist, Appalachian State University; **Brian Mellon**, Threat Intelligence Manager, University of Nebraska–Lincoln; **Dan Villanti**, Senior Security Engineer, Cornell University

The gale force winds of change are pushing higher education to deploy security information event management (SIEM) systems throughout their environments and the community. This panel session will feature campuses deploying SIEMs. The panelists will discuss their campus deployments, including options, integrations, apps, and future plans.

Outcomes: Explore SIEM usage in higher education • Hear how institutions are using SIEMs to improve their information security programs • Gain insight into where campuses are going over the next year with the SIEM usage

Strategic Leadership, Professional/Organizational Development, and Personnel Management

Break Through the Buzzwords and Achieve Measurable Cybersecurity Results

VEVEY 3, SECOND FLOOR EVENT CENTRE

Daniel Desko, Shareholder, Schneider Downs & Co.; **Thomas Dugas**, Director Information Security/New Initiatives, Duquesne University

Every day we receive calls from a vendor promising to measure and assess our information security programs in higher education. They all promise that they know our business and use every security buzzword, but when they show up, they use a process or checklist that doesn't fit our needs. At Duquesne, our internal audit team leveraged the HEISC Information Security Maturity Assessment to baseline our program when it began. Hear how we cut through the buzzwords and got a real assessment on our information security program.

Outcomes: Get an overview of the HEISC assessment tool • Learn how to get management and stakeholder buy-in for a maturity assessment • Apply our lessons learned using the maturity assessment • Learn how to obtain independence using internal audit resources • Build an action plan and continual improvement roadmap

10:15–11:00 a.m.

☕ Refreshment Break and Corporate Displays

ZURICH BALLROOM FOYER, FIRST FLOOR EVENT CENTRE, AND FOYER, SECOND FLOOR EVENT CENTRE

11:00 a.m.–12:00 p.m.

Governance, Risk, and Compliance (GRC)

Applying the NIST Cybersecurity Framework at Your Institution

VEVEY 4, SECOND FLOOR EVENT CENTRE

Kolin Hodgson, Senior Information Security Analyst, and **Jason Williams**, Director Information Security and Compliance, University of Notre Dame

The NIST Cybersecurity Framework is a popular solution to help institutions meet the foundational security requirements to effectively manage their risk. We'll outline the steps we took at the University of Notre Dame to adopt the framework with the aim of identifying and remediating security program gaps. Universities are often decentralized and heterogeneous environments, making the adoption of enterprise-wide standards challenging. We'll review how we addressed these issues and offer ideas for other schools to do the same.

Outcomes: Feel enthusiastic about and ready to implement a framework • See the power of engaging staff in assessing current maturity, giving them perspective on how leadership views security • Understand how evaluating your security program against a security framework can support program goals and make the case for continuing support of the program

Identity and Access Management

Are We Done Yet? A New IAM Implementation at UVA

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Mark Cox, Program Director, Identity and Access Management, and **Ernest Elliott**, Identity and Access Management Analyst, University of Virginia

We'll review how the IAM team at the University of Virginia managed, in a change-weary environment, to successfully implement a new identity governance administration product. Come hear about how the team accomplished this task within a year of the contract signing date. We'll cover moving from a legacy IAM system, redesigning all processes, implementing modern functionality with a self-service portal, and working to ensure compatibility with the implementation of Workday.

Outcomes: Explore the benefits of agile methodology • Get ideas for team management • Define your project milestones • Understand the value of project-independent validation and verification • Know the value of having a strong executive sponsor

Incident Management and Response

Practice to Prevent: Creating and Delivering IR Tabletop Exercises

MONTREUX, SECOND FLOOR EVENT CENTRE

Richard Sparrow, Director, Security Operations, The Pennsylvania State University

Annual tabletop exercises are often required by incident response plans. While some institutions may see this as a compliance box that needs to be checked, these exercises are an opportunity to identify gaps, improve processes, increase performance, and build high-functioning teams. At Penn State, we have leveraged tabletop exercises not only to positively impact incident response but also to develop teams that can work closely to address the complexities that arise during an actual incident. Learn how we create scenarios, manage the exercises, measure success, and learn from failures.

Outcomes: Leverage our strategies to build and deliver your own tabletop exercises • Understand the correlation between practice and execution • Develop opportunities to build resiliency into your IR activities

Security Architecture and Design

Bringing a Security Data Lake into View

VEVEY 1–2, SECOND FLOOR EVENT CENTRE

Philip Kobezak, Associate Director, University Information Security Initiatives, and **Randy Marchany**, University IT Security Officer, Virginia Tech

Data analytics has become a hot topic in many industries including higher education. In order to be competitive, universities need to leverage their data to improve business operations, the student experience, and research. One approach that has become common is the data lake model. While it has primarily focused on learning and administrative system data analytics, this model can also be leveraged for IT security. We'll discuss the concept and how it enables both operations and research. We'll also show research visualizations using augmented reality techniques. Lastly, we'll engage in an interactive discussion about the evolution of security data analytics.

Outcomes: Learn about the concept of a security data lake • Gain insight into Virginia Tech's approach and research use cases • Develop a direction for security analytics based on input from other institutions

Security Operations and Engineering

Reclaiming the Keys to the Kingdom: Higher Ed Admin Rights

ST. GALLEN, SECOND FLOOR EVENT CENTRE

Patrick Seymour, Manager, Application Delivery, Sinclair Community College; **Bryan Lewis**, Assistant Dean of Technology and Operations, McIntire School of Commerce, and **Eric J. Rzeszut**, Associate Director of Client Services, McIntire School of Commerce, University of Virginia

At many academic institutions, faculty and staff are still granted local administrative privileges on their computers. This is a security risk long since shunned in the corporate world, and for good reason: Microsoft research indicates that 80% of critical vulnerabilities could be mitigated by removing admin rights. Largely due to institutional inertia, local admin rights are still routinely granted in academia, which creates unnecessary risk. This interactive presentation will present original research in this space, survey attendees on the approaches at their institutions, and demonstrate some policies and solutions in use at the University of Virginia.

Outcomes: Learn about common approaches in academia for providing administrative access through the use of survey data • Gain a clearer understanding of the risks involved when faculty/staff use admin accounts on a daily basis • Understand realistic approaches (more nuanced than "take admin rights away from everyone!") that work in higher ed

Strategic Leadership, Professional/Organizational Development, and Personnel Management

You're All a Bunch of Phonies! Imposter Syndrome and Information Security

VEVEY 3, SECOND FLOOR EVENT CENTRE

Tara Hughes, Interim Manager of Administrative Services Center, California State University, Channel Islands

The far too common problem of imposter syndrome can cause outwardly successful individuals to be riddled with self-doubt. In the fast-paced world of information security, it can be easy to second-guess your abilities and attribute success to sheer luck. The consequences for doing so are severe, hurting your ability to grow, collaborate, and experience enjoyment in your career. In this presentation, we will discuss the signs of imposter syndrome and its impact on IT and InfoSec, as well as some positive steps to help combat self-doubt.

Outcomes: Learn what imposter syndrome is and how to identify it in yourself and others • Learn about the negative consequences of imposter syndrome both professionally and personally • Learn techniques to combat fears brought on by imposter syndrome

12:00–1:00 p.m.

☕ Lunch

Sponsored by SailPoint Technologies

ZURICH BALLROOM D-G, FIRST FLOOR EVENT CENTRE

Join colleagues to eat lunch and network informally.

1:00–2:00 p.m.

Governance, Risk, and Compliance (GRC)

Electronic Discovery: Good, Bad, or Plead the Fifth?

VEVEY 4, SECOND FLOOR EVENT CENTRE

Eric T. Wiessinger, IT Security Operations Engineer, Cornell University

Managing the process of litigation hold is critical but often challenging. It involves requirements from counsel, uncooperative users, and diverse platforms holding relevant data. In this session, Cornell University's IT Security Office will cover the processes and tools they use and how the service has evolved to become more streamlined and auditable and less error-prone.

Outcomes: Explore the history and evolution of Cornell's ED process • Review our process, templates, and tools • Get examples of implemented tools and how/why they were selected • Understand the dos and don'ts of establishing an ED practice • Learn how to streamline and optimize the administrative burden

Incident Management and Response

IR Planning with the FEMA NIMS Framework

MONTREUX, SECOND FLOOR EVENT CENTRE

Alan Bowen, Chief Information Security Officer, Franklin & Marshall College

Our incident response plan went from ad hoc heroic efforts of individuals to a well-defined, and unfortunately well used, incident response plan. Our response procedures were established and repeatable but lacking structure, modularity, and flexibility. This presentation will discuss the maturation of our incident response plan from early efforts to its current format with components from the National Incident Management System developed by FEMA. This framework will scale for incident response of all types for all size institutions.

Outcomes: Learn what FEMA NIMS is and how to apply it to your IR planning • Learn how one IR plan can apply to all information security events • Understand the importance of reviewing and revising your IR plan regularly

Security Architecture and Design

Secure the Workflow, Stupid!

VEVEY 1–2, SECOND FLOOR EVENT CENTRE

Anurag Shankar, Senior Security Analyst, Indiana University

Cybersecurity efforts today focus solely on individual components such as systems, networks, governance, and training. This is problematic because the risk equation is far more complex and dynamic. It affects the origin, timing, and nature of vulnerabilities and makes them change in both space and time. Total risk not remains a simple sum of individual pieces but also depends strongly on nuances in how the pieces intermesh and move. This talk will discuss the shortcomings of static risk treatment as practiced currently and show how securing workflows can address some of these limitations.

Outcomes: Understand the limitations of how we treat risk today • Learn how workflow security addresses them • Leave with strategies to try in your own environment

Security Awareness, Communications, and Training

Considerations for Security Awareness and Inclusive Design

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Tara Schaufler, Information Security Awareness and Training Program Manager, Princeton University; **Ben Woelk**, ISO Program Manager, Rochester Institute of Technology

Inclusive design and accessibility have become increasingly important over the past decade. As security awareness communicators, we must to be mindful of users' differing capabilities. Although technology can enable those with disabilities, it can also inadvertently present barriers. In this session, we will discuss the building blocks of technical information design, with an emphasis on incorporating inclusivity. We will also cover how inclusive design may impact the way you communicate with your campus community, such as making interpersonal communications, websites, and videos more accessible.

Outcomes: Understand the importance of inclusive design • Identify areas where you can improve accessibility • Obtain resources for learning about preparing inclusive communications

Security Operations and Engineering

EDUCAUSE, Internet2, and REN-ISAC's Adventures in Cybersecurity

ST. GALLEN, SECOND FLOOR EVENT CENTRE

Todd Herring, Membership Services Director, and **Kim Milford**, Executive Director, REN-ISAC, Indiana University; **Brian Kelly**, Director of the Cybersecurity Program, EDUCAUSE; **Nick Lewis**, Program Manager, Security and Identity, Internet2

This panel discussion will focus on how EDUCAUSE, Internet2, and REN-ISAC work collaboratively and independently to provide support for cybersecurity professionals, from facilitating the creation of shared tools that save you time and resources like the Higher Education Cloud Vendor Assessment Toolkit (HECVAT), to providing guidance on strategic and tactical security initiatives like combating DDOS. In addition to exploring services available to you, the experts panel will also answer your questions about risks and risk mitigation.

Outcomes: Get acquainted with the cybersecurity services offered by the 3 organizations • Explore the organizations' collaborations offering assistance to cybersecurity professionals • Provide feedback on the collaborations

Strategic Leadership, Professional/Organizational Development, and Personnel Management

Gravitational Leadership: Patching Your Soft Skills

VEVEY 3, SECOND FLOOR EVENT CENTRE

Monte Ratzlaff, Director, Cyber-Risk Program, University of California, Office of the President

Today's information security leaders typically have a lot to juggle security operations, meetings, deadlines, managing incidents, and leadership reports, just to name a few. Having to wear so many hats can be overwhelming. It's easy to forget the way we handle being overwhelmed affects our staff, colleagues, and even external partners, good and bad. This interactive session will step through strategies for you as a leader on the soft skills and approaches to daily interactions to be "gravitational" so others will want to work with you.

Outcomes: Understand overlooked or forgotten soft skills and approaches to information security leadership • Engage in live polling and dialogue to ask questions, share your experiences, and learn from other attendees • Take away new strategies to sharpen your soft skills and become a better leader

2:00–2:20 p.m.

☕ Dessert, Refreshment Break, and Corporate Displays

ZURICH BALLROOM FOYER, FIRST FLOOR EVENT CENTRE, AND FOYER, SECOND FLOOR EVENT CENTRE

2:20–3:20 p.m.

Incident Management and Response

Handling Incidents as Bees in TheHive

MONTREUX, SECOND FLOOR EVENT CENTRE

Anthony Miracle, IT Security Analyst, Duke University

Handling security incidents can present unique challenges in the higher education space. Shifting, heterogeneous networks and limited resources mean many of the frameworks available don't quite match your needs. We'll talk about how TheHive has given us flexibility to handle our own incidents and investigations, as well as the challenges we've faced and some of the ways we've solved them. We'll also talk about the opportunities TheHive and its associated projects create for higher ed institutions to collaborate and share the attack data we see to make us all more secure.

Outcomes: Learn what TheHive is and how it is able it to improve the way we investigate attacks • Understand how you can customize TheHive to work with your own unique challenges • Be inspired to contribute back to the community with your own improvements and data to help make us all safer

Privacy

Building an Impactful Privacy Program in Higher Ed

VEVEY 4, SECOND FLOOR EVENT CENTRE

Holly Swires, Chief Privacy Officer, Assistant Chief Information Security Officer, and HIPAA Privacy Officer, The Pennsylvania State University

Joseph Gridley, Assistant Chief Privacy Officer, The Pennsylvania State University

In the technologically and culturally diverse environment of higher education, impactful strategies for achieving successful privacy and information security compliance continue to evolve. Obtaining buy-in from leadership and stakeholders can be the most challenging aspect of building a successful program. In this dynamic session, you'll learn techniques for obtaining support for building your program, including developing a culture of privacy and compliance, establishing and adopting consistent privacy principles, and implementing compliance frameworks. Learn how to work in harmony with decision makers to understand the risk and value of implementing a comprehensive privacy and information security compliance program.

Outcomes: Understand the importance of leadership and stakeholder support• Learn techniques for developing enterprise-wide privacy and information security compliance programs • Get impactful tactics for achieving an accepted culture for privacy and information security compliance

Security Architecture and Design

Journey to the Cloud: Security by Design Approach

VEVEY 1–2, SECOND FLOOR EVENT CENTRE

Kyle Gustafson, Information Security Engineer, and **Douglas Lomsdalen**, Information Security Officer, California Polytechnic State University, San Luis Obispo

Security by design is a deliberate process of ensuring security is built into the entire process versus "bolted on" after the fact. We will discuss the shared security responsibility model: both the vendor and the customer are accountable for the security of the cloud. We will address organizational culture and change before moving to the cloud, reviewing people, processes, and technology, and explore the built-in and readily extensible audit capabilities of AWS and how it can enhance the security posture of a migration. Finally, we will review our journey of implementing security at every layer.

Outcomes: Understand the importance of addressing organizational culture before attempting a cloud migration • Learn about the various components of a cloud security model and how to implement them • Understand how security by design allows an organization to improve its security posture as it operationalizes its cloud environment

Security Awareness, Communications, and Training

Cybersecurity Awareness Campaigns: Overview, Materials, and Insights

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Hans Pongratz, Senior Vice President and CIO, Technische Universitat Munchen

Cybersecurity is a prerequisite for the IT-based handling of business processes for higher education institutions. Humans play a key role in ensuring cybersecurity. Likewise, users need to learn how to properly handle devices, techniques, and IT services. The Technical University of Munich (TUM) worked intensively on this topic. We collected information on possible activities then developed and implemented various educational campaigns targeted to students and staff. One of them was embedded in the European Cyber Security Month (ECSM). We used a variety of formats, including traditional events, ads, printed matter, and online-only methods.

Outcomes: Understand the importance of cybersecurity awareness campaigns • Identify good practices to adapt • Learn how to find the right wording to engage students and staff • Be able to start your own campaign

Strategic Leadership, Professional/Organizational Development, and Personnel Management

Agile Strategy for InfoSec

VEVEY 3, SECOND FLOOR EVENT CENTRE

Brian Smith-Sweeney, Chief Information Security Officer, Columbia University

The winds of information security are ever shifting, but many of us are chained to rigid strategic planning processes with immutable budgets and accountability via Gannt chart, if we have a process at all. I will present my experiences using a different tack: strategic planning for infosec that builds on agile principles, higher education culture, and some basic leadership and management philosophy. “Builds on” is of course a euphemism for “I have no new ideas.” To that end, come share your ideas, and let’s talk about how to change strategic planning from an annual obligation to a critical component of your security program.

Outcomes: Understand basic agile principles and how they apply to strategic planning for infosec • Understand the key components of an agile infosec strategy for higher ed • Compare your strategic planning experiences against your peers and understand how you can work collectively to improve

From the Bottom Up: Diversity Perspectives from a Security Engineer

ST. GALLEN, SECOND FLOOR EVENT CENTRE

Tyrone Smith, Security Engineer–Technical Security Group, University of Delaware

Diversity may be erroneously viewed as an exercise for HR and management to adjust staffing decisions to ensure compliance with institutional diversity statements. My personal experience is that diversity is a powerful tool to make teams and project outcomes better. In this session, I will share my experiences during a recent project to deploy two-factor authentication for the University of Delaware. In this project, diversity drove improved teamwork, formed the basis of team innovation, and led to a project outcome that was better and more resilient than envisioned by individual team members.

Outcomes: Identify tangible benefits of diversity in their project tasks • Identify enablers to improve teamwork • Align project and institutional diversity needs

3:30–4:30 p.m.

Tornado Talks in Ten

MONTREUX, SECOND FLOOR EVENT CENTRE

Niko Bailey, Vulnerability Management Analyst, Duke University; **Lance Huggins**, IT Director, Kansas City University of Medicine and Biosciences; **Randy Marchany**, University IT Security Officer, Virginia Tech; **Don Warrick**, IT Training Manager, California Lutheran University

Talk 1: CMSS: Plug in Some Security into Your CMS

Niko Bailey, Duke University

Content management systems provide an easy interface for users to alter website content and appearance but often leave security and IT professionals in the dark regarding the security state of the platform. Come join the fun as we explore how Duke is using modules and plug-ins to catalog important security data contained within each CMS and collect it centrally for vulnerability-alerting and incident response.

Outcomes: Understand how CMS data can be used to improve your web security posture • Identify methods of aggregating CMS data in your environment • Examine some potential strategies for inventorying your web presence

Talk 2: How to Survive a Successful Phishing Attempt

Lance Huggins, Kansas City University of Medicine and Biosciences

We experienced a successful phishing incident at KCU, which cost the university real dollars and forced us to create an incident management response team and ongoing security processes. We would like to share our story with other institutions, including what we did, and lessons learned that others can benefit from.

Outcomes: Apply lessons learned from our phishing experience to your own institution • Craft your own incident response plan • Identify tools and ideas to apply on your campus

Talk 3: NIST-800-63-3B Password-Vetting Compliance

Randy Marchany , Virginia Tech, and **Richard Tilley**

In June 2017, NIST Special Publication 800-63-3B established new guidelines regarding how organizations should vet user passwords. Rather than password composition policies that require a certain number of character sets, NIST now recommends that organizations check passwords against a list of banned passwords and reject those that are found on the list. As of July 2018, the list of known compromised passwords numbers more than half a billion strings. This presentation will demonstrate how to solve this problem at all levels of the organization and also share a specific technical solution using a Bloom filter at Virginia Tech.

Outcomes: Understand the drastic password-vetting changes introduced by NIST 800-63-3B as of June 2017 • Learn how these changes will impact every level of your organization and how to adapt • Learn how to solve the technical challenges brought about by the changes with a hybrid solution

Talk 4: Sleight-of-Hand Magic and Cybersecurity

Don Warrick, California Lutheran University

We’ll explore the commonalities between sleight-of-hand magic and cybersecurity, specifically, the neuroscience behind the way the observer/user interprets data they see and how the senses can be tricked both in magic and in cybersecurity.

Outcomes: Learn how to triage potential threats • Learn how to manage your attention to mitigate errors in judgement • Understand the science behind illusion and perception and its role in exploiting the user

Governance, Risk, and Compliance (GRC)

Pitt’s NIST 800-171 Assessment and Implementation

VEVEY 3, SECOND FLOOR EVENT CENTRE

Sean Gallagher, Security Analyst, **Joel Garmon**, Chief Information Security Officer, and **Chris Seiders**, Security analyst, University of Pittsburgh

We’ll present a case study of our phased approach to NIST 800-171 compliance at Pitt. Information security developed two Qualtrics surveys with multiple-choice responses to capture the data collected and the security controls in each department. The initial survey was sent to each department to capture the data types collected and the basic security controls in place. Security performed a risk assessment based on the initial survey results. Each department deemed high-risk data was sent a second survey based on the 800-171 controls. Finally, security analyzed the 800-171 survey results, identified gaps, and assisted the department in developing remediation plans.

Outcomes: Learn about Pitt’s process, methods and tools for performing NIST 800-171 assessments and mitigations• Obtain a copy of Pitt’s detailed NIST 800-171 survey questions • Understand some of the challenges with performing the NIST 800-171 assessment

Privacy

Education in Privacy Policies: Best Practices for Evaluating Edtech

VEVEY 4, SECOND FLOOR EVENT CENTRE

Sara Collins, Policy Counsel, Future of Privacy Forum

This session will cover the best practices of what should be included in an educational technology privacy policy. We’ll cover common flaws and pitfalls, as well as what to look out for.

Outcomes: Understand how to effectively read a privacy policy • Have a framework for evaluating a privacy policy • Know what questions to ask vendors about privacy when in negotiations

Security Architecture and Design

Building a Shelter for Sensitive Data

ST. GALLEN, SECOND FLOOR EVENT CENTRE

Cal Frye, Compliance Technologist, Case Western Reserve University

The winds are rising; will your researchers’ data be safe, or will it be scattered across the landscape? Using NIST reference standards, CWRU built a Secure Research Environment to provide both safe storage and a working environment for the most sensitive data. Such an undertaking required the cooperation of many offices across the University. A recent assessment tested our alignment with 800-171 guidelines.

Outcomes: Identify the institutional cooperation needed to bring such a project together • Understand the architecture meeting some NIST 800-171 recommendations • Serve your clients’ growing interest in protecting research data

Web Application Security by Design

VEVEY 1–2, SECOND FLOOR EVENT CENTRE

Guillermo Munoz, Applications Security Engineer, Texas A&M University

This presentation will discuss how development of a secure web application is more than just a matter of writing good code. Security must be an integral part of the entire software life cycle, starting from the very conception of the software development project. Security must be a priority to the developer(s) and other stakeholders, on par with functionality. We will examine how making security a priority affects each stage of development.

Outcomes: Understand the importance of prioritizing security throughout an application’s life cycle • Understand the effects of prioritizing security at each stage of the application’s life cycle • Recognize the importance of stakeholder involvement in prioritizing security

Security Awareness, Communications, and Training

Security Awareness Doesn’t Have to Be a Waste of Time

ZURICH BALLROOM BC, FIRST FLOOR EVENT CENTRE

Micah Nelson, Information Security Awareness Officer, Harvard University

Some say security awareness is a waste of time because you can’t fix stupid. They are wrong. Your community isn’t stupid, and even if they were, isn’t “fixing stupid” what education is all about? In this session, we will move beyond compliance and start reducing risk with the help of your colleagues through behavioral science. If you’re a skeptic, see how we reduce risk and measure the results. If you’re a practitioner, learn about our strategy, learn tactics for any budget, ask questions, and share your experiences.

Outcomes: Choose measurable awareness goals that will reduce risk • Incorporate behavioral science into your awareness activities • Demonstrate the value of your time and money spent on awareness