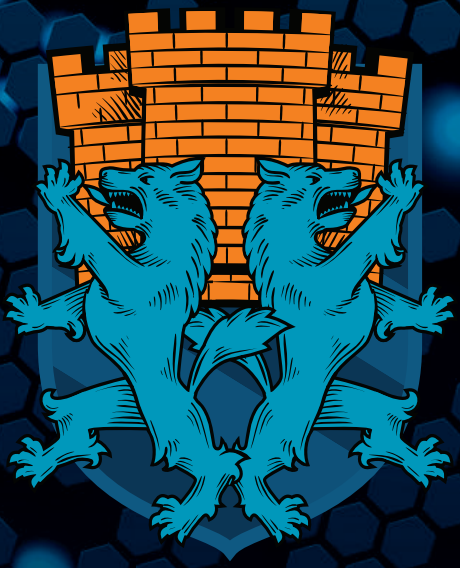
SANS The most trusted source for cybersecurity training, certifications, degrees, and research



Blue Team Summit

Program Guide

@SANSDefense #BlueTeamSummit

Agenda

All Summit Sessions will be held in the Olmstead 1-4 (unless noted otherwise).
All approved presentations will be available online following the Summit at ***sans.org/summit-archives***

Monday, March 2

7:00-9:00 am	**Registration & Coffee** (LOCATION: OLMSTEAD 1-3 PRE-FUNCTION AREA)
9:00-9:15 am	***Welcome & Opening Remarks*** ***Eric Conrad*** *@eric_conrad, Fellow, SANS Institute* ***Seth Misenar*** *@sethmisenar, Fellow, SANS Institute*
9:15-10:00 am	***Keynote: Blue Team is Not Just A Job, It's an Adventure*** Otto von Bismarck once said, "Only a fool learns from their own mistakes. The wise person learns from the mistakes of others." Most blue teamers are graduates of The School of Hard Knocks. In this talk, Marcus J. Carey will walk you through his journey as a blue teamer who has discovered through trial, error, and by interviewing hundreds of cybersecurity professionals for the Tribe of Hackers book series, how to build effective security models. Marcus will share insights on how to optimize cybersecurity technology, processes, and personnel for optimum impact. ***Marcus J. Carey*** *@marcusjcarey, Enterprise Architect, ReliaQuest; Co-Author, Tribe of Hackers*
10:05-10:40 am	***Creativity, Convergence, and Choices: Security Analyst Thinking Modes*** What makes someone a good security analyst? Even analysts who are good at catching bad guys aren't always very effective at explaining how they do it. The presenters recently sought to better understand the investigation process by exploring how analysts use convergent and divergent thinking in their day-to-day processes. In this session they will present the results from their original research on the role of thinking modes in investigative work, along with strategies for practicing and developing these types of thinking to become a more effective and metacognitively-aware analyst. ***Stef Rand*** *@techieStef, Associate Consultant, FireEye/Mandiant* ***Chris Sanders*** *@chrissanders88, @ruraltechfund, Founder, Applied Network Defense; Director, Rural Technology Fund*
10:40-11:05 am	**Networking Break** (LOCATION: OLMSTEAD 1-3 PRE-FUNCTION AREA)

Monday, March 2

11:10-11:45 am

Cobot Uprising: Smart Automation for Blue Teams

Despite using more automation than ever before in detection and response operations, organizations continue to be challenged by relatively unsophisticated attacks. Reliable detection requires time-consuming analysis and a level of data aggregation and correlation that is at best an art, and at worst cost-prohibitive. Meanwhile, attackers remain agile and inventive, continually (and rapidly) changing their infrastructure and approach with minimal costs and maximum benefit.

While there are some tasks that computers do far better than humans – such as rote and repetitive tasks and complex calculations – we will always be masters of analysis given our ability for complex thought, decision-making, and visual learning. With the introduction of security automation and orchestration to the defensive tool set, blue teams can now automate some of their investigative playbooks and save precious time. Unfortunately, this capability often drives automation for its own sake and expands tool sets that are already monolithic, rather than actually empowering our humans. Simply doing analysis faster is only a small part of the solution, and not all "improvements" are created equal!

How can we reframe this challenge to alter the calculus of attack and defense? Automation for the sake of doing so is a common trap that can actually degrade our capabilities and waste defensive cycles. However, applying automation in a controlled, strategic manner can be a game changer for defenders. With proper planning and an incremental, product-neutral approach to automation, we can measurably improve our defenses and start leveling the playing field.

Mark Orlando *@markaorlando, Co-Founder & CEO @bionic_sec; Instructor, @SANSInstitute*

11:50 am - 12:25 pm

Cops and Robbers: Simulating Adversary Techniques for Detection Validation

Your organization spends a lot of time and money on your security program. Shouldn't you be able to show that all of that investment is paying off? Many vendors are offering customers high-quality analytics, but how can you ensure that they are working correctly? What if you had a way to repeatedly emulate common and known adversary tactics, techniques, and procedures in your environment with no formal penetration test required? This presentation will showcase a tactical method for adversary emulation and detection using free tools and open-source projects, including Atomic Red Team from Red Canary, DetectionLab from Chris Long, ThreatHunting from Olaf Hartong, Splunk (Enterprise Trial), and Phantom (Community Edition). We'll show how this framework can simulate techniques, review the events that result, and test your detection capabilities against many techniques in the MITRE ATT&CK framework. The framework even has detailed instructions to spin it up in Amazon Web Services or locally in your environment so that you can start using it as soon as you return to the office.

Kyle Champlin *@dishwishy, Principal Product Manager, Splunk*

Tim Frazier *@timfrazier1, Security Strategist, Splunk*

12:30-1:30 pm

Lunch & Panel (LOCATION: OLMSTEAD 1-4/OLMSTEAD PRE-FUNCTION AREA)

IDS Highlander: There Can Be Only One

What is your preferred open source IDS: Snort, Suricata, or Zeek? Choose wisely, because you must pick only one. Our panelists will defend their choice to the death (figuratively) in this spirited panel discussion.

MODERATOR: ***Eric Conrad*** *@eric_conrad Fellow, SANS Institute*

PANELISTS: ***Dave Herrald*** *@daveherrald, Principal Security Strategist, Splunk*
Ryan Kovar *@meansec, Principal Security Strategist, Splunk*
Don Murdoch *@BlueTeamHB, BTHb, and Author/Range Officer, Regent University*
Mark Orlando *@markaorlando, Co-Founder & CEO @bionic_sec; Instructor, @SANSInstitute*
Chris Sanders *@chrissanders88 @ruraltechfund, Founder, Applied Network Defense; Director, Rural Technology Fund*

Monday, March 2

1:30–2:15 pm	***Put Some Power in Your Shell: POSH for Incident Response at Scale*** If your blue team doesn't understand how to do on-system analysis, then it's game over because the team won't be able to detect the hack or how to find signs of persistence or malicious behavior. Worse, the team won't know how to scale out. Automated tools help, but they depend on your blue team understanding what the data mean. This presentation will go over numerous tools and techniques with PowerShell to perform on-system analysis and script analysis for the enterprise. We'll also look at how to use other WinRM features to do analysis at scale. The presentation will list out common analysis challenges; go over WinRM setup requirements; review the use of PS-based tools to collect a baseline; demo remote analysis methods (including writing fault-tolerant PS code that tests for connectivity and fails gracefully, and writing job-based PS code for the defender); and examine running remote collection scripts so that you don't have to do all of the heavy lifting. ***Don Murdoch*** *@BlueTeamHB, BTHb, and Author/Range Officer, Regent University*
2:20–2:55 pm	***Orchestrating Detection within Security Onion*** This presentation will look at how to develop a customized playbook for your organization using the new Playbook tool in Security Onion. Playbook allows you to easily build new detection strategies using Sigma or import plays from other sources. The tool integrates into existing Security Onion tools by automatically creating Elastalert alerts and TheHive Project case templates based on your plays. This helps you document and automate the most important elements of your detection strategies: motivation (what are you looking for?), next steps (how to analyze the results), and the actual search query needed for the Elasticsearch backend. ***Josh Brower*** *@DefensiveDepth, Senior Engineer, Security Onion*
2:55–3:20 pm	**Networking Break** (LOCATION: OLMSTEAD 1-3 PRE-FUNCTION AREA)
3:25–4:00 pm	***Cybercrime Markets and Their Effects on Threat Intelligence and Detection*** Modern cybercrime consists largely of marketplaces where training, tools, services, access, and more are all for sale. However, most public threat intelligence reporting – and therefore the detection and response focus that it drives – remains focused on single actor groups. This skews attribution, detection, and response – sometimes with dire consequences. To properly apply an attack lifecycle model and track actors across it, we must first understand these marketplace relationships. This presentation will provide an overview of criminal marketplaces and how they affect the attack lifecycle, and also examine several case studies where cybercrime markets shape how attacks are carried out from beginning to end. ***Paul Melson*** *@pmelson, Senior Director – Cybersecurity, Target*

Monday, March 2

4:05-4:40 pm	***Computer Love: Love Letters and Log Analysis*** This presentation examines the communication connection between written human interaction and machine-generated events known as logs. Log events are the foundation of security monitoring, investigation, and forensics. This presentation will discuss what log analysis is, the importance of log analysis, along with some methods, tools, and techniques. Reviewing logs is a fundamental and integral aspect of being a security analyst. Logs always tell a story about machine-generated events that occurred during a certain time period in the same way a love letter can tell a story about a moment in time. When it comes to log analysis, security analysts must determine what to look for using the information at hand, formatting that information and reporting the findings. This insight will help a security analyst develop a proactive approach to monitor security events and remediate threats. By presenting a new perspective of log analysis, all attendees will gain a relative understanding on how to tell a better story based on communication from machine activity. ***Doug Bryant, Jr.*** *@CyberGent_101, Incident Response Analyst, Black Knight, Inc.; Co-Host, Intrusion Diversity System Podcast*
4:45-5:00 pm	***Day 1 Wrap-Up***
5:30-7:30 pm	***Taste of Louisville*** Stretch your legs on the short (0.4 mile) walk to Bluegrass Brewing Co., where we'll have the speakeasy-inspired Bourbon Barrel Loft all to ourselves. With bourbon tasting, local brews, special non-alcoholic concoctions, Derby pie, and bread pudding, there's something for everyone to get a taste of Louisville!

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.

Tuesday, March 3

7:00-9:00 am	**Registration & Coffee** (LOCATION: OLMSTEAD 1-3 PRE-FUNCTION AREA)
9:00-9:45 am	***Keynote: Threat Hunting via DNS*** DNS logs are one of the most powerful threat hunting resources, but encryption is rapidly changing that equation. Key DNS threat hunting techniques include detecting DNS tunneling and Domain Generation Algorithms (DGAs). It used to be simple(r): log DNS requests and responses on DNS forwarders, or sniff and analyze via tools like Zeek. DNS over TLS (DoT) and DNS over HTTPS (DoH) are disrupting the status quo: where does that leave network defenders? This talk will analyze the current state of DNS monitoring, and provide actionable steps for detecting malice on your network via DNS. ***Eric Conrad*** *@eric_conrad, Fellow, SANS Institute*
9:50-10:25 am	***Pushing the SOC Left To Achieve Nash Equilibrium*** As a defender we've seen the landscape change over the last few years. A shift to cloud, better endpoint detection capabilities, and overall acceptance of leveraging threat intelligence. All these items are advantages for SOC personnel, but how are we incorporating application security? The idea of "shifting left" is based upon secure SDLC, but how do we build detection, response, and monitoring of applications into the SOC? The normal gambit of next-generations firewalls and antivirus products aren't applicable as applications differ from build to build. This talk will focus on building out capabilities to help defenders identify attacks against the application, build detection mechanisms and how to leverage this information for triage. ***O'Shea Bowens*** *@SirMuDbl00d, Founder & CEO, Null Hat Security*
10:25-10:45 am	**Networking Break** (LOCATION: OLMSTEAD 1-3 PRE-FUNCTION AREA)
10:50-11:25 am	***Password-less! Can It Be Done?*** As industries start to move to password-less environments, the benefits are clear but the path to get there is not. Several large enterprises have started their password-less journey and you can too. Learn from their experiences in order to avoid pitfalls and accelerate deployment to enhance your security state. This presentation will provide you with some quick wins and next steps for the short term and a clear strategy for the long term. ***Joey Cruz*** *@404crux, Program Manager, Microsoft* ***Mark Morowczynski*** *@markmorow, Principal Program Manager, Microsoft*
11:30 am – 12:05 pm	***How to Build a Threat Hunting Team and Manage Rabbit Holes*** Hunting is one of the hottest buzzwords when it comes to cybersecurity – especially in defensive-oriented realms. As a result, there are hundreds of tools, articles, and books on how to hunt. Yet, if it was that simple – why are we still having issues doing this successfully – even if we ignore advanced threat actors? There are so many tools that may be able to report that something is happening on a network, but the blue teams themselves are unable to interpret these results in a timely manner, which results in potentially missing something critical. Therefore, rather than introduce a new tool, this talk will focus on how people can improve themselves to be better hunter and how better to structure teams to also hunt more effectively. ***Dr. Chelsea Hicks*** *@TheDrPinky, U.S. Dept. of Defense*
12:10-1:15 pm	**Lunch & Lightning Talks** (LOCATION: OLMSTEAD 1-3 PRE-FUNCTION AREA) Enjoying the Summit talks? Have something to add? Here's your chance! Sign up for a five-minute lightning talk on the Blue Team topic of your choice. This is a great low-risk opportunity to try out a topic or get some public speaking experience in a supportive environment. Sign up: **https://bit.ly/2NrtiqO**

Tuesday, March 3

1:20-1:55 pm	***DevBlue: Applying Software Engineering Practices to Blue Teaming for the Win!*** Have you wondered what happens when you get world-class devs and blue team experts in the same team? Meet DevBlue! In this talk, Lucia and Ismael will share lessons learned in a journey where devs and blue teamers have worked together to create an endpoint detection and response (EDR) product. But please keep reading, this is not a product talk! Rather, through the use of practical examples, we want to show you how proven software engineering practices can help you methodically grow your detection capabilities in weekly increments. In particular, we will cover how to set up and manage an engineering blue team (a.k.a. DevBlue) to apply practices such as issue tracking, peer review, unit testing, automated red teaming testing, continuous delivery, operational intelligence mining, post-exploitation tools, purple teaming, and security posture measurement using the MITRE ATT&CK matrix as a reference. ***Lucia Coppes**, EDR Software Engineer, McAfee* ***Ismael Valenzuela** @aboutsecurity, Principal Engineer, McAfee; Certified Instructor, SANS Institute*
2:00-2:35 pm	***Threat Intelligence: How to Focus Fire on the Bad Guys Coming for Your Network*** As a blue teamer or threat hunter, how many times have you been told to go "find evil?" How many times have you been expected to search for every adversary tactic until you MAYBE find the bad guy? NO MORE! This talk will examine what threat intelligence is and how it can be used to better inform defenders on prioritizing which bad guys to look for first. Now when most people hear "threat intelligence," they have the same reaction as to hearing buzzwords like blockchain, artificial intelligence, or synergistic management solutions. It's unfortunately true that threat intelligence has become a buzzword in the cyber security field. So how do we turn this buzzword into something that can be put into practice? Lucky for you, this very question will be answered here! You will see the process of discovering which specific adversaries are targeting your organization, all the way down to finding the tactics, techniques, and procedures the bad guys use to steal your data. Finally, we will close with a scenario, walking you through an example of how this threat intelligence process can be used in your organization's regular hunt operations. ***Kyle Hubert** @aptgetKubert, Network Analyst and Blue Team Lead, U.S. Air Force*
2:35-3:00 pm	**Networking Break** (LOCATION: OLMSTEAD 1-3 PRE-FUNCTION AREA)
3:05-3:40 pm	***Seeing Red: Top Five Things You Can Do to Catch a Physical Pen Tester*** Peek behind the curtain of a physical pen tester to learn how to keep us out of your organization. This talk will discuss the most common ways we gain access, acquire sensitive information, and avoid detection. Takeaways will help your organization be more secure and, of course, make my job much more difficult. ***Crystal Wilson** @unluckynum7, Associate Security Specialist, GreyCastle Security*
3:45-4:20 pm	***Blue Team To Go*** Hopefully after two days of talks, fortified by informal learning through networking with your peers, you're fired up to get back to the office and put these ideas to work. Seth will help you distill the key themes and advice from the Summit and organize them into manageable, actionable tasks that yield real results. ***Seth Misenar** @sethmisenar, Fellow, SANS Institute*

Tuesday, March 3

4:20- 5:00 pm	***Panel: Ask Us (Almost) Anything (About Blue Teaming)***

Before you go, take one last shot at getting all your questions answered. This interactive panel will let you bombard some of SANS's top blue team instructors with anything and everything you've been wanting to ask.

MODERATOR:

Seth Misenar *@sethmisenar, Fellow, SANS Institute*

PANELISTS:

John Hubbard *@SecHubb, Certified Instructor, SEC450*

Andy Laman *@andylaman, Certified Instructor, SEC503*

Scott Lynch *@packetengineer, Instructor, SEC555*

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.