SANS PURPLE TEAM SUMMIT & TRAINING

Dallas, TX | Summit: Oct 21-22 | Training: Oct 23-29

Monday, October 21, 2019	
9:00-9:15 am	Welcome & Opening Remarks **Stephen Sims, @Steph3nSims**, Fellow, The SANS Institute
9:15-10:00 am	*Keynote* **Purple Yourself** **Tim Medin @timmedin**, Red Siege Information Security Top red teamers are good at defense. The best blue teamers know offense. To up your game, you have to know the tools and techniques of your counterpart. In this talk, we'll discuss simple yet powerful tools and techniques used by red teamers with a focus on making the blue teamers more effective... and more purple.
10:00-10:30 am	Networking Break
10:30-11:05 am	**When Being Wrong Is Right: The Role of False Positives in Building a Detection Pipeline** **Ben Goerz**, @bengoerz, Cybersecurity Engineer, Kimberly-Clark Corporation If your Blue Team can't accidentally catch a vulnerability scanner, it has no hope against your Red Team or a real attacker. This talk will examine alarming data from actual incidents that turned out to be false positives, including internal password spraying and detecting a malware sinkhole. We will explore the uncertainty that occurs during the initial discovery, the embarrassment of realizing we were wrong, and how we embrace this as an inevitable part of building and tuning our detection pipeline. Attendees will come away with a better sense of the failures they should expect to encounter in their own program, and how they can turn false positives into better detections.
11:10-11:45 am	**Adaptive Adversary Emulation with MITRE ATT&CK™** **Timothy Schulz**, @teschulz, Senior Cyber Adversarial Engineer, The MITRE Corporation

	Lots of teams perform adversary simulation and emulation – you've probably heard of it. Adversary emulation blends threat intelligence into engagements to tailor red team behaviors to a real threat. This emulation allows the blue team to focus on the techniques employed by a specific adversary, but part of the challenge is that threat intelligence is a historical snapshot of an adversary's tactics and techniques. This talk will present an adversary emulation approach that allows red teams to mimic the adaptive nature of real threat actors. Using a combination of threat intelligence and adversary tradecraft, we can hypothesize how adversaries may be adapting their techniques to work in modern environments. We will use ATT&CK as a framework to help red teams add TTPs to their adversary emulations to enable blue teams to build more resilient defenses. Audiences can expect to walk away with how red teams can build more tailored adversary emulations and how blue teams can gain insight on possible variations of adversary behaviors.
11:50 am - 12:25 pm	**Evolving Your Adversary Playbooks: Incorporating Red Team Findings and Benchmarking** **Gert-Jan Bruggink**, @gertjanbruggink, Head of CTI, Deloitte One of the most resource-savvy ways to develop your adversary tracking mechanism is to focus on "how do they do it" – in other words, their playbooks. With intelligence-led red teaming, we're getting the opportunity to incorporate Red Team data into our adversary playbooks. Armed with these data, the detection team is further able to connect the dots from offensive activities in the network to what it sees in its logs. Additionally, the detection teams have the ability to fully understand what adversaries do and what the TTPs of attackers actually look like when active in their network. There's just one thing – this is not an easy journey. In this presentation, you'll learn how to combine cyber threat intelligence, red teaming and detection to improve your overall security posture against current and future attacks. We'll pay special attention to the potential failures one will likely encounter. Participants will get actionable insights on how to start their adversary playbooks. After the session, any relevant workflow(s) will be made available.
12:30-1:30 pm	Lunch
1:30-2:15 pm	**Red (Purple) Blue -> Collaboration for Optimum Results** **Prithvi Bhat**, Junior Manager - Cyber Risk, Deloitte B.V (Netherlands) **Himanshu Tonk**, Junior Manager - Cyber Risk, Deloitte B.V (Netherlands)

	Welcome to getting painted purple. A shift in attitude has paved the way for both offensive and defensive security teams to connect the dots to and from the activities on the other side. Cyber defense teams have to deal with large numbers of alerts every day to find that one event that might be of interest as well as all events based on the theoretical knowledge of TTPs that adversaries use. Asking the infamous Red Team to step out and share the techniques used and the attack path taken with the Blue Team has proven beneficial in building knowledge in the cyber defense team. In this presentation, we will discuss the tried and tested approach to Purple Teaming and how to get the most out of the activities to improve both Red and Blue Teams. Prithvi Bhat will share Deloitte B.V.'s experiences along with the benefits and the value of sessions conducted by customers. All the pillars of cybersecurity are intertwined, so it is interesting to see how collaborating can bring about a paradigm shift to benefit the industry.
2:20-2:55 pm	**Work it Out: Organizing Effective Adversary Emulation Exercises** **Jorge Orchilles**, @jorgeorchilles, Certified Instructor, SANS Institute As a highly technical InfoSec professional, you may not realize all of the non-technical considerations that go into organizing a week-long, in-person Purple Team Adversary Emulation Exercise. This talk will cover a number of items to consider, ranging from non-technical aspects (selling the exercise to senior management, obtaining budget approval, planning travel, finding a comfortable conference room, planning breaks, timing, fun, etc.) to technical aspects (identifying TTPs, setting up production systems and accounts, risk management, etc.). We will incorporate lessons learned from other Purple Team exercises performed by a number of organizations so that you can make your first exercise the most successful one possible!
2:55-3:20 pm	Networking Break
3:25-4:00 pm	**Emulating the Adversary While Training the Defenders: Purple Teaming with MITRE ATT&CK** **David Evenden** @jedimammoth, Vulnerability Exploitation Analyst, Centurylink Establishing the right processes and procedures isn't always as easy as it sounds for Blue Teams, and emulating the right adversary can sometimes seem like a daunting task when your Red Team becomes operational. We'll walk Red, Blue, and Purple teams through how to leverage the MITRE ATT&CK framework and open-source threat reporting around adversarial sector-based target attack patterns. The aim is to show how large organizations have transformed Purple Teaming into a science.
4:05-4:40 pm	**Guardians of the Purple Team Galaxy: The Purple Agenda**

	Ben Goerz, @bengoerz, Cybersecurity Engineer, Kimberly-Clark Corporation **Xena Olsen,** @ch33r10, Cyber Threat Analyst, Financial Services Industry To the guardians of Volume 1 of the Purple Team Galaxy, we pose the following question: In a world where cybersecurity is filled with con-men, rock stars, n00bs, security evangelists, dude-bros, and the rest of us, can Red and Blue Teams work together to save the galaxy? Join our intrepid band of defenders as they build out an Adversary Detection Pipeline and an Analysis Enrichment Dashboard. You'll learn how to work with the data you have to map well-known threat actors you suspect are attacking your organization to the MITRE ATT&CK framework and the Kill Chain. The focus will be on how you can create an Adversary Detection Pipeline for HUNT/DFIR/SOC with your existing tools, budget, and experience. To guardians of Volume 2 of the Purple Team Galaxy, we show that when the Red Team ATT&CKS travels with our superhero defenders to the planet of PWN ALL THE THINGS it can transform its Adversary Detection Pipeline into an Adversary Simulation menu that it can use to supercharge its ops and save the galaxy from total annihilation! On planet PWN ALL THE THINGS, some Red Team tactics are simply not realistic, including physically stealing servers, flying in drones, and socially engineering Amazon Web Services. By accepting this mission, you agree to make your Red Team more relevant to Blue by covering the TTPs of your adversaries that map back to the MITRE ATT&CK framework. You'll learn how to use the data you have to make an Adversary Detection Pipeline, how to develop a resource for DFIR/SOC to enrich analysis based on popular threat actors that attack your industry and that you suspect are attacking your environment, and how to repurpose the Adversary Detection Pipeline to create relevant adversary simulation ops.
4:45-5:00 pm	*Day 1 Wrap-Up*
5:00-7:00 pm	**Networking with a View** Meet us on the patio overlooking the lake at Trevi's Restaurant (in the hotel) for drinks, food, and networking overlooking the lake.
Tuesday, October 22, 2019	
9:00-9:45 am	**Keynote** **Enter Mordor: Pre-recorded Security Events from Simulated Adversarial Techniques** **Roberto Rodriguez** **@Cyb3rWard0g**, Security Researcher

	Whether you want to start learning about a new adversarial technique or want to validate a security analytic, you have to simulate the attack and work with the data produced. Even though It might be easy to say "just run this script," there are several other factors that need to be considered besides having the right code to run a successful simulation. Do you run it in a lab environment? Do you run it in production? Do you know how to even run it? Do you have the right audit policies deployed? Can you share the data with other teams or import it to other analytic platforms? If you do not have the right strategies in place, you might end up spending a lot of your time focused on how to produce the data rather than understanding and analyzing the data. This presentation will introduce the concept of working with pre-recorded datasets from a project named Mordor, and the benefits it has for purple operations.
9:50-10:25 am	**Optimizing Caldera for Automated Adversary Emulation** **Erik Van Buggenhout**, @ErikVaBu, Consultant, NVISO; Certified Instructor, SANS Institute MITRE ATT&CK is quickly gaining traction and becoming an important standard to assess the overall cybersecurity posture of an organization. Tools like ATT&CK Navigator and CALDERA facilitate corporate adoption and allow for a holistic overview of attack techniques and how organizations are preventing and detecting them. Furthermore, many vendors, technologies and open-source initiatives are aligning with ATT&CK. CALDERA is an automated adversary emulation system that performs post-compromise adversarial behaviour within Windows Enterprise networks. It generates plans during operations using a planning system and a pre-configured adversary model based on the ATT&CK project. These features allow CALDERA to dynamically operate over a set of systems using variable behavior, which better represents how human adversaries perform operations than systems that follow prescribed sequences of actions. MITRE released CALDERA 2.0 in April 2019. The new version includes a larger focus on “extendibility.” During this talk, we will leverage these features for maximum effect, highlight some interesting improvement opportunities in CALDERA, and focus on how to develop additional plugins and features. We’ll look at how we can improve CALDERA’s reporting engine and how we can adapt the system to work around common security controls in place at organizations. This talk will arm InfoSec professionals with the required skills to further extend their adversary emulation options without breaking the bank on a commercial tool! Our focus is to increase the adoption of CALDERA and help the community; we will also publicly release developed plugins and present several technical demos.

10:25-10:45 am	Networking Break
10:50-11:25 am	**One Hundred Red Team Operations a Year** **Ryan O'Horo**, @redteamwrangler, Lead Engineer, Red Team, Target Target's internal Red Team frequently carries out operations and extracts enormous value from each one. The company takes a microscope to its detection and response capabilities and adds minimal net-new risk doing it. This talk covers how Target diversifies its operation methodologies, tightly integrates them with the business, implements product engineering techniques, conducts training, and measures how it is achieving those goals.
11:30 am - 12:05 pm	**The Role of Threat Intelligence in Purple Team Tactics** **V. Susan Peediyakkal**, @v33na, Cyber Threat Intelligence Program Lead Consultant, Booz Allen Hamilton *Abstract to come*
12:10-1:15 pm	Lunch
1:20-1:55 pm	**Detecting and Mitigating FLAM1 Banking APT** **Huáscar Tejeda**, @htejeda, Co-Founder and CEO, F2TC Cyber Security **Rilke Petrosky Ulloa**, @xenomuta, Red Team Leader and Security Researcher, F2TC Cyber Security This hands-on Threat Intelligence workshop will present the detection, analysis of activities, reverse engineering of artifacts, and mitigation of an Advanced Persistent Threat (APT) targeting the Caribbean financial sector.
2:00-2:35 pm	**Air Force's Purple Teams: Lessons Learned from a Red Team Inside of a Blue Team** **Lillian Warner**, @blackburn_lilly, Cyber Vulnerability Assessment/Hunter (CVAH) Liaison Officer and Planner for 624 Operations Center, U.S. Air Force The rapidly increasing demand for Red Teams at the U.S. Department of Defense is stressing available resources, according to the Director of Test and Evaluation's Fiscal 2018 Report. Red Teams are busy executing in-depth cyber assessments and don't have time or personnel to address the security posture concerns of every unit, leaving warfighters and network owners with a false sense of confidence about the magnitude and scope of the cyber-attacks the department faces. Blue Teams also face tough calls. How do defenders know if there is no

	enemy to find? They need to prove that their posture on the network is sufficient, their analysts are well trained, and their response processes are useful. The Air Force's response is to create Purple Teams and Red Teams that live inside of Blue Teams. The operators in the Purple Team complete Tactical Validation Events, which is a fancy way of saying that the Red Team does things for two purposes. Purple Teams test security controls (how hardware and software responds) and security processes (how the defenders respond). This session will also discuss the reporting and feedback loop between the Blue and Purple Teams that enables the former to improve its posture on the network and its incident response processes. Attendees can expect to leave with an argument to take to their leadership as to why they need a Purple Team and what objectives they can expect such a team to accomplish.
2:40-3:25 pm	**Lessons in Purple Team Testing with MITRE ATT&CKs from Priceline and Praetorian** **Daniel Wyleczuk-Stern**, @Daniel_Infosec, Principal Security Engineer, Praetorian **Matt Southworth**, @bronx, Chief Information Security Officer, Priceline, Booking Holdings For the past year, Praetorian and Priceline have been working together to conduct a series of Purple Team exercises to improve Priceline's detection and response. These exercises have used tactics, techniques, and procedures (TTPs) from the MITRE ATT&CK framework to baseline Priceline's telemetry and analysis capabilities. Daniel Wyleczuk-Stern will begin this presentation by discussing Praetorian's contributions to the Metasploit Framework and how it can be used for TTP emulation. He'll briefly cover how to set up, deploy, and run TTPs, then conclude with a discussion on working collaboratively with the Blue Team both to decide what to execute and to draw on lessons learned and recommendations for insufficient detection. Matt Southworth will then take over to discuss how to implement program improvements based on the results of Purple Team testing. He'll review how his team prioritized the findings from the assessment and then discuss how the team determined the best course of action to remediate the issues faced when installing new tools, policy changes, configuration changes, or accepting risks. Attendees can expect to learn how to utilize Praetorian's TTP emulation framework, execute TTPs, and draw on the results of their tests to drive change.
3:25-3:45 pm	Networking Break
3:50-425 pm	
4:30-5:05 pm	**It's Hackers All the Way Down: Experiences in Improving Security by Transferring Adversarial Skills to Product Teams** **Joe Gervais**, @TryCatchHCF, Technical Director, Red Team Ops, Symantec

	Securing the digital ecosystems of Product/DevOps teams is critical to any organization. However, securing the Software Development Lifecycle (SDLC) and supporting infrastructure is often complex. In addition, product teams necessarily have access to sensitive and critical resources and credentials, making them desirable targets for adversaries. Security should be involved every step of the way, but security team resources are often constrained, and with the pace of Agile/DevOps workflows, the team can become a bottleneck. But what if every member of a product team was trained in the "Dark Arts" of attacking their own applications and infrastructure? This presentation will cover the results and lessons learned during a process of transferring real-world adversarial hacker skills to product team members. Taking a cue from the Marine Corps philosophy of "Every Marine is a Rifleman First," this approach aims to improve security in all phases of the product lifecycle by transferring adversarial hacker skills to product team members – creating what might be called an "Every Product Team Member is a Hacker First" skillset and culture. With an adversarial mindset distributed across the team, team members become force multipliers in securing their own products and environments, while reducing the traditional reliance on Blue and Red Teams. This can reduce the resource load on both those teams, while turning product members into security allies. This presentation will cover how to gain organizational support to launch such a pilot program, refine the curriculum, engage product teams, and establish rules of engagement. Attendees will learn what worked and what did not, and how to tailor this approach to fit the needs of their own organizations.
5:05-5:15 pm	*Wrap-Up and Takeaways*

Speaker Biographies

Prithvi Bhat, Junior Manager - Cyber Risk, Deloitte B.V (Netherlands)
Prithvi has been a cybersecurity professional for the past 8 years. Prithvi started as a security analyst in Cognizant- India , later moving to Europe and serves multiple clients, providing a wide range of services. At Deloitte she manages MSSP delivery and works as an advisor for building mature SOCs. Prithvi is married to another cyber security professional and resides in Amsterdam, Netherlands.

Gert-Jan Bruggink, @gertjanbruggink, Head of CTI, Deloitte
Gert-Jan assists leaders at Deloitte in making informed decisions by utilizing cyber threat intelligence and implementing relevant and sustainable cyber defenses through strategic change. He heads the Netherlands Cyber Threat Intelligence practice, leading a global top-tier intel team that specializes in strategic and operational intelligence products and intelligence-led (Red Team) exercises.

David Evenden, Vulnerability Exploitation Analyst, Centurylink
David Evenden is an experienced offensive security operator/analyst with over 12 years of active work experience inside the Intelligence Community (IC). During his time inside the IC, he learned Persian Farsi, worked at NSA Red Team and was a member of an elite international team operating in conjunction

Joe Gervais, @TryCatchHCF, Technical Director, Red Team Ops, Symantec
Joe has 25+ years of InfoSec and software engineering experience. He served as an Intelligence Analyst and Counterintelligence Specialist in the U.S. Marine Corps. He has a bachelor's degree in cognitive science and a master's degree in information assurance.

Ben Goerz, @bengoerz, Cybersecurity Engineer, Kimberly-Clark Corporation
Ben works in the Counter Threat Unit (Purple Team) at Kimberly-Clark, where he specializes in Threat Intel & Hunting. He holds an MS in information technology management and an MBA from UT Dallas.

Ryan O'Horo, @redteamwrangler, Lead Engineer, Red Team, Target
As a Red Team Lead Engineer, and former consultant, Ryan has a particular interest in continuous improvement and process analysis.

Xena Olsen, @ch33r10, Cyber Threat Analyst, Financial Services Industry
Xena is a cyber threat intelligence analyst in the financial services industry. A graduate of SANS Women's Academy with 6 GIAC certifications, an MBA IT Management, and a doctoral student in cybersecurity at Marymount University.

Jorge Orchilles, @jorgeorchilles, Certified Instructor, SANS Institute
Jorge founded The Business Strategy Partners in 2002 to provide consulting services to residential and small businesses, then founded Florida International University's MIS Club and was contracted to work on the university's Active Directory Migration Project. In 2007 he joined Terremark, a datacenter and cloud service provider acquired by Verizon. He helped build and secure Terremark's Infrastructure as a Service solution and was promoted to a Security Operations Center analyst in 2009 before moving on to an offensive analyst position with a global financial institution. Jorge has performed hundreds of application and infrastructure vulnerability assessments and penetration tests, and has led numerous teams of ethical hackers.

V. Susan Peediyakkal, @v33na, Cyber Threat Intelligence Program Lead Consultant, Booz Allen Hamilton As a Cyber Threat Intelligence Lead Consultant in Booz Allen Hamilton's Commercial Cyber Defense Program, V. Susan Peediyakkal she focuses on helping clients establish and cultivate industry-leading cyber threat intelligence programs. In March 2018, she was named one of "10 Women in Security You May Not Know But Should" by one of the most widely read cybersecurity news sites, Dark Reading.

Roberto Rodriguez, @Cyb3rWard0g, Security Researcher
Roberto Rodriquez is a Senior Threat Hunter and researcher specializing in the development of data analytics to detect advanced adversarial techniques. 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. blog at https://medium.com/@Cyb3rWard0g

Timothy Schulz, @teschulz, Senior Cyber Adversarial Engineer, The MITRE Corporation
Tim Schulz is a Senior Cyber Adversarial Engineer at The MITRE Corporation. He spends his days promoting purple teams to help sponsors improve their security. Tim contributes to MITRE's CALDERA, ATT&CK evaluations, and facilitates red team engagements. Before MITRE, Tim worked at Sandia National Labs and in a digital forensics lab.

Matt Southworth, @bronx, Chief Information Security Officer, Priceline, Booking Holdings

Matt leads the Priceline security team to reduce risk, improve customer trust, and fight the bad guys coming after our data. Matt joined Priceline in a security engineering role in 2013 and has overseen the growth and maturation of the security team and capabilities. His team is responsible for product security, network and infrastructure protection, user safety, managing PCI compliance, and incident response. His team also has operational responsibility for the security of Booking Holdings' users and data. Matt has hosted security summits for the security teams at all Booking Holdings brands, runs real-time collaboration tools to share technical data, and has also organized industry-wide Threat Exchange summits bringing together OTAs, GDSes, and metasearch providers. Prior to his time at Priceline and Booking Holdings, Matt held security engineering roles at membership and loyalty providers, health and life sciences companies, and several tech startups.

Huáscar Tejeda, @htejeda, Co-Founder & CEO, F2TC Cyber Security
Huáscar is a recognized cybersecurity expert with more than 20 years of experience in security research, penetration testing, software development, Linux kernel hacking, networking, and telecommunications.

Himanshu Tonk, Junior Manager - Cyber Risk, Deloitte B.V (Netherlands)
Himanshu is a Junior Manager in Cyber Risk Services of Deloitte Risk Advisory. He has 6 years of extensive experience working with variety of SIEM and possess sound knowledge of setting up security monitoring at various clients. He has sound knowledge around the identification on threats and converting them in technical deliverables. His areas of interest include SIEM, Threat Hunting & Incident Response.

Rilke Petrosky Ulloa, @xenomuta, Red Team Leader & Security Researcher, F2TC Cyber Security
Rilke is security tinkerer with over 15 years of experience in penetration testing, low-level programming, and telephone systems. He focuses on unexpected attack vectors, covert channels for command and control, and exfiltration. He is currently a security researcher and the Red Team leader for F2TC Cybersecurity engaged in adversarial emulation and security awareness.

Erik Van Buggenhout, @ErikVaBu, Consultant, NVISO; Certified Instructor, SANS Institute
Erik is the lead author of the SANS course SEC599: Defeating Advanced Adversaries and teaches SEC560: Network Penetration Testing & Ethical Hacking and SEC542: Web Application Penetration Testing & Ethical Hacking. In addition to his work with SANS, Erik is the co-founder of the European cybersecurity firm NVISO, which focuses on high-end cybersecurity services, specializing in government, defense, and the financial sector.

Lillian Warner, @blackburn_lilly, Cyber Vulnerability Assessment/Hunter (CVAH) Liaison Officer and Planner for 624 Operations Center, U.S. Air Force
Lillian is a Captain in the U.S. Air Force. She has been an operator, team lead, and planner for the Air Force's Purple Teams. She holds GXPN and GCFA certifications and is passionate about hacking networks in order to improve defenses.

Daniel Wyleczuk-Stern, @Daniel_Infosec, Principal Security Engineer, Praetorian
Daniel is the Purple Team lead at Praetorian, where he heads up assessments to examine and improve clients' detection and response capabilities via focused adversary emulation. He previously served as a Captain in the U.S. Air Force.