Monday, October 7	
9:00-9:15 am	Welcome & Opening Remarks • **Justin Henderson**, @@SecurityMapper, Summit Co-Chair • **John Hubbard,** @SecHubb, Summit Co-Chair
9:15-9:50 am	*Keynote* **John Hubbard**, @SecHubb, Summit Co-Chair
9:55-10:30 am	**Get the Basics Right!** **Balaji Nakkella,** Senior Consultant, Deloitte Canada **Rakesh Kumar Narsingoju,** @Rakeshwill, Solution Delivery Advisor, Deloitte US-India Most organizations deploy SIEM to serve two main purposes: achieve compliance and improve their security posture. Although there are multiple compliance-related frameworks specific to each industry, assessing existing security posture is a challenge. Hence, organizations leverage SIEM solutions for this purpose, but they fail to tap its true potential due to high volumes of data, lack of proper detection rules, and high false-positive rates. In most cases, SIEM solutions are deployed by third parties, and we need to ask those parties the right questions in order to have a high degree of confidence on detection capabilities and further improve security posture. This talk focuses on identifying the blind spots where the necessary data are not available; baselining rules and mapping them to threat categories; identifying areas where a SIEM solution is not enough for investigation; and examining automation strategies to reduce the mean time to detect and respond to incidents. We will provide a checklist that helps an organization go through all the phases from risk assessment to post-SIEM deployment maintenance. This checklist is neither industry- nor vendor-specific, but serves as a holistic reference guide for any organization.
10:30-11:00 am	**Networking Break**
11:00-11:35 am	**We Need to Talk about the Elephant in the SOC**

	Jim Apger, @JimApger, Security Specialist, Splunk Why have we accepted alert fatigue as a normal occurrence in the Security Operations Center (SOC)? And why are we compounding the problem by whitelisting and suppressing the noise to the point where we have essentially created a situational security numbness within the enterprise? Our data are trying to tell us a story. The MITRE ATT&CK framework helps us figure out where we are in terms of our ability to tease the story from the data while simultaneously providing guidance for building out our own threat models. In this talk, we will go into detail to describe a trend we are seeing that introduces a layer of abstraction between detection analytics and the alerting process; both align nicely with ATT&CK and also account for user/system-specific context when scoring anomalous or interesting behavior. Attendees will learn how an organization of any size can transform its SOC quickly by reducing the alert overload, improving its false positive rates, adding data/analytics without scaling up the number of analysts, and aligning against a framework of its choice.
11:40 am – 12:25 pm	**Custom Application Behavioral Security Monitoring Using SIEM** • **Prithvi Bhat,** Junior Manager, Deloitte Nederland • **Himanshu Tonk,** @tonkhimanshu2, Junior Manager, Cyber Risk Services, Deloitte Risk Advisory Welcome to the Application Security Monitoring session. This presentation will take you through the roller coaster ride that is setting up security monitoring for custom applications and devices. Limited communication between business owners and security teams can leave a gap in security monitoring, which poses a threat to your company's security. This session will focus on the detailed process of setting up security monitoring for crown jewels, including the identification of business risks and relevant applications; how to define technical-use cases to cover business risks and the onboarding of data to your SIEM platform. We will also discuss the implementation of SIEM content and best practices for setting up, alerting, and follow-up.
12:30-1:30 pm	Lunch
1:30-2:15 pm	*Panel to be announced*
2:20-2:55 pm	*Session to be announced*
2:55-3:20 pm	

	Networking Break
3:25-4:00 pm	**The Right Data at the Right Time** **Jeff Bollinger,** @jeffbollinger, CSIRT Investigations and Analysis Manager, Cisco **Matthew Valites,** @matthewvalites, US West Outreach Lead, Cisco Talos Analysts and incident responders have so many tools and data sources to choose from that it can be daunting to understand what is necessary versus what is simply nice to have. When putting together a monitoring playbook, it's essential to understand what data are available to you and how they can be used for security monitoring and incident response. Enterprise analysts may have different data preferences than analysts at smaller organizations. How can detection and incident response (IR) teams effectively protect their organizations with the right data sources? How can you deliver context with raw machine data? This presentation will draw from years of experience in designing and operating world-class network security operations to help you understand the "ideal" set of data sources for security monitoring and IR for any environment; consider data sources depending on your size or threat profile; operationalize event data (extract, transform, load); and understand the evolution of your security event data. We'll look at real-world incidents involving data perceived to be undervalued, and at clever ways to use other data sources.
4:05-4:40 pm	**Don't Be a SIEMingly SOAR Loser...** **Rob Gresham,** @socologize, Security Solutions Architect, Splunk This title is so perfect for this discussion. Security operations, automation, and response constitute an awesome path for security teams, whether it's automation attached to the SIEM or a stand-alone orchestration tool. We love innovation, yet it seemingly creates such a SOAR on our seating devices. Where is the value in our SOAR products, and how long will it take until we are rewarded? Is it measured by your detection or response time? Containment, reimage, or resolution times? Is it a ticketing tool, case management, or neither? What is the difference between ticketing and case management tools? There are generally two approaches to the SOAR implementation models. One is as infinite as the ocean and the other is how you "really" work. We will explore these areas, offer suggestions, and provide some definitive truths (IMHO). We'll use the TTP0 fractal to define our flows and I2A2 to collect that SOEL, and if you don't SOAR after implementing those. We will demonstrate how your existing use cases or tribal knowledge can be exploited to deliver powerful automation and response, and how the human-machine team can be taken up a notch and work immediate automation into your processes that will lead to true orchestration. SOARing isn't an easy task (even though some make it look so easy, right?) and yet all of us want to fly or be flown.

6:00-8:00 p.m.	**Summit Night Out** Give your overworked brain a rest and join us for complimentary food, drink, networking and fun. We'll announce the venue closer to the date.
Tuesday, October 8, 2019	
9:00-9:45 am	Keynote **Dr. Johannes Ullrich,** Fellow, SANS Institute
9:50-10:25 am	**Techniques to Reduce Alert Fatigue in Security Analysts** **Ram Shankar Siva Kumar,** @ram_ssk, Data Cowboy, Azure Security Data Science, Microsoft **Sharon Xia, @sharonxia,** Principal Program Manager, Cloud+AI Security, Microsoft Alert fatigue is real. Security analysts face a huge burden of triage because they not only have to sift through a sea of alerts, but also correlate them from different products manually or use a traditional correlation engine. This talk describes the flagship machine learning system embedded within Azure Sentinel, Microsoft's Cloud SIEM, to tackle alert fatigue. It will describe how to obtain a 90 percent reduction in alert fatigue for internal and external customers. Attendees will learn about three techniques to reduce alert fatigue (probabilistic kill chain, iterative attack simulation, and graphical inference); a framework to combine alerts from multiple cloud services; and a design pattern to scale detection systems. We'll then walk through the series of steps in the ML system within Azure Sentinel that go from low-fidelity alerts to security alerts, and we'll demo this system in action combining O365 logs with Azure Active Directory alerts. The talk will wrap up with a look at a framework to combine the system, sharing how to normalize events across different products and presenting an engineering pattern design for others to build on.
10:25-10:45 am	Networking Break
10:50-11:25 am	**Effective Log Monitoring & Events Management for Small and Medium-sized Businesses** **Russell Mosley**, @sm0kem, CISO, Dynaxys **Ryan St. Germain,** Senior Security Engineer, Dynaxys Russell and Ryan will walk through their log and events management strategy and implementation at a small technology company to meet security needs and compliance with government contractor regulations. Specifically, they will be covering log collection, analysis, and a review process sufficient to pass audit

	requirements. Learn what, why, and how to implement and achieve your goals through examples of 50-plus daily log review tickets. The presenters will go into detail, explaining their process so that you can replicate it with open-source or commercial tools. This talk will show you how to use this information to fine-tune your tools.
11:30 am – 12:05 pm	**Company Phishing Trip: Analysis of Brand Phishing Kits and Campaigns** **Jared Peck,** @medic642, Cyber Threat Intelligence Analyst, Fortune 500 Financial Company Individuals and companies lose hundreds of millions of dollars every year to phishing. Fast detection of phishing pages and the harvested credentials is an ever-challenging task, but all hope is not lost. Using free and open-source tools we can detect sites targeting our customers and track compromised credential use by using active defense techniques. This talk will look at how common phishing campaigns are put together; the anatomy of a phishing kit, including detailed code analysis of samples; and detection of brand phishing pages (open-source, paid, and home-grown detection). Takeaways will include how phishing campaigns work, how common phishing kits operate, and how to use active defense to detect phishing kits targeting your brand.
12:10-1:15 pm	**Lunch**
1:20-1:55 pm	**That SIEM ~~Won't~~ Will Hunt** **John Stoner,** @stonerpsu, Principal Security Strategist, Splunk Hunting is not the first thought that comes to mind when someone says SIEM, is it? But do you know that SIEM can be another tool that threat hunters on the security operations team can leverage effectively as part of their hunt? This talk uses the fictional advanced persistent threat group Taedonggang to demonstrate how SIEM can be used to aid our hunt activities. We will talk about MITRE ATT&CK and the intersection of threat hunting and security operations, and how threat hunt findings should be operationalized into SIEM for the security operations team. Operationalizing refers to more than just a blacklist of IP addresses and file hashes! John Stoner will show how we can tie our findings to adversary tactics and techniques that can then have automated responses built to address these techniques as they are identified in the future. Attendees will come away with an understanding how SIEM can be used during threat hunting; knowledge of how MITRE ATT&CK can serve as a common taxonomy in SIEM for both security operations and threat hunters; ideas for how to create SIEM alerts and views based on threat hunts; and a data set and instructional application that they can take home and play with!

2:00-2:35 pm	**Hunting with Sysmon to Unveil the Evil** **Felipe Esposito,** Senior Instructor at Blue Team Operations, BlueOps Consulting and Training **Rodrigo Montoro,** @spookerlabs, Head of Research and Development, Apura Cyber Intelligence System Monitor (Sysmon) is a Windows system service and device driver that, once installed, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. These logs provide investigators with a wealth of information that can be analyzed in many different ways. By splitting analysis in each field of a Sysmon event alert, you can create a deeper analysis of the event itself and create a hunting view that could point you towards certain processes or behaviors in order to better analyze or find uncommon processes in your endpoints. By correlating these alerts with your network and business requirements, you can make detection more accurate and generate less noise, thereby helping your staff prioritize which events to handle first. This presentation will discuss methods to analyze and score each field from those events, ideas for implementation, projects, and results based on deployment. We'll also show how you can improve your hunting capabilities by using Sysmon as a more powerful detection vector to identify specific user behaviors and activity patterns.
2:40-3:25 pm	*Talk to be announced* **Greg Scheidel** @Greg_Scheidel, Instructor, SANS Institute
3:25-3:45 pm	**Networking Break**
3:50-425 pm	**Operationalizing Incident Response** **Shane Harsch**, Senior Manager, RSA; Community Instructor, SANS Institute What are the roles required for successful live response operations? What does the team structure look like? Shane will share the experience of the RSA Global CIRT and discuss the fundamental structure and workflow for organizations even as small as three people.
4:30-5:05 pm	*Title and session description to come* **Scott Lynch**, Cyber Security Operations Manager, SSC Space U.S.
5:05-5:15 pm	*Wrap-Up and Takeaways*

6:30-9:30 pm	***SIEM NetWars*** SIEM NetWars is a hands-on, interactive learning scenario that enables security professionals to develop and master real-world, in-depth skills they need to efficiently and effectively leverage their SIEM to gain actionable intelligence and defend their organization. Participants learn in a cyber range while working through various challenge levels with a focus on mastering the skills information security professionals can use in their jobs every day. All Summit and training attendees are welcome to participate.

Speaker Biographies

Jim Apger, @JimApger, Security Specialist, Splunk
Jim earned his bachelor's degree in electrical engineering from Ohio State University, marking the beginning of his data-centric career. He has spent many years pushing electrons, packets, and analytics in the fields of engineering, networking, anti-fraud, and security.

Prithvi Bhat, Junior Manager, Deloitte Nederland
Prithvi has been a cybersecurity professional for the past eight years. She started as a security analyst in Cognizant-India, and later moved to Europe to do a wide range of work with different clients. She moved on to work at Deloitte, managing MSSP delivery and serving as an advisor for building SOCs and increasing their maturity. Currently, her focus is on innovation and business development in cyber risk. She is married to another cybersecurity professional and resides in Amsterdam, where she enjoys painting and hiking in her spare time.

Jeff Bollinger, @jeffbollinger, CSIRT Investigations and Analysis Manager, Cisco
Jeff joined Cisco Systems in 2002 supporting security technologies and solutions in its global technical support organization. He later moved to the Computer Security Incident Response Team and rapidly developed its global security monitoring and incident response capabilities. With over 15 years of information security experience, he has worked as a security architect, incident responder, and human resources manager for both academic and enterprise networks. He specializes in investigations, network security monitoring, log analysis, and intrusion detection. Jeff currently manages Cisco's SOC and investigations teams in the Western Hemisphere. He helped build and operate one of the world's largest corporate security monitoring infrastructures and regularly speaks at international FIRST conferences, while occasionally writing for the Cisco Security Blog. He co-authored the *Crafting the InfoSec Playbook.*

Felipe Esposito, Senior Instructor at Blue Team Operations, BlueOps Consulting and Training
Felipe has 10 years of experience in T.I., and a masters in computer systems and networking. His interests include network covert channels, information visualization, log analysis and incident response. He is currently employed by the Rio de Janeiro State Court in Brazil as a Network Security Administrator, working hard to make the government's environment as responsive as possible to threats.

Rob Gresham, @socologize, Security Solutions Architect, Splunk
Rob has over 15 years of experience in building security operations teams and conducting incident response. He has provided forensics and threat intelligence to both public and private entities in support of civil and criminal investigations. His experience includes years of instructing on cyber threat intelligence, incident response, and overall security operations architecture and design. He currently works as a global Security Solutions Architect at Splunk.

Justin Henderson, @@SecurityMapper, Summit Co-Chair
Justin Henderson is a passionate and dedicated Information Technology professional. He has been in the Information Technology field since 2005. Justin has a proven desire and ability to achieve comprehensive industry training and uses his knowledge and experience to mentor others. Justin has a high proficiency in technical platforms including operating systems, networking, security, storage, and

virtualization but has also applied himself in governance, project management, as well as service management. Currently, Justin holds a Bachelors of Science in Network Design and Administration from Western Governors University and has over 40 certifications.

John Hubbard, @SecHubb, Summit Co-Chair
John is a dedicated blue-teamer and is driven to help develop defensive talent around the world. Through his years of experience as the SOC Lead for GlaxoSmithKline, he has real-world, first-hand knowledge of what it takes to defend an organization against advanced cyber-attacks and is eager to share these lessons with his students. As a SANS Cyber Defense curriculum instructor and course author of SEC455, John specializes in threat hunting, network security monitoring, SIEM design and optimization, and constructing defensive postures that allow organizations to protect their most sensitive data.

Rakesh Kumar Narsingoju, @rakeshwill, Solution Delivery Advisor, Deloitte US-India
Rakesh is a lead security analyst at Deloitte USI serving global clients across various industries. As a cyber-warrior, he advises clients on security incidents and helps them in protecting from cyber-attacks. Off work, Rakesh loves playing cricket and wanderlust consumes him.

Rodrigo Montoro, @spookerlabs, Head of Research and Development, Apura Cyber Intelligence
Rodrigo has 18 years of experience deploying open-source security software. Currently he is Head of R&D at Apura Cyber Intelligence. He previously worked as a researcher at Clavis and Spiderlabs, and as Senior Security Administrator at Sucuri. He is the author of two patents involving the discovery of malicious digital documents and the analysis of malicious HTTP traffic.

Russell Mosley, sm0kem, CISO, Dynaxys
Russell has 18 years of experience in IT operations and security management, holds degrees from the University of Maryland Baltimore County, University of Maryland University College, and Towson State University, as well as the CISSP®, PMP®, and several vendor certifications. Yet he still knows how to use tcpdump! Russell is an organizer with BSides Charm and the DefCon Blue Team Village. He is passionate about network defense.

Balaji Nakkella, Senior Consultant, Deloitte Canada
Balaji is a Sr. SIEM Engineer at Deloitte helping Fortune 500 giants implement cyber security controls. Apart from keeping bad guys off the grid, Balaji enjoys cooking Indian cuisine and Vacation.

Jared Peck, @medic642, Cyber Threat Intelligence Analyst, Fortune 500 Financial Company
Jared is a threat intelligence analyst in the financial services industry. After 15 years as a firefighter and paramedic, he turned his computer hobby into a profession. He worked his way from network administrator to SOC analyst and now does cyber threat intelligence and develops attack detection logic.

Ram Shankar Siva Kumar, @ram_ssk, Data Cowboy, Azure Security Data Science
Ram is a data cowboy in Azure Security Data Science at Microsoft, where his work is in the intersection of machine learning and security. He is the founder of the Security Data Science Colloquium â€“ the only avenue where security data scientists from every major cloud provider congregate. Ram is also an affiliate at the Berkman Klein Center at Harvard University, and Technical Advisory Board Member at University of Washington. He graduated from Carnegie Mellon University with a masters in Computer Engineering and a second masters in Innovation Management.

Ryan St. Germain, Senior Security Engineer, Dynaxys
Ryan is a Senior Information Security Engineer with over 9 years of experience. He holds a Master of Science in Cyber Security and CISSP. He has presented at past BSides Charm, BSides Nova and BSides Rochester events.

John Stoner, @stonerpsu, Principal Security Strategist, Splunk
In his position as a Principal Security Strategist at Splunk, John enjoys building content, problem-solving, and blogging. When not doing cyber things, you can find him reading or binge-watching TV series' that everyone else has already seen. During the fall and winter, you can find him driving his boys to hockey rinks all over the northeast.

Himanshu Tonk, @tonkhimanshu2, Junior Manager, Cyber Risk Services, Deloitte Risk Advisory
Himanshu is a Junior Manager in Cyber Risk Services of Deloitte Risk Advisory. He has six years of extensive experience working with many types of SIEM frameworks and possesses sound knowledge about setting up security monitoring for various clients. His expertise includes threat detection, and his areas of interest are SIEM, threat hunting, and incident response.

Matthew Valites, @matthewvalites, US West Outreach Lead, Cisco Talos
With over a decade of information security experience, Matthew currently leads Cisco Talos' Outreach West. Previously he worked on Cisco's CSIRT as both an investigator and investigations manager, and most recently at Splunk as a Senior Security Specialist. He provides expertise in building security monitoring and incident response programs for cloud and hosted service enterprises, focusing on targeted and high-value assets via a threat-centric methodology. He is a published O'Reilly author with a proven ability to run global, high-profile, and complex multi-faceted investigations that impact service and revenue. Matthew strives to both learn from and share his knowledge with the global InfoSec community.

Sharon Xia, @sharonxia, Principal Program Manager, Cloud+AI Security
Sharon is the Principal Program Manager at Microsoft's Cloud+AI Security, where she oversees the ML and platform investments. Previously she was the Director of Cyber Security at GE Power Solutions and held roles as Security Architect. She is CISSP-ISSAP® certified.