Monday, August 19

11:00 a.m.	**Registration**

12:00 p.m. - 1:00 p.m.	**Networking Lunch**

1:00 p.m. - 1:30 p.m.

Welcome and Opening Remarks

Lisa Gau, VP, Corporate Sales, East Region, CDW
Bob Bragdon, SVP and Publisher, CSO

1:30 p.m. - 2:15 p.m.

The Future of Cybersecurity: A Friendly Hacker's Perspective

Keren Elazari, Cyber Security Analyst, Author & Researcher

Cybersecurity is no longer about protecting secrets. It's about our way of life that relies on digital technology, everywhere—from clouds to smartphones, from sensors to webcams, to stock markets and so much more. In this environment, are you and your organization thinking about what's next? Join us for this session where we'll inspire security and IT executives and managers to act on what matters most. We'll shed light on emerging security threats, new attack vectors and techniques, what we can learn from friendly hackers and how to work with them, and practical ideas on how executives and managers can make a difference in their organizations. We'll discuss the future workforce and business challenges in this space and how to foster more diversity in cybersecurity. Finally, we'll look at the future of cybersecurity and learn why resilience will be defined not just by our efforts to balance technology's benefits against the risks it brings with it, but by how we evolve our paradigms about security, privacy and digital access.

2:20 p.m. - 2:50 p.m.

Inside-Out Security: Why We Should Build Castles Instead of Warehouses

Alyssa Miller, Manager, Information Security Solutions Practice, CDW

Medieval castle builders made effective use of simple design principles to defend the most valuable assets inside. Centuries later, we've forgotten those valuable lessons as we defend our IT assets. From the moment we began enabling multi-user systems, we've approached how we defend our information in all the wrong ways. Join us for this session as we look at a completely different approach to designing security in our systems. We'll explore new ways to understand what assets are, what threats they face, and how to leverage three basic types of defense mechanisms to effectively protect what we hold most dear. To add context to this new approach, we'll draw on trends and lessons learned from thousands of security assessments and deployments across a vast portfolio of security technologies. All of this will show why it's time to defend your crown jewels inside a fortified castle rather than a thinly constructed warehouse.

2:50 p.m. - 3:20 p.m.

Networking Break

Ask the experts in "CDW's Bring IT On" area during the break. The answer to your challenge might be right here onsite!

3:20 p.m. - 3:45 p.m.	**Building an Evidence-Based Security Strategy and Program: An Executive Interview**

Dan Costantino, CISO, Penn Medicine
Bob Bragdon, SVP and Publisher, CSO

Penn Medicine is one of the world's leading academic medical centers, dedicated to the related missions of medical education, biomedical research, and excellence in patient care—and consists of the Raymond and Ruth Perelman School of Medicine at the University of Pennsylvania (founded in 1765 as the nation's first medical school) and the University of Pennsylvania Health System. As a leading academic medical center in the United States, Penn Medicine must maintain a secure technology environment ensuring the privacy and secure data of patients and colleagues. Join us for this session to learn about how they've rapidly evolved their security and risk posture across 40,000 employees and six hospitals, along with the evidence-based fundamentals they leverage to build on their future-forward security strategy.

4:00 p.m. - 4:45 p.m.

What is Zero Trust Endpoint Security—and Why Does It Matter?	**Accelerating Security to the Speed of Business**
Adam Licata, Director, Product Management, Endpoint Security, Symantec	David Roth, VP, US Northeast, Trend Micro
As new technologies permeate the business landscape, today's organizations face an ongoing and sophisticated battle in stopping attacks earlier and reducing the number of incidents and breaches. At the same time, Zero Trust concepts and strategies have emerged as contemporary frameworks to address these challenges and improve an organization's security posture. Why is Zero Trust Endpoint Security relevant today? And how can it reduce costs related to incident response and SOC staffing bandwidth assigned to endpoint detection and response toolsets? Join us for this session for answers to these questions—and to hear real world stories on how to optimize endpoint security across today's threats.	Today's business world is agile-driven, and various technology advancements have emerged to enable this agility including clouds, DevOps, containers and serverless architectures. In this environment, security leaders must rethink security success across a technology landscape teeming with automation and constant change. Join us for this session to understand strategies designed to meet today's security objectives—and at the speed the business requires.

4:45 p.m. - 5:30 p.m.   **Free Time**

5:30 p.m. - 7:00 p.m.   **Networking Dinner in the IT Showcase**

Grab a cocktail and network with SummIT attendees and partners. Don't miss the opportunity to ask the experts at CDW's "Bring IT On" area!

Tuesday, August 20

7:30 a.m. - 8:30 a.m.

Networking Breakfast with Birds of a Feather Discussion Tables

Engage with your executive peers in meaningful discussions. Pick a topic and share how it's working in your organization—or learn from others about what's working for them, including:

- Best Practices in Endpoint Security

- Best Practices in Identity and Access Management

- Managing Security in the Cloud Era

- Modern Strategies to Manage Cyber Risk

- Optimizing Network Security Monitoring Tools

- Infrastructure Protection Across Data Centers and Hybrid Environments

- Securing the Organization in the AI and Automation Era

- Modernizing Application Security with DevSecOps

- Best Practices in Communicating with Senior Management and the Board

8:30 a.m. - 8:45 a.m.

Welcome

Bob Bragdon, SVP and Publisher, CSO

8:45 a.m. - 9:30 a.m.

Winning at Cyber Leadership: Get Your IT Together

G. Mark Hardy, Founder & CEO, National Security Corporation

People, process, and technology. You hire for people. You budget for technology. But strategic success comes from successfully integrating your assets in a repeatable process that matures with time and expertise. Cyber security has fought its way to the boardroom agenda, but solutions require more than just throwing money at the problem. Like the shift to a wartime economy over 75 years ago, we must reprioritize assets to address the most critical risks we recognize as informed leaders. Join us for this session as we explore ways to integrate your security resources in a workable methodology that's responsive to executive governance, effectively manages cyber risk, and meets the ever-growing list of compliance requirements we face in a globalized economy.

9:35 a.m. - 10:20 a.m.

Adversary Tradecraft and the Importance of Speed to Take Action

Chris Kachigian, Sr. Director, Global Solutions Architecture, CrowdStrike

"Breakout Time"—the time it takes for an intruder to jump from a compromised machine and move laterally through an organization's network—is a crucial window to stop a breach, but isn't the only metric security leaders need to know about. When an attack is in progress, organizations have on average one minute to detect it, ten minutes to understand it and one hour to contain it. Is your organization ready to meet the 1/10/60 challenge? Join us for this session as we take an in-depth look at the findings in CrowdStrike's 2019 Global Threat Report, and discuss the techniques and unique behaviors of today's adversaries while highlighting the average time an organization needs to take action.

10:20 a.m. - 10:50 a.m.	**Networking Break**
	Grab some coffee and refreshments along with an opportunity to compare notes with your peers.

10:50 a.m. - 11:15 a.m. **Harnessing Blockchain for the Enterprise: An Executive Interview**

Arvin Bansal, Senior Director, Cyber, Data and Risk Governance, AmerisourceBergen
Bob Bragdon, SVP and Publisher, CSO

With more than $160 billion in annual revenue, and employing 21,000 associates in more than 50 countries, AmerisourceBergen provides pharmaceutical products, value-driving services and business solutions for healthcare providers, veterinary practices and livestock producers. In this vast supply chain environment, protecting customer data is paramount. Join us for this session to learn how the organization views the various data streams it must protect, and how they're harnessing a blockchain framework to improve security, identities and data protection.

11:30 a.m. - 12:15 p.m.

Hunting and Intel: How to Get Amazing Results from Existing People and Technology	**Who Are the Very Attacked People in Your Neighborhood? Adopting a People-Centric Approach to Security Awareness Training**
Steven Booth, CSO, FireEye	Dale Zabriskie, Security Awareness Training Evangelist, Proofpoint
The Defender vs. Adversary dynamic is all about people finding people. And while technology can detect malware, what about human behavior, artifacts, and tactics/techniques/procedures that indicate a human is doing evil in an environment? That's where the creative use of resources becomes paramount. Join us for this session to learn how to use intel to detect non-malware, understand APT techniques, link phishing campaigns to actors, build predictive defenses, and prioritize vulnerabilities and threats based on the actor—not what the press is reporting.	The roadmap of your IT environment is full of twists, turns, roadblocks and potholes. Those with access to critical information systems are navigating a perilous journey—often without explicit security awareness training to help identify warning signs along the way. If not properly trained to spot these threats, your users can become your greatest risk by clicking on malicious links that enable malware or expose confidential information. Join us for this session as we discuss best practices for adopting a people-centered, risk reduction approach to security awareness training that can transform your users from risky to ready navigators.

12:15 p.m. - 1:15 p.m.	**Networking Lunch with Birds of a Feather Discussion Tables**

Engage with your executive peers in meaningful discussions. Pick a topic and share how it's working in your organization—or learn from others about what's working for them, including:

- Best Practices in Endpoint Security

- Best Practices in Identity and Access Management

- Managing Security in the Cloud Era

- Modern Strategies to Manage Cyber Risk

- Optimizing Network Security Monitoring Tools

- Infrastructure Protection Across Data Centers and Hybrid Environments

- Securing the Organization in the AI and Automation Era

- Modernizing Application Security with DevSecOps

- Best Practices in Communicating with Senior Management and the Board

1:15 p.m. - 2:00 p.m.	**Zero Trust and the Flaming Sword of Justice**

Dave Lewis, Global Advisory CISO, Duo Security

Security breaches make headlines, and breach headlines that were rare just five years ago seem to occupy today's daily news cycle. Many data breaches are made possible by missteps and misconfigurations. Compounding this are security issues introduced to website authentication mechanisms that enforce bad end user behavior. As a result, security debt has become a significant problem for the vast majority of organizations, and attackers will exploit it to their advantage. In addition to keeping system hygiene front-of-mind, today's defenders need to focus on proper "network zone segmentation"—now more commonly called "zero trust networks." Join us for this session as we discuss the dissolution of the traditional perimeter, and why today's security leaders need to focus on the strength of authentication, authorization and trust models for users.

2:05 p.m. - 2:35 p.m.	**The Security Staffing Challenge: Strategies to Solve a Persistent Problem**

Dan Costantino, CISO, Penn Medicine
Mark Leary, CISO, Regeneron
Alyssa Miller, Manager, Information Security Solutions Practice, CDW
Ken Weirman, VP and CIO, AMETEK, Inc.
Bob Bragdon, SVP and Publisher, CSO

According to CSO's 2018 Security Priorities Study, more than half of enterprise organizations plan to increase the size of their security team. At the same time, qualified security professionals remain difficult to find. How are organizations coping with this supply and demand challenge? Where do they see opportunities to find new talent? And what can they do to make positions attractive for recruiting and retention? Join us for this session as we explore answers to these questions and more.

2:35 p.m. - 3:00 p.m.	**Wrap Up Remarks**

Lisa Gau, VP, Corporate Sales, East Region, CDW

3:00 p.m.	**Departures**