New York State Cyber Security Conference
June 8-9, 2016

BEST PRACTICES
AWARENESS & TRAINING
RISK MITIGATION
INCIDENT RESPONSE

FOCUSING THE CYBER SECURITY LENS

www.its.ny.gov/eiso/conference/2016

TERABYTE SPONSOR

PRESENTED BY

THE NYS FORUM

UNIVERSITY AT ALBANY
State University of New York
## Agenda Day 1 – June 8, 2016

<table>
<thead>
<tr>
<th>Time</th>
<th>Meeting Room 1</th>
<th>Meeting Room 2</th>
<th>Meeting Room 3</th>
<th>Meeting Room 4</th>
<th>Meeting Room 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00AM - 9:30AM</td>
<td>Opening of the Exhibit Hall</td>
<td>Opening of the Exhibit Hall</td>
<td>Opening of the Exhibit Hall</td>
<td>Opening of the Exhibit Hall</td>
<td>Opening of the Exhibit Hall</td>
</tr>
</tbody>
</table>

**Meeting Room 1 - Event Sponsor Area A (10:30am - 10:55am)**
- **Agenda:**
  - [Meet the Vendors] (World Security & Cryptography)

**Meeting Room 2 - Event Sponsor Area B (10:30am - 10:55am)**
- **Agenda:**
  - [Meet the Vendors] (World Security & Cryptography)

**Meeting Room 3 - Event Sponsor Area C (10:30am - 10:55am)**
- **Agenda:**
  - [Meet the Vendors] (World Security & Cryptography)

**Meeting Room 4 - Event Sponsor Area D (10:30am - 10:55am)**
- **Agenda:**
  - [Meet the Vendors] (World Security & Cryptography)

**Meeting Room 5 - Event Sponsor Area E (10:30am - 10:55am)**
- **Agenda:**
  - [Meet the Vendors] (World Security & Cryptography)
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:00am - 10:00am</td>
<td>Visit the Exhibitors (Tribeca Scooter Demo: AT1X 10:00am - 10:30am)</td>
<td>Meeting Room 1</td>
</tr>
<tr>
<td>10:00am - 10:30am</td>
<td>Human Element</td>
<td>Meeting Room 2</td>
</tr>
<tr>
<td>10:30am - 11:30am</td>
<td>Digital Maturity in the Government - The Legal Issues</td>
<td>Meeting Room 3</td>
</tr>
<tr>
<td>11:30am - 12:30pm</td>
<td>AGENDA DAY 2 – JUNE 9, 2016</td>
<td>Meeting Room 4</td>
</tr>
<tr>
<td>12:30pm - 1:30pm</td>
<td>Lunch on your own and visit the Exhibitors</td>
<td>Meeting Room 5</td>
</tr>
<tr>
<td>1:30pm - 2:30pm</td>
<td>Visit the Exhibitors (Megabyte Sponsor Demo)</td>
<td>Meeting Room 6</td>
</tr>
<tr>
<td>2:30pm - 3:45pm</td>
<td>Threat Intel</td>
<td>Meeting Room 7</td>
</tr>
</tbody>
</table>

**Session Overview**

- **Human Element**
  - Human Element: AT1X 10:00am - 10:30am

- **Digital Maturity in the Government - The Legal Issues**
  - Digital Maturity in the Government - The Legal Issues: AT1X 10:30am - 11:30am

- **AGENDA DAY 2 – JUNE 9, 2016**
  - AGENDA DAY 2 – JUNE 9, 2016: AT1X 11:30am - 12:30pm

- **Lunch on your own and visit the Exhibitors**
  - Lunch on your own and visit the Exhibitors: AT1X 12:30pm - 1:30pm

- **Visit the Exhibitors (Megabyte Sponsor Demo)**
  - Visit the Exhibitors (Megabyte Sponsor Demo): AT1X 1:30pm - 2:30pm

- **Threat Intel**
  - Threat Intel: AT1X 2:30pm - 3:45pm
June 8, 2016

Dear Colleague:

On behalf of the New York State Office of Information Technology Services, the University at Albany, State University of New York, and The NYS Forum, Inc., we welcome you to the 19th Annual New York State Cyber Security Conference.

This year's conference theme is Focusing the Cyber Security Lens. Cyber threats continue to grow in sophistication, exploiting vulnerabilities to steal information and threaten essential services. This year’s conference focuses on industry best practices and standards that help organizations improve security, assure secure design and compliance, and create resiliency against cyber threats.

With over 50 dynamic breakout sessions to choose from, the conference brings you the latest material on information security trends and solutions. Industry experts will speak on such topics as risk management, security strategies, the threat landscape, cyber legal issues, incident response, and more.

We are pleased to welcome Tim Brown on Wednesday, June 8, morning’s keynote. Mr. Brown is a Dell Fellow and CTO of Dell Security. With a career that has taken him from meeting with members of Congress to the Situation Room in the White House, Mr. Brown will present an engaging keynote on how to adapt to today's security challenges while embracing new technologies.

Top researchers in academia will present their papers on information security at the 11th Annual Symposium on Information Assurance (ASIA), concurrent with the conference.

On Thursday, June 9, the day will begin with ASIA’s keynote speakers, Jason Healey, Senior Research Scholar at Columbia University and Senior Fellow of the Atlantic Council, and Michele Markoff, Deputy Coordinator for Cyber Issues at the U.S. Department of State. Mr. Healey's talk will explore how to make cyberspace more defensible. Ms. Markoff will describe how the United States is working internationally to promote greater stability in cyberspace.

An Exhibit Hall featuring displays from our sponsors and exhibitors will also be available on site both Wednesday and Thursday.

Thank you for your continued commitment to cyber security. Enjoy the Conference!

Sincerely,

Margaret Miller
NYS Chief Information Officer
NYS Office of Information Technology Services

Joan M. Sullivan
Executive Director
The NYS Forum, Inc.

Robert J. Jones
President
University at Albany
State University of New York
Margaret Miller
Chief Information Officer
NYS Office of Information Technology Services

Governor Andrew M. Cuomo appointed Margaret Miller Chief Information Officer of the New York State Office of Information Technology Services in December 2014. Ms. Miller is responsible for setting the statewide technology agenda to promote the efficient and effective delivery of services. She sets policy for all Executive branch agencies and oversees the provision of IT services to state agencies and local governments. Ms. Miller is successfully leading one of the largest and most complex state IT transformations ever undertaken, which includes the consolidation of more than 50 disparate and obsolete data centers into a single state-of-the-art facility and the development of strategic enterprise platforms for critical services.

With a proven record as an innovative business technology leader, Ms. Miller’s public and private sector experiences make her uniquely qualified to manage the State’s IT services and deliver solutions that foster a technology-enabled government to best serve New Yorkers.

Ms. Miller previously served as Senior Vice President and Group Chief Information Officer at Warner Music Group, a Fortune 500 company, where she oversaw the optimization of the company’s global IT systems and business processes for the digital media age.

Prior to her role at Warner Music Group, Ms. Miller held positions as Chief Information Officer at Dell Europe and for a retailer with $20 billion in revenue. She also has extensive experience as a Chief Information Officer in the financial services and travel sectors.

Joan M. Sullivan
Executive Director
The NYS Forum, Inc.

Ms. Sullivan has served as the Executive Director of the NYS Forum since November 2012 after serving over 37 years in New York State Government. Ms. Sullivan retired from government as the Executive Deputy Comptroller of Operations in the State Comptroller’s Office. Appointed to that position in May 2007, she was responsible for the oversight of the Division of Payroll, Accounting, and Revenue Services and the Division of Contracts and Expenditures. Most notably during this tenure as Executive Deputy Comptroller, she oversaw the implementation of the Statewide Financial System (SFS) as well as the design and implementation of OpenBookNY, the Comptroller’s premier transparency initiative.

From February 2004 through May 2007, Ms. Sullivan served as the Assistant Comptroller of the State Financial Services Group. She was responsible for managing five bureaus as well as the project to redesign the State’s Central Accounting System (the predecessor to SFS) and the Vendor Responsibility initiative and system implementation (VendRep).

Ms. Sullivan joined the Comptroller’s Office in January 2000 as Assistant Director of Contracts, and in September 2001 was appointed to Director of Contracts. Prior to joining OSC, she managed the Strategic Technology Assessment and Acquisition Team for the Office for Technology. Before this assignment, she spent 21 years with the former Department of Social Services, rising to the level of Director of the Office of Contract Management and later Director of Administration for the Human Services Application Service Center.

NEW! Visit the Charging Station in the Convention Hall
Sponsored by Trend Micro
Robert J. Jones, Ph.D. became the 19th president of the University at Albany in January 2013. He came to UAlbany following 34 years at the University of Minnesota, where he had most recently served as senior vice president for academic administration at the University of Minnesota System since 2004. Before that, Jones spent more than 15 years in key administrative leadership positions at the University of Minnesota-Twin Cities, including vice president and executive vice provost for faculty and academic programs, vice president for campus life and vice provost for faculty and academic personnel, interim vice president for student development and president of the University of Minnesota Outreach, Research and Education (UMore) Park Development, LLC.

A native of Dawson, Georgia, Jones earned a bachelor’s degree in agronomy from Fort Valley State College, a master of science degree in crop physiology from the University of Georgia, and a doctorate in crop physiology from the University of Missouri, Columbia. After earning the Ph.D., he joined the University of Minnesota faculty as a professor of agronomy and plant genetics. He is an internationally recognized authority on plant physiology and has published numerous scientific papers, manuscripts and abstracts. His research focused on the role of cytokinins in stabilizing grain yields of maize against environmental stresses and global climate change. During his career, he has trained many students who have gone on to leading careers in higher education and the private and not-for-profit sectors. He is a fellow of both the American Society of Agronomy and the Crop Science Society of America.

From the outset of his career, Jones has worked to advance international education. He has been a visiting professor and featured speaker in North America, Europe, Asia and Africa. From 1984 to 1994, he served as an academic and scientific consultant for Archbishop Desmond Tutu’s South African Education Program. In 2010, he was awarded a University of Minnesota endowed chair in urban and international development; he was also named a recipient of the Michael P. Malone International Leadership Award by the Association of Public and Land-Grant Universities (APLU).

Jones is nationally recognized for his work to advance university-community engagement, and at UAlbany, he is leading efforts to strengthen the University’s community partnerships. He currently serves as Regional Council Co-Chair for the Capital Region Economic Development Council (CREDC) alongside Albany Medical Center President James J. Barba. In 2013, he was appointed a co-chair for Albany Mayor-elect Sheehan’s transition committee. Other boards on which he serves include the Center for Economic Growth, Saratoga Performing Arts Center, Capitalize Albany and Albany Promise. At the national level, he serves on the boards of the Bush Foundation, the Coalition of Urban Serving Universities and the Scholars at Risk Network. He is a member of the Committee on Equal Opportunities in Science and Engineering, an advisory committee to the National Science Foundation. Jones is a member of several SUNY and UAlbany-affiliated boards, including the University at Albany University Council, The University at Albany Foundation, the University at Albany Biotech Development Corporation, the University Auxiliary Services Corporation, Empire Commons Student Housing, Inc., Fuller Road Management Corporation, the University at Albany Alumni Association, RF Research Council and Rockefeller Institute.

Prior to his arrival at UAlbany, Jones held a gubernatorial appointment as a commissioner of the Midwestern Higher Education Compact and served on the board of directors for the Midwest Universities Consortium for International Activities. He was also a member of the Grammy award-winning Sounds of Blackness, a Twin Cities-based choral ensemble.

Jones and his spouse, Lynn Hassan Jones, M.D., have five children.
Tim Brown
Dell Fellow and the CTO of Dell Security

Tim Brown is at the front line of the most vexing challenge facing organizations today: IT security. As a former CTO, chief architect, distinguished engineer and director of security strategy, Tim deeply understands the challenges and aspirations of the person responsible for driving digital innovation and change. Tim has over 20 years of development experience in security technology, including identity and access management, security compliance, threat research, vulnerability management, encryption, managed security services and cloud security.

As a Dell Fellow and the CTO of Dell Security, Tim is developing the future of IT security, and it’s a future that is addressing customers’ biggest challenges using a proactive, rather than a reactive, approach. His strong industry knowledge in finance, healthcare, education, manufacturing, retail and government enables Tim to provide relevant and actionable insights.

Nationally, his trusted advisor status has taken him from meeting with members of Congress and the Senate to the Situation Room in the White House. He has been on the board of the Open Identity Exchange and a member of the Trans Global Secure Collaboration Program driving advancements in identity frameworks and working with the US government on security initiatives. He is a member of the Advisory board for Clemson University and holds 20+ patents on security related topics.

Presentation:

Focusing the Cyber Security Lens

2016 finds us in the middle of a perfect storm. Technology is advancing at an incredible rate, the adversary is adapting and adjusting their business models and the cyber security professional is stretched to the limit. This presentation will focus on how to adapt to today’s challenges and say yes to embracing new technologies and new opportunities. It will provide actionable information and knowledge enabling you to focus on the most important assets, prioritize security efforts and prepare for the future.
Michele G. Markoff
Deputy Coordinator for Cyber Issues at the U.S. Department of State
Michele Markoff is Deputy Coordinator for Cyber Issues in the Office of the Coordinator for Cyber Affairs. Since 1998 Michele has been the senior State Department subject matter expert overseeing the development and implementation of foreign policy initiatives on cyberspace issues. She helps to coordinate United States policy on the spectrum of cyber-related policy issues across the Department, develops diplomatic strategies to encourage states to join the United States in taking steps to protect their critical networks and to cooperate internationally to enhance and preserve global cyber stability. She implements those strategies through negotiations in a wide variety of venues. Her initiative led to the successful completion of the first ever bilateral agreement on confidence-building in cyberspace between the United State and the Russian Federation, announced in June, 2013.

Michele also has been the United States Government Expert on three Groups of UN Government Experts (2005, 2010, and 2013) devoted to cyber issues. The last two led to landmark consensus reports regarding norms for state activity in cyberspace. Ms. Markoff was trained as an expert in Russian and Chinese military affairs and decision-making and spent the first half of her career in a variety of strategic nuclear arms control-related posts, among them as State Department Advisor and then Executive Secretary to the START I Talks; later as Senior Policy Advisor and Director of the U.S. Arms Control and Disarmament Agency’s Policy Planning Group.

Ms. Markoff has a B.A. in International Relations from Reed College, an M.A. in International Relations and an M.Phil in Political Science from Yale University, and a M.Sc. in National Security Strategy from the National War College of the United States. She also attended the Chinese University of Hong Kong.

Presentation:
Reducing Cyber Risk Through Diplomacy
We all have a part to play in making our networks more secure, but the global nature of cyber threats means that there is a unique role for diplomacy in reducing risk. Michele Markoff, Deputy Coordinator for Cyber Issues at the U.S. Department of State, will describe how the United States is working internationally to promote greater stability in cyberspace. Her talk will touch on efforts to build consensus among governments on principles of responsible state behavior in cyberspace, to develop practical confidence building measures to reduce the risk of conflict, and improve global cybersecurity.
**Insider Fraud in Financial Services**
Jason Clark, Carnegie Mellon University
11:00 a.m. – 11:50 a.m.
Meeting Room 2

The content described in this session is based on an insider threat study funded by the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) in collaboration with the U.S. Secret Service (USSS) and the CERT Insider Threat Center, part of Carnegie Mellon University's Software Engineering Institute. Researchers extracted technical and behavioral patterns from 67 insider and 13 external fraud cases; all 80 cases occurred between 2005 and the present. Using this information, we developed insights and risk indicators of malicious insider activity within the banking and finance sector. This information is intended to help private industry, government, and law enforcement more effectively prevent, deter, detect, investigate, and manage insider threats in this sector.

**CyberFinance: Why Cybersecurity Risk Analytics must Evolve to Survive 90% of Emerging Cyber Financial Threats, and, What You Can Do About It?**
Yogesh Malhotra, Global Risk Management Network, LLC
1:00 p.m. – 1:50 p.m.
Meeting Room 2

The primary focus of this presentation is on helping advance insights of 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 of cyber risk which is increasingly intertwined with financial risk. Using the metaphor of the iceberg with 90% of emerging cyber financial threats invisible to the human eye, it sheds light on emerging cyber risks that threaten the financial survival of national and regional economies, global and local business enterprises, information infrastructure entities, as well as individuals. Backed by research ranked for worldwide impact among finance and IT Nobel laureates, this presentation will help you see cyber risk and its implication for finance at various levels like you have never seen before. It advances upon industry-leading research that recently developed robust foundation of global Cyber Risk Insurance standards with oversight of cyber security experts affiliated with U.S. Air Force Research Lab and New York State Cyber Research Institute.

**Small Business Track**

**Consumer Tips for Staying Safe Online Part I: NCSA’s National Cybersecurity Awareness Campaign and Two Steps Ahead Demonstration**
Jill Heath, National Cyber Security Alliance
2:10 p.m. – 3:00 p.m.
Meeting Room 2

This session will introduce the National Cyber Security Alliance (NCSA), its mission, education initiatives and annual campaigns including National Cyber Awareness Month (NCAM). We will also focus on online safety via a Two Steps Ahead demonstration, and introduce proactive tools to secure confidential, personal, and proprietary information and data. In order to know how to secure data, it is vital to understand the potential risks that come with technology use, such as privacy concerns, identity theft, cyberbullying, and phishing scams. Police departments, other government entities, businesses, non-profits and consumers all can better secure online data and accounts by moving beyond reliance on simple passwords for protection. By combining a strong password with factors such as a fingerprint or a single-use code delivered in a text message, you can significantly strengthen data security. This focus on multifactor authentication is central to the National Cyber Security Alliance’s (NCSA) new National Cybersecurity Awareness Campaign, designed to give consumers simple and actionable information to protect themselves online in an increasingly digital world. We will offer resources you can use to implement security protocols in your department and reach out to community members to help protect them online.

**Re-energize with a beverage and snack!**
June 8
3:00 p.m. - 3:20 p.m.
Sponsored by Symantec
Consumer Tips for Staying Safe Online Part II: Scams and Identity Theft
Aiesha L. Battle and Melanie Grossman, NYS Division of Consumer Protection
Emma Fletcher, Council of Better Business Bureaus
3:20 p.m. – 4:15 p.m.
Meeting Room 2
As scammers become ever more sophisticated in infiltrating the online environment, the Better Business Bureau is using technology to help consumers fight back. A new tool on BBB’s national website at bbb.org enables consumers and businesses to report every type of scam activity from bogus IRS notices, to phishing scams and fake online lotteries. This session will demonstrate how BBB Scam Tracker collects and presents scam data in a “heat map” format showing consumers the number and types of scams and hoaxes reported in their communities. BBB uses this information to issue tips and alerts, warning consumers and businesses that they may be targeted, and to assist law enforcement in investigating scam activities.

Identity theft is one of the fastest growing crimes in the United States. Victimizing someone is easier than ever, with widespread information available on-line. With only a few pieces of valid personal information significant and devastating damage can be done. Data security breaches also compromise the privacy of personal identifiable information and increase the likelihood of identity theft. Consumers will be made aware of what steps to take should their information suffer a breach. This session will educate attendees on recognizing the signs of identity theft, how to avoid victimization, and discuss where to go for assistance in mitigating the damage caused by fraud.

Implementing an IT Risk Program using the NIST Cyber Security Framework
Bobby Dominguez, Lynx Technology Partners, Inc.
11:00 a.m. – 11:50 a.m.
Meeting Room 6
The NIST CyberSecurity Framework from 2013, based on existing standards, was created to reduce cyber risks to critical infrastructure. This session will describe the key elements of the NIST CSF, and will be of value to those who have deployed the CSF already and those who have yet to deploy. This discussion will focus on best practices for leveraging the CSF to implement an IT Risk Program. Specific examples for operationalizing the standard will be reviewed. Interaction with those that have not deployed the CSF will be encouraged.

Know Thy Cyber-Self: Understanding Your Network Before, During and After
John Stoner, Splunk Inc.
1:00 p.m. – 1:50 p.m.
Meeting Room 3
In recent years, government and commercial organizations have placed significant focus on establishing state-of-the-art, intelligent information networks to thwart ever-evolving security threats and attacks. It is no longer acceptable for cyber to be a reactive game, government and commercial agencies can’t afford to wait for the next attack to determine what security measures need to be put into place. The key to hunting and mitigating unknown threats is establishing a proactive defense—knowing your network inside and out to actively prevent security vulnerabilities and risks. In today’s threat landscape all data is security relevant, thus a new approach to understanding networks is required. It is imperative for government and commercial agencies to employ continuous, shared operational and situational awareness to fully comprehend their network infrastructure as there are different views for each user level. Ingestion of cyber intelligence from any source is necessary to anticipate at risk systems on a network and proactively defend them. IT security teams must also leverage analytics to discover critical systems on a given network to help visualize and monitor system components separate from the rest of the network. These efforts will further facilitate indications and warnings of an attack based on external data sources and internal signaling between security devices across the enterprise. Understanding data’s value is imperative to address challenges and determine valuable solutions that are necessary to achieve a stable security infrastructure. During this session, attendees will learn: different approaches to discovering opportunities for understanding your network infrastructure; the pros and cons of conventional use case driven approaches to IT management; current attack trends and what type of data is needed to tackle these trends; and operationalizing inherently biased viewpoints into situational awareness.

You Think You Are Secure, But Can You Pass a Compliance Audit or Data Breach Investigation?
Mike Semel and Rose Ketchum
Semel Consulting LLC
2:10 p.m. – 3:00 p.m.
Meeting Room 6
You know that you can invest a lot of money and resources in IT Security and Compliance, and still suffer a major data breach. You know that a lot of your data is regulated by HIPAA, financial regulations, or other data breach laws, which can prompt an audit at any time. It is hard to get your executives to fund the security tools you need, but it isn’t hard to imagine them blaming you for any breach or audit failure, is it? In fact, when we do data breach planning drills the first question from management is “How did our IT Department fail which caused this to happen???” Data breaches can become very public... very fast. They can cost millions of dollars-- even for smaller organizations-- in fines, penalties, notifications, lawsuits, legal fees,
and reputation management costs. Many breaches result in the firing of IT staff, and larger breaches have also cost the jobs of senior executives. In the public sector you will undoubtedly face the scrutiny of the media and elected officials. Mike Semel, a former school district and hospital Chief Information Officer, will go through case studies and examples of audits and data breaches, and discuss the lessons you can learn to prevent becoming a case study yourself. He will show you results of audits including what the IT managers said they were doing, and what the audits found they were really doing. This presentation will help you understand what you must do to be ready for an audit or breach investigation, because once an audit or investigation letter arrives you won’t have a lot of time to get things together or start creating documentation that didn’t already exist. You will also learn how to communicate with non-technical decision-makers, to help get the budget and resources you need.

Measuring Security: How Do I Know What a Valid Metric Looks Like?
Ben Smith, RSA, The Security Division of EMC
3:20 p.m. – 4:15 p.m.
Meeting Room 3

There is no universally accepted method to measure security. So how do we translate operational measurements into meaningful security metrics for the business? Doing so effectively is essential, because you can’t manage what you don’t measure. This session will touch on the following general questions: Why are security metrics important, from both a compliance and an operational perspective? What are some best practices to keep in mind when selecting security metrics? Does your audience(s) dictate which metrics to select? What behaviors are you trying to influence with these metrics? What are some unexpected sources of security metrics? How should you communicate those metrics internally within your organization for maximum impact? Are there any examples of poor metrics which should be avoided in most cases?

Privacy Track

Eat, Sleep, Surveillance, Repeat
Raj Goel, Brainlink
11:00 a.m. – 11:50 a.m.
Meeting Room 3

Disney, Google, Facebook, Baidu, Verizon, GM, Tesla, Apple, Netflix, GE, Samsung - every corporation and vendor is in an escalating surveillance arms race. The new business model seems to be “build a widget, embed surveillance; pray you make money on monetizing data.” This presentation demonstrates how corporate surveillance has penetrated every room in the home, office, car and subway platform.

Hell is Empty and All the Devils are Here
Reg Harnish, GreyCastle Security
1:00 p.m. – 1:50 p.m.
Meeting Room 6

The right to privacy has become the corollary to the assurances of security - both counter-intuitive in the information age and ironic in their implementations. Security does not necessarily help nor hinder privacy, and privacy cares as much about security as it does about bowling. They are not often interconnected, and even when they are they oscillate independently. Agree or disagree, because it doesn’t matter anyway. Privacy has become a currency - the only one accepted at Internet endpoints all over the world. It’s a pay to play world, and while we reluctantly eat the cookies of our Internet favorites, we collectively decide that a diet of digital abstinence tastes far worse. Our data collectors lack transparency, and we’re OK with that. We donate our deepest, darkest secrets to Google search histories while posting our rants about privacy rights on Facebook. The system is broken and that’s just how we like it. Join GreyCastle Security as we explore the ironies of privacy and security in a digital world.

Digital Intel Track

Extracting Novel Information from Digital Data
Robert Dora, Assured Information Security, Inc.
2:10 p.m. – 3:00 p.m.
Meeting Room 3

AIS has developed a variety of continuous monitoring solutions, including Remote Suspect Identification for the AFRL that authenticated users at login and continuously verified them afterwards using keystroke dynamics with accuracy upwards of 95%. AIS has developed more comprehensive continuous monitoring solutions that include mouse data, application usage, menu clicks, and gaze tracking. Many of these collectors have open-source options, are unobtrusive, and do not require additional hardware. As a result, these collectors can be relatively easy to incorporate in a variety of environments. This data, however, provides far more value than simply verifying a user; it can be used to measure cognitive states, demographic features, personality traits, and many other things. As part of the Air Force Office of Scientific Research (AFOSR) Basic Research Initiative, AIS identified a statistically significant negative correlation between suspicion and keystroke interval times - the timing between key presses. More research is forthcoming, but the ability to measure simple cognitive states (e.g., cognitive workload) using keystrokes and other complementary sensors seems feasible. With more research, such technology could provide significant advances to insider threat detection, operator scheduling, and many other areas. This data can provide more information than just cognitive states - under another AFOSR effort, AIS developed predictive models to use keystroke data to identify demographic features ranging from ethnicity to handedness. Consider an outside attacker that breaks into a network - their keystrokes can be collected with a
intrusion investigations. In place to support future nation-state house technical talent should you have what capabilities, software tools, and in-cyber incident responders on day one and expect (and not expect) from government to nation-state intrusions. What can you DHS to NSA and DoD, track and respond of how the U.S. Government, from FBI and techniques to order to explore the reality across the spectrum of actor sets and talk, let us revisit some of these intrusions exploitation tradecraft. In an unclassified still goes to Russia for superior cyber Sony; though the ‘best-in-show’ award who is worthy of an honorable mention for the noise. And let us not forget North Korea and so pervasive that even cyber criminals China, the ‘silent intruder’, is now so noisy to large-scale DDoS and data destruction. Finally, social networking data could rapidly identify them for future and in sophistication. Iran, once known simply for web defacements, has moved to large-scale DDoS and data destruction. In the last five years, we have watched computer intrusions grow both in numbers and in sophistication. Iran, once known simply for web defacements, has moved to large-scale DDoS and data destruction. China, the ‘silent intruder’, is now so noisy and so pervasive that even cyber criminals repurpose Chinese malware to hide among the noise. And let us not forget North Korea who is worthy of an honorable mention for Sony; though the ‘best-in-show’ award still goes to Russia for superior cyber exploitation tradecraft. In an unclassified talk, let us revisit some of these intrusions across the spectrum of actor sets and techniques to order to explore the reality of how the U.S. Government, from FBI and DHS to NSA and DoD, track and respond to nation-state intrusions. What can you expect (and not expect) from government cyber incident responders on day one and what capabilities, software tools, and in-house technical talent should you have in place to support future nation-state intrusion investigations.

From 2010 to 2015: Lessons Learned and the Future of Government-Initiated Cyber Incident Response
Christopher Hallenbeck and Andre McGregor, Tanium Inc
3:20 p.m. – 4:15 p.m.
Meeting Room 6
In the last five years, we have watched computer intrusions grow both in numbers and in sophistication. Iran, once known simply for web defacements, has moved to large-scale DDoS and data destruction. China, the ‘silent intruder’, is now so noisy and so pervasive that even cyber criminals repurpose Chinese malware to hide among the noise. And let us not forget North Korea who is worthy of an honorable mention for Sony; though the ‘best-in-show’ award still goes to Russia for superior cyber exploitation tradecraft. In an unclassified talk, let us revisit some of these intrusions across the spectrum of actor sets and techniques to order to explore the reality of how the U.S. Government, from FBI and DHS to NSA and DoD, track and respond to nation-state intrusions. What can you expect (and not expect) from government cyber incident responders on day one and what capabilities, software tools, and in-house technical talent should you have in place to support future nation-state intrusion investigations.

Access and Authentication Track
Reducing BYOD Risk Using Advanced Threat Detection - A Case Study
Eric Green, Mobile Active Defense
Kirsten Bay, Cyber adAPT
11:00 a.m. – 11:50 a.m.
Meeting Room 4
By definition BYOD is high risk - 85% of devices are out of the control of the enterprise. Traditional means to secure that environment have failed either due to vendors pushing workstation type solutions to mobile devices or privacy concerns of the user base, among other things. Yet other mobile security solutions change the desired user experience of mobile devices causing a list of other issues, not the least of which include users finding a way around such solutions. Enter a philosophy of how threat detection in fact can see bad behavior and remediate, all the while not changing the user experience. It’s all well and fine in theory and philosophy but how is it used in practice.

Upcoming Trends for Authentication Mechanisms
Karl Muenzinger, JANUS Associates
1:00 p.m. – 1:50 p.m.
Meeting Room 4
As we all know, password management is an arduous task which consumes a large portion of our time. Likewise, granting, revoking and auditing access control systems is a lengthy and drawn out procedure. However, new technologies are working their way into the mainstream which are aimed at simplifying security control management, reducing the cost of implementing security controls and fulfilling requirements of regulatory standards. This discussion will describe some of the emerging trends and technologies in identity management, authentication, authorization and access control which will affect the way consumers and organizations in every sector protect their identities and their data.

Best Practices Track
Intelligent Devices vs. Secure Life
The NYS Forum Information Security Workgroup
2:10 p.m. – 3:00 p.m.
Meeting Room 4
Cyber physical systems will dominate the landscape of technological advancements in the next two decades with the Smart Grid, connected vehicles, and implantable medical devices leading the way. Each of these innovations will fundamentally alter our lifestyles as much as or even more than the Internet has done in the last two decades. Smart Grid technologies will provide visibility into the power grid that will allow incorporation of micro-energy sources (including renewables) seamlessly and at the same time improve efficiency and resilience of the grid. Connected vehicle technology will lead to the creation of millions of ad hoc networks in the road transportation network, leading to collision avoidance systems being deployed, improvement of traffic flow, and ultimately leading to self-driving vehicles. Finally, implantable medical devices will enhance quality of living for millions of people by allowing precise control of medication and other interventions to correct medical issues. While all of these advancements are fascinating, these technologies rely extensively on communication technologies which are subject to cyber threats just like we have on the Internet but with much more grave consequences to the health and life of humans. In this session, we discuss the security challenges across cyber physical systems in general, and specifically in the areas of the Smart Grid, Connected Vehicles, and Implantable Medical Devices.
orchestration methodologies. Traditionally, technologies coupled with novel service augmentation of layered virtualization service (SaaS) have evolved through as a service (PaaS), and System as a Infrastructure as a service (IaaS), Platform of traditional Cloud services such as networked services. The underpinnings associated with securing and managing to the standard administration tasks services has added significant challenges devices to large scale Cloud-orchestrated (IoT), ranging from mobile embedded recent explosion of the Internet of Things becoming increasingly more complex. Modern networked computing systems are Meeting Room 5

Network Security – Threat Update and Best Practices Michael Singer, AT&T 3:20 p.m. – 4:15 p.m. Meeting Room 4

Michael Singer will share highlights from his work in network security starting in 2002. This will include security data visualizations, trend charts and examples. Michael will also cover security best practices to consider.

Data Protection Track

Next Generation Cloud-Enabled Architectures Michael Corley and Sean Bird, Quanterion Solutions Inc. 11:00 a.m. – 11:50 a.m. Meeting Room 5

Modern networked computing systems are becoming increasingly more complex. The recent explosion of the Internet of Things (IoT), ranging from mobile embedded devices to large scale Cloud-orchestrated services has added significant challenges to the standard administration tasks associated with securing and managing networked services. The underpinnings of traditional Cloud services such as Infrastructure as a service (IaaS), Platform as a service (PaaS), and System as a service (SaaS) have evolved through augmentation of layered virtualization technologies coupled with novel service orchestration methodologies. Traditionally, type-1 hypervisor solutions have existed at the heart of IaaS. Docker is a fairly new and widely adopted application management platform that works with underlying Linux Containers (LXC) available in a contemporary kernel to aid productivity of tasks associated with software development, and application distribution and deployment. Unikernels are a novel technology that enable specialized single address space machine images in which services are built from a modular stack of libraries necessary for the service to run. A unikernel-based service consists of the minimalist set of libraries compiled together with the application code to produce sealed, fixed-purposes service images which can run without an intervening host operating system, directly on hardware, on a hypervisor, and from within a Docker container image. In this presentation we will provide a brief background, and the evolution of the core architectural components present in current and next generation Cloud enabled services. We will consider the challenges associated with management functions, including the benefits and consequences of unikernel-based services relative to security, general administration, and service deployment.

Cloud Security: What you need to know Manny Morales, Independent Consultant 1:00 p.m. – 1:50 p.m. Meeting Room 5

Going to the Cloud for a business entity is no longer a far-fetched idea but a reality. The Cloud has now become the norm for businesses to run their operations and save money. However, the Cloud comes with challenges, security and privacy being the issues. Security professionals can no longer say ‘No’, but need to embrace what the business wants to do and why they want to go to the Cloud. In this session, the speaker will present what the security and privacy concerns are, how they can be addressed, what the legal implications are, what needs to be in a Cloud contract, what and where to audit, and what the future holds for doing business in the Cloud.

Vendor Risk: The Back Door You Can't Leave Unlocked Keith Robertson, GreyCastle Security 2:10 p.m. – 2:50 p.m. Meeting Room 5

As we’ve seen time and time again, cybercriminals take the path of least resistance. Based on recent high profile breaches, hackers have learned that contractors and other third-party providers can provide an opening into otherwise-secured corporate networks. You’ve spent time, money and energy securing your organization internally, only to have the back door wide open. How can you extend your internal security controls to your vendors and help reduce your organization’s risk? Join GreyCastle Security for an in-depth look into vendor risk management. Learn what’s working, what’s not, and how your organization can better manage one of the most challenging security issues facing organizations today.

Leveraging the Federal Risk and Authorization Management Program (FedRAMP) for State Implementation Abel Sussman, Coalfire 3:20 p.m. – 4:15 p.m. Meeting Room 5

The Federal Government’s “Cloud First” policy mandates that agencies take full advantage of cloud computing benefits to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize cost. The Federal Risk and Authorization Management Program (FedRAMP) is a mandatory government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. There are many advantages for state and local government in adopting parts of the FedRAMP program to meet their IT and security needs. An overview of FedRAMP, and security controls will be provided with real-world examples and recommendations.

Please remember to complete the Conference survey at https://www.surveymonkey.com/r/NYScyber16
As society has become increasingly transformed through Internet-based communication and data exchange, cyber threats have increased in both sophistication and frequency. In many agencies and organizations, executives know that cyber incidents can lead to high-profile losses; rampant media exposure; and damage to client, customer, or investor confidence. State and business leaders have begun to acknowledge that, despite strong security controls, cyber incidents will occur. How heavily they impact an organization's reputation, bottom line, and market standing depends, in part, on how well-prepared the organization is to analyze and contain an incident as it unfolds, respond decisively, and manage the aftermath. Cyber threat war-gaming services help government agencies and organizations establish “muscle memory” and multi-function coordination to better manage the business crises that cyber incidents can cause. Deloitte will be facilitating a “role-playing” cyber war gaming exercise where attendees participate in a simulated cyber breach and interact to manage the risk and response efforts.
Thursday, June 9, 2016 – Day Two Sessions

Health Sector Track

A New Shared-Services Model for Cybersecurity in the Healthcare Industry
John Bay and Kathaleene Riolo, Cyber Research Institute
10:30 a.m. – 11:20 a.m.
Meeting Room 1

With Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), and emerging information sharing arrangements as encouraged by the recently-enacted Cyber Information Sharing Act (CISA), shared information analysis is becoming a standard model for threat intelligence. While all of these organizations recognize the inherent value of shared network and security information, they each provide a different set of services to their members. Some organizations are sector-specific, and some are regional. This session will present a model of an information sharing and services consortium that goes beyond threat intelligence and intrusion detection, to offer specific services and analysis, and includes a research component and technology transfer from publicly-funded programs. The concept, which we call dataRAMPART is cross-sector, but provides for communities of interest to focus on sector-specific needs and requirements. It includes a multi-level suite of services that can be tailored to organizations of any size. The CRI is now launching a pilot program to demonstrate the effectiveness of dataRAMPART in the healthcare sector. It has been determined that healthcare records are among the most valuable to hackers and damaging to the owners. In this session we will describe this pilot program and discuss how it can be extended beyond healthcare, to finance, transportation, and other industries. We will also discuss the importance of this and other shared-information security models in the emerging legal and regulatory environment.

Medicaid Modernization – Data Integration Meets Security Challenges
NYSDOH & Partners – Panel Discussion
Anton Venter and Logan Tierney, New York State Department of Health; Anthony DiVirgilio, New York Medicaid Management Information System; Joel Ryba, XchangeWorx, Inc.; Slawomir Marcinkowski and Robert Zeglen, NYSTEC
11:40 a.m. – 12:30 p.m.
Meeting Room 1

The use of big data, specifically Medicaid claims data, lies at the foundation of New York State Department of Health (NYSDOH) Medicaid modernization and cost reductions efforts. The NYSDOH Medicaid Management Information System (NYMMIS) program will intake the data and provide the New York State Medicaid Program with enhanced flexibility, interoperability, and data sharing capabilities, resulting in improved claims adjudication, fiscal management, and fraud and abuse deterrents.

The NYSDOH Delivery System Reform Incentive Payment (DSRIP) Program will use the data and is the main mechanism by which New York State will fundamentally restructure the health care delivery system by reinvesting in the Medicaid program, with the primary goal of reducing avoidable hospital use by 25% over 5 years. Within this program, 25 different entities called Performing Provider Systems (PPS) receive Medicaid data from NYS on over 5 million Medicaid members in order to implement and oversee their population health projects. One PPS can have upwards of 550,000 attributed members to receive PHI for. The PPSs work closely with their regional health information organizations (RHIO). The Statewide Health Information Network for New York (SHIN-NY) will support access to claims data for their Participants which includes PPSs. NYSDOH seeks to build a 360-degree view of a Medicaid patient by integrating claims data with clinical data made available through the SHIN-NY.

Data security is critical for success of the NYSDOH NYMMIS and DSRIP initiatives. NYSDOH teams have taken an innovative approach to build security in early, that leverages education and outreach. By working with vendor and provider communities early on, risks associated with the processing and sharing of very large volumes of Medicaid data can be more effectively mitigated. Both projects are utilizing a Center for Medicaid Services (CMS) Minimal Acceptable Risks Standard (MARS) and NIST 800-53 based framework to build upon and track progress through measurable criteria. DOH has mapped MARS to NYS Policies and Standards and call it MARS Plus.

This session will include a brief overview of the NYSDOH approach in each program and will be followed by a panel discussion with representatives from DOH, NYSTEC as well as the provider and vendor communities. The panel discussion will address challenges and solutions being incorporated.

Government Track

Cyber Threat Landscape: What can you do to mitigate the risks?
Andrew Dolan, Multi-State Information Sharing and Analysis Center
1:40 p.m. – 2:30 p.m.
Meeting Room 6

Cybersecurity is quickly becoming a top concern for every sector in our country. The worldwide reach of the internet means that cyber threats can come from hackers in the United States and from foreign counties. In this session, the heads of Stakeholder Engagement for both the Multi-State Information Sharing and Analysis Center and the US Department of Homeland Security: Office of Cybersecurity and Communications will speak about the emerging cyber threats to the government sector and what steps they can take to minimize the risk and mitigate these threats.
Cyber Initiatives in New York State
Peter Bloniarz, New York State Cyber Security Advisory Board
2:50 p.m. – 3:45 p.m.
Meeting Room 6
As New York continues its aggressive cyber agenda, come hear the details as to the various initiatives under way and planned.

Legal Track

Government Use of Social Media: The Legal Issues
David Menken, Smith Buss & Jacobs LLP
10:30 a.m. – 11:20 a.m.
Meeting Room 6
The session will discuss issues facing local government use of social media such as Facebook, Twitter, Linkedin, and Instagram. The session will quickly identify the many benefits of using social media in government, including improved transparency, increased collaboration, enhanced citizen participation, and improved efficiency. The session will then identify two important issues relating to government use of social media: (1) the extent to which government can regulate free speech via social media by public citizens and government employees, and (2) compliance by government entities with legal requirements which were developed in a paper-based environment. The presentation will review the application of the First Amendment to local government and limitations on speech in the public forum by the public and governmental employees. It will also review evolving laws relating to government involvement with social media, specifically the Freedom of Information Act, the Open Meetings Law, Record Retention Laws and the NYS Personal Privacy Protection Law. Finally, the session will propose a range of social media policies which might be appropriate for a local government entity to adopt in order to minimize liability, maximize safe participation, and comply with good government laws.

Malware/Threat Intel Track

Adventures in Obfuscation: Unraveling the Code
James Antonakos, Trustwave
1:40 p.m. – 2:30 p.m.
Meeting Room 1
In this session, James will present examples of obfuscated JavaScript and Visual Basic code, and discuss techniques to de-mystify and decode the meaning of the malicious code and its purpose. The knowledge and skills required to deobfuscate code and determine its functionality are explained. Ways to detect obfuscated threats are also discussed.

Threat Intel
Scott Sattler
2:50 p.m. – 3:45 p.m.
Meeting Room 1
This session covers sourcing, collecting and processing Threat Intelligence which is used in Cyber Defense Organizations to detect and prevent threat actors from compromising enterprise systems. The rapid change of tactics and tools utilized by Threat Actors makes their digital fingerprint an invaluable piece of the puzzle in solving this complex problem.

Encryption: the Good, the Bad, the Ugly
Steve Treglia, Absolute Software Corporation
11:40 a.m. – 12:30 p.m.
Meeting Room 6
Even in 2016, despite all the highly-publicized massive personal data security breaches and equally massive monetary penalties for such breaches, many professionals still associate the word “bad” with “encryption.” Encryption slows computer performance, it takes time to install and employ, it confuses users and even some IT staff, or worse yet, and some organizations do not employ sufficiently qualified staff to deploy it properly.

And yet, operating computer systems without using encryption is getting uglier by the minute. The regulatory world, in its various forms (e.g., HIPAA, PCI, NY breach notification laws), are making encryption more of a required standard. Ethical rules requiring lawyers to encrypt their clients’ data appear to be right around the corner, if not already mandatory. On the other hand, many entities utilizing encryption these days improperly assume the mantra, “Once I encrypt, I’m safe.” This presentation touches on the evolution of modern encryption methodology, as well as analyzes the development of legal and regulatory requirements mandating the use of such technology. It also predicts the near future of personal data storage and transfers and the increasing role encryption will play for both the private and public sector.
Cyber Workforce Development: Lessons Learned and Ways Forward
Fernando Maymi, The Army Cyber Institute at West Point
1:40 p.m. – 2:30 p.m.
Meeting Room 2

While the ranks of threat actors are swelling at home and abroad, our nation struggles to find qualified professionals with which to defend itself in cyberspace. The need for talent is equally dire in government, corporations and academia, and there are no signs indicating that this is changing anytime soon. What is needed is a whole-of-nation approach to identifying, inspiring and developing individuals who have what it takes (whether or not they know it) to defend our information systems. This talk begins with a “State of the Cyber Nation” report, focusing on both human assets and threat sources. This leads to a discussion on various approaches to developing the cyber workforce in both government and industry, and the role that our academic institutions play in this process. The successes and challenges of the Army’s Cyber Branch present an interesting case study. The talk then delves into the gaps and opportunities that must be considered in searching for actionable solutions to our cyber workforce challenges. Finally, specific actions are recommended for organizations ranging from small to large that benefit both those who take them and the community at large.

Cybersecurity White Belt: Foundational Knowledge for Cyber Self-Defense
Todd Brasel and Bruce Barnett, NYSTEC
2:50 p.m. – 3:45 p.m.
Meeting Room 2

Do you hear about security breaches and cyber attacks, but don’t really understand who carries out the attacks, or their motivations? Are you confused about how to best to protect yourself from cybercrime? In this presentation, you’ll gain foundational knowledge that you can apply right away to your personal online activities. You’ll learn about what makes your online presence interesting to cyber attackers, how attacks are planned and carried out, and what attackers do after they’ve gained access to your accounts. Basic strategy and techniques to protect yourself against cybercrime, including mobile device usage, will also be discussed. By following real-life examples and industry-standard practices, you’ll raise your awareness of how and why cyber attacks are committed; learn how to protect yourself and your children online; discover sources of free information to learn more about cybersecurity; and learn about no-cost or low-cost tools and techniques to improve security.

The 2016 NYS Cyber Security Conference would like to thank all of our sponsors, exhibitors, speakers, volunteers, and attendees for making this another successful year!
Methods of Network Segmentation – Pro’s and Con’s
Ken Kaminski, Cisco Systems
11:40 a.m. – 12:30 p.m.
Meeting Room 3
Network segmentation discussions and resulting orders to implement have become board level discussions in many enterprises due to the expanding number, increasing sophistication, and severity of security breaches. The Internet of Things continues to expand and with it a need to segment and isolate these devices. This session will discuss the various ways to segment a network using both static configuration and dynamic classification of endpoints using various identity authentication and authorization technologies. We will discuss using access control lists, VLANs, stateful firewalls, routing VRFs, and some more advanced methods such as Cisco TrustSec. Each will be examined with their pros and cons including their impact on network and security operations teams. The need for visibility and the ability to measure and ensure the various methods are functioning will be examined along with tools to accomplish this auditing requirement. This talk focuses on the enterprise network for end users and devices, and not the data center.

Hide and Seek, where are you? What’s your Incident Response Recipe?
Renault Ross, Symantec
1:40 p.m. – 2:30 p.m.
Meeting Room 3
Public and private sector organizations are struggling with where and how to start building their Incident Response Strategy. Since breaches are inevitable, the industry is focusing on containment and quicker restoration of business services post breach. This session will help government leaders to understand the building blocks of an effective Incident Response Strategy and provide best practices used by other successful organizations to mitigate security risk.

Fighting Targeted Attacks: Tools and Tactics
Leonard Popyack and Cynthia Gonnella, Utica College
2:50 p.m. – 3:45 p.m.
Meeting Room 3
Every organization is a potential target for cyber attacks which can result in compromise, data theft, monetary losses, customer churn, and embarrassment. Large organization will have a malware analysis shop set-up specifically to look for targeted attacks against their organization. It is an expensive but necessary undertaking today. In this talk, we present some methods and tools that can be constructed and implemented for relatively low cost in which smaller organizations can take significant positive action. Many of the tools are free or low cost. Targeted attacks are distinctly different than mass malware. You or your organization can be targeted by highly sophisticated malicious actors or insiders which may likely result in some form of intrusions and data exfiltration of your computer systems or your network without being detected. Normal anti-virus is ineffective in these cases. External attacks and insiders alike are a risk for any organization. Our talk will take you through some of the necessary tools, techniques, and procedures you can employ to combat these very real threats. We will demonstrate malware detection and analysis using tools and techniques that you can put to use without large investments, immediately after attending the presentation.

Internet of Things Track
Are Converged IT/OT Transportation Networks Immune From Attack?
Anthony Concolino and Russell Kiernan, QEDNational
Ken Garmson, Arup
10:30 a.m. – 11:20 a.m.
Meeting Room 4
Transportation systems, especially rail, were traditionally immune from cyber-attack as their networks and equipment were isolated from the outside world. With convergence of operational and corporate IT networks, the question must be asked – “how immune is the transportation network from attack?” This session will include: an overview of the transportation sector IT network topology - Transport for London view; the evolution of SCADA systems, the convergence of IT and OT networks, and the introduction of new, critical risks; current trends - Increased complexity and connectivity of systems (i.e., “Smart Ticketing”, “Computer Based Signaling”, passenger Information Systems); and discuss development of a comprehensive, risk-based approach and enhanced set of controls. Currently, security of OT networks is not a perceived risk and, as an informed audience, we should be helping the transportation sector tackle this issue. Transportation systems designers (SCADA systems, converged networks, etc.) need to understand emerging cyber risks and implement appropriate controls. Policy alone is not the solution. A comprehensive, risk-based approach and enhanced set of controls is required.

Session Tracks & Session Descriptions
Join us for a Continental Breakfast each morning in the Exhibit Hall!
June 8 breakfast sponsored by Cisco Systems
June 9 breakfast sponsored by Hewlett Packard Enterprise
Incorporating the Internet of Things (IoT) in your Strategy  
Michael Corby, CGI, Inc.  
11:40 a.m. – 12:30 p.m.  
Meeting Room 4  
The advances in providing Internet connectivity to non-traditional devices poses a challenge to all security programs. Breaches of security have already occurred when a non-traditional device introduces a vulnerability to a previously secured environment. How can a security program be updated to accommodate connected devices including medical equipment, building environment controls, light bulbs, doorbells, automobiles and just about everything? This session will present some process recommendations that address the incorporation of these advances in a security strategy.

How the Internet of Things is Redefining Data Privacy, Safety, Governance and Trust  
Bruce Snell, Intel Security  
1:40 p.m. – 2:30 p.m.  
Meeting Room 4  
With the rise of the Internet of Things (IoT) comes a new data ecosystem that needs to be protected with a well-defined, industry-wide strategy so that trust, data privacy, safety and governance are not lost. The adoption of wearable devices as part of the IoT trend means that consumers’ personal health and daily activities are tracked, stored and shared in more ways than ever before. The protection of this new ecosystem is imperative and will define the success or failure of the entire networked device industry as security vulnerabilities, privacy concerns and regulation issues surface. Tying security to the Internet of Things is imperative to safely unleashing the transformative power of a world in which every device is connected.

Trains, Planes, and Automobiles - Reducing Cybersecurity Risks  
Leonard Jacobs, Netsecuris Inc.  
2:50 p.m. – 3:45 p.m.  
Meeting Room 4  
There have been some significant disclosures of cyber risk involving real-time items of “motion” lately. The presenter will provide an overview of cyber risk and decipher for the audience the true extent and impact of cyber risks to items of “motion” and other industrial control systems. The presenter proposes that trains, planes, and automobiles fall into the category of industrial control systems. The presenter will provide potential solutions for reducing cyber risks utilizing network security monitoring techniques.

Threat Landscape Track

2016 Data Breach Investigations Report  
Christopher Novak, Verizon Enterprise Solutions  
10:30 a.m. – 11:20 a.m.  
Meeting Room 5  
In today’s complex threat landscape, how can you prioritize your security efforts? The Verizon Data Breach Investigations Report shows you the top threats affecting different industries, based on an analysis of nearly 80,000 security incidents, including more than 2,100 confirmed breaches.

Check Before You Wreck: Operationalizing the Verizon Data Breach Investigation Report (DBIR)  
Joan Ross, Verizon Enterprise Solutions  
11:40 a.m. – 12:30 p.m.  
Meeting Room 5  
Over the past eleven years, qualitative and quantitative breach investigation research and analysis yields ongoing and significant cyber security breach trends. The Verizon DBIR details nine major threat categories that continue to be responsible for 97% of documented exploits, and the additional factors that are negatively impacting globally connected business. In September, Verizon was awarded the Frost & Sullivan 2015 New Product Innovation Award for the Verizon DBIR App for Splunk. The tool takes the guess work out of cyber threats by harnessing the rich historical breach intelligence gathered by Verizon’s data breach investigations team over the past decade and making it actionable with Splunk security analytics software. We’ll examine how to use this easily downloadable tool that is designed to better enable enterprises to benchmark and prioritize their security and information technology tools to navigate and get ahead of an increasingly sophisticated cyber threat landscape. Additionally, we’ll present a customized installation with a leading organization CISO on how the Verizon DBIR app was tailored and customized to achieve: A CISO visual display dashboard for correlation of security activities; real-time analysis of integrated tool monitoring and reporting; determination of tools rationalization for achieving accurate security information and metrics; optimized security strategy capabilities; and security budget validations and refinement.

View the Conference agenda and your schedule with the Conference Mobile Event Guide: https://www.regonline.com/register/m/?eventid=1797068
Hey I know You! A Penetration Tester’s year in review
Tyler Wrightson, LeetSystems
1:40 p.m. – 2:30 p.m.
Meeting Room 5
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. Attack vectors include intrusions via external, internal, social engineering, physical, and more.

The Latest Cybersecurity Threats and a Framework to Deal with them
Peter Romness, Cisco
2:50 p.m. – 3:45 p.m.
Meeting Room 5
We all are expecting more from our information technology systems including new means of access like social media, mobile apps, cloud computing and the Internet of Things. At the same time, threats to organizations are increasingly sophisticated, better organized and more frequent. This discussion takes a look at some of the recent incidents and recent trends in the industry while suggesting a framework, using the latest technologies to protect ourselves “Before, During, and After” an attack.

Annual Symposium
Thursday, June 9, 2016
Meeting Room 7
SYMPOSIUM SESSION 5: Terrorism
Chair: Sanjay Goel, University at Albany, SUNY
Paper: Towards Cognitive Immunization of Potential Criminals against Cyberterrorism
Merrill Warkentin and Ali Vedadi, Mississippi State University, Joshua M Regan, University of New Haven, Amin G Kosseim, New York City Police Department, Carl J. Jensen, Society of Police Futurists International
Paper: Ranking Terrorist Nodes of 26/11 Mumbai Attack using Analytical Hierarchy Process with Social Network Analysis
Pankaj Choudhary, Upasna Singh, Defence Institute of Advanced Technology

SYMPOSIUM SESSION 6: Multimedia Forensics
Chair: Fabio Auffant, University at Albany, SUNY
Paper: Forensic Linguistic Applications to Social Engineering: Illustration of Language Features of IRS Phone Scam Calls
Judith Tabron, Hofstra University
Paper: Facebook Forensics for Windows 10
Pankaj Choudhary, Upasna Singh, Nitesh Bharadwaj, Bhupendra Singh, Defence Institute of Advanced Technology

SYMPOSIUM SESSION 7: Web Security
Chair: Pradeep Atrey, University at Albany, SUNY
Paper: Covert Channel in HTTP User Agents
Susan Heilman, Daryl Johnson, Jonathan Williams, Rochester Institute of Technology
Paper: Don’t See me, Just Edit Me: Towards Secure Cloud-based Video Editing
Odd-Arild Kristensen, University at Albany, Manoranjan Mhanty, New York University Abu Dhabi, Pradeep Atrey, University at Albany

SYMPOSIUM SESSION 8: Security Legislation and Privacy
Chair: Victoria Kisekka, University at Albany, SUNY
Paper: Cybersecurity Benefits of Executive Order 13,694
William Augustine, University at Albany
Talk: Privacy Preserving Driving Style Recognition Against Semi-honest and Malicious Adversaries
Ethan Sprissler, Nicholas Rizzo, Yuan Hong, Sanjay Goel, University at Albany

Continuing Legal Education (CLEs) credits are sponsored by the Albany County Bar Association for the following June 9 sessions:
- Government use of Social Media – The Legal Issues
- Encryption: The Good, The Bad, The Ugly
When managing security in an all-IP network, it helps to see the big picture.

AT&T security experts analyze more than 310 billion flow records each day for anomalies that indicate malicious activity. It's what makes us uniquely qualified to help state and local government agencies address the security challenges they face. Our proactive network-based approach to managed security delivers some of today's most powerful weapons to combat cyber security attacks – helping to safeguard all the elements of your IP infrastructure. To learn more, download the CIO Security Guide at att.com/govsecurity

©2016 AT&T Intellectual Property. All rights reserved. All other marks used herein are the property of their respective owners.
Application Security Solutions for your Enterprise!

A trusted Platinum Partner, Melillo has been delivering HPE Infrastructure, Applications & Professional Services Solutions for over 28 years!
Security Everywhere

Threat-Centric Security
cisco.com/go/security
Enduring Values. Inspired Performance.

Every day CSRA makes a difference in how the government serves our country and our citizens. This year, CSRA’s New York Health and Human Services team celebrates our 30-year legacy of working closely with our State and Local government partners to provide reliable service to New York’s citizens by helping over 6 million New Yorkers gain access to higher quality healthcare and health insurance through New York’s Medicaid Program (eMedNY) and the New York State of Health™ Marketplace.

www.csra.com
Risk powers performance.

Expanding your business, capturing new markets and driving efficiency create cyber risk. It’s unavoidable. But it doesn’t have to derail performance. At Deloitte, our Secure.Vigilant.Resilient.™ approach to cyber helps you confidently deploy new technologies, pursue new strategies and, ultimately, outperform your competition.

www.deloitte.com/risk
ENSURING REGULATORY COMPLIANCE AND PROTECTING INFORMATION ASSETS AGAINST THE EVER-CHANGING THREAT LANDSCAPE.

Presidio Albany Office
20 Corporate Woods Blvd, Suite 306
Albany, NY 12211
518.213.9310 | www.presidio.com

CELEBRATING 100 YEARS | The Sage Colleges

Russell Sage ONLINE

ADVANCE YOUR EDUCATION + YOUR CAREER

Russell Sage Online, the distance learning component of The Sage Colleges, is ranked in the Top 10 Best Online Colleges in New York state.*

CYBERSECURITY & INFORMATION TECHNOLOGY
BACHELOR'S DEGREES + CERTIFICATES

› Certificates in Cybersecurity and Information Technology
› Bachelor's degree in Information Technology & Cybersecurity
› Designed to prepare students to sit for many cybersecurity certifications
› Taught by highly experienced experts in the field of information security
› Program Director: Michael Weisberg, CISSP

LEARN MORE:
(518) 292-8615
cyber@sage.edu
online.sage.edu

Be. Know. Do. MORE

The Sage Colleges
ALBANY | TROY | ONLINE

*onlineschools.net, 2016
Security is a process. Built in, not bolted on!

NYSTEC can help you build security into your networks and systems.

infosec.nystec.com

BRINGING CLARITY
To Complex Technology Projects

www.nystec.com

TRACK, PURSUE, AND NEUTRALIZE THREATS.

The longer threats remain undetected, the more damaging they become. Take control of your information and fight threats on your terms. It’s time to start advancing security.

Take the next step at symantec.com

Copyright © 2016 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
Proud to Partner with:

Proud to Partner with:

Where Technology Means More®

18 Corporate Woods Blvd., 2nd Floor, Albany, NY 12211
www.eplus.com

© 2016 ePlus Inc. All rights reserved. ePlus, the ePlus logo, and all referenced product names are trademarks or registered trademarks of ePlus Inc. All other company names, logos, and products mentioned herein are trademarks or registered trademarks of their respective companies.

Join us at IEEE’s Cybersecurity Initiative
https://www.computer.org/web/ieee-cybersecurity

Visit the IEEE Computer Society for Secure Design

IEEE Syracuse Section

Optimized Security for Hybrid Cloud Deployments

Go with the global market leader in server security

- Comprehensive set of security controls
- Optimized for leading platforms
- Automated across hybrid environments

© 2016 Trend Micro, Inc. All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro, Inc. All other trademarks are the property of their respective owners.
government technology

TECHNOLOGY NEWS. BEST PRACTICES. INNOVATIVE SOLUTIONS.

Get an in-depth view of the government IT market, from the top trends and best practices for cyber security, to the most innovative projects.

(Always FREE)

Subscribe today:
govtech.com/NYSforumcsc2016
Government is where innovation happens. Delivering services to constituents where they live and work, agencies are using technology to strengthen community connections. AT&T continues to spearhead the network revolution, driving innovation and investing more capital than any other US public company. By bringing together solutions that protect, serve and connect—committed AT&T professionals are working with the public sector to identify and implement technology to transform the business of government.

It’s our business to protect.
Analyzing over 10 petabytes of traffic each and every day, it’s our business to help prevent, detect and respond to cyber threats.

Community action starts with data.
The explosive growth in government data requires the ability to securely capture, store and transform data into action.

Your voice is unleashed.
The convergence of voice and data onto a single platform promises a range of new applications that will transform how you connect.

The office is mobile.
From delivering services to meet the needs of millennial constituents to increasing workforce productivity, mobility solutions make it happen.

Public has gone private.
For both mobile and IP traffic, private network connectivity offers enterprise-grade security, data integrity and higher quality of service.

The network is on demand.
AT&T is transforming its infrastructure to a software-defined architecture that enables intelligent, dynamic on-demand networking.

Visit www.att.com/stateandlocal to learn more.

Cisco delivers intelligent cybersecurity for the real world. This vision is based on a threat-centric approach to security that reduces complexity while providing superior visibility, continuous control, and advanced threat protection across the entire attack continuum. With this new security model organizations can act smarter and more quickly before, during, and after an attack.

Hewlett Packard Enterprise is an industry leading technology company that enables customers to go further, faster. With the industry’s most comprehensive portfolio, spanning the cloud to the data center to workplace applications, our technology and services help customers around the world make IT more efficient, more productive and more secure. Hewlett Packard Enterprise provides security solutions to mitigate risk and defend against today’s most advanced threats. HPE Security enables organizations to take a proactive approach through application security, network defense and security analytics. More information about Hewlett Packard Enterprise Security is available at Hpe.com/security
Dell Security solutions help you create and maintain a strong security foundation with interconnected solutions that span the enterprise. From endpoints and users to networks, data and identity, Dell Security solutions mitigate risk and reduce complexity so you can drive your business forward. www.dell.com/security

Presidio is a leading US-based IT solutions provider offering consulting, professional services, and cloud and managed services. By taking the time to deeply understand how our clients define success, we architect technology solutions that address their evolving business needs. Our approach blends the credibility to deliver practical results today, with the creativity to drive the business visions of tomorrow. More than 2,700 Presidio professionals, 1,500 of whom are engineers with over 5,800 industry-leading certifications, are based in 60+ offices across the US. We serve over 6,500 clients through a local delivery model while capitalizing on our scale as a $2.8 billion national industry leader. www.presidio.com

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world’s largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

ePlus engineers transformative technology solutions for the most visionary organizations in the world. Through our master architects, engineers, and consultants, we see our clients’ horizons and craft sustainable IT roadmaps to get them there. Then we make it happen. This takes imagination, relentless client service, and the tenacity to enable our clients to achieve their visions. Our deep partnerships with top manufacturers—many who look to us for their own technology needs—keep us immersed across the IT ecosystem. From strategy to fulfillment to managed services, we enable our clients to realize what it means for technology to do more.
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.

Bay Path University’s completely online MS in Cybersecurity Management prepares graduates for both initial placement and mid-level positions in career track jobs in cybersecurity, information assurance, and risk management fields. This program has been designed for college graduates who want to work in the cybersecurity industry in a leadership capacity. An extensive technical background is not needed to apply to this program, however, some level of proficiency with computing, particularly networks, would be beneficial.

For more information, please contact: Diane Ranaldi, M.Ed., Dean of Graduate Admissions by phone: (413) 565-1332, or email: Graduate@baypath.edu

AppSense is the leading provider of UEM solutions for the secure endpoint. AppSense user virtualization technology allows IT to secure and simplify workspace control at scale across physical, virtual and cloud-delivered desktops. AppSense Solutions have been deployed by over 3,600 enterprises worldwide to 9 million endpoints. The company is headquartered in Sunnyvale, CA with offices around the world. For more information please visit www.appswsense.com.

CA Technologies is the leading provider of application development, management, and security solutions. Providing software that fuels transformation for agencies and corporations alike and enabling them to seize the opportunities of the application economy. Software is at the heart of every agency and every business across every industry. From planning to development to management and security, CA works with agencies and companies worldwide to change the way we live, transact and communicate. CA Technologies, where Business is Rewritten by Software.
Carousel Industries is a recognized leader in helping organizations evolve the way they communicate and orchestrate the flow of information throughout their networks. Carousel enables clients to connect and collaborate the way modern IT users demand and advance from their current network infrastructure to meet tomorrow’s standards. With deep expertise across a vast portfolio of communication, network, and security technologies, Carousel is able to design, implement, and support solutions tailored to meet the unique needs of each customer. By offering professional and managed services with flexible deployments in the cloud, Carousel ensures clients achieve agility and utilize technologies in the way most effective for their business.

CrowdStrike is the leader in next-generation endpoint protection, threat intelligence and response services. CrowdStrike’s core technology, the Falcon platform, stops breaches by preventing and responding to all types of attacks – both malware and malware-free. CrowdStrike has revolutionized endpoint protection by combining three crucial elements: next-generation AV, endpoint detection and response (EDR), and a 24/7 managed hunting service — all powered by intelligence and uniquely delivered via the cloud in a single integrated solution. Falcon uses the patent-pending CrowdStrike Threat Graph™ to analyze and correlate billions of events in real time, providing complete protection and five-second visibility across all endpoints. Many of the world’s largest organizations already put their trust in CrowdStrike, including three of the 10 largest global companies by revenue, five of the 10 largest financial institutions, three of the top 10 health care providers, and three of the top 10 energy companies. CrowdStrike Falcon is currently deployed in more than 170 countries.

Every day, CSRA makes a difference in how our government serves our citizens. We believe that by working together; we can deliver exceptional next-generation IT solutions and professional services to enable the safety, security, health and well-being of our nation. We are proud of our 30-year legacy of service to New York State, working together to help one out of every three New Yorkers gain access to affordable healthcare using our reliable eMedNY operations and the New York State of Health™ Marketplace. CSRA’s enduring values and inspired performance help New York State make its citizens’ lives better.

CyberArk is the only security company that proactively stops the most advanced cyber threats – those that exploit insider privileges to attack the heart of the enterprise. The company has pioneered a new category of targeted security solutions to lock down privileged accounts and protect against cyber threats before attacks can escalate and do irreparable business damage. CyberArk is trusted by the world’s leading companies – including 40 of the Fortune 100 – to protect their highest value information assets, infrastructure and applications, while ensuring tight regulatory compliance and audit requirements.
DynTek, Inc. provides professional IT consulting services, end-to-end IT solutions, managed IT services and IT product sales to mid-market commercial businesses, state and local government agencies, and educational and healthcare institutions. At DynTek, we specialize in architecting solutions beyond any single vendor or subsystem. We design, build, operate and support cloud solutions that encompass our client’s entire infrastructure - from the data center to the desktop. From virtualization and cloud computing to unified communications and collaboration, DynTek architects professional technology solutions across the core areas of your technical environment: Infrastructure/Data Center, Microsoft Platforms and End Point Computing.

Cyberspace has become the new battleground against crime and terrorism and Excelsior College has risen to the challenge with nine online programs in cybersecurity on undergraduate and graduate levels. Whether you’re an IT professional, government employee or contractor, law enforcement professional or military service-member, Excelsior has a flexible and affordable cybersecurity program that’s right for you. Excelsior’s multidisciplinary curriculum features broad coverage on strategies, policy, ethics and legal compliances, operational processes, and cybersecurity techniques and technologies. Our courses give you the know-how and leadership skills you need to succeed.

FBI/NYSIC Cyber Partnership

The FBI’s Albany Field Office Cyber Intrusion Program is responsible for investigating federal crimes related to computer intrusions and high technology in central, eastern, and northern New York. Through close partnership with federal prosecutors and our state and local partners, the FBI investigates criminal and state sponsored computer intrusions. These investigations, along with the gathering and dissemination of intelligence, help to prevent future cyber crime and strengthen computer network security in both the private and public sector.

The New York State Intelligence Center (NYSIC) is the officially-designated fusion center for New York State. As one of the nation’s network of 78 fusion centers, the NYSIC is a multi-jurisdictional operation responsible for the collection, analysis, and dissemination of criminal and terrorism intelligence. The NYSIC is located in the greater Capital Region and hosts dozens of law enforcement and homeland security partner agencies. The NYSIC’s newly developed Cyber Analysis Unit gathers, analyzes and disseminates cyber threat information and intelligence (criminal or homeland security-related) to law enforcement, government agencies and the private sector.

Stop by to see how the FBI and NYSIC are partnering to fulfill their cyber security missions.

GreyCastle Security is a cybersecurity consulting firm focused on risk management, awareness and operational security. Our company was established to counter rapidly evolving cybersecurity threats and manage risks in people, process and technology. GreyCastle Security is comprised exclusively of highly certified professionals with prior security experience in healthcare, education, retail and gaming. Our team members are all former CISOs, ISOs, security specialists and operators. We bring a client perspective to everything we do. All we do is cybersecurity. All day, every day. We provide assessments, training, testing and response capabilities to organizations of all sizes, types and industries. We bring passionate practicality to cybersecurity.
The Griffiss Institute (GI) was established in 2002, by the State of New York, as an independent 501(c)(3) entity governed by a Board of Directors. The primary role of the 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 Lab (AFRL) Information Directorate to further strengthen our nation’s security. By partnering AFRL with private industry and academia, the GI is able to facilitate and grow the technology base of the Upstate NY region.

Interface Masters Technologies is a leading provider of high speed networking solutions focused on Gigabit, 10 Gigabit, 40 Gigabit and 100 Gigabit Ethernet. For over 20 years, the company has been providing innovative networking solutions with customization services to OEMs, large enterprises and sophisticated end users. Interface Masters has been an OCP member contributing multiple white box designs to the project while supporting customer SDN development. Interface Masters Technologies offers standard product and customization services for Smart NICS, Ethernet switches and networking appliances. Complete software environments include diagnostics, Linux, SDK and vertically integrated solutions from Interface Masters and partners. All products are designed and manufactured in San Jose, California.

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company’s award-winning platform unifies next-generation SIEM, log management, network and endpoint forensics and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides innovative compliance automation and assurance, and enhances IT intelligence.

LogRhythm
The Security Intelligence Company

Lynx Technology Partners (Lynx) is your trusted information security and risk management partner. We help customers recognize and control IT-related risks, maintain compliance with major industry regulations, and improve security posture.

We offer comprehensive security and risk solutions, including:
- IT Risk Management
- Cybersecurity
- IT GRC Solutions
- Compliance 911
- talent management

Lynx supports critical projects in Federal, State and Local Government, Fortune 500, and Higher education. Inc. 5000 ranked Lynx as #80 amongst the fastest-growing privately held companies, ranked #1 in top security companies, and is a certified Minority Business Enterprise (MBE) headquartered in New York, NY.
M. A. Polce Consulting is a Managed IT Support company with a focus on Security. We provide Private Cloud services out of our own data centers to complement Managed IT. We also provide consulting and implementation services in several key disciplines such as networking & wireless, storage, virtualization, desktop virtualization, and business intelligence. Today's rapidly evolving threat landscape demands smarter and more responsive security measures. Our services help safeguard your network, critical internal assets, remote users, and customers. We provide round-the-clock monitoring and management of systems, network devices and firewalls, performing software and signature upgrades, and responding to alerts.

Cyber Soldiers train and operate on a traditional part-time basis, in support of state and federal missions. When mobilized for federal active duty, Cyber Soldiers provide surge support to Army Cyber Command and support to defensive and offensive cyberspace operations. Cyber Soldiers are elite, trained, trusted, disciplined and highly skilled professionals responsive to the needs of the nation while boosting the state and federal cyber defense capabilities. Citizen Soldiers are an essential part of The Cyber Team, these cyber professionals, many of whom bring private sector experience, enhance the total Army’s cyberspace capabilities and capacities.

Meridian IT is a technology solutions provider built on proven infrastructure knowledge and experience across our advanced teams of consultants and engineers. We design and implement and support transformative solutions in infrastructure, end-user computing, intelligent data management, unified communications, hosting/cloud, managed services, IT lifecycle management.

To respond to evolving threats, information security must be a continuous effort encompassing policy, process, procedure, education, monitoring, and enforcement.

NYSTEC is a vendor-neutral, independent advisor to clients and we consistently put your best interests first. We understand that good security is not a product, but rather a process that must address threats with multiple layers of controls. With our in-depth experience with federal and New York State government regulations and policies, we are uniquely positioned to help you develop a layered security strategy and plan that will increase the integrity, confidentiality, and availability of your IT systems.
Quanterion operates the Cyber Security and Information Systems Information Analysis Center (CSIAC); a DoD sponsored Center of Excellence specializing in cybersecurity and advanced information technology (IT). CSIAC collects, analyzes, processes, synthesizes, produces and disseminates Scientific & Technical Information. CSIAC provides access to vast knowledge repositories and conducts novel core analysis tasks (CATs) to address customer focused technological shortfalls. Quanterion’s expert staff develop agile, innovative, responsive, state-of-the-art cybersecurity solutions and exploit best practices for achieving information assurance (IA). Quanterion personnel are experienced in conducting the Risk Management Framework (RMF) Assessment and Authorization (A&A) process. Quanterion examines computer systems and networks to identify potential cyber vulnerabilities within an organization’s IT infrastructure.

Regional Computer Recycling & Recovery (RCR&R) is a R2/RIOS Certified Electronics Recycler and a licensed, NAID AAA Certified Data Destruction Contractor. RCR&R focuses on recovery of value from idle, obsolete and excess electronic equipment and operates a large-scale processing facility in Rochester, NY and two regional consolidation facilities in Albany and the New York City area.

SafeConnect products automate BYOD secure on-boarding, guest self-enrollment, context-aware network access assignment, and device security compliance. SafeConnect is an industry leader in securely managing the explosion of Internet of Things (IoT) devices, and provides real-time contextual intelligence (identity, device type, location, ownership, and security posture) to 3rd party security management platforms. SafeConnect can also leverage existing IDS/ATD providers to provide policy-based device enforcement and orchestration based on threat severity and device context. The SafeConnect Network Access Management product suite is available through the New York State Office of General Services Information Technology Umbrella Contract (Lot 1 Software). Visit www.impulse.com

The Sage Colleges is a small university comprised of the undergraduate Russell Sage College for women in Troy, NY; the coeducational undergraduate Sage College of Albany in Albany, NY; and three graduate schools operating on both campuses – the Esteves School of Education, School of Health Sciences and School of Management. Sage, which celebrates its Centennial in 2016, also offers flexible programs for working adults through the School of Professional and Continuing Education and via its distance learning arm, Russell Sage Online.
SANS is the most trusted and by far the largest source for information security training in the world. Our computer security courses are developed by industry leaders in numerous fields including cyber security training, network security, forensics, audit, security leadership, and application security. Courses are taught by real-world practitioners who are the best at ensuring you can apply it immediately. In addition to top-notch training, we offer certification via GIAC, an affiliate of the SANS Institute, a certification body featuring over 20 hands-on, technical certifications in information security, and optional Master’s Degree programs through SANS Technology Institute.

Nearly 40 years ago, SAS pioneered the use of analytics to solve complex business problems. Today, SAS is the leader in business analytics software and services, and the largest independent vendor in the analytics market. Through innovative solutions delivered within an integrated framework, SAS helps state governments prevent fraud, enhance public safety, improve program performance and enable a higher degree of transparency. SAS’ industry-leading big data analytics and experience in real-time decision making helps anticipate and mitigate cyber events. SAS leverages big data, high-performance and predictive analytics while using and complementing your existing security infrastructure to proactively assess security risks.

Splunk Inc. (NASDAQ: SPLK) provides the leading software platform for real-time Operational Intelligence. Splunk® software and cloud services enable organizations to search, monitor, analyze and visualize machine-generated big data coming from websites, applications, servers, networks, sensors and mobile devices. More than 10,000 enterprises, government agencies, universities and service providers in over 100 countries use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, prevent fraud, improve service performance and reduce costs. Splunk products include Splunk® Enterprise, Splunk Cloud™, Splunk Storm®, Hunk®, Splunk Analytics for Hadoop and premium Splunk Apps. To learn more, please visit http://www.splunk.com/company.

Tri-Delta Resources is a leading provider of hardware, software and services solutions to help organizations manage their computing architecture. Tri-Delta Resources is the value leader among National Disaster Recovery Service Providers. We have the facilities, equipment and expertise in our data center, located in Canandaigua, New York, to handle your disaster recovery planning, testing and emergency needs. Tri-Delta Resources has one of the largest sales and support Citrix teams in the northeast.

SMS Passcode is a technology partner of Tri-Delta Resources offering multi-factor authentication, improving enterprise security and productivity by delivering an easy to use and intelligent solution that helps ensure the safety of corporate networks and applications.
Utica College offers regionally accredited Online Bachelor’s, Master’s and Certificates in Cybersecurity and Cyber Policy with specializations in Intelligence, Investigations, Computer Forensics, Cyber Operations, Information Assurance, and Cyber Data Fusion and Analysis taught by highly experienced faculty. Utica College has earned three designations as a National Center of Excellence by the NSA and DHS, DC3 and EC-Council. With the renowned Economic Crime & Cybersecurity Institute, and the Center for Identity Management and Information Protection, the College collaborates with industry and government to develop innovative curriculum and provide students with unique credentials and career opportunities. Call 315-732-2640 or visit http://programs.online.utica.edu/programs/security.asp for more information.

Varonis is a leading provider of software solutions that protect data from insider threats and cyberattacks. Varonis allows organizations to analyze, secure, manage, and migrate their volumes of unstructured data, which often contain an enterprise’s financial information, product plans, strategic initiatives, intellectual property, and confidential employee, customer or patient records. For more information visit www.varonis.com

Today’s complex IT requirements demand a flexible process that better addresses your needs. Vandis challenges the assumption that IT acquisition is a push model by developing quality relationships with our clients based on joint problem solving using the most appropriate technologies available. Achieving solutions that offer maximum performance and yield greatest results requires proven expertise, a close working relationship built on trust, and a diverse network of technology partners.

With over 32 years of experience, Vandis has the proven ability to navigate the ever-changing technology and business landscape. Vandis’ high-level engineering capabilities and close relationships with market leading and niche manufacturers allow us to make timely recommendations based on your specific environment.

At Verizon Enterprise Solutions, we help organizations like yours improve customer experience, drive growth and manage risk. We offer solutions for your industry, built on our secure mobility, IT solutions, networking, Internet of Things and advanced communications platforms, so you can seize new opportunities to innovate and grow. www.verizonenterprise.com
VMware (NYSE: VMW), is a global leader in cloud infrastructure and business mobility. The company’s solutions enable IT organizations to innovate in new ways that leverage the cloud and business mobility. Through its One Cloud, Any Application, Any Device architecture, VMware dramatically simplifies IT complexity through a software-defined approach that allows customers to rapidly develop, automatically deliver and safely consume traditional and cloud-native applications on any device. VMware offers a unified platform to automate and streamline IT service delivery across clouds and the data center and through virtualized workspaces. With 2014 revenues of more than $6 billion, VMware has more than 500,000 customers worldwide and offers a robust ecosystem of more than 75,000 partners. Learn more at www.vmware.com.

WatchGuard® Technologies, Inc. is a global leader of integrated, multi-function business security solutions that intelligently combine industry-standard hardware, best-in-class security features, and policy-based management tools. WatchGuard provides easy-to-use, but enterprise-powerful protection to hundreds of thousands of businesses worldwide. WatchGuard is headquartered in Seattle, Wash. with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com. For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuardTech on Facebook, or on the LinkedIn Company page.

Sponsor

Demonstration Schedule

Terabyte Sponsor

AT&T
June 8
10:35 a.m. – 10:55 a.m.
June 9
10:05 a.m. – 10:25 a.m.
Booth #20-22

Megabyte Sponsors

Cisco Systems
June 8
1:55 p.m. – 2:05 p.m.
June 9
11:25 a.m. – 11:35 a.m.
Booth #32-33

Hewlett Packard Enterprise
June 8
3:05 p.m. – 3:15 p.m.
June 9
2:35 p.m. – 2:45 p.m.
Booth #37-38
Passport Drawing: Visit our exhibitors for a chance to win some amazing prizes. All you need to do is bring the Exhibitor passport to each of the listed booths and have it stamped, it’s that easy! Once the passport is stamped please bring it to the Registration Table. Drawings will be held at 3:00 p.m. on Wednesday, June 8 and at 1:30 p.m., Thursday, June 9. Prizes must be picked up by the end of the Conference. The passport is sponsored by Presidio and made possible by generous donations from our sponsors and exhibitors.