CYBER SECURITY WORLD

June 28-29, 2017 | Workshop June 27 | Hotel Magnolia Denver | Denver, CO

Featuring 2 Tracks Addressing:

- Measuring cyber risks
- Defending against cybercrime with cognitive security
- Improving incident response time
- Integrating cyber threat intelligence
- Conducting effective forensic investigations
- Improving cybersecurity through enterprise risk management

Keynote Speakers

MIKI CALERO
Veteran Public Sector
CISO and Founder
Urbis Global LLC

DARREN VAN BOOVEN
CISO
Idaho National Labs

Earn up to
22 CPEs

#CYBWORLD17

CYBERSECURITYWORLD.MISTI.COM

GOLD SPONSOR
DARKTRACE

MEDIA PARTNER
ITSP MAGAZINE

MISTI™
TRAINING INSTITUTE

CYBER SECURITY WORLD

TECHNICAL LEVEL
○ LOW ◐ MEDIUM ● HIGH

CONFERENCE AT-A-GLANCE

WEDNESDAY, JUNE 28, 2017		
	Foundational Elements	**Next-Gen Security**
8:00 AM - 9:00 AM	*Registration & Continental Breakfast*	
9:00 AM - 10:00 AM	**KEYNOTE:** Let's Get Critical: Executing the Nuclear Option for Next Generation Cyber Security *presented by Darren Van Booven*	
10:00 AM - 10:15 AM	Unsupervised Machine Learning: A New Approach to Cyber Defense *presented by* DARKTRACE	
10:30 AM - 11:00 AM	*Refreshment Break with Exhibitors*	
11:00 AM - 11:50 AM	**A1** When the Levee Breaks: Fixing the Foundations of Your Information Security Program before the Flood *Michael Kearn* ○	**B1** Late-breaking session
11:50 AM - 1:00 PM	*Lunch on your own*	
1:00 PM - 1:50 PM	**A2** Toward Measuring Cyber Risks in a Business Context *Jacqueline Johnson* ○	**B2** Identifying Abnormal Activity to Improve Incident Response Time *Erik Goldoff* ◐
2:00 PM - 2:50 PM	**A3** Late-breaking session	**B3** Understanding the Risks of Smart Cities *Jon Clay* ◐
2:50 PM - 3:20 PM	*Refreshment Break with Exhibitors*	
3:20 PM - 4:10 PM	**A4** The Insider Impact on Enterprise Security: Why Malicious Hackers Aren't Your Biggest Problem *Christy Wyatt* ○	**B4** How Cyber Threats Shape Next-Gen SOCs *Etay Maor* ●
4:15 PM - 5:05 PM	**A5** Integrating Cyber Threat Intelligence *Ken Dunham* ○	**B5** Dealing with Ransomware: How Not to Be a Victim, and What to Do When You Become One *Ben Rothke* ◐
5:05 PM - 6:00 PM	*Networking Reception*	
THURSDAY, JUNE 29, 2017		
7:30 AM - 8:30 AM	*Registration & Continental Breakfast with Exhibitors*	
8:45 AM - 9:45 AM	**KEYNOTE:** Improving Cybersecurity through Enterprise Risk Management *presented by Miki Calero*	
9:45 AM - 10:00 AM	Tech Spotlight	
10:15 AM - 10:45 AM	*Refreshment Break with Exhibitors*	
10:45 AM - 11:35 PM	**A6** Running Security Operations Agilely–Without Tripping! *Kristy Westphal* ◐	**B6** The Insecurity of Industrial Things *Jamison Utter* ◐
11:45 AM - 12:15 PM	**KEYNOTE**	
12:15 PM - 12:50 PM	*Networking Luncheon*	
1:00 PM - 1:50 PM	**A7** How to Defend Against Cybercrime with Cognitive Security *Willie Wong* ○	**B7** Speeding Up Triage and Incident Response by Speaking to Malware *Todd O'Boyle* ●
2:00 PM - 2:30 PM	**A8** Vulnerability Management is NOT Dead (Despite Our Best Efforts to Kill It) *Nathan Wenzler* ◐	
2:30 PM - 3:00 PM	*Coffee & Dessert with Exhibitors*	

Workshop

Tuesday, June 27

9:00 AM – 5:00 PM 8 CPEs

W2 Web Application Security Testing with Kali Linux

Mike Landeck, Director of Corporate Security, CISO

Brandon Archer, Information Security Architect, Adams County

Kali Linux is a powerful and popular tool for penetration testing and cybersecurity assessments. However, for a beginner it can be confusing and intimidating. This workshop is designed for the passionate beginner who wants a structured, plain-English environment to learn the basics of web application security testing using Kali. Attendees will leave with an understanding of the basics as well as step-by-step documentation allowing them to go back to their organizations to do rudimentary assessments.

Attendees will:

- Learn to navigate Kali Linux and run the applications necessary to do a web application security assessment
- Learn how to run an open source web vulnerability scanner
- Leave with a step-by-step test plan allowing them to conduct their own web application security assessments
- Receive templates and cheat sheets for documenting their findings
- Learn light web hacking skills to assist in their assessments

Agenda:

Part 1: Set-up

- Orientation to the tools and target site

Part 2: Recon and Intel

- Identifying sub-domains
- Checking for firewalls
- Fingerprinting the server and services

Part 3: Web Scanning

- Spider a web site
- Run an open source web vulnerability scanner
- Audit and interpret the results

Part 4: Manual Inspection

- Follow a comprehensive test plan to identify and document common web vulnerabilities

Part 5: Beginning Web Pen Testing

- Exploit the SQL injection found by the scanner to dump credit card numbers from a database
- Exploit the file upload vulnerability found by the scanner to run the code on the server
- Exploit the cross-site scripting vulnerability found by the scanner to redirect users

The class will follow a "See it, read it, do it" model where each exercise is demonstrated live by the instructor and the students will have a step-by-step guide to use as they complete the exercise. An assistant instructor will be available to help those who may fall behind.

Prerequisites:

Students must bring their own laptop. Prior to the workshop each student will be required to download the necessary software and confirm it runs on their laptop. A list of software and system requirements will be provided in advance.

When students leave they will take the test site and documentation with them, allowing them to begin assessments at their organizations.

Conference Agenda

Wednesday, June 28

9:00 AM – 10:00 AM

Keynote: Let’s Get Critical: Executing the Nuclear Option for Next Generation Cyber Security

Darren Van Booven, CISO, Idaho National Labs

In a time when a breach can be as simple as “Point, Click, and Destroy,” it’s time for a quantum leap in our thinking if we truly dare to change the zero-sum game we’ve seen over the last 20 years. How do you protect a modern network that includes nuclear reactors, supercomputers, cloud services, petabytes of data and its own power grid?

This talk will propose and explore innovative methods to secure today’s diverse technology landscape and the governance and tools needed to create and maintain an advantage over the adversary in the future.

Attendee take-aways include:

- Overview of today’s sophisticated threat landscape
- Devising a modern unified threat strategy
- Managing a tool portfolio to address the kill chain
- Key considerations needed when trying to protect critical infrastructure and other non-enterprise technologies
- Ways information technology can achieve buy-in with operational technology and physical security technology

10:00 AM – 10:15 AM

Unsupervised Machine Learning: A New Approach to Cyber Defense

Jesse Hood, Cyber Security Account Executive, Darktrace

From insiders to sophisticated external attackers, the reality of cyber security today is that the threat is already inside. Legacy approaches to cyber security, which rely on knowledge of past attacks, are simply not sufficient to combat new, evolving attacks, and no human cyber analyst can watch so much or react quickly enough. A fundamentally new approach to cyber defense is needed to detect and investigate these threats that are already inside the network - before they turn into a full-blown crisis.

Self-learning systems represent a fundamental step-change in automated cyber defense, are relied upon by organizations around the world, and can cover up to millions of devices. Based on unsupervised machine learning and probabilistic mathematics, these new approaches to security can establish a highly accurate understanding of normal behavior by learning an organization’s ‘pattern of life,’. They can therefore spot abnormal activity as it emerges and even take precise, measured actions to automatically curb the threat.

Discover why unsupervised machine learning is the future of defense and how the ‘immune system’ approach to cyber security provides complete network visibility and the ability to prioritize threats in order to better allocate time and resources.

In this session, learn:

- How new machine learning and mathematics are automating advanced cyber defense
- Why full network visibility allows you to detect threats as or before they emerge
- How smart prioritization and visualization of threats allows for better resource allocation and lower risk
- Real-world examples of unknown threats detected by ‘immune system’ technology

11:00 AM – 11:50 AM

A1 When the Levee Breaks: Fixing the Foundations of Your Information Security Program before the Flood ◔

Michael Kearn, VP, Principal Security Architect & ISO, US Bank

The shiny new product is not always the most effective solution to mitigate risk. In fact, more companies are breached because they had fundamental vulnerabilities in their security posture.

A house of sand will never stand, and layering next-gen solutions on top of a security program with a weak foundation won’t either. This presentation will discuss what many of us in our profession consider the basic building blocks of an effective security program, in addition to examining how current technologies can help create a stronger foundation. Learn how accurate risk assessments, threat modeling, and layering controls appropriately can help you set a firm foundation upon which to build your own program. We don’t always need a new set of tools, but sometimes a new or different perspective can make the biggest difference in securing our organizations.

- Encryption is not just for data obfuscation
- Encapsulation can be an effective control
- Creating roles and groups to manage identities is not difficult. Managing them and maintaining them is.
- Privileged access management needs to be a key component of any security program
- Understanding how to accomplish this is the challenge
- Understanding how to assess threats and identify layers that collectively will effectively mitigate risk, not just adding Band-Aids hoping the risk diminishes

11:00 AM – 11:50 AM

B1 Late-breaking session

TECHNICAL LEVEL
◔ LOW ◑ MEDIUM ● HIGH

1:00 PM – 1:50 PM

A2 Toward Measuring Cyber Risks in a Business Context

Jacqueline Johnson, Head of IT Security Architecture, Nordea

Most executives recognize that cyber risks are no longer on the horizon, but are an imminent cost of doing business. In this situation, executives ask themselves, “What does it mean for my business, how probable is a significant breach and what will it cost us?” Still, very few have developed the means to assess and quantify their cyber risk exposure.

In this session, the cyber value-at-risk framework introduced at World Economic Forum will be presented. The core components will be illuminated and some practical examples of how they can be quantified will be demonstrated.

Attendees will learn about:

- The World Economic Forum report on the cybersecurity value-at-risk model
- How to calculate cyber resilience metrics using the financial valuation principle
- Feeding of compliance metrics and threat intelligence into CyVaR
- Using CyVaR at boards and business units to raise security investments

1:00 PM – 1:50 PM

B2 Identifying Abnormal Activity to Improve Incident Response Time

Erik Goldoff, Principal Consultant, Symantec

In today’s threat landscape, it’s not a matter of if you will get attacked, it’s when... and how soon you can recognize and react can determine the level of incursion and damage. According to the Ponemon Institute, the average time to detect a breach is over 170 days, and this may be conservative compared to other studies. When you are breached, would you rather apologize to 30 million customers, 300,000 customers, or only 300?

The only way to determine when abnormal activity is occurring is to become familiar with what “normal” is. This includes bandwidth, memory and CPU utilization across your infrastructure and resources, as well as log volume and content. You may not be able to prevent the bad guy from kicking in your door, but you might be able to prevent him from leaving with your valuables if you catch him in time.

Attendees will learn:

- How to baseline performance of infrastructure and resources
- How to recognize abnormal activity compared to baseline
- How to create an Operations Guide (Run Book) to help complete routine surveys of your environment by any level of your staff
- The importance of having a proper incident response plan in place, and education of your staff on this plan
- How to use feedback to constantly review (and improve where possible) your security best practices

2:00 PM – 2:50 PM

A3 Late-breaking session

2:00 PM – 2:50 PM

B3 Understanding the Risks of Smart Cities

Jon Clay, Senior Manger Global Threat Communications, Trend Micro

As the urban population around the world continues to rise, both public and private sectors have begun investing in smart technologies to improve efficiency. Governments aiming to improve their provision of services—such as communication, transportation and waste management—as well as strengthen their public security measures are opting for smart cities. Building a smart city entails both generating vast amounts of data and making existing datasets more accessible to relevant organizations and government bodies. Consequently, generating big data to optimize a city can pose potential security and privacy issues that may stem from improper data analysis, sharing and use.

Attend this talk to hear results from recent research on several smart cities across the globe and learn about the various vulnerabilities that governments, public companies, citizens and tech leaders must be aware of. Best practices and recommendations on how to secure data and devices will also be shared.

Attendees will learn:

- Steps to take to secure company data in an age of smart cities
- Practical advice for securing devices with in their home and work using network segmentation, data classification and other techniques
- Why the complex attack surface of smart cities could have serious repercussions for end users and smart city providers
- How to minimize the risk of critical infrastructure from attacks

3:20 PM – 4:10 PM

A4 The Insider Impact on Enterprise Security: Why Malicious Hackers Aren’t Your Biggest Problem

Christy Wyatt, CEO, Dtex Systems

The modern cybersecurity landscape is more complicated than ever. There are more attack methods, more malware strains, and an abundance of solutions promising to protect organizations from the looming threat of cyberattacks. How are security teams and business executives supposed to make sense of what solutions are both necessary and effective?

While there is certainly no one-size-fits-all solution, one of the largest gaps in enterprise security strategy is user vulnerability and the insider threat. 80% of breaches are caused directly or indirectly by people—60% by enterprise insiders. The convenience of modern tools such as cloud applications, proxy bypass tools, and anonymous VPN sites contribute to this problem, and companies are at a loss for how to protect the organization and their employees effectively.

This session will explore the critical nature of the insider threat in a modern world, offering practical tips and considerations for stopping malicious hackers by protecting employees from their natural susceptibility to potential threats both on and off the company network.

Attendees will learn:

- Why malicious users and nation state actors are not the largest direct threat to your enterprise
- The most common misconceptions about the insider threat
- How insider threats such as negligent users compromise your data on a regular basis—often without realizing it
- Which key components are often overlooked when protecting against the insider threat
- What immediate steps organizations can take to strengthen cyber defenses

3:20 PM – 4:10 PM

B4 How Cyber Threats Shape Next-Gen SOCs

Etay Maor, Executive Security Advisor, IBM Security

We read about hacks and breaches on a daily basis—attacks conducted by cybercriminals that result in millions of compromised credentials, loss of millions of dollars, or denial of service attacks that can almost bring the internet to a halt. But how do these underground groups conduct these attacks? Where do they communicate and coordinate? What products and services do they buy and sell?

In this session we will dive into the world of organized cybercrime and take a peek! After reviewing the latest threat landscape we will see how these (and other threats) shaped the way SOCs (Security Operation Centers) are built. Not only the new technology (like cognitive computing for security) that is now being deployed, but also the types of training and simulations the staff have to go through, such as military-grade cyber threat simulation and response. We will see and review some of these simulations and talk about the back-end strategies and front-end tactics being used.

4:15 PM – 5:05 PM

A5 Integrating Cyber Threat Intelligence

Ken Dunham, Senior Director of Technical Cyber Threat Intelligence, Optiv

Cyber Threat Intelligence (CTI) is far more than scraping IOCs and looking for known malicious data within a network. Attend this session to learn leading practices that will help you avoid the pitfalls that so many have stepped into as they address this emergent need for managing enterprise cyber risk.

Attendees will learn how to:

- Accurately define CTI
- Integrate CTI into a strategic roadmap
- Identify common pitfalls with CTI integration
- Evaluate a successful implementation strategy
- Provide real-world lessons learned for implementing CTI

4:15 PM – 5:05 PM

B5 Dealing with Ransomware: How Not to Be a Victim, and What to Do When You Become One

Ben Rothke, Principal Security Consultant, Nettitude, Ltd.

Ransomware is malicious software that denies access to a user's data by encrypting data with a key only known to the hacker who deployed the ransomware, until the ransom is paid. It's 2017 and with tens of billions of dollars spent in information security, ransomware is bringing the IT systems of businesses from hospitals to police departments, to their knees.

Attendees will learn:

- What ransomware is and various ransomware families
- The importance of having good backups of all your data
- To pay the ransom or not to pay. Answering the question.
- Why ransomware writers love Bitcoin, and how to get a Bitcoin wallet
- Steps to ensure you don't become a victim
- What to do when you are a victim

Thursday, June 29

8:45 AM – 9:45 AM

Keynote: Improving Cybersecurity Through Enterprise Risk Management

Miki Calero, Veteran Public Sector CISO and Founder, Urbis Global LLC.

An Enterprise Security Risk Management (ESRM) program unifies physical security and cybersecurity to protect all organizational assets. While your organization may not be quite ready to implement a fully functioning, holistic ESRM program, adopting elements from this approach to the cybersecurity program can immediately reduce your organization's risk of cyber threats.

Find out how to start making your security program more risk centric, as Miki Calero reviews lessons learned from the award-winning implementation of the Enterprise Security Risk Management program at the City of Columbus, Ohio.

9:45 AM – 10:00AM

Tech Spotlight

10:45 AM – 11:35 AM

A6 Running Security Operations Agilely–Without Tripping!

Kristy Westphal, Senior Manager, Charles Schwab

As information security managers and directors, we have struggled with showing the value that our teams deliver to an organization. We've tried metrics, scare tactics, and used real-life stories, but we continue to struggle. While the Agile methodology has traditionally been used in software development, it has a lot of applicability to how we can manage our teams and more easily show value. No this isn't DevOps, but it is a way to better measure and monitor the progress of your security organization.

Join this session to learn more about the long journey from chaos into a more controlled chaos!

In this session attendees will hear:

- Overview of the Agile methodology
- A cross-walk of how Agile can help manage security operations
- Measuring progress more accurately than just project completion
- Reporting opportunities
- How this can be implemented in your organization

10:45 AM – 11:35 AM

B6 The Insecurity of Industrial Things

Jamison Utter, VP, Senrio

When hearing the buzzword "Internet of Things (IoT)," we typically think of the consumer world: smart toasters and connected fridges. However, there is a staggering number of network-embedded devices that perform life- and mission-critical tasks that our daily lives depend on. We haven't thought of these new types of devices as miniature computers that need the same care in deployment, management, and protection as our servers, computers and mobile phones. This is a HUGE blind spot. Embedded devices, such as ICS and SCADA systems, are the low-hanging fruit for potential attackers: They are fairly easy to compromise, are connected to high-value networks and detection often only happens after the fact.

This talk will share experiences exploiting embedded systems used in industrial control environments and discuss the reasons why these insecure design patterns exist, including business drivers and technology factors. We will share stories and anecdotes based on 10 years of research, training and consulting. Attendees will get an inside view into how attackers operate and walk away knowing what to look for when future-proofing our critical infrastructure networks.

Attendees will learn:

- ICS = IoT, IT - OT, and here is why
- Why traditional security does not work for IoT
- How to benefit from IoT without compromising safety and privacy
- Actionable steps for securing industrial IoT for security practitioners, operations staff and managers

11:45 AM – 12:15 PM

Sponsored Keynote

1:00 PM – 1:50 PM

A7 How to Defend Against Cybercrime with Cognitive Security

Willie Wong, Executive, IBM Security

Cybercrime is a growing threat, costing the global economy as much as $500 billion per year. The reality is, most organizations lack the in-house skills and resources to quickly identify, prioritize and react to these attacks. Security leaders are looking for cognitive security solutions that can help address the skills gap, accelerate incident response time, and reduce the cost and complexity of dealing with threats and vulnerabilities.

Cognitive systems such as Watson for Cyber Security use data mining, machine learning, natural language processing and human-computer interaction to understand, reason, and learn about evolving security threats—at a depth, speed and scale never before seen.

1:00 PM – 1:50 PM

B7 Speeding Up Triage and Incident Response by Speaking to Malware

Todd O'Boyle, CTO & Co-Founder, Strongarm

For an attacker to steal from you, they need persistent access. This means ensuring their C2 is reliable and resilient to takedown. That's the main reason why over 90% of malware uses the domain name system (DNS) for command & control and exfiltration. The good news is that this persistence is something we can use against the attackers to find their accesses and then improve how we respond.

This session will explore some research and practical approaches to engaging attackers once you find them. We will help you find other dependencies across their "kill chain" and then use those dependencies against them. We will wrap up with a shared brainstorming session to improve how everyone in the audience can respond when under attack.

Attendees will learn:

- Just how asymmetric being a passive defender is
- How "speaking malware" can speed up your forensics and incident response processes
- The technical and psychological benefits of attacker observation and control
- How to use the "Pyramid of Pain" visual model to find ways to make attackers' lives harder and thus increase the value of your security program

2:00 PM – 2:30 PM

A8 Vulnerability Management is NOT Dead (Despite our Best Efforts to Kill It)

Nathan Wenzler, Chief Security Strategiest, AsTech Consulting

Attendees will learn:

- Why organizations let their Vulnerability Management (VM) programs languish
- Why VM programs are a key component of a successful security program
- Common obstacles to creating a successful VM program
- Real-world case studies to help audience re-evaluate their technology to re-launch a successful VM program

VENUE & ACCOMMODATIONS

Magnolia Hotel Denver
818 17th Street, Denver, CO 80202

Cyber Security World 2017 will be held at the Magnolia Hotel Denver in Downtown Denver, CO. A block of discounted rooms at a rate of **$189.00** per night has been reserved on a space-available basis until **June 6, 2017**. To reserve your room book online by visiting **cybersecurityworld.misti.com/hotel** or call the hotel directly at **888-915-1110**. Please mention MIS Training Institute to receive the discounted block rate.

Registration Information

TO REGISTER

Online cybersecurityworld.misti.com
E-Mail customerservice@misti.com
Call 508-879-7999 ext. 501

FEES

All fees must be paid in advance in US dollars. The conference fee includes admission to sessions, all conference materials (excluding optional workshops), continental breakfasts, refreshments, lunch on Thursday and the networking reception. Workshop fees include all materials for the workshop you attend.

TEAM DISCOUNT

Register 2 and the 3rd attends at 50%!
The discount will apply to the registration of lowest value, cannot be combined with any other discount offers, and does not apply to previous registrations. Team registrations must be made and paid for at the same time by calling Customer Service.

GENERAL DISCOUNT RULES

One discount per customer (discounts can not be combined). All discount codes must be provided at the time of the registration and cannot be applied to previous registrations. The government rates are listed prices, therefore promotional discounts would apply.

CONTINUING EDUCATION CREDITS

Conference attendees are eligible to receive 14 hours of credits for the conference, and 8 for each full-day workshop.

MIS Training Institute is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

Field of Study: Information Technology

REGISTRATION DESK HOURS

The conference registration desk will be open on Tuesday, June 27 at 8:00 AM for Workshop 1 and 2 and Wednesday, June 28 at 8:00 AM for conference registration.

CANCELLATIONS, TRANSFERS AND SUBSTITUTIONS

If you can no longer attend the conference, please review the MISTI cancellation policy below and provide written notice to MISTI Customer Service at customerservice@misti.com. Cancellation policies are subject to change without notice.

- Cancellations received before May 12 will be entitled to a 100% refund less an administrative fee of $195.
- You may elect to substitute another individual from your organization for the same event at any time without incurring an administrative fee of $195. Registrations are non-transferable to other events.
- Cancellations received between May 13-June 5 will be refunded 50% of the amount paid.
- No refund will be given for cancellations received June 6 or after.

THE MISTI HIGH-YIELD/NO-RISK GUARANTEE

If you attend the conference and feel you did not benefit from it, simply tell us why on your organization letterhead and you will receive full credit toward another program.

PACKAGES	Tier 1 Until 4/30	Tier 2 5/1 - 6/19	Tier 3 after 6/19	CPEs
Cyber Security World	$1,395	$1,695	$1,995	14
Government Main Conference Discount *(main conference registration only)*	$1,255	$1,525	$1,795	14
Full-Day Workshop	$795	$795	$895	8