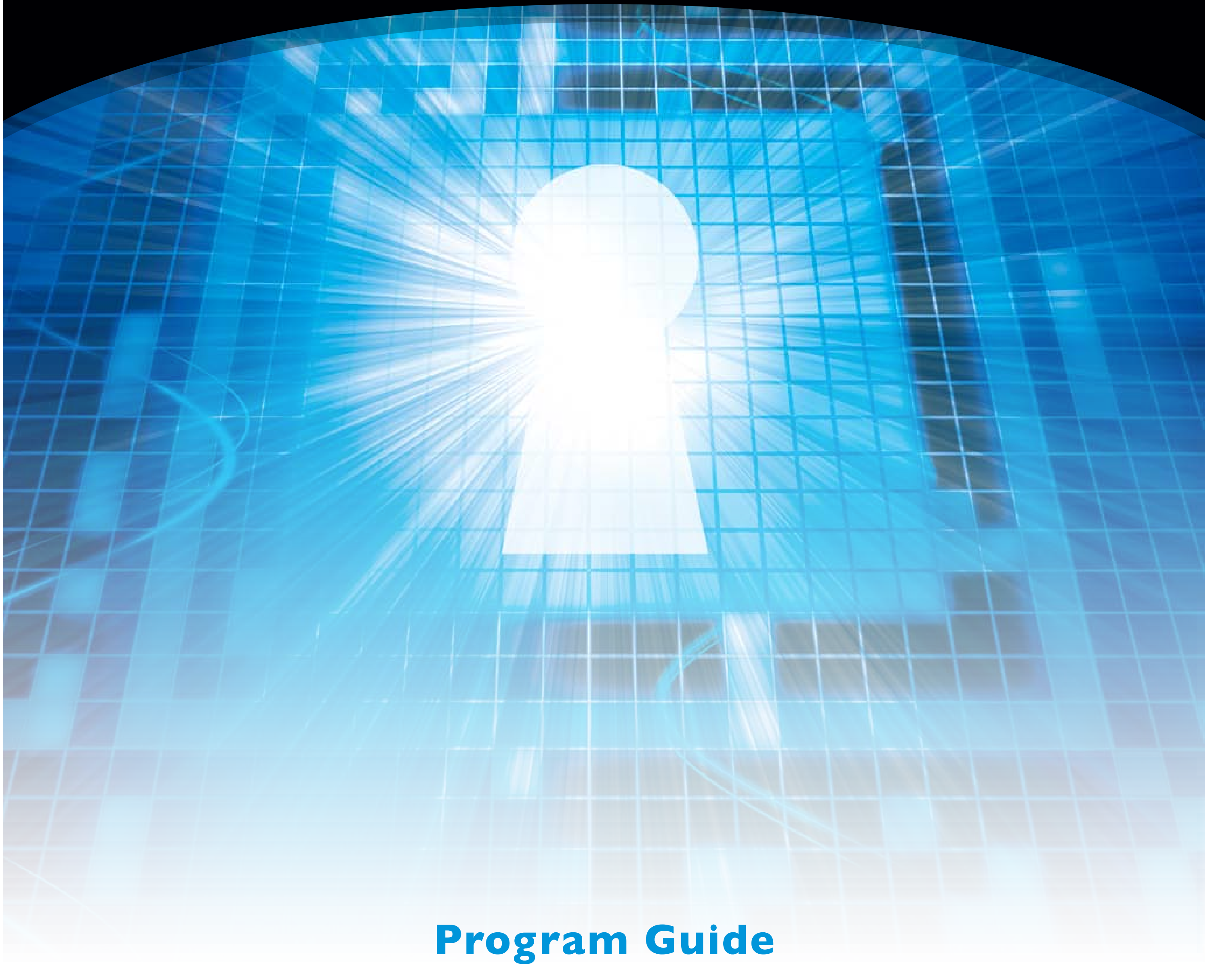
SANS Security Operations Center SUMMIT



Program Guide

Summit Co-Chairs: Dr. Eric Cole and Jim Goddard

#SOCSummit

@SANSDefense @SANSForensics

Agenda

All Summit Sessions will be held in the Potomac Ballroom (unless noted).

Summit presentations will be posted via the following URL, ***http://cyber-defense.sans.org/resources/summit-archives****,*
typically within five business days of the Summit. An email will be sent to all attendees once live.

Portions of the Summit may be video-recorded. These videos may be used for marketing or other purposes, but will not be available for distribution or viewing on demand at this time.

Thursday, April 30

7:45 - 8:45am

Registration & Coffee
(LOCATION: POTOMAC FOYER)

8:45 - 9:30am

Key Strategies for Running a World Class Security Operations Center

Dr. Eric Cole*, Fellow, SANS Institute*

SOC is the latest buzz word, and most organizations are setting up, deploying or outsourcing a SOC in order to better address current and future threats. However, just because an organization has a room called a SOC does not mean it is functioning correctly and doing everything that is should. Dr. Cole, a world renowned security expert, has built, evaluated and run a wide variety of SOCs and will pull out his "secret book" and share the strategies that differentiate a world-class SOC from an inefficient room that contains computers. After evaluating over 55 different SOCs, Dr. Cole started noticing patterns that all world-class SOCs have in common. He also noticed that none of the SOCs that were failing were implementing these strategies. Over a decade, he has developed strategies that he usually only shares with his clients, but during this keynote he will give you the checklist that you can use to determine if your SOC has what it takes.

9:30 - 9:50am

Networking Break & Vendor Expo
(LOCATION: POTOMAC FOYER)

9:50 - 10:35am

Building the Team for a Successful SOC

Donald Warnecke*, Lead - IT Operations Technology (OT) Security, Consumers Energy*

In the battle over your network, you have three broad weapons: your policies, your technologies, and your people. Time and time again, the success or failure of your SOC will be determined by the people who are tasked with finding the interlopers on your network. Whether you are building, improving, or maintaining a SOC, your human capital is a critical component that requires your attention. During this talk, we will discuss the mission of the SOC, keeping the right people engaged, and ensuring that your team works as one.

10:35 - 11:15am

Hunting Your Adversary – How to Operate and Leverage an Incident Response Hunt Team

Rob Lee*, Fellow, SANS Institute*

Over 80% of all breach victims learn of a compromise from third-party notifications, not from internal security teams. In most cases, adversaries have been rummaging through your network undetected for months or even years. Incident response tactics and procedures have evolved rapidly over the past several years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in your enterprise; they are compromising hundreds.

To counter this, many incident response teams are either responding for incidents or hunting for the next ones. As a result, Incident Response Hunt teams have become a dedicated component to most modern SOCs. Incident response techniques that collect, classify, and exploit knowledge about these adversaries – collectively known as cyber threat intelligence – enable network defenders to establish a state of information superiority that decreases the adversary's likelihood of success with each subsequent intrusion attempt. Learn how IR/Hunt teams are formed, operate, best practices, and how they engage their targets across the enterprise.

Learn how to hunt your adversaries or simply become another victim.

11:15am - Noon

Using Managed Security Services to Deliver or Augment Your SOC Functions

MODERATOR:
John Pescatore*, Director of Emerging Security Trends, SANS Institute*

PANELISTS:
Randy Conner, *GSLC, GCPM, CISM, CISSP, PMI PMP*
Stephen Coty*, Chief Security Evangelist, AlertLogic*
Jeff Schilling*, Chief Security Officer, FireHost*

For many organizations building and staffing a SOC in-house is just not feasible. There are a variety of options available, from completely outsourcing SOC functionality to hybrid/shared management approaches to temporary or tactical "insourcing" of a few critical areas.

This panel will explore these options and answer your questions about what approach makes the best business and security sense for your organization.

Noon - 1:15pm

Lunch Break

1:15 - 2:00pm

Maximizing the SOC: Operator-Driven Solutions

MODERATOR:
Dr. Eric Cole*, Fellow, SANS Institute*

CONFIRMED PANELISTS:
Brandon Cass*, Manager, IT Security Operations Center & Investigations, Texas Instruments*
Jack Crook*, Senior Incident Handler, General Electric*
Robert Maxwell*, Security Operations Manager, University of Maryland College Park*

It is important to have a security operations center (SOC) to continuously monitor metrics, but the real question is whether you are designing and configuring the SOC in a way that it is operational. Engineers running the SOC need to ultimately drive the components that need to be delivered. In this interactive panel, the audience will have a chance to learn from actually user/operators of a SOC to share what is most important to them.

2:00 - 2:45pm

Building Out a SOC

***Randy Marchany**, CISO, Virginia Tech*

This talk discusses the components that need to be in place to build a SOC. Some of the components include your Continuous Monitoring, sensitive data protection and policy structure. This presentation shows examples of how these components can be built using existing information and tools within your organization.

2:45 - 3:05pm

Networking Break & Vendor Expo

(LOCATION: POTOMAC FOYER)

3:05 - 3:45pm

Top 10 Dashboards

***Craig L. Bowser**, Sr. Security Engineer, Dept. of Energy*

Dashboards are a critical capability of a Security Information Event Monitor (SIEM) as they are able to display the near real time status of the health, operational availability, security posture and compliance level of networks of all sizes. While there are numerous papers, blog posts and examples of dashboards that provide deep insights, specific security alerts or complicated compliance metrics for your network, I wanted to create a list of dashboards that provided a solid starting point for Security Operation Centers to use when they installed their first SIEM. These are suggested quick-win, industry-agnostic dashboards which were chosen because of their ease of implementation and simple graphical presentation that provide SOC personnel an initial view into the security posture of a network.

3:45 - 4:30pm

Extreme Makeover: Metrics Edition

***Mary N. Chaney**, Esq., CISSP, Director – Security Operations Center, Johnson & Johnson*

In this talk, attendees will learn the difference between informative and actionable metrics, when to use them, and how to create scorecards for different parts of the organization based on the same underlying metrics. In addition, attendees will learn why stakeholder engagement is important to include in metrics.

4:30 - 5:15pm

Intelligence-Driven Approaches to False Positive Reduction

***Mike Cloppert**, CIRT Chief Research Analyst, Lockheed Martin*

One of the biggest challenges to the operation of a SOC is management of false positives (FPs). FP reduction is critical to avoid analyst desensitization and improve the overall quality of detection and response, and can have a major impact in the effectiveness of your organization's overall network defense posture. This talk, will discuss techniques for applying threat intelligence models, methodologies, and data to your SOC's transactional feeds in a way that will help reduce false positives and better prioritize the remaining events.

Thank you for attending the SANS Summit.

**Please remember to complete your evaluations for today.
You may leave completed surveys at your seat
or turn them in to the SANS registration desk.**

Friday, May 1

8:00 - 8:30am

Registration & Coffee

(LOCATION: POTOMAC FOYER)

8:30 - 9:15am

Getting Executive Support for a SOC

***Jim Goddard**, Executive Director, Security Monitoring and Incident Response, Kaiser Permanente*

A security operations center requires significant investment in people, process and technology over a long period of time. Attention spans can be short, so gaining initial executive commitment is not enough. For a SOC to achieve its goal, you have to not only gain initial interest but maintain it for the duration. This talk, based on best practices developed during the creation of the SOC at Kaiser Permanente, will describe practices for not only getting executives excited about a SOC but also maintaining and growing interest.

Topics we will cover include:

- How much investment is really needed
- Timing and trust
- Managing expectations
- Translating security value for non-technical executives
- Incremental wins and success metrics
- Making the SOC sticky

9:15 - 10:00am

Building a SOC: Lessons from Industry

MODERATOR:

***Jim Goddard**, Executive Director, Cyber Risk Defense Center, Kaiser Permanente*

PANELISTS:

***Nick Essner,** Sr. Manager, Global SOC/CIRT Lead, Mandiant, a FireEye Company*
***Curley Henry**, Practice Manager – Americas, HP*
***Dave McGinnis**, Associate Partner, Security Operations Optimization, IBM Security Services*

What does it take to build the people, process and technology that makes up a successful SOC. Industry experts will discuss lessons they learned along the way. Topics will include:

- Where to hire, what to contract
- Why some succeed and others fail
- How to manage your vendors
- How to find staff
- Tools analysts need
- Coverage models
- Technology criteria
- Critical processes

10:00 - 10:20am

Networking Break & Vendor Expo

(LOCATION: POTOMAC FOYER)

10:20 - 11:00am

Threat Detection and Response Control Point Management: Developing a Visibility and Measurement Platform that Manages and Improves Operations

***Nancy Thompson**, CISSP, CRISC, Director of Operations, Cyber Risk Defense Center,*
Cyber Security/Technology Risk Office, Kaiser Permanente

Kaiser Permanente has adopted an approach for threat detection and analysis which aligns our teams to the Cyber Kill chain. With an approach that does not follow the traditional "level one, level two" security operations center model, we required a new approach towards case management. This talk will review what we faced, why we made the decisions we did and the benefits we receive by satisfying our requirements with a generic work flow platform.

11:00 - 11:45am

Metrics: Beyond ROI

***Shawn Chakravarty**, Senior Manager of Security Incident Response, PayPal*
***Kevin Tyers**, Network Security Engineer, PayPal*

Information security is most effective when decisions are based on facts. Metrics provide the story around those facts. Metrics provide a story to the audience with those facts. When done properly, metrics provide direction, business justification, and proof of ROI. They can also be a motivating force for a security organization achieving greater effectiveness. Conversely, poor or nonexistent metrics can severely hinder a security organization's performance and longevity. In this talk, Shawn Chakravarty and Kevin Tyers will share their experiences with developing, using, and presenting metrics to business users of all levels.

11:45am - 1:00pm

Lunch Break

1:00 - 1:45pm

Building Value Across the Enterprise

***David Nathans**, Author, Designing and Building a Security Operations Center*

The security operations center is filled with activity focused on monitoring and managing countless devices that generate millions, if not billions, of events per day. Security practitioners in these types of environments are keenly aware of the threats to an enterprise and the potential impacts on a daily basis. The growing threats and impending doom the SOC is designed to protect and defend against don't always get met with more staff and resources. The SOC needs to find ways to build value across organizational boundaries and make security part of everyone's day. This talk will explore ways to build extended teams, maximize the value of the SOC across the enterprise and ultimately win executive support.

1:45 - 2:30pm

10 Biggest Mistakes in Implementing Continuous Monitoring

***Ismael Valenzuela**, Lead, Foundstone IR/Forensics; Technical Practice Manager, Intel Security & Community SANS Instructor*

Organizations are investing more time, money and people than ever to combat cyber threats and prevent cyber attacks, but despite this tremendous effort, the number of compromised organizations and the cost of these breaches is ramping up quickly. How can you make sure you are doing your best to avoid the same mistakes that seem to be at the root of most of these breaches?

In this talk, Ismael Valenzuela will share the facts, flaws and foibles that are common to these crises, and how you can avoid them using a better approach to continuous monitoring and security operations to ultimately increase your detection and reaction capabilities and prevent a next-time.

2:30 - 3:15pm

Using Threat Intel to Improve the Efficiency of Your SOC

MODERATOR:

***John Pescatore**, Director of Emerging Security Trends, SANS Institute*

PANELISTS:

***Paul Alderson**, Chief Technical Analyst - Production & Analysis, iSIGHT Partners, Inc.*
***Dr. Paul Vixie**, CEO and Chairman, Farsight Security, Inc.*
***Andrew Wild**, CISO, Lancope, Inc.*

To deliver high levels of security and business value, the most mature Security Operations Centers use a mix of skilled people, repeatable processes and technology/automation. Security products and tools can be force multipliers, freeing up SOC analysts for higher value tasks. This panel will present lessons learned from users of conference sponsors' products as part of advanced SOC operations.

3:15 - 3:30pm

Networking Break & Vendor Expo

(LOCATION: POTOMAC FOYER)

3:30 - 4:15pm

Certification and Training in the SOC

***Courtney Imbert**, Information Security Engineer - Exam Development, GIAC*
***Jeff Pike**, Director of Technology, GIAC*

Does the existing ecosystem of certification and training options fit the needs of the SOC? Is there a need for training and/or certifications tailored specifically to the SOC environment? This talk will explore those questions. The first half of the talk will set the stage for Summit attendees to share their viewpoints with the Global Information Assurance Certification (GIAC) and potentially impact future offerings.

4:15 - 5:00pm

After the Breach: 4 Years of Lessons Learned

***Garrett Schubert**, EMC CIRC Manager, EMC Corporation*

Four years after the RSA breach, Garrett Schubert shares lessons learned from the EMC CIRC, including what they learned about building better IR teams.

5:00 - 5:15pm

The Future of Security Operations Centers

***Dr. Eric Cole**, Fellow, SANS Institute*

Dr. Cole will provide a final dose of perspective on all the case studies, ideas and best practices of the past two days, and send you back to work excited about taking your SOC to the next level.

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat
or turn them in to the SANS registration desk.

EXHIBITORS

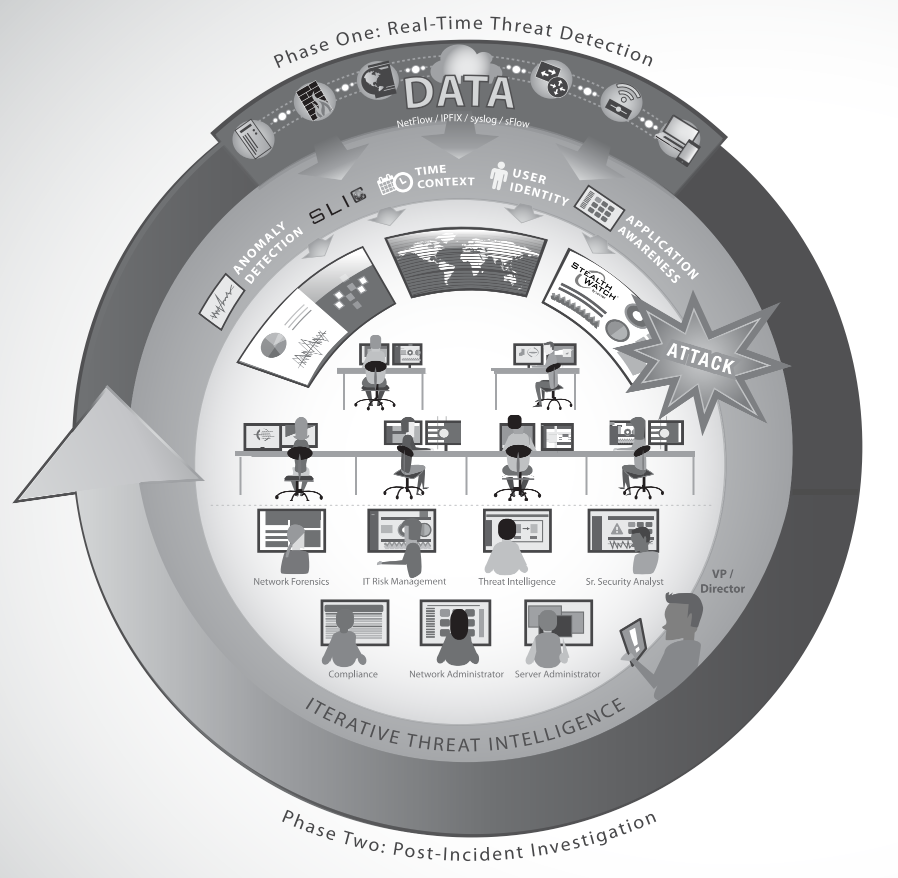
CYBERARK®

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 protect against cyber threats before attacks can escalate and do irreparable business damage.

Lancope®

Lancope, Inc. is a leading provider of context-aware security for real-time insider threat detection, incident response and forensic investigations. As part of Cisco's Cyber Threat Defense solution, Lancope's StealthWatch System transforms the network into a virtual sensor grid for obtaining continuous network visibility and security intelligence to reduce agency risk and assists with compliance to Federal policies. Armed with pervasive network insight, organizations can better protect against APTs, DDoS, zero-day malware and insider threats. Lancope's security capabilities are continuously enhanced with cutting-edge research from StealthWatch Labs. For more information, visit **www.lancope.com**.

ManTech
International Corporation®



SANS Summit

UPCOMING SUMMITS & TRAINING EVENTS

SANS/NH-ISAC Healthcare Cybersecurity SUMMIT & TRAINING
Atlanta, GA | May 12-19

Industrial Control Systems TRAINING
Houston, TX | Jun 1-6

Digital Forensics & Incident Response SUMMIT & TRAINING
Austin, TX I Jul 7-14

Cyber Defense SUMMIT & TRAINING
Nashville, TN | Aug 11-18

Security Awareness SUMMIT & TRAINING
Philadelphia, PA | Aug 17-25

Law Enforcement Cyber TRAINING
Dallas, TX | Sep 21-26

Pen Test Hackfest SUMMIT & TRAINING
Washington, DC | Nov 16-23

For more information on speaking at an upcoming summit or sponsorship opportunities, e-mail SANS at **summit@sans.org**.

Visit **sans.org/summit** for detailed summit agendas as they become available.

#SOCSummit @SANSDefense @SANSForensics

Austin, TX SUMMIT: July 7-8 | TRAINING: July 9-14

SANS DFIR 2015

SAVE $400 on any course by paying before May 20th
SAVE $500 when combining any course with the Summit

The Premier Digital Forensics and Incident Response Training and Summit

Check out these top 4 reasons to attend:

1. **DFIR-Focused Training**
   Six DFIR courses with top-rated instructors
2. **Summit Talks**
   Two days of session talks with industry experts
3. **DFIR NetWars**
   FREE when you register for a DFIR course
4. **Networking**
   Endless networking opportunities

Courses to choose from:

SEC504: **Hacker Tools, Techniques, Exploits, and Incident Handling** Bryce Galbraith

FOR408: **Windows Forensic Analysis** Chad Tilbury

FOR508: **Advanced Digital Forensics and Incident Response** Rob Lee

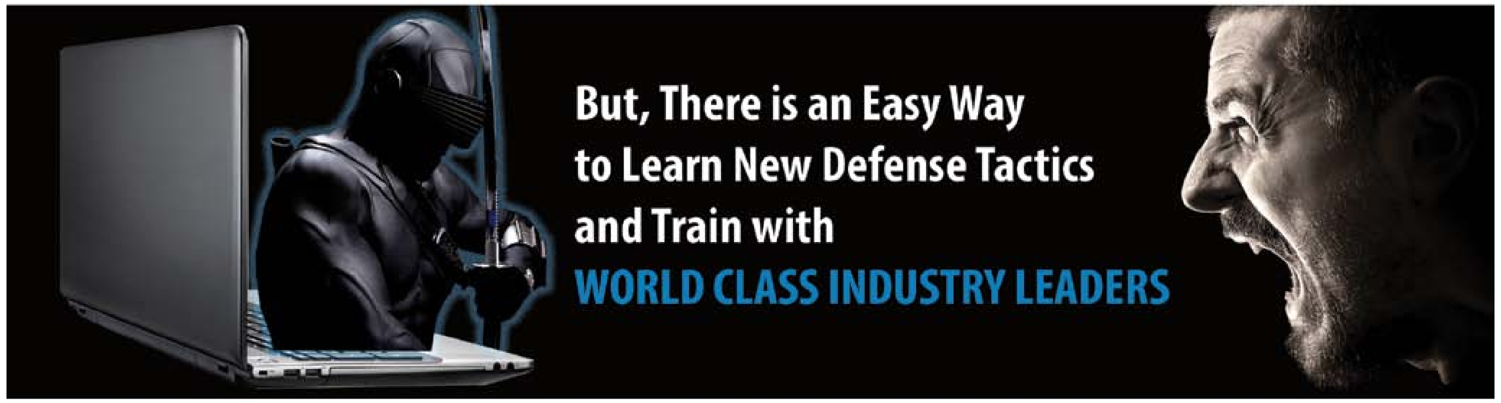
FOR526: **Memory Forensics In-Depth** Alissa Torres

FOR572: **Advanced Network Forensics and Analysis** Philip Hagen

FOR610: **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** Hal Pomeranz

Register today **sans.org/event/digital-forensics-summit-2015** **#DFIRSummit**

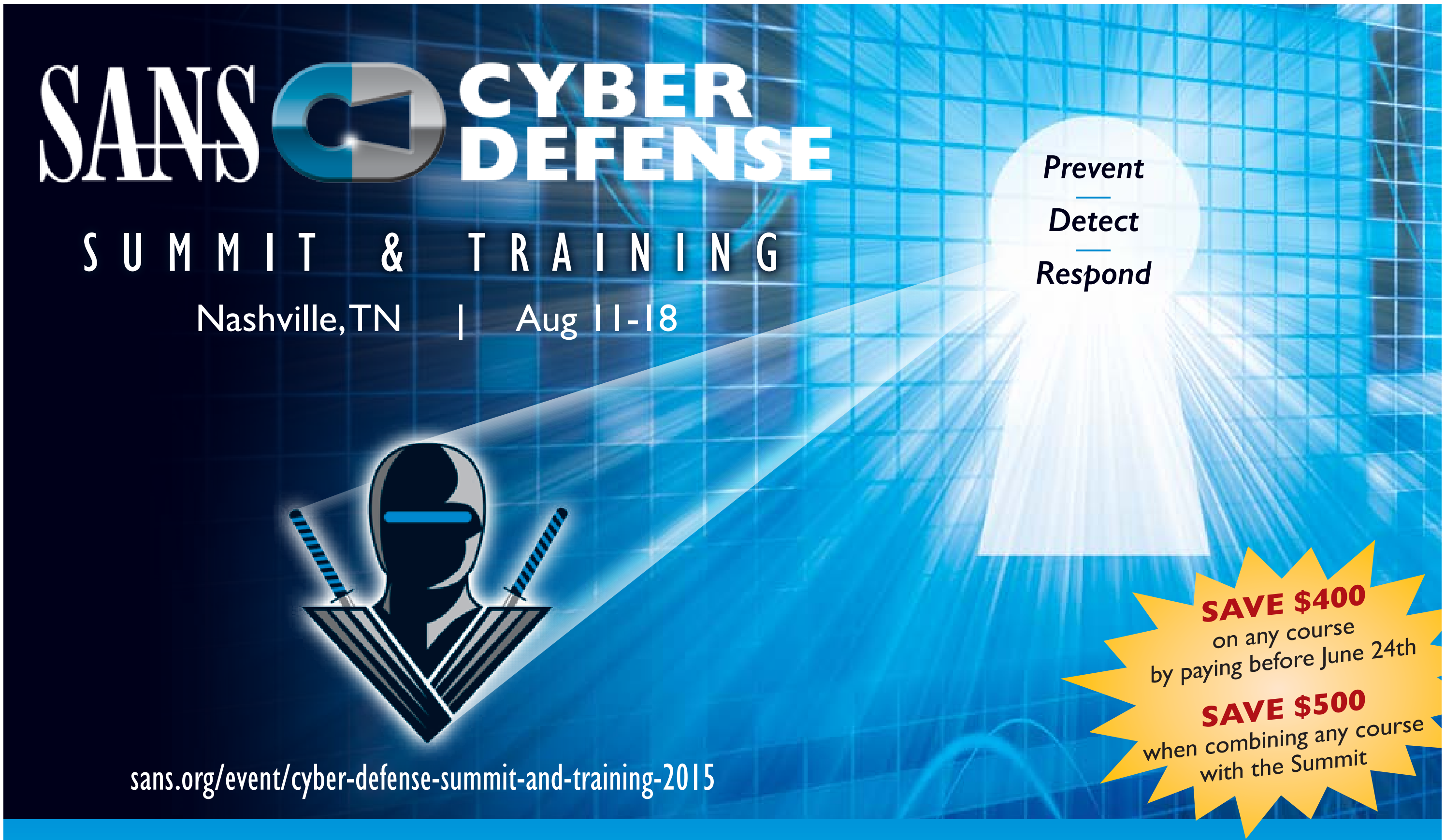
When it Comes to Defending There is no EASY Button


But, There is an Easy Way
to Learn New Defense Tactics
and Train with
WORLD CLASS INDUSTRY LEADERS

SANS CYBER DEFENDERS

The Cyber Defense Curriculum at SANS Institute
The Foremost Authority in Cyber Security Training
Train the Way you Learn
Live| OnDemand | vLive

Cyber-defense.sans.org Follow us on Twitter @sansdefense



SANS CYBER DEFENSE

SUMMIT & TRAINING

Nashville, TN | Aug 11-18

SAVE $400 on any course by paying before June 24th

SAVE $500 when combining any course with the Summit

sans.org/event/cyber-defense-summit-and-training-2015

Learn the essential skills and techniques needed to protect and secure an organization's critical information assets and business systems at the Cyber Defense Summit & Training. Hear real-life success stories, best practices, and tips that are immediately actionable at the Summit. And choose from 5 technical courses that will teach you the essential skills and techniques needed to play winning defense to protect and secure your organization.

Courses to choose from:

SEC401: Security Essentials Bootcamp Style
Dr. Eric Cole

SEC503: Intrusion Detection In-Depth
Jonathan Ham

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
Adrien de Beaupre

SEC511: Continuous Monitoring and Security Operations
Eric Conrad

SEC566: Implementing and Auditing the Critical Security Controls - In-Depth
Randy Marchany

Register Today to receive the training and knowledge you need to advance your career.
sans.org/event/cyber-defense-summit-and-training-2015

#CyberDefSummit @SANSDefense