SANS Security Operations Center

SUMMIT

Program Guide

@SANSDefense

#SOCSummit

Mary N. Chaney

Ismael Valenzuela

Welcome to the **Security Operations Center Summit**! We are so excited to be part of this event dedicated to addressing the challenges of establishing effective security operations. Over the next two days, top experts will present case studies to help you identify gaps in your SOC, use threat intelligence effectively, and develop meaningful metrics to define your SOC's success. Our goal is for you to be able to take what you learn here and use it to better secure your organization.

We have information security professionals from all over the country with many different backgrounds and experiences. Take this opportunity to introduce yourself to those sitting around you and join one of the many conversations during the networking breaks. Attendees tell us time and again that the greatest value of a Summit is the plethora of newly forged or deepened industry connections made during their time with us.

Finally, let's have fun! Engage with our expert speakers during the breaks, ask questions during the Q&A sessions, and weigh in on Twitter **#SOCSummit**. Your participation is what makes the Summit a truly wonderful and unique event.

Sincerely,

Mary N. Chaney
Ismael Valenzuela
SOC Summit Co-Chairs

Agenda

All Summit Sessions will be held in the Crystal Ballroom Salon A&B (unless noted).

All approved presentations will be available online following the Summit at
http://cyber-defense.sans.org/resources/summit-archives
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Wednesday, May 25	
8:00-9:00am	**Registration & Coffee** (LOCATION: SALON C/D/E)
9:00-9:45am	***Ten Strategies of a World-Class Cyber Security Operations Center*** Today's Cyber Security Operations Centers (CSOCs) should have everything they need to mount a competent defense of the ever-changing IT enterprise: a vast array of sophisticated detection and prevention technologies, a virtual sea of cyber intelligence reporting, and access to an exploding workforce of talented IT professionals. Yet most CSOCs continue to fall short in keeping the adversary— even the unsophisticated attacker-- out of the enterprise. Why is this? In this talk, the presenter will offer some observations on what it takes to do Computer Network Defense well in the modern IT enterprise. He will present ten fundamental qualities of an effective CSOC that cut across elements of people, process, and technology. He will have hard copies of the accompanying book by the same name for distribution; it is also available for free download. ***Carson Zimmerman**, Principal Engineer – Cyber Security Technical Center, MITRE*
9:45-10:30am	***The Healthy SOC: Preventing the Vicious Cycle of Security Failure by Addressing Root Cause*** Adversaries routinely attempt to re-compromise organizations that have been previously compromised, and, in most cases, they're highly successful. Is it because the vulnerabilities that they exploited weren't ever remediated? Or is it because the systemic issues that led to the incident are not being addressed? In this talk, Ismael Valenzuela, will provide answers to these questions, sharing practical advice on how SOCs can maintain a sustained defensible advantage by using continuous monitoring and threat hunting techniques to address root cause and avoid falling into the vicious cycle of security failure. ***Ismael Valenzuela**, GSE #132, Incident Response Practice Lead, Intel Security; Instructor, SANS Institute*
10:30-11:00am	**Networking Break and Vendor Expo** (LOCATION: CRYSTAL BALLROOM SALONS CDE)

Wednesday, May 25

11:00-11:45am **Solutions Session**

SOLUTIONS SESSION
(LOCATION: HARRISON)

Presented by

ARBOR NETWORKS
The Security Division of NETSCOUT

When the World's Watching – Lessons Learned From the 2012 RNC

Michael D. Molinaro,
Msc.IT, CISSP, CGEIT, C|CISO, CISM, CRISC, ITIL –
Chief Information Security Officer –
Vice President, Information Technology –
BioReference Laboratories Inc.

High-profile events like national political conventions are targeted by a wide range of adversaries with motivations including hacktivism, disruption, and extortion. And just like candidates, attackers unveil new strategies, tactics, and techniques to gain an edge. Success required a blend of tried-and-true practices and new strategies, tools, and techniques. Which SOC practices were effective under this blitz and which wilted when decisions had to be made in minutes? What new approaches added value to under-the-gun security teams and which yielded little? Join Michael Molinaro, CISO of BioReference Laboratories and the head of IT and cyber defense for the 2012 Republican National Convention for an interactive session on strategic choices, real-world experiences and pragmatic insights that SOC teams of all sizes can apply to increase day-to-day effectiveness.

SOLUTIONS SESSION
(LOCATION: WILSON)

Presented by

onapsis
Securing Business Essentials

The CISO Imperative – Taking Control of Cyberattacks on SAP

Sage Wagner,
Senior Sales Engineer, Onapsis

Business-critical applications running on SAP and Oracle are emerging as the next big target of attacks and the ultimate economic targets for cyber attacks. They are also the biggest blind spot for CISOs. In this session CISOs will learn about the top attack vectors targeting SAP, how the attacks access sensitive information and the top 5 things to incorporate into an information security strategy.

SOLUTIONS SESSION
(LOCATION: VAN BUREN)

Presented by

CYBERSPONSE
ENABLED SECURITY

Next Generation SOC: Eliminating Pain Points Through Automation

Joseph Loomis,
Founder & CEO, CyberSponse

Need help eliminating many of the painful and frustrating alerts that waste your valuable time operating in the SOC? In this session, CyberSponse will demonstrate simple automation playbooks designed to eliminate the majority of the noise and pain felt in today's SOC environments. Through API-enabled connectivity to various SIEM, IDS, IPS, MS Exchange and other products, playbooks or Courses of Action (COA) can eliminate many manual-based incident response efforts resulting in hours upon hours of lost time each day. SOC teams can operate CyberSponse in manual, semi- or fully-automated remediation plans, providing situational awareness and data enrichment-based incident records for better categorization and best use of a SOC's time.

11:45am-12:30pm ***SOC It To Me! - SOC Implementation Experiences from the Real World***

Do you feel like you're a pugilist constantly fighting to keep up with an onslaught of management dysfunction, unreasonable expectations, budget shortfalls, staffing skill limitations, constant reminders to do more with less, and relentless and seemingly innumerable adversaries? Panelists share their experiences trying to dodge the blows and make it a full twelve rounds.

MODERATOR: ***Chris Crowley**, Certified Instructor, SANS Institute*

PANELISTS: ***Zoher Anis**, Senior Consultant – IR & Forensics, Dell SecureWorks*
***Ismail Cattaneo**, Sr. Manager – U.S. Security Operations, Verizon*
***Cory Mazzola**, Global Manager - Security Programs & Strategic Services, Mandiant*
***Steve Mead**, Cyber Security Operation Lead, Common Securitization Solutions*

12:30-1:30pm **Networking Lunch** (LOCATION: CRYSTAL BALLROOM SALONS CDE)

Network with fellow attendees and visit with exhibiting vendors.
Lunch sponsored by the Summit vendors.

Wednesday, May 25

1:30-1:45pm	***Hiring and Firing a SOC*** Experts are predicting a "severe" shortfall in the cybersecurity workforce come 2019. With a quick look at all the available jobs out there today it seems the problem is happening now, or is it? This talk is designed to cover roles, job descriptions and misalignments of those descriptions, problems with HR and cyber, expectations or unrealistic expectations and how we are creating this problem ourselves. It will also look at experience, and growth in the roles typically seen in a Security Operations Center, as well as hiring at an enterprise vs. hiring at an MSSP. Finally, the talk will cover when you need to call it quits and short your staff to better the organization or leave yourself. ***David Nathans**, Author, Designing and Building a Security Operations Center*
1:45-2:30pm	***Recruiting for the Enterprise and for MSSPs*** A perspective from recruiting to enterprise and to an MSSP. This panel will explore the differences and similarities of enterprise vs. MSSP and how recruiters and HR departments need to bridge the gaps in language, skill sets and expectations. MODERATOR: ***David Nathans**, Author, "Designing and Building a Security Operations Center"* PANELISTS: ***Mary N. Chaney**, Esq., CISSP, Director – Security Operations Center, Johnson & Johnson* ***Deidre Diamond**, Founder & CEO, Cyber Security Network* ***Melissa Kaiser**, Director, SOCsoter* ***Jim Michaud**, Director – Cyber Talent Solutions, SANS Institute*
2:30-3:15pm	***Coach's Corner: A Belichickian Approach to Incident Response*** Tom and Justin will examine security operations in 2016 through their own experiences as consultants and practitioners and then filter it through the genius perspective of coach Bill Belichick, the six-time super bowl champion. We will cover these phases of the game: • Staying ahead of the pack with fundamentals • Drafting talent [elite QBs/rock stars vs. next man up (develop your own people)] • Playbook – situational security (process, response procedures) • Bend but don't break defense – resiliency, Cyber Kill Chain penetration • Game playing opponent (Cyber Adversaries) – take away the best player/capability (TTP) • A win is a win – (attribution vs. containment) • Deflate gate – (if you ain't cheatin', you're not trying hard enough) – Tricks to win executive support for your mission Attendees of this fun but insightful presentation will gain an appreciation for incident response and security operation fundamentals from people, process, and technology purviews, whether they are a Belichick fan or not. ***Justin Grosfelt**, Advanced Cyber Defense Advisory Consultant, RSA Security* ***Thomas Needham**, Manager – Cyber Threat Action Center, St. Jude Medical*
3:15-3:45pm	**Networking Break and Vendor Expo** (LOCATION: CRYSTAL BALLROOM SALONS CDE)

Wednesday, May 25

3:45-4:30pm	***Judo Threat Intelligence*** SOC and Threat Intel teams are tasked with protecting shareholder value and customer trust while facing attackers of limitless stamina, varying ingenuity and considerable resources. Internal Threat Intelligence can generate value through effective strategies and support meeting these objectives. By combining Security Operations principles with Judo principles, we can generate meaningful and efficient results. This presentation shows these principles and the results of applying them to Dun & Bradstreet. ***Frank Angiolelli**, CISSP, Director of Security Operations, Lead – IT Security, Dun & Bradstreet*
4:30-5:15pm	***Security v. Ops: Bridging the Gap*** For years we in the security industry have talked about the communication challenges between us and users. But what about between us and our fellow IT workers? How is your relationship with them? Do you have a solid partnership or do you barely talk? How much is the security of your enterprise helped or hurt by the cooperation, or lack thereof, between Operations and Security? Is it possible to have a fully OPERATIONALLY SECURE network without these two groups working well together? Unfortunately, these two groups usually are in opposition to each other, where each is complaining that the other doesn't know what they are doing, doesn't understand what's important and doesn't know how to run a network. This presentation will discuss the reasons for some of the most common misunderstandings and provide suggestions for resolution. By bridging the gap between these two groups, we will increase our ability to provide our customers and our users a secure environment to work in so they can accomplish their mission. ***Craig L. Bowser**, Sr. Security Engineer, Dept. of Energy*

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.

Thursday, May 26

8:00-9:00am	**Registration & Coffee** (LOCATION: SALON C/D/E)
9:00-9:45am	***The Evolving Role of the SOC*** As with many terms in security, SOC has become a buzzword used by executives to techies. Organizations often are asked whether they have a SOC or state that they have a SOC to justify the level of security within an organization. While the importance of a SOC has grown over the years, the real question is whether it is providing a measurable improvement in security. As we have seen with numerous breaches, the SOC has received alerts of the attack but based on poor tuning and lack of proper staff, the alerts are ignored and the breach goes undetected. As SOCs continue to become the hub of security within an organization, it is important that it role properly evolves to include tracking the correct metrics and creating an effective dashboard for monitoring and tracking breaches. In this engaging talk, industry expert Dr. Cole will outline how to evaluate the current state of a SOC, identify gaps and provide a checklist for improving the overall effectiveness. Key metrics will be discovered and showing how to achieve a concise security dashboard will also be discussed. ***Dr. Eric Cole**, Fellow, SANS Institute*
9:45-10:30am	***SOC vs. SIC*** In today's ever-changing threat landscape, SOC leaders must move from purely response-driven to intelligence-driven defense. In this session, attendees will learn how crowdsourcing security can help small, medium and large SOCs understand their specific threat actors. By marrying intelligence and your business model, you will be able to create better situational awareness into the security-related events in your environment and move from reactive to proactive defense. ***Mary N. Chaney**, Esq., CISSP, Director – Security Operations Center, Johnson & Johnson*
10:30-11:00am	**Networking Break and Vendor Expo** (LOCATION: CRYSTAL BALLROOM SALONS CDE)
11:00-11:45am	***Stop Armoring the Sheep, Start Hunting the Wolves*** As adaptive defensive becomes a critical capability for the traditional SOC, the security skills needed to identify advanced threat activity also change. Learn how you can infuse hunting skills into your security analysts and scale up your adaptive response. The discussion will focus on lessons learned from the front lines. ***Marcel Hoffman**, Hewlett Packard Enterprise*
11:45am-12:30pm	***Depth Charges: Defense-in-Depth is More Critical than Ever*** We all have heard some security professionals describe defense-in-depth as "dead." This could not be farther from the truth. The truth of the matter is that the art and science of defense-in-depth should be expanded in many organizations. This talk will cover how increasing defense-in-depth can help you find the adversary's in your network; not just to slow them down. We'll also discuss specific use cases that can be implemented to help identify danger. Even if your organization doesn't benefit from the segmentation aspects, we will consider how the concepts can be applied in other ways. Defense-in-depth can greatly augment hunting and active defense; it is not eliminated by it. ***Donald Warnecke**, Lead – IT Operations Technology (OT) Security, Consumers Energy*

Thursday, May 26

12:30-1:30pm **Lunch & Learns**

LUNCH & LEARN
(LOCATION: HARRISON)

Presented by

ARBOR NETWORKS
The Security Division of NETSCOUT

Your Team Can Start Hunting APTs Now; Really!

***Paul Bowen**, Principal Security Technologist, Arbor Networks*

Stopping stealthy attackers already inside your perimeter means proactively analyzing lots of clues and hunting them down. However unless you have scarce Incident Response experts on your team you can't execute this strategy - right? Not true. Join Arbor's Paul Bowen to learn how security analysts of all levels - from senior to novice, can use the high confidence clues that only network traffic reveals to uncover and disrupt APTs in minutes, not hours.

LUNCH & LEARN
(LOCATION: WILSON)

Presented by

onapsis
Securing Business Essentials

Protecting Your Business Critical Applications

***Sage Wagner**, Senior Sales Engineer, Onapsis*

SAP systems and applications are the lifeblood of the world's largest companies as they manage their most sensitive information and processes. Despite housing an organization's "crown jewels" – intellectual property, financial, credit card, customer data, supplier data and database warehouse information – SAP systems and their application layer are not protected by traditional security solutions. As SAP applications continue to be the target of stealthy breaches, it is imperative that organizations implement the right security products to gain visibility into the status of SAP applications and active threats against those systems. Join us for a demonstration of the Onapsis Security Platform – the first SAP cybersecurity solution that combines vulnerability, compliance, detection and response capabilities. Through continuous monitoring, the Onapsis Security Platform delivers a near real-time preventative, detective and corrective approach for securing SAP systems and applications.

LUNCH & LEARN
(LOCATION: VAN BUREN)

Presented by

cybereason

Hunt or Be Hunted

***Dan Mitchell**,*
Solutions Engineer, Cybereason

A post-breach mindset requires actively hunting for an adversary that has already compromised your network. Join us for a demonstration of Cybereason, the first platform to fully automate the detection of malicious behaviors. Learn how organizations from across the globe are seeing complete hacking operations in real time and staying ahead of the attacker. Join our discussion to learn how to:

- Shift to a proactive hunting approach
- Automate the detection of complete cyber attacks
- Cut investigation time by getting complete visibility of the attack story

1:30-1:50pm

The Race for Cyber Talent: How to Keep Your SOC Full (Or Finding and Keeping the Talent You Need)

With nearly 260,000 openings in information security in 2015 and the number of openings currently growing by nearly 15% percent a year, finding the right talent with the right set of skills and experience is becoming increasingly difficult for cyber leaders. In addition, many organizations are experiencing turnover in this field in excess of 20% annually. In this presentation, we will discuss what successful companies are doing to find and keep the talent they need. We will also review how SANS is helping to grow the future talent base available, while increasing diversity, in these mission critical roles.

***Jim Michaud**, Director – Cyber Talent Solutions, SANS Institute*

Thursday, May 26

1:50-2:50pm	***Enterprise Defense vs. Security Monitoring and Responses in the Cloud*** How do you defend something with no walls which allows every threat in the front door? This is what it is like to do proactive incident response for cloud-based environments. We will discuss traditional enterprise monitoring\response (aka the SOC) and how it differs in cloud-based environments. We will analyze how the techniques we have developed in standard enterprise monitoring can be adapted to securing the cloud. Finally, we will compare and contrast how the people, process, and technology of enterprise SOCs need to evolve to meet the demands of the cloud. ***Garrett Schubert**, Manager, Incident Response and Threat Intelligence, Acquia Inc.*
2:50-3:20pm	**Networking Break and Vendor Expo** (LOCATION: CRYSTAL BALLROOM SALONS CDE)
3:20-4:05pm	***Applying Data Science to Identify Malicious Actors in Enterprise Logs*** The presentation will provide guidelines on information security data science insights with repeatable process and examples on visualizing and applying machine leaning to information security data for identifying malicious actors. One of the key strengths of security teams is access to enterprise log data, meta-data, network traffic data, and netflow data. The challenge is finding and isolating the bad actors from legitimate traffic. Security professionals can benefit by applying machine learning and data science on enterprise data to find anomalies and identify patterns which will be helpful in isolating events which might indicate compromise. Steps involved in applying machine learning algorithms are to visualize and combine data cleansing with clever feature engineering, choose right metric/method for estimating model performance and then spend a lot of time tuning the parameters. The presentations will include use cases/ demos on Real Intelligence Threat Analysis or (RITA)/ELK framework. ***Balaji Balakrishnan**, Senior Information Security Officer, World Bank*
4:05-4:50pm	***Assessing and Securing for Cyber Threat Intelligence*** As you build your SOC and/or IR Program with a company of breadth of sites and assets, using specific aspects of Threat Intelligence will allow you to not only understand your own network, but the threats to the network. By becoming the threat leader, you can find, fix, finish, analyze, exploit and disseminate threat intelligence to your internal tools so that you can find not only new threats, but dormant ones. ***James Billingsley**, National Guard; SOC Analyst, SCANA* ***Rob Gresham**, National Guard; Incident Responder, Intel Security*
4:50-5:00pm	***Closing Remarks*** ***Mary N. Chaney**, Esq., CISSP, Director – Security Operations Center, Johnson & Johnson* ***Ismael Valenzuela**, GSE # I 32, Incident Response Practice Lead, Intel Security; Instructor, SANS Institute*

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.

@SANSDefense  **#SOCSummit**