New York State Cyber Security Conference
June 7-8, 2022

Governor Kathy Hochul

Angelo "Tony" Riddick, NYS CIO

Presented by

NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

SCHOOL OF BUSINESS
UNIVERSITY AT ALBANY
State University of New York

THE NYS FORUM

Table of Contents

Empire State Plaza Public Space WIFI:
ESP-Public Wifi

Welcome Letter

June 7, 2022

Dear Attendee:

Welcome to the 24th Annual New York State Cyber Security Conference and the 16th Annual Symposium on Information Assurance (ASIA)! On behalf of the New York State Office of Information Technology Services (ITS), the School of Business at the University at Albany, State University of New York (SUNY), and The NYS Forum, Inc., it is our pleasure to offer you an agenda packed with exciting sessions and the opportunity to meet people from all over the country who share your passion for cyber security.

As information technology continues to evolve at an extraordinary pace we must continue to push forward and understand how the latest innovations impact you, your organization, and your cyber security environment.

To face the challenges that bring significant risk to our information, systems, and networks, cyber security must be an integrated part of our environment. Under the leadership of Governor Kathy Hochul, New York State continues to lead the nation in its efforts to continuously improve cyber security by innovating, securing, and transforming technology to help protect all New Yorkers and their businesses with some of the strongest cyber protections available.

We all have a role to play in cyber security. Whether you are just starting a career in cyber security or are already a seasoned professional or are just looking to improve your overall cyber awareness, this conference has something for you. With more than 50 sessions to choose from, this conference brings you the latest on security evolution, the current threat landscape, and the newest technology trends. To get the most out of your conference experience, we encourage you to engage with your peers, dive into the sessions, get motivated by the keynote speakers, participate in the interactive training, and be inspired by what we can learn working together.

Thank you for attending the 24th Annual New York State Cyber Security Conference and bringing your expertise. We hope you leave with the vision, knowledge, and experience to help us strengthen our cyber security future. Thank you for your continued commitment to cyber security and for being part of this great event. Enjoy the conference!

Sincerely,

Mario J. Musolino

Executive Director
The NYS Forum, Inc.

Angelo Riddick
COL US Army Retired, PMP
NYS Chief Information Officer and
Director of Office for Technology

Dr. Nilanjan Sen

Massry Center for Business

Conference Co-Hosts

Mario J. Musolino
Executive Director NYS Forum

Mario J. Musolino, joined the NYS Forum as Executive Director in 2019. Previously Mr. Musolino spent twelve years as Executive Deputy Commissioner and Acting Commissioner at the NYS Department of Labor where he supervised operations of the Department and developed policies and procedures impacting millions of New Yorkers. In that role he oversaw upgrades to the Unemployment Insurance System, the Career Center network, and the NYS Job Bank among other technology projects.

Prior to his appointment at the Department of Labor, Mr. Musolino was the Executive Director of the Troy Housing Authority and the Deputy Director of the Office of Management and Budget for the City of Troy, with a broad range of responsibilities including Public Safety, Community Development, and Technology. Mr. Musolino also served as the Deputy Director of the New York State Job Training Partnership Council and the Executive Director of the Governor's School and Business Alliance Program. Mr. Musolino also worked for three years as a policy analyst for the Minority Leader of the New York State Senate. He began his career in public service as a youth counselor in Rensselaer County Jail.

Mr. Musolino holds an Associate Degree in Criminal Justice from Hudson Valley Community College and a Bachelor's Degree in Political Science from the State University of New York. He has also completed graduate coursework in public administration at Rockefeller College.

Join us for a Continental Breakfast each morning
in the Exhibit Hall!
June 7 breakfast sponsored by Google Cloud
June 8 breakfast sponsored by Deloitte

Conference Co-Hosts

Angelo Riddick, COL US Army Retired, PMP

NYS Chief Information Officer and Director of Office for Technology

In 2020, Angelo "Tony" Riddick, began serving as the Chief Information Officer (CIO) for the New York State Office of Information Technology Services (ITS), the state's governmental IT service and delivery operation, where he oversees more than 3,400 employees who perform a variety of services for the NY State IT Enterprise ranging from application development to Cyber Security and Data Center Operations.

As a highly decorated, retired U.S. Army Colonel having served 30 plus years active duty, including supporting Operations Desert Storm, Desert Shield, and participating in Operation Enduring Freedom and New Dawn, Tony held several key military Combat, Logistics and IT positions.

In 2014, Colonel Riddick retired from the military. His final assignment was as the Chief of Concepts Directorate for the Army's newly formed Cyber Command. He began working for a private defense contractor providing business development services in Cyber Security and IT.

Prior to joining ITS, Tony served as the Chief Information Officer and Director of the Bureau of Information Technology for the United States Virgin Islands. During this time, he engineered the reestablishment of all communications and rebuilt the IT infrastructure following the 2017 devastation from hurricanes Maria and Irma, earning the 2018 State Scoop State Executive of the Year Award for his efforts. He served as CIO for nearly 3 years.

Tony was commissioned at Marion Military Institute and attended Albany State University in Georgia. He earned his post graduate degree from the National Graduate School and executive education at the National Defense University (NDU), where he became a faculty member, and upon graduation, taught master's degree level courses in Information Technology Leadership, Cyber Security and CIO Operations over the next six years.

Tony holds a master's degree in Quality System Management from the National Graduate School and several IT certificates from the National Defense University. He is also a certified Project Management Professional. Tony is a graduate of all requisite U.S. Army military schooling, including the Command & General Staff College and was selected to participate in the Army's War College in 2005.

He has chaired numerous Information Technology Committees including a 5-state region for the Omega Psi Phi Fraternity where he led the effort to update and modernize Information Technology services for the 10,000+ membership region and served briefly as the fraternity's IT Committee chair overseeing IT services for the 200,000+ membership base.

Tony is married to the former Brenda J. Walker and has two sons, Gary and LaRico.

Conference Co-Hosts

Dr. Nilanjan Sen

Massry Center for Business

Nilanjan Sen, Ph.D., C.F.A. is currently the Dean, School of Business at UAlbany, State University of New York. Professor Sen received his Ph.D. from Virginia Tech and was previously a tenured faculty member at Arizona State University and Nanyang Technological University, Singapore. Dr. Sen currently teaches Mergers and Acquisitions and other advanced topics in Corporate Finance. He has published extensively in academic and practitioner journals.

UAlbany, School of Business is currently in the process of revising their program curriculum and initiating several new programs at undergraduate and graduate level, including double degrees with Asian universities. He is actively involved in UAlbany's ongoing capital campaign. Dr. Sen plans to work closely with School's alumni and industry partners to accelerate both internationalization and diversity initiatives and expand the footprints in executive education and talent management for the capital region.

Dr. Sen has provided leadership in several key initiatives at NTU. He was Associate Dean of executive programs from 2008-2014. He substantially expanded the open and custom program portfolio that included specialized programs for banks and MNCs in one of the highest growing regions. He launched an innovative EMBA program in 2007 that includes several industry tracks and attracts funding from multiple professional bodies and government agencies. The Nanyang EMBA made a debut at number 13 and was ranked as high as number 8 in the Financial Times ranking. He has also worked with several leading U.S. universities including Wharton, Cornell, Berkeley, and Georgetown McDonough Business schools to launch various Advanced Management Programs, targeting specific industry needs.

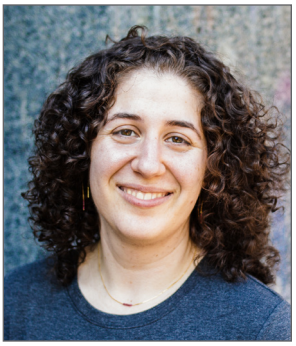
Dr. Sen subsequently led the school's initiative in integrating all of the graduate programs under the office of Graduate Studies to garner synergies in operations, marketing, and career services. He oversees curriculum, marketing, staffing as well combined budget for all graduate programs. The portfolio includes MBA, Executive MBA and several specialized masters. During his tenure, the school has also successfully launched Professional MBA and Masters in Accountancy. The Nanyang MBA program has doubled its enrolment in the last three years and was recently ranked number 18 in 2018 Financial Times Ranking. He is currently exploring innovative tripartite models in business education that deploy customized curriculum and diversified funding to include private sector businesses, governments and network ready graduates. This model seeks to build partnership with key academic institutions and expand the ecosystem that can jointly serve the expanding global talent development needs. He is also leading school's current initiative in brand positioning and associated curriculum review of all graduate programs to ensure that the future leaders are fully prepared for ongoing digital transformation in global business world.

Dr. Sen has conducted training programs for several corporations, banks, and government agencies, was the chief examiner for Certified Investment and Security Analyst Institute (CISA) in Thailand, and continues to be involved in CFA Level 3 review programs under FTC Kaplan. He has taught courses at various universities in China, Italy, India, Ireland, Norway, Spain and Switzerland. Professor Sen received the Researcher of the Year Award from School of Global Management and Leadership, Arizona State University and Best Teacher Award from the division of Banking and Finance, Nanyang Business School. He is also the recipient of the Teacher of the Year award in Executive MBA in 2016 and Financial Engineering program for 2006 and 2008. Dr. Sen enjoys squash, hiking, traveling and meeting people from diverse cultures.

Keynote – Day 1

International Cyber Conflicts and Development of Global Cyber Norms

June 7, 2022 | Meeting Room 6 | 9:00 a.m. - 10:30 a.m.



State-sponsored cyber campaigns have been an element of international conflicts for decades, but the ongoing Russian invasion of Ukraine has upended many assumptions and prior established patterns about how countries typically use cyber capabilities in the context of such conflicts. This talk will consider prior examples of Russian cyberattacks in Estonia, Georgia, and Ukraine, and then focus on the uses of cyber capabilities by Russia, Ukraine, and other countries and private companies over the course of the ongoing conflict and consider the ways in which these stakeholders have diverged from previous examples of cyber conflict. Finally, we'll consider the progress towards developing cyber norms through international forums since the early 2000s, and what lessons we can draw about cyberattacks and cyber conflict more broadly from this history, as well as how we can continue to update our ideas about the potential and risks of cyber capabilities for impacting international conflict.

Bio: Josephine Wolff is an associate professor of cybersecurity policy and has been at The Fletcher School at Tufts University since 2019. Her research interests include liability for cybersecurity incidents, international Internet governance, cyber-insurance, cybersecurity workforce development, and the economics of information security. Her first book "You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches" was published by MIT Press in 2018. Her second book "Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks" will be published by MIT Press in 2022. Her writing on cybersecurity has also appeared in Slate, The New York Times, The Washington Post, The Atlantic, and Wired. Prior to joining Fletcher, she was an assistant professor of public policy at the Rochester Institute of Technology and a fellow at the New America Cybersecurity Initiative and Harvard's Berkman Klein Center for Internet & Society.

Keynote – Day 2

Cyber Threat Landscape with FBI Albany

June 8, 2022 | Meeting Room 6 | 9:00 a.m. - 10:30 a.m.

FBI will discuss the evolution of cyber threats affecting the region and how the return to work after COVID has created new attack surfaces.

At-A-Glance Schedule, Day 1: June 7, 2022

8:00am – 4:15pm	**New York State Cyber Security Conference**						
9:00am	**Opening of the Exhibit Hall**						
9:00am – 10:30am	**Welcome Address** **ASIA Keynote: "International Cyber Conflicts and Development of Global Cyber Norms"** **Dr. Josephine Wolff, The Fletcher School at Tufts University**						
10:30am - 11:00am	**Visit the Exhibitors (Terabyte Sponsor Demo: Fortinet 10:35am-10:55am)**						
	Assessing Risk	**Cyber Strategy**	**Law & Policy**	**Security Evolution**	**Awareness**	**Threat Landscape**	**ASIA**
11:00am – 11:50am	State of New York: Breaking down IT Complexities and Risk Vulnerabilities Shawn Surber Tanium	Approaches to Integrating Multi-organization Security Jim Richberg Fortinet	What a Formula 1 Racing Crash Can Teach Us About Incident Response Mike Semel Rose Ketchum Semel Consulting, LLC	Cryptocurrency & Cybercrime an Introduction William Mendez Friedman CyZen	Be better, listen to a hacker Tyler Wrightson Leet Cyber Security	Verizon 2022 Data Breach Investigations Report Neal Maguire Verizon	**Cyber Threats**
	Meeting Room 5	**Meeting Room 4**	**Meeting Room 3**	**Meeting Room 2**	**Meeting Room 6**	**Meeting Room 1**	**Meeting Room 7**
11:50am – 1:00pm	**Lunch on your own and Visit the Exhibitors**						
1:00pm – 1:50pm	Size Matters – Why Cybersecurity Fails for 99.9% of Us Reg Harnish OrbitalFire	Star Power! Level up your cybersecurity program Jeff Baez Splunk	Digital Identity in support of the modern college experience Jeremy Anderson Gagan Pall Deloitte	Adapting Your Security Program to Evolving Cyber Threats Jennifer McLarnon Manoje Nair Accenture	Security Awareness Training Isn't Working. But This Will Robert Siciliano ProtectNowLLC.com	The Need to Improve Enterprise Resiliency to Combat Disasters and Cyber Attacks Hector Rodriguez Amazon Web Services	**Cybersecurity in Healthcare**
	Meeting Room 5	**Meeting Room 4**	**Meeting Room 3**	**Meeting Room 6**	**Meeting Room 2**	**Meeting Room 1**	**Meeting Room 7**
1:50pm – 2:10pm	**Visit the Exhibitors (Megabyte Sponsor Demo: Google Cloud 1:55pm-2:05pm)**						
2:10pm – 3:00pm	Assessing and Quantifying Cyber Risk Asha Abraham HubSpire Corp	The current cyber threat environment, Shields Up and CISA Cyber Security Resources Michael Hastings Cyber Security and Infrastructure Security Agency (CISA)	National Cybersecurity Policy: Prescriptive, Voluntary or Hybrid Robert Mayer US Telecom Association	War and Cyberwar Expert Panel Arctic Wolf	Common Security Challenges and Best Practices in a Hybrid Cloud Environment NYS Forum Information Security Workgroup	Managing Digital Identity Threats Through Data-Driven Risk Decisioning George Freeman LexisNexis Risk Solutions	**Invited Talk**
	Meeting Room 5	**Meeting Room 4**	**Meeting Room 3**	**Meeting Room 6**	**Meeting Room 2**	**Meeting Room 1**	**Meeting Room 7**
3:00pm – 3:20pm	**Visit the Exhibitors (Megabyte Sponsor Demo: Deloitte 3:05pm-3:15pm)**						
3:20pm – 4:15pm	Cybersecurity Tsunami is coming, are you ready? Sanjay Deo 24by7Security, Inc.	How to win friends and influence people: The secrets to getting security initiatives implemented and funded Matt Malone Vistrada, LLC	Mightier than the Sword: A discussion of the New York SHIELD Act Derek Boczenowki Compass IT Compliance, LLC	Demystifying Quantum Computing and associated risks: How do I deal with a threat that has not emerged yet? Kiran Bhujle SVAM International Shahryar Shaghaghi Quantam Exchange	The Fifth Dystopia: How AI Weaponizes Human Bias Antony Haynes Albany Law	Protecting Your Business in the Age of Ransomware Steven Keys Dell Technologies	**Cybersecurity in Critical Infrastructure**
	Meeting Room 5	**Meeting Room 4**	**Meeting Room 6**	**Meeting Room 3**	**Meeting Room 2**	**Meeting Room 1**	**Meeting Room 7**

At-A-Glance Schedule, Day 2: June 8, 2022

8:00am – 4:15pm	**New York State Cyber Security Conference**						
9:00am	**Opening of the Exhibit Hall**						
9:00am – 10:30am	**Welcome Address** **Keynote: "Cyber Threat Landscape with FBI Albany"**						
10:30am - 11:00am	**Visit the Exhibitors (Terabyte Sponsor Demo: Fortinet 10:35am-10:55am)**						
	Cloud Security	**Vulnerabilities**	**Defend & Protect**	**Zero Trust**	**Cyber Industry**	**ASIA**	**Interactive Learning**
11:00am – 11:50am	Securing Your Cloud Network Thomas Ricardo Vandis	Avoiding Server-Side Request Forgery (SSRF) Vulnerabilities in ColdFusion/CFML Applications Brian Reilly	VBS, DLLs, Obfuscation, Oh My! How I Safely Teach Malware Analysis James Antonakos Broome Community College	The Truth About Zero Trust: How to Mitigate Cyber Risks Ted Ede Rubrik	Everything You Ever Wanted to Know About How New York Elections Are Secured but Were Afraid to Ask Jeannine Jacobs Sean Murray NYSTEC Michael Haber Ben Spear NYS Board of Elections	Cyber Security Resilience	**Blue Team Challenge** **TrendMicro** **11:00am - 3:30pm**
	Meeting Room 2	**Meeting Room 3**	**Meeting Room 4**	**Meeting Room 5**	**Meeting Room 6**	**Meeting Room 7**	
11:50am – 1:00pm	**Lunch on your own and Visit the Exhibitors**						
1:00pm – 1:50pm	Ansible for the CDM use case Ajay Chenampara Red Hat	A Dynamic Process for Minimizing the Likelihood and Impact of Cyber Attacks Chris Jensen Tenable	Gotcha! How to Avoid the Top 10 Pitfalls in Security questionnaires, cyber Insurance Applications, Privacy Policies, and more Mike Semel Semel Consulting, LLC F. Paul Greene	Cybersecurity Culture: Effectively Promoting Security Throughout an Organization Dylan Famolaro iSECURE	How Cyber Insurance Integrates with Technology Companies Adam Cottini Crowdstrike	Insider Threats & Critical Infrastructure Threats	
	Meeting Room 2	**Meeting Room 3**	**Meeting Room 4**	**Meeting Room 6**	**Meeting Room 5**	**Meeting Room 7**	
1:50pm – 2:10pm	**Visit the Exhibitors (Megabyte Sponsor Demo: Deloitte 1:55pm-2:05pm)**						
2:10pm – 3:00pm	Managing Cloud Computing's Cybersecurity and Information Risk Dean Maloney GreyCastle Security	Managing Business Risks Using Vulnerability Scanning Diane Reilly Carson & SAINT Frederick Scholl Monarch Information Networks	At the Heart of the SOC: Apache Kafka & Data Streaming for Cyber Operations Bert Hayes Bob Liebowitz Confluent	How You Can Implement Well-Architected 'Zero Trust' Hybrid-Cloud Computing Beyond 'Lift & Shift': Cloud-Enabled Digital Innovation At Scale with Infrastructure as Code (IaC), DevSecOps & MLOps Dr. Yogesh Malhotra Global Risk Management Network, LLC	Hardened DevSecOps Pipelines – Secure Your Software Supply Chain Darren Pulsipher Intel Corp	Forensics Education	
	Meeting Room 2	**Meeting Room 3**	**Meeting Room 6**	**Meeting Room 4**	**Meeting Room 5**	**Meeting Room 7**	
3:00pm – 3:20pm	**Visit the Exhibitors (Megabyte Sponsor Demo: Google Cloud 3:05pm-3:15pm)**						
3:20pm – 4:15pm	Centralized Data Protection Gateway Phaneendra Bhyri Karl Erber Prutech Solutions	Securing APIs in an increasingly connected ecosystem Bhaskar Agarwal Nagarro Inc.	At the Heart of the SOC: Apache Kafka & Data Streaming for Cyber Operations Bert Hayes Bob Liebowitz Confluent	Zero trust execution in 2022 Matthew McFadden General Dynamics Information Technology	How to improve the current state of Industrial Control Security David Beidelman Stratascale	Intrusion Detection	
	Meeting Room 2	**Meeting Room 6**	**Meeting Room 4**	**Meeting Room 3**	**Meeting Room 5**	**Meeting Room 7**	**Meeting Room 1**

2022 Session Descriptions

DAY 1
June 7 - 11:00am-11:50am

State of New York: Breaking Down IT Complexities and Risk Vulnerabilities

Shawn Surber, Tanium

Every 11 seconds, there is a ransomware attack. Yet organizations are spending over $160B on cybersecurity this year alone. While security budgets are rising every year, the vulnerability gap isn't improving - it's only getting worse. In addition, the network and end point landscape has become overly complex. Managing risk is one of the top responsibilities of any elected official in the public sector. But they can only manage the risks they know about. And with silos that often plague public sector agencies of all types, from the state government to K-12 school districts, there can be many unknowns. Silos don't work in IT. The old model of unreliable tools, broken processes and incomplete outcomes is being disrupted. Public sector organizations need unified data platforms to enable the flow of information across teams, agencies, and departments to surface critical data faster and more accurately. Identifying and remediating risk is mission-critical, but the proliferation of data and devices has created a constantly morphing and expanding network edge. Organizations need to unify tools and data, creating a system that acts as the backbone for all crucial interactions and IT decisions. A single control plane that functions as the nerve center of the domains in IT Operations, Security, Risk and Compliance Management. During this session, we'll discuss:

- Identifying and Remediating Risk
- Modernizing Legacy Platforms and Environments
- Ongoing Compliance and Regulatory Demands
- Converging IT Operations and Security to tackle challenges at one team - one fight

Tweet the conference at #nyscyber

Approaches to Integrating Multi-organization Security

Jim Richberg, Fortinet

With New York creating a Joint Security Operations Center, government and critical infrastructure owners/operators receiving funding to refresh infrastructure and increase cybersecurity, and increasing serious cyber threats, producing shared cyber situational awareness and integrated response is a top-of-mind issue. The challenges of creating a federated/joint capability across organizations is different from building a Security Operation Center within a single enterprise. The session will explore the building blocks, alternative approaches, and some of the presenter's lessons learned from building and integrating these capabilities in the U.S. Government.

What a Formula 1 Racing Crash Can Teach Us About Incident Response

Mike Semel and Rose Ketchum, Semel Consulting LLC

When it comes to cyber incident response, there's a lot to be learned from a Formula One crash. There's more in common than you might think between what it took for a driver to survive a high-speed wreck and what you can do to survive a data breach or ransomware attack. I'll put you in the driver's seat to see if you could have survived the crash, and if you are really prepared to survive a cyber incident. (Don't be so sure that you are invincible.)

Cryptocurrency & Cybercrime: An Introduction

William Mendez, Friedman CyZen

The session will introduce participants to the world of cryptocurrency and its dual role in facilitating crime and as a victim of cyber attacks perpetrated by cyber criminals. The presentation provides a basic high-level introduction to block chain technology as it relates to cryptocurrency. It will also provide a general overview of why cryptocurrency is used by cybercriminals and discuss concepts of anonymity and laundering. As more people and organizations begin to dabble in cryptocurrency or blockchain general, it is important that they understand the emerging cyberthreats in this space. As such, the presentation will discuss current cyberattacks against legitimate cryptocurrency organizations and their clients. The ultimate goal is to provide the participants with a basic knowledge of cryptocurrency, its ability to facility criminal activity, and current threats that may affect anyone thinking of investing in cryptocurrency.

2022 Session Descriptions

Be better, listen to a hacker

Tyler Wrightson, Leet Cyber Security

There are common challenges with every cybersecurity program. To effectively lower risk from hackers you must understand them, think like them, and most importantly communicate about them. Join Tyler (a pure red teamer) to understand strategic and tactical things you can do tomorrow to increase the efficacy of any cybersecurity program or position.

Verizon 2022 Data Breach Investigations Report

Neal Maguire, Verizon

Dive deep into the latest publication of the Verizon Data Breach Investigations Report – the most widely read security research report in the world. The session will cover the most notable and actionable shifts in the cybersecurity threat landscape along with key insights from Verizon's Insider Threat Report. Attendees will learn from real-world investigations regarding threat actor tools, techniques, and procedures, along with a walkthrough of a recent case study. The report leverages dozens of contributing organizations from around the world in order to provide the best possible cross-sectional view of the threat landscape.

ASIA Session 1: Cyber Threats

Paper: FRUITY: Automated Behavioral Convert Channels on the Discord Application

Paper: Covert Channels in Poptropica

Don't forget to grab your official conference bag at registration. AT&T is the 2022 NYSCSC Bag Sponsor!

DAY 1
June 7 - 1:00pm-1:50pm

Size Matters – Why Cybersecurity Fails for 99.9% of Us

Reg Harnish, OrbitalFire

When cybersecurity was invented some 60 years ago, it had a big job. Protecting cold war secrets from hostile state actors meant thinking through all possibilities and all threats – after all our lives depended on it. Fast forward 60 years, and cybersecurity has become even bigger and more complex. Today, most common frameworks have hundreds – even thousands – of controls. Perhaps this makes sense for Fortune 500 enterprises, but it's incomprehensible for 99.99% of the US economy: small businesses. If we have any shot at herd immunity, we're going to need to inoculate more than just the biggest organizations on the planet.

Join Reg Harnish, CEO of OrbitalFire, Founder and former CEO of GreyCastle Security and former EVP of the Center for Internet Security as we explore cybersecurity solutions that are more accessible, affordable, and applicable to the rest of us.

Star Power! Level Up Your Cybersecurity Program

Jeffrey Baez, Splunk

A Security Maturity Methodology (S2M2) is a security assessment tool that aligns the strategic and operational goals of a cybersecurity program, combining equal parts people, process, and technology, to help organizations mature their security program born out of several security best practices, frameworks, and industry standards. For SLED leaders to derive value associated with data, innovation requires visibility across the technology stack. Without access to ITOps, DevOps, or SecOps data, and the analysis to make sense of it all, it is virtually impossible to reduce overall risk effectively. This eloquently sums up the challenge executives face to protect their organizations from cyber attacks but often fail to prioritize preparation or assume a bevy of security products has them covered. The S2M2 assesses the maturity of a cybersecurity program using measures pertaining to the various cybersecurity frameworks and a guided journey to understand existing business operations and then provide guidance on how to mature their operations based upon business priorities. The outcome of the S2M2 provides a security roadmap that an organization can use to bring their security program maturity to the next level. The maturity model in the

2022 Session Descriptions

roadmap uses a multi-level model, signified by "Maturity Indicator Levels (MIL)," to assess the current state and to identify the areas that need to be worked on.

Key Benefits:

- Demonstrable decreased business risk
- High fidelity, contextual security alerts
- Discover true positives faster
- Identify and remediate gaps in SOC operations
- Proactively detect, investigate, and defend against threat actors
- Automations that decrease response time and team effort
- Achieve internal and external compliance

Digital Identity in support of the modern college experience

Jeremy Anderson and Gagan Pall, Deloitte

In support of a modernized college experience, higher education IT infrastructure is changing rapidly. Enabling future direction is the idea of marrying in-person and remote users with on-premises and cloud-based resources into a single hub, then wrapping this virtualized student union in a frictionless identity-centric blanket of security. Learn how colleges and universities are using digital identity to enable student experiences, promote collaboration and integration across institutions.

Adapting Your Security Program to Evolving Cyber Threats

Jennifer McLarnon and Manoje Nair, Accenture

In this session we will provide an overview of the global threat and information landscape, especially in light of Russia's invasion of Ukraine, subsequent cyber-related events, as well as threats from the Great Resignation. We will highlight industry-specific threats and share universal, practical recommendations to help organizations increase their resiliency, mitigate risks, and protect access to and counter rising costs of cyber liability insurance. We will focus on tactical measures and the benefits of targeted assessments, roadmaps, incident response retainers and the pros and cons of managed security services.

Security Awareness Training Isn't Working. But This Will.

Robert Siciliano, ProtectNowLLC.com

Our philosophy is "all security is personal." Personal security is violence and theft prevention in the physical and virtual world. People don't want to think about, nor do they believe, that security incidents can or will happen to them; therefore they generally discount the realities or the vulnerabilities that they or their business might face. They function in denial that it can happen to them. As a result of this denial, they fail to engage in security functions in the workplace. We show them through a transformative process how security is easy, good for you, empowering and a personal benefit to them, as well as how it enriches their lives and benefits their employers. We provide a very different and positive perspective. When teaching security awareness and making it personal, the student is more likely to take action in the workplace as it is first about them Our goal is to elevate the attendees' experience and change their behavior to the level of "security appreciation," which is not simply an acknowledgment of security issues, but an action-oriented appreciation for the value that security provides.

The Need to Improve Enterprise Resiliency to Combat Disasters and Cyber Attacks

Hector Rodriguez, Amazon Web Services

Disasters, whether human-made or natural, are unavoidable, so planning for them is critical to ensuring your organization can continue to operate regardless of the situation. Most organizations are aware of and planning for high-profile data breaches and ransomware, but many are not prepared for the most common types of disasters and human errors. Any IT downtime can impact data access and cause interruptions in operational performance system wide. This session will outline common IT disasters, explore the need for organizations to be more resilient, and provide an overview of enterprise resilience and where it's needed. As well as differentiate between resiliency and disaster recovery, discuss resiliency, and explore more resilient options for preparing for and mitigating risks. Attendees will learn how a hospital has started its journey to be more resilient to disasters (use case).

ASIA Session 2: Cybersecurity in Healthcare

Paper: Security Breaches in Healthcare Organizations: An Exploratory Mixed Method Study

Paper: Impact of ransomware on health and safety of individuals: Reflections from recent breaches

2022 Session Descriptions

DAY 1
June 7 - 2:10pm-3:00pm

Assessing and Quantifying Cyber Risk

Asha Abraham, HubSpire Corp

Data, intellectual property, and other technologies drive market value today – these are the intangible assets that fuel our digital economy. The World Economic Forum's 'The Global Risks Reports' ranks cybersecurity failure as a significant global risk for the last few years now. In an increasingly connected world where technology domains converge to create new and innovative digital business opportunities, cyber threat scenarios have the potential to challenge business viability if cyber risk management is not built into the business strategy. In this session, we will talk about how to make cyber risk more measurable for your organizations and enable data-driven decision making.

The Current Cyber Threat Environment, Shields Up and CISA Cybersecurity Resources

Michael Hastings, Cybersecurity and Infrastructure Security Agency (CISA)

National Cybersecurity Policy: Prescriptive, Voluntary or Hybrid

Robert Mayer, US Telecom Association

The session will explore major cybersecurity policy directions and the expanding role of multiple entities including initiatives in Congress, the White House, regulatory agencies and at key cabinet agencies. Given the increasing threats from nation state adversaries and the reality that the vast majority of U.S. critical infrastructure is in the hands of the private sector, the session will draw on current research and developing government infrastructure to assess the viability of public-private partnerships, compliance regimes, and other emerging innovative hybrid models.

War and Cyberwar Expert Panel

Arctic Wolf

Gas prices are at an all-time high. Nation state threat actors have crippled hundreds of corporations in recent high-profile breaches. Russia is at war with Ukraine, raising fears of retaliation against U.S. infrastructure, financial, and other segments.

This presentation is meant to unpack some of the behind-the-scenes geopolitical and cyber posturing that is happening across the world right now. After this event, you'll be better prepared to defend against and respond to cyber-attacks and to do so expeditiously.

Our experts have decades of combined experience in both offensive and defensive cybersecurity risk management and law. We've been a part of breaches, including working with law enforcement agencies on a local and federal level.

Common Security Challenges and Best Practices in a Hybrid Cloud Environment

Grace Dillon, NYS Information Technology Services, Moderator
The NYS Forum Information Security Workgroup
Stephen Clark, Fortinet
David McCurdy, Amazon Web Services
Andre Alves, Trend Micro
Jonathon Mahoney, Presidio

Please join the NYS Forum's Information Security workgroup for this fireside chat regarding Common Security Challenges and Best Practices in a Hybrid Cloud Environment. Grace Dillon, executive Director of Revenue, Finance and Public Integrity Portfolio at the New York State Office of Information Technology Services, will moderate this engaging and interactive panel and pose questions to four experts in the field. Our expert speakers will answer questions such as: How are organizations handling the transition form on Prem, hybrid to cloud-only applications; Is cloud-native security really fundamentally different than my already well-established cybersecurity practice; What lessons did the CTO of Colorado learn after being subject to a state cyber attack; and, Why is there often a disconnect between the DevOps team and the traditional Security Team? Our experts will also be able to answer your questions on these and other questions.

2022 Session Descriptions

Managing Digital Identity Threats Through Data-Driven Risk Decisioning

George Freeman, LexisNexis Risk Solutions

Identity fraud is impacting organizations globally resulting in endless data breaches, new threat vectors like supply-chain attacks, and user personally identifiable information (PII) harvesting through social engineering. A recent statistic confirms that approximately one-third of online transactions are from BOTs or fake identities. Add to that the exponential volume of stolen identity data, which is being bought and sold on the dark web, has fueled recent increases in identity fraud. As digital identity gradually replaces physical identity, online users are now facing a growing world of identity threats. Digital identity data-driven risk decisioning provides a robust workflow that addresses the rising threat of identity fraud utilizing multiple touch points. The differentiator in this design is a secure repository of global device and user-persona history data. Protecting organizations' portals from bad actors is accomplished by matching customer, citizen, or employee device/identity attributes to a data analytics-driven digital identity and its digital risk history. By processing this data through an intelligent, rules-based policy, organizations can make split-second automated risk decisions on any device/identity before letting them through the front door.

ASIA Session 3: Invited Talk

Invited Talk: Digital Privacy

Thank you to NYSTEC for sponsoring lanyards for the 2022 NYSCSC!

DAY 1
June 7 - 3:20pm-4:15pm

Cybersecurity Tsunami is Coming; Are You Ready?

Sanjay Deo, 24By7Security, Inc.

With increasing earth population and over 4.5 billion humans connected to the internet, everybody is leveraging internet connectivity for productivity increase and financial benefits. As the internet is being used by companies and people alike for their benefits, so are bad actors who are using the internet to perpetrate various crimes, posing huge risks to businesses and to each other. This level of connectivity and advancement has led to the rise of cyber crime, which is focused on stealing data, hacking into IOT devices, and stealing intellectual Property. The U.S. Government has implemented a number of recommendations and regulations regarding Critical Infrastructure Protection and reporting. This presentation is focused on discussing the implications of privacy and security and how to manage the cybersecurity risks.

Learning Objectives: Executives will learn

- Cybersecurity Landscape and impact on various industries, specifically Financial Services
- Privacy and Security Regulations and various risks (Regulatory, Financial, Reputation)
- Cybersecurity Terminology to decipher what the CIOs and CISOs are talking about
- Ransomware mechanics - Roles, Responsibilities and To Pay or not to Pay?

How to Win Friends and Influence People: The Secrets to Ggetting Security Initiatives Implemented and Funded

Matt Malone, Vistrada, LLC

When trying to implement security, one of the main hurdles is people. Lack of buy-in, not seeing the ROI, security is complicating things – there are lots of reasons that security initiatives are not funded. This course is designed to show attendees ways to get things funded, get initiatives moving and change the culture of the organization. People fund things, people hold things up, people go around security controls when it's more convenient. We will teach security professionals how to bring people together, to change company culture and to sell security as a benefit and not a cost.

2022 Session Descriptions

Mightier than the Sword: A Discussion of the New York SHIELD Act

Derek Boczenowski, Compass IT Compliance, LLC

Join us as we look at the Stop Hacks and Improve Electronic Data Security (SHIELD) Act. The act was enabled in 2019 to strengthen New York State data security requirements. During this presentation, we will provide guidance on what the law contains, who is required to adhere to it, go over private information definitions (based on the SHIELD act), discuss the safeguards the law requires to be in place, and offer suggestions on steps to take both internally and technologically to achieve compliance and secure private information!

Demystifying Quantum Computing and Associated Risks: How do I deal with a Threat That Has not Emerged Yet?

Kiran Bhujle, SVAM International Inc.

Shahryar Shaghaghi, Quantam Exchange

Until a few years back, quantum computing was often seen as a technology that would emerge in the distant future. Since then, we have been seeing a significant push to bring quantum computers into the mainstream, which will have a transformative impact on organizations, businesses, and society. In this session, we will discuss the evolution of quantum computers, the timeline, and what can I do now?

The Fifth Dystopia: How AI Weaponizes Human Bias

Antony Haynes, Albany Law

Without swift, decisive action, the promise that machine learning/artificial intelligence will bring about a more just and humane world will not simply be frustrated but permanently inverted. A world of unceasing and unchallenged inequity, permanently enshrined by invisible, ubiquitous, computer code would be a future closer to racial and genetic caste system of Aldous Huxley's Brave New World than anything resembling the ideals of liberal democracy. The world we are creating is a software algorithmically-enforced apartheid, where automated decision-making software enforce an eternally rigged status quo. Step by step, line of code by line of code, our smartest and most innovative organizations in technology and science are ensuring that all the technology – from sink faucets to package delivery, from resume scanners to language translation, from face recognition to criminal sentencing – all encode and perpetuate the gender, racial, and other biases present in human society.

Protecting Your Business in the Age of Ransomware

Steven Keys, Dell Technologies

Data is the lifeblood of business and other organizations in this digital age. Yet that data and the applications running the business are under constant attack. Nation states create cyber weapons that lock up data centers, sophisticated criminals employ the latest capabilities to gain access and encrypt data for ransom while destroying backups, and the threat of insiders becomes more critical as the stakes grow higher. In this session, learn the details about how sophisticated cyber-attacks occur; why cyber insurance isn't enough and why paying a ransom must be the option of last resort; and techniques and capabilities that can ensure your businesses' ability to recover safely and efficiently from even a sophisticated cyber disaster.

ASIA Session 4: Cybersecurity in Critical Infrastructure

Paper: Emerging Ransomware Threats: Insights from Recent Research

Paper: Cybersecurity for Autonomous Vehicles: Attacks and Defense Strategies

DAY 2
June 8 - 11:00am-11:50am

Securing Your Cloud Network

Thomas Ricardo, Vandis

Today over 40% of enterprise workloads run in the public cloud. Network and security teams must overcome hurdles such as visibility and access control of ephemeral cloud assets in the environment. These teams need to adopt Infrastructure as a Code (IaaC) best practices and begin the process of migrating their change control to adapt to a CI/CD model of deployment. Not only are teams changing what they are working on, but they must also adapt to the way they operate and execute. The session will discuss how to overcome these challenges and provide insights into how to secure your cloud network. Topics will include a discussion on the evolution of cloud networking, lessons learned, and the future of securing hybrid networks. We will focus on role-based access control, the elimination of the edge, SD-WAN integration into the cloud, and cloud networking constructs like Virtual Networks and Virtual Private Clouds (VNets and VPCs). We will also highlight the security concerns and solutions built to help teams adapt to the changing landscape of networking.

2022 Session Descriptions

Avoiding Server-Side Request Forgery (SSRF) Vulnerabilities in ColdFusion/CFML Applications

Brian Reilly

ColdFusion/CFML remains a popular application development platform for government, commercial, non-profit, higher education, and other industries. My goal for this talk is to raise awareness about what may be a security blind spot for some ColdFusion developers. Server-Side Request Forgery (SSRF) vulnerabilities allow an attacker to make arbitrary web requests (and in some cases, other protocols too) from the application environment. Exploiting these flaws can lead to leaking sensitive data, accessing internal resources, and (under certain circumstances) remote command execution. Several ColdFusion tags and functions can process URLs as file path arguments, including some tags and functions that you might not expect. If these tags and functions process unvalidated user-controlled input, this can lead to SSRF vulnerabilities in your applications. In addition to providing a list of affected tags and functions, I'll cover some approaches for identifying and remediating vulnerable code.

VBS, DLLs, Obfuscation, Oh My! How I Safely Teach Malware Analysis

James Antonakos, Broome Community College

In this presentation I will show how a second-semester, 15-week Malware Analysis course is taught to students with only a single programming course under their belts. Malicious examples of VBS, Javascript, Powershell, EXE, DLL, ASP and more are provided, all culled from actual DFIR investigations. Details are provided on how each type of malware is handled safely, as well as the different tools used during the course, from CyberChef to IDA.

The Truth About Zero Trust: How to Mitigate Cyber Risks

Ted Ede, Rubrik

Every week the news on ransomware attacks gets worse. When you're up against an organized, well-resourced attacker, you need to think again about how your municipality defends against attacks. But when you don't know the blast radius of an attack, whether sensitive data is affected, and how long it may take to recover, often the only option is to pay up. The best defense is Zero Trust - employing security at the point of data. But how do you employ Zero Trust, and how do you put in place an architecture that means your backups truly are immutable?

Attend this session to learn:

- Why you need to think differently about data security.
- Why Zero Trust should be a strategic priority for every organization.
- Best practice for implementing the principles of Zero Trust.
- How to build effective protection against ransomware.

Re-energize with a beverage and snack!
Afternoon Breaks sponsored by Zerto
June 7 at 3:00 p.m. – 3:20 p.m.
June 8 at 3:00 p.m. – 3:20 p.m.

2022 Session Descriptions

Everything You Ever Wanted to Know About How New York Elections Are Secured but Were Afraid to Ask

Sean Murray and Jeannine Jacobs, NYSTEC
Ben Spear and Michael Haber, NYS Board of Elections

Since the U.S. Government acknowledged foreign intrusion attempts in 2016 and 2020, election security has been an increasingly hot topic for discussion. With misinformation and attacks on election trust and integrity appearing in the news and media on a regular basis, understanding the truth about the procedures and protections in place to protect the electoral process here in New York is more important than ever. In a moderated panel discussion, our panel of election and security experts from the NYS Board of Elections and NYSTEC will address the topics below as well as answer questions from the audience:

- Election Infrastructure in New York Security and Oversight of Voting Technology
- County Operations and Systems
- Vote Tabulation and Audit of Results
- Paper Ballots & Absentee Voting
- And So Much More!

ASIA Session 5: Cybersecurity Resilience

Paper: A Combative approach for enhancing Cybersecurity Resilience: Systemic Synthesis of Industry Risks, Practices and Outcomes

Paper: Vulnerability Assessments

Join us next year for the 25th Anniversary of the New York State Cyber Security Conference!

DAY 2
June 8 - 1:00pm-1:50pm

Ansible for the CDM use case

Ajay Chenampara, Red Hat

The Continuous Diagnostics and Mitigation (CDM) Program provides a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM technical capabilities laid out by Homeland security lists 4 Phases to this approach. In this talk we'll look at how Ansible can help agencies achieve the CDM capabilities through repeatable, reusable automation.

A Dynamic Process for Minimizing the Likelihood and Impact of Cyber Attacks

Chris Jensen, Tenable

Cyber attacks, including ransomware and other state-sponsored exploits, continue to increase with no letup in sight. Defending against those attacks is a challenging, but not impossible, task. An effective cyber defense needs to be multi-layered, just like an effective physical security plan. In this presentation, we will highlight the importance of a dynamic risk-based vulnerability management program that focuses on three primary attack paths, and we will recommend defensive measures to disrupt those attack paths and prevent damaging cyber attacks. These three attack paths, most commonly used by cyber hackers, are: 1) unpatched known vulnerabilities; 2) Web Application Scanning for dynamic scans and unique fully qualified domain names; and 3) insecure Active Directory (AD). In this session, we will provide recent real-world examples that demonstrate how the failure to secure these attack paths has resulted in damaging cyber attacks. Highlights include: How to overcome vulnerability overload with a risk-based approach to Vulnerability Management that enables you to concentrate on the small percentage of vulnerabilities that actually pose cyber risk; Why Directory Services, such as AD, are the center of trust and a critical part of establishing a «Zero Trust» environment; How a dynamic AD security solution enables you to see all of your vulnerabilities; Predict which pathways attackers may target, and act to detect, shut down and prevent attacks; Why employing secure configurations and other safeguards to harden your environment can minimize the damage and prevent data exfiltration; Why using a dynamic tool to measure, continuously monitor, and address vulnerabilities is essential to prevent cyber attacks.

2022 Session Descriptions

Gotcha! How to Avoid the Top 10 Pitfalls in Security Questionnaires, Cyber Insurance Applications, Privacy Policies, and more

Mike Semel, Semel Consulting LLC

F. Paul Greene, Harter Secrest & Emery

Hackers aren't the only risk a security team faces. The sheer volume of security questionnaires, self-assessments, applications, and other forms the security team is handed, or handles, can often get in the way of actually implementing the controls required to keep a system safe. On top of that, these forms can be full of "gotcha" questions that can create more risk for an organization than an attacker or unpatched vulnerability can. This discussion will use real-world examples of these "gotcha" questions and offer proven strategies for mitigating the ever-increasing "gotcha" risk. It will address the vendor due diligence process, insurance applications and policy terms, and even the risk inherent in an organization's privacy policy, where promises and disclosures can both help and hurt an organization. Participants will leave with a better understanding of these often hidden risks and a set of actionable principles they can use to mitigate them.

Cybersecurity Culture: Effectively Promoting Security Throughout an Organization

Dylan Famolaro, iSECURE, LLC

This session will focus on the dynamics behind Zero Trust while highlighting how to get all departments within an organization on board with cybersecurity. As cybersecurity seems to be looped in as an "IT issue," this session will focus on how to make cybersecurity a priority for all departments and instill basic principles that can be enacted within an organization. Real life case studies and ideas will be shared to allow listeners to takeaway ideas to make cybersecurity exciting in their organization.

How Cyber Insurance Integrates with Technology Companies

Adam Cottini, CrowdStrike

From 2020 to present, ransomware increased in frequency and severity, resulting in significant cyber insurance claims. Insurers modified their underwriting guidelines in 2021 and continue to demand that insureds implement appropriate risk-reducing solutions, while at the same time increasing premiums and changing terms and conditions. Key underwriting criteria and controls that will be presented include: Multi-Factor Authentication, Endpoint Detection and Response and Managed Detection and Response, and Identity Protection.

ASIA Session 6: Insider Threats & Critical Infrastructure

Paper: Compressed Folders as Covert Channels

Paper: Expected paper on Critical Infrastructure Threats

DAY 2
June 8 - 2:10pm-3:00pm

Managing Cloud Computing's Cybersecurity and Information Risk

Dean Maloney, GreyCastle Security

Public and private-sector organizations across every industry have and continued their migration to the cloud in some capacity. Some aren't even fully aware as they are purchasing third-party offerings that exist completely in the cloud but appear to execute locally on their desktop. While cloud computing solutions offer very real and measurable benefits, it also requires a continued analysis and understanding of cybersecurity and information risk.

Join GreyCastle Security for a look at cloud computing and associated cybersecurity and information risks that should be considered. This session will provide the top trends of cloud computing's impact on cybersecurity as well as important considerations for utilizing this architecture.

Managing Business Risks Using Vulnerability Scanning

Diane Reilly, Carson & SAINT

Frederick Scholl, Monarch Information Networks

Vulnerability scanning is a common method to help manage risks, but it is hampered by the challenge to make it business relevant. In this presentation we will show how to connect "Tier 2" mission and business process information to "Tier 1" systems and network vulnerabilities. Tier 2 information is collected using Obashi templates and then stored in the scanning tool's database. Using this method, security practitioners can rank vulnerabilities by business impact, thereby focusing limited resources on remediation. Reporting is therefore easier to understand by business leaders. A demonstration will be included using SAINT and Obashi run against a model business organization.

2022 Session Descriptions

Overcoming Cyber Challenges: How to Respond, Remediate and Collaborate

Allen McNaughton, Infoblox Public Sector

In the unfortunate event of an incident, there are three key challenges to overcome - time to respond, time to remediate and improve collaboration. Working across disparate organizations or with a coordinated attack, these three challenges can become exponentially more difficult. This session will help you better understand how certain technologies can help you reduce your time to respond, remediate attacks, and increase collaboration both within and across an organization.

How You Can Implement Well-Architected 'Zero Trust' Hybrid-Cloud Computing Beyond 'Lift & Shift': Cloud-Enabled Digital Innovation at Scale with Infrastructure as Code (IaC), DevSecOps & MLOps

Yogesh Malhotra, Global Risk Management Network, LLC

Exponential improvements in Cloud Computing architectures and capabilities offer unprecedented speed and agility for global digital innovation, along with much needed integration of smart automation and cyber resilience at scale. However, as evident from industry surveys of business and technology executives, most need help in getting up to speed with the rapidly evolving Cloud technology platforms and architectures. Given the rapidly accelerating pace and sophistication of global cyber-attacks threatening critical IT and OT infrastructures, advancing beyond "legacy" on-premises and virtualized data centers is not a matter of discretionary choice, but a matter of existential survival. Drawing upon our Big-3 Cloud Computing Network Partner practices with comparative understanding of the leading Cloud Computing Providers and related Cloud Computing implementation and migration strategies, we shall advance technology leaders' understanding about the key Cloud Computing implementation-migration strategies and related technological-architecture issues hence enabling systematic Cloud adoption.

Hardened DevSecOps Pipelines – Secure Your Software Supply Chain

Darren Pulsipher, Intel Corp

When organizations think about security, they focus their scarce resources on securing production environments and data. However, recent attacks on the development process led to infiltration of the software on which supply chain developers rely. A modern approach to hardened DevSecOps environments can utilize hardware root of trust, secure build enclaves, attested traceability of build steps and ingredients, and incorruptible CICD pipelines. Find out how to leverage today's technologies to harden your DevSecOps pipeline and help guarantee software integrity.

ASIA Session 7: Forensics Education

Discussion: Digital Forensics Education: Future Directions

DAY 2
June 8 - 3:20pm-4:15pm

Centralized Data Protection Gateway

Phaneendra Bhyri and Karl Erber, PruTech Solutions

In this session, we will cover an approach and reference architecture we developed to help a client meet several regulatory and compliance requirements for hundreds of web applications being migrated from on-prem to cloud. We met the goals by centralizing the data protection policies through a highly scalable (built using Docker and Kubernetes stack) and secure gateway that enforced fine grain access control using RBAC and ABAC policies to automatically secure data by applying tokenization, encryption and/or masking. This approach significantly reduced the effort on application team part (in some cases, it took just a few lines of code changes per web app).

2022 Session Descriptions

Securing APIs in an Increasingly Connected Ecosystem

Bhaskar Agarwal, Nagarro Inc.

As the organizations increasingly need to and find new ways to innovate, they need APIs to make the exchange of data that much more refined, easier and more omnichannel as well as contextual. This session will focus on highlighting aspects of creating and curating secure APIs at every step of the way in their development lifecycle:

- Common cyber-attack paths
- Understanding the potential risks with APIs
- Securing APIs during the design
- API-as-a-Product
- Threat Modeling
- API authentication & authorization
- API development & documentation
- Machine-readable formats
- Catching API drifts in implementations
- Data Security
- API Security testing
- Deployment, Discovery, and associated infrastructure:
- API Inventorization: Discovery & cataloging
- Logging & monitoring
- Network security for APIs - message safety and confidentiality
- Runtime protection

At the end of the session the audience will have a better understanding of security considerations at each important API lifecycle stage and can appreciate the associated challenges and concepts more deeply.

At the Heart of the SOC: Apache Kafka & Data Streaming for Cyber Operations

Bert Hayes and Bob Liebowitz, Confluent

Apache Kafka has become table stakes for cloud native applications. Its data streaming approach has made microservices architecture scalable by boosting the speed of integrating disparate assets, while slashing the overhead needed for maintaining constantly changing integration requirements. Because it is an open-source data streaming platform, Kafka has been widely adopted by SOC's responsible for complex, multi-tenant operations in the federal government. SIEM technologies including Splunk, Elastic, ArcSight, and others all maintain connectors to push and receive data through Kafka. This talk will highlight how several SOCs in the federal government have adopted Kafka to streamline their operations.

Zero trust execution in 2022

Matthew McFadden, General Dynamics Information Technology

In this session, we will provide execution insight of Zero Trust architecture beyond the buzzwords and define reality including use cases and strategy for implementation in thwarting adversaries. Zero Trust is a cyber strategy that users, applications, data, and networks should never be trusted and should always be verified. Learn how to develop a defense in depth approach to a Zero Trust ecosystem and establish an architecture and strategy for the enterprise that leverages automation, AI/ML, and native technologies to drive a prevention-focused transformation model. GDIT will provide insight around Zero Trust execution and strategy supporting various use cases of enterprise Zero Trust implementations across the federal landscape.

How to Improve the Current State of Industrial Control Security

David Beidelman, Stratascale

We will dive into the world of Industrial Control environments and learn how these systems have become increasingly vulnerable to attack. We answer why this has become such a problem today. A top-level security evaluation approach will then be covered which is the catalyst for building a strong security program for operational technology networks and systems.

2022 Session Descriptions

ASIA Session 8: Intrusion Detection

Paper: Intrusion Detection using Multifactor Corroboration

Paper: Intrusion Detection using Graph-Based Approaches

Trellix is keeping attendees hydrated as the 2022 Water Station Sponsor. Thank you!

Interactive Learning: Blue Team Challenge
June 8 - 11:00am-3:30pm

Trend Micro

Calling all security experts! Imagine that a company is in a critical situation – you're being attacked by cybercriminals. Would you be ready to face the challenge?

Navigate a simulated cyberattack in real-time. The online game is designed to provide hands-on experience tackling real-world security problems using threat hunting and breach detection. Whether you are a novice or a skilled security professional, this experience has something for everyone. Compete in teams alongside your peers to run cyberattacks in a controlled environment. Join this fast-paced online challenge and:

- Understand the tools and techniques used by hackers
- How to remediate a vulnerability and Identify infrastructure security gaps
- Plan and implement security measures and respond to threats

2022 Conference Sponsor Demonstration Schedule

Terabyte Sponsor

Fortinet

June 7
10:35 a.m. – 10:55 a.m.
June 8
10:35 a.m. – 10:55 a.m.
Booth #51 - 53

Megabyte Sponsor

Google Cloud

June 7
1:55 p.m. – 2:05 p.m.
June 8
3:05 p.m. – 3:15 p.m.
Booth #5-6

Megabyte Sponsor

Deloitte

June 7
3:05 p.m. – 3:15 p.m.
June 8
1:55 p.m. – 2:05 p.m.
Booth #32 - 33

2022 Conference Sponsors

TERABYTE

Fortinet

Fortinet cybersecurity solutions help state and local governments to better prepare for potentially damaging attacks with a holistic, integrated security architecture that brings cyber and physical security under a single umbrella. Such an approach enables entities to respond to future attack vectors without ripping and replacing their security infrastructure every few years. It also optimizes the use of taxpayer funds by increasing operational efficiency and streamlining security operations.

Fortinet is recognized as a Leader in the Gartner Magic Quadrant for Network Firewalls. The company has also achieved nine "Recommended" ratings from NSS Labs and achieved the best score in its NGFW Security Value Map.

State and local governments are increasingly targeted by cyber criminals, and they must be prepared to fight back against potentially devastating attacks. The Fortinet Security Fabric helps unify an entity's security architecture, simplifying security operations while providing real-time, multilayered threat response. https://www.fortinet.com

MEGABYTE

Deloitte

Deloitte provides industry-leading audit, consulting, tax and advisory services to many of the world's most admired brands, including nearly 90% of the Fortune 500® and more than 7,000 private companies. Our people come together for the greater good and work across the industry sectors that drive and shape today's marketplace – delivering measurable and lasting results that help reinforce public trust in our capital markets, inspire clients to see challenges as opportunities to transform and thrive, and help lead the way toward a stronger economy and a healthier society. Deloitte is proud to be part of the largest global professional services network serving our clients in the markets that are most important to them. Building upon more than 175 years of service, our network of member firms spans more than 150 countries and territories. Learn how Deloitte's more than 330,000 people worldwide connect for impact at www.deloitte.com.

Google Cloud

Google Cloud is helping state and local governments empower their workforce and improve the lives of their constituents with our secure, interoperable, intelligent platform. Whether your organization is looking to build new applications in the cloud or transform your current infrastructure, we can help modernize service delivery. https://cloud.google.com/solutions/state-and-local-government

2022 Conference Sponsors

KILOBYTE

Carson & SAINT

Carson & SAINT is an award-winning security firm serving both public and private sectors globally. With over 30 years of deep experience in security services, cybersecurity technology, and industry-specific solutions, we combine compliance standards expertise with cutting-edge technology to identify risks, prioritize remediation, and ensure you are both secure and compliant. By identifying and prioritizing your business' most critical assets, we can help you build a culture of security and bridge the gap between your security team and your business executives.

Infoblox

Infoblox is the global leader in providing Secure DNS and Cloud Managed Network Services for a wide array of federal agencies, state and local governments, and educational institutions. Infoblox brings DNS security, reliability and automation solutions to on premises, cloud and hybrid deployments allowing for a single pane of glass for network management.

SVAM

SVAM International Inc. is a leading global Information Technology (IT) services provider focused on delivering innovative and cost-effective solutions to its clients from its centers in the USA, Mexico, India, and Bangladesh.

Headquartered in Great Neck, New York, SVAM is committed to simplifying and amplifying digital transformation for its clients and providing world-class, cutting-edge IT solutions to bring value and improve the bottom line.

Our global team assists clients with application development and modernization, Cybersecurity, RPA, Cloud, Data & Analytics, Consulting & Staffing Services, Managed Services, digital transformation, and related IT services.

ThunderCat Technology/Confluent

ThunderCat Technology is a Service-Disabled Veteran-Owned Small Business (SDVOSB) that delivers technology products and services to government organi-zations, educational institutions, and commercial enterprises. We are a VAR that brings an innovative approach to solving customer problems in and around the datacenter by providing strategies for Infrastructure, Cyber Security, and Cloud Transformation.

Confluent is pioneering a fundamentally new category of data infrastructure fo-cused on data in motion. Confluent's cloud-native offering is the foundational plat-form for data in motion – designed to be the intelligent connective tissue enabling real-time data, from multiple sources, to constantly stream across the organization. With Confluent, organizations can meet the new business imperative of delivering rich, digital front-end customer experiences and transitioning to sophisticated, real-time, software-driven

2022 Conference Sponsors

Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our unified cybersecurity platform protects over 500,000 organizations and millions of individuals across clouds, networks, devices, and endpoints.

The Trend Micro One unified cybersecurity platform delivers advanced threat defense techniques, extended detection and response (XDR), and integration across the IT ecosystem, including AWS, Microsoft, and Google, enabling organizations to better understand, communicate, and mitigate cyber risk.

With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. TrendMicro.com

VMware

VMware is a leading provider of multi-cloud services for all apps, enabling digital innovation with enterprise control.

With VMware Cross-Cloud™ services and our global ecosystem of partners, we deliver the smartest path to cloud, edge and app modernization. Customers gain multi-cloud autonomy and consistent operations while creating a more secure, frictionless experience for their distributed workforce. As the trusted foundation to accelerate innovation, VMware gives businesses the freedom and flexibility they need to build the future. More information is available at www.vmware.com

Enhance your conference experience with our mobile app:
Review your schedule and get event announcements.
Connect with sponsors and attendees.
Visit https://crowd.cc/s/4go5m now to begin!
QR CODE:

2022 Conference Exhibitors

Advizex

We are an industry leading technology provider for infrastructure and enterprise application solutions. We are a community of experts who believe in the power of IT to elevate organizations and their businesses through innovations in system solutions, technology and service. We are united by our mission of "Customers for life".

AFRL

The Information Directorate is the Air Force's and nation's premier research organization for Command, Control, Communications, Computers and Intelligence (C4I) and Cyber technologies. The directorate explores, prototypes and demonstrates high-impact, affordable and game-changing technologies. These technologies transform data into information and subsequently knowledge for decision makers to command and control forces. This knowledge gives our air, space and cyberspace forces the competitive advantage needed to protect and defend the nation. Mission of the AFRL Information Directorate: To explore, prototype and demonstrate high-impact, game-changing technologies that enable the Air Force and Nation to maintain its superior technical advantage.

Albany Law School

Albany Law School's Online Cybersecurity and Data Privacy programs provide cybersecurity professionals with the skills and knowledge to navigate a rapidly changing legal, regulatory, and policy landscape. Students gain a fundamental understanding of applicable laws and experience researching, analyzing, reasoning, problem-solving, communicating, and exercising proper professional and ethical responsibilities to clients, organizational leaders, and other stakeholders through a rigorous curriculum taught by faculty leaders in information security, data privacy, cybercrime, intellectual property law, and more. Online Graduate Degree options and scholarships are available for both lawyers and non-lawyers. For more details, contact graduateadmissions@albanylaw.edu.

Amazon Web Services (AWS)

Amazon Web Services (AWS) Worldwide Public Sector helps government, education, and nonprofit customers deploy cloud services to reduce costs, drive efficiencies, and increase innovation across the globe. With AWS, you only pay for what you use, with no up-front physical infrastructure expenses or long-term commitments. Public Sector organizations of all sizes use AWS to build applications, host websites, harness big data, store information, conduct research, improve online access for citizens, and more. AWS has dedicated teams focused on helping our customers pave the way for innovation and, ultimately, make the world a better place through technology.

2022 Conference Exhibitors

Anjolen

Anjolen provides expertise in cybersecurity, compliance, and cyber forensic services. We understand the challenges faced by businesses to increase efficiency by integrating technology into daily production. We recognize few organizations have the expertise to identify and address risk and cyber threats. From network security systems to customer data protection, we help secure your business now to prevent a security incident in the future.

Our principals are subject matter experts who have worked in military, intelligence, law enforcement and commercial application environments. They understand the complexity of protecting against data theft, and the importance of keeping staff current with regulatory concerns.

Arctic Wolf

Arctic Wolf is the global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk. Powered by threat telemetry spanning endpoint, network, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes trillions of security events each week to enable critical outcomes for most security use cases. The Arctic Wolf® Platform delivers automated threat detection and response at scale and empowers organizations of any size to stand up world-class security operations with the push of a button.

Automox

Automox is the cloud-native IT operations platform for modern organizations. It makes it easy to keep every endpoint automatically configured, patched and secured – anywhere in the world. With the push of a button, IT admins can fix critical vulnerabilities faster, slash cost and complexity, and win back hours in their day. Join thousands of companies transforming IT operations into a strategic business driver with Automox.

Compass IT Compliance

Founded in 2010, Compass IT Compliance is a nationwide leader in providing IT security, compliance, and risk management services to organizations across all industries. Our mission back in 2010 remains the same today: To partner with your organization to help you mitigate your overall information security risk while providing you with the best customer service possible. Whether you are working with our Security Specialists or our Compliance Auditors, you can rest assured knowing that our team is committed to partnering with you to provide you with expert knowledge around your risks and steps you can take to mitigate those risks.

CrowdStrike

Government institutions need a solution that protects against all cyber threats - simple and sophisticated. CrowdStrike a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike. Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

2022 Conference Exhibitors

Dell

We create technologies that drive human progress. Our story began with a belief and a passion: that everybody should have easy access to the best technology anywhere in the world. That was in 1984 in Michael Dell's University of Texas dorm room. Today, Dell Technologies is instrumental in changing the digital landscape the world over. We are among the world's leading technology companies helping to transform people's lives with extraordinary capabilities. From hybrid cloud solutions to high-performance computing to ambitious social impact and sustainability initiatives, what we do impacts everyone, everywhere.

DynTek

For over 25 years, DynTek Services has focused on delivering exceptional, cost-effective professional IT services, solutions, and products to New York state and local government, educational, healthcare and enterprise customers. With a local presence in Albany, our broad range of technical expertise, vendor partnerships, and contract vehicles allow us to deliver IT Security, Managed Security Services, Digital Infrastructure, Modern Workplace, Data Center and Cloud solutions to meet your critical requirements.

EWaste

EWASTE+ is a R2/RIOS Certified Electronics Recycling company and a licensed, NAID AAA Certified Data Destruction Contractor. EWASTE+ focuses on recovery of value from idle, obsolete and excess electronic equipment and operates a large-scale processing facility in Rochester, New York and two regional consolidation facilities in Albany and New York City. The company utilizes environmentally sound processing methods to maximize value and recovery while eliminating disposal of electronics in landfills.

Federal Bureau of Investigation

The Federal Bureau of Investigation is the principle federal law enforcement agency of the United States. In it's mission to protect the American people and uphold the Constitution, the FBI takes a lead role in protecting the United States from terrorist threats, cyber attacks, espionage and public corruption. If you'd like to learn more about working at FBI or partnering with FBI through InfraGard, please stop by.

Forescout

Forescout delivers automated cybersecurity across the digital terrain, maintaining continuous alignment of customers' security frameworks with their digital realities, including all asset types – IT, IoT, OT, IoMT. The Forescout Continuum Platform provides complete asset visibility, continuous compliance, network segmentation and a strong foundation for Zero Trust. For more than 20 years, Fortune 100 organizations and government agencies have trusted Forescout to provide automated cybersecurity at scale. Forescout customers gain data-powered intelligence to accurately detect risks and quickly remediate cyberthreats without disruption of critical business assets.

2022 Conference Exhibitors

The Griffiss Institute

he Griffiss Institute cultivates talent and technology that tackles the world's biggest challenges. It does so alongside the United States Department of Defense's Air Force Research Laboratory Information Directorate (AFRL/RI) and an international network of academic, government, and industry partners. Founded in 2002 in the Mohawk Valley region of CNY, Griffiss Institute has origins as an incubator of ideas. With technology transfer at its core, it forges connections and pathways that enable real-life solutions to make their way from the lab bench to the kitchen counter. Griffiss Institute continues to elevate the next generation of STEM students, professionals, and technologies that enhance our national security.

HubSpire

Cyber resilience is essential to stay viable as a business entity and requires comprehensive strategies for cybersecurity.

We can help you understand your cyber risk profile, develop a holistic approach to resist and respond to disruptive threats, operationalize a security strategy that evolves to address your most current risk profile, protect your 'crown jewels' and establish trust throughout your digital ecosystem.

iSECURE

iSECURE is a cybersecurity company located in Rochester, New York focusing on improving cybersecurity hygiene within its client's infrastructure. The company was formed in 2011 with the mission to inspire a cybersecurity culture through education and collaboration.

iSECURE utilizes intelligence, process, and experience to architect creative solutions that proactively protect each client through our professional services and robust security solution offerings.

Legit Security

Legit Security secures your software development lifecycle by protecting the pipelines, infrastructure, code and people. Legit Security keeps your software factory secure and ensures that every software release is "legit". We offer a SaaS-based platform that supports both cloud and on-prem resources and protects and organization's software supply chain environment from attack. The platform combines unique automated discovery and analysis capabilities with hundreds of security policies developed by industry experts with real-world SDLC experience. This integrated platform keeps your software factory secure and provides continuous assurance that your applications are released without vulnerabilities.

2022 Conference Exhibitors

LP3

LP3 was formed in 2004 as a high-technology cyber security services firm supporting mission critical Intelligence, DoD, Federal, State and business organizations across many sectors such as local governments, finance, and manufacturing, including defense articles and medical devices.

LP3 provides a full spectrum of cyber security solutions to protect government, businesses, and non-profit organizations from cyber-attack. We offer globally experienced cybersecurity consulting, technical auditing, and assessment services and as well as insider threat and infrastructure protection services for complex global enterprises.

See https://LP3.com for complete list of services.

Nagarro

Nagarro is a leading global provider of IT consulting services, partnering with clients on some of their most strategic technology projects. Recognized worldwide for expertise in systems integration and digital transformation services, Nagarro brings unmatched technical excellence, thought leadership, and a complete commitment to success to every project.

As a CMMI Level 5 and ISO 27001 certified organization, we have a relentless passion for delivery excellence, and are proud to have a consistent track record of on-time, on-budget and high-quality delivery.

Our digital government offerings include solutions for education, homeless prevention, veterans' assistance, child services, health and human services, public safety, and more.

Netwrix

Netwrix makes data security easy thereby simplifying how professionals can control sensitive, regulated and business-critical data, regardless of where it resides. More than 11,500 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers. Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S. For more information, visit www.netwrix.com

NYSTEC

NYSTEC is an independent nonprofit technology consulting company, advising organizations, agencies, institutions, and businesses since 1996. We help clients plan and manage the acquisition, implementation and security of their IT systems. With offices in Rome and Albany, NY, as well as New York City, NYSTEC employs proven processes for project management, business analysis and system integration to serve clients in many sectors, including the company's main client base, government. We are a trusted partner to government at the county, state, city and local level, advising our clients on how to use the right technology and helping them achieve real business outcomes.

2022 Conference Exhibitors

Recorded Future

Recorded Future is the world's largest intelligence company. Recorded Future's Intelligence Cloud provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries. Learn more at recordedfuture.com.

Red Hat/Carahsoft

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments.

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-performing GSA Schedule, SEWP and SLSA contract holder, Carahsoft has served as Red Hat's master government aggregator and distributor for more than 15 years.

Rubrik

Rubrik delivers a radically simplified approach to data management for state & local governments to recover from ransomware attacks, accelerate cloud mobility, and streamline operations in this new norm.

SHI

With over 30 years' experience delivering solutions across the IT spectrum, we help organizations reduce their digital attack surface using a dynamic approach that strikes the right balance between people, process, and technology.

Our vendor-independent approach, leading technology solutions, state-of-the-art Customer Innovation Center and expert services help ensure your infrastructure, data and people are protected as cybersecurity threats and the regulatory landscape change.

2022 Conference Exhibitors

Splunk

Splunk is the data platform leader for security and observability. Our extensible data platform powers enterprise observability, unified security and limitless custom applications. Splunk helps tens of thousands of organizations turn data into doing so they can unlock innovation, enhance security and drive resilience.

T-Mobile

T-Mobile for Government provides innovative connectivity solutions that help government better serve citizens by enabling agencies to work more intelligently, efficiently, and securely. Our mobile device management solutions help safeguard sensitive data. Our network is ideal for unlocking game-changing IoT technology. And we provide 24x7x365 support, so we're ready when communications are critical. It all starts with America's largest, fastest, and most reliable 5G network, as well as the tools that help you take advantage of 5G. We also offer an exceptional customer experience and outstanding value – with no tradeoffs. To learn more, please visit T-Mobile.com/Government.

Tanium

Tanium is the platform that organizations trust to gain visibility and control across all endpoints in on-premises, cloud and hybrid environments. Our approach addresses today's increasing IT challenges and delivers accurate, complete and up-to-date endpoint data – giving IT operations, security and risk teams confidence to quickly manage, secure and protect their networks at scale. State and local governments, educational institutions, federal civilian agencies and multiple branches of the U.S. Armed Forces trust Tanium to help see and control every endpoint, everywhere. The power of certainty. Visit www.tanium.com.

Trellix

We're no strangers to cybersecurity. But we are a new company. Trellix is a global company redefining the future of cybersecurity. Our open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. We created an XDR architecture that can be tailored to your government's organization, delivering higher resilience and agility. Curious? Let's connect today at: www.trellix.com

Vandis

Vandis provides Managed Services and IT Solutions to optimize the security and performance of network infrastructures, both on-premise and in the cloud. Leveraging deep subject matter expertise, we design IT solutions to meet each organization's unique needs and goals. For over 38 years, from SMB to enterprise clients, Vandis is a trusted partner to provide comprehensive strategies for secure and stable IT infrastructures. Contact us at www.vandis.com.

2022 Conference Exhibitors

Veracode

Veracode is a leading AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. With its combination of process automation, integrations, speed, and responsiveness, the Veracode Platform helps government agencies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities. Veracode, named a Leader for the ninth consecutive time in the 2022 Gartner Inc. Magic Quadrant for Application Security Testing, is the only vendor recognized as a Leader every single year since the report was first published.

Zerto

A world of uninterrupted technology is a world where organizations across all industries can thrive without downtime or disruptions for their customers. From 24/7 continuous patient care in hospitals, to interruption-free airline travel, to keeping ecommerce systems running without a hitch, the path to this always-available world starts with Zerto. We help our 9000+ customers realize this vision though our Zerto platform, which brings together disaster recovery, backup, and data mobility into a single, simple cloud data management and protection solution that enables digital transformation, reduces downtime and data loss, and helps businesses move workloads seamlessly across clouds or datacenters. With Zerto, a world of truly uninterrupted technology is within reach.

The 2022 NYS Cyber Security Conference would like to thank all of our sponsors, exhibitors, speakers, volunteers, and attendees for making this another successful year!

Modernize security operations with Chronicle

Enhance your security operations at Google scale and speed, while leveraging Google's threat intelligence and big data systems for superior economics and positive security outcomes.

Stop by Google Cloud's booth to learn more!

Google Cloud | carahsoft.

Passport Raffle

Visit our exhibitors for a chance to win some amazing prizes. All you need to do is bring the Exhibitor Passport to each of the listed booths and have it stamped; it's that easy! Once the passport is stamped please bring it to the Registration Table. Drawings will be held during the 3:00 p.m. break on Tuesday, June 7 and Wednesday, June 8. Prizes must be picked up by the end of the conference. The passport is made possible by generous donations from our conference sponsors and exhibitors.

The NYS Cyber Security Conference Scholarship helps provide scholarship opportunities to University at Albany students with a demonstrated interest in cyber security.
Congratulations to the 2022 recipients:
Sabrina Hussain
Deanna Greenblatt

Please take a moment to provide feedback via the mobile app at the end of each session you attend, as well as at the conclusion of the conference. We value your comments.

Notes

2022 Conference Exhibitors

Advizex

ALBANY LAW SCHOOL
ONLINE GRADUATE PROGRAMS

ANJOLEN
Securing Your Cyber Future

AFRL
THE AIR FORCE RESEARCH LABORATORY
LEAD | DISCOVER | DEVELOP | DELIVER

aws

ARCTIC WOLF

COMPASS
IT COMPLIANCE

DELL Technologies

AUTOMOX

CROWDSTRIKE

DYNTEK
DYNAMIC TECHNOLOGY SOLUTIONS

GRIFFISS INSTITUTE

EWASTE+
REGIONAL COMPUTER RECYCLING & RECOVERY

FORESCOUT

HubSpire

LEGIT SECURITY

iSECURE

LP3
LIGHTSPEED
Produce, Protect, Perform

rubrik
public sector

netwrix

Recorded Future

Red Hat
carahsoft

NYSTEC
YOUR INDEPENDENT TECHNOLOGY ADVISOR

SHI

TANIUM

splunk>

T-MOBILE FOR GOVERNMENT

Trellix

VERACODE

VANDIS

Zerto
a Hewlett Packard Enterprise company

TERABYTE Sponsor

FORTINET®

MEGABYTE Sponsors

Deloitte.

Google Cloud

KILOBYTE Sponsors

CARSON & SAINT

Infoblox®

SVAM INTERNATIONAL, INC.

THUNDERCAT TECHNOLOGY | CONFLUENT

TREND MICRO™

vmware®

Booth Assignments

Company	Number
Conference CoHosts	1 - 2
FBI	3
Trellix	4
Google Cloud – MEGABYTE	5 - 6
DynTek	7
LP3	8
Albany Law School	9
AWS	10
VMware – KILOBYTE	11
Trend Micro – KILOBYTE	12
Carson & SAINT – KILOBYTE	13
SHI	14
Forescout	17
Compass IT Compliance	18
Splunk	19
HubSpire	20
Ewaste	21
Dell	22
Tanium/TVT	23
Legit Security	24
Arctic Wolf	25
Thundercat/Confluent – KILOBYTE	26 - 27
Red Hat/Carahsoft	28
Zerto	29
Netwrix	30
Veracode	31
Deloitte – MEGABYTE	32 - 33
Infoblox – KILOBYTE	34
SVAM – KILOBYTE	35
Anjolen	36
Vandis	37
NYSTEC	38
Griffiss Institute	39
AFRL	40
Rubrik	41
Recorded Future	42
Automox	47
Nagarro	48
iSecure	49
T-Mobile	50
Fortinet – TERABYTE	51 - 53
CrowdStrike	54
Advizex	55