

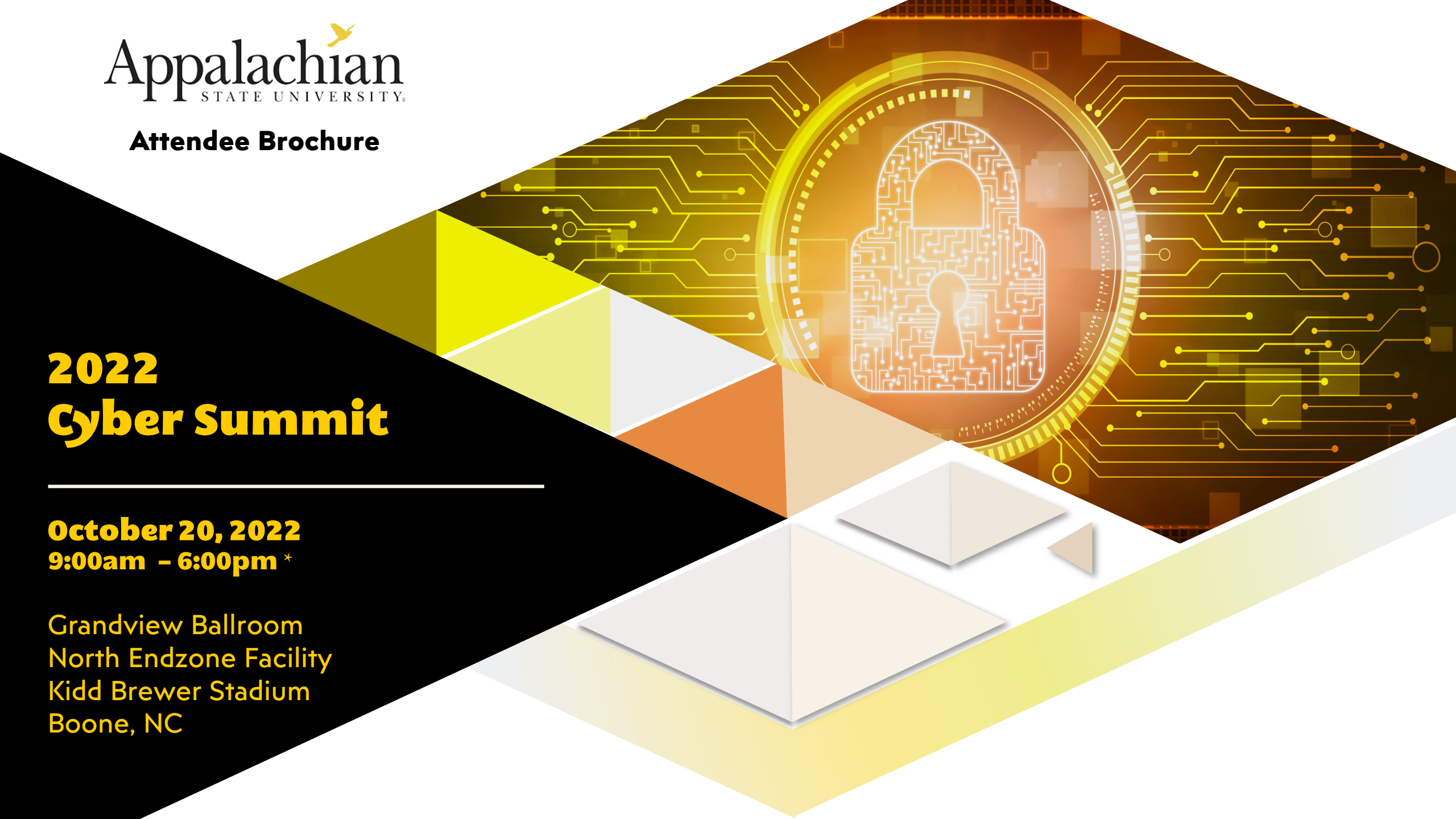


Attendee Brochure

2022 Cyber Summit

October 20, 2022
9:00am – 6:00pm*

Grandview Ballroom
North Endzone Facility
Kidd Brewer Stadium
Boone, NC





The Venue

The Appalachian State Cyber Summit is held in the Grandview Ballroom in the North End Zone Facility of Kidd Brewer Stadium, one of the most scenic football venues in the country.

The October date will provide a beautiful backdrop of fall foliage for this year's event.

2022 Event

This year's Cyber Summit will be held on **October 20, 2022**, the day after the Appalachian State Mountaineers play the Georgia State Panthers in a key Sunbelt Conference game. As with last year, we expect many attendees and presenters to arrive early for the game and stay for the Cyber Summit the following morning.

Hear from industry leaders including Lowe's, HighPoint, TrendMicro, SentinelOne, Optiv/Veracode, Duke Energy, Checkpoint, NTT Data, Palo Alto Networks, and NetFoundry on relevant cybersecurity topics. The Cyber Summit will provide opportunities to network with area business and technology leaders with furnished breaks, lunch, and an event-ending social hour.



Our Focus

The Cyber Summit is managed by the Appalachian State's Computer Information Systems (CIS) Advisory Board. The Appalachian State CIS Department is one of the few institutions in North Carolina to offer a Cyber Security concentration and minor.

Our goal is to build the leading Cyber Security educational program in the Southeast. As such, all proceeds from the Cyber Summit event goes toward funding scholarships for CIS students needing financial assistance.

Keynote Speakers



Jim Guido
EVP Engineering
HighPoint

Jim Guido is a veteran leader and consultant with over 25 years of relative industry experience. Due to his extensive background in cybersecurity, networking, datacenter, Unified Communications and disaster recovery, Mr. Guido supplies critical insights into the design, operation, and response processes. He has successfully leveraged his depth of experience to benefit clients in many ways to meet key business objectives, including internal and external network security and risk assessments, advanced persistent threat assessments, monitoring, logging and alerting solutions, secure network design solutions, and incident response procedures and tabletop exercises.

Mr. Guido is the EVP of Engineering at HighPoint. He works closely with the leadership team to advance the organization's mission, vision, core values, strategic priorities, and growth goals. Through building many teams and facilitating supportive corporate culture, he has learned the importance of putting employees first to provide clients with unprecedented value.

He received his BS degree in Business Management from the University of Bridgeport in Connecticut. He currently lives in Mooresville, NC with his wife and five children. In addition to spending time with his family, he enjoys the outdoors, working on construction projects and classic automobiles.



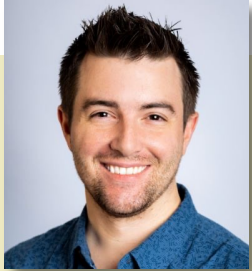
Marc Varner
Chief Information Security
Officer
Lowe's Companies, Inc

As vice president, chief information security officer, Marc Varner is responsible for the global security strategy and program, ensuring all Lowe's information assets and technologies are properly protected. He collaborates with senior technology and business leaders to implement the best security practices to protect and serve our customers and overall business. He joined Lowe's in 2021.

Marc has over 25 years of experience in technology and has expertise in global cybersecurity strategy, security architecture and process, information security governance and controls and regulatory compliance. Prior to Lowe's, he served as vice president and global chief information security officer at Yum! Brands, where he was responsible for global cybersecurity and strategic cybersecurity planning. He previously served as vice president and global chief information security officer at McDonald's.

Marc is on the advisory board of a number of leading cybersecurity companies and serves as a global chair for the Cyber Security Collaborative, which he co-founded in 2012.

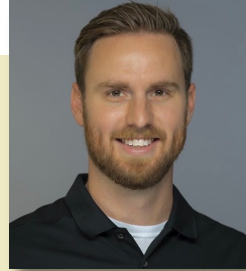
| Speakers |



Chris Boehm **Technology Strategist** **SentinelOne**

Chris Boehm currently works as Technology Strategist at SentinelOne. As a cybersecurity thought leader, he drives strategy and works closely with some of the largest organizations in the world. Prior to SentinelOne, he was a Senior Product Manager at Microsoft in the Azure Security engineering division.

In his 5 years at Microsoft, he focused on driving product strategy and delivering strategic customer enablement. Chris worked closely with the Microsoft Cyber Defense Operations Center (CDOC) and Microsoft Threat Intelligence team (MSTIC) to work side by side on research and enablement to create a more intuitive investigation experience for Security Operations Centers.



Austen Byers **Technical Director, Americas** **TXOne Networks**

As Technical Director at TXOne Networks, Austen leads the company's efforts in providing design, architecture, and engineering technical direction and leadership.

Austen is a sought-after thought leader in operational technology (OT) cybersecurity with more than 10 years in the cybersecurity space. He has spoken at numerous industry events as a subject-matter expert to provide insight into the state of industrial cybersecurity, the intricacies of OT breaches, and providing strategies to help organizations keep their assets and environments safe.



Elliot Johnson **Principal Solutions Architect** **Veracode**

Elliot started working with technology and hardware in the late 90's but has been working in the security space since 2010 and has been with Veracode since 2017 focusing on application security.

Originally from Chicago, he now resides in Raleigh North Carolina with his wife and two daughters. With applications everywhere – from smart TVs to phones to smart enabled household appliances – its more important than ever to make sure applications and devices are secure by design and continually tested throughout development.

Security isn't a point in time event, it's a mindset and something that needs to be considered from inception of an idea all the way to delivery.

| Speakers |



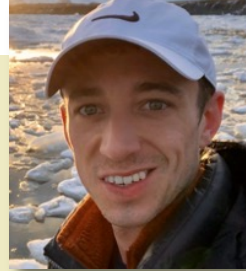
Sushila Nair

**Vice President, Security Systems
NTT Data**

Sushila Nair is the VP for Security Services at NTT DATA's Chief Digital Office. Sushila has previously served as a CISO for 10 years and has over 30 years of experience in computing infrastructure, business and security.

An experienced cybersecurity thought leader, she has worked in diverse areas across telecom, risk analysis, and credit card fraud, and served as a legal expert witness. She also worked with the insurance industry in Europe and America on methods of underwriting e-risk insurance based on ISO27001. Sushila has published numerous articles and collaborated on several books. She is the VP of ISACA Greater Washington, DC chapter and is part of the ISACA emerging technologies working group.

Sushila is regularly featured in global technical events and in the press. She actively supports best practices & skills development in the cybersecurity community.



Aaron Rose

**Cyber Security Evangelist,
Security Architect
Check Point**

Aaron Rose is a Cyber Security Evangelist, Security Architect & Member of the Office of the CTO at Check Point Software Technologies. A subject matter expert in Cloud, Internet of Things, and Application security; Aaron has focused his career on securing organizations & their resources beyond the perimeter of the traditional network firewall.

An avid international traveler, Aaron welcomed the opportunity to spend three months in Tel Aviv, Israel training with Check Point's research & development teams at the company's global headquarters.



Doug Sept

**Systems Engineer
Palo Alto Networks**

Doug Sept is a Systems Engineer with Palo Alto Networks where he specializes in SASE (Secure Access Service Edge), a new cloud-based security model built on ZTNA (Zero Trust Network Access) principles. Doug has been in the network and security industry for over 30 years as a developer, integrator and deployer of network and security technologies for Cisco Systems and VMware in addition to Palo Alto Networks.

| Speakers |



Martin Strasburger **Chief Information Security Officer** **Duke Energy**

Martin Strasburger leads the cybersecurity department at Duke Energy Corporation, one of the largest combined gas and electric utilities in the United States. In this role, Martin works with company executives and the board of directors to define the company's cybersecurity strategy across the corporate network, the operational network, and the cloud. He leads a team of 150 highly skilled employees across all cybersecurity disciplines. Prior to joining Duke Energy,

Martin was a Senior Director leading the cybersecurity department at Pacific Gas and Electric Company. Martin started his career in Deloitte's Security and Privacy Services practice where he rose to Senior Manager and was a practice leader for the Identity and Access Management practice. Martin holds the CISSP designation. Martin has a bachelor's degree in MIS from California State University, Chico.



Galeal Zino **CEO and Founder** **NetFoundry**

Galeal is the Founder and CEO of NetFoundry. Prior to NetFoundry, Galeal was Founder and President at LocalReplay, VP of Engineering at Teleglobe and VP of Development and Engineering at ITXC. Galeal's teams helped develop and engineer the world's largest VoIP network and build global collaboration and video meeting products.

Galeal has been awarded eight patents for the software and platforms powering those products, and the patented software currently powers the services of many of the world's top communications providers. Galeal was born in New York, graduated from Bucknell University and currently resides Salisbury, NC area with his wife and their four children.



Tommy Todd **Vice President of Security** **Code42**

Tommy Todd is Vice President of Security at Code42 with over 20 years of cybersecurity experience, primarily focused on data privacy and data protection strategies.

Prior to Code42, Tommy served in security roles at Symantec, Ionic Security, and Optiv as well as many other firms. Throughout his career, he has acted as a leader, mentor, engineer, architect, and consultant to solve difficult data protection challenges.

Tommy is passionate about data – both consumer and commercial – and strives to improve the security posture in organizations he works with.

Event Agenda

8:00-9:00am Exhibitor Area Open, Attendee Networking *

9:00-9:05am Session Kick-off

9:05-9:15am Welcome Message from Appalachian State

9:15-10:00am **Morning Keynote: Managing Cyber Risk & Protecting Your Organization's Most Important Asset**

Marc Varner, Chief Information Security Officer, Lowe's

In this module Marc will share his views and experiences on the role risk management plays in an organization's ability to apply appropriate level of control and security to protect its most valuable asset.

10:00-10:30am **Software Bill of Materials – Understanding the Executive Order & Helping Developers Be Secure**

Elliott Johnson, Principal Solutions Architect, Veracode

The most recent Executive Order requires organizations to produce a Software Bill of Materials to deliver software to the Federal Government. The impact this has on Software Development Companies by far exceeds what most anticipated and many are yet to understand its implications. Modern applications use many Open-source libraries to speed delivery and shorten time to market (why reinvent the wheel if you don't have to?). However, it is important to understand what is in these libraries, so if there are vulnerabilities then they can be addressed properly and reported on accurately. This presentation will explain the Executive Order, its importance, and how you can leverage Veracode to generate an SBOM and help developers be more secure in their application development process.

10:30-10:45am **MORNING BREAK** – Exhibitor Area Open

10:45-11:15am **What Security Professionals Get Wrong About OT/ICS Security (and what it could cost)**

Austen Byers, Technical Director, Americas, TXOne Networks

In this presentation, we take a close look at how OT breaches occur, and how the financial impact of these breaches has tangible long-term effects on organizations. Learn proactive approaches to OT security that are being adopted by some of the world's largest industry leaders, as well as how to ensure that your OT security strategies generate value for your customers and shareholders.

11:15-11:45 am **Trends in Cyber Security & The Growing Talent Gap**

Aaron Rose, Cyber Security Evangelist, Check Point

In the last 25 years, attacks and security protection have advanced rapidly. Looking back it's easy to identify the different generations of attacks and security products that protect against them. However, today the velocity of attack evolution is far outpacing the level of security that organizations have deployed. This has surfaced another issue, talent. There is an estimated 3.5 million open cyber security jobs globally. Given the dangerous threat landscape this means the skills shortage represents an existential threat to our nation, critical infrastructure, and society at large. In this session we'll discuss the evolution of cyber threats, protections to counter them, and how the educational institutions of the world can help address the growing cyber talent gap.

Event Agenda

11:45-12:15pm

Zero Trust Network Access 2.0: A Framework for Network Security

Doug Sept, Systems Engineer, Palo Alto Networks

As enterprise architectures have become more distributed, interest in zero trust strategies has exploded. However, confusion with regard to zero trust has risen even as the term has become ubiquitous. Zero trust should be viewed as a strategy or framework on which a security program can be built around 3 key principles: (1) Never trust, always verify, (2) Least-privilege, and (3) Continuous assessment.

12:15-1:15pm

Lunch

1:15-2:00pm

Afternoon Keynote: Prevention, Detection, and Response

Jim Guido, EVP Engineering, HighPoint

Identifying key digital assets is the start of an effective cybersecurity prevention, detection, and response program. Understanding the state of the threat landscape and attack vectors is critical to align resources and initiatives to reduce the risk associated with cybersecurity strategy. Effective cybersecurity strategies include digital, physical, and human measures.

2:00-2:30pm

Cyber Threats to the Power Grid

Martin Strasburger, Chief Information Security Officer, Duke Energy

The power grid is arguably our nation's most critical infrastructure and in 2022 the threat of cyber attack is very real. Russia demonstrated in 2015 and again in 2016 that a well-executed cyber-attack against the power grid can cause crippling blackouts. Without reliable power all of our modern technologies and advances are rendered useless which is why protecting the power grid is top of mind for many people. In this presentation, Martin Strasburger – VP/CISO at Duke Energy, will discuss the cyber threats facing the United States power grid and the key actions that the US government and private grid operator are taking to defend against these threats.

2:30-3:00pm

Enhancing SecOps Practices with MITRE

Chris Boehm, Technology Strategist, SentinelOne

MITRE Engenuity ATT&CK Evaluations emulations are constructed to mimic an adversary's known TTPs and are conducted in a controlled lab environment to determine each participating vendor's product efficacy. Understand how to continuously tune your security strategy and leverage the connection between TTPs, adversary emulation plans, and real-world adversary groups.

3:00-3:15pm

AFTERNOON BREAK – Exhibitor Area Open

Event Agenda

- 3:15-3:45pm** **Cybercrime & War in the New Digital World**
Sushila Nair, VP Security Services, NTT Data
The Pentagon calls cyber-space the fifth domain of conflict in addition to land, sea, air and space. Cyberspace offers vast opportunities for businesses, but it also increases the risk of becoming the focus of attack from criminals or unfriendly nation states. In 2017 the world came the closest it has ever come to cyberwar. There is no doubt that at some point a crippling cyber-attack on critical infrastructure in a major economy will reoccur. In this session, we will cover the evolution of cyberwar and cybercrime. We will look at how businesses should work to minimize the risk of becoming collateral damage in the war of tomorrow.
- 3:45-4:15pm** **The Evolution of Zero Trust Networking**
Galeal Zino, Founder and CEO, NetFoundry
We are in the early innings of zero trust networking, and it can be difficult and complex. The next major step is for the zero trust networking experience to be closer to building encryption into an application, as opposed to "bolting-on" day two networking and security infrastructure. This both provides a more secure environment, and one that is simpler to manage, extend and scale.
- 4:15-4:45pm** **Changing Behaviors Through Meaningful Response**
Tommy Todd, VP of Security
In today's remote world where insider risk is a growing concern, security teams everywhere are having to rethink their technical controls and how they impact the end user. By combining an insider risk response with "in the moment" micro training, security teams can dramatically change behaviors to prevent further data exposure. By attending this session, we will discuss how taking advantage of complete data visibility and combining it with a more meaningful non-technical response can be a game changer for security professionals.
- 4:45-4:55pm** **Meeting Recap & CIS Cyber Program Update**
- 4:55-5:00pm** **Social Hour Kick-off, Gary Daemer, InfusionPoints**
- 5:00-6:00pm** **Social Hour**
- 6:00pm** **Event Ends**

Event Sponsors

Platinum



Gold



Social



Silver





Cyber Summit Event Tickets are \$75

Please Register at <https://cis.appstate.edu/cyber-summit-2022>

For more information, please contact the Cyber Summit Event Coordinator,
Samantha Williams at williamsse11@appstate.edu