Monday, June 24	
9:00-9:15 am	*Welcome and Opening Remarks* **Chris Crowley (@CCrowMontance), Summit Chair and Principal Instructor, SANS Institute**
9:15-10:00 am	*Keynote* **Lessons Learned Applying ATT&CK-Based SOC Assessments** The ATT&CK framework has seen a rise in popularity in the security community, with more and more Security Operations Centers (SOCs) wanting to ATT&CK. To help SOCs get into the game of using ATT&CK, MITRE has developed a process to quickly gauge a SOC's detective capabilities as they relate to the ATT&CK framework, producing a coverage heatmap as well as a set of recommendations the SOC can use to improve its operations. The process is low-overhead, focusing only on interviews and documentation analysis, but it provides useful results for SOCs that want to understand how their current capabilities stack up to ATT&CK. In this talk, we'll call on our practical experiences to describe some of the key lessons learned we've discovered when applying ATT&CK-based SOC assessments, ranging from the best ways to conduct the assessment to how to effectively communicate results to leadership. The lessons and tips that we present will be widely accessible, helping those who are interested in conducting third-party assessments, who want to assess their own SOCs, or who just want to learn about the assessment process in general. Attendees should walk away with a better understanding of how they can run and use ATT&CK-based SOC assessments, including tips on avoiding traps and pitfalls in the process. **Andy Applebaum (@andyplayse4), Lead Cyber Security Engineer, MITRE**
10:00-10:30 am	**Networking Break**
10:30-11:05 am	**Use Case Development Utilizing an ARECI Chart** This presentation will describe use case development from the perspective of a Managed Security Service Provider (MSSP) but that is also useful for internal SOCs/CERTs. The case starts with a simple requirement statement, through scenario development, and on to the Analysis of Required Evidence for Correlation and Investigation (ARECI) chart to help inform engineers about alert development and system owners about detection development. The ARECI chart consists of a list of data/sources that analysts and engineers will rely on to conduct their respective work. This data/source list will be categorized, broken down into specific sources, and then analyzed for its value to alert development as well as incident response investigation. Data and sources are not limited to ingested log/event streams. Data can include data retained in the SIEM from system infrastructure, asset databases, configuration databases, org personnel data, threat intelligence,

	etc. Once a few team members (OPs and engineering alike), have derived what data/sources they think they need to complete their work, attention turns to the environment to ascertain if those data are available, available in the SIEMS, or not available at all. This then completes the ARECI chart and allows for conducting a feasibility assessment to determine whether the use case should move forward into an engineering phase, the environment needs to be adjusted, or new capability needs to be added to satisfy (remove gaps from) the chart requirements. Multiple ARECI charts from similar enough use cases can then be stacked to produce a compound list of gaps, which can then be ranked, prioritized, and packaged for advice to the customer. Finally, a key component to the use case development life cycle is teamwork. The fusion of security operations/analytics staff and SIEMS engineering staff at the early stage of the development life cycle helps both sides appreciate their distinctly different work and discreet goals. It creates a developer/user relationship that enhances the overall development of detection and alert presentation, and helps SOCs keep ahead of efforts to evade detection while improving their own capability and avoiding atrophy. **Nathan Clarke (@GeekNathn), APAC Advanced SOC (ASOC) Manager, Verizon Australia**
11:05-11:40 am	**Use Cases Development as a Driver for SOC Maturation** When developing a Security Operations Center (SOC), it is important to define what you want to accomplish and to develop a road map to get there. The road map initially includes the development of policies, procedures, and process implementation to mature the SOC to a point where it is defined and repeatable. It is capped off by identifying and reporting on metrics, and having management review the program on an annual basis for effectiveness. At the heart of process development is identifying and maturing use cases. When standing up a Security Operations Program, whether it is a stand-alone program in large organizations or involves conducting security operations as another aspect of everyday information security policies, it is important to understand what a mature program should look like. Example goals and objectives might focus on understanding what is “on the wire” and “how endpoints are behaving”. This means knowing what protocols, connections, and data are in use, being made, and flowing in, out, and through the network. It also requires understanding what services, processes, and applications are running on each endpoint. Attendees will learn about developing the desired outcomes for the SOC, identifying use cases, and the understanding the process of maturing the use cases. Two examples of use cases developed and consistently matured will be shared, including identifying malicious user agent strings and suspect SMB connections. Attendees will learn how effective alerting becomes when the use cases that are employed are matured over time, focusing on attack vectors specific to threats the entity faces and specific protocols, services, and processes available internally. By the end of the presentation you will be armed with activities that you can begin using on your first day back at the office. **Eric C. Thompson (@ectcyberhipaa), Director of Information Security and IT Compliance, Blue Health Intelligence**

11:40 am – 12:15 pm	**IOCs: Indicators of Crap** "You should be looking at Indicators of Compromise!" exclaims your CISO, regulator, vendor, and mom. No problem, right? You're using the most expensive security intelligence vendor, and all you have to do is correlate in your expensive Security Information and Event Management platform! Well, if you have tried this, then you are laughing with us. Come hear this exploration into implementing IOCs at a major U.S. insurance company and bank. We'll address the differences between Indicators of Compromise and Indicators of Attack, and we'll give you some tips on how to use the MITRE ATT&CK framework – as well as how not to use it. The goal is to save you from the pitfalls of dealing with Indicators of Crap. **Xavier Ashe @xavierashe, VP - Security Engineering and Delivery, SunTrust**
12:15-1:15 pm	**Lunch**
1:15-1:50 pm	**Mental Models for Effective Searching** One of the most intimidating challenges many analysts face 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 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; and Founder, Rural Technology Fund (@RuralTechFund)**
1:50-2:25 pm	**Rapid Recognition and Response to Rogues** The need to detect rogue devices on a network is part of the first control listed in the CIS Top 20 Critical Security Controls (Actively Manage Inventory and Control of all Hardware Assets). There are many solutions to monitor, detect, and respond to rogue devices on enterprise networks. These include commercial, open-source, and home-grown capabilities. Each solution uses different methods of determining what a rogue device is. In this talk we will cover several of those methods along with their strengths and weaknesses. We'll also discuss the pros and cons of different responses that enterprises can take when rogues are found. But we will focus on using different techniques to show how a simple detection, which is usually just an IP address, can be enhanced to provide enough details to the analyst to speed up response decisions and even automate some responses based on business logic. We'll demonstrate this by using one rogue detection tool to tackle a simple detection of a suspicious IP, add information to the event to make analysis easier, and show how that enhanced event can be used for automated responses. **Craig Bowser (@reswob10), Senior Security Engineer, U.S. Department of Energy**

2:25-2:55 pm	**Networking Break**
3:00-3:35 pm	**Virtuous Cycles: Rethinking the SOC for Long-Term Success** Many Security Operations Centers (SOCs) have a burnout problem that leads to negativity and constant turnover. With the increasing cybersecurity talent shortage, keeping the people we have will only become increasingly important. The problem is that "Tier 1" and other SOC roles seem destined to burn people out. So what do we do? While the field of psychology understands the factors that cause burnout, many SOCs do not take the time to do the research and create an environment to fight it. Though meticulously defined process and tiering may be the norm, does it lead to sacrificing quality in the long term? Using science-backed research on intrinsic motivation and studies on SOC burnout factors, this talk will make the case that it's time to reconsider how we structure SOCs in order to create long-term success that benefits both the individual and the organization. **John Hubbard (@SecHubb), Author and Certified Instructor, SANS Institute**
3:35-4:30 pm	**2019 SANS SOC Survey Preview: Live Simulcast** The 2019 SANS SOC Survey will be released early July. Join Chris Crowley during this live webcast at the SOC Summit for a discussion of what's new in this year's survey, and a sneak peak into topics and responses from this year's results. He will talk about the detailed interviews included this year, and highlight the methodology used to develop the results that many organizations use to direct SOC activities for the following year. If you can't attend the 2019 SANS SOC Summit in New Orleans, this is a great webcast to attend. **Chris Crowley (@CCrowMontance), Senior Instructor, SANS Institute**
4:30-4:45 pm	*Day 1 Wrap-Up and Action Items*
6:00 – 8:00 pm	*Summit Night Out* **Let's Roll!** Head down the street just a few blocks to Fulton Alley. Food, drinks, bowling lanes, and shoe rentals are on us. Bragging rights up for grabs. Wear your attendee badge for access to the event.
Tuesday, June 25	
9:00-9:45 am	*Keynote* *To be announced*
9:45-10:15 am	**Networking Break**
10:15-10:50 am	

	Breach -> ATT&CK -> Osquery: Learning from Breach Reports to Improve Cross-platform Endpoint Monitoring There's plenty of news about breaches, but the reporting is usually so vague that as defenders we don't get good enough useful information about what actually happened to help us improve our defenses. However, in 2018, both the SingHealth (Singapore) and Equifax (United States) breaches resulted in significant, detailed reports. In this talk, we will look at significant findings from these reports and map them to the MITRE ATT&CK framework in order to understand if our defenses are effective. We will then look to see how we can monitor our systems with the open-source and cross-platform tool Osquery in order to detect such breaches on Windows, Mac, and Linux. **Guillaume Ross, Lead Security Researcher, Uptycs**
10:50-11:25 am	**Shared Security Services: How to Adjust to an Ever-growing Landscape of Security Operations Center Responsibilities** As organizations have grown to understand the importance of growing their Security Operations Centers (SOCs) to support the needs of their business units, security teams have also had to take on greater workloads and demands. SOCs are forced to accommodate to the growth of the business at the expense of the quality of their own work. This talk will help you realize the full potential of your SOC and consolidate its success for years to come. Topics of takeaway will include metrics that can be used to track a SOC that is being overworked; how to approach upper management to ask for resources to help grow and strengthen a shared SOC; how using threat intelligence can make more informed and smarter alerts to help reduce workloads; how to grow SOCs using a risk-based approach; and how growth spurs the need for a SOAR-based approach, and how to implement such an approach. **Kevin Garvey (@TheKevinGarvey), Manager - Incident Response and Threat Management, Warner Media**
11:25 am-12:10 pm	**The Call Is Coming from Inside the House: How Does Your SOC Respond When Attackers Are On-Site?** Many of the most agile and well-trained blue teams rehearse response procedures and conduct tabletop scenarios to better prepare for incidents as overt as targeted phishing campaigns by outsiders, as subtle as illicit data exfiltration by a data breach, and as innocuous as unauthorized network activity by over-zealous employees. And while you may think you've prepared and practiced for a wide range of threats, have you ever considered how your Security Operations Centers (SOC) would react during a physical compromise? My team engages in physical security penetration, inserting ourselves within your perimeter and proceeding on-site through corporate campuses, office buildings, and data centers. During the course of such operations, we engage in a wide range of tactics specifically geared to frustrate and confuse SOC teams. This talk will walk attendees through a series of case studies of what can happen if attackers have direct access to doors, compromise your communication system, or don your own company uniforms.

	How would your SOC react to attackers who don't simply show up on network maps, but rather show up at the front door? **Deviant Ollam (@deviantollam), Director, CORE Group**
12:10-1:30 pm	**Lunch**
1:30-2:05 pm	**How to Literally Think Like an Attacker to Become a Better Defender** For years, defenders have been educating themselves on the tradecraft being used by adversaries. At the same time, defenders continue to lose the battle, even when armed with some of the greatest talent and technologies in the world. Why is this? This talk will examine why technology alone is not helping close the gap and explain the importance that our own minds play in the role of defense. Attendees will learn: • Key similarities between defenders and attackers • How to avoid counterfactual thinking that focuses on past negative events • The role our thoughts play in behavior and outcomes • Strategies for adopting a new forward-looking mindset that instills ownership, pride, and confidence **Eric Groce, Incident Handler, Red Canary**
2:05-2:40 pm	*Talk to be announced*
2:40-3:00 pm	**Networking Break**
3:00-3:35 pm	*Talk to be announced*
3:35-4:10 pm	**Managing Security Operations in the Cloud** Our goal is to prevent unexpected access to cloud resources. To do this we must maintain strong identity and access policies (IAM) and effectively detect and react to changes. In this session we will discuss tools within the cloud for managing IAM in order to control access to cloud resources. We will also cover how to deploy and control cloud infrastructures using code templates that include change management policies. **Marc Baker, Online Training Subject-Matter Expert, SANS Institute**
4:10-4:45 pm	*Talk to be announced*
4:45-5:00 pm	*Wrap-Up and To Do List*

Speaker Biographies

Andy Applebaum (@andyplayse4), Lead Cyber Security Engineer, MITRE
Andy Applebaum is a Lead Cyber Security Engineer at MITRE where he works on applied and theoretical security research problems, primarily in the realms of cyber defense, security automation, and automated adversary emulation. Andy has contributed to MITRE's ATT&CK framework and CALDERA adversary emulation platform, as well as other projects within MITRE's internal research and development portfolio. Prior to working at MITRE, Andy received his PhD in computer science from the University of California Davis, where his dissertation topic was using argumentation logic for reasoning in cyber security. Andy has published numerous papers and spoken at multiple academic and industry conferences, most recently at Black Hat Europe. In addition to his PhD, Andy holds a BA in computer science from Grinnell College and the OSCP certification.

Xavier Ashe is a Georgia Institute of Technology alumnus and has 25 years of hands-on experience in information security. Working for various security vendors and consulting firms for the last 15 years, including IBM, Gartner, and Carbon Black, Xavier has been focused on helping secure companies of all sizes. Xavier was the first hire at the startup Drawbridge Networks, where he was instrumental in bringing the first microsegmentation solution for servers and workstations to market. Xavier served on the IBM Security Architecture Board driving many internal IBM projects. Xavier has been invited to speak at several conferences including DefCon, BSides, and SANS and has published several papers. Mr. Ashe holds many industry certifications, including CISM, CISSP, ITIL, SOA, and others.

Marc Baker, Online Training Subject-Matter Expert, SANS Institute
Marc Baker 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 master,s 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 (Cloud Practitioner and Certified Solutions Architect - Associate).

Craig Bowser (@reswob10) Senior Security Engineer, U.S. Department of Energy
Craig Bowser is an InfoSec professional with 18 years of experience in the field. He is a SANS Mentor for SEC555: SIEM with Tactical Analytics. He has worked as an Information Security Manager, Security Engineer, Security Analyst, and Information System Security Officer at the Departments of Defense, Justice, and Energy. Craig is a father, husband, geek, and scout leader who enjoys woodworking, sci-fi fantasy, home networking, tinkering with electronics, reading, and hiking. And he has a to-do list that is longer than the to-do time slots available.

Chris Crowley (@CCrowMontance), Senior Instructor, SANS Institute
Chris Crowley has 15 years of industry experience managing and securing networks. He currently works as an independent consultant in the Washington, DC area focusing on effective computer network defense. His experience includes penetration testing, security operations, incident response, and forensic analysis. He is the course author for SANS MGT 517: Managing Security Operations and MGT535: Incident Response Team Management. He holds the GSEC, GCIA, GCIH (gold), GCFA, GPEN,

GMOB, GASF, GREM, GXPN, and CISSP® certifications. His teaching experience includes FOR585, MGT517, MGT535, SEC401, SEC503, SEC504, SEC560, SEC575, and SEC580; Apache web server administration and configuration; and shell programming. He was awarded the SANS 2009 Local Mentor of the year award, which is given to instructors who excel in leading SANS Mentor Training classes in their local communities.

Nathan Clarke (@GeekNathn), APAC Advanced SOC (ASOC) Manager, Verizon Australia
Nathan's career in IT began within the Australian Defense Force (Army) from 1996 to 2015. His experience has spanned a multitude of strategic and tactical information systems, administration, planning, security, deployment and withdrawal of purpose built systems domestically and globally supporting military operations.

Nathan specializes in Cyber Security Operations, Incident Response, and Detection Development. Having worked in three SOCs, he is extremely passionate about the development of incident responders, their training/mentoring, process development, SIEMS development, and running the day-to-day operations of a SOC.

Kevin Garvey (@TheKevinGarvey), Manager - Incident Response and Threat Management, Warner Media
Kevin Garvey has worked in IT for 8 years and has been devoted to cyber security since 2013. Since becoming an analyst, he has worked at New York Power Authority, JP Morgan and is currently employed at Time Warner as a manager of Threats and Incident Response. Kevin has always has had a passion to hunt down the adversary has loved the challenges his current role has thrown at him. Kevin is incredibly excited to share this knowledge with everyone taking the course!

Deviant Ollam (@deviantollam), CORE Group
Deviant Ollam - While paying the bills as a security auditor and penetration testing consultant with The CORE Group, Deviant Ollam is also a member of the Board of Directors of the US division of TOOOL, The Open Organisation Of Lockpickers. His books Practical Lock Picking and Keys to the Kingdom are among Syngress Publishing's best-selling pen testing titles. At multiple annual security conferences Deviant runs the Lockpick Village workshop area, and he has conducted physical security training sessions for Black Hat, DeepSec, ToorCon, HackCon, ShakaCon, HackInTheBox, ekoparty, AusCERT, GovCERT, CONFidence, the FBI, the NSA, DARPA, the National Defense University, the United States Naval Academy at Annapolis, and the United States Military Academy at West Point. His favorite Amendments to the US Constitution are, in no particular order, the 1st, 2nd, 9th, & 10th.

Deviant's first and strongest love has always been teaching. A graduate of the New Jersey Institute of Technology's Science, Technology, & Society program, he is always fascinated by the interplay that connects human values and social trends to developments in the technical world. While earning his BS degree at NJIT, Deviant also completed the History degree program at Rutgers University

Guillaume Ross @gepeto42, Lead Security Researcher, Uptycs
Guillaume researches better ways to use data at Uptycs to protect and monitor systems. With experience in startups, tech and finance, from Fortune 50 to fewer than 50 employees, bringing usable ways to truly secure systems beyond the usual best-practices is what he likes the most about his job.
Chris Sanders (@ChrisSanders88), Mentor, SANS Institute; Founder, Network Defense; Director, Rural Technology Fund
Chris Sanders is a network security researcher, consultant, and author originally from around Paducah, Kentucky. He currently resides in Charleston, South Carolina.

Chris serves in a leadership position as a government defense contractor where he interfaces with various federal entities in an effort to provide a more secure cyber posture for United States defense networks.
His book Practical Packet Analysis is widely respected as one of the best practical use books on its topic and has sold several thousand copies internationally. Along with this, Chris has written and co-written hundreds of articles on the topics of packet analysis, intrusion detection, and general network security.
In 2008, Chris founded the Rural Technology Fund. The RTF is a 501(c)(3) non-profit organization designed to provide scholarship opportunities to students from rural areas pursuing careers in computer technology. The organization also promotes technology advocacy in rural areas through various support programs. You can read more about the RTF at http://www.ruraltechfund.org.
Chris has a bachelor's degrees in telecommunications from Murray State University and currently holds several industry certifications including being recognized with CISSP, GCIA, GCIH, GSEC, and GREM distinctions. His personal blog is located at http://www.chrissanders.org.

Eric C. Thompson (@ectcyberhipaa), Director of Information Security and IT Compliance, Blue Health Intelligence

Eric Thompson is a GIAC Certified Incident Handler and Intrusion analyst. He is currently the Director of Information Security and IT Compliance at Blue Health Intelligence, a company focused on data analytics in the Healthcare Payer space. Eric's skills include implementing and maturing continuous monitoring, vulnerability management, threat intelligence and incident response programs. He loves working with Bro, especially scripting, Snort and perusing packets in Wireshark. Eric also has significant experience assessing and managing cyber risks and complying with HIPAA.