



INNOVATE • SECURE • TRANSFORM

Governor Andrew M. Cuomo

Robert H. Samson, NYS CIO

Presented by



**Office of Information
Technology Services**



Table of Contents

Conference Co-Hosts	5
Keynotes	7
Session Descriptions.....	9
Sponsors	28
Exhibitors	30
Agenda At-A-Glance	44-45
Booth Assignments & Floor Plan	48

Empire State Plaza
Public Space WiFi:
ESP-Public Wifi



Welcome Letter

June 4, 2019

Dear Attendee:

Welcome to the 22nd Annual New York State Cyber Security Conference and the 14th Annual Symposium on Information Assurance. On behalf of the New York State Office of Information Technology Services, the School of Business at the University at Albany, State University of New York, and The NYS Forum, Inc., it is our pleasure to offer you an exciting agenda packed with inspiring sessions and the opportunity to meet people from all over the country who share your passion for cyber security.

As technology continues to advance in ways never imagined, we must continue to look forward and understand how each advance impacts you, your organization, and your cyber security environment.

Every day, we face new cyber security challenges that pose significant risk to the information, systems, and networks within our organizations. Here in New York State, we lead the nation in cyber security by innovating, securing, and transforming technology to help protect our citizens and businesses. Governor Andrew M. Cuomo remains steadfast in his longstanding commitment to cyber security and keeping New Yorkers safe. Through Governor Cuomo's leadership, New York has created some of the strongest cyber protections in the nation. We continue to create a path forward that other states can emulate.

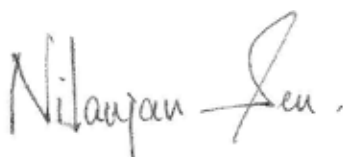
When it comes to cyber security, we all have a part to play. Whether you are just starting out in cyber security or are already a seasoned professional, the conference has something for you. With more than 50 sessions to choose from, the conference brings you the latest on security evolution, the current 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 speeches, and participate in one of the interactive training workshops.

Thank you for attending the 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,



Robert H. Samson
NYS Chief Information Officer
NYS Office of Information Technology Services



Nilangen Sen
Dean
School of Business
University at Albany
State University of New York



Mario Musolino
Executive Director
The NYS Forum, Inc.



**Office of Information
Technology Services**



CISO Welcome

About the conference

Dear Attendee:

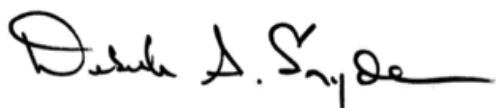
As the Chief Information Security Officer for New York State, my mission is to advance the State's ability to safeguard information, systems and critical infrastructure, defend against cyber threats, and ensure secure government services for our citizens. In today's digital and interconnected world, cyber security is a business imperative. Cyber-attacks continue to grow in number, speed and impact. No matter where you are from—*government, academia, business, or the general public*—we all can be vulnerable. We have a shared responsibility to ensure personal information and organizations are protected.

The 22nd Annual New York State Cyber Security Conference and the 14th Annual Symposium on Information Assurance highlights the critical need for all of us to be forward-thinking when we utilize technology to protect our personal and organizational data. The conference showcases the evolution of security and features best practices to maximize data protection and minimize cyber threats. Attendees will gain real-world information and skills to remain vigilant and strengthen their organizations' cyber security posture.

This year, we are pleased to welcome Michael Aiello, Cybersecurity Executive for Google Cloud Platform Security, as our opening keynote. Mr. Aiello is certain to offer us a unique perspective on the future of security in this exciting age of continuous technology advancements.

At the conclusion of the conference, I hope you take away valuable information you can immediately apply to manage cyber risk head on. Thank you for your continued interest in cyber security and for being a part of this important event.

Sincerely,



Deborah A. Snyder
NYS Chief Information Security Officer
NYS Office of Information Technology Services



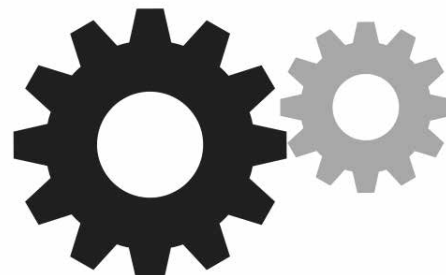
Office of Information
Technology Services

June 2019 marks the 22nd Annual New York State Cyber Security Conference.

First held in 1998 as a one-day seminar for state and local government, the event has grown to two full days with more than 50 breakout sessions. The conference offers keynotes from nationally-recognized cyber security experts and cutting-edge training.

New York State is a recognized leader in the field of cyber security and Governor Andrew M. Cuomo remains committed to putting systems and practices into place that protect New York's critical assets and keep New Yorkers safe from cyber threats. The conference is part of a statewide effort to boost cyber security awareness and empower state and local governments, academia, organizations, and citizens to take better control of their digital security.

The conference offers something for everyone—whether you're a technology user, IT professional, government employee, or business owner. Learn from leading experts in the industry and participate in engaging sessions that provide real-world information you can apply immediately in minimizing the cyber risks in your own environment.



Tweet the conference at #nyscyber

Conference Co-Hosts

Robert H. Samson

Chief Information Officer

NYS Office of Information Technology Services

In April 2017, Governor Andrew M. Cuomo appointed Robert H. Samson to the position of New York State Chief Information Officer at the New York State Office of Information Technology Services.

Mr. Samson had a rewarding 36-year career with IBM until August 2009, when he retired. While at IBM, he served in various leadership positions where he led teams focused on helping governments transform using innovative approaches and technologies. His most recent positions at IBM included serving as the Vice President of the Worldwide Systems and Technology Group, and the General Manager of IBM's Global Public Sector, where he was responsible for IBM's business with governments, education, healthcare and life sciences industries.

In 2011 and 2012, Mr. Samson served as a member of the Governor's Spending and Government Efficiency (SAGE) Commission. As a member of the SAGE Commission, Bob and his SAGE colleagues developed recommendations for modernizing and right-sizing New York State government to improve performance, increase accountability, and save taxpayer money. As part of the Commission's final recommendations to the Governor, the Office of Information Technology Services (ITS) was created in 2012 to transform IT services, make state government work smarter for its citizens, and make the state more accessible for businesses through the use of technology.

Mr. Samson received a lifetime achievement award from Government VAR magazine in recognition of his contributions in working with governments around the world, and is passionate on the topics of leadership, mentoring and developing competent inspiring leaders. Mr. Samson delivered a keynote speech at the National Defense University titled "Challenges and Opportunities, the Power of Values that Change the World," which appeared in Vital Speeches of the Day.

In 2019, Mr. Samson was recognized with a "Top 25 Doer, Dreamer, Driver Award" by *Government Technology*. In 2018, Mr. Samson was recognized by *StateScoop* as "State Executive of the Year" for leading state government into a new technology landscape with innovative ideas and by inspiring others to get on board.

Mr. Samson is a founding member of the New York State Mentoring Program and continues to serve on its Advisory Council with Founder and Chair Mrs. Matilda Raffa Cuomo. In addition, he serves as a member of the Advisory Board for the SUNY Center for Technology in Government.

He is a graduate of SUNY Plattsburgh and completed the Program for Management Development at Harvard Business School.

Conference Co-Hosts

Mario Musolino

Executive Director
The NYS Forum Inc.

Mario J. Musolino, recently joined the Forum staff as Executive Director. Prior to accepting the position with the Forum, Mr. Musolino spent 12 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.

Prior to his appointment at the Department of Labor, Mr. Musolino served as 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. Among other positions, Mr. Musolino 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's 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.

Dr. Nilanjen Sen

Dean, School of Business
University at Albany, State University of New York

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 to 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 eight 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 enrollment 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 was 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

June 4, 2019 | Convention Hall | 9:00 a.m. - 10:30 a.m.



Michael Aiello

Google Cloud Platform Security

As a Cybersecurity Executive at Google, Mike serves as Director of Product Management for Google Cloud Platform Security.

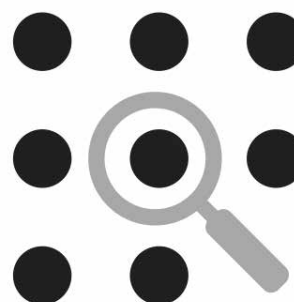
Additionally, Mike serves as a Board Director or Board Advisor to cybersecurity, technology and investment companies in New York, California and Maryland. At Google, Mike's risk management, data protection, and privacy products help secure thousands

of businesses and billions of people every day. In 2017 and 2018, these products unblocked more than one billion dollars of revenue for Google Cloud.

Before joining Google, he served as Chief Information Security Officer at Goldman Sachs, where he helped secure Marcus, the company's digital retail bank and established the company's Consumer Trust and Technology Risk Committee. Mike has spent the last 20 years as a technology innovator and entrepreneur. Mike was the founder and CEO of DIFRwear, a leading manufacturer of radio-frequency identification (RFID) blocking wallets, passport cases, and badge sleeves. The company and products have been featured in *The New York Times*, *The Wall Street Journal*, *Wired*, and others. Mike also founded LifeEnsured, a company allowing customers to privately manage their online identities after death, which was acquired in 2012 by DSwiss.

Mike has spoken for a variety of audiences from large cyber events like the Gartner Information Security & Risk Management Conference to policy discussions at the Council on Foreign Relations. He regularly works with CEOs, CIOs, and CISOs advising on technology and security risk management. Mike serves on the U.S. Leaders Council for Cordaid, an international relief organization.

Mike has an MBA from the University of Oxford and a master's degree in Computer Science focused on Information Assurance from New York University's Tandon School of Engineering and has authored several patents related to cybersecurity and privacy.



Cyber Fragility in 2019

The keynote will provide an overview of Cyber Fragility, its importance and the drivers of Cyber Fragility in 2019. The talk will encourage audience members to consider approaches modern organizations are taking to reduce risk and build trust in technology and to analyze how emerging attacks may impact themselves and their organizations.

ASIA Keynote – Day 2

June 5, 2019 | Convention Hall | 9:00 a.m. - 10:30 a.m.

Daniel P. Bagge



Cyber Attache of the Czech Republic to the United States and Canada

Daniel P. Bagge was appointed as the Cyber Attache of the Czech Republic to the United States and Canada in August 2018. In this capacity, he is responsible for government to government relations in the field of cyber security. He works for the National Cyber and Information Security Agency, and is based at the Embassy of the Czech Republic in Washington D.C. Among his duties are strengthening relations among

partner organizations and entities such as the FBI, DHS and other federal agencies, also including U.S. Congress, Department of State and the National Security Council with his parent organization. His mandate however is broader than G2G. He is also reaching out to private industry and academia, forging partnerships with stakeholders that are essential in cybersecurity.

Until August 2018 he was the Director of Cyber Security Policies, first in the National Security Authority and later in the National Cyber and Information Security Agency. In this capacity, he was responsible for the implementation of the National Cyber Security Strategy, which he co-authored, as well as overseeing the process of Critical Information Infrastructure Protection of the country. While being responsible for creation of the first national and international policies on cyber security in the Czech Republic, he founded the Strategic Information and Analysis Unit, Education and Exercise Unit, International Organizations and Law Unit, National Strategies and Policies Unit and the Critical Information Infrastructure Protection Unit. As part of international outreach and cooperation, he provided the expertise of his department to ACT NATO, USCYBERCOM, USAFRICOM, the U.S. Congress, and others.

He deals with the conceptualization of threats and since 2013 has worked as the Secretary of the Cyber Security Council, chaired by the Prime Minister of the Czech Republic. He is regularly invited to speak at cyber security events around the world. In 2015, he became intrigued by the use of cyber enabled activities to influence decision making on all levels of governance. This led to publishing his book called *Unmasking Maskirovka: Russia's Cyber Influence Operations (2019)*.

He holds M.A. from the Bundeswehr University in Munich/George C. Marshall Center in Germany and studied in the Czech Republic and Israel.



The Importance of International Alliances in Strengthening Cybersecurity: The Case of Information Superiority and Technology Dependence

Cybersecurity has been seen as a purely technical matter for far too long. Although cybersecurity is inherently about protecting infrastructure and information, it has reached the realms of diplomacy, geopolitics, strategic balance of power. Apart from talking about the importance of international alliances based on shared values and diplomacy, I would like to discuss two state actors, Russian Federation and PRC - and how allies across the Atlantic work on mitigating some of the challenges posed by the actions coming from these two actors.



Session Descriptions

Tuesday, June 4, 2019 Day One Sessions

PEN TESTING TRACK

Here We go Again. Red Teaming Stories from the Trenches

Tyler Wrightson, Leet Cyber Security
11:00 AM – 11:50 AM

In this talk, Tyler reviews the interesting, hilarious, unique, awesome and familiar things that happened in the past year during penetration tests. All of the information is from first hand experience and will give attendees insight into how organizations are actually broken into. The attack vectors include intrusions via external, internal, social engineering, physical, and more.

Unleash the Infection Monkey: A Modern Alternative to Pen-Tests

Dave Klein, Guardicore
1:00 PM – 1:50 PM

The security testing toolset available to security professionals today consists mainly of penetration testing and vulnerability scanners. These tools were designed for traditional, relatively static networks and can no longer address ALL the possible vulnerabilities of today's dynamic and hybrid network. While there is no replacement to a highly skilled human pen-test hacker, penetration tests are limited to specific parts of a network, are expensive, and may become obsolete within months. Automatic vulnerability scanners have limited accessibility and cannot simulate today's advanced lateral movement attack methods. The result is network blind spots which is where security threats often arise. This calls for a new approach to

testing network security resilience. An ideal tool would be easy to use, budgetary conscious, autonomous and scalable. We propose using the Infection Monkey, an open source breach and attack simulation tool, designed to thoroughly test a network from an attacker's point of view. Inspired by Netflix's Chaos Monkey that would randomly delete servers in Netflix' infrastructure to test a service's ability to withstand server failures, Infection Monkey, "infects" your network to test its defenses capabilities. Freely available, Infection Monkey spins up an infected virtual machine inside random parts of your data center, to test for potential security failures. By "inside," we mean behind the firewall and any other perimeter defense you are deploying for your computing infrastructure. By equipping the monkey with advanced exploitation abilities (without destructive payloads), it can spread to any vulnerable machine within reach. Along with the ability to spread onwards from its victims, the monkey can detect surprising weak spots throughout the network.

Attendees of this session will:

- identify vulnerabilities still in the industry's collective blind spot;
- understand how testing can shed light on weaker parts of the security chain; and
- become advocates for better testing as a means to strengthen security.

Thank you to NYSTEC
for sponsoring lanyards
for the 2019 NYSCSC!

SUPPLY CHAIN MANAGEMENT TRACK

Supply Chain Risk Management - Where Security, Trade and Politics Converge

Robert Mayer, USTelecom
2:10 PM – 3:00 PM

With relentless cyber attacks emanating from foreign nations including Russia, China, Iran and North Korea, the United States government is now working closely with industry experts to identify and mitigate supply chain risks. The hyper-interconnected digital ecosystem and the highly distributed nature of the supply chain can make the risk mitigation process appear overwhelming, yet organizations must address the risks associated with an increasingly diverse chain of custody for both hardware and software inputs. Products such as Kaspersky, ZTE and Huawei have come under intense scrutiny, but the range of potential threats go well beyond these vendors.

In response to the cyber threats generally, the Department of Homeland Security (DHS) recently created the National Risk Management Center in which joint Federal government and private sector collaboration is underway in areas addressing systemic risk, cross-sector collaboration and supply chain risk management. In this session, you will get a broad perspective of multiple government and industry initiatives in this arena and hear directly from one of the co-chairs on the important work being undertaken as part of the DHS Information and Communications (ICT) Supply Chain Risk Management Task Force.



Session Descriptions

Contracting for Cybersecurity (And What To Do When You Can't Get Everything You Want)

Mark Francis,
Holland & Knight LLP
3:20 PM – 4:15 PM

The global economy relies heavily on supply chains. Cybersecurity risk management and data privacy considerations are increasingly a critical factor in those supplier relationships, with many business, technology and legal implications arising from the parties' respective contractual commitments, cyber and privacy practices, and allocation of risk.

Although there is a lot of public information available on industry standards and frameworks, as well as legal developments, much if not most activity around vendor risk management takes place behind closed doors, as businesses negotiate with each other on security and privacy practices, and negotiate contractual commitments and in these areas. This session will address key risks and common stress-points around cybersecurity and data privacy issues in such relationships, with helpful tips and options for consideration.

SECURITY EVOLUTION TRACK

The Leadership Vision for Security and Risk Management

Jeffrey Wheatman, Gartner Research
11:00 AM – 11:50 AM

Digital transformation continues to challenge the conventions of information risk and security management. It requires a coherent digital security program based on a clear vision and strategy.

This presentation will:

- share a compelling vision for security and risk management and
- identify the key digital differences that must be integrated into the security program.



Reenergize with a beverage and snack!

Afternoon Breaks

June 4 at 3:00 p.m. - 3:20 p.m.

June 5 at 3:00 p.m. - 3:20 p.m.

Biometrics, Facial Recognition and Autonomous Vehicles

CLE Eligible
Gail Gottehrer
1:00 PM – 1:50 PM

As biometrics and facial recognition technology become more prevalent, concerns about the privacy and security of the data they generate increase, along with calls for government regulation and legislation. Similarly, as Level 4 autonomous vehicles take to the road and with predictions of vehicles with Level 5 technology becoming available in the next few years, more attention is being focused on the significant amount of geolocation and other sensitive data associated with these vehicles and related security issues. This panel will discuss the data collected by these emerging technologies, the state of the law and regulations applicable to them, and cybersecurity guidance and best practices.

Who Owns Your “Personal” Emails and Social Media Data

CLE Eligible
Mark A Berman
Shawndra G. Jones
2:10 PM – 3:00 PM

With many companies maintaining Bring Your Own Device (BYOD) policies and with employees posting on social media as part of their job or sending personal emails using work or personal accounts, who actually owns “personal” email and social media data? And, to further complicate the matter, who owns information stored in the cloud? When the duty to preserve arises, to what extent might electronic data stored on personal devices by current or former employees be implicated? This panel will examine these questions, privacy and information security issues, and applicable ethics and privilege concerns that attorneys face.

Session Descriptions



From the Engine Room to the Board Room

Chris Hallenbeck, Tanium

3:20 PM – 4:15 PM

This session will focus on articulating the value of security to non-technical leadership.

COMPLIANCE TRACK

Navigating Security and Privacy Compliance Challenges

Michael Corby,
M Corby & Associates, Inc.

11:00 AM – 11:50 AM

In nearly every industry, security and privacy compliance is a key consideration. In fact, very few IT projects exist without security or privacy implications. There is a robust cottage industry based on collecting personal or company data from a variety of sources to assemble profiles, which can then find their way into the hands of cyber criminals. The wise Cyber Security leader will keep security and privacy concerns in focus. The project sponsor may not recognize or acknowledge the risk of failure that is present when IT projects are audited for the security and privacy compliance elements left out during project charter creation. This session will present the challenges of strengthening information security, while staying focused on project objectives, performance and quality.

A Calm Approach to Regulatory Confusion

Mike Semel, Semel Consulting LLC

F. Paul Greene,
Harter Secrest & Emery LLP

1:00 PM – 1:50 PM

Every business in the United States has to comply with a data breach laws. If you are in healthcare, you know about HIPAA. If you are in finance, you know about the strict NYS DFS cyber security regulations. But, do you know about New York's data breach law and the proposed SHIELD Act? You work in New York, but do you understand why should you be worried about the Massachusetts Attorney General? How does the European Union's GDPR regulations affect you, and do you know if California's version of GDPR will or won't affect your company? What if you are a health plan that has to comply with HIPAA and NYS DFS Part 500 and New York's data breach laws, in a way that satisfies your cyber liability insurance policy? What questions will your executives and board want answers to? Do you understand how to leverage regulations to lower your risks of a lawsuit settlement or jury award? Information security and privacy Attorney Paul Greene and cyber security and compliance expert Mike Semel will help guide you through the confusing maze of cyber security regulations. You will learn how to build a practical security and compliance program to address multiple requirements. You will leave with a better approach to deal with existing regulations, and how to be prepared for the increased legislation that's on its way.

State and Federal Privacy Regulations Abound: What It Means for New York Businesses

Dimitri Sirota, BigID

2:10 PM – 3:00 PM

With the transitional period under the New York State Department of Financial Services Cybersecurity Regulation ending, New York state Senator Brad Hoylman recently proposing the Right to Know Act, and other federal and state privacy regulations being introduced, businesses based in and doing work in New York are facing a new data privacy reality—they must understand what data they have, whose data it is, where it resides and who has access to it if they're going to meet the requirements of regulations and the demands of customers.

In this session, you will explore how organizations can better meet these new regulations, including implementing automated data discovery programs to better inventory data, manage consent requirements, fulfill data subject access requests, improve breach notifications and more. Adopting a cost-effective way to integrate and analyze massive amounts of data across all data sources—not just structured data—to expand enterprises data-driven intelligence, and the ability to make more meaningful data-driven decisions will also be explored. Applying new techniques, such as AI-based automation, to better understand personal data, address security, privacy and regulatory requirements affecting both that data, will reduce corporate risk. By reconsidering how to manage and secure personal data, organizations can not only become more effective and responsible stewards of personal information, they can improve business decision-making and performance.

Join us for a Continental Breakfast
each morning in the Exhibit Hall!
June 4 breakfast sponsored by TrendMicro



Session Descriptions

Privacy and Breach Protection - Achieving Safe Harbor by Knowing What You Have and How to Protect it

Robert Roy,
Micro Focus Government Solutions
3:20 PM – 4:15 PM

With new rules like the European Union General Data Protection Regulation (GDPR) for all entities hosting EU citizen data, and New York State Breach Notification and privacy laws, you may be wondering if your agency is at risk and what you can do about that risk. The data lifecycle of most organizations, both in the public and private sector, may lack rigid structure that enables the rapid discovery, classification, governance, knowledge management, security, and other functions. While data is important to the daily mission of New York agencies, it comes with a variety of opportunities to increase its value to the mission, while simultaneously placing the organization at risk of a data breach impacting the personal and sensitive data of state citizens. Join this session to learn more about data management opportunities and a surefire way to protect yourself in the event of a data breach.

DATA PROTECTION

Digital Identity - The Fabric Connecting and Securing Internal and External Access

Mike Wyatt, Deloitte
11:00 AM – 11:50 AM

In this age of digital transformation with continuous engagement of new technology and digitization of services and information, the door has opened even wider for potential risks around the wrong entity getting to targeted information or assets. Digital transformation and connected assets are essential for government to provide

services, drive economic development, and improve citizens quality of life. The spheres of an individual's identity points—as a government employee, consumer or business owner, and private citizen—are interlinked in a complex digital structure, like a piece of fabric. The growing ability to piece together an individual's digital picture and enable appropriate levels of access is critical - now more than ever.

Join Mike Wyatt for a discussion on steps organizations can take to help make digital identity (ID) a strong fabric that supports their digital economy. Mike will discuss key points in your digital journey where digital ID strategies should be considered or evolved. Whether helping to proof the identities of internal human resource staff, or providing a new licensing mobile app to business owners, there are strategies to create efficiencies, help reduce risk, and plan for evolution to support the change needs of business. Developing methods that are scalable and adaptive is also key. Digital ID, when strategically designed as part of your digital journey, can help create a personalized, frictionless user experiences across different channels to better engage with citizens and internal staff, while also addressing risks to help close the door on unwanted access.

Digital Compliance: Understanding Your Sensitive Data Footprint

Michael Giordano, DynTek Services
1:00 PM – 1:50 PM

As both government and enterprise continue to digitally transform their organizations and operations, more and more digital and private data is making its way through our networks, data centers and cloud environments. With the mounting tide of data privacy compliance initiatives, such as GDPR and the California Consumer Privacy Act, the impending

impact on New York State government institutions and businesses is inevitable. Join us for a discussion on how to start preparing now to protect your constituents and future proof your digital infrastructure.

We will discuss:

- impact of recent compliance legislation;
- future of data privacy;
- how data privacy relates to government;
- understanding how your organization's data footprint leads to smarter security overall; and
- how to accurately assess your data risk.

Importance of Having an End to End Integrated Security Fabric

David Leinberry, Fortinet
2:10 PM – 3:00 PM

This session will cover the current cyber and malicious threats confronting organizations today. The importance of having an end to end, integrated security fabric to proactively alert, block and update all the surfaces and fronts within your network. Getting your Firewalls, Web, mail, endpoint, File-share and East - West traffic, sharing threat intelligence with one another all centered around a sandbox, the last line of defense. Whether in the cloud or on premise. The goal is to have automated detection with assisted mitigation, looking for Zero Days, Polymorphic Ransomware, targeted attacks and APTs. Then, the significance of getting a holistic view of your entire network by using a SIEM, that will alert to brute force attacks, DLP, stolen credentials, miss configurations and vulnerabilities with in your network. A SIEM will also provide regulatory and compliance reporting for auditors and government regulations.



Protect Your Data by Understanding How a White Hacker finds a Data Leak

Tom Buoniello, BinaryEdge

3:20 PM – 4:15 PM

By understanding the techniques used to find “a data leak,” attendees will be better positioned to protect their data from external “eyes.”

The presentation will:

- define a Data Leak, describe where data typically “lives” in an organization;
- list out a few recent (or well known) Data Leaks;
- define White Hacker;
- describe generic approach White Hacker uses;
- describe typical tools a White Hacker uses;
- show in detail how a Data Leak is found; and
- describe how a Data Leak is reported.

MANAGING AI

Immoral Software: How AI Embeds Human Bias and Distorts Our Decision Making Prejudice

Antony Haynes, Albany Law

11:00 AM – 11:50 AM

Leading diverse organizations not only requires consciously engaging human beings and culture but also requires carefully selecting and evaluating what automated systems are employed in all aspects of decision-making. Technologies ranging from resume scanners to language translation, from face recognition to criminal sentencing software, all encode and perpetuate biases present in human society. These systems show we cannot program away human prejudice by blindly relying on computer

code. The purpose of this talk is to raise awareness of the ways computer algorithms reflect the biases of their human designers and to present a call to action for a code of ethics and for benchmarking standards around automated decision making systems.

Rise of the Machines: Cybercannibals or Humanity’s Last Hope?

Reg Harnish,
Center for Internet Security

1:00 PM – 1:50 PM

The Internet has, in a single lifetime, become the single greatest invention in the history of mankind. The ubiquitous connectedness of devices and humans has transformed every aspect of life today, and irreversibly changed every aspect of life tomorrow. And while the ubermodern conveniences of connectedness have simplified the way we communicate, learn and live, this fundamental shift in human evolution has produced tragic consequences of epic proportions. Worse yet, the next chapter in this saga is already written—computers that think, decide and act for themselves. Perhaps worst of all, this evolutionary path continues to lay waste to privacy, security and the very essence of human interaction. The machines have risen.

Attendees will be treated to:

- a fresh perspective on the emerging technologies and their risks;
- a thought-provoking dissection of the most important risks you never thought of; and
- an unhealthy slathering of cybersecurity contrarianism.

Augmented Intelligence in Cybersecurity: Data Driven Risk Reduction

Ed Cabrera, Trend Micro

2:10 PM – 3:00 PM

Some of the greatest advancements recently include artificial intelligence (AI) and machine learning (ML). While these initiatives are only just coming to the forefront in many areas, a number of forward-thinking security organizations have invested in these innovations for years—particularly when it comes to their applications for cybersecurity. However, now these same models are now being utilized in augmented intelligent SOC’s to speed up detection, response, and remediation. The future will bring greater opportunities in augmented intelligent Risk Operation Centers (ROC) to identify enterprise wide cyber risks using dark data from across the organization from corporate, business applications and data lakes.





Session Descriptions

AI-Machine Learning Augmentation and Cybersecurity: Why Smart Minds Using Smart Tools are Critical for Minimizing Risks and What You Can Do About It

Yogesh Malhotra, Global Risk Management Network, LLC

3:20 PM - 4:15 PM

The primary focus of the presentation is on helping advance intuitive understanding about AI-Machine learning augmentation and cybersecurity for auditors, business managers, critical infrastructure owners, educators, executives, information security professionals, forensic specialists, IT professionals, law enforcement, process improvement managers, and project managers about the emerging contours. With great power comes great responsibility! In the case of AI and machine learning technologies, the realization and application of such great power can yield unprecedented automation and optimization capabilities for developing more sophisticated cybersecurity and cyber risk management capabilities. However, the same AI and machine learning technologies also provide the adversary with unprecedented deception, manipulation, and attack capabilities to launch much more sophisticated cyberattacks with unprecedented destructive power. Furthermore, designers, developers and users of AI and machine learning technologies, have responsibility to acutely recognize the limitations of underlying mathematical models and algorithms and to for smartly deploy human imagination, intuition, and insight. This make up for the mechanistic limitations inherent in the design of the machines and related automation technologies. This will advance upon the latest insights generated, hi-tech practices developed, and lessons learned from leading global industry leaders at MIT, Princeton, and industry conferences such as the latest Armed Forces Communications and Electronics Association (AFCEA) C4I conference. By doing so, we will help develop intuitive understanding about AI-Machine Learning Augmentation as well as its most critical role in minimizing the downside risks in ongoing and future Cybersecurity and Risk Management capabilities and practices development and deployment.

Annual Symposium Tuesday, June 4, 2019

SYMPOSIUM SESSION 1: Deviant Behavior and Deception

Paper: Workplace Deviance in the Indian Organizational Context

Paper: Security Perceptions and Antecedents

SYMPOSIUM SESSION 2: SCADA Security

Talk: Current Challenges in State-of-the Art IoT Security

Paper: Multi-Domain Modeling for Industrial Control Systems Using Graph and Adaptive Methods

SYMPOSIUM SESSION 3: Mobile/SCADA Security

Paper: D.I.F.E.N.S.E.: Distributed Intelligent Framework for Expendable Android Security Evaluation

Paper: Passive Automatic Extraction of Industrial Control System Model

SYMPOSIUM SESSION 4: Privacy & Media

Paper: Harmonizing Privacy Concerns

Session Descriptions



Wednesday, June 5, 2019 Day Two Sessions

SECURING IDENTITY TRACK

Insider Threat Investigations

Matthew J. Lane, Janus Associates

11:00 AM – 11:50 AM

Insider threats are an ongoing concern for any organization, and they present arguably the biggest risks to data security in the Government sector today. Understanding the fundamentals of an Insider Threat can minimize your downside risk, and preparing a plan of action in advance can shorten the response time and yield better investigatory results.

This presentation will highlight the following areas:

- how to prepare for the inevitable;
- chain of custody - what it is and how to properly implement and maintain it; and
- how to investigate an insider threat or attack.

Securing Apps, Data and Infrastructure

Mike Hobbs, Microsoft

1:00 PM – 1:50 PM

The vast majority of security breaches take place when attackers gain access to an environment by stealing a user's identity. While hybrid identities allow the flexibility of using existing identities for cloud resources alongside on-premises workflows, moving to the cloud also means your traditional perimeter defense isn't able to fully protect your environment from modern threats. In today's world, identity is the new security boundary, influencing how you create policies, use tools, and protect users, devices, data, and citizens.

Attendees will learn:

- why user identity is one of your business's most important assets;
- technologies used to secure cloud-based identities; and
- identity protection capabilities that can help initiate mitigation more quickly.

SECURITY AWARENESS TRACK

Warfare of the Mind: Revolutionizing Cybersecurity Awareness

Alexander Stein, Dolus Advisors

Gopal Padinjaruveetil,

Auto Club Group

2:10 PM – 3:00 PM

Using an engaging non-traditional format, this session will address such questions as, "Can cybersecurity awareness be trained?" "Does increased awareness catalyze positive behavioral changes for improved security?" "What tools and techniques are available to more effectively decode the underpinnings of human motivation and behavior?" These and other questions will frame a discussion of their inter-disciplinary collaboration in an actual use-case, which also involved an organizational change management team from a global consulting firm, in designing and deploying an innovative cybersecurity awareness program.

Conventional cybersecurity training involves periodically dispensing modules that present key concepts and recommended actions using technical information, facts, and best practices. There is broad agreement that this is ineffective, especially in an increasingly complex cyber threat landscape. While recognizing that a different approach to enhancing information security is needed, solutions have been elusive.

The presenters will discuss the primary differentiators in this innovative cybersecurity program, from concept, blue-print and development to architecture, execution and outcome. The starting premise: examine the deficiencies of standard methods to develop solutions which actually address the core problems. The answer: leverage state-of-the-art expertise in psychological functioning and organizational psychodynamics which integrate sophisticated models of the underpinning drivers, impedances and complex psychosocial factors in human awareness, decision-making and behavior to effectively facilitate learning and foster behavioral change.

The presenters will also discuss conceptual, logistical, institutional challenges and obstacles, lessons learned and recommendations for over-the-horizon enhancements, and concludes with ample time for Q&A.

Play Your Way to Success: Building Tomorrow's Workforce

Laurin Buchanan, Secure Decisions

Jake Mihevc, Mohawk Valley

Community College

3:20 PM – 4:15 PM

Learn how cyber competitions and games can help grow the workforce! The National Initiative for Cybersecurity Education (NICE) Working Group brings together public and private sector participants to develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development. The Competitions Sub Group promotes the use of competitions in order to nurture and expand a diverse national talent pool by advancing knowledge, skills and abilities. Join members of the NICE Working Group's Competitions Sub Group



Session Descriptions

as they share how organizations of all kinds are now using competitions to both recruit new talent and provide valuable training and practice opportunities for current employees. Using case studies with different types and formats (online/in-person; individual/ team) of competitions and exercises, the presenters will illustrate how these experiences benefit both participants and sponsoring organizations.

Attendees will get a look into the wide spectrum of new competition activities across different levels of the cyber career pipeline: attracting interest in cyber careers; as part of formal education; practice training and education for the cyber workforce; and advanced, professional cyber competitions.

Presenters will also share information and resources about competitions and discuss how they fit in with certifications and the NICE Workforce Framework. Attendees will have opportunities to ask questions and weigh in on upcoming efforts by the Competitions Subgroup.

LEGAL ISSUES TRACK

-ISM in Tech: Racism, Sexism, Ableism, Classism and the Impact on Cybersecurity and Civil Rights

Raj Goel, Brainlink International Inc.
11:00 AM – 11:50 AM

This talk will explore the global trend for embedding obvious and hidden biases in technology. The social, civil rights and security impacts of hidden sexism, racism, classism and ableism embedded in technology that surrounds us. We will cover incidents and case studies from the US, China, India, Google, Microsoft, Tencent, Reddit, etc.

Practical Tips to Avoid Data Breaches

CLE Eligible

John Bandler

1:00 PM – 1:50 PM

Preventing cybercrime and data breaches requires knowledge, awareness and good information security decisions, whether at home or in large organizations, even if you are tech savvy. Everyone needs to protect themselves, their family, their organization, and the data and information kept on behalf of others. For lawyers, reasonable cybersecurity is a professional responsibility where deficiencies can have serious consequences. Law and regulation are shaping the standards for cybersecurity in business and society, and lawyers and government are playing a positive role in this development and education. To understand cybercrime and cybersecurity, and make choices that protect us and our organizations, we need knowledge and experience. There are information security principles that apply to home and organization, which can be implemented in a prioritized manner, so come hear them described in this fun and informative talk.

Social Media - Security, Confidentiality and Privacy!

CLE Eligible

Michael Fox

Tarique Collins

2:10 PM – 3:00 PM

This program will delve into the use of social media, discovery of social media in legal matters, and the ethics of using social media - both as an attorney and as a private citizen. Can you communicate with parties and witnesses over social media? Can you research parties, witnesses and jurors? We will answer these questions and consider others, and the answers are more complicated than you may think. Further, have

you ever considered the security risks and dangers for your and your clients' electronic information when you travel internationally? If not, you should, and this program will address those security concerns for electronic devices and electronically stored information. Finally, the program will examine storage of client confidential information utilizing the cloud and will analyze the specific and real ethical concerns before and while engaging in electronic storage.

Operationalizing Data Protection and Privacy Legal Requirements (and Ensuring Adoption)

Bob Siegel, Privacy Ref, Inc.

3:20 PM – 4:15 PM

Protecting the personal information of your customers, employees, and other stakeholders has increasingly become the subject of legal oversight and regulation. While cyber controls can help meet some of these requirements, ultimately an organization needs to rely on the behaviors of their employees to successfully meet these requirements. Employees all come with their own perceptions of what privacy (or data protection) means. This is influenced by their cultural background as well as their generational perspective. This begs the question of, "How do you get employees to deprecate their own perspectives on privacy in favor of the organization's?" This session will review the complexities in current privacy and data protection laws/regulations and discuss techniques to ensure the understanding, operationalization, and adoption of these requirements by your organization.

Session Descriptions



THREAT LANDSCAPE TRACK

The 2019 Verizon Data Breach Investigation Report (DBIR): Understanding the Threats You Face

Neal Maguire, Verizon
11:00 AM – 11:50 AM

All organizations are challenged by the ever-evolving changing cyber threat landscape. The Verizon 2019 Data Breach Investigations Report (DBIR) can help. It's a widely respected report that provides detailed information on the threats governments and other organizations face and how they can mitigate them. Where many other reports are based on surveys, the DBIR is based on analysis of real security incidents. Neal Maguire will provide insight into current cyber threat trends so your organization can effectively prepare, identify and respond; address moving from a reactive perimeter approach to a proactive asset-centric approach to better protect your organization; and share the results of the 2019 DBIR, now in its 12th edition, and how your organization can learn from the analysis.

Thank you to
NYSBA for
sponsoring
CLE credits

Cybersecurity 101: MS-ISAC and the U.S. Department of Homeland Security

Andrew Dolan, MS-ISAC/ U.S. Department of Homeland Security
Zia Anderson, U.S. Department of Homeland Security
1:00 PM – 1:50 PM

Cybersecurity has emerged as one of the most important issues facing public and private organizations today. The worldwide reach of the Internet means that cyber threats can come from criminals both in the United States and from foreign countries. In this session, the MS-ISAC and DHS will speak about emerging cyber threats to the government sector and what the steps and resources are that can minimize and mitigate these threats.

Zero Trust, CARTA, CJIS, CSF - OMG, How Can I Address All of These (and Other Cybersecurity Topics)?

Peter Romness, Cisco Systems
2:10 PM – 3:00 PM

You may have heard all of these as buzz words, you may have been asked about them, or you may be digging into some or all of these topics in more depth. But why are they important and how can you address them with your limited time and resources. This engaging session provides an overview of all of these topics and more. It shows how they all are efforts to guide agencies as they protect against modern cybersecurity threats. It shows how a modern information platform can enable Cybersecurity Excellence without busting the budget or throwing out your current investment. "Cybersecurity Excellence" means finding a way to both efficiently and effectively manage cyber risks. It means asking the right questions and focusing

investments in the security controls that matter most. It means successfully defending critical systems and sensitive information despite persistent threats, ongoing talent shortages, and ever-present budget constraints.

This session shows how networks and security tools can be automated to create bandwidth for security professionals, so they can focus on making operational security enhancements to the environment – improving overall cyber posture. Don't run away from these topics, come learn how to use them to your advantage to make sure your organization is secure and relieve some of the drudgery of keeping it that way.

The Modern State of Insecurity

Owen Lamb, Varonis
3:20 PM – 4:15 PM

Online security is in a constant state of flux; we face threats today that are entirely new to those we dealt with only a year or two ago. Yet at the same time, we're still dealing with the same fundamental threats we were decades ago with the likes of SQL injection and ransomware dating as far back as the 80s. This dichotomy also plays out in the sophistication of attacks we're seeing today with news headlines announcing nation state backed espionage with equal regularity to Amazon S3 buckets exposing everything to the public due to simple configuration errors. In this talk, you'll see how these threats are evolving and which are the ones we need to be especially conscious of in the modern era. It looks at real world examples of both current and emerging threats and talks about actionable steps we need to take as an industry to stem the flow of data breaches and other malicious activity. The modern state of insecurity is a scary yet necessary lesson on how we're still getting security wrong today.



Session Descriptions

ACCESS MANAGEMENT TRACK

So What's the Buzz Around Zero Trust

Renault Ross, Symantec

Salah Nassar, Symantec

11:00 AM – 11:50 AM

Zero Trust has grown in its scope and definition, evolved beyond network and becoming a practical framework capable of guiding security practitioners across all IT areas.

This session will cover:

- basics of Zero Trust;
- extended ecosystem model; and
- where to start on your journey of Zero Trust.

What is SDP (Software Defined Perimeter) and Why Does It Matter to Security Professionals?

Leo Taddeo, Cyxtera Technologies

1:00 PM – 1:50 PM

This session introduces a new, open model for network security: the Software-Defined Perimeter (SDP). This security architecture, published by the Cloud Security Alliance (CSA) and others, provides a “zero trust” model. SDP or the Software Defined Perimeter has recently been the focus of numerous articles, whitepapers and keynote presentations, and is seen by some as the evolution of Network Access Control (NAC). Gartner calls the SDP “quite disruptive to traditional network technologies with positive implications for both enterprise networks and cloud deployments of the future.” SDP can reduce or eliminate traditional networking equipment from the infrastructure, reducing IT costs and security professional headaches. The

Software-Defined Perimeter specification is a new and different way to approach network security, with rapidly growing adoption.

It is critical that security professionals have a solid understanding of this technology, the core standard, the various implementations, and how best to leverage it in their enterprise.

Actionable Takeaways include having a better understanding of Software-Defined Perimeter and Single-Packet Authorization to make informed decisions about the technology. How SDP can reduce or eliminate traditional networking equipment from the infrastructure, reducing IT costs and security professional headaches will also be explored. Leo will also discuss breaches and how SDP could have prevented or minimized losses we have seen recently.

Exception Handling for Access Management - Contingent Users & JIT Access

Mark Brooks, Identity Automation

2:10 PM – 3:00 PM

Effective and timely onboarding, offboarding, and lifecycle management is a necessary component of security in today's digital world. But what about temporary access needs for your employees? And how should you handle access for external users—a small but often forgotten subset of any organization's workforce? All too often, these ad-hoc requests are handled manually by the helpdesk or IT personnel. However, this lack of centralized oversight leaves the door wide open to attack. This session delves into the concepts of least privileged access and exception handling with just in time access. Learn how to evaluate your organization's

current processes and how they can be automated with modern Identity and Access Management to ensure proper oversight for access management.

Zero Trust Access: Five Steps to Securing the Extended Enterprise

Sean Frazier, Duo Security

3:20 PM – 4:15 PM

The perimeter-based security approach of the last century is no longer adequate for securing the modern enterprise. Today, organizations must secure a mobile workforce that uses a mix of corporate-owned and personal devices to access cloud-based applications and services, often from outside corporate networks. Attend this session to learn how this model works and explore practical implementation strategies for your organization in five logical steps.

CLOUD TRACK

The Reality of Cloud Security

Garth Whitacre, SHI International

11:00 AM – 11:50 AM

This session will cover the continuously changing topic of cloud security. We will define cloud security for the purpose of the discussion. Coverage will reference IaaS PaaS as well as SaaS models, considerations and responsibilities for each. The speaker will then provide input on key IaaS players capabilities what to expect in terms of capability and integration. Additionally, we will discuss good practices and key areas of focus for security teams as they architect cloud services. Finally, a hybrid model and its complexities will be discussed with overlapping security considerations for good practices.

Session Descriptions



Cloud Security Automation

Edward Luna, Red Hat Inc

1:00 PM – 1:50 PM

Maintaining visibility, control, and security, while ensuring governance and compliance remains paramount, but it becomes more difficult and time consuming in a hybrid infrastructure consisting of physical, virtual, cloud, and container environments. You'll learn how to face these challenges in your hybrid infrastructure by automating security and compliance. Specifically, in your hybrid infrastructure, you'll learn how to easily provision a security-compliant host, how to quickly detect and remediate security and compliance issues, how to ensure governance and control in an automated way, how to do proactive security and automated risk management, how to perform audit scans and remediations on your systems, and how to automate security to ensure compliance against regulatory or custom profiles.

RESOURCES TRACK

Workforce of the Future

Panel Discussion

2:10 PM – 3:00 PM

Forward-leaning organizations must act now to anticipate the impact of technologies that are driving business transformation and shifting skill requirements in the workplace. This session will explore what will mean for the workforce, and what universities and training providers can do to help organizations retrain existing teams and build the workforce of the future.

Using DNS and DHCP Strategically in Malware, Analytics and Compliance Architectures

Michael Katz, Infoblox

3:20 PM – 4:15 PM

Security architects have a wealth of tools available to solve security and compliance challenges. The problem is that security tool budgets are constrained and specialized teams that run tools are hard to retain. As a result, CISOs are forced to look at different ideas to solve security and compliance challenges. Many CISOs are looking for new ideas from the ground up. DNS, DHCP and IP Address Management are foundational protocols of e-business that can be used strategically to build more adaptive and efficient security architectures. This discussion will focus on the benefits of using these foundational protocols in incident response, cyber threat intel, SOAR, analytics and compliance architectures. Foundational security offers the CISO a great opportunity to do more with less in security architectures. Learn some new strategies in this discussion.

CYBER DEFENSE TRACK

Cyber Incident Response Planning - In 50 Minutes

Robert Zeglen, NYSTEC

Paul Romeo, NYSTEC

11:00 AM – 11:50 AM

In today's threat landscape, it is not a matter of if, but when, your organization will need to respond to a cyber incident. Hold off on buying that shiny new expensive security tool until you learn just how effective your incident response capability can become, simply by implementing the appropriate processes, procedures, and configurations into your existing environment. When it comes to incident response, communication

and preparation are everything, because there may not be time to react properly, as things are moving too fast when an incident happens. In this session, we will cover the full incident response lifecycle and share with you the simple steps to immediately prepare your organization to respond to an incident effectively. We will share best practices and freely available resources that you can use to prepare. It is our goal that after this presentation, you will return to your organization with an approach to plan to prepare your organization in how to respond when a cyber incident happens.

Make Your SOC Work Smarter, Not Harder

Lee Imrey, Splunk

1:00 PM - 1:50 PM

The volume and complexities of today's security incidents can tax even the largest security teams. This leaves big gaps in threat detection and incident response workflows that can put organizations at great risk. Your team can't scale to manually catch and address every incident, so which ones should you focus on and which ones should you ignore? You shouldn't be forced to make a choice. In this session, find out how leading-edge SIEM technologies combined with automation and orchestration capabilities deliver rapid incident prioritization, increased efficiencies to security teams, eliminate lethargy and reduce overall agency risk exposure. Learn how to achieve big results from intelligently streamlined incident detection and response workflows—accelerating your actions, scaling your resources, and optimizing your security operations.

The Cyber Forensics Lab Evidence Review: Insights on Nation State Attacks, Cryptocurrency Hacks, and the “eBay” of the Dark Web

Ondrej Krehel, LIFARS

2:10 PM – 3:00 PM

From evidence and insights from actual cyber forensic cases learn the methodologies, attack vectors, Indicators of Compromise, and most importantly actionable insights for preventing these attacks.

Cases reviewed will include:

- APT10 - Nation States Attacks Using Malware PlugX and RedLeaves;
- Cryptocurrency Theft of Bitcoins Valued at 75 Million USD; and
- xDedic a Dark Web Business for Buying Access to Compromised Systems.

Data Defined. The Good, the Bad and the Ugly!

Shamlan Siddiqi, NTT DATA

3:20 PM – 4:15 PM

We're at a pivotal moment in the development of the data economy, with big changes in regulations and in public perception of corporate behavior. The rules and expectations keep changing. Individual consumers have more power than ever before. Companies and consumers are grappling with this new reality. Consumers share sensitive data but don't trust the companies they share with, or fully understand how much is collected and used. for example, only 23% don't accept cookies. They also see value in data sharing but are concerned about the impact of the data economy on daily life. They also worry about privacy, but do not do enough to protect it. Companies, on the other hand. Underestimate consumer privacy concerns – only 8% of consumers strongly agree that they trust businesses to keep personal information safe. They're better at protecting their own data than their customers and, they're investing in emerging technologies like artificial intelligence (AI) to power the next wave of growth.

Thank you to TurnKey Solutions
for sponsoring pens for the
2019 NYSCSC!

Annual Symposium Wednesday, June 5, 2019

SYMPOSIUM SESSION 5: Risk Assessment

Paper: Learning Risk Assessment using Jupyter Notebooks

Paper: Managing Emerging Risks in Containerized Environments

SYMPOSIUM SESSION 6: Intrusion Detection

Paper: The Construction of Cyber Security Testbed for Intrusion Detection

Talk: State of the Art in Intrusion Detection

SYMPOSIUM SESSION 7: Linguistics and Fraud Detection

SYMPOSIUM SESSION 8: Security Education

Round Table: “Advances in Security & Forensics Education”



Thank you to Deloitte
for sponsoring bags for
the 2019 NYSCSC!

Lunch & Learn

Know Your Adversaries: Live Demo

Convention Hall

June 4, 2019

12:00 PM – 1:00 PM

Aelon Porat, Cision



Grab your lunch and meet us in the convention hall for a live demo. This live demo will reenact an infiltration to an organization's network. We will follow the attacker's footsteps to learn how they gain access to a desktop and the internal environment, then discuss how each part of the attack could have been detected and/or prevented. We begin by taking control of a user's desktop using one of a few common techniques and connecting it to a command-and-control center for the rest of the attack. Next, we steal passwords and documents, copy screen and email content, install a clandestine keylogger, record sound and stream user videos, control the mouse and keyboard, modify anti-malware settings, execute programs, reshape network traffic, and create a hidden, persistent data exfiltration channel. If time allows, we'll perform network reconnaissance and scrape login tokens to take over other computers, bypassing MFA and network segregation restrictions. This interactive demonstration will be rendered in a simulated, but fully operational, corporate setting. Our objective is to carefully examine and understand the attack procedures step-by-step, and then detail several defensive strategies against them.

Lunch will be available for purchase in the convention hall during this event.

Sponsor Demonstration Schedule

Terabyte Sponsor

AT&T

June 4

10:35 a.m. - 10:55 a.m.

Booth #56 - #58

June 5

10:35 a.m. - 10:55 a.m.

Booth #56 - #58

Megabyte Sponsor

Trend Micro

June 4

1:55 p.m. - 2:05 p.m.

Booth #54 - #55

June 5

1:55 p.m. - 2:05 p.m.

Booth #54 - #55

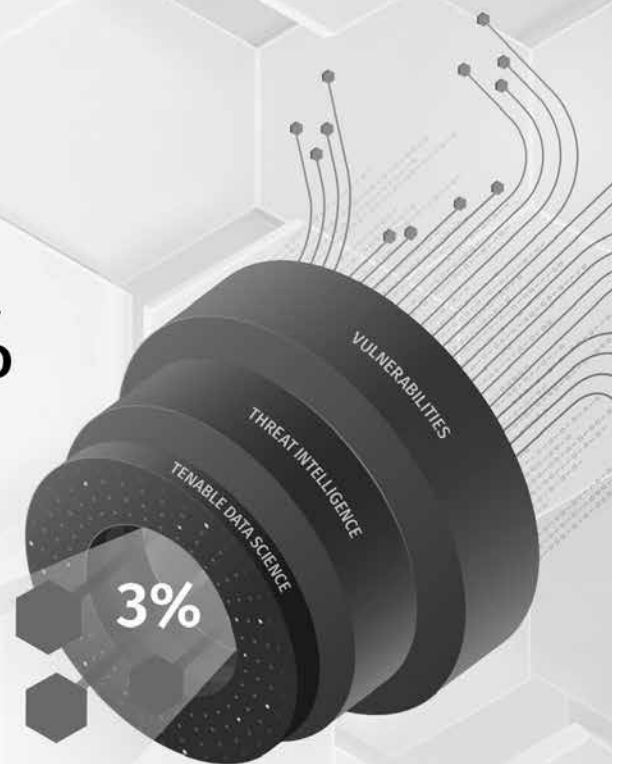


PREDICTIVE PRIORITIZATION

FOCUS ON THE 3%

of vulnerabilities that have been - or will be - exploited

The Cyber Exposure Company
tenable.com



TRAIL OF BITS

Dig Deeper

Trail of Bits combines high-end security research with a real-world attacker mentality to secure some of the world's most targeted organizations and products. We're especially well suited for the technology, finance and defense industries.

Our Services

- Engineering
- Software Assurance
- Cryptography
- Research & Development
- Training

Contact us

with your most
difficult security
challenges.

info@trailofbits.com
[@trailofbits](https://twitter.com/trailofbits)

FOUNDATIONAL SECURITY, SIMPLIFIED

Protect Your Brand and Investigate Threats Faster

REDUCE RISK using
a scalable ubiquitous
cybersecurity platform

**IMPROVE
ORCHESTRATION**
of your security tools

AUTOMATE threat
investigation and
hunting

For more information, visit
www.infoblox.com



Secure your cloud transformation

The Zscaler Cloud Platform secures state and local
agencies as they move to the cloud, providing:

- Fast user experience
- Identical protection for every user, everywhere
- The full security stack, no compromises
- Local internet breakouts
- Unmatched security, no appliances

zscaler.com

© 2019 Zscaler, Inc. All rights reserved. Zscaler is a trademark or registered trademark of Zscaler, Inc. in the United States and/or other countries. All other trademarks are the properties of their owners.



Faster Smarter Safer

As new technologies emerge at an exponential pace and security threats multiply, old network strategies simply won't work.

Download the government guide to prepare for the network of tomorrow, today.

bit.ly/GovtGuide



© 2019 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.



CYBERSECURITY CAN BE BEAUTIFUL.

At Trend Micro, we've made cybersecurity an art form, orchestrating our proven foresight, XGen™ security strategy, and passionate people to secure your connected world.

Because when you can prepare for, withstand, and rapidly recover from threats, you're free to go further and do more.

That's The Art of Cybersecurity.

Join Trend Micro's Ed Cabrera at the 2019 New York State Cybersecurity Conference for his speaking session on:

Augmented Intelligence in Cybersecurity:
Data Driven Risk Reduction

Ed Cabrera, Trend Micro

2:10 p.m. to 3:00 p.m.

Check the mobile app for location details

Stop by booth number 54 and 55 to learn about our **hybrid cloud**, **user protection**, and **network defense** solutions and don't forget to enter for a chance to win a JBL CLIP 3 speaker while you're there!

Learn more about how we've made cybersecurity beautiful at
TheArtofCyberSecurity.com



Phishing attacks detected and stopped by Trend Micro beyond native Microsoft® Office 365® security. **Created with real data by artist Matt DesLauriers.**

FORTINET®

***Join us for a highly informative session and enter to win
this 1:14 Bugatti Veyron Remote Control Car!***



***Tuesday, June 4, 2019 @ 2:10pm - Room #4
“The Importance of having an end to end, integrated Security
Fabric: Sandbox - Mail - Client - Web - Firewall & SIEM”***

The Conference is proud to support cyber security education.

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 2018 - 2019 recipients:

Eric Carpenter

Bryan Vargas

Sponsors



TERABYTE SPONSOR

Our first name has always been American, but today you know us as AT&T. We're investing billions into the economy, providing quality jobs to over 200,000 people in the U.S. alone. We're supporting the veterans who make our country stronger and providing disaster relief support to those who need it the most. By bringing together solutions that help protect, serve and connect – committed AT&T professionals are working with the public sector to transform the business of government. No company is more invested in America's future than AT&T. www.att.com/publicsector



MEGABYTE SPONSOR

Trend Micro, a global leader in cybersecurity, is passionate about making the world safe for exchanging digital information, today and in the future. Artfully applying our XGen™ security strategy, our innovative solutions for consumers, businesses, and governments deliver connected security for data centers, cloud workloads, networks, and endpoints. Our connected threat defense enables seamless sharing of threat intelligence and provides centralized visibility and investigation to make organizations their most resilient.

With over 6,500 employees in 50 countries and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. www.trendmicro.com.

Sponsors



KILOBYTE SPONSOR

Infoblox leads the way to next-level DDI with its Secure Cloud-Managed Network Services with 8,000 customers including 350 of the Fortune 500. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Next-level security helps protect against the rising flood of cyberattacks, leveraging 14 billion threat indicators and 30 plus API security integrations. Next-level reliability provides a Tier 1 foundation with five nines availability, delivered as software-defined services. Next-level automation reduces manual tasks by 70% and annual costs by more than \$1 million. www.infoblox.com



KILOBYTE SPONSOR

Tenable is the Cyber Exposure company. Over 27,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Our goal is to arm every organization, with the visibility and insight to answer four critical questions at all times: Where are we exposed? Where should we prioritize based on risk? Are we reducing our exposure over time? How do we compare to our peers?



KILOBYTE SPONSOR

Zscaler offers two service suites that eliminate the cost and complexity of gateway appliances. Zscaler Internet Access securely connects users to internet and SaaS applications, scanning every byte of traffic to protect against cyber threats and data leakage. Zscaler Private Access provides fast access to internal applications hosted in the data center or public clouds—without the need for a VPN.

Exhibitors



With headquarters at Rome, NY, the Air Force Research Laboratory Information Directorate (AFRL/RI) research vector develops novel and affordable Command, Control, Communications, Computing, Cyber and Intelligence (C4I) technologies. RI is recognized as a national asset and leader in C4I. Refining data into information and knowledge for decision makers to command and control forces is what we do. This knowledge gives our air, space, and cyberspace forces the competitive advantage needed to protect and defend this great nation.



Centripetal delivers intelligence-driven security. Centripetal invented the Threat Intelligence Gateway and leverages its technologies to deliver CleanINTERNET, a comprehensive intelligence-led cyber service. With Centripetal, customers across every vertical and of every size can persistently prevent over 90% of known threats with intelligence applied in advance. Gartner, Inc. has named Centripetal a "Cool Vendor" in security for 2017, and the Security Innovation Network (SINET) named Centripetal a "SINET-16" awardee. Centripetal's technology is protected by over 50 US and international patents.



Ana-Data is an Inc. 5000 full-service IT products and services-related company providing custom software development, technology consulting, business intelligence, data analytics and information security solutions. Services we offer are built on our more than two decades of rich industry experience, technological competence and operational excellence. Our Information security services include both proactive and reactive strategies – we help in creating policies, conducting end-to-end assessments, and implementing cyber resilient methodologies. This includes recovery services, awareness training, and test systems to identify vulnerabilities.

Clear Infosec services integrates automation, deep analytics and correlation across multiple domains of security to provide enhanced visibility and situational awareness across the network, applications, IOT Security and the Cloud-via a single-pane view with extensive reporting capabilities. Clear GRC product assists in effectively assessing and managing enterprise risks by providing guidance on Governance, Risk and compliance."



Checkmarx is the Software Exposure Platform for the enterprise. Over 1,400 organizations around the globe rely on Checkmarx to measure and manage software security risk at the speed of DevOps. Checkmarx serves five of the world's top 10 software vendors, four of the top American banks, and many government organizations and Fortune 500 enterprises, including SAP, Samsung, and Salesforce.com. Learn more at [Checkmarx.com](https://checkmarx.com) or follow us on Twitter: @checkmarx.

Exhibitors



CSDNET has been providing innovative IT design, implementation and support services for over 25 years. Our comprehensive cyber security designs leveraging real network segmentation and “next-generation” firewall technologies provides a high performance IT security platform. Our carefully integrated network, cyber and physical security implementations combined with our support packages are effective in mitigating cyber breaches as well as protecting against IOT breaches - creating a stable environment with limited downtime. Our partnerships with Sonicwall, Extreme Networks and Genetec Security Center enables us to provide the best hardware and software platforms using industry standards technologies.



Cyxtera brings together a worldwide footprint of 50+ data centers, a unique hyperconverged infrastructure (HCI) on-demand solution and a modern, hybrid- and cloud-ready security portfolio providing more than 3,500 enterprises, government agencies and service providers an integrated, secure and cyber-resilient infrastructure platform for critical applications and systems. For more information about Cyxtera visit, <http://www.cyxtera.com/>.



Cybereason, creators of the leading Cyber Defense Platform, gives the advantage back to the defender through a completely new approach to cybersecurity. Cybereason offers endpoint detection and response (EDR), next-generation antivirus (NGAV), and active monitoring services, powered by its cross-machine correlation engine. The Cybereason suite of products provides unmatched visibility, increases analyst efficiency and effectiveness, and reduces security risk. Cybereason is privately held, has raised \$189 million from top-tier VCs, and is headquartered in Boston, with offices in London, Tel Aviv, and Tokyo.



Duo Security, now part of Cisco, is the leading provider of Trusted Access security and multi-factor authentication. Duo's zero-trust security platform, Duo Beyond, enables organizations to provide trusted access to all of their critical applications - for any user, from anywhere, and with any device. Duo is a trusted partner to more than 14,000 customers globally, including Dresser-Rand, Etsy, Facebook, Paramount Pictures, Random House, Zillow and more. Founded in Ann Arbor, Michigan, Duo has offices in growing hubs in Detroit; Austin, Texas; San Mateo, California; and London. Visit duo.com to find out more.

Exhibitors



DynTek Services is a leading provider of professional technology services to state and local governments, educational institutions and commercial entities in the largest IT markets nationwide. DynTek creates security solutions that protect your business information and thoroughly safeguard your entire IT environment – but we don't stop there. From virtualization and cloud computing to networking and mobility, DynTek provides professional technology solutions across the core areas of our customers' technical environment and serves as a single source for all your most critical technology requirements. www.dyntek.com



ENSIL

enSilo protects businesses around the world from data breaches and disruption caused by cyber attacks. The enSilo Endpoint Security Platform comprehensively secures endpoints in real-time pre- and post-infection without alert fatigue, excessive dwell time or breach anxiety while also containing incident response costs by orchestrating automated detection, prevention and incident response actions against advanced malware. enSilo's patented approach stops advanced malware with a high degree of precision, provides full system visibility and an intuitive user interface and combines next-generation antivirus (NGAV), application communication control, automated endpoint detection and response (EDR) with real-time blocking, threat hunting, incident response, and virtual patching capabilities in a single agent. The platform can be deployed either in the cloud or on-premises and supports multi-tenancy.



The mission of Empire State Development ("ESD") is to promote a vigorous and growing state economy, encourage business investment and job creation, and support diverse, prosperous local economies across New York State through the efficient use of loans, grants, tax credits, real estate development, marketing and other forms of assistance. esd.ny.gov

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.

Exhibitors



Exabeam is the Smarter SIEM™ company. We empower enterprises to detect, investigate, and respond to cyberattacks more efficiently so their security operations and insider threat teams can work smarter. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines™, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures.



Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 375,000 customers trust Fortinet to protect their businesses.



Forescout Technologies is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environment and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, 100-percent real-time discovery and classification, as well as continuous posture assessment. As of December 31, 2018, 3,300 customers in over 80 countries rely on Forescout's infrastructure-agnostic solution to reduce the risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance and increase security operations productivity. Learn how at www.forescout.com.



Google is a trusted technology partner who understands how to help agencies transition from legacy architectures and utilize their data to fuel true mission success. Google Cloud Platform provides cloud-native infrastructure with layered security, machine learning and analytics at web-scale to rapidly innovate and advance agency goals.

Exhibitors



The primary role of the Griffiss Institute (GI) is to advocate and facilitate the co-operation of private industry, academia, and government in developing solutions to critical cyber security problems. Another prime role is to build upon technologies under development at the Air Force Research Laboratory Information Directorate (AFRL/RI) to further strengthen our nation's security. By partnering AFRL/RI with private industry and academia, the GI can facilitate and grow the technology base of the Upstate New York region. Our goal is to foster research leading to new solutions in information sciences and spinning out new business opportunities, locally and nationally.



Why IBM?

In an industry focused on building walls, IBM Security is focused on creating an open, connected security ecosystem that leverages artificial intelligence, cloud, orchestration and collaboration to help you improve compliance, stop threats, and grow your business securely. Our strategy reflects our belief that today's defenses will not suffice tomorrow. It challenges us to approach our work, support our clients and lead the industry with forward-thinking integrated solutions and proven experts, allowing you to be fearless in the face of cyber uncertainty. <https://www.ibm.com/security>



**Hewlett Packard
Enterprise**

Hewlett Packard Enterprise is a global technology leader focused on developing intelligent solutions that allow customers to capture, analyze, and act upon data seamlessly from edge to cloud. HPE enables customers to accelerate business outcomes by driving new business models, creating new customer and employee experiences, and increasing operational efficiency today and into the future.



**IDENTITY
AUTOMATION™**

Identity Automation helps organizations embrace security, increase business agility, and deliver an enhanced user experience with RapidIdentity, the most complete identity, access, governance, and administration platform available. Deployments take weeks, not months or years. Identity Automation operates globally, with over 950 customers and tens of millions of identities managed across on-premises and cloud resources.

Exhibitors



iSECURE is a woman-owned, IT Security company based in Upstate New York. Founded in 1995 as an ISP, iSECURE has extensive knowledge and practice in information technology, and has evolved into being an experienced, trusted and focused only on IT Security Solutions. Our multi-dimensional experience in IT Operations with a Security-focus gives us an edge that most other companies lack. We began our Security charge in these early ISP years, providing managed security services to customers collocating their servers in our datacenter. Our experience as a carrier gave us great insight into the concerns and hardships that today's infrastructures are exposed to. Clients have always leaned on us both for our expertise as well as our ability to listen and understand their needs.



Meridian IT Inc. is part of Meridian Group International, operating since 1979. Headquartered in Deerfield, IL, Meridian IT works with clients domestically and across many international borders to modernize technology strategies, deliver innovation, and maximize business productivity. Partner with us to unlock your company's true potential. Learn more at www.meridianitinc.com or www.onlinemeridian.com.



iV4 is an IT consulting organization specializing in aligning our customers with tailored technology solutions that enable them to modernize, protect, and grow their business. iV4 operates with a 'security by design' mentality by managing, assessing, and architecting networks with security best practices ingrained in every engagement.



NYSTEC is an independent advisor to clients. We understand that security is not a product but rather an ongoing process that must address threats with multiple layers of controls. We have in-depth experience with Federal and NYS government regulations and policies, and can help you develop a layered strategy to increase the integrity, confidentiality and availability of your IT systems. Our security consultants average 20-plus years of experience and have advanced degrees and required certifications, including CISSP. Cybersecurity must be a continuous effort encompassing policy, process, procedure, education, monitoring and enforcement. NYSTEC can help you secure your networks and systems.

Exhibitors



Paraben provides technology for digital forensic investigations, forensic-grade auditing, and digital data intelligence. Processing capabilities include computer, cloud, email, mobile device, smartphones, and IoT data processing. Paraben's innovative solutions are always on the pulse of technology with an easy to approach process for digital data.



Privacy Ref emphasizes alignment of privacy practices with our clients' organizational and operational goals through assessment, consulting, coaching, and training services. We offer tailored solutions that enhances current or develops new, effective data privacy programs using our experience and industry best practices. Your goals drive the hands-on approach of Privacy Ref consultants. We develop effective processes which minimize disruption to day-to-day operations, creating a custom-made privacy program unique to your business needs. Privacy Ref offers one of the most cost-effective approaches to privacy in the industry.



PPM Associates, Inc. (PPMA) is a veteran-owned company, founded in 1993. PPMA was established to provide clients with the most comprehensive network and communications products available. Since our founding, PPMA has evolved into a security and network communication company which provides the best-of-breed products and services for our on-premise and cloud-based clients across all industries.

At this show, we will be working with one of our leading and most comprehensive vendors, Heimdal Security. Heimdal Security's Thor product line is a modular End Point security product that is includes Thor Vigilance "Next-Gen" Antivirus w/EDR, DarkLayer GUARD w/ Vector-N Detection DNS-based malware filtering and especially, Xploit Resilience, for Automated Vulnerability and Patch Management for all your top 3rd Party apps & Microsoft/Windows software.



Proofpoint is a leading cybersecurity company that protects organizations' biggest risks and greatest assets: their people. With an integrated suite of cloud-based threat, information and user protection solutions, we help organizations around the world mitigate their most critical security and compliance risks. More than half of the Fortune 100 trust us to stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. No one protects people, the data they create, and the digital channels they use more effectively than Proofpoint.

Exhibitors



RSA, a Dell Technologies business, offers mission-driven security solutions that uniquely link business context with security incidents to help organizations manage digital risk and protect what matters most. Award winning cybersecurity solutions from RSA can detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world and helps more than 90% of Fortune 500 companies thrive in an uncertain, high-risk world. For more information, visit rsa.com.



SHI International Corp. is a global provider of information technology products and services. Driven by an experienced sales force and backed by software volume licensing experts, hardware procurement specialists, and certified IT services professionals, SHI delivers custom IT solutions to Corporate, Enterprise, Public Sector and Academic customers.

SHI offers our NYS customers many contract vehicles to purchase IT solutions, including 30+ NYS OGS Manufacturer Umbrella contracts, the "miscellaneous hardware and software" Distributor Umbrella contract, and various national contracts such as National IPA. SHI has a large field presence in NYS with representatives across NYC and UNY, and is a recognized MWBE in NYC.

Founded in 1989, SHI is headquartered in Somerset, N.J., and realized \$10 billion in revenue while topping 4,000 employees in 2018.



SailPoint enables state governments and public agencies to prevent data breaches, maintain regulatory compliance and reduce IT workloads. Recognized by Gartner, Forrester and KuppingerCole as the leading authority on identity, SailPoint's comprehensive solution governs and secures all user access to sensitive citizen data stored in applications and files, in the cloud and on premises. Furthermore, it leverages machine learning and artificial intelligence to provide deliver actionable insights while boosting IT efficiency.



Splunk Inc. (NASDAQ: SPLK) helps organizations ask questions, get answers, take actions and achieve business outcomes from their data. Organizations use market-leading Splunk solutions with machine learning to monitor, investigate and act on all forms of business, IT, security, and Internet of Things data. Use Splunk software in the cloud and on-premises to improve service levels, reduce operations costs, mitigate security risks, enable compliance, enhance DevOps collaboration and create new product and service offerings. Join millions of passionate users and try Splunk software for free: www.splunk.com/free-trials.

Exhibitors



Tanium gives the world's largest enterprises and government organizations the unique power to secure, control and manage millions of endpoints across the enterprise. Serving as the "central nervous system" for enterprises, Tanium empowers cybersecurity and IT operations teams to ask questions about the state of every endpoint across the enterprise in plain English, retrieve data on their current state and execute change as necessary, all within seconds. Visit us at www.tanium.com or follow us on Twitter at @Tanium.



Currently ranked #59 on the Solution Provider 500, the award winning ThunderCat Technology is a Service-Disabled Veteran-Owned Small Business (SDVOSB) that delivers technology solutions and services to government organizations, educational institutions, and commercial companies. Specifically, ThunderCat is a systems integrator that brings an innovative approach to solving customer problems in and around the datacenter by providing strategies for Data Storage, Networking, Cyber Security, and Cloud Transformations. A proven leader, ThunderCat Technology provides and optimizes technologies from best of breed manufacturers. Clients include DOD, HHS, DHS, VA, Treasury, FBI, State of Virginia, Hawaii Health Systems, and Avery Dennison.



Tech Valley Talent (TVT), a Certified Woman-Owned Business (WBE), is an Information Technology (IT) Professional Services firm that is well-known and highly respected for providing specialized IT services and solutions to clients. These services include our practice areas in IT Security, Data Management, Web Solutions, and Advisory Services. Centrify is redefining the legacy approach to Privileged Access Management by delivering cloud-ready Zero Trust Privilege to secure modern enterprise use cases. Zero Trust Privilege mandates a "never trust, always verify, enforce least privilege" approach. Over half the Fortune 100, and 150+ public sector agencies, trust Centrify to stop privileged credential abuse.



TurnKey Internet is a full-service Data Center and Cloud Hosting Solutions provider focused on helping businesses simplify their IT infrastructure by leveraging the best-in-class technologies of The Cloud. Headquartered in New York's Tech Valley Region, TurnKey Internet's Flagship company owned data center is SSAE-18 SOC 2 certified, as well as HIPAA compliant. The facility is powered exclusively by on-site solar and hydroelectric sources to provide a 100% renewable energy footprint. Services offered include Enterprise Colocation, Public Cloud, Private Cloud, Dedicated & Bare Metal Servers, Virtual Servers, Backup & Disaster Recovery, Online Storage, Web Hosting, Managed Hosting, and Hybrid Solutions.

Exhibitors



Vandis Security, Cloud, Networking, Mobility and Infrastructure practices are focused on helping our clients build secure and stable systems, both on-prem and in the cloud. Securing your data and network is a bigger, more challenging, and more critical job than ever before. Vandis has assembled a team of architects and engineers with broad experience and extensive training to provide you with the assistance you need. This expertise allows us to meet your goals from Design Consultation through Implementation and Managed Services. With over 35 years of experience, Vandis has the proven ability to navigate the ever-changing technology and business landscape.



As a leading provider of communications and security services, Verizon understands that one size doesn't fit all. That's why Verizon stands ready to deliver the breadth of our capabilities to address the specific needs of the many municipalities, counties, institutions of higher learning, public schools and small/medium businesses we serve. Our products supporting these sectors are broad and deep, ranging from networking solutions and collaborative services to data security and Smart Cities. With our strong portfolio of relevant products and services, Verizon remains dedicated to the public sector we proudly serve. www.verizon.com/businessmarkets

The 2019 NYS Cyber Security Conference would like to thank all of our sponsors, exhibitors, speakers, volunteers, and attendees for making this another successful year!



See you in June 2020 for the
23rd Annual NYS Cyber Security Conference

Additional Exhibitors



BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, Cylance protects the endpoint without increasing staff workload or costs. We call it the Science of Safe. Learn more at www.cylance.com.



Public Sector enterprises need a solution that protects against all cyber threats - simple and sophisticated. CrowdStrike is the leader in cloud-delivered endpoint protection and goes beyond traditional antivirus to provide complete protection. CrowdStrike Falcon seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates 40 billion security events from across the globe to immediately prevent and detect threats. CrowdStrike's ultimate goal is to help its customers stop breaches immediately, with minimal time, effort and impact on their business processes.



Corelight makes powerful network security monitoring (NSM) solutions that transform network traffic into rich logs, extracted files, and security insights, helping security teams achieve more effective incident response, threat hunting, and forensics. Corelight Sensors run on Zeek (formerly called "Bro"), the open-source NSM tool used by thousands of organizations worldwide. Corelight's family of network sensors dramatically simplify the deployment and management of Zeek and expand its performance and capabilities. Corelight is based in San Francisco, California and its global customers include Fortune 500 companies, large government agencies, and major research universities. For more information, visit <https://www.corelight.com>



Deloitte's Government & Public Services practice – our people, ideas, technology and outcomes – are all designed for impact. Our team of over 12,000 professionals across the country bring fresh perspective to help you anticipate disruption, reimagine the possible, and fulfill your mission promise. Whether you are at the crossroads of AI and workforce transformation, cyber and IT modernization or digital and citizen experience—we bring actionable insights to drive bold and lasting results. Our shared purpose and passion help you make an impact and improve the lives of citizens.

How can we make a difference together? Contact us to get started. www.deloitte.com/us/government@DeloitteGov

Passport Raffle

win *Great* PRIZES!

22nd Annual **NYS CYBER SECURITY** Conference
14th Annual Symposium on Information Assurance
June 4-5, 2019

Drawings will be held:
Tuesday, June 4 at 3:00 pm*
Wednesday, June 5 at 3:00 pm*

Complete the passport with all exhibitor stamps for a chance to win. Hand in the completed passport by 3:00pm on June 4 to be entered in the drawings on both days!

Please enter your name and contact information on the completely stamped passport prior to drop off at registration.

Complete the information below before entering:

NAME: _____

PHONE: _____

EMAIL: _____

Winners must collect prizes by end of day

See reverse side for sponsors and exhibitors



Conference Sponsors and Exhibitors

PLEASE VISIT EACH BOOTH FOR A STAMP AND SHOW YOUR SUPPORT!



Empire State
Development



FORESCOUT



[illegible]

At-A-Glance Day 1 – June 4, 2019

7:30am – 4:15pm	New York State Cyber Security Conference						
8:00am	Opening of the Exhibit Hall Convention Hall						
9:00am – 10:30am	Welcome Address: Robert H. Samson, New York State CIO Keynote: Michael Aiello, Product Management Director, Google						
10:30am – 11:00am	Visit the Exhibitors (Terabyte Sponsor Demo: AT&T 10:35am-10:55am)						
11:00am – 11:50am	Pen Testing	Security Evolution	Compliance	Data Protection	Managing AI	ASIA	Deviant Behavior and Deception
	Here We go Again. Red Teaming Stories from the Trenches Tyler Wrightson Leet Cyber Security	The Leadership Vision for Security and Risk Management 2019 Jeffrey Wheatman Gartner, Inc.	Navigating Security and Privacy Compliance Challenges Michael Corby M Corby & Associates, Inc.	Digital Identity—The Fabric Connecting and Securing Internal and External Access Mike Wyatt Deloitte	Immoral Software: How AI Embeds Human Bias and Distorts Our Decision Making Antony Haynes Albany Law		
11:50am – 1:00pm	Meeting Room 6	Meeting Room 2-3	Meeting Room 5	Meeting Room 4	Meeting Room 1	Meeting Room 7	SCADA Security
	Convention Hall Unleash the Infection Monkey: A Modern Alternative to Pen-Tests Dave Klein Guardicore	Biometrics, Facial Recognition and Autonomous Vehicles CLE Credit	A Calm Approach to Regulatory Confusion Mike Semel Semel Consulting LLC F. Paul Greene Harter Secrest & Emery LLP	Digital Compliance: Understanding Your Sensitive Data Footprint Michael Giordano DynTek Services	Rise of the Machines: Cybercannibals or Humanity's Last Hope? Reg Harnish Center for Internet Security		
1:00pm – 1:50pm	Meeting Room 6	Meeting Room 2-3	Meeting Room 5	Meeting Room 4	Meeting Room 1	Meeting Room 7	
1:50pm – 2:10pm	Visit the Exhibitors (Megabyte Sponsor Demo: Trend Micro 1:55pm-2:05pm)						
2:10pm – 3:00pm	Supply Chain Management	Who Owns Your "Personal" Emails and Social Media Data?	State and Federal Privacy Regulations Abound: What it Means for New York Business	Importance of having an End to End Integrated Security Fabric	Augmented Intelligence in Cybersecurity: Data Driven Risk Reduction	Mobile/SCADA Security	
	Where Security, Trade and Politics Converge Robert Mayer USTelecom	Mark A. Berman Shawndra G. Jones CLE Credit	Dimitri Sirota BigID	David Leinberry Fortinet	Ed Cabrera Trend Micro		
3:00pm – 3:20pm	Meeting Room 1	Meeting Room 2-3	Meeting Room 5	Meeting Room 4	Meeting Room 1	Meeting Room 7	
3:20pm – 4:15pm	Visit the Exhibitors	From the Engine Room to the Board Room	Privacy and Breach Protection - Achieving Safe Harbor by Knowing What You Have and How to Protect it	Protect your Data by Understanding How a White Hacker Finds a Data Leak	AI-Machine Learning Augmentation and Cybersecurity: Why Smart Minds Using Smart Tools are Critical for Minimizing Risks, and, What You Can Do About it.	Privacy & Media	
	Contracting for Cybersecurity (and What to do When You Can't Get Everything You Want) Mark Francis Holland & Knight LLP	Chris Hallenbeck Tanium	Robert Roy Micro Focus Government Solutions	Tom Buoniello Binary Edge	Yogesh Malhotra Global Risk Management Network, LLC		
	Meeting Room 1	Meeting Room 4	Meeting Room 5	Meeting Room 6	Meeting Room 2-3	Meeting Room 7	

At-A-Glance Day 2 – June 5, 2019

7:30am – 4:15pm	New York State Cyber Security Conference												
8:00am	Opening of the Exhibit Hall												
9:00am – 10:30am	Convention Hall												
10:30am – 11:00am	ASIA Keynotes: Daniel P. Bagge, Cyber Attaché of the Czech Republic to the United States and Canada												
11:00am – 11:50am	Visit the Exhibitors (Terabyte Sponsor Demo: AT&T 10:35am-10:55am)												
11:50am – 1:00pm	1:00pm – 1:50pm	1:50pm – 2:10pm	2:10pm – 3:00pm	3:00pm – 3:20pm	3:20pm – 4:15pm	Securing Identity	Legal Issues	Threat Landscape	Access Management	Cloud	Cyber Defense	ASIA	
						Insider Threat Investigations Matthew J. Lane Janus Associates, Inc.	-ISM in tech. Racism, Sexism, Ableism, Classism and the Impact on Cyber Security and Civil Rights Raj Goel Brainlink International Inc.	The 2019 Verizon Data Breach Investigation Report (DBIR): Understanding the Threats You Face Neal Maguire Verizon	So What's the Buzz Around Zero Trust? Renault Ross Salah Nassar Symantec	The Reality of Cloud Security Garth Whitacre SHI International	Cyber Incident Response Planning - In 50 Minutes Robert Zeglen Paul Romeo NYSTEC	Risk Assessment	
						Meeting Room 5	Meeting Room 1	Meeting Room 2	Meeting Room 3	Meeting Room 4	Meeting Room 6	Meeting Room 7	
						Lunch on your own and Visit the Exhibitors							
						Securing Apps, Data, and Infrastructure Mike Hobbs Microsoft	Practical Tips to Avoid Data Breaches John Bandler CLE Credit	Cybersecurity 101: MS-ISAC and the U.S. Department of Homeland Security Andrew Dolan MS-ISAC Zia Anderson U.S. Department of Homeland Security	What is SDP (Software Defined Perimeter) and Why Does it Matter to Security Professionals? Leo Taddeo Cyxtera Technologies	Cloud Security Automation Edward Luna Red Hat Inc.	Make Your SOC Work Smarter, Not Harder Lee Imrey Splunk	Intrusion Detection	
						Meeting Room 5	Meeting Room 1	Meeting Room 6	Meeting Room 3	Meeting Room 2	Meeting Room 4	Meeting Room 7	
						Visit the Exhibitors (Megabyte Sponsor Demo: Trend Micro 1:55pm-2:05pm)							
						Security Awareness	Social Media - Security, Confidentiality and Privacy! Michael Fox Tarique Collins CLE Credit	Zero Trust, CARTA, CJIS, CSF - OMG, How Can I address All of These (and Other Cybersecurity Topics)? Peter Romness Cisco Systems	Exception Handling for Access Management - Contingent Users & JIT Access Mark Brooks Identity Automation	Resources	The Cyber Forensics Lab Evidence Review: Insights on Nation State Attacks, Cryptocurrency Hacks, and the "eBay" of the Dark Web Ondrej Krehel LIFARS	Linguistics and Fraud Detection	
						Warfare of the Min: Revolutionizing Cybersecurity Awareness Alexander Stein Dolus Advisors Gopal Padingjaruveetil Auto Club Group				Workforce of the Future Panel Discussion			
						Meeting Room 5	Meeting Room 6	Meeting Room 2	Meeting Room 3	Meeting Room 1	Meeting Room 4	Meeting Room 7	
						Visit the Exhibitors							
						Play your Way to Success: Building Tomorrow's Workforce Laurin Buchanan Secure Decisions	Operationalizing Data Protection and Privacy Legal Requirements (and Ensuring Adoptions) Bob Siegel Privacy Ref, Inc.	The Modern State of Insecurity Owen Lamb Varonis	Zero Trust Access: Five Steps to Securing the Extended Enterprise Sean Frazier Duo Security	Using DNS and DHCP Strategically in Malware, Analytics and Compliance Architectures Michael Katz Infoblox	Data Defined. The Good, The Bad and the Ugly! Shamlan Siddiqi NTT Data	Security Education	
						Meeting Room 5	Meeting Room 1	Meeting Room 2	Meeting Room 3	Meeting Room 6	Meeting Room 4	Meeting Room 7	

Enhance your conference experience with our mobile app:

- Review your schedule and get event announcements
 - Connect with sponsors and attendees

Visit <https://crowdcc/s/2HxGQ> now to begin!



After the Conference

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.

TERABYTE SPONSOR



MEGABYTE SPONSOR

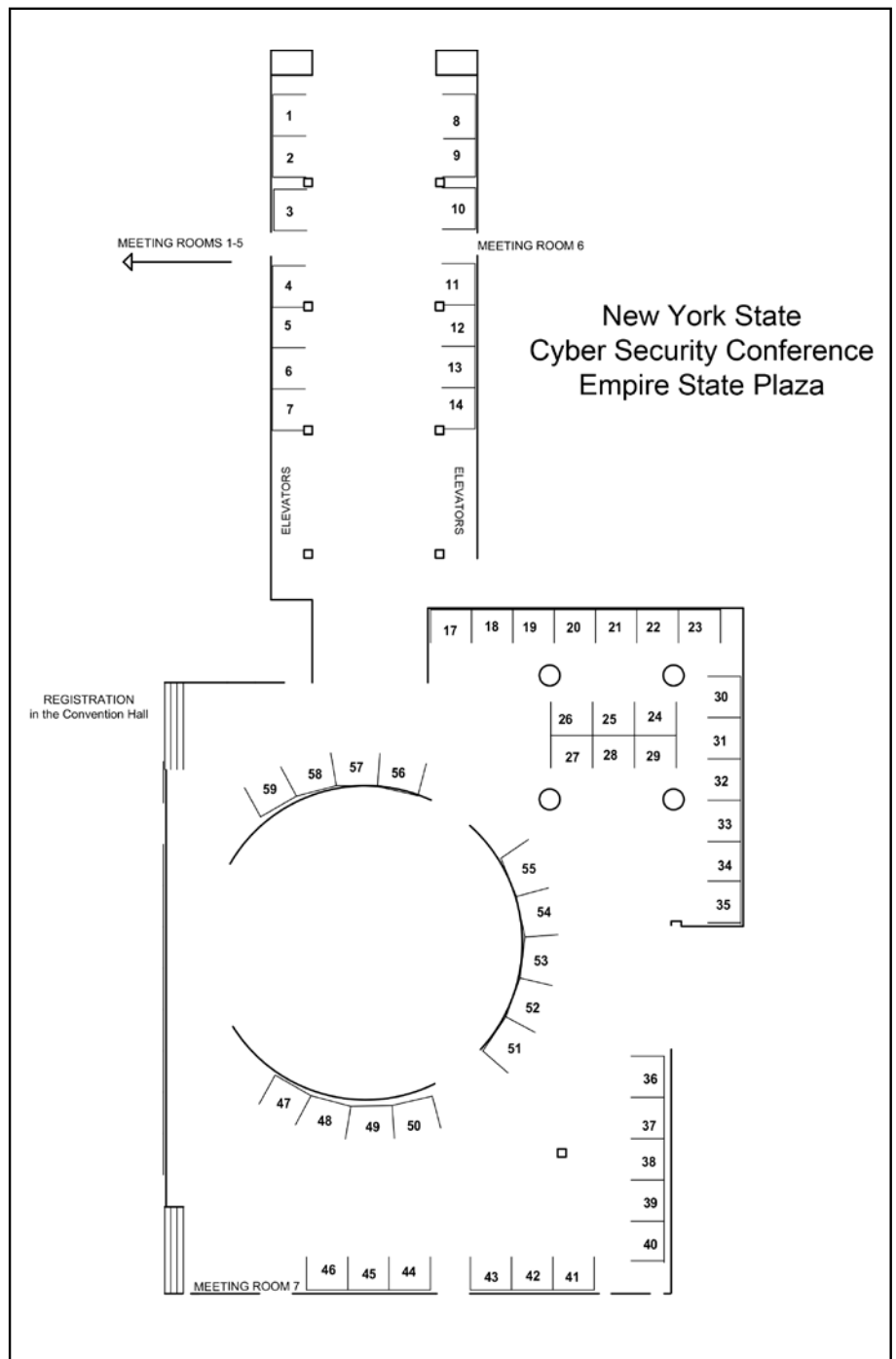


KILOBYTE SPONSORS



Booth Assignments

CrowdStrike.....	1
Ewaste	2
Dyntek.....	3
Vandis	4
Centripical Networks	5
Tanium	6
SHI	7
PPM.....	8
Proofpoint.....	9
Splunk.....	10
cybereason.....	11
HPE	12
Exabeam	13
Privacy Ref	14
Meridian	17
Thundercat Technologies.....	18
Forescout	19
Empire State Development (ESD).....	20
CSDNET.....	21
Checkmarx	22
IBM.....	23
Isecure	24
Cyxtera/Subsidium	25
Fortinet.....	26
Tenable- KILOBYTE.....	27
Sailpoint	28
DUO Security	29
Conference Co-Hosts.....	30, 31
Paraben	32
iv4.....	33
Zscaler- KILOBYTE.....	34
Infoblox- KILOBYTE.....	35
NYSTEC.....	36
Verizon	37
Ensilo	38
Griffis Institute	39
AFRL.....	40
RSA	41
Blackberry /Cylance.....	42
Corelight.....	43
ANA Data.....	50
Turnkey Solutions	51
Carahsoft/ Google.....	52
Identity Automation.....	53
Trend Micro- MEGABYTE	54, 55
AT&T- TERABYTE	56, 57, 58
Tech Valley Talent	59



Passport Raffle: Visit our exhibitors for a chance to win some amazing prizes. All you need to do is bring the Exhibitor Passport (found on page 41) 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. breaks on Tuesday, June 4 and Wednesday, June 5. 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.