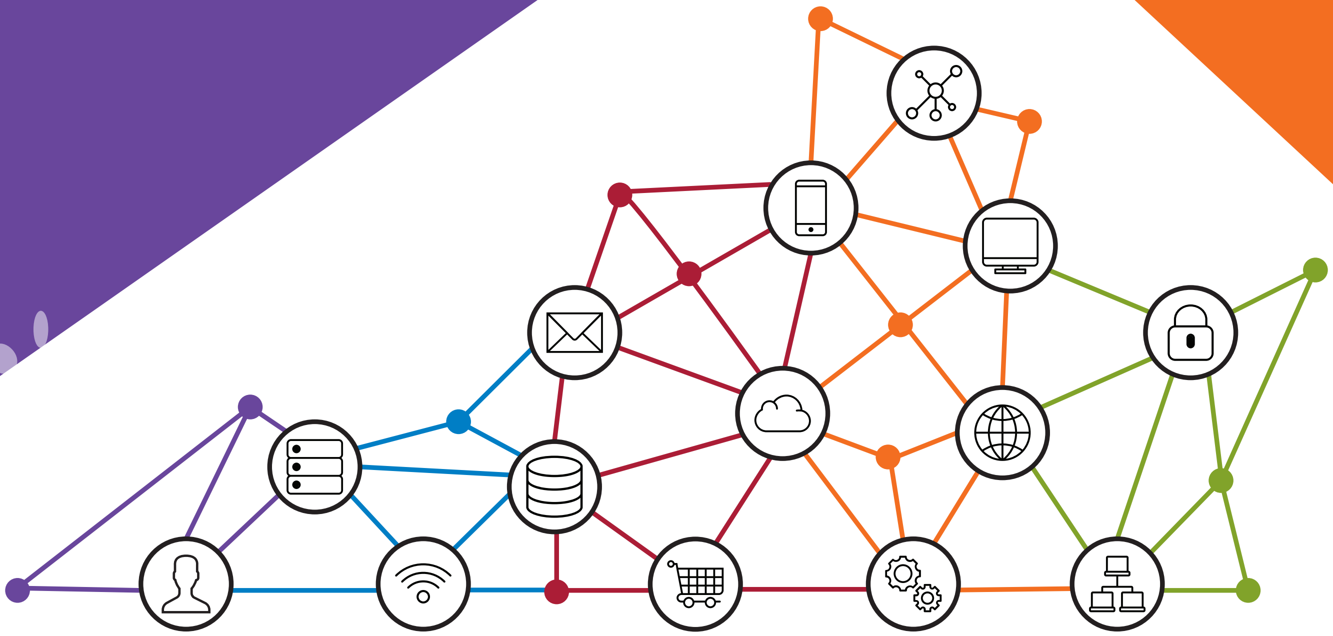
LEVEL UP

YOUR CYBER SECURITY MATURITY

CONFERENCE PROGRAM

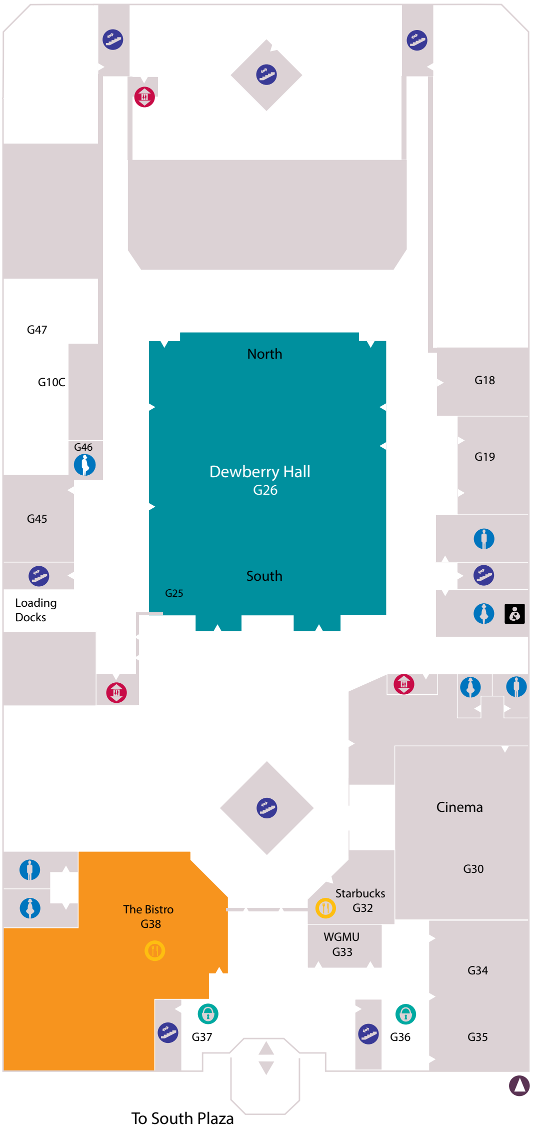
VASCAN
2018



October 16-17, 2018
George Mason University
Fairfax, Virginia

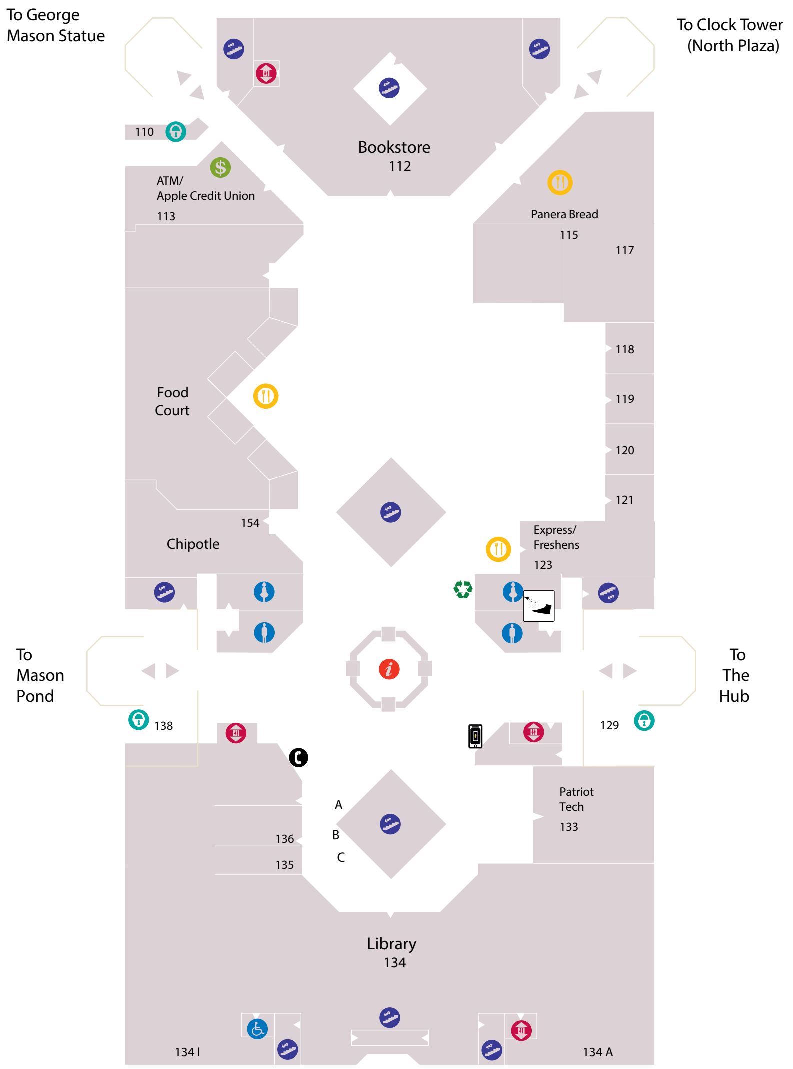
MAP OF JOHNSON CENTER

GROUND FLOOR



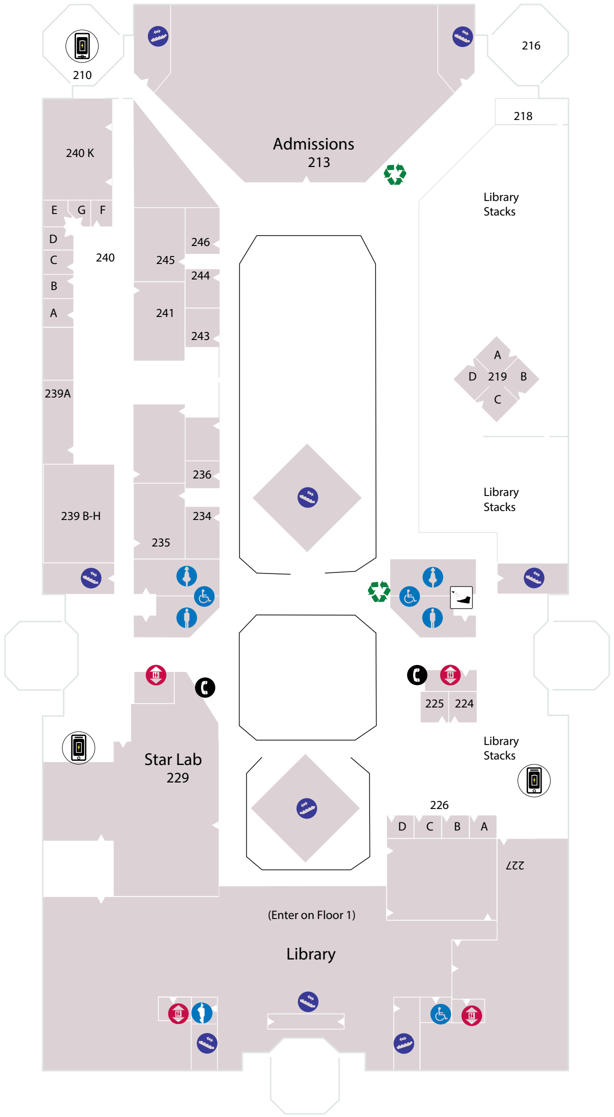
Registration
Dewberry Hall
The Bistro
Vendor Area

FIRST FLOOR

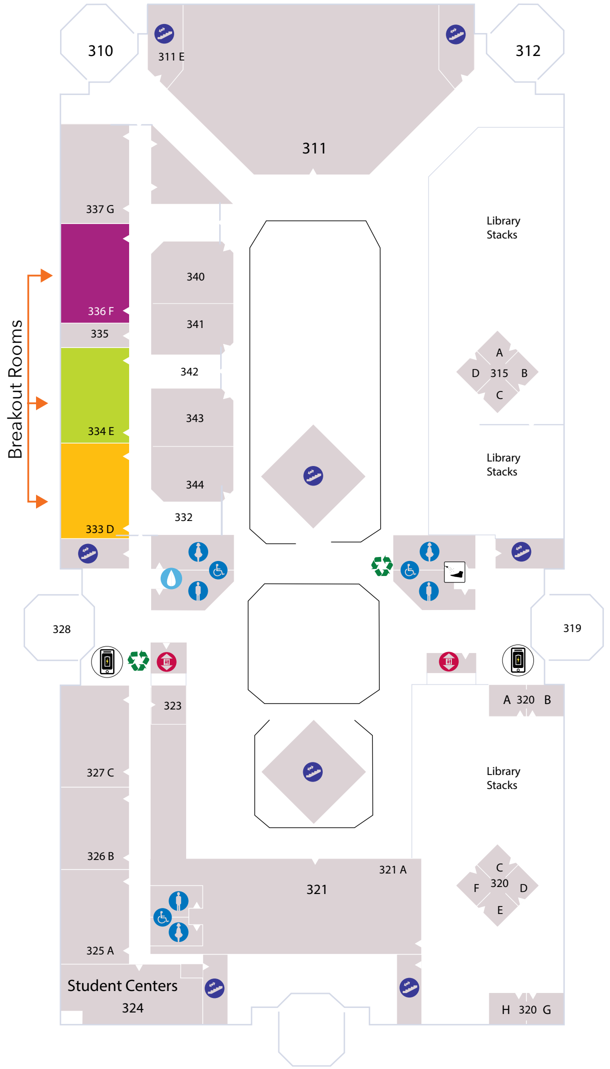


- Accessible to Disabled
- Restaurant
- Elevator
- Women's Restroom
- Men's Restroom
- Unisex Restroom
- Public Lockers
- Charging Station
- Stairway
- Information
- Recycling
- Lactation Room

SECOND FLOOR



THIRD FLOOR



Meeting Room D
Meeting Room E
Meeting Room F

SCHEDULE

DAY ONE: TUESDAY, OCTOBER 16, 2018

TIME	DEWBERRY	ROOM D	ROOM E	ROOM F
7:15 a.m.	Registration and Breakfast in Dewberry Hall			
8:45 a.m.	Welcome and Keynote (Level Up Your Cyber Security Maturity)			
10:30 a.m.	Cybersecurity Governance and Addressing Third-Party Cyber Risks	The Human Element	The DNS Firewall Architecture of Virginia Tech	Forensics for Web Applications
11:30 a.m.	Build it Secure: Continuous Improvement in Secure System Provisioning		Our Path to Controlled Unclassified Information (CUI) Compliance for Researchers	Using Student Interns to Augment your Security Program
12:30 p.m.	Lunch in Dewberry Hall			
2:00 p.m.	Building Cybersecurity Culture, Teams, and Leaders	Transforming Security via a Cyber-Enabled Data Center Architecture	Risk-Based, Data-Driven Audit Preparation	IT Governance Risk and Compliance of University Servers
3:00 p.m.	How to Build a Solid Foundation for Effective Cyber Defense Operations	Thinking Differently: Protecting the Public, Faculty, Students, Alumni, and the Supply Chain through DMARC Enforcement	Automating IT Security: Letting Security Analysts Be Analysts	Architecture Standards Review Board (ASRB): University Partnerships for Security and other Risk Identification and Mitigation
4:00 p.m.	IT Security Auditing, a Behind-the-Scenes Look	Endpoint Protection: How and Why to Evaluate New Solutions	Reflections on 35+ years of 'Being the Man'	Climbing Survey Platforms to Elevate Policy & Compliance Programs
4:45 p.m.	Reception & Shirley Payne Award in The Bistro			

DAY TWO: WEDNESDAY, OCTOBER 17, 2018

TIME	DEWBERRY	ROOM D	ROOM E	ROOM F
7:15 a.m.	Breakfast in Dewberry Hall			
9:00 a.m.	CIS 20 Critical Security Controls (Presentation Format)	Managing Risk: From "Just Getting By" to "Making it Great" by Improving Processes	Complying with NIST 800-63-3b Password Checking Guidelines	Hazards of Cyber Defense: Failure of Imagination
10:00 a.m.	Threat Hunting Workshop (Hands-on)	Artificial Intelligence Versus Malware	The Virginia Cyber Range: Cloud-Based Resources for Hands-on Cybersecurity Education and Training	Revisiting the CAN-SPAM Law
11:00 a.m.		Threat Landscape in Higher Education	Introduction to the Cloud	Utilizing OSINT in Threat Analytics and Incident Response
12:00 p.m.	Lunch in Dewberry Hall			
1:00 p.m.	BOSS of the SOC (Hands-on)	VASCAN Meeting - Conference Hotwash		
2:00 p.m.				
3:00 p.m.				
4:00 p.m.	(ending at 4:30 p.m.)			

DAY ONE PRESENTATIONS

LEVEL UP YOUR CYBER SECURITY MATURITY

Rick Howard

The keynote presentation cover the concepts and ideas of how to orchestrate your security kit deployment. It will provide a history of how we have arrived here and give recommendations for what all network defenders should be doing in the future. It will also cover the NIST Framework, the Capability Maturity Model Integration levels, and provide strategies for how organizations with tiny budgets can approach the problem.

DAY ONE: FIRST SESSION

CYBERSECURITY GOVERNANCE AND ASSESSING THIRD-PARTY CYBER RISKS

J.P. Auffret

With the Wyndham Worldwide and Target breaches and reliance by organizations on third-party vendors, contractor risk is an increasing priority for boards, executives, information technology, and cybersecurity leaders. Not only are there risks to personal and financial data and IT systems, there are also risks to connected industrial control systems. How are boards viewing and addressing third-party cyber risk? What are key considerations for developing a third-party vendor cybersecurity management program? What are approaches for vendor evaluation, contracting, and ongoing management? What are compliance considerations? How are efforts to strengthen the cybersecurity of vendor ecosystems progressing?

THE HUMAN ELEMENT

Gabriel Whalen

Layer 8 – The human factor as a driving force for security assessments in advance of technology solutions.

- The hunter gatherer brain
- Strength/weaknesses of the human brain
- The free-rider threat & modern ecosystems
- Free-riding v. doing the right thing
- Herding cats – getting people to do the right thing
- Goals of security assessment, getting to CMMI
- The coming regulation wave
- The ROI on security assessment (spending money where it makes sense and actual wins)
- Solutions

THE DNS FIREWALL ARCHITECTURE AT VIRGINIA TECH

Brad Tilley

A high-level overview of the DNS firewall architecture and implementation at Virginia Tech and how the system is used to protect client machines from malicious sites and code on the Internet. The presentation will cover the design and infrastructure (hardware, software, networking), custom source code (database and API) and daily processes used to implement and operate the system.

FORENSICS FOR WEB APPLICATIONS

Michael Richardson

Public-facing web applications can introduce vulnerability into an otherwise secure environment. Both open-source and commercial products can have hectic patch release schedules as new vulnerabilities are discovered, and application administrators can (and do) neglect upgrading for various reasons. The question becomes not if the application will be compromised, but when and how. Based on a recent investigation of a compromise of a CMS server, we will discuss various methodologies for verifying integrity of the application itself, inspecting back-end databases, and releasing content to the owner. We will also discuss strategies to protect and adequately log application activity.

DAY ONE: SECOND SESSION

BUILD IT SECURE: CONTINUOUS IMPROVEMENT IN SECURE SYSTEM PROVISIONING

Dan Han and Craig Kilgo

With the emergence of DevOps models and cloud service provisioning, expediency in provisioning of services is one of the top priorities for many business units across organizations. The inability for IT to quickly meet the needs of these business units can often drive units to adopt shadow IT operations through other service providers, leading to the potential loss of control on sensitive data and information. This presentation will follow VCU's journey in establishing a system provisioning process, providing the needed expediency to its customers while maintaining a reasonable expectation of quality and security for its assets. The presenters will discuss the evolution of the system provisioning process and the role of security, in addition to challenges and lessons learned through the transformation. Additionally, the presenters will discuss future plans for the process.

OUR PATH TO CONTROLLED UNCLASSIFIED INFORMATION (CUI) COMPLIANCE FOR RESEARCHERS

Tim F. Jost Tolson

Over the course of the past two years, the University of Virginia has worked to create a computer system and network that would be compliant with the NIST 800-171 standards for Controlled Unclassified Information (CUI). From a starting point of a high-level committee, through an inventory of current systems and networks and a process of establishing both what was required for compliance, and how we met that control, we strove to meet compliance without creating a new, separate, compute system for researchers. This spring, with the help of an outside consultant, we completed our first Systems Security Plan (SSP) and Plan of Action and Milestones (POAM) for a DOD grant for our so-called Ivy-CUI compliant system. This talk will review the highlights of our march to CUI compliance and look at some topics on the CUI horizon.

USING STUDENT INTERNS TO AUGMENT YOUR SECURITY PROGRAM

Tony Houdek

Maximize your IT security office and operations with student internships. We will talk about our office culture and program in utilizing interns across our analyst and engineering operations. From hiring to integrating and making operational various roles, learn how to achieve better outcomes for your office and individual student interns. At least one of our current interns will join the presentation and discussion. Please come see what it is like to work in our office as a student intern.

DAY ONE: THIRD SESSION

BUILDING CYBERSECURITY CULTURE, TEAMS, AND LEADERS

Mansur Hasib

Cybersecurity is a team sport—people are central to any strategy. Yet people are often denigrated as the weakest link. We continue to spend countless funds on technology and not enough attention is devoted to people and governance. Through culture and teamwork fostered through leadership, people can become our greatest strength. Leadership is the key element of success of any organizational cybersecurity strategy. Dr. Hasib will explain why cybersecurity is people powered perpetual innovation. He will discuss the role of people and innovation in cybersecurity, inspiring innovation and leadership in everyone, and building teams of leaders.

TRANSFORMING SECURITY VIA A CYBER-ENABLED DATA CENTER ARCHITECTURE

Bill Roche

In today's cyber landscape with both the frequency and cost of breaches rising, what can be done to harness the power of existing compute, network, and storage infrastructure for the purpose of greater cybersecurity readiness? This session will explore the ability to up level an organization's security posture by focusing on key aspects of data center architecture that enable greater visibility, protection, and threat detection. By augmenting and instrumenting existing compute, network, and storage components within the data center, analytical threat data can be greatly enhanced thereby increasing the speed and fidelity in which a response and recovery can be orchestrated. The session will include examples of higher education institutions that have implemented this approach and discuss the benefits they have realized. Benefits include compliance with relevant higher education security standards including NIST, PCI and HIPAA.

RISK-BASED, DATA-DRIVEN AUDIT PREPARATION

Doug Streit

We all know that being compliant and auditable is not the same as being secure. We need to be prepared to defend our information security practice at any time if called into court or in response to a compromise. Our audit preparation is an exercise in defending out practice. No school has resources to administer an audit/compliance program that produces a complete audit trail for all of the services and systems across their technical ecosystem. A risk-based approach is essential to focusing the most effort on the highest risk. Audit preparation starts with our standards and applies risk-based practices that allow schools with limited resources to focus on securing and defending the highest risks, without spending precious resources on lower risk services and systems.

IT GOVERNANCE RISK AND COMPLIANCE OF UNIVERSITY SERVERS

Bilal Ahmad

We'll present our journey of rolling out an ITGRC tool to improve the security posture around Mason's IT resources. We introduced workflows to Information Technology Services and distributed IT partners in phases, which include inventory and classification of university servers (CIS Control No. 1), and formalizing a risk management process via vulnerability and control information.

DAY ONE: FOURTH SESSION

HOW TO BUILD A SOLID FOUNDATION FOR EFFECTIVE CYBER DEFENSE OPERATIONS

Ron Bushar

An overview of basic building blocks for resiliency, intelligence, detection, and response capabilities that lay the groundwork for more effective and proactive hunting capabilities as organizations mature their cyber defense functions.

THINKING DIFFERENTLY: PROTECTING THE PUBLIC, FACULTY, STUDENTS, ALUMNI, AND THE SUPPLY CHAIN THROUGH DMARC ENFORCEMENT

Denis Ryan, Sr.

Impostor email continues to be a challenge for most security professionals. We will discuss the various tactics used to impersonate a domain, brand, and supply chain partner, focusing on the email threat landscape, how to identify potential exposure, and how to leverage authentication methods such as DMARC to protect your faculty, students, brand, and alumni.

AUTOMATING IT SECURITY: LETTING SECURITY ANALYSTS BE ANALYSTS

Steve Huff

The tools and appliances available within the IT landscape have expanded the analysis and monitoring capabilities available to IT security personnel. However, these tools rarely integrate with each other and are often not designed to play well outside their defined scope. While Security

Analysts have more power at their fingertips than ever before to identify and track down threats, without an automated way to connect these systems, numerous cycles are wasted performing tedious tasks that detract from time that could be spent better understanding and monitoring the security threats faced by the university. Learn how our IT Security Office has developed several web applications and tools that leverage the APIs of various security appliances, Google Drive, and Service-Now in order to provide connective tissue where appropriate and eliminate manual data entry whenever possible.

ARCHITECTURE STANDARDS REVIEW BOARD: UNIVERSITY PARTNERSHIPS FOR SECURITY AND OTHER RISK IDENTIFICATION AND MITIGATION

Andrew Krell, Curtis McNay

Technology moves fast, and so must we. But it is impossible to be an expert on everything. George Mason University has put together a group focused on reviewing incoming technology to identify risk, and mitigation strategies to reduce that risk. This includes working with internal university groups, vendors, and subject matter experts both inside and outside of IT departments. This presentation will go over a brief history of how and why the group was formed, its maturation process, and how the process has improved Mason's security posture.

DAY ONE: FIFTH SESSION

IT SECURITY AUDITING: A BEHIND THE SCENES LOOK

Alex Roeglin

A contributing factor to leveling up your information security program is to understand and leverage independent external IT security audits, such as those provided by the Auditor of Public Accounts (APA). This presentation will provide an overview of the IT security audit function at the APA, including a behind the scenes look at planning audits, performing test work, and reporting audit results. The presentation will also examine security standards & best practices, designing technical audit programs, and automated control evaluation tools & resources. Attendees will be provided tips on how to prepare for an upcoming IT audit and an overview of current and potentially future trends in IT auditing.

ENDPOINT PROTECTION: HOW AND WHY TO EVALUATE NEW SOLUTIONS

Mark DeDomenic

The market for anti-virus products has significantly changed over the last several years as existing vendors add new functionality to compete with "next-generation" entrants built on machine learning and cloud-based threat intelligence sharing. To add further complexity, many endpoint detection and response (EDR) vendors have now adopted preventative capabilities. What decision points should your institution consider when determining if it is time to consider new solutions and how should you scope the search? ODU conducted a thorough evaluation of the endpoint protection platform (EPP) market earlier this year to assess the effectiveness of new solutions versus what was currently deployed. This session will cover our approach to the evaluation, and provide some suggestions for how to conduct one at your institution.

REFLECTIONS ON 35 PLUS YEARS OF 'BEING THE MAN'

John Hanks

You cannot really appreciate 'Leveling Up' without an understanding of where you have been. This presentation will highlight some of the 'basic principles' used in cybersecurity today through true stories from the past where things did not always go right, including one story never told in public before.

CLIMBING SURVEY PLATFORMS TO ELEVATE POLICY & COMPLIANCE PROGRAMS

Cory Brant and Margaret Gokturk

This presentation will illustrate how a survey platform can be used to help identify and measure risk and achieve compliance across an institution. It will cover specific Qualtrics use cases including a university-wide departmental risk management assessment, an analysis of the flow of Controlled Unclassified Information (CUI) across multiple information systems, and a third-party risk evaluation of prospective hospital vendors.

DAY TWO PRESENTATIONS

SECOND-DAY TRAINING (PART I): CIS 20 CRITICAL SECURITY CONTROLS ASSESSMENT (PRESENTATION FORMAT)

Craig Vincent and Sondra Russell

Participants will review the 20 Critical Security Controls as identified by the Center for Internet Security, and learn how to apply these important security controls in a real-world setting by analyzing real, existing data. After participants understand the environment, they will spend the remainder of the morning identifying threats. The trainers will introduce theories and processes of investigation, threat hunting, and incident response using a variety of endpoint, network, and threat intelligence data sources.

DAY TWO: FIRST SESSION

MANAGING RISK: FROM "JUST GETTING BY" TO "MAKING IT GREAT" BY IMPROVING PROCESSES

Mike D'Arezzo

Many of us are trying to do more with less by adding functions to an already overwhelmed staff. The next thing you know, the team is faced with an enormous unplanned challenge: a new regulatory requirement, new operational challenges, or perhaps an unfortunate event like a breach or malware explosion. Moving up the Capability Maturity Model is more than just reacting and increasing capabilities—its maturing processes not only simplify but streamline for faster turnaround to allow more time to improve your environment or responding to internal requests or unplanned challenges. This presentation will walk through examples of how to improve or create processes to simplify security without "watering it down" and help security employees change how they view the "everyday" by examining what the time and effort is spent on and how to reduce or improve the through/output.

COMPLYING WITH THE NIST-800-63-3B PASSWORD CHECKING GUIDELINES

Brad Tilley

In June 2017, The National Institute of Science and Technology (NIST) Special Publication 800-63-3b established new guidelines with regard to how organizations should vet user passwords. Rather than 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 number is expected to grow even larger as more online sites are compromised. The Virginia Tech IT Security Office solved this problem by using a bloom filter running in a small Docker container in AWS. This talk will discuss the design and operation of this new service. Full source code along with working examples will be provided.

HAZARDS OF CYBER DEFENSE: FAILURE OF IMAGINATION

Steve Faehl

Good cyber investment strategy is based on risk. How do we identify the most important risks and more accurately predict future threats? How do we prioritize investment? Which attacks should we invest in preventing? Learn how Microsoft is changing its approach to cyber solution product development. Hear the stories behind the product announcements made at Ignite and walk away with behind-the-scenes insights that will help you chart a course for cyber preparedness.

DAY TWO: SECOND SESSION

ARTIFICIAL INTELLIGENCE VERSUS MALWARE

Keith Rayle

This session will focus on Artificial Intelligence/Machine Learning and how these technologies relate to Information Security. Because of the wide range of readily available resources for creating malicious payloads, such as coders for hire and Software as a Service, malware is an exponentially growing issue. Threat actors are able to rapidly assemble and deploy high volumes/varieties of malicious code to users. Current malware management models are simply overwhelmed or incapable of providing complete protection while reducing false positives toward that magical zero rate. We will provide a view into a system comprised of highly efficient deep machine learning neural networks that are currently deployed and proactively defeating malware attacks.

THE VIRGINIA CYBER RANGE: CLOUD-BASE RESOURCES FOR HANDS-ON CYBERSECURITY EDUCATION AND TRAINING

David Raymond

The Virginia Cyber Range has a mission to enhance cybersecurity education in the Commonwealth's high schools and colleges. We provide cloud-based network infrastructure for experiential learning in isolated network environments, as well as courseware to enhance cybersecurity classes. We also provide capture-the-flag environments to educators across the state, and host multiple annual collegiate cybersecurity competitions. Our unique approach is cost-effective, user-friendly, and a model for others. During this talk and demo, we will describe our progress and discuss lessons learned while using cloud resources in a unique way. While we are currently a Virginia resource, we plan to expand availability in the coming year to other states.

REVISITING THE CAN-SPAM LAW

David Landry

The CAN-SPAM law was designed by Congress to set national standards for commercial email and help consumers cope with the onslaught of spammers. Fifteen years after this law's enactment, both large and small businesses are either unaware or ignoring the detailed requirements of CAN-SPAM. This presentation will review the basics of CAN-SPAM and show university security professionals how to leverage this law to reduce spam and phish and how to hold companies accountable for their actions. Vendors should also attend this presentation to understand how to design more effective email communications.

DAY TWO: THIRD SESSION

THREAT LANDSCAPE IN HIGHER EDUCATION

Josh Burgess

While cyber incidents and compromises are now regularly making headline news, organizations often focus on stopping malware or minimizing the incident. However, employing research and intelligence resources to better understand the threat landscape and more specifically, who the attacker is and how they operate will allow organizations to better understand their risk and build their defenses effectively.

INTRODUCTION TO THE CLOUD

Jillian Leo

At AWS, security is always job zero. This presentation will provide an introduction on how AWS approaches security, including controls in its environment and ways to meet security objectives.

UTILIZING OSINT IN THREAT ANALYTICS AND INCIDENT RESPONSE

Christopher Beiring

Validating potential incidents or indicators of compromise (IOCs) in today's fast paced environment can be overwhelming and difficult. Sometimes a team does not believe they have all of the tools and resources to quickly and accurately identify, verify, and rectify a potential indicator in their environment in time. Relying on one piece of data for IOC validation is a bad idea, even if that resource is the best in the industry. The approach is to use not only the tools you have, but to augment them with existing open source tools that will enrich your investigation, provide accuracy, and supplement your ability to quickly and accurately respond to valid threats in order to increase your security team's effectiveness. The purpose of this presentation will be to walk users through the value of Open Source Intel and how to use the tools available effectively to help research and identify potential issues during an incident response engagement.

DAY TWO: FOURTH SESSION

SECOND-DAY TRAINING (PART II): BOSS OF THE SOC (HANDS-ON)

Craig Vincent and Sondra Russell

Participants will engage in a hands-on training. Teams made up of four or five players will compete in a blue-team capture-the-flag exercise called Boss of the SOC. Each team will be handed a data set and a series of challenges. Teams will be scored on accuracy, speed, and ingenuity. Teams will compete for prizes, but more importantly, bragging rights.

VASCAN MEETING: CONFERENCE HOTWASH

VASCAN members are invited to discuss the conference.

BIOGRAPHIES

KEYNOTE: RICK HOWARD

CHIEF SECURITY OFFICER // PALO ALTO NETWORKS

Howard has responsibility of the company's internal security program. He leads the Palo Alto Network's Threat Intelligence Team (Unit 42), directs the company's efforts on the Cyber Threat Alliance Information Sharing non-profit. He also hosts the Cybersecurity Canon Project, and provides thought leadership for the company and the Cybersecurity community at large. His prior jobs include TASC CISO, iDefense General Manager, Counterpane SOC Director, and Commander of the U.S. Army's Computer Emergency Response Team where he coordinated network defense, network intelligence, and network attack operations for the Army's global network. Rick holds a Master of Computer Science degree from the Naval Postgraduate School and an engineering degree from the US Military Academy, where he taught computer science from 1993 to 1999.

BILAL AHMAD

IT SECURITY ANALYST // GEORGE MASON UNIVERSITY TITLE

Ahmad received his bachelor's degree in information technology in 2014 from Mason. He started his career as an IT generalist in the private sector. Curiosity in IT security and a commitment to helping users better secure their information led him back to Mason. His primary role includes SIEM monitoring, threat and vulnerability analysis, and leading risk assessment projects to grow Mason's IT security posture.

J.P. AUFFRET

ASSOCIATED DIRECTOR, CENTER FOR ASSURANCE RESEARCH AND ENGINEERING

VOLGENAU SCHOOL OF ENGINEERING // GEORGE MASON UNIVERSITY

In addition to his work with the Volgenau School of Engineering, Dr. Auffret is also the director of research partnerships in the School of Business at Mason. He is co-founder and current president of the International Academy of CIO. Auffret's work and research span a range of applied technology fields including cybersecurity leadership and addressing cybersecurity challenges for cities and counties, CIO and ICT governance; and with APEC, NSF and IBM. In addition, he has worked with World Bank and ITU on mobile and ICT for Development. He has served on several Commonwealth of Virginia commissions including the Health Information Technology Advisory Commission. His experience includes executive positions with MCI and its joint venture with British Telecom, Concert, and academic positions with George Mason, Duke University's Center for International Development, and as physicist-in-residence at American University. Auffret earned a bachelor's degree from Duke University where he was an A.B. Duke Scholar; a MBA from the University of Virginia, and Ph.D. in physics from American University.

CHRISTOPHER M. BEIRING

SECURITY ENGINEER // SLAIT CONSULTING

Beiring is a security engineer with SLAIT Consulting. He has his Network+, Security+, SANS GCIH, SANS GMON, and is currently working on his SANS GNFA. With more than eight years of IT Network and Security experience with MSP's, he has worked in various security roles as a lead security analyst and in penetration testing. Beiring has focused on incident response and threat analysis in various environments to help clients build a better security stance in their infrastructure. He specializes in performing threat intelligence analysis and is passionate about OSINT as it pertains to investigative analysis.

CORY BRANT

POLICY AND COMPLIANCE ANALYST // UNIVERSITY OF VIRGINIA

Brant serves as a policy and compliance analyst with the University of Virginia's Information Security office. He has almost two and a half years of experience working in policy with a focus on automating risk and compliance objectives. He built UVA's current information security risk management assessment, and he is working on a third party risk assessment for UVA's health system. He holds a GSEC certification.

JOSH BURGESS

CYBER INTELLIGENCE OFFICER // CROWDSTRIKE

Burgess has extensive expertise in cyber threat analysis and intelligence, incident response, reverse engineering, security policy, and security engineering and architecture. He draws from more than a decade of experience gained through multiple positions in the intelligence community, Department of Defense, defense industrial base, as well as the financial sector.

RON BUSHAR

VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER – PUBLIC SECTOR // FIRE EYE

Bushar is a seasoned and innovative cyber security leader with extensive Federal government, cyber security, risk management, and network operations experience. He has more than 19 years of experience in the areas of information assurance, information security, cyber operations, and incident response services. He began his career in the United States Air Force serving in the Information Warfare Aggressor Squadron at Lackland Air Force Base. Bushar holds a master of science in management of information systems and a bachelor of science in electrical engineering. He is a certified Project Management Professional, a Certified Information System Security Professional, a Certified Information System Security Architecture Professional, and maintains a professional membership with the Institute of Electrical and Electronic Engineers.

MIKE D'AREZZO

DIRECTOR OF SECURITY SERVICES // SLAIT CONSULTING

D'Arezzo is known for his track record of operational excellence, innovative problem solving, and regulatory compliance expertise. He brings with him more than 15 years of experience from GE, AMF, and Micros/Oracle, where he focused on driving standards, consistency, performance, compliance and regulatory affairs. D'Arezzo supports clients by developing secure operations and policies and identifying vulnerabilities in configuration in the network and processes. He reviews daily operations and existing policies to identify potential risk and resolve, mitigate, or create compensating controls. Other responsibilities include executing penetration testing, vulnerability scans, perform audits against industry developed or internal controls, and review business processes and create security improvements for clients and SLAIT.

MARK DEDOMENIC

ASSISTANT INFORMATION SECURITY OFFICER // OLD DOMINION UNIVERSITY

DeDomenic is the lead for the Security Operations team and serves as one of two assistant information security officers at ODU. He graduated from ODU with a bachelor's degree in computer science in 2007 and has been working in information technology at the university since then. Mark currently holds certifications from GIAC and Palo Alto Networks.

STEVE FAEHL

CYBERSECURITY LEAD // MICROSOFT UNITED STATES

Faehl excels at incubating new products and strategies to disrupt emerging cyber threats. His main focus is to delineate and evangelize what is working well and what isn't when it comes to cyber defense tactics. He covers all Microsoft products from a security perspective and works with leading security experts from every area of Microsoft, which gives him a unique view into the emerging threat landscape. Steve also works with many of the most attacked organizations in the world to enhance their cyber defense capabilities and ensure that Microsoft's approach to security remains pragmatic based on real-world customer evidence.

MARGARET GOKTURK

SENIOR INFORMATION SECURITY POLICY AND COMPLIANCE ANALYST // UNIVERSITY OF VIRGINIA

Gokturk is a senior information security policy and compliance analyst at UVA. Her background encompasses security awareness training, security analysis, IT audit, risk management, policy development and compliance, and regulatory and PCI compliance. Current survey platform-based projects at UVA include the Information Security Risk Management program and Student Financial Services Controlled Unclassified Information (CUI) project. She holds CISA, CISSP, and GLEG certifications.

DAN HAN

CHIEF INFORMATION SECURITY OFFICER // VIRGINIA COMMONWEALTH UNIVERSITY

Han has worked in various areas in information technology over the past 20 years, with a strong focus on information security for the past 13 years. Han is a technology enthusiast who loves to continuously learn about and experiment with various computer technologies. He holds a master's of science degree and a MBA with concentrations in information technology management and information assurance along with a number of industry recognized certifications.

JOHN HANKS

SENIOR ADVISORY NETWORK ENGINEER // GEORGE MASON UNIVERSITY

Hanks has worked in various roles for the IT department at Mason for over 37 years, mostly involving networking. His current position has influence over all data, video, and voice communications across all of Mason's campuses. He has a bachelor's degree in electrical and computer engineering from Mason.

MANSUR HASIB

PROGRAM CHAIR, CYBERSECURITY TECHNOLOGY, THE GRADUATE SCHOOL // UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE

Dr. Hasib has 30 years of experience leading organizational transformations through digital leadership and cybersecurity strategy in healthcare, biotechnology, education, and energy. He served as Chief Information Officer for 12 years. His seminal book *Cybersecurity Leadership* has been widely acclaimed by practitioners and scholars alike and is listed among the best IT and cybersecurity books of all time. Dr. Hasib is one of the first few in the world to earn a Doctor of Science in cybersecurity. He is the recipient of numerous Information Security awards.

TONY HOUDEK

IT SECURITY ANALYST // GEORGE MASON UNIVERSITY

Houdek has more than 15 years of professional information technology experience across multiple sectors including K-12, federal government contracting, and higher education. He spent more than 5 years at the University of North Dakota as a systems administrator. He has spent the last five years at Mason as a security analyst responsible for working on SIEM monitoring, risk assessments, network architectures, and compliance projects. He oversees the student internship program consisting of both analyst and engineering internships. He is a lifelong learner and always strives to better himself and others.

STEVE HUFF

IT SECURITY ANALYST // VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Huff has worked at Virginia Tech since 2005 and joined IT Security Office in 2017 and quickly saw ways he could put his coding skills to work to recover time ITSO Security Analysts were spending on manual tasks, like data input into the university's help desk ticket system. Steve obtained his CompTIA Security plus certification, GIAC Certified Enterprise Defender, GIAC Python Coder certification and is a member of the GIAC Advisory Board.

CRAIG KILGO

PROJECT MANAGER // VIRGINIA COMMONWEALTH UNIVERSITY

Kilgo focuses on technology projects within VCU's Technology Services division. He has managed IT projects of nearly every size for more than a decade for both higher education and the Department of Defense.

ANDREW KRELL

MANAGER, SYSTEMS INTEGRATION // GEORGE MASON UNIVERSITY

Krell serves as the Chair of the Architecture Standards Review Board. He has a background as an ERP analyst, identity management developer, and solutions architect. He recently lead the project to implement Two-Factor Authentication for Mason's data center, VPN, and CAS SSO.

DAVID LANDRY

CHIEF INFORMATION SECURITY OFFICER // GEORGE MASON UNIVERSITY

Landry provides cybersecurity leadership to protect Mason's diverse portfolio of academic, administrative, and research needs. Prior to Mason, David supported the United States Computer Emergency Readiness Team. He served as a cyberspace and communications officer in the U.S. Air Force for 20 years. During his career he protected Department of Defense networks from malicious cyber threats and operated as a shift leader overseeing the entire Air Force enterprise. He is a Certified Information Systems Security Professional and a published app developer.

JILLIAN LEO

SOLUTIONS ARCHITECT // AWS

Leo has been working with public sector customers for the past three years. During this time, she has helped federal customers migrate to the cloud, as well as create cloud native applications. Her focuses are on networking and security.

CURTIS MCNAY

DIRECTOR, IT SECURITY // GEORGE MASON UNIVERSITY

DOUG STREIT

CHIEF INFORMATION SECURITY OFFICER // OLD DOMINION UNIVERSITY

Streit has served at ODU for nearly 20 years, working as a systems engineer, technical manager and IT director. For six years he managed the Server Systems Group, including Window, Linux, UNIX, storage, printing, and integration support services. Current responsibilities include strategic and operational planning, an Information Security Program, in-house identity and middleware development, IT Project Management, and University Records Management. He enjoys working with a very talented and committed team of developers, security administrators, managers, and directors within his organization. He has a Bachelor's of Science degree in Engineering with an emphasis in Oceanography from the United States Naval Academy and he maintains a certification as a Certified Information Systems Security Professional.

BRAD TILLEY

SENIOR SECURITY ARCHITECT // VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Tilley has worked in computer programming, IT management, and information technology for the last 18 years with 10 of those years specifically focused on university-wide cyber security initiatives, including time as the Information Security Officer at Radford University.

KEITH RAYLE

SECURITY STRATEGIST // FORTINET

Rayle has more than 20 years of governance and operational security experience. He has provided executive level security consulting which includes program/portfolio creation and management. He has also provided board level reporting, security strategy creation and implementation, and global business security integrations. Rayle has acted as the chief information security officer for large corporations and led large multi-project teams at the program level. He has also given oversight of multiple simultaneous and complex implementations of technical security projects and has designed and implemented most aspects of corporate security programs. He is a 21-year military veteran as a nuclear weapons technician, threat officer, OH-58/AH-1/UH-60 helicopter pilot and maintenance operations officer.

DAVID RAYMOND

DIRECTOR // VIRGINIA CYBER RANGE

DEPUTY DIRECTOR, IT SECURITY OFFICE AND LAB // VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Dr. Raymond teaches courses on networking and cybersecurity in the Virginia Tech master's of information technology program and is co-author of *On Cyber: Toward an Operational Art for Cyber Conflict*. Raymond holds Ph.D. in computer engineering from Virginia Tech, a master's degree in computer science from Duke University, and a bachelor's degree in computer science from the United States Military Academy.

MICHAEL RICHARDSON

SECURITY OPERATIONS ENGINEER AND FORENSICS TECHNICIAN // GEORGE MASON UNIVERSITY

Richardson has 18 years of professional experience in software development, systems engineering, and security operations. For the past three years, he has served as security operations engineer and forensics technician for the IT Security Office at George Mason University. Mike has a bachelor's degree in information technology and is pursuing a master's degree in digital forensics and cyber analysis at Mason. He holds GIAC certifications in Security Essentials and Certified Incident Handler.

BILL ROCHE

SYSTEM ENGINEERING DIRECTOR // VWMARE

Roche focuses on solving cybersecurity challenges for government, education, and healthcare clients using emerging technologies to counteract a constantly evolving threat landscape. He joined VMware from HyTrust, Inc., where he led the system engineering team for the public sector around insider threat and privileged access. Before joining VMware, Roche was with Computer Sciences Corp for 11 years as the director of IT Services for the Department of Defense Distributed Lab (D2Lab) driving its growth from inception to enterprise lab service provider. He is a graduate of James Madison University with a bachelor's degree in political science.

ALEX ROEGLIN

AUDIT SUPERVISOR, INFORMATION SYSTEMS SECURITY TEAM // AUDITOR OF PUBLIC ACCOUNTS

Roeglin has worked on roughly 50 different information systems security related audits. He holds two bachelor's degrees from Liberty University and is working on a master's degree at Virginia Commonwealth University. He also holds two certifications, a CISSP and a CISA.

SONDRA RUSSELL

SENIOR SALES ENGINEER // SPLUNK

Russell has been a "Splunker" for eight years, starting when she was a devoted customer of Splunk at National Public Radio. While at Splunk, she's focused on working with higher education customers on a variety of use cases, including security and compliance, application monitoring, Internet of Things, and business analytics.

DENIS RYAN

SENIOR DIRECTOR, EMAIL FRAUD // PROOFPOINT, INC.

Ryan has held management positions at several well-known high-tech companies including Nominum (now part of Akamai), Tellabs (now Coriant), Verizon, and IBM. As a sales leader of the fastest growing business unit in Proofpoint, Ryan oversaw the go to market sales and sales engineering strategy post the Return Path business unit acquisition. The diverse background of IT and security solutions allows him to overlay the Proofpoint sales efforts in multiple verticals, most notably healthcare as Proofpoint has ramped this specialized team to improve email authentication practices.

TIM F. JOST TOLSON

DIRECTOR, IT POLICY AND COMPLIANCE // UNIVERSITY OF VIRGINIA

Tolson, along with his two colleagues, work in partnership with units and individuals across the university to formulate information technology policies, assess security risk, comply with security and privacy laws and regulations, and implement security safeguards. He holds a Ph.D. in psychology from the University of Virginia and has worked in information technology in higher education for more than 30 years.

CRAIG VINCENT

SOLUTION ENGINEER AND SECURITY SUBJECT MATTER EXPERT // SPLUNK

Vincent is a solution engineer and regional Security Subject Matter at Splunk. After joining Splunk, Vincent has supported customers in Higher Education, Healthcare, and State & Local Government. Before joining Splunk, he held a security research role at the National Cable & Telecommunications Association and worked in the Security Operation Center at Mandiant, acquired by FireEye, Inc. Based in the DC area, Vincent's technical passions include security, containerization, automation, and program management. Vincent holds a B.S.E in Electrical & Computer Engineering from Duke University.

GABRIEL WHALEN

PRINCIPAL FIELD SOLUTION ARCHITECT // CDWG

Whalen has spent 14 years in the national security arena fulfilling roles in counterintelligence across the U.S. military, the Defense Intelligence Agency, and the Federal Bureau of Investigation's Counterintelligence Division. Whalen holds a master's degree in forensic psychology, and was a recipient of the National Counterintelligence and Security Center's Supply Chain Protection Award. He is a Certified Information System Security Professional and graduate of the Software Engineering Institute's Insider Threat Program Manager course. In the commercial sector, Gabriel has fulfilled roles as an insider threat official and conducted enterprise security assessments across a variety of verticals.

ABOUT VASCAN

WHO WE ARE

The Virginia Alliance for Secure Computing and Networking (VASCAN) exists for the purpose of strengthening information technology security programs within the Commonwealth of Virginia.

The Alliance brings together Virginia higher education security practitioners who developed and maintain security programs widely emulated by other institutions, and researchers who create cybersecurity instruction and research programs nationally recognized for excellence. VASCAN is made up of security professionals from George Mason University, James Madison University, the University of Virginia, Virginia Tech, and the Virginia Commonwealth University as well as researchers and staff from the Center for Security Information Systems at George Mason University, the Institute for Infrastructure and Information Assurance at James Madison University, and the joint George Mason/James Madison Critical Infrastructure Protection Project.

WHAT WE DO

VASCAN began offering products and services in March of 2003. These offerings are based upon the principle that the most lasting improvements to security programs can be made not by performing security functions for organizations, but rather by educating and guiding management and staff teams in defining and carrying out their own security strategies and ongoing security operations.

FOR MORE INFORMATION

Please visit the VASCAN web site: **www.vascan.org**

SPECIAL THANKS

The Mason Committee for the 2018 Virginia Alliance for Secure Computing and Networking would like to thank all of our colleagues for their assistance in putting this conference together. Without their help, it would not have been possible.

We like to send a special thank you to those who went beyond the call of duty to assist us in bringing together all the details—great and small.

INFORMATION TECHNOLOGY SERVICES

Brian Gantt
Finance Director

Toni Mehrman
Finance Specialist

Michael Richardson
Operations Engineer, IT Security Office

Kerin Seward
Creative Director, Communications and Marketing

Marilyn T. Smith
Vice President and Chief Information Officer

Charlie Spann
Assistant Vice President/Deputy CIO

Whitney Sublett
Office of the Vice President and CIO

IT Security Office staff and interns

The Communications and Marketing Staff

ITS Volunteers

FISCAL SERVICES

Brian Davern, Head Cashier
Denise Groat, E-Commerce Specialist
Heather Strange, Director of Fiscal Policy and Communications
Chris Wagaman, Travel Manager
The Cashier's Office

UNIVERSITY EVENTS

Heather Crandall, Scheduling Manager
George Mason University Events Management

MASON CATERING

Diana Trifonas, Catering Manager, Sodexo

OUTSIDE OF GEORGE MASON UNIVERSITY

Amy Kobezak
Darlene Quackenbush
Sondra Russell
The Shirley Payne Award Committee

If we missed anyone, know your work and contributions are appreciated. None of this would have ever been possible with you.

The Mason VASCAN Committee
David Landry, Chief Information Security Officer
Curtis McNay, Director of IT Security
Karen L. Bates, Communications Coordinator

THANK YOU VASCAN 2018 SPONSORS

LEVEL UP
YOUR CYBER SECURITY MATURITY

Your generous support makes this conference possible!

PLATINUM

CROWDSTRIKE

FORTINET®

aws

shi™

vmware®
carahsoft.

GOLD

ABS TECHNOLOGY

ASSURA INC

CAMBRIDGE Computer EST. 1991

CAMPUSGUARD® A Merchant Preservation Services Company

CDW·G®

CISOBOX

CYBERARK®

CYLANCE®

EDGEWISE ZERO TRUST NETWORKING

FireEye®

KENNA Security

FISCHER™ INTERNATIONAL

Infoblox® NEXT LEVEL NETWORKING

Jazz Networks

SOPHOS

netskope

NTS NETWORKING TECHNOLOGIES + SUPPORT

proofpoint.

SyCom Connected.

SLAIT Consulting

paloalto NETWORKS®

splunk> bai FEDERAL

WHOLEPOINT SYSTEMS INNOVATIVE IT SOLUTIONS
docker

SILVER

VIRGINIA CYBER RANGE

Microsoft