THREAT INTELLIGENCE SUMMIT

November 29-30, 2017 | Hyatt Regency Austin | Austin, TX

Topics We Will Address:

- Threat intelligence maturity
- Evaluating Threat Intelligence Platforms (TIP)
- Creating an automated threat intelligence system
- Managing a threat program
- Windows computer forensics
- Building an open source intel and trailhead management program
- And much more!

KEYNOTE SPEAKERS

Brian Engle
Executive Director
Retail Cyber Intelligence Sharing Center (R-CISC)

Larry Whiteside Jr.
CEO
Whiteside Security LLC

EARN 14 CPEs!

THREATINTELLIGENCE.MISTI.COM

MIS|TI™ TRAINING INSTITUTE

PLATINUM SPONSOR
digital shadows_

GOLD SPONSOR
INFOARMOR
DETECTION IS THE NEW PREVENTION

SILVER SPONSORS
DOMAINTOOLS
REVERSINGLABS

ASSOCIATION SPONSOR
OFFICIAL (ISC)² CHAPTER | AUSTIN

THREAT INTELLIGENCE

SUMMIT

Keeping up with cyber threats is a continual and time-intensive process.

Cyber threat intelligence helps organizations gain a better grasp on their threat landscape and respond to emerging threats faster and more effectively. But threat intelligence is only useful if it's real intelligence and not just data. Join your peers from across the country at our Threat Intelligence Summit to learn how you can use threat intelligence to understand the relevance of data found, the likelihood of an attack (based on the intelligence) and how your organization's security team can take action.

TECHNICAL LEVEL

○ LOW ◒ MEDIUM ● HIGH

SUMMIT AT-A-GLANCE

	Strategy	Tools, Technology and Processes
Wednesday, November 29		
8:00 AM - 9:00 AM	*Registration and Continental Breakfast*	
9:00 AM - 10:00 AM	Keynote: The Castaway's Guide for Escaping Threat Intel Island, *presented by Brian Engle*	
10:00 AM - 10:15 AM	Tech Spotlight	
10:15 AM - 10:45 AM	*Refreshment Break with Sponsors*	
10:45 AM - 11:35 AM	A1 Riding the Log Flume: Please Keep Your Policies and Procedures Inside the Company at all Times *Brian Struc* ◒	B1 A Visual Juggernaut to Solve Security Hungers *Ryan Trost & Patrick Tatro* ◒
11:45 AM - 12:30 PM	A2 Late-Breaking Session	B2 Introduction into Windows Computer Forensics *Jacquelyn Blanchard* ●
12:30 PM - 1:45 PM	*Networking Luncheon*	
1:45 PM - 2:35 PM	A3 Cultivating Intel Superheroes *Dave Ockwell-Jenner* ○	B3 Late-Breaking Session
2:45 PM - 3:30 PM	A4 Building an Open Source Intel and Trailhead Management Platform *Chris Ensey* ◒	B4: Practical Application of Network Intel for Analysts and Threat Hunters *Tim Helming* ●
3:30 PM - 4:00 PM	*Refreshment Break with Sponsors*	
4:00 PM - 4:50 PM	A5 Looking for Intel in all the Right Places *DJ Goldsworthy* ◒	B5 International Cyber Conflicts: Threats Against Critical Infrastructure *Carla Panattoni* ◒
5:00 PM - 6:00 PM	*Networking Reception with Sponsors*	
Thursday, November 30		
8:00 AM - 9:00 AM	*Continental Breakfast with Sponsors*	
9:00 AM - 10:00 AM	Keynote: Stop Buying Crap That Doesn't Help You Deal with Real Threats...Here's How, *presented by Larry Whiteside Jr.*	
10:00 AM - 10:15 AM	Tech Spotlight	
10:15 AM - 10:45 AM	*Refreshment Break with Sponsors*	
10:45 AM - 11:30 AM	Panel: Organizational Barriers to Managing a Threat Program *Moderated by Dave Ockwell-Jenner*	
11:40 AM - 12:30 PM	A6 Threat Intelligence Maturity *Edward McCabe* ○	B6 Deception: Tools and Techniques to Foil the Adversary *Pete Lindstrom* ○
12:30 PM - 1:45 PM	*Lunch on your own*	
1:45 PM - 2:35 PM	A7 OSINT: Where is My Toaster? *Anthe Koelpin* ◒	B7 Intelligence Preparation of the Battlespace and Cyber Threat Intelligence *Anthony Zech* ◒
2:35 PM - 3:00 PM	*Coffee and Dessert with Sponsors*	
3:00 PM - 3:50 PM	A8 Pragmatic Threat Intelligence *Tim Callahan* ○	B8 Achieve Higher Levels of Business Continuity Through Threat Detection and Response *Mike Adler* ◒
4:00 PM - 5:00 PM	A9/B9 TIP of the Spear: A Threat Intelligence Platform Acquisition *Jason Wonn* ◒	

SUMMIT AGENDA

Wednesday, November 29, 2017

9:00 AM – 10:00 AM

Keynote: The Castaway's Guide for Escaping Threat Intel Island

Brian Engle, Executive Director, Retail Cyber Intelligence Sharing Center (R-CISC)

The interrelated nature of essentially every business creates a connected and dependent entity that cannot operate in isolation. However, many information security organizations continue to navigate the treacherous seas of the global threat landscape from their own island of solitude. Much change is occurring in the realm of information sharing and threat intelligence.

This keynote will break down what's happening in the world of information sharing, evaluating benefits and the practical value of sharing and collaboration as it relates to threat intelligence and cybersecurity defenses. From strategic decision support to tactical threat mitigation, let's move past the message in a bottle approach and look at information sharing as the raft we use to escape from Threat Intel Island.

This keynote will:

- Dispel rumors and dogma surrounding threat intelligence
  - "Actionable" in the context of capability
  - Acquiring threat intelligence as a commodity instead of approaching it like a process
  - Fast, good and cheap apply, and none of the above may be what you get
- Discuss considerations for automation
  - The context dilemma: lightweight, bite-sized intel at wire speed lacks the story needed to provide intelligence
  - More indicators; faster, is not alone the answer to your threat intelligence questions
- Purpose-driven information sharing
  - Our maps may not be great, so let's chart a course for threat intelligence together before we set sail
  - Back to the basics—let's use collaboration to analyze our threat model, and information sharing to solve some problems

10:00 AM – 10:15 AM

Tech Spotlight

10:45 AM – 11:35 AM

A1 Riding the Log Flume: Please Keep Your Policies and Procedures Inside the Company at All Times ◒

Brian Struc, Senior Information Security Analyst, First Command Financial Planning

Every organization is unique in its combination of services, culture, policies, compliance, risk acceptance and concern criteria. In this regard, system logs can provide an invaluable service to an entire organization when implemented systematically and logically. Value is best obtained via large initial effort, understanding the various components, meaningful correlation and effective reduction.

This presentation will provide a guideline to obtain and implement a business-specific solid foundation of intelligent analysis leading to a cost-effective, enhanced in-house solution or migration to a managed solution.

You will learn:

- Best practice recommendations for effective log management
- The value of extensive planning prior to implementation
- How to improve performance, compliance, and communication across the entire organization

10:45 AM – 11:35 AM

B1 A Visual Juggernaut to Solve Security Hungers ◒

Ryan Trost, CTO, ThreatQuotient

Patrick Tatro, Cyber Intelligence

Security visualizations continue to be an Achilles heel for the industry because cyber analysts aren't visualization experts and visualization experts aren't cyber analysts. Histograms, sparklines, spider graphs, time-series, link-analysis, box-plots, parallel coordinates, etc. cater to very pointed security use cases but none of them allow for viewing overlapping datasets—a fundamental concept in correlation.

However, a new revolutionary framework developed by Harvard is tearing down obstacles from C-Levels to analysts! The framework provides executives with a point-in-time summary of the organization's security posture by highlighting the intersections of threat landscapes, peripherals and "ammunition inventories." It also offers analysts a way to find overlap across cyber disciplines—intelligence collection, situational understanding, malware fingerprinting, or adversary attribution.

This new capability will provide a huge leap forward for the security industry and help hone the tradecraft.

11:45 AM – 12: 30 PM

A2 Late-Breaking Session

11:45 AM – 12: 30 PM

B2 Introduction into Windows Computer Forensics ●

Jacquelyn Blanchard, Computer Forensic Examiner, Lockheed Martin

We hear about cyber breaches and attacks in the news daily, but once an attack is discovered, there is more to it than the public announcement and damage control. In most cases, even before the public hears about the incident, the company has called in a Digital Forensic Incident Response (DFIR) professional. What are DFIR professional's responsibilities? What exactly are they looking for? How do they assist the organization? If your organization is the affected victim, do you have the forensics capabilities in house to perform these duties?

During this presentation, Jacquelyn Blanchard will share basic tools and methods you can use to analyze a forensic image of a Windows host to identify a computer intrusion.

You will learn:

- How to scratch the surface of forensics
- How to properly document findings
- How to acquire an image and review it for indicators of compromise
- About free and commercial tools you can use to conduct an analysis

1:45 PM – 2:35 PM

A3 Cultivating Intel Superheroes ◒

Dave Ockwell-Jenner, Senior Manager, STORM and CISO, SITA

Unless you are lucky enough to inherit a ready-made threat intelligence team, one of the first problems you need to solve is how to stand up a team and get them productive as quickly as possible.

In this session, SITA's Dave Ockwell-Jenner will walk through some of the options available, and share the lessons learned in building SITA's Threat Intelligence capability. Specifically, he will focus on how to leverage your existing security and IT talent to cultivate your own threat intelligence superheroes!

1:45 PM – 2:35 PM

B3 Late-Breaking Session

2:45 PM – 3:30 PM

A4 Building an Open Source Intel and Trailhead Management Platform ◒

Chris Ensey, COO, Dunbar Armored

This talk will focus on using threat intelligence feeds along with open source technologies to enable rapid detection, investigation and response in real time to network and end user based threats.

Chris Ensey is the co-creator of the Cyphon open source incident management platform, and the leader of Dunbar's cybersecurity division. His team has been leveraging threat intel from both closed and open sources within their MSSP platform. Attend this talk to hear an overview of how tools like snort, bro NSM and Cyphon can be combined with threat intelligence to better manage the incident response process.

You will learn:

- Centralizing trailhead management in a team environment
- Making threat intelligence work with network security tools
- Fundamentals of correlation across multiple sources
- Simple steps to get started with free and open source technologies

2:45 PM – 3:30 PM

B4 Practical Application of Network Intel for Analysts and Threat Hunters ●

Tim Helming, Director, Product Management, DomainTools

Threat intelligence and hunting hold great potential for helping network defenders block adversaries who have not yet breached them, and finding evidence of those who may have. While external threat intel feeds can be great, most organizations are also sitting on a potential gold mine of useful forensic data. However, making practical and impactful use of the data can be tricky. It doesn't have to be.

Tim Helming will demonstrate straightforward methods and data sources to strengthen your security posture without breaking the bank, using real-world examples of network and DNS-based threat hunts that expose attack campaign infrastructure. The talk concludes with a simple 5-point checklist you can apply immediately to begin your organization's threat intel evolution.

4:00 PM – 4:50 PM

A5 Looking for Intel in all the Right Places ◒

DJ Goldsworthy, Director, Security Operations and Threat Management, AFLAC

Whether you already have a mature threat intelligence program or are looking for a place to start, join this session to discover sources of intelligence that may be at your fingertips, and the methods to incorporate them into an automated threat intelligence system.

You will learn:

- Where to find excellent external sources of threat intelligence data
- How to glean intelligence from your own cloud and on-premise solutions
- How to turn threat intelligence into successful preventative and detective controls

4:00 PM – 4:50 PM

B5 International Cyber Conflicts: Threats Against Critical Infrastructure ◒

Carla Panattoni, Risk & Threat Analyst, Intelligence Monitoring & Reporting Program, University of Washington

Cybercrime and cyber warfare exploit computer networks and computing devices to cause harm and compromise critical infrastructure sectors, such as financial, energy, commercial, public healthcare, transportation and water. This research presents the psychopathologies of why people commit crime; the challenges with anonymity; and how cyber adversaries, such as the Islamic State in Iraq and al-Sham, promote strategic and fundamental objectives (Siebert, Von Winterfeldt and John, 2016).

Although the Combined Joint Task Force—Operation Inherent Resolve—has reduced terror organization's military command and control, a cyber presence remains. The principles of trust and confidence building measures will also be presented.

Thursday, November 30, 2017

9:00 AM – 10:00 AM

Keynote: Stop Buying Crap That Doesn't Help You Deal with Real Threats...Here's How

Larry Whiteside Jr., CEO, Whiteside Security LLC

Organizations are spending millions of dollars on technology that is not helping them stop the threats they face on a daily basis. Why does this practice continue? This talk will discuss why and how to stop it moving forward.

Attend this keynote to learn:

- Trends in security technology spending (and why following trends can be a detriment to your business)
- Simple ways to avoid spending inappropriately
- Why we have failed thus far as an industry
- Techniques and tactics that will help you select the right tools to protect your business

10:00 AM – 10:15 AM

Tech Spotlight

10:45 AM – 11:30 AM

Panel: Organizational Barriers to Managing a Threat Program

Moderated by Dave Ockwell-Jenner, Senior Manager, STORM and CISO, SITA

11:40 AM – 12:30 PM

A6 Threat Intelligence Maturity ◒

Edward McCabe, Co-Founder & Principal, Rendition InfoSec LLC

How do you know you're doing the right thing when it comes to threat intelligence? How do you know you're growing your threat intelligence capabilities?

We've all heard the old adage, "you can only manage what you can measure," but what does that really mean? What should you be measuring, and how? Attend this talk to take a peek behind the curtain and learn about a soon-to-be-released method of improved threat intelligence management! The goal of this presentation is to share and review how threat analysts can show (and measure!) demonstrable growth in our threat intelligence programs.

You will learn:

- Threat intelligence process life-cycle
- Threat intelligence process goals
- Threat intelligence process areas
- Threat intelligence tasks
- Threat intelligence management program integration

TECHNICAL LEVEL
○ LOW ◒ MEDIUM ● HIGH

11:40 AM – 12:30 PM

B6 Deception: Tools and Techniques to Foil the Adversary ○

Pete Lindstrom, Vice President of Security Research, IDC

In the security field, we often lament "security through obscurity" as a crutch for folks who don't want to put in the hard work of really securing an enterprise. But the time has come to rethink obscurity from a deception perspective. Enterprises today may increase the confidence of detection, limit the impact of a compromise, or otherwise benefit their program using deception techniques. This session will describe the philosophy, fit it into our existing security models, and identify various tools and techniques for success.

You will learn:

- Why using deception techniques may increase confidence or limit the impact of a compromise
- The philosophy of a deception program

1:45 PM – 2:35 PM

A7 OSINT: Where is My Toaster? ◒

Anthe Koelpin, Senior Threat Analyst, GE Digital

In an interconnected world, not every device connected to the internet was actually meant to be connected. This presentation will describe our journey to find and identify connected devices, the pitfalls, the risks, legal considerations and the pain to make it actionable.

You will learn:

- Challenges and risks to finding your internet-connected devices/services with OSINT tools
- Some OSINT tools and their basic differences
- What you can legally do with your findings
- How to obtain actionable intel for your end goal

1:45 PM – 2:35 PM

B7 Intelligence Preparation of the Battlespace and Cyber Threat Intelligence ◒

Anthony Zech, Data Security Consultant, Cargill

Much of today's work in cyber intelligence ignores proven traditional intelligence processes—processes that correlate to frameworks like the CIS's Top 20 Critical Security Controls. Answers and context for many of your security issues, including some you may not know about, can be found by conducting a process in U.S. Military doctrine called Intelligence Preparation of the Battlespace (or Joint Intelligence Preparation of the Environment). This talk steps you through Intelligence Preparation of the Battlespace and explains how it relates to objectives, terrain and threats that allow intelligence sections to provide context and ensure your organization's security.

You will learn:

- In any security environment, prioritization of resources to match business objectives is paramount to avoid wasting efforts
- Understanding your environment is critical to any analytical effort
- Intelligence Preparation of the Battlespace (IPB) is a structured process that methodically relates business objectives to environment to threat activity to enable effective decision making
- The five-step process for IPB

3:00 PM – 3:50 PM

A8 Pragmatic Threat Intelligence ○

Tim Callahan, Senior VP, Global Chief Security Officer, AFLAC

When a company is considering the implementation of a threat intelligence program, there are many questions. What is threat intelligence? How will we know when we are successful? What are the benefits to demonstrate the value to leadership? How much will it cost and will I be creating a money pit? These are all valid questions that must be answered if a program is to get the support needed.

This presentation will define threat intelligence, share how to recognize intelligence and sources, demonstrate ways to gather data and offer practical and proven tips in implementing and operating a threat intelligence program.

3:00 PM – 3:50 PM

B8 Achieve Higher Levels of Business Continuity through Threat Detection and Response ◒

Mike Adler, VP Product, RSA NetWitness

This session will explain how the right combination of processes and technologies can be effective in protecting an organization. The speaker will demonstrate how to defend your organization with optimal efficiency, know with confidence whether a breach has occurred, understand the damage caused, and respond rapidly.

You will learn:

- Current requirements for organization to protect themselves against cyberattacks and remediate when they occur
- What combination of people, process and technologies are needed to build a successful SOC
- Know with confidence whether a breach has occurred, understand the damage caused

4:00 PM – 5:00 PM

A9/B9 TIP of the Spear: A Threat Intelligence Platform Acquisition ◒

Jason Wonn, Principal Security Specialist, Cyber Trends, Walt Disney Co

Military organizations have long known of the value of intelligence, but commercial entities only realized its importance in the last five years. Cyber Threat Intelligence (CTI) recently became a priority for the average commercial company which now requires a threat intelligence analysis capability. Are you a security-geek like Jason Wonn, who was recently hired to provide that world-class CTI program for your company with very little time and an even smaller budget? … Good luck with that! Jason cannot present that solution in an hour, but he will guide you through the process to evaluate a Threat Intelligence Platform (TIP) and discuss how he made the metrics meaningful to the executives. In this talk, discover the benefits of employing a TIP and the technical evaluation of a TIP through requirements development to ensure it is measurable and meaningful to your leadership.

You will learn:

- The definition of and process to evaluate a Threat Intelligence Platform (TIP)
- TIP benefits: preventing analyst overload, enriching IoCs and creating organizational intelligence
- How to choose the right TIP for your organization: needs assessment, requirements building

INTERESTED IN SPONSORING THREAT INTELLIGENCE SUMMIT 2017?

CONTACT OUR SALES DIRECTOR:

Adam Lennon
646-590-4557
alennon@misti.com

VENUE & ACCOMMODATIONS

Hyatt Regency Austin
208 Barton Springs, Austin, Texas, 78704

Threat Intelligence Summit 2017 will be held at the **Hyatt Regency Austin in Austin, Texas**. A block of discounted rooms at a rate of **$219.00** per night has been reserved on a space-available basis until **November 6, 2017**. To reserve your room call the hotel at **(512) 477-1234**. Please mention MIS Training Institute to receive the discounted block rate.

REGISTRATION INFORMATION

TO REGISTER

Online threatintelligence.misti.com
Call 508-879-7999 ext. 501
E-mail customerservice@misti.com

FEES

All fees must be paid in advance in US dollars. The summit fee includes admission to sessions, all conference materials, continental breakfasts, refreshments, lunch on Wednesday and the networking reception.

TEAM DISCOUNT

Register 2 and the 3rd attends at 50% OFF!

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.

NATIONAL REGISTRY OF CPE SPONSORS

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 summit registration desk will be open on Wednesday, November 29 at 8:00 AM for summit registration.

CANCELLATIONS, TRANSFERS AND SUBSTITUTIONS

If you can no longer attend the Threat Intelligence Summit, 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 October 13 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 October 13-November 6 will be refunded 50% of the amount paid.
- No refund will be given for cancellations received after November 7.

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	Early Bird Before 10/1	Standard 10/1 - 11/27	Onsite	CPEs
Threat Intelligence Summit	$1,395	$1,795	$1,995	14
ISACA & ISSA Member Discount *(summit registration only)*	$1,255	$1,615	$1,705	14