SANS

PURPLE TEAM
SUMMIT & TRAINING

Program Guide

@SANSPenTest  **#PurpleTeamSummit**

Agenda

All Summit Sessions will be held in the Mandalay Ballroom E&W (unless noted otherwise).
All approved presentations will be available online following the Summit at ***sans.org/summit-archives***

Monday, October 21

7:00-9:00 am	**Registration & Coffee** (LOCATION: MANDALAY FOYER)
9:00-9:15 am	***Welcome & Opening Remarks*** ***Stephen Sims****, @Steph3nSims, Fellow, SANS Institute*
9:15-10:00 am	***Keynote: Purple Yourself*** 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. ***Tim Medin****, @timmedin, Founder and Principal Consultant, Red Siege Information Security; Principal Instructor, SANS Institute*
10:05-10:40 am	***When Being Wrong Is Right: The Role of False Positives in Building a Detection Pipeline*** 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. ***Ben Goerz****, @bengoerz, Cybersecurity Engineer, Kimberly-Clark Corporation*
10:40-11:05 am	**Networking Break** (LOCATION: MANDALAY FOYER)
11:10-11:45 am	***Adaptive Adversary Emulation with MITRE ATT&CK™*** 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. ***Timothy Schulz****, @teschulz, Senior Cyber Adversarial Engineer, The MITRE Corporation*

Monday, October 21

11:50 am – 12:25 pm	***Evolving Your Adversary Playbooks: Incorporating Red Team Findings and Benchmarking*** 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. ***Gert-Jan Bruggink**, @gertjanbruggink, Head of CTI, Deloitte*
12:30-1:30 pm	**Lunch** (LOCATION: MANDALAY FOYER)
1:30-2:15 pm	***Red (Purple) Blue -> Collaboration for Optimum Results*** 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. ***Prithvi Bhat**, Junior Manager – Cyber Risk, Deloitte B.V (Netherlands)* ***Himanshu Tonk**, Junior Manager – Cyber Risk, Deloitte B.V (Netherlands)*
2:20-2:55 pm	***Work it Out: Organizing Effective Adversary Emulation Exercises*** 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! ***Jorge Orchilles**, @jorgeorchilles, Certified Instructor, SANS Institute*
2:55-3:20 pm	**Networking Break** (LOCATION: MANDALAY FOYER)

Monday, October 21

3:25-4:00 pm	***Emulating the Adversary While Training the Defenders: Purple Teaming with MITRE ATT&CK*** 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. ***David Evenden**, @jedimammoth, Vulnerability Exploitation Analyst, CenturyLink*
4:05-4:40 pm	***Guardians of the Purple Team Galaxy: The Purple Agenda*** VOL. 1: ADVERSARY DETECTION PIPELINES. 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. The focus will be on how you can create an Adversary Detection Pipeline for HUNT/DFIR/SOC with your existing tools, budget, and experience. VOL. 2: ADVERSARY SIMULATION - WHEN RED TEAM ATT&CKS! Travel with our Defenders to the planet of PWN ALL THE THINGS as they turn their Adversary Detection Pipeline into an Adversary Simulation menu that red team 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: physically stealing servers, flying in drones, socially engineering AWS, and more. By accepting this mission, you agree to make your Red Team more relevant to Blue thru covering the TTPs of your adversaries that map back to the MITRE ATT&CK framework. In this talk, you'll learn how to use the data you have to make an Adversary Detection Pipeline, how to develop a resource for HUNT/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. ***Xena Olsen**, @ch33r10, Cyber Threat Analyst, Financial Services Industry* ***Ben Goerz**, @bengoerz, Cybersecurity Engineer, Kimberly-Clark Corporation*
4:45-5:00 pm	***Day 1 Wrap-Up***
5:00-7:00 pm	**Networking with a View** (LOCATION: TREVI'S RESTAURANT) Meet us on the patio overlooking the lake at Trevi's Restaurant (in the hotel) for drinks, food, and networking.

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, October 22

7:00-9:00 am	**Registration & Coffee** (LOCATION: MANDALAY FOYER)
9:00-9:45 am	***Keynote: Enter Mordor: Pre-recorded Security Events from Simulated Adversarial Techniques*** 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. ***Roberto Rodriguez**, @Cyb3rWard0g, Security Researcher*
9:50-10:25 am	***Optimizing Caldera for Automated Adversary Emulation*** 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. ***Erik Van Buggenhout**, @ErikVaBu, Consultant, NVISO; Certified Instructor, SANS Institute*
10:25-10:45 am	**Networking Break** (LOCATION: MANDALAY FOYER)
10:50-11:25 am	***One Hundred Red Team Operations a Year*** 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. ***Ryan O'Horo**, @redteamwrangler, Lead Engineer, Red Team, Target*

Tuesday, October 22

11:30 am – 12:05 pm	***The Role of Threat Intelligence in Purple Team Tactics*** All disciplines of the SOC can assist the Purple Team; where the red mimics the tactics, techniques, and procedures of the adversary and the blue uses all it's available resources to defend and maintain the environment's security posture. So how can Cyber Threat Intelligence (CTI) strengthen the work of the purple team? Looking at the strategic, operational, and tactical aspects within CTI, we will explore how each can provide the necessary information and reinforce the mission of Purple Teaming. The audience will leave with new insight, approaches, and strategies for building the purple teams relationship with CTI. ***V. Susan Peediyakkal**, @v33na, Cyber Threat Intelligence Program Lead Consultant, Booz Allen Hamilton*
12:10-1:15 pm	**Lunch** (LOCATION: MANDALAY FOYER)
1:20-1:55 pm	***Detecting and Mitigating FLAM1 Banking APT*** 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. ***Huáscar Tejeda**, @htejeda, Co-Founder and CEO, F2TC Cyber Security* ***Rilke Petrosky Ulloa**, @xenomuta, Red Team Leader and Security Researcher, F2TC Cyber Security*
2:00-2:35 pm	***Air Force's Purple Teams: Lessons Learned from a Red Team Inside of a Blue Team*** 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. ***Lillian Warner**, @blackburn_lilly, Cyber Vulnerability Assessment/Hunter (CVAH) Liaison Officer and Planner for 624 Operations Center, U.S. Air Force*
2:35-3:00 pm	**Networking Break** (LOCATION: MANDALAY FOYER)

Tuesday, October 22

3:05-3:40 pm	***Lessons in Purple Team Testing with MITRE ATT&CKs from Priceline and Praetorian*** 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. ***Daniel Wyleczuk-Stern**, @Daniel_Infosec, Principal Security Engineer, Praetorian* ***Matt Southworth**, @bronx, Chief Information Security Officer, Priceline, Booking Holdings*
3:45-4:20 pm	***It's Hackers All the Way Down: Experiences in Improving Security by Transferring Adversarial Skills to Product Teams*** 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. ***Joe Gervais**, @TryCatchHCF, Technical Director, Red Team Ops, Fortune 500 Company*
4:20-4:30 pm	***Wrap-Up and Takeaways***

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.

@SANSPenTest #PurpleTeamSummit