SANS
Blue Team Summit & Training
Louisville, KY | SUMMIT: Apr 11-12 | TRAINING: Apr 13-18
LEARN MORE

Thursday, April 11	
9:00-9:15 am	*Welcome & Opening Remarks* • **Seth Misenar (@sethmisenar), Principal Consultant, Context Security; Senior Instructor, Co-Author SEC511 and SEC542, SANS Institute**
9:15-10:00 am	*Keynote* **Eric Conrad (@eric_conrad), CTO, Backshore Communications; Senior Instructor, Co-Author SEC511 and SEC542, Author MGT514, SANS Institute**
10:00-10:30 am	**Networking Break**
10:30-11:05 am	**Azure AD Security Recommendations and the Customer Stories That Prove It** Azure Active Directory has lots of features to help increase your organization's security posture. But which ones should you prioritize deploying? This session will discuss the key security quick wins you can go back and do immediately, best practices of deployment, and what has happened to other customers when they didn't deploy the security features they needed. **Mark Morowczynski (@markmorow) Principal Program Manager, Microsoft**
11:05-11:10 am	Q&A
11:10-11:45 am	**Skill Sharpening @ the CyberRange: Developing the Next-Generation Blue Team** How do you gain defender skills? Do you know exactly how offense should inform defense? Are you learning on the job in the heat of the moment? How to you measure outcomes and ensure success? The development of blue team cyber operation skills depends on reusable, repeatable, and measurable scenarios that reflect complex networks to pit the blue team against a modern attacker. It isn't enough to take a class and run through a lab. Attackers and red teams have dozens of options (including your network), and so does the blue team. You can practice on a cyber range, but it's about much more than a few virtual machines. It's about a real outcome achieved by trained operators armed with tools, techniques, and practices that enable them to get in the hunt. This presentation will introduce you to a modern range, survey best-of-breed tools and capabilities, and highlight how a range can support skill development for the blue team operator. **Don Murdoch, author of *Blue Team Handbook: Incident Response* and *Blue Team Handbook:*** *SOC, SIEM, and Threat Hunting Use Cases*
11:45-11:50 am	Q&A

11:50am – 12:25 pm	**To Blue with ATT&CK-Flavored Love** MITRE ATT&CK was originally created by red and blue teamers working together in a giant lovefest known as the Fort Meade Experiment. Building on that history, this talk will provide a love letter rekindling that flame. The talk is more than an ATT&CK overview. The presenter will use his unique perspective from real-world red teaming experience to cover insights, lessons learned, and a general perspective of defense and the hunt in order to show how ATT&CK is a valuable tool to help red and blue teams work together to improve their defenses. Specific topics to be covered include: • Research Soap Boxes vs. the Mad, and Expensive, Real World – How the field of red team research is different from the real world and what that means for blue teamers. • Sensing and Analytics Done Right…Maybe – The sensor data blue teamers should be collecting in order to have the best chance to catch red teamers and adversaries, as well as how to write behavioral analytics to catch them. • What Does It Mean to Hunt and How Can Your Red Team Help? – Advice for blue teamers trying to undertake the mammoth task of threat hunting, and what that actually means. • How Do You Really Use ATT&CK? – ATT&CK is the new hotness. That's great and all, but how can we use it for real to make our defenses stronger? **Jamie Williams, Cyber Adversarial Engineer, MITRE**
12:25-12:30 pm	Q&A
12:30-1:30 pm	**Lunch**
1:30-2:05 pm	**Seriously, I Can Still See You** Last year in Deadwood, South Dakota, strangers broke into my hotel (i.e., my network) and thought no one would notice the sound of the crashing front door. And no one did. Then they broke into an empty room (i.e., a desktop) and thought no one would notice that sound either. Again, no one did. Then they started to crack the locks between adjoining rooms and moving between them, thinking no one would notice. But I did, because my room was occupied, and I can show you how easy it was to see them. Silly thieves! I was there and my lights were on! And who uses the side doors anyhow?! This year the same thing happened, and it started the same way, but the attackers were smarter. Instead of breaking into the rooms one by one, they just slid notices under each door that said: "When you're ready to check out, don't dial zero as that extension is currently out of service. Instead, dial extension 666, and confirm your payment details there. Sorry for the inconvenience, and we hope you had a nice stay! – Management." Again, the attackers thought this would work nicely because guests wouldn't think anything of it, and because the real hotel management wouldn't notice until it was too late. Normally that would have worked, as it almost always does. But I watched them do it because, again, I was paying attention. When the room party at extension 666 was raging, I was standing outside the door. Imagine their surprise! Abuse of the Link Local Multicast Name Resolution (LLMNR) and Web Proxy Auto Detection (WPAD) protocols are probably the easiest way for an attacker to hijack your entire fleet's credentials and web traffic from right under your nose, LAN by LAN. Pay attention. I'll show you how easy it is to see. [Caveat venditor: no commercial tools are required!]

	Jonathan Ham (@jhamcorp), Principal Systems & Security Architect, Rendition Infosec
2:05-2:10 pm	Q&A
2:10-2:45 pm	**Using Statistical Analysis to Reduce Noise and Improve Efficacy** Security analysts and engineers in Security Operations Centers all around the world are treading water. They come to work and respond to alerts. But there's a queue of alerts when they get to work, and the queue is still there when they leave. A few of the alerts may be legitimate indicators of malicious activity, but many are false positives, and still others are impossible to classify as either malicious or benign. This talk will demonstrate how to track the amount of time your blue team is spending on alerts and analyze relevant statistics to "tune" or even get rid of those alerts that are unnecessarily bogging you down. You'll learn what to measure and how to calculate useful data points, handle outliers, and build a security scoreboard. You'll also see when to take action, what "tuning" means for you, and how to track the impact of the decisions you end up making. Also included are specific examples in Splunk and Python and lessons learned along the way. Ultimately, this talk will empower you to optimize team resources, allowing your analysts to spend more time on fulfilling, proactive work. In other words, they can spend more time swimming and less time treading water or drowning. **Keshia Levan, Detection Engineering Lead, Red Canary** **Kyle Rainey (@verri3r), Detection Engineering Lead, Red Canary**
2:45-2:50 pm	Q&A
2:50-3:15 pm	**Networking Break**
3:15-3:50 pm	**Cloud Security Challenges for the Blue Team** It seems like we are being bombarded by reports of exposed data due to misconfigurations in cloud services. Gartner estimates that up to 95 percent of cloud security failures will be "the customer's fault" by 2020. There are many security benefits for the blue team, but it seems we are lacking the skills necessary to take advantage of these. This talk will focus on the security benefits provided by the cloud and the necessary skill sets that the blue team must focus on developing in order to ensure that our organizations do not become another cloud security failure. **Marc Baker, Online Training Subject-Matter Expert, SANS Institute**
3:50-3:55 pm	Q&A
3:55-4:30 pm	**Zero-Trust Networks: The Future Is Here** The traditional perimeter-based security architecture used in sectors ranging from education to government and communications has basically failed to protect internal assets. New technologies such as the Internet of Things and mobile devices will force a new approach to network security architecture. Zero-trust networks (ZTNs) assume that the network is hostile, attackers are already inside the net, and segmentation isn't sufficient to determine trust, among other characteristics. This talk will describe

	zero-trust network properties and how we are integrating this architecture with existing cybersecurity defense strategies. We believe all sectors will have to adopt this strategy in the near future. In this talk, we'll explore ZTN components and their relationships, determine what off-the-shelf software can be used to build a ZTN, and help you improve your overall security posture by integrating ZTN concepts into your existing network architecture. **Randy Marchany (@randymarchany), CISO, Virginia Tech; Instructor, SANS Institute**
4:30-4:35 pm	Q&A
4:35-5:10 pm	*Talk description to come* **Greg Foss (@Heinzarelli), Senior Threat Researcher, Carbon Black**
5:10-5:15 pm	Q&A
6:00 pm	Networking Event TBA

Friday, April 12	
9:00-9:15 am	*Opening Remarks* • **Eric Conrad (@eric_conrad), CTO, Backshore Communications; Senior Instructor, Co-Author SEC511 and SEC542, Author MGT514, SANS Institute** • **Seth Misenar (@sethmisenar), Principal Consultant, Context Security; Senior Instructor, Co-Author SEC511 and SEC542, SANS Institute**
9:15-10:00 am	*Keynote to be announced*
10:00-10:30 am	**Networking Break**
10:30-11:05 am	*Talk description to come* **Roberto Rodriguez (@cyb3rward0g), Senior Threat Hunter, SpecterOps**
11:05-11:10 am	Q&A
11:10-11:45 am	**Mental Models for Effective Searching** One of the most intimidating challenges many analysts encounter is a blank search bar. That search bar is the only thing standing between you and a mountain of data containing the answers you need to determine if a compromise has occurred on your network. It's for this reason that effective searching is a core competency for investigators. This presentation will provide a conceptual framework for effective searching, show you how to master any search tool faster, and offer strategies to combat the biases and limitations of the mind that can negatively affect your ability to process search results. **Chris Sanders (@chrissanders88), Founder, Applied Network Defense; Founder, Rural Technology Fund (@RuralTechFund)**

11:45-11:50 am	Q&A
11:50am – 12:25 pm	*Talk description to come* **David Mashburn (@d_mashburn), Certified Instructor, SANS Institute**
12:25-12:30 pm	Q&A
12:30-1:30 pm	**Lunch**
1:30-2:05 pm	**Relentless Team Building** Given the current demand for highly skilled InfoSec professionals, it's easy to overlook how one achieves that level of proficiency. Drive, aptitude, and devotion all contribute to an individual's skillset, but one critical factor may often be disregarded: The importance of the team. Not everyone transitions from layperson to professional overnight. Some people need constructive mentoring to realize their growth potential. Others may simply need the opportunity to break into the field at large to find their niche before progressing on to future endeavors. If a key asset to professional growth is being part of a great team, who is supposed to build the team and how? This presentation focuses on the positive aspects of building, coaching, managing, and cultivating healthy teams. It covers the importance of maintaining ethical group and individual standards, effective measurements of success, and the value of investing in human capital. We will also cover the need for continual team enrichment through training and situational exercises. "The only thing worse than training your employees and having them leave is not training them and having them stay." – Henry Ford **Dustin Lee (@_dustinlee), Principal Engineer, Security Onion Solutions LLC**
2:05-2:10 pm	Q&A
2:10-2:45 pm	**One Phish, Two Phish, Red Phish, Green Phish** Body: Every single organization has an incredible amount of distributed horsepower just sitting around and doing nothing in their building. We are, of course, talking about your users! Many, if not hopefully all, orgs have some sort of "Phishing@acme.com" account that users can send suspicious emails for analysis by the information security team. However, without immediate gratification or response, they often become disenchanted with the process. Imagine if your user base was able to send emails in and have an automated process give a green/yellow/red response. This talk discusses how to use the tools stoQ and Splunk to automate analysis and defense while simultaneously improving user satisfaction. **Dave Herrald (@daveherrald), Staff Security Strategist, Splunk** **Ryan Kovar (@meansec), Principal Security Strategist, Splunk**
2:45-2:50 pm	Q&A
2:50-3:15 pm	**Networking Break**
3:15-3:50 pm	

	Statically Analyzing Infrastructure as Code As more and more companies move towards a DevOps philosophy, Infrastructure as Code is gaining popularity. Tools like terraform, CloudFormation, puppet, Ansible, now allow us to define our security controls as code. The upside of this is we can now apply Application Security methodologies to our Infrastructure. At Wayfair, I am developing a tool called terrafirma (https://github.com/wayfair/terrafirma) to statically analyze terraform plans within our CI/CD pipeline. It is currently used within our production environment. However, this approach can easily translate to almost any orchestration framework to catch configurations and even outdated software before they ever make it to deployment. **Mike Siegel (@ml_siegel), Senior Security Engineer, Wayfair LLC**
3:50-3:55 pm	Q&A
3:55-4:30 pm	**Network Flow Data: A Cornucopia of Value** Did you realize that many network devices, such as routers, offer a treasure trove of data that can be analyzed to find unusual traffic patterns and intrusion activities on your network? Sure, most diligent companies have intrusion detection systems and sensors but even the best tuned solutions miss malicious behavior due to blind spots like sensor placement and encrypted payloads. Network flow data is a feature available on almost all networking products but is often overlooked as part of a defensible architecture. Need to hunt for lateral movement on a user segment that doesn't have a sensor? Flow data can provide visibility where other solutions fail. Come join me to learn tips for taking advantage of already available data. **Andrew Laman (andylaman), Founder & Principal Consultant, A4 InfoSec; Certified Instructor, SANS Institute**
4:30-4:35 pm	Q&A
4:35-4:45 pm	*Closing Remarks* • **Eric Conrad (@eric_conrad), CTO, Backshore Communications; Senior Instructor, Co-Author SEC511 and SEC542, Author MGT514, SANS Institute** • **Seth Misenar (@sethmisenar), Principal Consultant, Context Security; Senior Instructor, Co-Author SEC511 and SEC542, SANS Institute**

Marc Baker, Online Training Subject-Matter Expert, SANS Institute Marc has more than 10 years of experience in information technology and security. He is the curriculum lead for blue team courseware with the Online Training Subject Matter Expert Curriculum Team at the SANS Institute. He gained information security experience first as the owner of a business serving numerous small businesses and then as the Security Administrator for a state college in Florida and Security Analyst at a large pharmaceutical company. Marc has a masters degree in Information Assurance with a specialty in

Cybersecurity and he also has earned numerous industry certifications from ISACA (CRISC), GIAC (GSEC, GCED, GCIA, GMON, GCPM, GISP, GCFE, GNFA, GCIH), and AWS.

Eric Conrad (@eric_conrad), CTO, Backshore Communications; Senior Instructor, Co-Author SEC511 and SEC542, Author MGT514, SANS Institute Eric is the lead author of SANS MGT414: SANS Training Program for CISSP® Certification, and coauthor of both SANS SEC511: Continuous Monitoring and Security Operations and SANS SEC542: Web App Penetration Testing and Ethical Hacking. He is also the lead author of the books the CISSP Study Guide, and the Eleventh Hour CISSP: Study Guide. His career began in 1991 as a UNIX systems administrator for a small oceanographic communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and health care. He is now CTO of Backshore Communications, a company focusing on hunt teaming, intrusion detection, incident handling, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications. Eric also blogs about information security at www.ericconrad.com.

Greg Foss (@Heinzarelli), Senior Threat Researcher, Carbon Black Greg is a Senior Threat Researcher with Carbon Black's Threat Anaysis Unit. In prior roles, he build and ran a global security operatios program, consulted as an ethical hacker, and worked as a security analyst for the past five years, focused on understanding the technology and the security implications that these technologies will have on the future of digital currency. Greg is a very active member of the Denver information security community who loves to give back and support the industry.

Jonathan Ham (@jhamcorp)**, Threat Hunting Operations Lead, Rendition Infosec, Principal Systems & Security Architect, JHamCorp, Principal Instructor, SANS Institute.** For over 20 years, Jonathan has been an independent consultant who specializes in large-scale enterprise security issues, from policy and procedure, through staffing and training, to scalable prevention, detection, and response technology and techniques. With a keen understanding of ROI and TCO (and an emphasis on process over products), he has helped his clients achieve greater success, advising in both the public and private sectors, from small startups to the Fortune 50. He's been commissioned to teach NCIS investigators how to use Snort, performed packet analysis from a facility more than 2000 feet underground, chartered and trained the CIRT for one of the largest U.S. civilian Federal agencies, and taught network intrusion analysis techniques directly to the NSA. He has variously held the CISSP, GSEC, GCIA, and GCIH certifications, is a member of the GIAC Advisory Board, and has taught for the SANS Institute as a Certified Instructor for over 10 years. Jonathan is the co-author of "Network Forensics: Tracking Hackers Through Cyberspace" (Prentice Hall, 2012)---the first comprehensive textbook on the subject. He is also the co-author (with Shon Harris) of the CISSP Practice Exams, now in it's 5th Edition (McGraw-Hill, 2018). A former US Navy field corpsman, Jonathan has also spent 10 years volunteering his time to both practice and teach a different kind of emergency response, for both the American Red Cross and the National Ski Patrol, of which he is a Senior Alpine member and Certified Instructor.

Dave Herrald (@daveherrald), Staff Security Strategist, Splunk Dave is a technical information security professional working as a staff security strategist for Splunk and focuses on the Splunk Boss of the SOC(BOTS), performing research in to adversary simulation for blue teams, training technical security sales teams around the globe, and helping Splunk customers to implement advanced security use cases.

He has worked in various information security roles including pre-sales engineer, strategic security consultant, penetration tester, hands-on security architect/engineer/analyst, and chief information security officer and holds a number of security certifications including GIAC Security Expert (GSE) #79.

Ryan Kovar (@meansec), Principal Security Strategist, Splunk Ryan worked at the Defense Advanced Research Projects Agency (DARPA) on a team dedicated to detecting and mitigating advanced threats. Ryan moved onto Splunk as a Staff Security Strategist where he helps out with IR, hunting, and solving fun problems. Ryan despises printers.

Andrew Laman (@andylaman), Founder & Principal Consultant, A4 InfoSec; Certified Instructor, SANS Institute Andrew is the founder and principal consultant at A4 InfoSec, an independent consulting firm with services focusing on monitoring, detection, and incident response. Andy has more than 25 years of information technology and security experience in multiple industries. He has held lead security positions in Fortune 500 and several global companies. Andy is a course contributor and teaches SEC503: Intrusion Detection In-Depth, for the SANS Institute. In addition to the CISSP, Andy holds multiple GIAC certifications including the prestigious GIAC Security Expert (GSE #142) certification as well as multiple other industry certifications.

Dustin Lee (@_dustinlee), Principal Engineer, Security Onion Solutions LLC
Bio to come

Keshia Levan, Detection Engineering Lead, Red Canary Keshia likes building tools with Ruby and Python, is mocked for her Splunk obsession, and spends too much time playing with logs and json to develop security content (or at least pretty graphs). She's worked in several SOCs, triaging alerts and analyzing EDR data before focusing more on security engineering.

Randy Marchany (@randymarchany), CISO, Virginia Tech; Instructor, SANS Institute Randy is the Chief Information Security Officer of Virginia Tech and the Director of Virginia Tech's IT Security Laboratory. He is a co-author of the original SANS Top 10 Internet Threats, the SANS Top 20 Internet Threats, the SANS Consensus Roadmap for Defeating DDoS Attacks, and the SANS Incident Response: Step-by-Step guides. Randy is currently a certfied instructor for the SANS Institute and joined SANS in 1992. He was a member of the Center for Internet Security development team that produced and tested the CIS Solaris, HPUX, AIX, Linux and Windows2000/XP security benchmarks and scoring tools. He was a member of the White House Partnership for Critical Infrastructure Security working group that developed a Consensus Roadmap for responding to the DDOS attacks of 2000. He has written or co-authored over 35 papers on cybersecurity. He was a recipient of the 2016 Shirley C. Payne IT Security Advancement award, the 2000 SANS Institute's Security Technology Leadership Award, the 2003 VA Governor's Technology Silver Award, and a member of the team that won the EDUCAUSE Excellence in Information Technology Solutions Award in 2005. He is a co-holder of two cybersecurity patents. His blog is http://randymarchany.blogspot.com

David Mashburn (@d_mashburn), Certified Instructor, SANS Institute David has experience working as an IT security professional for several civilian federal agencies, and over 15 years of experience in IT. He holds a masters degree in computer science from John Hopkins University, and a B.S. from the University of Maryland at College Park. David holds multiple security-related certifications, including CISSP, GPEN, GCIH, GCIA, and CEH. He is also a member of the SANS / GIAC Advisory Board, and has previously taught courses in the Cybersecurity curriculum at the University of Maryland - University College.

Seth Misenar (@sethmisenar), Principal Consultant, Context Security; Senior Instructor, Co-Author SEC511 and SEC542, SANS Institute Seth is a Cyber Security Expert who serves as a Faculty Fellow with the SANS Institute and Principal Consultant at Context Security, LLC. He is numbered among the few security experts worldwide to have achieved the GIAC GSE (#28) credential. Seth teaches a variety of cyber security courses for the SANS Institute including two very popular courses for which he is lead author: the bestselling SEC511: Continuous Monitoring and Security Operations and SEC542: Web Application Penetration Testing and Ethical Hacking.

Seth's background includes security research, network and web application penetration testing, intrusion analysis, incident response, and security architecture design. He has previously served as a security consultant for Fortune 100 companies, as well as the HIPAA Security Officer for a state government agency.

He has Bachelor of Science degree in Philosophy from Millsaps College and resides in Jackson, Mississippi with his wife, Rachel, and children, Jude, Hazel, and Shepherd.

Mark Morowczynski (@markmorow), Principal Program Manager, Microsoft Mark has been a member of the Identity Product Group for the last 3 years working with some of the world's largest and most complex customers on their Azure AD deployments.

Don Murdoch (@BlueTeamhb), author of *Blue Team Handbook: Incident Response* and *Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases* Don Murdoch, GSE, MSISE, MBA is a seasoned IT leader with over 20 years of IT and InfoSec experience across several disciplines. Most recently, Don is the Director of a MSSP and Security Operations Practice for SLAIT Consulting, where he works with businesses of all sizes to implement SIEM, improve Security Operations, and provide security architecture consulting with an emphasis on risk reduction and mitigation.

The first half of his career emphasized software development, network and systems management, and database administration. At his career midpoint he worked as the Information Systems Security Officer for Old Dominion University in Virginia, where he spent most of his days in the Wild, Wild West of academic computing and put most of his SANS education to the test. For the remainder of his career, Don has worked in computer, network, and information security as the lead Security Engineer/Security Architect, and then Director for the Strategy and Planning team for the Infrastructure division within a Fortune 500 Medicaid focused Insurance company.

Don has significant experience with the SANS Institute, including Local Mentor, Community Instructor, GCIH grader, active Advisory Board member, and courseware developer for SANS.

Kyle Rainey, (@verri3r), Detection Engineering Lead, Red Canary. Kyle spent years providing proactive and reactive incident response and forensics services to Fortune 500s. He has extensive experience strengthening organizations' security postures, monitoring their health and maintenance, and increasing their performance. At Red Canary, he helps lead the Detection Engineering team as it develops and improves detection strategies.

Roberto Rodriguez (@cyb3rward0g), Senior Threat Hunter, SpecterOps Roberto is a Senior Threat Hunter at SpecterOps where he specializes in the development of analytics to detect advanced adversaries techniques. His experience performing incident response and threat hunting engagements, in various industries, has encouraged him to help organizations improve their security posture and share his knowledge with the information security community. He is also the author of several open source projects, such as the Threat Hunter Playbook and HELK, to aid the community development of techniques and tooling for hunting campaigns. He currently maintains his blog at https://cyberwardog.blogspot.com.

Chris Sanders (@chrissanders88), Founder, Applied Network Defense; Founder, Rural Technology Fund (@RuralTechFund) Chris has written five books including three editions of “Practical Packet Analysis”, which has sold tens of thousands of copies internationally, and “Applied Network Security Monitoring”.He has authored hundreds of articles on the topics of packet analysis, intrusion detection, and general network security and administration. worked in multiple roles for the US Department of Defense where I served as a security analyst, eventually building and leading teams of analysts. Chris eventually left the defense sector and began working in private industry with great people at InGuardians and Mandiant/FireEye. In late 2016 he decided it was time to focus on serving others through non-profit work. He then founded Applied Network Defense, where Chris focuses on delivering high quality, affordable security training.

Mike Siegel (@ml_siegel), Senior Security Engineer, Wayfair LLC
Mike Siegel has worked in the Information Security space for the past thirteen years, working for organizations such as Blue Cross Blue Shield, The Federal Reserve, Vistaprint and various consulting companies. Originally entering the profession as a network engineer/firewall engineer he has since branched out into application security, DevSecOps and Penetration Testing/Red Teaming. Mike is currently the lead of the Red Team at Wayfair, transitioning after two years on the Infrastructure Security team.

Jamie Williams, Cyber Adversarial Engineer, MITRE Jamie is a Cyber Adversarial Engineer at MITRE where he is a core member of the ATT&CK team. He explores industry research and documents techniques in ATT&CK based on his years of growing operational experience. Jamie also serves as a red teamer for ATT&CK-based evaluations. Before joining MITRE, Jamie received degrees from Johns Hopkins University and the University of Maryland, Baltimore County (UMBC).