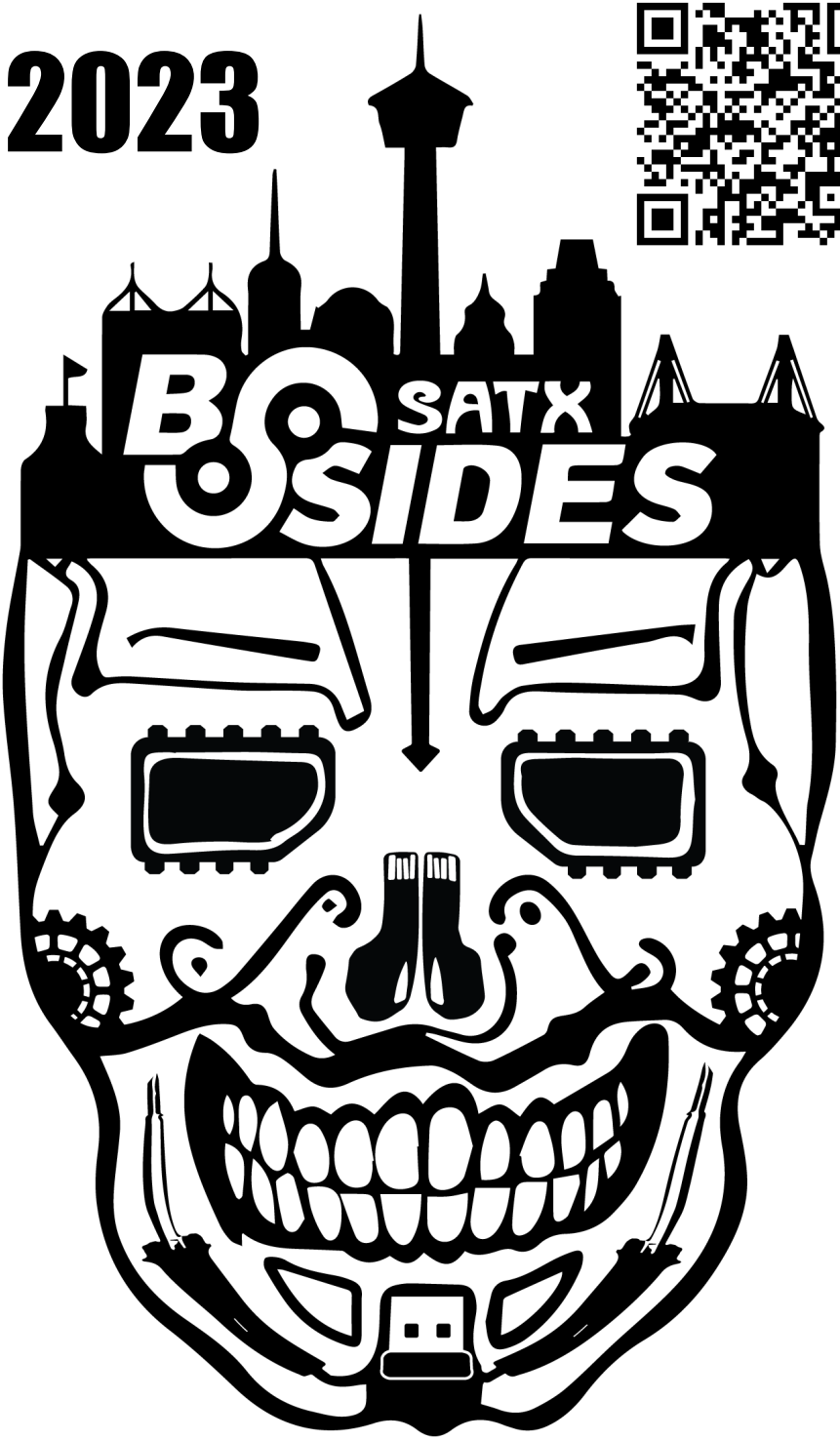
Online schedule

2023



Track 1 (UC Conference Rm A)

10:00	I Came in Like a Wrecking Ball -iamv1nc3nt
11:00	Malware and Malicious Code in the Open Source Software Supply Chain -Ross Bryant, Ph.D.
11:30	The Darkside of GraphQL -Parth Shukla
13:00	SciFi to Reality: Use of AI in Cybersecurity -Sandip Dholakia
14:00	Driving Your Own Vulnerability: How to Navigate the Road of BYOD Attacks -Dana Behling
14:30	Homophonic Collisions: Hold Me Closer, Tony Danza -Reagan Short, Justin Ibarra
15:00	How LockBit Orchestrated the Destruction of a Domain and Network and How We Kicked Them Off Stage -Jacob Wellnitz
16:00	Kickstarting your in-house Red Team: Challenges and approaches -Daniel C. Marques, Victoria Dea

Track 2 (Moody Rm 101)

10:00	Two Sides of the Same Coin: Interview lessons, as learned by both interviewee and interviewer -Sara Friedfertig
11:00	CyberPatriot: Mentoring the Next Generation -Frank Hall
12:30	Cybersecurity Careers: How to Find Your Fit -Frank Buckholdt
13:00	Discovering the Dark Side: An Introduction to Malware Reverse Engineering -Andrew Neumann
14:00	SIEM Slam: Tricking Modern SIEMs with Fake Logs and Confusing Blue Teams (Pre-Recorded) -Ozgun Kultekin
15:00	DefectDojo, Taking your DevSecOps to 11 -Matt Tesauro
16:00	Accidentally Exposed - Classifying Publicly Exposed Cloud Files -Dan Eldad
16:30	Use DMARC, do not let others abuse your brand! -Paul Guido, CISSP, CCSP

Track 3 (Moody Rm 102)

10:00	Challenging the Standard -Dr. Melisa Joyner
11:00	Trending cloud security threats and defense -Gabe Schuyler
13:00	How I Learned to Stop Worrying and Build a Modern Detection & Response Program -Allyn Stott
14:00	Writing Effective Triage Notes in the SOC: The Importance of Clarity, Actionability, and Leadership Support -Abhishek Tripathi
14:30	Cover your SaaS: Cloud threat Detection beyond Endpoints -Jeremy Galloway
15:00	Infrastructure as Remote Code Execution: How to abuse Terraform to elevate access -Michael McCabe
16:00	Cybersecurity Metric, KPIs and KRIs -Gideon T. Rasmussen

Deloitte.

Cyber

https://www.deloitte.com/us/cyber

Careers

https://careers.deloitte.com

Thank you, Deloitte! Please go visit them in our sponsor area, upstairs in the UC!

Lunch available in the UC Cafeteria from 11:30-13:00

Track 1 (UC Conference Rm A)

10:00
I Came in Like a Wrecking Ball
by iamv1nc3nt

In this presentation, we will cover the methods an attacker can take to conceal their identity and disguise their digital footprints, as well as real-world examples from the previous year in which full compromise was achieved through human error, seemingly harmless configurations, and insecure products. Then, we'll examine opportunities for engaging employees and management through gamification and highlight cost-effective strategies for creating a more secure environment.

11:00
Malware and Malicious Code in the Open Source Software Supply Chain
by Ross Bryant

Bad actors are targeting your developers through open source software. In this talk you will find a variety of specific examples of recent supply chain attacks in software ecosystems such as npm and PyPI. You will also learn about recent trends and techniques in these attacks, and ideally you will learn about how to lower the risk of a compromise in your software development environment. This talk is intended for all audiences, and no prior knowledge of malicious code or malware is assumed.

Track 1 (UC Conference Rm A)

11:30
The Darkside of GraphQL
by Parth Shukla

GraphQL is a query language for APIs that provides a powerful and efficient way to query and manipulate data. As powerful and versatile as GraphQL is, its downside is that it can be vulnerable to certain security threats. In this presentation, we will discuss the security vulnerabilities associated with GraphQL, from the basics to more advanced threats, and how to best protect against them. After this presentation, attendees will have a better understanding of security vulnerabilities in GraphQL

13:00
SciFi to Reality: Use of AI in Cybersecurity
by Sandip Dholakia

Global spending on AI is expected to reach $500 billion by end of 2023, how will hackers use this technology?

Join SAP Cybersecurity Expert Sandip Dholakia and find out more about how AI will be used by cybercriminals to infiltrate systems and how the cybersecurity industry is fighting back.

Sandip will enlighten the audience with facts about how hackers can compromise your privacy and security using AI and how cybersecurity professionals can use AI to protect your data and information.

Track 1 (UC Conference Rm A)

14:00
Driving Your Own Vulnerability: How to Navigate the Road of BYOD Attacks
by Dana Behling

Detecting and preventing attacks that use Bring Your Own Vulnerable Drivers (BYOVD) pose a unique threat to Windows security, but what makes a driver vulnerable, and how prevalent are vulnerable device drivers? In addition to answering these questions, this talk provides categories of vulnerabilities that are unique to windows drivers and provides real world vulnerable driver case studies to illustrate the theoretical concepts.

14:30
Homophonic Collisions: Hold Me Closer, Tony Danza
by Reagan Short, Justin Ibarra

We'll demonstrate a few practical approaches to exploiting human misunderstanding as a result of homophones to passively collect sensitive information, along with some redacted real-world examples. Domains registered for soundsquatting purposes are likely to be missed by typosquatting detection tools like DNSTwist. We will release defensive and detection mechanisms to help find vulnerable use cases within registered domains, language packaging pipelines, and social media handles.

Track 1 (UC Conference Rm A)

15:00
How LockBit Orchestrated the Destruction of a Domain and Network and How We Kicked Them Off Stage
by Jacob Wellnitz

In this talk we take the audience through a LockBit 3.0 and LockBit ESXi investigation, containment, and recovery case. We cover how we identified infected systems, attacks that don't match TTPs from the FBI and CISA, and how we helped our client get back up and running again.

16:00
Kickstarting your in-house Red Team: Challenges and approaches
by Daniel C. Marques, Victoria Dea

This talk aims to help attendees address these challenges and kickstart their internal red team programs, proposing approaches to improving communication, integrating enterprise functions, and measuring program effectiveness. It covers our experiences managing a team of red team operators, helping organizations build a red team program, and what was observed in many companies trying to develop similar initiatives.

Track 2 (Moody Rm 101)

10:00

Two Sides of the Same Coin: Interview lessons, as learned by both interviewee and interviewer

by Sara Friedfertig

When people think of interviews – especially in cybersecurity – they focus on the opposition of interviewer vs. interviewee, of hiring company vs. potential candidate. However, successful interviews result when the perspectives of both interviewer and interviewee are kept in mind, regardless of what side of the proverbial table you're sitting on. In this talk, hiring managers and potential new hires alike will learn how to approach all stages of "The Interview" from both perspectives.

11:00

CyberPatriot: Mentoring the Next Generation

by Frank Hall

For everyone that is currently working in the cyber/ I.T. industry, have you thought to yourself "I wish they had CyberPatriot when I was in school?" In CyberPatriot XV San Antonio there were nearly 400 teams registered under the San Antonio City of Excellence. The one thing all of these teams' need are technical mentors to guide the next generation of cyber professionals. Come to my session to learn about CyberPatriot and how to be a technical mentor.

Track 2 (Moody Rm 101)

12:30
Cybersecurity Careers: How to Find Your Fit
by Frank Buckholdt

Join for an informative and entertaining presentation on some of the many jobs and career paths available in cybersecurity. I will provide an rundown of some of the more common roles and responsibilities within cybersecurity and highlight the "entry-level" jobs that are available in this exciting and ever-changing field.

13:00
Discovering the Dark Side: An Introduction to Malware Reverse Engineering
by Andrew Neumann

This course would provide an overview of most common RE tools and how to use them for beginners wanting to look into malware reverse engineering. This course will specifically avoid assembly based tools as they are more advanced and time consuming to cover fully in the timeslot.

Track 2 (Moody Rm 101)

14:00
SIEM Slam: Tricking Modern SIEMs with Fake Logs and Confusing Blue Teams (Pre-Recorded)
by Ozgun Kultekin

Our research has uncovered a sneaky tactic that attackers use to outsmart modern Security Information and Event Management (SIEM) tools, such as Splunk. By creating and injecting fake logs, attackers can divert the attention of blue teams and conceal their real attacks. In this study, we explore this devious approach and provide an in-depth analysis of how it can be used to deceive security operations. Specifically, we examine the vulnerabilities of SIEM tools, with Splunk as a prime example.

15:00
DefectDojo, Taking your DevSecOps to 11
by Matt Tesauro

DefectDojo was created by DevSecOps people for DevSecOps people. In this talk, you'll learn about DefectDojo and how to make the most of it. DefectDojo can be your single pane of glass for discovered security vulnerabilities, report generation, aggregation of over 150+ different security tools, and so much more. DefectDojo was the heart of an AppSec automation effort that saw an increase in assessments from 44 to 414 in two years. Don't you want 9.4 times more output from your AppSec program?

Track 2 (Moody Rm 101)

16:00
Accidentally Exposed - Classifying Publicly Exposed Cloud Files
by Dan Eldad

Join this talk, for a technical deep dive into the analysis and classification of publicly exposed files in cloud buckets and how those buckets get exposed in the first place.

16:30
Use DMARC, do not let others abuse your brand!
by Paul Guido, CISSP, CCSP

DMARC is the best way to make sure bad actors cannot use your good brand against you. Hint, the hardest part is working with your vendors.

Thank you so much to Fortra for their sponsorship! You can find them at **fortra.com** and also in our sponsor area, upstairs in the UC

FORTRA™

Track 3 (Moody Rm 102)

10:00
Challenging the Standard
by Melisa Joyner

With the ever-evolving threat landscape, the cyber community faces new challenges daily. From advanced persistent threats (APTs) to targeted attacks, the need for comprehensive threat intelligence has never been greater. This presentation will delve into the threat intelligence strategies used by threat hunters to detect and thwart APTs, as well as highlight the actions that the industry must take to stay ahead of the game.

11:00
Trending cloud security threats and defense
by Gabe Schuyler

If you're responsible for defending a cloud estate -- of any size -- you know that there are myriad threats, but which do you focus on first? This talk begins with a survey of the current top threats to cloud infrastructures, such as stolen credentials, misconfiguration, multi-cloud complexity, and even attackers' use of AI and automation. As we go, we'll discuss effective defenses against these threats, as well. We'll wrap up with general tips and best practices for protecting the cloud.

Track 3 (Moody Rm 102)

13:00
How I Learned to Stop Worrying and Build a Modern Detection & Response Program
by Allyn Stott

You haven't slept in days. Pager alerts at all hours. Constant firefights. How do you get out of this mess? How do you successfully build a modern detection and response program, all while riding the rocket of never ending incidents and unforgiving on-call schedules? This talk gives away all the secrets you'll need to go from reactive chaos to building and running a finely tuned detection & response program (and finally get some sleep).

14:00
Writing Effective Triage Notes in the SOC: The Importance of Clarity, Actionability, and Leadership Support
by Abhishek Tripathi

With remote work and ever-evolving threat scenarios, Security Operations Center(SOC) has a significant role. The SOC lays its foundation on people, processes, and technology. The confluence of process and technology plays a vital role in the analyst triaging/reviewing the alerts. In this presentation, I would go over a few tips for writing good triage notes, a topic that is not very well discussed, and the role of leadership.

Track 3 (Moody Rm 102)

14:30
Cover your SaaS: Cloud threat Detection beyond Endpoints
by Jeremy Galloway

As businesses around the world continue to rapidly adopt SaaS solutions and products, defenders need to evolve their threat detection and response capabilities to this new landscape, which means thinking beyond the standard endpoint and into the SaaS applications themselves. Defense-in-depth means not just monitoring activity on your own systems and infrastructure but actively looking for threats and suspicious activities within the myriad SaaS applications in use at your organization.

15:00
Infrastructure as Remote Code Execution: How to abuse Terraform to elevate access
by Michael McCabe

This talk will focus on ways to abuse the use of Terraform to elevate privileges, expose data, and gain further footholds in environments from a developer's perspective. We'll cover the common uses of Terraform and how a malicious actor could abuse Terraform and even bypass security controls to execute unapproved code. This talk will include multiple demos of ways to exploit Terraform cloud.

Track 3 (Moody Rm 102)

16:00
Cybersecurity Metrics, KPIs and KRIs
by Gideon T. Rasmussen

This session provides practical advice to establish cybersecurity metrics, KPIs and KRIs. Provides tips to design metrics based on a new process or function. Includes examples attendees can leverage upon returning to work. The session includes 22 metrics and seven resources for many more.

All Day Events

Thank you so much to Polarity for their sponsorship! You can find them at **polarity.io** and also in our sponsor area, upstairs in the UC

POLARITY

Malware Traffic Analysis Workshop

Presenter: Brad Duncan

This training provides a foundation for investigating packet captures (pcaps) of malicious network activity. It begins with basic investigation concepts, setting up Wireshark, and identifying victims in network traffic. Participants learn characteristics of various windows-based malware infections. The training concludes with exercises designed to give participants experience in writing incident reports.

Max Participants: 20

All Day Events

Pen-Testing Cloud Rest APIs

Presenter: Rodney Beede

Participants will learn how to perform OWASP Top 10 authorization and fuzzing testing against real cloud REST APIs. This will be a guided lab with hands-on participation.

Note: this event is offered in the morning and afternoon as two separate sessions, please only attend one or the other.

Crypto Challenge

Presenter: Carl Mehner

Try your hand at deciphering this year's challenge! There are ten puzzles in all, how many can you complete during the day?

Prerequisites: The registration link will be provided the day of here and in Discord.

Lock Picking Village

Presenter: Douglas Copeland

Whether you're a novice or an experienced lock picker, this challenge offers an opportunity to hone your abilities and have fun in the process. The event is set up in a casual drop-in/drop-out format, allowing participants to come and go as they please throughout the duration of the conference.

Secure Coding Tournament

All Day Events

Presenter: Alicia Gordon

Secure Code Warrior brings you a defensive security-based tournament from a developer's perspective. The tournament allows you to test your skill against the other participants in a series of vulnerable code challenges that ask you to identify a problem, locate insecure code, and fix a vulnerability. You don’t need extensive programming knowledge as this will be a great way to learn the foundations and intermediates of leveraging code that is not only functional but is also secure.

More details on the BSides SATX website at https://www.bsidessatx.com/events-2023.html

SnekWars Python Challenge

Presenter: David Waters

SnekWars is a series of increasingly difficult Python challenges meant to test your Python programming skills.

SnekWars will take place throughout the day of BSides SATX - it will consist of a couple dozen challenges that will test your Python skills.

Prerequisites: A laptop with internet access and Python.

Hardware Hacking Village

Presenter: Andrew Neumann

Morning Events

Pwning Web Apps

Presenter: Phillip Wylie

In this intro to web application penetration testing workshop, participants will learn the basics of web application penetration testing including; methodology, tools, techniques, and resources. The skills taught in this workshop are valuable to aspiring bug hunters for use in bug bounties.

Prerequisites: Virtualization software (VMware, VirtualBox, etc.) and Kali Linux VM (downloadable here; https://www.kali.org/get-kali/#kali-virtual-machines)

More details on the BSides SATX website at https://www.bsidessatx.com/events-2023.html

Max Participants: 20

Value of Table Top Exercises

Presenter: Rob Dodson

Incident Response Tabletop exercise designed to identify the value of exercising tabletops to improve responses.

Follow up conversation about what to do about the Security Personnel Shortage.

Max Participants: 5 participating (up to 15 may spectate)

More details on the BSides SATX website at https://www.bsidessatx.com/events-2023.html

Afternoon Events

Intro to Hacking Workshop

Presenter: Vincent

This session provides an introduction to hacking in a welcoming and encouraging environment. Ideal for those with little to no hacking experience, it offers the chance to learn hacking techniques in an enjoyable, accessible, and practical manner.

Prerequisites: Participants need a laptop equipped with WiFi, VirtualBox, Kali Linux, and enough system resources to run an additional virtual machine with 2GB of memory. Basic Linux / Kali experience is preferred. *NOTE: Mac Silicon (Apple M1/M2) has issues with hypervisors.

Max Participants: 20

More details on the BSides SATX website at https://www.bsidessatx.com/events-2023.html

This space intentionally left blank

ST. MARY'S UNIVERSITY

Deloitte.

FORTRA™

POLARITY

corelight

ARCTIC WOLF

OFFICIAL (ISC)² CHAPTER ALAMO

Secure Apps

no starch press