SECURITY BSIDES LAS VEGAS, INC. PRESENTS

BSidesLV: 194 countries, 1 community...

AUGUST 6–7, 2019

TUSCANY SUITES & CASINO
LAS VEGAS, USA

What is BSides Las Vegas?

BSides Las Vegas is a nonprofit organization formed to stimulate the Information Security industry and community by providing an annual, two-day conference for security practitioners and those interested in (or looking to) enter the field.

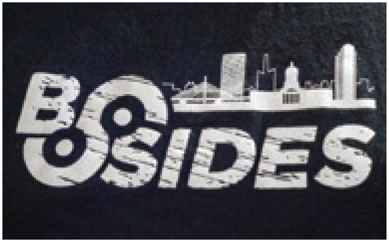
Our event is a source of education, communication, and collaboration. The technical and academic presentations at BSidesLV are given in the spirit of peer review and for the dissemination of knowledge among all specialties. This allows the field of Information Security to grow and continue its pursuit of a world where privacy and security are attainable.

LAS VEGAS BSIDES

Table of Contents

Security BSides Las Vegas, Inc. is a federally recognized 501(c)(3) since 2012.

Printed in the USA



From the COO and the President of the Board

We're writing to you a joint letter this year. It is a change from past years, which is apt as this is a year of changes for us.

We (the staff and the board of directors) have realized that we need to keep up with the times, and accept our organic growth as the BSides event that's looked at as the first of its kind and the pace-setter for hacker conferences. Hopefully with these changes you won't notice any difference as a participant, other than us being able to offer more (maybe while being slightly less stressed?).

It's been a year of reflection for us. Are we still doing the right things? We asked ourselves hard questions, and took action based on what we found. At the end of the day, we feel a responsibility to keep watching the community, so we can cater to what it wants and needs with regard to education and enablement. One of the biggest changes is that we got rid of walk-in badges (no more early morning lines), while trying to maintain community access for students, locals, and veterans. We added some fun things and some spaces for calm too, alongside a brand-new full-day track. We're going to keep making changes, and sooner or later this may mean a venue change…but that's a conversation for another channel (:tacfac:).

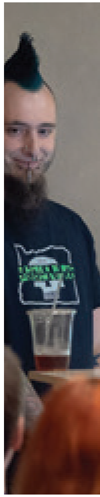
Today, we're grateful for the ability to put in countless hours to make your 48 hours in Las Vegas the pinnacle of your "hacker summer camp" experience. We are humbled and honored to be here. It's a privilege to help you all learn, engage, network, train, teach, mentor, and develop your career. We can't thank our staff and volunteers enough (feel free to thank them as well), as they help BSides Las Vegas, and BSides as whole, keep doing the right thing for the community.

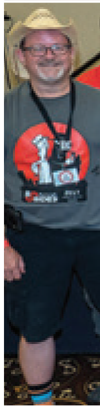
But know this; no matter how much changes, the core of our intention and our love for this community and this event will always remain. Thank you so much for being part of the Security BSides community as we celebrate the 10th anniversary of this tremendous movement!

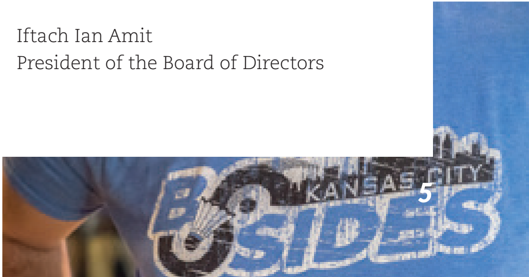
—nous

nous, aka Kelly Gardner
Chief Operations Office
and Executive Producer

Iftach Ian Amit
President of the Board of Directors







BSides Las Vegas 2019

Celebrating 10 Years of the Global BSides Movement

Thank you for joining us! We are super excited to welcome everyone back to where it all started, Las Vegas, to celebrate a decade of BSides events and BSides community around the world!

One bit of important information for you before you dig in: We have renamed The *Chillout* Room. It's now known as **MIDDLE GROUND**. It's the center of action; where we hold the contests and the keynote; where you can meet our sponsors, buy a t-shirt, or get a drink; and where you have to walk to access most of our tracks. If you're looking for a place to chill, a place that just brings to mind a little ease from the chaos, we have **The Quiet Room** downstairs off the casino. Tuscany calls it the Copa Lounge.

We have TWELVE amazing tracks of content for you to choose from:

- **Ground Floor** features foundational talks on topics relevant to security practitioners today.
- **I Am The Cavalry,** where the community is working together to make The Internet of Things a safer place for our neighbors, our children, our parents, and our friends.
- **Ground1234!** is all about passwords and other aspects of authentication with sessions ranging from why we need to rethink using passwords entirely, to how we can make them easier for the end-user without compromising security.
- **Underground** is where we hold off-the-record talks on subjects best discussed AFK. No press, no recording, no streaming, no names. Just you and your peers, talking about what matters, behind closed doors.
- **Breaking Ground** covers new and ongoing research, presented by speakers who want your feedback, insight, and opinion.
- **Common Ground** covers an assortment of other topics that are near and dear to the heart of InfoSec.
- **Proving Ground** gives people speaking for the first time at a national or international level a platform to have their voice heard in a welcoming environment—with the support of a mentor.
- **Ground Truth** is focused on innovative computer science and mathematics as applied to information security; natural language processing, machine learning, statistics, and all manner of big data manipulation and analysis.
- **Training Ground** features workshops and classes to give students hands-on experience learning valuable information security skills. **NOTE:** Training Ground sessions are held at the Platinum Hotel, just Northwest of the Tuscany.
- **Hire Ground** is a career-focused track with sessions to provide the tools and knowledge needed for job search and career development. Resume reviews by industry recruiters and career coaching sessions by industry veterans are available all afternoon on a first come, first served basis. Hire Ground sponsors are available all day to chat about current and future job opportunities.
- **Public Ground**, a collaboration between I Am The Cavalry and the Hewlett Foundation, gives the BSidesLV participants a forum to engage in public policy conversations with policymakers and others who are reaching out to our community.
- **CISO Track** is a brand new initiative! We're hosting 50 active CISOs (no vendors or consultants) for a full day of sessions around topics that have been picked by our track participants. The track takes place behind closed doors, under Chatham House Rule, and all participants are vetted beforehand. These are discussion sessions, rather than presentations, and the proceedings of the track will be published for the benefit of everyone who wants to learn how organizations deal with the challenges discussed.

Video recordings will also be posted to our **YouTube** channel (and to **archive.org**) a month or so after the event, so check back to catch video of the sessions you missed. Special thanks to **Source of Knowledge**, our streaming and recording provider, for enabling us to get our content out to the world.

Don't miss our contests and events! We have a **Lockpick Village**, where you can practice your picking or show off your skills by teaching someone new, as well as the **Pros vs. Joes CTF**, pitting Red Team against Blue to teach the Joes new defense and offense skills in a fun, controlled environment. We're also pleased to welcome the **OSINT CTF**, a fun challenge with an important mission, to BSidesLV this year!

Just for laughs, we've invited the folks from **Hacker Summer Camp Hacker Standup Comedy** to bring comedians to our stage during happy hour on Tuesday and Wednesday.

Our **Silent Auction and Raffle** this year will benefit our Supported Charities: **The EFF**, **No Starch Foundation**, **The Diana Initiative**, and **The United Way of Southern Nevada**. Raffle prizes will be awarded during happy hour on Tuesday and Wednesday as well as during closing ceremonies. Silent auction bidding closes just before the ceremony begins.

Of course, no InfoSec conference would be complete without after-hours activities!

On Tuesday, the **QueerCon Mixer** down at the pool starts at **20:30**, and the return of **The New Hacker Pyramid** starts at **21:30** in Middle Ground. Rounding out our triple threat of good times, we have **Karaoke** in the private room at PUB 365 between **22:00** and **02:00**!

Wednesday night at **22:00**, we have the **BSidesLV Pool Party**, with musical guests **An Hobbes**, **DJ Jackalope**, **Circuit Static** and **djdead**!!!!

We hope we've created an event that you find as fulfilling to participate in as we do making it happen! If you've got something you want to tell us about BSidesLV, especially if you wanna let us know what really worked for you, please email us at **feedback@bsideslv.org** or hit us up on Twitter **@bsideslv**.

From all of us at Team BSidesLV, participate, have fun, and help us spread the BSides ethos: Education! Communication! Collaboration!

BSides Las Vegas Code of Conduct

There have been calls for a more comprehensive and strictly defined code of conduct for BSides Las Vegas, and other events across the country. While we appreciate the sentiment behind such requests, we believe strict definitions of acceptable behavior only allow instigators and abusers to operate within the letter of the law while still causing a disruption to our participants and event.

We have ZERO TOLERANCE for harassment of any kind, be it physical, verbal, or sexual.

We strive to create an environment that encourages the free and open sharing of ideas. We've created a home at BSides Las Vegas and have invited you all inside to be inspired and educated. It is impossible to keep the free and open sharing of ideas without risking someone getting their feelings hurt. We don't expect adult and professional behavior at all times; a little mischief can be fun. We do however, expect you to be respectful of our space and our other invited guests.

In the end it is up to us, the organizers of BSides Las Vegas, to define bad behavior. If you are engaging in bad behavior (e.g. heckling or haranguing speakers, or violating the photo policy), you will be given a warning that your behavior is not acceptable. If you continue, you will be asked to leave.

Unless, of course, your bad behavior is so egregious that it warrants immediate ejection from the conference (e.g., initiating a physical altercation or attempting to defraud the conference or the venue).

If someone is engaging with you in a way that makes you afraid or uncomfortable, please inform a member of our Safety Operations team (in the blue BSides Las Vegas shirts) or a staff member (in the purple BSides Las Vegas shirts).

We have a special group in Safety Operations who are trained to handle such situations. They have an escalation path and will help you determine the next steps for you to feel safe and ensure your concerns are promptly addressed. This could include any or all of the following: contacting hotel security, local law enforcement, or other emergency services as needed.

TL;DR Do not be an ass or we will kick your ass out, and we're the final arbitrators of what being an ass means.

Photo, Video, & Recording Policy

Bsides Las Vegas is an open space, where everyone participating should feel free to share their ideas, stories, and any other passion they pursue. With that said, privacy is a big concern in the hacker community, as well as with the public at large, and we need to establish a clear set of boundaries when it comes to balancing privacy and capturing moments.

Using your best effort and judgement, please try to ensure you have permission from anyone you photograph or record. This includes, but is not limited to, anyone in the background of your shot. For the record, "crowd shots" from the front (facing the crowd) are strongly discouraged.

IN THE UNDERGROUND TRACK, THERE IS TO BE NO PHOTOGRAPHY OR VIDEO RECORDINGS UNLESS PERMISSION IS OBTAINED FROM THE SPEAKER THEMSELVES. THIS EXEMPTION EXCLUDES PHOTOGRAPHY OR VIDEO OF PARTICIPANTS IN THE UNDERGROUND TRACK.

If you've taken a picture without permission, delete it. If you're asked by a participant to delete or blur a picture they did not give you permission to take, and you are on BSides Las Vegas property, do so immediately.

We require press photographers to adhere to this policy as well. **A press badge is not a pass to break these rules and guidelines**.

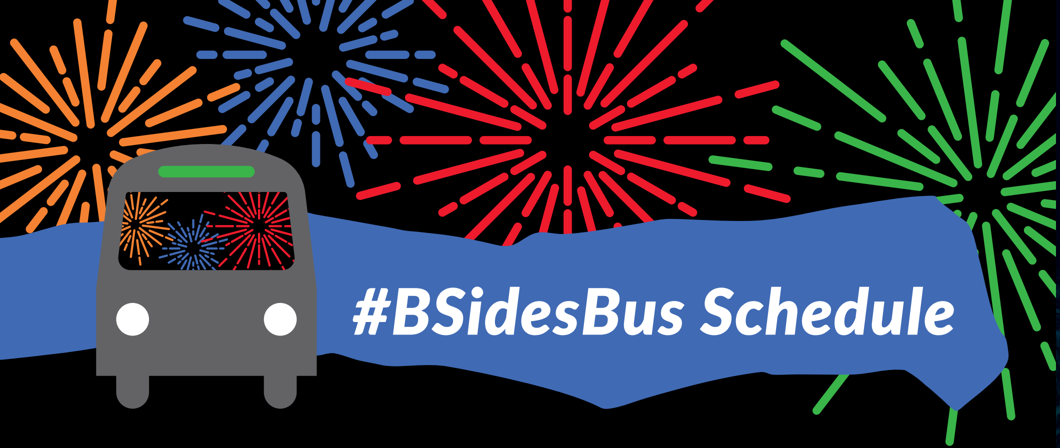
Upon a first infraction, you will receive one warning from BSides Las Vegas staff. Upon a second infraction you will be asked to give up your device to BSides Las Vegas Safety Operations for secure storage for the duration of your stay at the event; or you'll be asked to leave the event with your device—your choice. You may return to the event once you have deposited your device somewhere else.

There are official BSides Las Vegas Photographers. They will have professional cameras and staff badges. They are aware of this policy and are not exempt, except in cases where they have been requested to document activities, official parties, or presentations for BSides Las Vegas purposes.

If you believe that anyone is breaking these rules please bring it to the attention of BSides Las Vegas Safety Operations or any BSides Las Vegas staff member.

AS A REMINDER TO THE MEDIA: THERE IS ABSOLUTELY NO PRESS ALLOWED IN THE UNDERGROUND TRACK.

Thank you for your cooperation!



#BSidesBus Schedule

Monday, August 5

Starts at Las Vegas McCarran Airport at **06:00**, delivers riders to Tuscany Hotel, continues on to Mandalay Bay for pick-up, then circles back to LAS. Loop runs until **23:59**.

Tuesday, August 6

Starts at Las Vegas McCarran Airport at **06:00**, delivers riders to Tuscany Hotel, continues on to Mandalay Bay for pick-up, then circles back to LAS. Loop runs until **12:00**. From **12:00** on, the shuttle runs between Tuscany Hotel and Mandalay Bay until **03:00 Wednesday**.

Wednesday, August 7

Starting at **06:00**, the shuttle loops between Tuscany and Mandalay Bay until **06:00 Thursday**.

Thursday–Sunday

We're running the shuttle among Tuscany, Mandalay, Planet Hollywood, and Bally's Thursday **06:00** until Friday **06:00**.

Friday **06:00** until Monday **6:00**, the loop is Tuscany, Planet Hollywood, and Bally's.

Pick-up Locations

Tuscany

Hotel entrance (NOT the Casino). Wait on the far side of the bell stand, under the carport.

Mandalay Bay

Convention center entrance

Bally's

North door (Flamingo Rd. entrance)

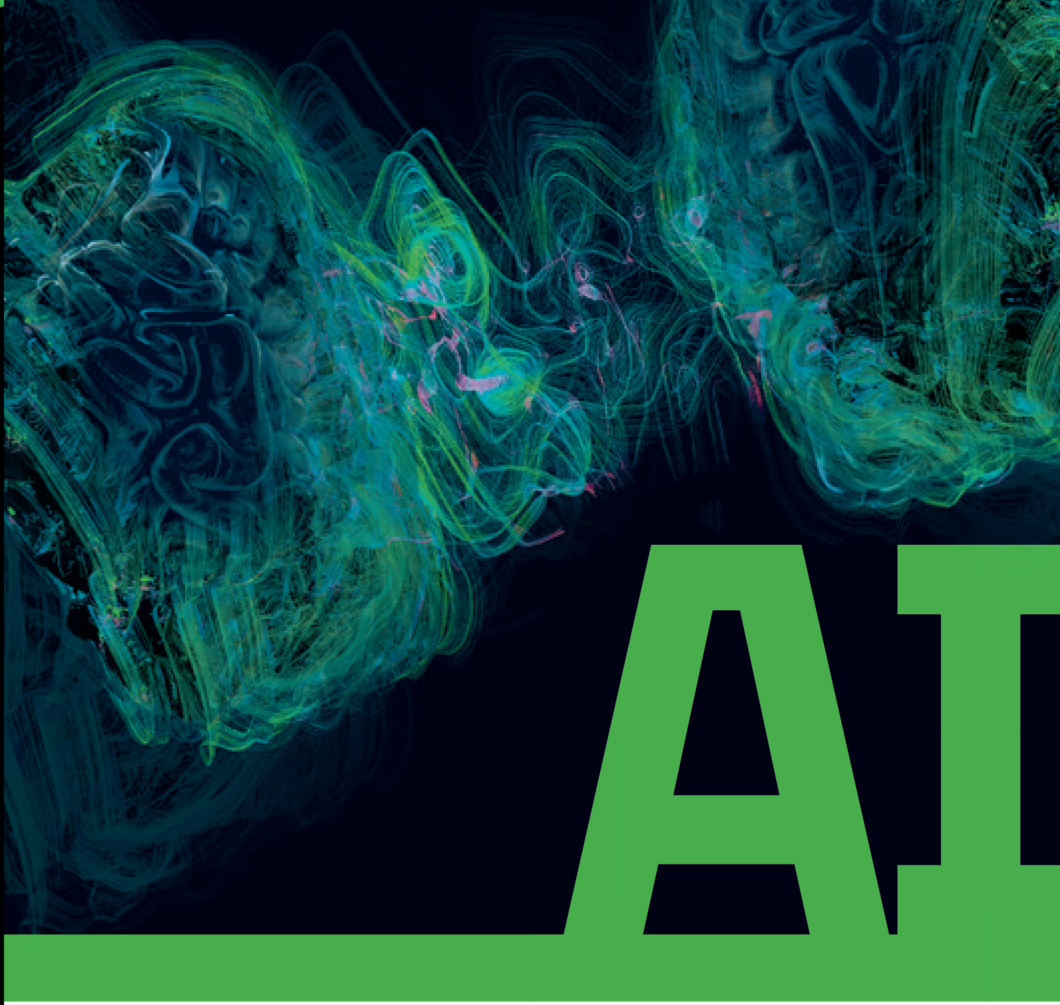
Planet Hollywood

Tour bus plaza (exit from the hotel lobby)

LAS Airport

Terminal 1: 0-level in bus slots 13–15.

Terminal 3: outside door #51 by the car rental shuttle buses



Bob Lord

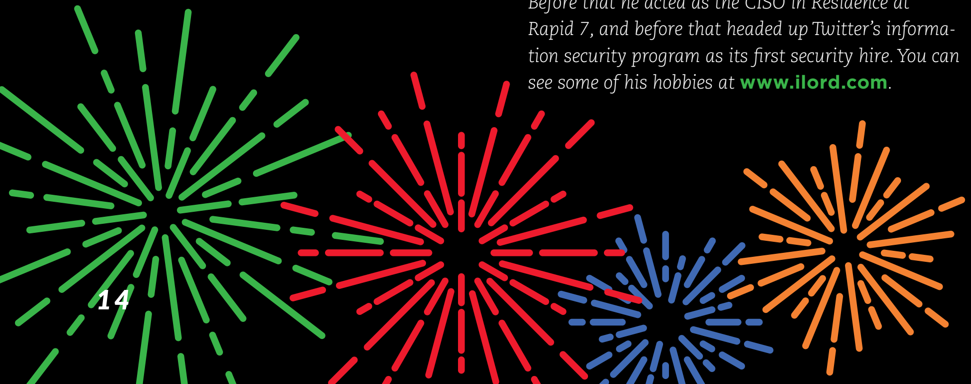
Opening Keynote

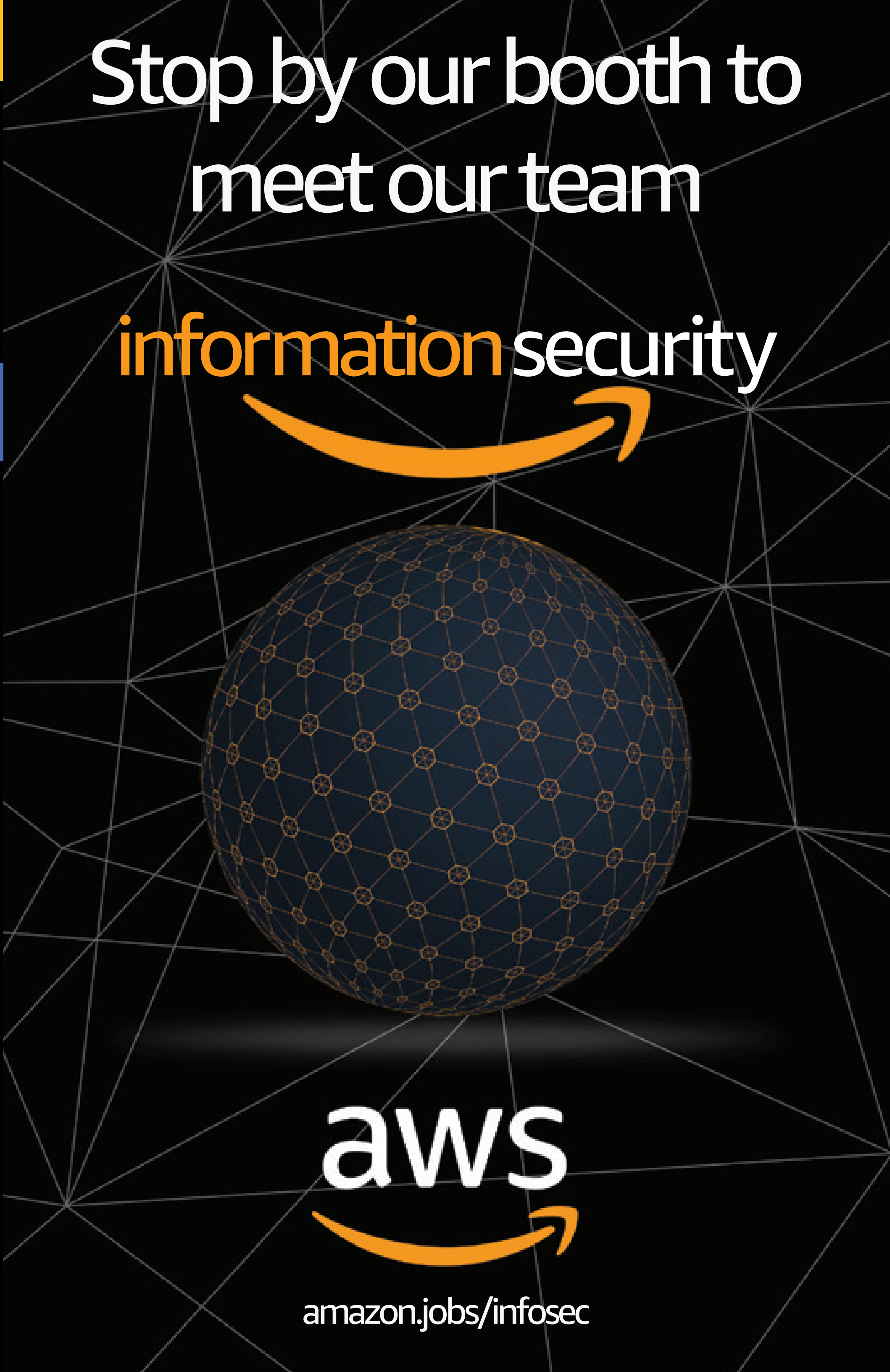
Tuesday, August 6th, 10:00–10:55

Middle Ground (Florentine C&D)

This is the 10th anniversary of BSides LV. A lot has changed and even improved over the past decade, but some persistent challenges remain. We've seen high-profile attacks, the rise of nation-state attacks, and many other changes in the threat landscape. More recently we've seen some attackers favoring disinformation and hybrid attacks. We've also seen some products inching towards a "secure by design" model. Bob has had a front row seat to some of these events and transformations. He'll share some of his observations and a few key reasons to be optimistic about the future, and ways you can help.

Bob Lord is the Chief Security Officer at the Democratic National Committee, bringing more than twenty years of experience in the information security space to the Committee, state parties, and campaigns. Previously he was Yahoo's CISO, covering areas such as risk management, product security, security software development, e-crimes, and APT programs. Before that he acted as the CISO in Residence at Rapid 7, and before that headed up Twitter's information security program as its first security hire. You can see some of his hobbies at **www.ilord.com**.





Breaking Ground

Groundbreaking Information Security research, and conversations on the "Next Big Thing."

Room: Florentine A

TUESDAY

BG **BEEMKA / Electron Post-Exploitation When The Land Is Dry**
11:30–12:25
Pavel Tsakalidis

BG **Unpacking pkgs: A look inside macOS Installer packages and common security flaws**
14:00–14:55
Andy Grant

BG **Using Machines to exploit Machines—harnessing AI to accelerate exploitation**
15:00–15:55
Guy Barnhart-Magen, Ezra Caltum

BG **Meltdown's Aftermath: Leveraging KVA Shadow To Bypass Security Protections**
17:00–17:55
Omri Misgav, Udi Yavo

BG **Neurosecurity: where Infosec meets Brain-machine Interface**
18:00–18:55
Ben D Sawyer, Matt Canham

WEDNESDAY

BG **Loki: Add a little chaos to your USB drive**
10:00–10:55
Michael Rich

BG **From EK to DEK: An Analysis of Modern Document Exploit Kits**
11:00–11:55
Joshua Reynolds

BG **From email address to phone number**
12:00–12:25
Martin Vigo

BG **Virtual Breakpoints for x86_64**
14:00–14:55
Gregory Price

BG **ROP with a 2nd Stack, or This Exploit is a Recursive Fibonacci Sequence Generator**
15:00–15:55
Nicholas Mosier

BG **At Your Service—Abusing the Service Workers Web API**
17:00–17:55
Daniel Abeles, Shay Shavit

BG **State of DNS Rebinding—Attack & Prevention Techniques and the Singularity of Origin**
18:00–18:55
Gerald Doussot, Roger Meyer

Common Ground

Topics of general interest to the security community, e.g., lock-picking, hardware hacking, mental health/burnout, law, privacy, regulations, risk, activism, technical tutorials, etc.

Room: Florentine F

TUESDAY

CG **DLP Sucks and Why You Should Use It**
11:30–12:25
John Orleans

CG **Where in the world are Carmen's $adjective cyber attacks: The game show that wonders why things aren't worse**
14:00–14:55
Allan Friedman, Chris Kubecka, Bryson Bort

CG **The Contemplator Approach: Data Enrichment Through Elastic Stack**
15:00–15:55
Rodrigo Brenes, Pedro Rodriguez

CG **Mind the Diversity Gap—A Panel Discussion**
17:00–17:55
Alyssa Miller, Chloé Messdaghi, Stephanie Ihezukwu

CG **Meet the CISO**
18:00–18:55

WEDNESDAY

CG **The Road to Hell is Paved with Bad Passwords**
10:00–10:55
Chris Kubecka

CG **Prisoner Number Six**
11:00–11:55
Nimrod Stoler, Lavi Lazarovitz

CG **Excuse Me, Your Sword Is In My Eye: Responding to Red Teams and 'IRL' Threats in 2019 and Beyond**
12:00–12:25
Jeremy Galloway

CG **Escape the Questionnaire Quagmire: A thoughtful approach to addressing security inquiries from customers and prospects**
14:00–14:25
Katie Ledoux

CG **Getting CVSS, NVD, and CVEs to Work for You: Standardizing and Scaling Your Vulnerability Risk Analysis**
14:30–14:55
Matthew Hahn, Luke Szczutowski

CG **Have You Distributed Randomness?**
15:00–15:55
Yolan Romailler

CG **CloudSec Rules Everything Around Me (C.R.E.A.M.)**
17:00–17:55
Kyle Dickinson

CG **Meet the Nation This Week on Sunday: A Special Vulnerability Edition**
18:00–18:55
Jen Ellis, Leonard Bailey, Tod Beardsley, Colin Morgan

Talks by Track

CISO Track

The BSidesLV CISO track aims to provide participants with a closed-door environment where sharing information and practices with peers is the name of the game. No vendor pitches. No “talks”. These are peer to peer discussions. Invite Only.

Room: Ballroom
4th Floor, Platinum Hotel

TUESDAY ONLY

CS **Board Communications**
09:30–10:25
NACD

CS **Zero Trust**
11:00–11:55
Duo Security

CS **Supply Chain Security**
13:00–13:55
Panorays

CS **AppSec/SDLC/DevSecOps**
14:30–15:25
WhiteHat

CS **Crisis Communication & Brand Monitoring**
15:30–16:25
ZeroFOX

CS **CISO Unconference**
16:30–17:25

Ground Floor

Foundational talks on topics relevant to security practitioners today.

Room: Florentine E

WEDNESDAY ONLY

GF **CTFs for Fun and Profit: Playing Games to Build your Skills**
10:00–10:55
David Tomaschik

GF **Hidden Networks Pivoting: Redefining DNS Rebinding Attack**
11:00–11:55
Tomer Zait, Nimrod Levy

GF **Low & Slow—Techniques for DNS Data Exfiltration**
12:00–12:25
Dimitri Fousekis

GF **Windows 10 DFIR Challenges**
14:00–14:55
Andrew Case

GF **ATT&CKing Your Adversaries—Operationalizing cyber intelligence in your own environment for better sleep and a safer tomorrow.**
15:00–15:55
Jamie Williams, Sarah Yoder

GF **Cyber Threat Intel & APTs 101**
17:00–17:55
John Stoner, Ronnie Obenhaus

GF **Musings of an Accidental CISO**
18:00–18:55
Brian Markham

Ground Truth

Focused on use of data science and statistics to solve problems in infosec.

Room: Firenze

TUESDAY

GT **Applying Information Security Paradigms to Misinformation Campaigns: A Multidisciplinary Approach**

11:30–12:25

Pablo Breuer, SJ Terp

GT **Building an enterprise security knowledge graph to fuel better decisions, faster**

14:00–14:55

Jon Hawes

GT **Grapl—A Graph Platform for Detection and Response**

15:00–15:55

Colin OBrien

GT **Profiling User Risk: Borrowing from Business Intelligence to Understand the Security of Your Userbase**

17:00–17:55

Emily Austin

GT **Reducing Inactionable Alerts via Policy Layer**

18:00–18:25

John Seymour

GT **Trying (Unsuccessfully) to Make Meterpreter into an Adversarial Example**

18:30–18:55

Andy Applebaum

GT **Evaluating Code Embeddings**

19:00–19:25

Rob Brandon

WEDNESDAY

GT **Security data science—Getting the fundamentals right**

10:00–10:55

Richard Harang

GT **Is This Magikarp a Gyarados?: Using Machine Learning for Phishing Detection**

11:00–11:55

Veronica Weiss

GT **Old things are new again: efficient automatic signature generation for malware classification**

12:00–12:25

Hyrum Anderson

GT **Reduce, Reuse and Recycle ML models—and the security powers is yours**

14:00–14:55

Ram Shankar Siva Kumar

GT **Scheming with Machines: Using ML to Support Offensive Teams**

15:00–15:55

Will Pearce, Nick Landers

GT **Birthday Hunting**

17:00–17:25

Jack Burgess

GT **All that glitters isn't Chrome: Hunting for suspicious browser extensions**

17:30–17:55

Mike Sconzo

GT **Scratching the Surface of Risk**

18:00–18:55

Benjamin Edwards, Wade Baker

Ground1234!

Focused on the (in)security of passwords and other authentication solutions. This track explores all facets of authentication security, from analysis and education to creating, securing, cracking, and exploiting authentication solutions.

Room: Tuscany

TUESDAY

G! **SSO Wars: The Token Menace**

11:30–12:25

Alvaro Munoz, Oleksandr Mirosh

G! **My quest for (privileged) identity to own your domain**

14:00–14:55

Nir Yosha

G! **Enterprise Overflow: How Breached Credentials Impact Us All**

15:00–15:55

Robert Paul

G! **Give the dog a bone—Exploring OSINT capabilities of pen-testing tools**

17:00–17:55

John Brunn

G! **Why FIDO Security Keys & WebAuthn are Awesome**

18:00–18:55

Jen Tong

WEDNESDAY

G! **Breaking Smart [Bank] Statement**

10:00–10:55

Manuel Nader

G! **An investigation of the security of passwords derived from African languages**

11:00–11:55

Sibusiso Sishi

G! **(Im)proper Database Authentication**

12:00–12:25

Mitch Wasson

G! **Who dis? The Right Way To Authenticate**

14:00–14:55

Lakshmi Sudheer,
Dhivya Chandramouleeswaran

G! **Exploiting Windows Group Policy for Reconnaissance and Attack**

15:00–15:55

Darren Mar-Elia

G! **Why can't we be friends? (Ask a Fed & the EFF.)**

17:00–17:55

Russell Handorf, Kurt Opsahl

G! **Ham Exams**

18:00–18:55

Falcon Darkstar

Hire Ground

A career focused track with sessions to provide the tools and knowledge needed for job search and career development. Resume reviews by industry recruiters and career coaching sessions by industry veterans are available all afternoon on a first come, first served basis. Hire Ground sponsors are available all day to chat about current and future job opportunities.

Room: Florentine B

TUESDAY

HG **Networking**
10:00–17:55

HG **Now that you hacked the plane, what are you going to do about your career?**
11:30–11:55
Chris Roberts

HG **Career Coaching & Résumé Reviewing**
12:00–17:55

HG **Addressing non-linear InfoSec career paths**
12:00–12:25
Sarah Young

HG **Discovering Your Passion in Cyber Security**
14:00–14:25
Cherie Burgett

HG **Hack (Apart) Your Career—How to Fund Doing What You Love**
14:30–14:55
John Grigg

HG **How to Fail Well (In Order to be Successful)—From IT to Infosec & More**
17:00–17:25
Roy Wattanasin

HG **Behind the Recruiting Curtain: What Do Recruiters Really Say and Do**
17:30–17:55
Matt Duren [SPONSORED PANEL]

WEDNESDAY

HG **Networking**
10:00–17:55

HG **The Importance of Culture in Security**
10:30–11:25
Mike Murray

HG **Hacking from Above: A Brief Guide for Transitioning to Leadership**
11:30–11:55
Joey Maresca

HG **Career Coaching & Résumé Reviewing**
12:00–17:25

HG **Noobs: Training the Next Generation of Security Engineers**
13:30–13:55
David Seidman

HG **Startup Security Leadership: Lessons to Level Up from Fortune 100 to Tech Startup**
14:00–14:25
Ty Sbano

I Am the Cavalry

The I Am The Cavalry track focuses on security issues that can affect public safety and human life, across our domains: Transportation, Healthcare, Infrastructure, and Home IoT.

Room: Siena

TUESDAY

IATC **I Am The Cavalry Track Welcome and Overview**

11:30–11:55

Joshua Corman, Beau Woods

IATC **Can the CAN bus fly—Risks of CAN bus networks within avionics systems**

12:00–12:25

Patrick Kiley

IATC **Coordinated Disclosure of ICS Products: Who's got time for that?**

14:00–14:25

Jay Angus

IATC **AIs Wide Open—Making Bots Safer Than Completely $#%cking Unsafe**

14:30–14:55

Davi Ottenheimer

IATC **The Case for Software Bill of Materials**

15:00–15:55

Allan Friedman

IATC **Automatic Security Analysis of IoT Firmware**

17:00–17:55

Matt Brown

IATC **I Just Want to Help Make Flying More Secure...not Work with the Government or How I Learned to Love a Govvie**

18:00–18:55

Steve Luczynski

WEDNESDAY

IATC **How to Treat Your Hacker (and Responsible Vulnerability Disclosure)**

10:00–10:55

Monta Elkins

IATC **Hacking the Pentagon: How a Rebel Alliance Shifts Culture to Protect National Security**

11:00–11:55

Brett Goldstein, Harlan Lieberman-Berg

IATC **Certification and Labeling in IoT**

12:00–12:25

Richard Manning

IATC **Real World Security in a Clinical Healthcare Environment: Hacking a Hospital**

14:00–14:55

Paul Dant

IATC **Why journalists and hackers need each other (a panel discussion with infosec reporters)**

15:00–15:55

Sean Lyngaas, Kim Zetter,
Joseph Cox, Lily Hay Newman

IATC **We the People: Providing for a 'common defence' with CVD**

17:00–17:55

Cameron Dixon, Matthew Cornelius

IATC **No IOUs with IOT**

18:00–18:25

Bryson Bort

IATC **"Hackers of the world—unite?"**

18:30–18:55

Keren Elazari

Proving Ground

Rookie speakers who were paired with veteran mentors present their original research, theory, or practical tutorials on a fascinating array of subjects.

Room: Florentine G

TUESDAY

PG **Bestsellers in the Underground Economy—Measuring Malware Popularity by Forum**

11:30–11:55

Winnona DeSombre

MENTOR: Russell Butturini

PG **Examining DES-based Cipher Suite Support within the TLS Ecosystem**

12:00–12:25

Vanessa Frost

MENTOR: Jeff Man

PG **Satellite Vulnerabilities 101**

14:00–14:25

Elizabeth Wilson

MENTOR: Philip Young

PG **Analyzing user decision making on phishing sites—using mouse data and keyboard dynamics**

14:30–14:55

Sanne Maasakkers

MENTOR: Chris Eng

PG **Broken Arrow: applying InfoSec and Forensic practices to escape domestic abuse**

15:00–15:25

Will Baggett

MENTOR: Brendan O'Connor

PG **The Human API: Evolving End Users From Authorized Adversaries Into Our Best Defense.**

15:30–15:55

Ty Atkin

MENTOR: Tom Kopchak

PG **Burpsuite Team Server—Collaborative Web Pwnage**

17:00–17:25

Tanner Barnes

MENTOR: Tom Eston

PG **The Resilient Hacker: Growth Mindset, Health Hacks & Powerful Help to Navigate Personal Challenges**

17:30–17:55

Serenity Smile

MENTOR: Nathaniel Davis

PG **So you think you can CHMOD**

18:00–18:25

Jared Chandler

MENTOR: Emily Gladstone Cole

PG **Building the badge—How you can make small, cheap and custom hardware for function or fashion**

18:30–18:55

James Dietle

MENTOR: Rachael Lininger

PG **Salesforce Data Governance What dark secrets lurk in your instance??**

19:00–19:25

Pete Thurston

MENTOR: Wendy Knox Everette

WEDNESDAY

PG **Making your website vulnerable for fun and security awareness**

10:00–10:25

Kenny Jansson

MENTOR: Bill Weiss

PG **Human honeypots, or: How I learned to stop worrying and love the NFC Implant**

10:30–10:55

Nick Koch

MENTOR: Patrick McNeil

PG **The struggles of teaching automation**

11:00–11:25

Joe O’Connell

MENTOR: Ming Chow

PG **The SOC Counter ATT&CK**

11:30–11:55

Mathieu Saulnier

MENTOR: Ethan Gregory Dodge

PG **The drunk colonel and the flipped stone: Game Theory for a Defensive Strategic Advantage**

12:00–12:25

Vanessa Redman

MENTOR: Allan Friedman

PG **I’m a hunter! But what does that mean?**

14:00–14:25

Yasmine Johnston-Ison

MENTOR: Cheryl Biswas

PG **Breaking the Bodyguards**

14:30–14:55

Chrissy Morgan

MENTOR: Nick Rosario

PG **Cover Your A****

15:00–15:25

Suchi Pahi

MENTOR: Clint Gibler

PG **Cyber Deception after Detection: Safe observation environment using Software Defined Networking**

15:30–15:55

Toru Shimanaka

MENTOR: Claus Houmann

PG **Deepfakes, Deep Trouble: Addressing Potential Market Manipulation Caused by Deepfakes**

17:00–17:25

Anna Skelton

MENTOR: John Seymour

PG **Baited Canaries—Monitoring attackers with active beacons**

17:30–17:55

Gregory Caswell

MENTOR: Michael Aguilar

PG Securing Fast (and Furious) DevOps pipelines

18:00–18:25

Abdessamad Temmar

MENTOR: Tyler Shields

PG Please inject me, a x64 code injection

18:30–18:55

Alon Weinberg

MENTOR: Maddie Stone

Public Ground

Public Ground, a collaboration between I Am the Cavalry and the Hewlett Foundation, gives BSidesLV participants a forum to engage in policy conversations with policymakers and stakeholders.

Room: Boardroom
4th Floor, Platinum Hotel

TUESDAY

PB Professionalization—Possibilities and Potholes

09:00–09:55

Andrea Matwyshyn

PB Reverse Engineering the Cyber Policy API

10:00–11:55

Maurice Turner, Katherine Pratt

PB What's Next in Coordinating Vulnerability Disclosures

14:00–15:55

Katie Trimble

PB AIs Wide Open—Making Bots Safer Than Completely #$%cking Unsafe

16:00–17:55

Davi Ottenheimer

WEDNESDAY

PB Free and Fair Elections in an Internet Era

09:00–09:55

Maurice Turner, Andre McGregor

PB Let's hear from the Hackers: What should DOJ do next?

10:00–11:55

Leonard Bailey

PB Certification and Labeling for IoT

14:00–15:55

Richard Manning

PB Why we need a Cyber Peace Institute

16:00–17:55

Eli Sugarman

Training Ground

Workshops and classes to give students hands-on experience learning valuable information security skills.

Rooms: 4th Floor, Platinum Hotel

TUESDAY

TG1 Malware Traffic Analysis Workshop

Diamond Room, Platinum Hotel

08:00–17:55

Bradley Duncan

TG2 Windows Breakout and Privilege Escalation

Emerald Room, Platinum Hotel

08:00–17:55

Rohan Durve

TG3 Hack Back! Malware Reverse Engineering and Command & Control Server Exploitation

Opal Room, Platinum Hotel

08:00–11:55

Barrett Darnell, Felix Guerrero

TG4 Knowing the Unknown: Using PCAP to Break Down Application-Layer Protocols

Pearl Room, Platinum Hotel

08:00–11:55

David Pearson

TG3 Hands-on: How to Use CALDERA's Chain Mode

Opal Room, Platinum Hotel

14:00–17:55

David Hunt, Alexander Manners

TG4 Active Directory security: 8 (very) low hanging fruits and how to smash those attack paths

Pearl Room, Platinum Hotel

14:00–17:55

Remi Escourrou, Nicolas Daubresse

WEDNESDAY

TG1 Using Wireshark for Incident Response and Threat Hunting

Diamond Room, Platinum Hotel

08:00–17:55

Michael Wylie

TG2 Hacking the STORM

Emerald Room, Platinum Hotel

08:00–17:55

Justin Whitehead, Kevin King

TG3 Introduction to Cryptographic Attacks

Opal Room, Platinum Hotel

08:00–11:55

Matt Cheung

TG4 Linux Hardening—The Easy Way

Pearl Room, Platinum Hotel

08:00–11:55

Guy Barnhart-Magen

TG5 Tournament: The Ultimate Secure Coding Throw Down

Ballroom, Platinum Hotel

08:00–11:55

Steve Allor, Jim Manico

TG3 Hands on Hacking The OWASP TOP 10 and beyond

Opal Room, Platinum Hotel

14:00–17:55

Chris Hanlon

TG4 Pentesting ICS 102

Pearl Room, Platinum Hotel

14:00–17:55

Alexandrine Torrents, Arnaud Soullie

TG5 Finding Evil with Mitre ATT&CK and the Elastic Stack

Ballroom, Platinum Hotel

14:00–17:55

Matteo Rebeschini, Kent Brake

Talks by Track

Underground

Off-the-record talks on subjects best discussed off-line. No press, no photos, no recording, no streaming, no attribution. Just you and your peers, discussing what matters, behind closed doors.

Room: Florentine E

TUESDAY ONLY

UG Duck and (Re)Cover—The missing link in the security evolution

11:30–12:25

Peter Lidell

UG Reverse Engineering Mobile Apps: Never Pay for Transit Again

14:00–14:55

Priyank Nigam

UG Giving Credit Where It's Not Due: Visualizing Joker's Stash

15:00–15:55

Ian Gray, Maxwell Aliapoulios

UG China as a New Russia? Analyzing Similarities and Differences of Chinese Threat Actors from their Russian Counterparts

17:00–17:55

Anne An

UG Ask the EFF

18:00–18:55

Kurt Opsahl, Eva Galperin,
Nathan Shepard, India McKinney

Keynotes

KN Opening Remarks

Tuesday, 09:30–09:55

Middle Ground (Florentine C&D)

KN Keynote with Bob Lord

Tuesday, 10:00–10:55

Bob Lord

Middle Ground (Florentine C&D)

This is the 10th anniversary of BSides LV. A lot has changed and even improved over the past decade, but some persistent challenges remain. We've seen high-profile attacks, the rise of nation-state attacks, and many other changes in the threat landscape. More recently we've seen some attackers favoring disinformation and hybrid attacks. We've also seen some products inching towards a "secure by design" model. Bob has had a front row seat to some of these events and transformations. He'll share some of his observations and a few key reasons to be optimistic about the future, and ways you can help.

KN Keynote Q&A

Tuesday, 11:00–11:25

Breaking Ground (Florentine A)

KN Closing Ceremonies

Wednesday, 19:00–19:55

Middle Ground (Florentine C&D)

Special Events

SE Middle Ground and Stage

Middle Ground (Florentine C&D)

The Main Stage in Florentine C&D is ground zero for all of our off-track activities. Ongoing announcements, music and other surprises will happen throughout the conference. Stop in, and relax, talk with your friends, visit our charities, sponsors, friendly staff, or just enjoy the music.

SE Hacker Summer Camp Hacker Standup Comedy

Middle Ground (Florentine C&D)

See your favorite hackers/code crackers/channel slackers in the inaugural 2-day event of Standup Comedy, featuring the comedic styles of Bryson Bort, Munin, 5urv1va7rix, JoshJay, MasterChen, SciaticNerd, Larci Robertson, JoJoBabie.

Happy Hour, Day 1: First time comedians bring the comedy. Crowd favorite earns a slot in Happy Hour, Day 2.

Happy Hour, Day 2: Tuesday's champ, plus a lineup of experienced hacks/comedians you know and love with a special guest!

SE Silent Auction & Raffle

Middle Ground (Florentine C&D)

After raising $7500 for our charity partners in 2018, we're looking to blow that number out of the water this time around.

This year the Electronic Frontier Foundation and The Diana Initiative will be joined by the No Starch Foundation, and the United Way of Southern Nevada. Our charity partners do so much good in the community, let's show them how grateful we are by winning slick prizes and sniping winning bids.

Raffles will have three draws during Happy Hour each day, and at the closing ceremonies. To enter the raffle, purchase tickets by making donations right at the table and enter them in the draw boxes for each drawing. You must be present during the drawing to win.

Silent Auction bidding officially closes at **19:00** on Wednesday, just before the closing ceremonies. To win, you must be present at the time of the auction and you must be able to make payment by cash or paypal. Any other questions? Want to donate something to the raffle or silent auction? Drop by our table in Middle Ground and let us know.

SE Lockpick Village

Middle Ground (Florentine C&D)

Want to try your hand at the art of lockpicking? Come visit the Lockpick Village! We bring the locks and picks. All you'll need is a sense of curiosity. We'll also have contests and beginner sessions on both days of the conference. All skill levels are welcome, as volunteers will be on hand to help you get started. Beginner sessions will be held at noon each day. If you're feeling competitive, drop by for one of the contests held at **16:00** daily!

SE Pros Vs Joes CTF

Middle Ground (Florentine C&D)

Pros vs Joes is a Capture the Flag event where inexperienced users learn from seasoned professionals in a fierce competition of attack and defend. Blue Teams of Joes work with Pro Captains to compete against other defending Teams, protecting horrifically vulnerable networks from assault by a dangerous and relentless Professional Red Team. For two days the battle will rage on a field rife with desktops and servers running Linux and Windows, on systems and software that are both old and new. Come witness the teams do battle after weeks of preparation. Only the strongest will survive, but all will learn and have fun!

SE OSINT CTF for Missing Persons

Trace Labs Missing CTF

Middle Ground (Florentine C&D)

Join us for the Trace Labs OSINT CTF for Missing Persons Challenge! Each day we will present eight (8) real missing persons for you to track and submit Open Source Intelligence (OSINT) into our CTF platform. Prizes awarded at the end of the day include licenses for Hunchly, the software every OSINT operator needs, and a variety of Trace Labs swag items! This is a fantastic opportunity to get into the OSINT community, learn intelligence gathering, and to become a hero. Get your team together or work individually and join us at the Trace Labs table in the contest area to get started.

SE The Quiet Room

Tuesday, 11:30–19:00

Wednesday, 10:00–16:00

Copa Room, Tuscany ground floor, near casino

Check in to the Quiet Room to relax and step away from the usual conference hustle. Open during the day, this space is reserved for people who need a quiet environment to recharge, think, or just rest their ears.

SE Queercon Mixer

Tuesday night, 20:30–23:30

Tuscany pool

Queercon is excited to be part of BSides Las Vegas again this year. Join us **Tuesday night** at the Tuscany pool from 8:30 PM until 11:30 for the Queercon BSides Mixer!

SE Hacker Pyramid

Tuesday night, 21:30–02:00

Middle Ground (Florentine C&D)

"We keep screwing up, and yet they keep asking us to return." The New Hacker Pyramid returns yet again at BSidesLV 2019. Join us for games, drinks, and retro-fun. There will be prizes, audience participation, a number of secret guest appearances, and an EXTRA SPECIAL EVENT that you will have to be there to see! Things are so secret WE don't even know what they are! *Pour un version français de cette message, appuyez sur '2'.*

SE Hacker Karaoke

Tuesday night, 22:00–02:00

Pub 365 back room, Tuscany ground floor

Sing, yell, rap or just mumble your favourite party songs all night long! Join us **Tuesday** night in Pub 365 for hours of singing with Tina and your favorite hackers.

SE BSides LV Pool Party

Wednesday night, 22:00–04:00

Tuscany pool

It's not BSides without the pool party! Drink, eat, and float around the Tuscany's fantastic pool while listening to djdead, Jackalope, An Hobbes, and Circuit Static playing all of the best music you've never heard before. Don't forget your swimsuit and conference badge!

Presenters

Daniel Abeles

At Your Service—Abusing the Service Workers Web API

Breaking Ground, Wednesday, 17:00–17:55

Michael Aguilar

MENTOR to Gregory Caswell

Baited Canaries—Monitoring attackers with active beacons

Proving Ground, Wednesday, 17:30–17:55

Experienced computer nerd with a high degree of slack. I guess it all started with an IBM terminal and went uphill from there. I compute to live. Not vice versa. Experiences include Red Teams, Blue Teams and project oriented teams. Areas of work include AV/Consulting/OTHER. I wreck terminals and patience.

Maxwell Aliapoulios

Giving Credit Where It's Not Due: Visualizing Joker's Stash

Underground, Tuesday, 15:00–15:55

co-presenting

Maxwell Aliapoulios is a PhD student at NYU Tandon. Max's published work includes tracking ransomware, IPTV piracy, and supply chains in underground cybercriminal marketplaces. He continues to apply academic research principles to understand cybercrime activity, including natural language processing, stylometry, and machine learning. Max also works as a Research Developer at Flashpoint.

Steve Allor

Tournament: The Ultimate Secure Coding Throw Down

Training Ground, Wednesday, 08:00–11:55

Steve Allor is Director of the Americas for Secure Code Warrior, a global security company that makes software development better and more secure. Since joining Secure Code Warrior soon after its inception, Steve has been passionate about helping large global enterprises in the finance, technology and telecommunications industries to scale an engaging, interactive learning approach, enabling these organizations to rally their developers as the first line of defense in their cybersecurity strategies. Over the past 20 years, Steve has held various executive leadership roles in sales, business development and marketing for technology companies, where his focus was on enabling customer success as he helped scale and grow the business. Steve has earned a Bachelor of Science degree in Marketing at Boston College Carroll School of Management, as well as a Master of Business Administration at Harvard.

Anne An

China as a New Russia? Analyzing Similarities and Differences of Chinese Threat Actors from their Russian Counterparts

Underground, Tuesday, 17:00–17:55

Anne An is a senior security researcher at McAfee's Advanced Programs Group (APG), where she leads threat analysis projects, performs qualitative research on advanced attacks and monitors cybercriminal threats in the Asia-Pacific region. Prior to joining McAfee, she held a variety of research positions at Intel Corporation, Dell SecureWorks, VeriSign iDefense (Accenture) and the Project 2049 Institute.

Hyrum Anderson

Old things are new again: efficient automatic signature generation for malware classification

Ground Truth, Wednesday, 12:00–12:25

Hyrum Anderson is the Chief Scientist at Endgame, where he leads research on detecting adversaries and their tools using machine learning. Prior to joining Endgame he conducted information security and situational awareness research as a researcher at FireEye, Mandiant, Sandia National Laboratories and MIT Lincoln Laboratory. He received his PhD in Electrical Engineering (signal and image processing + machine learning) from the University of Washington and BS/MS degrees from BYU. Research interests include adversarial machine learning, large-scale malware classification, and early time-series classification.

Jay Angus

Coordinated Disclosure of ICS Products: Who's got time for that?

I Am The Cavalry, Tuesday, 14:00–14:25

Jay Angus is a career civil servant and currently the federal lead for Industrial Control System vulnerability management and coordination. He has worked for the federal government for 15 years and spent the past ten years involved in cybersecurity. Specifically the past five years he has worked with the Department of Homeland Security supporting industrial control system operations and vulnerability management.

Andy Applebaum

Trying (Unsuccessfully) to Make Meterpreter into an Adversarial Example

Ground Truth, Tuesday, 18:30–18:55

Andy Applebaum is a security researcher at The MITRE Corporation, where he works on applied and theoretical security research problems, including as one of the leads on the CALDERA automated adversary emulation project and as a member of the ATT&CK team. His work tends to lie at the intersection of security, automation, and reasoning, with a growing personal interest in understanding how attackers can thwart machine learning algorithms in security settings. Andy received his PhD in computer science from the University of California Davis and he holds the OSCP certification. Outside of work, Andy is an avid chess player, having recently won the 2018 DEF CON chess championship.

Ty Atkin

The Human API: Evolving End Users From Authorized Adversaries Into Our Best Defense.

Proving Ground, Tuesday, 15:30–15:55

MENTOR: Tom Kopchak

Highly sought-after dinner guest Ty Atkin is a Security Operations Center Lead and Co-Founder of FullMetal CyberSecurity. Firm believer that anything worth doing is not only worth doing right but should be done with excellence. Ty strives to touch the "Corner Post" in all aspects of his life. Ty wants to live so that you wonder if he's working or playing. Hard work, self-reliance, respect, humor, determination and honor are not antiquated beliefs. "I want those values to be contagious and rub off on others when they interact with me." Ty's wife is the classiest and prettiest lady in the history of… well, everything. True story. Ty is a swashbuckling Patriot, debonair rogue, DeLorean time traveling consultant, and stately gentleman. Ty loves 80's movies and music, playing guitar, drag racing, heavy metal, Firefly, and Grandma Atkin's homemade Pumpkin Roll.

Emily Austin

Profiling User Risk: Borrowing from Business Intelligence to Understand the Security of Your Userbase

Ground Truth, Tuesday, 17:00–17:55

Emily is a Senior Engineer at Mailchimp, where she leads the Defensive Security team. With a background in data science, she takes an analytical approach to blue teaming and uses statistical methods to guide abuse prevention and security efforts. Under her guidance, the team has developed data-driven procedures for monitoring and detection and continues to explore other innovative ways to defend Mailchimp. An avid runner and triathlete, you can find her on the trails when she's not in front of a screen.

Will Baggett

Broken Arrow: applying InfoSec and Forensic practices to escape domestic abuse

Proving Ground, Tuesday, 15:00–15:25

MENTOR: Brendan O'Connor

Former Intelligence Community officer, current NATO SOF cyber trainer and volunteer of many BSides conferences. I was a SME for iOS and Mac forensics and now apply these skills to the private sector. I have teenage twins at New Mexico State University, I graduated from Georgia Tech, and I enjoy teaching others what I have learned.

Leonard Bailey

Let's hear from the Hackers: What should DOJ do next?

Public Ground, Wednesday, 10:00–11:55

Meet the Nation This Week on Sunday: A Special Vulnerability Edition

Common Ground, Wednesday, 18:00–18:55

co-presenting

Leonard is Special Counsel for National Security in the Department of Justice's (DOJ) Computer Crime and Intellectual Property Section (CCIPS) and Head of CCIPS' Cybersecurity Unit. He joined DOJ's Terrorism and Violent Crime Section in 1991. In the late 1990's, he served as Special Counsel and Special Investigative Counsel to DOJ's Inspector General and supervised sensitive investigations of Department officials and programs. In 2000, he joined CCIPS where he has prosecuted computer crime and intellectual property cases; advised on matters related to searching and seizing electronic evidence and conducting electronic surveillance; and chaired the Organization of American States' Group of Government Experts on Cybercrime. Leonard has taught courses on cybersecurity and cybercrime at Georgetown Law School and Columbus School of Law in Washington, D.C.

Wade Baker

Scratching the Surface of Risk

Ground Truth, Wednesday, 18:00–18:55

co-presenting

Wade Baker is co-founder of the Cyentia Institute. In addition to his role with the Cyentia Institute, Wade is a professor in Virginia Tech's College of Business, teaching in the MBA and Master of IT programs. He's also proud to serve on the Advisory Boards of the RSA Conference and FAIR Institute. Wade loves learning from cybersecurity data and sharing those lessons to help others learn as well—whether that's in the classroom, boardroom, or anywhere in between. Prior to founding Cyentia, Wade was the VP of Strategy and Analytics at ThreatConnect and before that had the great fortune of leading Verizon's Data Breach Investigations Report team for a number of years.

Tanner Barnes

Burpsuite Team Server—Collaborative Web Pwnage

Proving Ground, Tuesday, 17:00–17:25

MENTOR: Tom Eston

Tanner is a full scope penetration tester for Aon providing red team, social engineering, physical security, and source code review consulting for a myriad of clients in diverse industries. As a software engineer, he discovered the cyber security world through his first job and has been hooked ever since! Now he applies his knowledge of writing software towards breaking it along with developing tools to enhance his and other hackers abilities.

Guy Barnhart-Magen

Using Machines to exploit Machines—harnessing AI to accelerate exploitation

Breaking Ground, Tuesday, 15:00–15:55

Linux Hardening—The Easy Way

Training Ground, Wednesday, 08:00–11:55

BSidesTLV chairman and CTF lead, public speaker, and recipient of the Cisco "black belt" security ninja honor—Cisco's highest cyber security advocate rank. With nearly 20 years of experience in the cyber-security industry, Guy held various positions in both corporates and start-ups. He is currently a Cyber Security Consultant, focusing on OS and Services Hardening, Cryptography, AI Security, and Reverse Engineering. https://meliorsec.com

Tod Beardsley

Meet the Nation This Week on Sunday: A Special Vulnerability Edition

Common Ground, Wednesday, 18:00–18:55

co-presenting

Elizabeth Biddlecome

Reverse Engineering Android Apps

Training Ground, Tuesday, 08:00–11:55

co-presenting

Elizabeth Biddlecome is a senior researcher at Bowne Consulting, an independent consultant, and a part-time instructor at City College San Francisco, delivering technical training and mentorship to students and professionals. She leverages her enthusiasm for architecture, security, and code to design and implement comprehensive information security solutions for business needs. Elizabeth enjoys wielding everything from soldering irons to scripting languages in cybersecurity competitions, hackathons, and CTFs.

Cheryl Biswas

MENTOR to Yasmine Johnston-Ison

I'm a hunter! But what does that mean?

Proving Ground, Wednesday, 14:00–14:25

Cheryl Biswas is a Strategic Threat Intel Analyst with TD Bank in Toronto, Canada, where she monitors and assesses international relations, threat actors, vulnerabilities and exploits. In her previous role with KPMG Canada, she was a Cyber Security Consultant and worked on security audits and assessment, privacy, breaches, and DRP. She has worked in a variety of fields, and her experience includes project management, vendor management and change management. Cheryl holds an ITIL certification and a specialized honours degree in Political Science. Her areas of interest include APTs, mainframes, ransomware, ICS SCADA, and building threat intel. She actively shares her passion for security online, and as a speaker and a volunteer at conferences. Cheryl is a founding member of "The Diana Initiative," whose mandate is to encourage and support women and diversity in Infosec.

Sam Bowne

Reverse Engineering Android Apps

Training Ground, Tuesday, 08:00–11:55

Sam Bowne is the proprietor of Bowne Consulting and an instructor at City College San Francisco, and has been teaching hacking and security classes for ten years. He has presented talks and workshops at Defcon, HOPE, RSA, BSidesLV, BSidesSF, and many other conferences. He has a CISSP and a PhD and is a DEF CON Black Badge co-winner.

Bryson Bort

Where in the world are Carmen's $adjective cyber attacks: The game show that wonders why things aren't worse

Common Ground, Tuesday, 14:00–14:55

co-presenting

No IOUs with IOT

I Am The Cavalry, Wednesday, 18:00–18:25

Bryson is the Founder of SCYTHE, a start-up building a next generation attack emulation platform, and GRIMM, a boutique cybersecurity consultancy, and Co-Founder of the ICS Village, a non-profit advancing awareness of industrial control system security. He is a National Security Institute Fellow and an Advisor to the Army Cyber Institute. Prior, Bryson led an elite offensive capabilities development group. As a U.S. Army Officer, he served as a Battle Captain and Brigade Engineering Officer in support of Operation Iraqi Freedom before leaving the Army as a Captain. Bryson received his Bachelor of Science in Computer Science with honors from the United States Military Academy at West Point. He holds a Master's Degree in Telecommunications Management from the University of Maryland, a Master's in Business Administration from the University of Florida, and completed graduate studies in Electrical Engineering and Computer Science at the University of Texas.

Kent Brake

Finding Evil with Mitre ATT&CK and the Elastic Stack

Training Ground, Wednesday, 14:00–17:55

co-presenting

Kent Brake is a Principal Solutions Architect based in Richmond, VA. At Elastic, Kent works with Department of Defense customers as well as commercial partners with a focus on security analytics. Before joining Elastic, Kent spent 9 years building Cloudmark based messaging security with customers like AT&T, Facebook and FireEye.

Rob Brandon

Evaluating Code Embeddings

Ground Truth, Tuesday, 19:00–19:25

Rob is a researcher on the Advanced Threat Hunting team in Booz Allen Hamilton Dark Labs. He has a PhD in computer science from the University of Maryland, Baltimore County and multiple years of experience in the computer security field. His research interests include semantic modeling of computer programs, reverse engineering, and cataloging the inevitable failure of human efforts to build well-engineered systems.

Rodrigo Brenes

The Contemplator Approach: Data Enrichment Through Elastic Stack

Common Ground, Tuesday, 15:00–15:55

Professional on Information Technology with over seven years of work experience in the Information Security field. He has worked for large companies, including HP and IBM on Enterprise Vulnerability Management and Secure Operation Center, and he is currently employed as the Information Security Operations Lead at National Instruments. In his current role, Rodrigo supports the security event and incident management plus other security initiatives and projects.

https://www.linkedin.com/in/brenessa

Pablo Breuer

Applying Information Security Paradigms to Misinformation Campaigns: A Multidisciplinary Approach

Ground Truth, Tuesday, 11:30–12:25

Pablo Breuer is currently the director of US Special Operations Command Donovan Group and senior military advisor and innovation officer to SOFWERX. He's served at the National Security Agency and U.S. Cyber Command as well as being the Director of C4 at U.S. Naval Forces Central Command. He is a DoD Cyber Cup and Defcon Black Badge winner, and has been adjunct faculty at National University, California State University Monterey Bay, and a Visiting Scientist at Carnegie Mellon CERT/SEI. He has taught classes for various U.S. government agencies and industry on topics ranging from malware reverse engineering and exploit development to cyber policy and authorities. Pablo is also a founder and board member of The Diana

Initiative, an InfoSec event focused on advancing the careers of women in cyber security, and is on the staff for BSides Las Vegas and CircleCityCon. Pablo holds degrees in computer science.

Matt Brown

Automatic Security Analysis of IoT Firmware

I Am The Cavalry, Tuesday, 17:00–17:55

Matt Brown works by day as an infosec professional and by night as a Free Software hacker. His interests in IoT security began at his first Defcon (23) where he placed 2nd in the IoT CTF. Today, Matt works as an internal IoT pentester for a major home security company. Matt specializes in IoT pentesting and reverse engineering. When not hacking, you will find Matt serving at his local church or gaming on his PCI passthrough setup.

John Brunn

Give the dog a bone—Exploring OSINT capabilities of pen-testing tools

Ground1234!, Tuesday, 17:00–17:55

John has over 20 years of infosec experience, and is currently head of security at CMD. Settling in San Francisco in 2000, he has run security teams at retail and travel e-commerce companies, as well as a mobile security startup. He once cooked the breakfast bar at Michigan Big Boy restaurants. In his free time he plays guitar in an Alt-Country band and plays beer-league ice hockey. His dog probably hates him.

Jack Burgess

Birthday Hunting

Ground Truth, Wednesday, 17:00–17:25

Trained physicist, now security data scientist, Jack has worked with companies large and small to enhance their capabilities through the practical application of analytics. Having lead a number of Spark / Metron based security projects in Melbourne, New York, and Los Angeles working on distributed computing and infosec problems are passions followed very closely by talking about them.

Cherie Burgett

Discovering Your Passion in Cyber Security

Hire Ground, Tuesday, 14:00–14:25

Cherie Burgett is an Intelligence Analyst, Threat Researcher, Public Speaker, Theologian, and ISAC Operations, Director. As the Director of ISAC Operations for the Mining and Metals ISAC, Cherie Burgett leads the ISAC's cyber intelligence program, enables sharing and coordinates responses to active threats, provides the link between the public and private sector, and supports companies develop strategies as they undergo digital transformation.

Russell Butturini

MENTOR to Winnona DeSombre

Bestsellers in the Underground Economy—Measuring Malware Popularity by Forum

Proving Ground, Tuesday, 11:30–11:55

I've been a mentor for Bsides Las Vegas twice before, in 2015 and 2018. It's a super rewarding experience that I enjoy greatly. I'm really proud of the talks my mentees have put together and the finished product. I've also been a presenter multiple times at Derbycon, other BSides, and the Wall of Sheep.

Megan Calidonna, Cylance

Behind the Recruiting Curtain: What Do Recruiters Really Say and Do [SPONSORED]

Hire Ground, Tuesday, 17:30–17:55

co-presenting

Ezra Caltum

Using Machines to exploit Machines—harnessing AI to accelerate exploitation

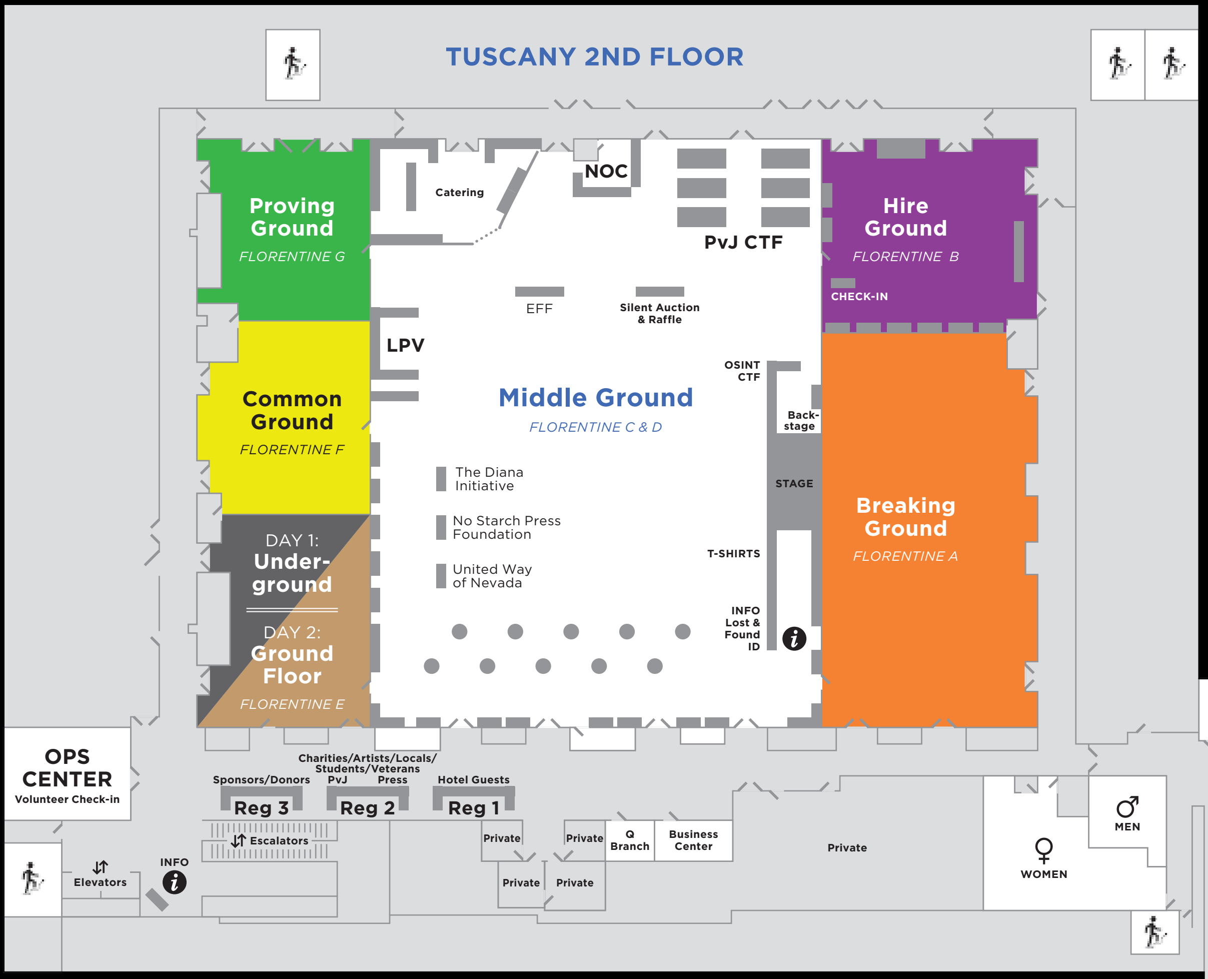
Breaking Ground, Tuesday, 15:00–15:55

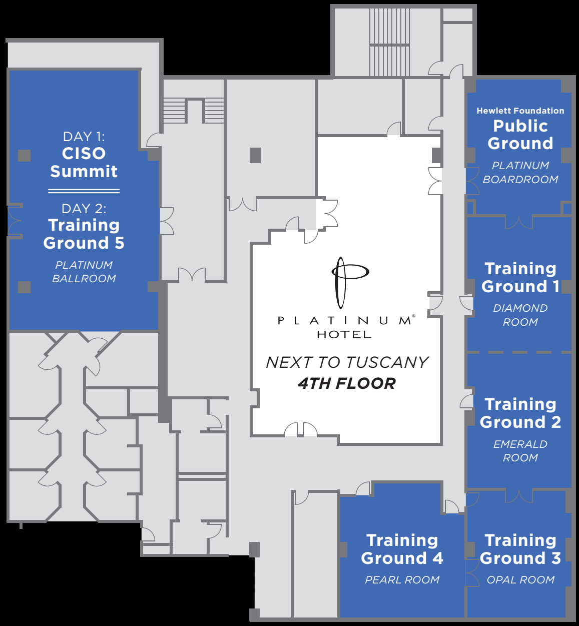
co-presenting

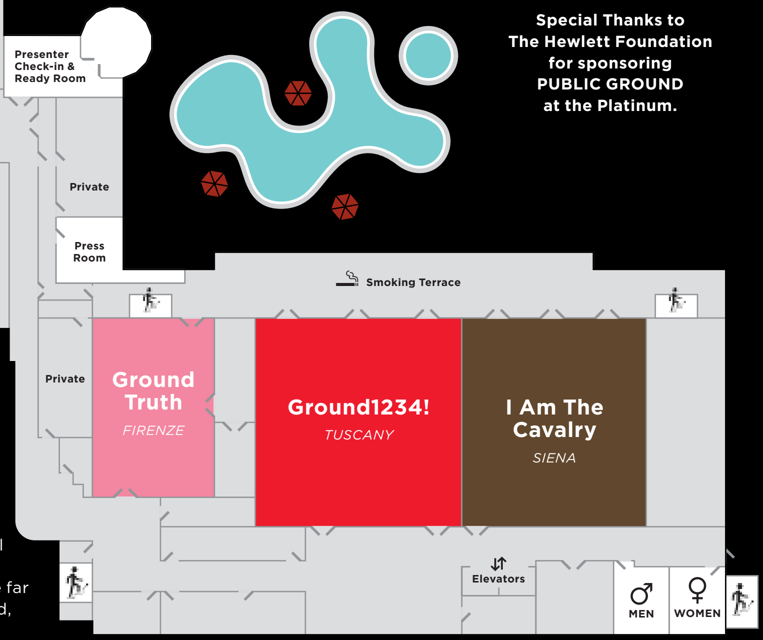
Ezra is an information security practitioner, with a passion for reverse engineering, data analysis, and exploitation. He is the leader of the Tel Aviv DC9723 Defcon group and a co-founder and organizer of BSidesTLV. Currently, he works as a Security Research Manager at a Fortune 500 company. Ezra has presented at T2 Infosec Conference, BSidesLV, 44CON, Skytalks, BlackHat Arsenal, AppsecIL.

2019 Map of Venues

NOTE: Training Ground and Public Ground are at The Platinum Hotel, just northwest of The Tuscany, on the 4th floor.







Special Thanks to
The Hewlett Foundation
for sponsoring
PUBLIC GROUND
at the Platinum.

The Quiet Room

COPA ROOM
TUSCANY CASINO FLOOR

BSidesLV: 194 countries, 1 community...

The #BSidesBus will be at LAS airport, Tuscany, and Mandalay Bay, then Bally's and Planet Hollywood through DC27. Schedule is on page 12, and at bsideslv.org/shuttle-schedule.

The shuttle stop is at the Tuscany Hotel entrance (NOT the Casino). Wait on the far side of the bell stand, under the carport.

Matt Canham

Neurosecurity: where Infosec meets Brain-machine Interface

Breaking Ground, Tuesday, 18:00–18:55

co-presenting

Former supervisory agent with the FBI, PhD in Cognitive Psychology, deep expertise in infosec, and a faculty position at UCF's IST group. There, Matt is a member of LabX (Laboratory for Autonomy-Brain Exchange), and works with UCF's own infosec groups to build large-scale experiments into what makes individuals susceptible to cyberattack.

Andrew Case

Windows 10 DFIR Challenges

Ground Floor, Wednesday, 14:00–14:55

Andrew Case is the Director of Research at Volexity and a core developer of the Volatility memory analysis framework. His professional experience includes digital forensic investigations, incident response handling, malware analysis, penetration tests, and source code audits. Andrew is a co-author of the award-winning book "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory". Andrew also co-teaches the "Digital Forensics & Incident Response" class at Black Hat. Andrew's primary research focus is physical memory analysis, and he has presented his research at conferences including Black Hat, RSA, SecTor, SOURCE, BSides, OMFW, GFirst, and DFRWS.

Gregory Caswell

Baited Canaries—Monitoring attackers with active beacons

Proving Ground, Wednesday, 17:30–17:55

MENTOR: Michael Aguilar

Greg Caswell is an engineer at heart who enjoys helping make software systems slightly less terrible. For the past five years he has been building and managing an application security team at Indeed, responsible for teaching security concepts to developers, assessing the security of 1000's of applications, triaging bug bounty submissions, and automating as much as they can in the process. He holds degrees in electrical and computer engineering. Outside of security, he enjoys bee-keeping, aquaponics, and cooking.

Jared Chandler

So you think you can CHMOD

Proving Ground, Tuesday, 18:00–18:25

MENTOR: Emily Gladstone Cole

Jared Chandler is a graduate student at Tufts University. His research is focused on automated reverse engineering of network protocols and other applied formal methods in support of cybersecurity. He has over a decade of industry experience as a software developer and systems engineer. Prior to studying computer science at Tufts he studied European history and fine arts, receiving degrees in both from the University of Alaska Anchorage.

Dhivya Chandramouleeswaran

Who dis? The Right Way To Authenticate

Ground1234!, Wednesday, 14:00–14:55

co-presenting

Dhivya Chandramouleeswaran is a Security Researcher at Adobe. She received her master's degree in Information Security and Information Technology from Carnegie Mellon University in 2017. At Adobe, she provides proactive security guidance to key product teams, devel-ops security automation tools and enjoys reviewing security of new technologies. She loves talking about her open source projects at conferences, most recent being Girls Who Code, DefendCon and CISO summit.

Matt Cheung

Introduction to Cryptographic Attacks

Training Ground, Wednesday, 08:00–11:55

Matt Cheung started developing his interest in cryptography during an internship in 2011. He worked on implementation of a secure multiparty protocol by adding elliptic curve support to an existing secure text pattern matching protocol. Implementation weaknesses were not a priority and this concerned Matt. This concern prompted him to learn about cryptographic attacks from Dan Boneh's crypto 1 course offered on Coursera and the Matasano/cryptopals challenges. From this experience he has given talks and workshops at the Boston Application Security Conference and the DEF CON Crypto and Privacy Village.

Richard Cho, Robinhood

Behind the Recruiting Curtain: What Do Recruiters Really Say and Do [SPONSORED]

Hire Ground, Tuesday, 17:30–17:55

co-presenting

Ming Chow

MENTOR to Joe O'Connell

The struggles of teaching automation

Proving Ground, Wednesday, 11:00–11:25

Ming Chow is a Senior Lecturer at the Tufts University Department of Computer Science. His areas of interest are web and mobile security, and Computer Science education. He has served as a mentor to BSides Las Vegas Proving Ground track speakers since 2014, a track focused on helping new speakers in the information security and hacker communities acclimate to public speaking. Ming was named the 2016 Henry and Madeline Fischer Award recipient at Tufts, awarded annually to a faculty member of the School of Engineering judged by graduating seniors of the School of Engineering to be "Engineering's Teacher of the Year." He was named the 2017 Lerman-Neubauer Prize for Outstanding Teaching and Advising recipient at Tufts, awarded annually to a faculty member who has had a profound intellectual impact on his or her students, both inside and outside the classroom.

Emily Gladstone Cole

MENTOR to Jared Chandler

So you think you can CHMOD

Proving Ground, Tuesday, 18:00–18:25

Emily is currently a Senior Security Engineer for Agari Data, Inc., and spends a lot of time thinking about the ways that DevOps and Security intersect. Emily has performed critical organizational roles of security research, incident response, product security, devops engineer, system administrator, tech support, security expert, operations specialist, and project lead. Emily specializes in Unix security and is a co-author of a book on Solaris Security for the SANS Institute, and serves as a Mentor for SANS' CyberTalent Immersion Academy for Women. She has spoken about DevOps and Security at DevOpsDays Silicon Valley, BSides Las Vegas, and the USENIX LISA conference. She holds GSEC, GCED, GPPA, GCIH, and ITIL certifications, and is a Certified Scrum Master.

Joshua Corman

I Am The Cavalry Track Welcome and Overview

I Am The Cavalry, Tuesday, 11:30–11:55

Joshua Corman is a Founder of I am The Cavalry (dot org) and CSO for PTC. Corman previously served as Director of the Cyber Statecraft Initiative for the Atlantic Council, CTO for Sonatype, Director of Security Intelligence for Akamai, and in senior research & strategy roles for The 451 Group and IBM Internet Security Systems. He co-founded RuggedSoftware and IamTheCavalry to encourage new security approaches in response to the world's increasing dependence on digital infrastructure. Josh's unique approach to security in the context of human factors, adversary motivations and social impact has helped position him as one of the most trusted names in security. He also serves as an adjunct faculty for Carnegie Mellon's Heinz College and on the Congressional Task Force for Healthcare Industry Cybersecurity.

Matthew Cornelius

We the People: Providing for a 'common defence' with CVD

I Am The Cavalry, Wednesday, 17:00–17:55

co-presenting

Matthew Cornelius is a Senior Advisor for Technology and Cybersecurity at the Office of Management and Budget (OMB). He leads OMB's Federal IT Modernization Cross Agency Priority Goal, recently published as one of the key pillars of the President's Management Agenda. Mr. Cornelius worked with Congress to authorize and appropriate the Modernizing Government Technology Act (MGT Act), which established the Technology Modernization Fund (TMF). He established the Technology Modernization Board (chaired by the Federal CIO) that oversees the evaluation of projects for funding by the TMF and serves as executive secretary and principle executor of the TMF. Previously at OMB, he led the development of the Report to the President on Federal IT Modernization. Prior to OMB, Mr. Cornelius served as the Senior Advisor for Cybersecurity to the Administrator of the General Services Administration. He began his Federal career as a Policy Analyst at the Department of the Treasury.

Joseph Cox

Why journalists and hackers need each other (a panel discussion with infosec reporters)

I Am The Cavalry, Wednesday, 15:00–15:55

co-presenting

Joseph Cox covers the digital underground, hackers, and social media platforms for VICE's Motherboard. His work has triggered multiple government investigations into the sale of AT&T, T-Mobile, and Sprint real-time location data, and his series on Facebook content moderation caused the world's biggest social network to ban white nationalism.

Paul Dant

Real World Security in a Clinical Healthcare Environment: Hacking a Hospital

I Am The Cavalry, Wednesday, 14:00–14:55

My interest in security began in 1987, fueled by the need to protect my lame video games from pirates. Ever since, I've been interested in the security of systems, and information in general, as it pertains to people using systems. To that end, I've hacked unlikely things like tent-pole film sets, nuclear energy facilities, banks, and hospitals.

Falcon Darkstar

Ham Exams

Ground1234!, Wednesday, 18:00–18:55

Winnona DeSombre

Bestsellers in the Underground Economy—Measuring Malware Popularity by Forum

Proving Ground, Tuesday, 11:30–11:55

MENTOR: Russell Butturini

Winnona DeSombre is an Asia Pacific threat intelligence researcher at Recorded Future, focusing on Chinese underground hacking communities and East Asian cyber espionage campaigns. She tracks trends in cybercriminal activity, analyses new malware and tooling, and improves East-Asian sourcing within Recorded Future. In recent years, Winnona spoke at the Forbes 30 under 30 summit, won the Harvard Belfer Center D3P Hackathon by constructing risk rule calculation software to combat social media influence campaigns, and was a semi-finalist in the Atlantic Council's Cyber 9/12 competition. She was also one of the youngest individuals featured in Threatcare's "Tribe of Hackers" book, containing career advice from some of the world's best information security professionals.

Nathaniel Davis

MENTOR to Serenity Smile

The Resilient Hacker: Growth Mindset, Health Hacks & Powerful Help to Navigate Personal Challenges

Proving Ground, Tuesday, 17:30–17:55

Nathaniel is a Senior Security Threat Consultant for a major US consulting firm. His current focus is in security orchestration and automation. Previously he has consulted on incident response, rogue system detection, SIEM deployments, network architecture, boundary defense and wireless platforms. Outside of work, he serves on the board of directors for B-Sides DC where he is a volunteer coordinator.

Nicolas Daubresse

Active Directory security: 8 (very) low hanging fruits and how to smash those attack paths

Training Ground, Tuesday, 14:00–17:55

co-presenting

Nicolas Daubresse (@nicolas_dbresse) is senior security consultant at Wavestone. For four years, he has mainly performed penetration tests on global IT infrastructure and Active Directory environments. Involved in the CERT-W, he also had the occasion to see the other side of the attack and saw these vulnerabilities exploited in the wild.

Kyle Dickinson

CloudSec Rules Everything Around Me (C.R.E.A.M.)

Common Ground, Wednesday, 17:00–17:55

Kyle is a Cloud Security Architect/Shaman/Dude with experience in AWS and Azure and dealing with large Enterprises. When he's not Securing the world from the Cloud that may fall, he enjoys teaching those about Cloud Security, mixing his own experiences in to achieve how to obtain peace between their company and skylords.

James Dietle

Building the badge—How you can make small, cheap and custom hardware for function or fashion

Proving Ground, Tuesday, 18:30–18:55

MENTOR: Rachael Lininger

James is a computer enthusiast who started off slinging CAT5, coax and silver satin in exchange for ice cream at the age of eight. As a naval officer in the intelligence community, he worked with NSA across the world and has over 13 years of Information Technology management experience. More recently he has been burning out GPUs, stopping criminals, and spreading comradery through cheap pcb.

Cameron Dixon

We the People: Providing for a 'common defence' with CVD

I Am The Cavalry, Wednesday, 17:00–17:55

Cameron's service in government has focused on internet scanning and direct reporting as a policy forcing function. He was the product manager for "Cyber Hygiene", a vulnerability scanning service that helps users detect flaws and adopt modern security protocols. He was the lead technical author of several cybersecurity directives that require civilian executive branch agencies maintain good practices in web encryption, email authentication, and DNS security. He also managed the development of open source tools to track the directives' progress. In 2018, Cameron served as the deputy program manager for the .gov top-level domain at the General Services Administration, where he ran day-to-day operations. Key outcomes of his work included mandatory two-factor authentication to the .gov registrar, a plain-language website for the TLD, and guiding new domain registrants to publish a security contact to WHOIS and adopt security features like HSTS preloading or strong DMARC policies.

Ethan Gregory Dodge

MENTOR to Mathieu Saulnier

The SOC Counter ATT&CK

Proving Ground, Wednesday, 11:30–11:55

Ethan Gregory Dodge has 5 years experience as a Security Engineer and Analyst. He specializes in security monitoring and incident response. He is the co-founder and Technical Director of the Truth & Transparency Foundation, a non profit newsroom dedicated to exposing abuse and corruption within religious institutions. The Foundation operates the sites MormonLeaks and FaithLeaks. Ethan is responsible for the secure communications and ensuring that sources remain anonymous.

Gerald Doussot

State of DNS Rebinding—Attack & Prevention Techniques and the Singularity of Origin

Breaking Ground, Wednesday, 18:00–18:55

He is currently a Cyber Security Consultant, focusing on OS and Services Hardening, Cryptography, AI Security, and Reverse Engineering.

Bradley Duncan

Malware Traffic Analysis Workshop

Training Ground, Tuesday, 08:00–17:55

After 21 years of classified intelligence work for the US Air Force, Brad transitioned to cyber security in 2010, and he is a currently a Threat Intelligence Analyst for Palo Alto Networks Unit 42. Brad specializes in network traffic analysis. He is also a handler for the Internet Storm Center (ISC) and has posted more than 140 diaries at isc.sans.edu. Brad routinely blogs technical details and analysis of infection traffic at www.malware-traffic-analysis.net, where he provides traffic analysis exercises and over 1,600 malware and pcap samples to a growing community of information security professionals.

Matt Duren

Behind the Recruiting Curtain: What Do Recruiters Really Say and Do [SPONSORED]

Hire Ground, Tuesday, 17:30–17:55

Matt Duren has been in recruiting since he graduated college in 2001. Starting out in a technical staffing agency, Matt quickly transitioned to corporate recruiting and has lead recruiting teams responsible for IT and college recruiting, as well as Employment Branding. Matt is currently a Sr. Recruiting Manager at Tenable, located in Columbia, MD. Originally from Virginia, Matt has lived in Maryland since graduating from James Madison University. He also holds a Masters in Organizational Development and Strategic HR from Johns Hopkins. When he's not recruiting, you can find Matt enjoying family-time with his wife and two daughters, training for the occasional Obstacle Course Race, and eating Gummy Bears…lots of Gummy Bears.

Rohan Durve

Windows Breakout and Privilege Escalation

Training Ground, Tuesday, 08:00–17:55

Rohan (@Decode141) started his career as a bounty hunter and then moved into specialist consultancy. He primarily assesses Windows systems, but has previously contributed to application and software research (such as Formula Injection and client-sided code execution vulnerabilities in common software). Rohan holds certs such as OSCE, OSCP and CREST CCT.

Benjamin Edwards

Scratching the Surface of Risk

Ground Truth, Wednesday, 18:00–18:55

Benjamin Edwards joined the Cyentia Institute as a Senior Data Scientist at the beginning of 2019. He was formerly with IBM Research, where he worked in applying advanced machine learning techniques to solve real world security problems and shaped the next generation of analytical security models. Before that he received his Ph.D. from the University of New Mexico with a research focus that blended the fields of security, data science, and complex systems. His work has lead to a better understanding of global attack trends, the effects of security interventions, and even nation state cybersecurity policy.

Keren Elazari

"Hackers of the world—unite?"

I Am The Cavalry, Tuesday, 12:00–12:25

Keren Elazari is an internationally recognized researcher, author and speaker on all matters cyber security and hacker culture. Since 2000, Keren has worked with leading security firms, public organizations and Fortune 500 companies. Keren's independent research about cyber security has been featured by Scientific American, WIRED , TED, CNN, Financial Times and more. Keren's TED talk "Hackers: the Internet's immune system" has been viewed by millions online, translated to 30 languages, selected as "Most Powerful Ideas" and helped shape a global conversation about the role of hackers in the information age. In 2016 Keren founded BSidesTLV, a community event for hackers in Israel. Keren is also a visiting faculty member of Singularity University. In 2016 she collaborated on the Amazon bestseller book for "Women in Tech" (Penguin Random House).

Monta Elkins

How to Treat Your Hacker (and Responsible Vulnerability Disclosure)

I Am The Cavalry, Wednesday, 10:00–10:55

Monta Elkins is "Hacker-in-Chief" for FoxGuard Solutions, an ICS patch information provider. A security researcher/consultant and U.S. patent grantee, he is considered by many of his friends to be the Chuck Norris of ICS Cybersecurity. Monta has been a speaker at more security conferences than even his enormous ego can remember including: DEFCON, CS3STHLM, BSIDES, GE Digital Energy, ICSJWG, Toshiba ICS, GridSecCon, ICS CyberSecurity, UTC Telecom, SANS ICS Summit and was named Cybersecurity Professional of the Year by EnergySec. In his spare time, Monta creates the totally-safe-for-work "Coke and Strippers" electronic projects YouTube channel https://tinyurl.com/y6vpmbw4. Monta is the author of "Defense Against the Dark Arts" hands-on hacker tools and techniques classes, and a Certified SANS instructor. He is also a guest lecturer for colleges, universities and elsewhere. As a small child, he entertained himself by memorizing Pi—backwards.

Jen Ellis

Meet the Nation This Week on Sunday: A Special Vulnerability Edition

Common Ground, Wednesday, 18:00–18:55

Jen Ellis is the vice president of community and public affairs at Rapid7. Jen's primary focus is on building productive collaboration between those in the security community and those operating outside it. She works extensively with security researchers, technology providers and operators, and various government entities to help them understand and address cybersecurity challenges. She believes effective collaboration is our only path forward to reducing cybercrime and protecting consumers and businesses. She has testified before Congress and spoken at a number of security industry events including SXSW, RSA, Derbycon, Shmoocon, SOURCE, UNITED, and various BSides.

Chris Eng

MENTOR to Sanne Maasakkers

Analyzing user decision making on phishing sites—using mouse data and keyboard dynamics

Proving Ground, Tuesday, 14:30–14:55

Chris Eng is Chief Research Officer at Veracode. A founding member of the Veracode team, he is responsible for all research and product security initiatives. Chris is a frequent speaker at industry conferences, and he serves on program committees for BlackHat USA and the Kaspersky Security Analyst Summit. Bloomberg, Fox Business, CBS, and other prominent media outlets have featured Chris in their coverage.

Remi Escourrou

Active Directory security: 8 (very) low hanging fruits and how to smash those attack paths

Training Ground, Tuesday, 14:00–17:55

Remi Escourrou (@remiescourrou) is senior security consultant at Wavestone. For four years, he has been developing his skills as a pentester of IT infrastructure, red teamer and more specifically on Active Directory environment. He is also involved in the CERT-W as First Responder and already saw the other side of the attack.

Tom Eston

MENTOR to Tanner Barnes

Burpsuite Team Server—Collaborative Web Pwnage

Proving Ground, Tuesday, 17:00–17:25

Tom Eston is the Manager of Penetration Testing at Veracode. Tom's work over his 14 years in cybersecurity has focused on network, red team and application penetration testing as well as security and privacy research. He has led multiple projects in the cybersecurity community, improved industry standard testing methodologies and is an experienced team manager and leader. He is also the founder and co-host of the weekly Shared Security Podcast; and a frequent speaker at security user groups and international cybersecurity conferences including Black Hat, DEF CON, DerbyCon, SANS, InfoSec World, OWASP AppSec, and ShmooCon.

Wendy Knox Everette

MENTOR to Pete Thurston

Salesforce Data Governance What dark secrets lurk in your instance??

Proving Ground, Tuesday, 14:00–14:25

Wendy is a software developer who burned out and went to law school, where she completed a concentration in National Security Law and interned with the FTC, FCC, and some other three letter agencies (no, not the fun ones). After law school she completed a fellowship in privacy and information security law at ZwillGen. She currently lives in Seattle, where she is a Senior Security Advisor at Leviathan Security Group.

Dimitri Fousekis

Low & Slow—Techniques for DNS Data Exfiltration

Ground Floor, Wednesday, 12:00–12:25

Dimitri has been in the security industry for over 15 years, and is the CTO of a cyber security company. Having enjoyed many years of Passwords, and password-related talks, he is branching out to cover another one of his passions: Ways to exfiltrate data. Dimitri has spoken at BSides in a few countries as well as PasswordsCon and other conferences.

Allan Friedman

Where in the world are Carmen's $adjective cyber attacks: The game show that wonders why things aren't worse

Common Ground, Tuesday, 14:00–14:55

The Case for Software Bill of Materials

I Am The Cavalry, Tuesday, 15:00–15:55

MENTOR to Vanessa Redman

The drunk colonel and the flipped stone: Game Theory for a Defensive Strategic Advantage

Proving Ground, Wednesday, 12:00–12:25

Allan Friedman is Director of Cybersecurity at National Telecommunications and Information Administration in the US Department of Commerce. He coordinates NTIA's multistakeholder processes on cybersecurity, focusing on addressing vulnerabilities in IoT and across the software world. Prior to joining the Federal Government, Friedman spent over 15 years as a noted InfoSec and tech policy scholar at Harvard's Computer Science Department, the Brookings Institution and George Washington University's Engineering School. He is the co-author of the popular text Cybersecurity and Cyberwar: What Everyone Needs to Know, has a degree in computer science from Swarthmore College and a PhD in public policy from Harvard University, and is quite friendly for a failed professor-turned-technocrat.

Vanessa Frost

Examining DES-based Cipher Suite Support within the TLS Ecosystem

Proving Ground, Tuesday, 12:00–12:25

MENTOR: Jeff Man

Vanessa Frost is a current cybersecurity graduate student working with Dr. Kevin Butler at the FICS research lab at the University of Florida. Her research interests include protecting consumer data privacy from third-parties, limiting the effectiveness of mass-surveillance techniques, and promoting anti-censorship technologies and protocols. After two years in a PhD program, she's pretty convinced that nothing is secure and never will be and that the human species really took the Stone Age for granted. She's grateful for the Internet that allows her to play video games with friends and still can't wrap her head around the fact that most of the giants in computer science are still living. Her heroes include her mother and caffeine. She hates lima beans and public speaking.

Jeremy Galloway

Excuse Me, Your Sword Is In My Eye: Responding to Red Teams and Intrusions in 2019 and Beyond

Common Ground, Wednesday, 12:00–12:25

Jeremy Galloway has been active in the security scene since 2002, focusing on the dark corners of the internet, hacktivism, pen-testing, intelligence gathering, privacy technologies, and incident response. When he's not reading old text files or dreaming in 7-bit ASCII, his time is spent cycling, hiking, meditating, making street art, and generally practicing civil disobedience. Although he aims to protect the internet at large, his dream is to become Beyoncé's personal cyber-bodyguard. Jeremy is a proud member of both the Electronic Frontier Foundation and The Satanic Temple.

Eva Galperin

Ask the EFF

Underground, Tuesday, 18:00–18:55

co-presenting

Eva Galperin is EFF's Director of Cybersecurity. Prior to 2007, when she came to work for EFF, Eva worked in security and IT in Silicon Valley and earned degrees in Political Science and International Relations from SFSU. Her work is primarily focused on providing privacy and security for vulnerable populations around the world. To that end, she has applied the combination of her political science and technical background to everything from organizing EFF's Tor Relay Challenge, to writing privacy and security training materials (including Surveillance Self Defense and the Digital First Aid Kit), and publishing research on malware in Syria, Vietnam, Kazakhstan. When she is not collecting new and exotic malware, she practices aerial circus arts and learning new languages.

Clint Gibler

MENTOR to Suchi Pahi

Cover Your A**

Proving Ground, Wednesday, 15:00–15:55

Clint Gibler is a research director at NCC Group, a global information assurance specialist providing organizations with security consulting services. He's helped companies implement security automation and DevSecOps best practices as well as performed penetration tests for companies ranging from large enterprises to new startups. Clint is also a co-founder of Practical Program Analysis, LLC, a boutique security firm that builds tools to make application security teams more efficient and effective. Clint has previously spoken at conferences including BlackHat USA, AppSec USA, and AppSec EU. Clint holds a Ph.D. in Computer Science from the University of California, Davis.

Brett Goldstein

Hacking the Pentagon: How a Rebel Alliance Shifts Culture to Protect National Security

I Am The Cavalry, Wednesday, 11:00–11:55

Brett Goldstein is the Director of Defense Digital Service, where he leads a team of technologists focused on high-impact problems at the Department of Defense. Throughout his career, Brett has served in a range of mission-driven leadership roles across government, the private sector, and academia. He is deeply committed to improving government through data and technology, and by creating tools and new approaches for smarter decision making and better services. Brett began his technology career at OpenTable, where he helped grow the company from an early stage startup to a multinational corporation. He later joined the Chicago Police Department where he led the department's efforts at predictive analytics. He became Chicago and the nation's first Chief Data Officer and later Chicago's Chief Information Officer. Brett continues to serve as a Senior Fellow and Special Adviser for Urban Science at the University of Chicago.

Andy Grant

Unpacking pkgs: A look inside macOS Installer packages and common security flaws

Breaking Ground, Tuesday, 14:00–14:55

Andy Grant is a Technical Vice President for NCC Group. While at NCC Group, Andy has worked on a wide-variety of security assessment and advisory projects. He has performed numerous application assessments on mobile (Android, iOS, WP7), desktop (OS X/macOS, Windows, Linux), and web platforms. He has also performed many internal and external network penetration tests and widget/third-party platform reviews. Andy has worked with small tech start-ups, small and large software development groups, and large financial institutions. Andy has a BS in Computer Science and Advanced Computer Security Certificate from Stanford University.

Ian Gray

Giving Credit Where It's Not Due: Visualizing Joker's Stash

Underground, Tuesday, 15:00–15:55

Ian Gray is the Director of Americas Research and Analysis at Flashpoint, where he focuses on Deep & Dark Web intelligence. Ian actively researches cybercriminal usage of new and emerging technologies for malicious purposes in English and Portuguese language communities. Additionally, he has been researching policy gaps that contribute to various forms of fraud, as well as the economic factors contributing to cybercrime. Ian is also an adjunct Professor at Fordham University's Master of Cybersecurity Program.

John Grigg

Hack (Apart) Your Career—How to Fund Doing What You Love

Hire Ground, Tuesday, 14:30–14:55

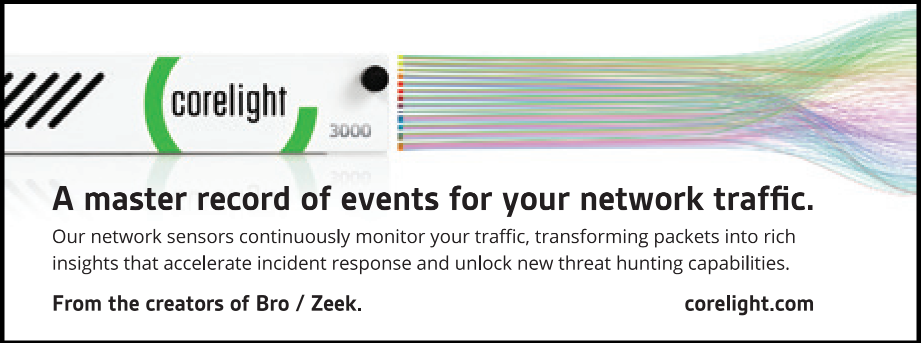
I have 12 years of experience within the Navy, the Intelligence Community, and in the corporate cyber security world with focuses on building and maturing Security Operations / InfoSec teams, SIEM/IDS/IPS engineering, malware analysis, and cyber operations. I'm currently working for my own company that focuses on "unique" requests for solutions.

Matthew Hahn

Getting CVSS, NVD, and CVEs to Work for You: Standardizing and Scaling Your Vulnerability Risk Analysis

Common Ground, Wednesday, 14:30–14:55

Matt is a Director of Information Security at First Information Technology Services with over 10 years of professional experience in the regulatory environments of IT security, housing, and accounting. He specializes in vulnerability management and risk analysis, and he is an expert in FedRAMP Continuous Monitoring with working knowledge of the entire FedRAMP process. In his role at FITS, Matt manages continuous monitoring work for commercial clients and provides guidance to customers for their compliance audits. He uses his expertise to help customers drive vulnerability remediation and improve their cybersecurity risk posture.



Russell Handorf

Why can't we be friends? (Ask a Fed & the EFF.)

Ground1234!, Wednesday, 17:00–17:55

Russ Handorf works for the United States Federal Bureau of Investigation. Russ is a lot of things: hacker, friend, father, husband, teacher and a Fed. While not chasing squirrels… Well, he is always chasing squirrels. Who he is actually isn't important, but what he's bringing is; cyber ninjas, you're invited.

Chris Hanlon

Hands on Hacking The OWASP TOP 10 and beyond

Training Ground, Wednesday, 14:00–17:55

During the workday: Chris Hanlon runs an Information Security Consulting Business where he monitors and protects Endpoints, Routers, Servers, and Cloud Systems. In addition to protecting infrastructure, Chris also coaches software companies on ways to minimize vulnerabilities in their code, and reduce their vulnerability to social engineering attacks. During his "free time", Chris finds/reports security vulnerabilities, hosts hack-a-thons, uses real world exploits to help developers understand security vulnerabilities, lectures at colleges, presents at conferences , organizes security conferences, and volunteers on the presentation review board for a BSides Conference. Based on multiple vulnerability submissions, Chris was added to the Google Security Hall Of Fame in 2014. Chris has also been recognized for security vulnerabilities reported to the University of British Columbia and a Linux Kernel File System Module.

Richard Harang

Security data science—Getting the fundamentals right

Ground Truth, Wednesday, 10:00–10:55

Richard Harang is a Director of Data Science Research at Sophos with over eight years of research experience at the intersection of computer security, machine learning, and privacy. Prior to joining Sophos, he served as a scientist at the U.S. Army Research Laboratory, where he led the research group investigating the applications of machine learning and statistical analysis to problems in network security. He received his PhD in Statistics from the University of California, Santa Barbara. Research interests include randomized methods in machine learning, adversarial machine learning, and ways to use machine learning to support human analysis. By day he uses bad guys to catch math. By night he teaches killer robots to protect his garden from squirrels.

Jon Hawes

Building an enterprise security knowledge graph to fuel better decisions, faster

Ground Truth, Tuesday, 14:00–14:55

Jon runs the Detect function at Photobox Group, which covers Security Operations, Incident Response and Red Team Testing. He also leads the Security Innovation Hub, running projects to evaluate technologies and processes that support data-informed decision making, process automation and a DevOps engineering culture. Prior to Photobox, Jon worked in various roles doing strategy, architecture, product management, project management and data analytics for companies that ranged from startups to federated multi-nationals. When he's not doing security he's either longboarding or writing music.

Claus Houmann

MENTOR to Toru Shimanaka

Cyber Deception after Detection: Safe observation environment using Software Defined Networking

Proving Ground, Wednesday, 15:30–15:55

Claus is a former bank CISO, a former Analyst and infosec blogger who has now turned Cloud Security lead for a CSIRT. Claus loves everything infosec and has been trying to learn at least the basics over the last many years. Claus has presented extensively at conferences on doing the basics well or at least better and has previously focused a lot on helping SMBs become more secure.

David Hunt

Hands-on: How to Use CALDERA's Chain Mode

Training Ground, Tuesday, 14:00–17:55

David Hunt is a Principal Cyber Security Engineer at MITRE, where he works on automated adversary emulation. He is currently leading development of the open-source CALDERA platform, along with contributing to other projects in MITRE's internal research and development portfolio. Prior to MITRE, David led engineering for FireEye's threat intelligence division from 2016 to 2018. There, he orchestrated the storage and assimilation of APT behavioral data at scale, improving analysts' access to sensitive information. In addition to a decade in systems and software engineering, David has 5 years of experience in red team environments for both large companies and security start-ups. This time in the field has given David valuable insight into how adversaries operate in the wild. He has a passion for combining these experiences to solve real-world problems in creative ways.

Stephanie Ihezukwu

Mind the Diversity Gap—A Panel Discussion

Common Ground, Tuesday, 17:00–17:55

co-presenting

Stephanie is the resident Information Security Analyst for a global law firm. She is the creator and editor of StephAndSec.com, a blog focused on technology, inclusion and lifetime learning. She spends her time mentoring high school students, hosting virtual labs via Women In Tech-a-thons, being Chapter Head for WoSEC Houston, and giving back to the community.

Kenny Jansson

Making your website vulnerable for fun and security awareness

Proving Ground, Wednesday, 10:00–10:25

MENTOR: Bill Weiss

Security Manager in the Norwegian Insurance Corporation Storebrand, with responsibility of ensuring security in digital services and increasing web application awareness, working closely with developers and DevOps teams. Previously Cyber Threat management consultant in EY, leading teams in penetration testing engagements. Holder of multiple certifications including GXPN, GWAPT, GPEN, OSCP.

Yasmine Johnston-Ison

I'm a hunter! But what does that mean?

Proving Ground, Wednesday, 14:00–14:25

MENTOR: Cheryl Biswas

I started tinkering with webpage vulnerabilities when I was around 17 years old. I had no clue it was a real job. I was soon, purposefully, infecting my own computers with spyware to see what happens and how they work. Then I joined the military (around 19 years old) as a Signals Intelligence Analyst (National Guard 2003, active duty Army 2005, and ended my career last year in the reserves). I've done some threat targeting downrange in Afghanistan and Iraq and even more targeting back here stateside. I left the targeting-focused world for a short time when I worked at the Department of Energy as their Senior Reverse Engineer. Currently, I am working at Fidelis as a Principal Threat Researcher. As you can see, my career grew up in the shadows of digital conversations. I saw and learned so much. A target is a target—human or digital.

Kevin King

Hacking the STORM

Training Ground, Wednesday, 08:00–17:55

co-presenting

Over years working both on a contractual basis and as an employee for New Horizons (NH), Kevin has become a world-class CCSI & MCT instructor teaching classes to thousands of students from Microsoft MCSE Networking and MCSE Private Cloud to Cisco's CCNP and CCNA classes. Kevin has several times ranked in the top 10 NH instructors worldwide and has won Cisco's coveted "Routing & Switching | Instructor Excellence Award" over many consecutive years. He has taught over 20,000 hours. Kevin has been mainly hacking Cisco, Microsoft, and linux networks and devices in his capacity as systems/network Admin and infrastructure networking consultant. He enjoys creating/using Raspberry Pi tools and a good SQLi.

Nick Koch

Human honeypots, or: How I learned to stop worrying and love the NFC Implant

Proving Ground, Wednesday, 10:30–10:55

MENTOR: Patrick McNeil

Cybersecurity student out of Pensacola Fl, who spends his time breaking electronics, fixing them, and breaking them again. I have been experimenting with hardware and software for 13 years, mainly focusing on setting up networking and security for small businesses and amateur radio. Now I spend most of my time trying to finish up my degree program, and educating my friends on security best practices through my blog.

Tom Kopchak

MENTOR to Ty Atkin

The Human API: Evolving End Users From Authorized Adversaries Into Our Best Defense.

Proving Ground, Tuesday, 15:30–15:55

Tom Kopchak is the Director of Technical Operations at Hurricane Labs, where he pretends to manage a team of Splunk engineers, but is still an engineer and technology geek at heart. Tom's speaking experience includes a previous talk at DC24 (Sentient Storage—Do SSDs Have a Mind of Their Own?) as well as many talks at other conferences around the country (and BSides LV in 2013). He holds a Master's degree in Computing Security from the Rochester Institute of Technology, and volunteers as the white team captain for the National Collegiate Penetration Testing Competition (CPTC). When he is not working with computers, Tom enjoys composing, music improvisation (Acts of Music), and playing both the piano and organ.

Chris Kubecka

Where in the world are Carmen's $adjective cyber attacks: The game show that wonders why things aren't worse

Common Ground, Tuesday, 14:00–14:55

co-presenting

The Road to Hell is Paved with Bad Passwords

Common Ground, Wednesday, 10:00–10:55

Chris is the founder and CEO of HypaSec. Previously, Chris headed the Information Protection Group, network operations, security operations and joint-international intelligence team for the Aramco family, helping to recover Aramco from a nation-state attack to implement digital security and reconnect international business operations. Responsible for all digital IT and ICS assets throughout the EMEA region (minus KSA) and Latin America. Subsequently, establishing and assisting global digital security teams, standards, security driven legal contracts for secure software development with third parties, the Aramco EU/UK Privacy group with internal and external council and computer emergency response teams. Chris has practical and strategic hands-on experience in several cyber warfare incidents; USAF Space Command, detecting and helping to halt the July 2009 Second Wave attacks from the DPKR against South Korea and helping to recover and reestablish international business operations after the world's most devastating cyber warfare attack, Shamoon in 2012. Expert advisor and panelist for several governments and parliaments. Author of several books, offensive security trainer, digital security course creator, recognized expert in several digital security fields including IT/IOT/ICS SCADA space, maritime, aviation, oil & gas, electric, water and nuclear.

Ram Shankar Siva Kumar

Reduce, Reuse and Recycle ML models—and the security powers is yours

Ground Truth, Wednesday, 14:00–14:55

Ram Shankar is a Data Cowboy in Azure Security Data Science at Microsoft, working on the intersection of Machine Learning and Cyber Security. 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.

Nick Landers

Scheming with Machines: Using ML to Support Offensive Teams

Ground Truth, Wednesday, 15:00–15:55

co-presenting

Nick Landers is the Technical Lead at Silent Break Security. His work involves security consulting, red team operations, malware development, and offensive research. He has authored and presented the "Dark Side Ops" course series for over 3 years at BlackHat and other conferences. Internally, he develops tooling, evasions, and strategies for offensive operations.

Lavi Lazarovitz

Prisoner Number Six

Common Ground, Wednesday, 11:00–11:55

co-presenting

Lavi leads a group of security researchers called Group Charlie which is focused on security research of emerging technologies. Lavi and his group are doing vulnerability research; writing about information security for security magazines and blogs in Israel and internationally; and coding prototypes and proof of concepts. Lavi holds a master's in computer science and cryptography and a CISSP which is always nice to have. Prior to his work at CyberArk, he served in the Israeli Air Force for 11 years as a pilot and as an intelligence officer.

Katie Ledoux

Escape the Questionnaire Quagmire: A thoughtful approach to addressing security inquiries from customers and prospects

Common Ground, Wednesday, 14:00–14:25

Katie Ledoux the Manager of Trust and Security Governance at Rapid7 in Boston, Massachusetts. Her team is responsible for security risk management, security compliance, security awareness training, security policy development and exception management, business continuity plan and IR plan development and testing, and access recertification. She has also contributed to projects in data privacy and responsible vulnerability disclosure. You can find her on Twitter @kledoux.

Nimrod Levy

Hidden Networks Pivoting: Redefining DNS Rebinding Attack

Ground Floor, Wednesday, 11:00–11:55

co-presenting

Nimrod Levy is a seasoned security researcher with over a decade of experience in the field of web application penetration testing and infrastructure attack simulations (i.e. Red Team). Nimrod is the CTO and Co-founder at Scorpiones, a cyber security company which, among rest, illustrate potential attack vectors routes for its clients and recommending how to mitigate them. Nimrod enjoys giving back to the community, therefore the security tools he wrote in his free time are available through open-source projects.

Peter Lidell

Duck and (Re)Cover—The missing link in the security evolution

Underground, Tuesday, 11:30–12:25

Peter is an accomplished information security and risk management professional that for the past 20+ years has excelled in both the information security domain and the business domain. He has worked as an information security and risk management business leader in a variety of industries among others Maritime, Oil and Gas, Banking, Insurance and Food and Beverage. Peter is an expert practitioner of the discipline of collaboration across an organization to achieve desired goals. He has defined and executed (IT) information security and risk management strategies in some of the biggest and most complex global organizations and has always done so through the optics of the business strategy and with an inclusive holistic business approach.

Rachael Lininger

MENTOR to James Dietle

Building the badge—How you can make small, cheap and custom hardware for function or fashion

Proving Ground, Tuesday, 18:30–18:55

Information security analyst, risk consultant, Cthulhu cultist. Lawful good. Opinions belong to my autocorrect, not my employer. I have mentored three years in a row—ask me anything! Please read the biographies and abstracts of our wonderful speakers.

Bob Lord

Keynote, Tuesday, 10:00–10:55

Bob Lord is the Chief Security Officer at the Democratic National Committee, bringing more than twenty years of experience in the information security space to the Committee, state parties, and campaigns. Previously he was Yahoo's CISO, covering areas such as risk management, product security, security software development, e-crimes, and APT programs. Before that he acted as the CISO in Residence at Rapid 7, and before that headed up Twitter's information security program as its first security hire. You can see some of his hobbies at https://www.ilord.com.

Steve Luczynski

I Just Want to Help Make Flying More Secure...not Work with the Government or How I Learned to Love a Govvie

I Am The Cavalry, Tuesday, 18:00–18:55

Steve Luczynski retired from the Air Force in 2017 after a 25-year career flying F-15s & F-22s. He transitioned to cyber policy as the Deputy Director for Cyber Plans & Operations, Office of the Secretary of Defense at the Pentagon. Steve worked closely with National Security Council staff, other government agencies, the Joint Staff, and US Cyber Command on efforts to counter foreign threats and protect U.S. interests. He created and led Department-wide initiatives to ensure compliance with Presidential directives that enabled military cyberspace operations. Steve played a key leadership role in the Department's increased support for US government efforts to address aviation cybersecurity challenges. Steve is currently the Chief Information Security Officer for T-Rex Solutions, LLC where he oversees the protection of corporate and customer data across all lines of business and is responsible for directing information security risk management, compliance, policies, and standards.

Sean Lyngaas

Why journalists and hackers need each other (a panel discussion with infosec reporters)

I Am The Cavalry, Wednesday, 15:00–15:55

Sean Lyngaas has been writing about security issues as a journalist for several years. He is currently senior reporter at CyberScoop, where he focuses on the security of industrial control systems, medical devices, and other machines of modern society. He likes to talk to as many hackers as possible. Sean's reporting career outside of infosec has seen him cover military mutinies and presidential elections in West Africa, asylum seekers in the United States, and democracy activists in the Persian Gulf.

Sanne Maasakkers

Analyzing user decision making on phishing sites—using mouse data and keyboard dynamics

Proving Ground, Tuesday, 14:30–14:55

MENTOR: Chris Eng

Sanne Maasakkers works as a Cyber Security Expert / Ethical Hacker at Fox-IT. In her current role, Sanne mainly deals with performing internal penetration tests, web app penetration tests, code reviews and social engineering. Next to this she stands 'for a more secure society', for example during awareness trainings, hack demos and guest lectures (also for kids!).

Jeff Man

MENTOR to Vanessa Frost

Examining DES-based Cipher Suite Support within the TLS Ecosystem

Proving Ground, Tuesday, 12:00–21:25

Respected Information Security expert, advisor, evangelist, co-host on Paul's Security Weekly, and recently returned to a Consulting/Advisory role at Online Business Systems. Over 35 years of experience working in all aspects of computer, network, and information security, including risk management, vulnerability analysis, compliance assessment, forensic analysis and penetration testing. Previously held security research, management and product development roles with the National Security Agency, the DoD and private-sector enterprises and was part of the first penetration testing "red team" at NSA. For the past twenty years, has been a pen tester, security architect, consultant, QSA, and PCI SME, providing consulting and advisory services to many of the nation's best known companies.

Jim Manico

Tournament: The Ultimate Secure Coding Throw Down

Training Ground, Wednesday, 08:00–11:55

co-presenting

Jim Manico is the founder of Manicode Security where he trains software developers on secure coding and security engineering. He is also an investor/advisor for KSOC, Nucleus Security, Signal Sciences, Secure Cicle and BitDiscovery. Jim is a frequent speaker on secure software practices, is a member of the Java Champion community, and is the author of "Iron-Clad Java: Building Secure Web Applications" from Oracle Press. Jim also volunteers for the OWASP foundation as the project co-lead for the OWASP Application Security Verification Standard and the OWASP Proactive Controls. For more information, see http://www.linkedin.com/in/jmanico.

Alexander Manners

Hands-on: How to Use CALDERA's Chain Mode

Training Ground, Tuesday, 14:00–17:55

co-presenting

Alexander Manners is a Lead Cyber Security Engineer at The MITRE Corporation and a Cyber Warfare Operations Officer in the United States Air Force (USAF) Reserve. He is a member of MITRE's Adversary Emulation and Security Orchestration team where he researches and develops red team and blue team automation solutions. Prior to MITRE, Alex separated from the USAF after four years as a Cyber Warfare Officer and went to work at BIT Systems (A CACI Subsidiary) in their Cyber Capabilities and Development Division filling a variety of different roles. His operational experience and technical background provides a solid footing for developing new, relevant cyber technologies.

Richard Manning

Certification and Labeling in IoT

I Am The Cavalry, Wednesday, 12:00–12:25

Certification and Labeling for IoT

Public Ground, Wednesday, 14:00–15:55

With over 20 years in IT security and associated subjects, Richard has held both offensive and defensive roles encompassing operational, research and strategic tasks. Richard has worked for a range of government and industry organisations in highly trusted positions and currently holds a senior technical role in the UK's National Cyber Security Centre, supporting the UK economy and its citizens.

Darren Mar-Elia

Exploiting Windows Group Policy for Reconnaissance and Attack

Ground1234!, Wednesday, 15:00–15:55

A 14-year Cloud and Datacenter Microsoft MVP, Darren has a wealth of experience in Identity and Access Management and was the CTO and founder of SDM software, a provider of Microsoft systems management solutions. Prior to launching SDM, Darren held senior infrastructure architecture roles in Fortune 500 companies and was also the CTO of Quest Software. As a Microsoft MVP, Darren has contributed to numerous publications on Windows networks, Active Directory and Group Policy, and was a Contributing Editor for Windows IT Pro Magazine for 20 years. As a thought leader, Darren has over 20K subscribers to his blog (gpoguy.com) and an extremely active twitter following @grouppolicyguy.

Joey Maresca

Hacking from Above: A Brief Guide for Transitioning to Leadership

Hire Ground, Wednesday, 11:30–11:55

Joey Maresca is the Director of Security at Data Machines and has over 13 years experience in information security with a background that covers certification & accreditation, encryption compliance, and red-team offensive security testing. This experience has covered a variety of business sectors including commercial technology companies, government, healthcare, and financial sectors. Joey is a lifelong hacker who enjoys finding security problems, discovering solutions to fix them, and sharing his knowledge while hosting the Hackers with Bourbon weekly video stream.

Brian Markham

Musings of an Accidental CISO

Ground Floor, Wednesday, 18:00–18:55

Brian manages an incredible team of security professionals at the George Washington University. He attended college at University of Maryland and has been working in information security for over 16 years. When not reviewing resumes or contracts, he's explaining vulnerabilities in plain English, valiantly fighting off vendors, and trying (failing) desperately to get to inbox zero.

Andrea Matwyshyn

Professionalization—Possibilities and Potholes

Public Ground, Tuesday, 09:00–09:55

Andrea Matwyshyn is a professor in the law school and engineering school at Penn State, the Associate Dean of Innovation at Penn State Law (University Park), and the founding director of the Penn State PILOT Lab (Policy Innovation Lab of Tomorrow), an interdisciplinary technology policy lab. In 2014, she served as the Senior Policy Advisor/ Academic in Residence at the U.S. Federal Trade Commission.

Andre McGregor

Free and Fair Elections in an Internet Era

Public Ground, Wednesday, 09:00–09:55

co-presenting

Andre was Head of IT Security at Tanium, a cybersecurity software company, where he was responsible for security operations, engineering, incident response, and governance/risk/compliance of Tanium systems and networks worldwide. Most notably, Andre served as an FBI Cyber Special Agent in New York City, before being promoted to Supervisory Special Agent at FBI Headquarters in Washington DC. Before entering the FBI Academy at Quantico in 2009, Andre earned his degree from Brown University, and started his career at Goldman Sachs and Cardinal Health. He is on the Board of Directors for the National Cybersecurity Center and on the CFTC's Technology Advisory Committee. In his free time, Andre is the technical consultant for the NBCUniversal TV show Mr. Robot.

India McKinney

Ask the EFF

Underground, Tuesday, 18:00–18:55

co-presenting

Prior to joining EFF, India spent over 10 years in Washington, DC as a legislative staffer to three members of Congress from California. Her work there primarily focused on the appropriations process, specifically analyzing and funding programs in the Departments of Veterans Affairs, Homeland Security, and Justice. Her biggest legislative accomplishment was authorizing, funding and then naming a new outpatient VA/DoD clinic that will serve over 80,000 people. India's passion has always been for good public policy, and she's excited to be using skills developed during legislative battles to fight for consumer privacy and for robust surveillance oversight.

Patrick McNeil

MENTOR to Nick Koch

Human honeypots, or: How I learned to stop worrying and love the NFC Implant

Proving Ground, Wednesday, 10:30–10:55

Patrick is a Principal Solutions Architect, developing application security programs with Veracode's largest customers, successfully integrating security testing into their software development lifecycles. From his diverse background in defense, banking, telecom, carrier VoIP, product security, and DDoS mitigation, Patrick understands the challenges and intersections of software development, networking, operations, and management. Patrick is a hacker and #telephreak at heart, passionate about teaching and mentoring. He has shared his knowledge at a number of conferences, including DEF CON, DerbyCon, BSidesLV, CarolinaCon, ISSA and DevOps conferences, regional OWASP meetings, and various telecom industry and fraud prevention educational meetings such as CFCA. Patrick enjoys growing his local security community by serving as a board member of BSidesRDU and by organizing Oak City Locksport.

Chloé Messdaghi

Mind the Diversity Gap—A Panel Discussion

Common Ground, Tuesday, 17:00–17:55

co-presenting

Chloé Messdaghi is Security Researcher Advocate, board member for 4 nonprofits, one of the Women in Security (WoSEC) founders & heads SF Chapter, founder of WomenHackerz online community, mentors women to enter infosec and remain, speaker on diversity and inclusion, bug bounty, and safe harbor in InfoSec, and Drop Labels founder. https://www.chloemessdaghi.com Twitter: @ChloeMessdaghi

Roger Meyer

State of DNS Rebinding—Attack & Prevention Techniques and the Singularity of Origin

Breaking Ground, Wednesday, 18:00–18:55

co-presenting

Roger Meyer is a Principal Security Engineer at NCC Group with extensive experience in managing and leading complex engagements. Roger specializes in web application security, network penetration testing, configuration reviews, and secure software development and architecture design. Roger has conducted over a hundred security audits, penetration tests, source code reviews, and architecture reviews over the last 6 years at NCC Group.

Alyssa Miller

Mind the Diversity Gap—A Panel Discussion

Common Ground, Tuesday, 17:00–17:55

Alyssa is a hacker, blue-teamer, experienced speaker and security evangelist with over 15 years of experience in the security industry. She is the Manager of the Information Security Solutions Practice for CDW, working with customers to deliver security assessment and strategic advisory services. Alyssa is also the head of the WoSEC Milwaukee chapter and an advocate for developing truly inclusive culture as an avenue for promoting sustainable diversity within organizations and the information security community.

Oleksandr Mirosh

SSO Wars: The Token Menace

Ground1234!, Tuesday, 11:30–12:25

co-presenting

Oleksandr Mirosh has over 11 years of computer security experience, including vulnerability research, penetration testing, reverse engineering, fuzzing, developing exploits and consulting. He is working for Fortify Software Security Research team in Micro Focus investigating and analyzing new threats, vulnerabilities, security weaknesses, new techniques of exploiting security issues and development vulnerability detection, protection and remediation rules. In the past, he has performed a wide variety of security assessments, including design and code reviews, threat modelling, testing and fuzzing in order to identify and remove any existing or potentially emerging security defects in the software of various customers.

Omri Misgav

Meltdown's Aftermath: Leveraging KVA Shadow To Bypass Security Protections

Breaking Ground, Tuesday, 17:00–17:55

Omri has a decade of experience in the security field leading the R&D of large-scale defensive security solutions, performing incident response and conducting low-level research. Nowadays, as the security research team leader at enSilo he digs into OS internals and exploits, reverse engineer malware and develops new offensive and defensive techniques. Omri is a past speaker in BSidesLV.

Chrissy Morgan

Breaking the Bodyguards

Proving Ground, Wednesday, 14:30–14:55

MENTOR: Nick Rosario

Chrissy heads up the IT Security Operations for a Close Protection company by day and is a Security Researcher by night. Being an ex-Bodyguard herself, she brings this unique perception into the community and currently undertakes security research to help protect her the guys on the front-line. She is actively involved within the information security community across a wealth of subjects including the rights for researchers within vulnerability disclosure. As a recent masters graduate, she has accomplished the following successes so far: Winner of Cyber Security Challenge UK (University Challenge—Team Edinburgh Napier), Finalist for Pragyan CTF, A BlackHat Challenge Coin winner for OSINT from Social Engineer.org and Black Hat Scholarship, the Steelcon Award, a WISP Sponsorship, she was the BSides London Rookie Track Winner for 2018 and lastly finalist for (ISC)^2 up and coming information security professional for 2019.

Colin Morgan

Meet the Nation This Week on Sunday: A Special Vulnerability Edition

Common Ground, Wednesday, 18:00–18:55

co-presenting

Nicholas Mosier

ROP with a 2nd Stack, or This Exploit is a Recursive Fibonacci Sequence Generator

Breaking Ground, Wednesday, 15:00–15:55

Nick is an undergraduate at Middlebury College and a computer science major focusing in computer systems. He first became interested in computer security after the disclosure of the Spectre and Meltdown hardware vulnerabilities last year. He has an interest in assembly programming and compilers, and ROPC is a natural combination of these two.

Alvaro Muñoz

SSO Wars: The Token Menace

Ground1234!, Tuesday, 11:30–12:25

Alvaro Muñoz (@pwntester) is Principal Security Researcher at Micro Focus Fortify where he researches new software vulnerabilities and implement systems to detect them. His research focuses on web application frameworks where he looks for vulnerabilities or unsafe uses of APIs. Before joining the research team, he worked as an Application Security Consultant helping enterprises to deploy application security programs. Muñoz has presented at many Security conferences including BlackHat, DEF CON, RSA, OWASP AppSec US & EU, JavaOne, etc. and holds several infosec certifications, including OSCP, GWAPT and CISSP. He plays CTFs with Spanish int3pids team and blogs at http://www.pwntester.com.

Mike Murray

The Importance of Culture in Security

Hire Ground, Wednesday, 10:30–11:25

For over two decades, Mike has focused on building highly performing organizations that solve important and challenging problems in security. Most recently, he was the Chief Security Officer at Lookout, where he ran teams that discovered major threat actors in the mobile space and the protection of Lookout's customer base of over 150M mobile users. He previously lead Product Development Security at GE Healthcare, where he built a global team to secure the Healthcare Internet of Things. Prior to that, he co-founded The Hacker Academy and MAD Security, and has held leadership positions at companies including nCircle Network Security, Liberty Mutual Insurance and Neohapsis.

Manuel Nader

Breaking Smart [Bank] Statement

Ground1234!, Wednesday, 10:00–10:55

Manuel Nader is a Security Researcher at Trustwave Spiderlabs. He works on tracking new vulnerabilities, identifying how those vulnerabilities are exploited and writing code that detects the presence of or exploits those vulnerabilities. Previously worked in the offensive side of security and before that he worked on the defensive side of security. Manuel's favorite independent research involve web attacks.

Lily Hay Newman

Why journalists and hackers need each other (a panel discussion with infosec reporters)

I Am The Cavalry, Wednesday, 15:00–15:55

co-presenting

Lily Hay Newman is a staff writer at WIRED Magazine focused on information security, digital privacy, and hacking. She previously worked as a technology reporter at Slate magazine and was the staff writer for Future Tense, a publication and project of Slate, the New America Foundation, and Arizona State University. Additionally her work has appeared in Gizmodo, Fast Company, IEEE Spectrum, and Popular Mechanics. She lives in New York City.

Priyank Nigam

Reverse Engineering Mobile Apps: Never Pay for Transit Again

Underground, Tuesday, 14:00–14:55

As a senior security engineer, Priyank's primary areas of focus are mobile application penetration testing and secure source code reviews. Over the past 4 years, he has advised Fortune 500 brands and startups and does mobile and IoT related research in his spare time. He also believes it is unwise to place trust in your smartphones.

Joe O'Connell

The struggles of teaching automation

Proving Ground, Wednesday, 11:00–11:25

MENTOR: Ming Chow

I'm a security analyst at Rally Health on their secops team and I am very focused on teaching others. I've been working in security for 2 years and over the those 2 years I've realized that automation is a must in security ops and I've created a format to teach the rest of my teammates. Keeping them motivated as well as challenged are things I want to talk about.

Brendan O'Connor

MENTOR to Will Baggett

Broken Arrow: applying InfoSec and Forensic practices to escape domestic abuse

Proving Ground, Tuesday, 15:00–15:25

Described by coworkers as "not the lawyer we need, but the lawyer we deserve" (and he's pretty sure that wasn't meant as a compliment), Brendan O'Connor does in-house security for a company, and occasionally works as a security researcher, consultant, and/or attorney based in Seattle. His day job is building security programs, but at night, he transforms into a person who spends too much time arguing with people who are wrong on the Internet. If caught, any sane company will deny all knowledge of this presentation. At Hacker Summer Camp, he runs https://narwhal.be.

Ronnie Obenhaus

Cyber Threat Intel & APTs 101

Ground Floor, Wednesday, 17:00–17:55

co-presenting

Ronnie Obenhaus is a cybersecurity professional with over 20 years of experience in varying fields. He served with the United States Army and solidified his background in Network Defense and brings that background knowledge to the forefront of his job with the Defense Cyber Crime Center (DC3) as the Deputy Chief of Analytics. He loves movies and comic books. Do not ask him about the latter unless you are prepared for a lengthy conversation about the state of the industry today.

Colin OBrien

Grapl—A Graph Platform for Detection and Response

Ground Truth, Tuesday, 15:00–15:55

Colin began his career at Rapid7, working to take research from the data science team, build production quality services, and integrate them into the InsightIDR platform. Eventually, after working on IDR's detection team to build attacker signatures for its customers, Colin started working at Dropbox. Since working on the Detection and Response Team at Dropbox Colin has had the chance to dive deep into D&R work, learning to engage with the red team, and take on challenges that D&R teams face.

Kurt Opsahl

Ask the EFF

Underground, Tuesday, 18:00–18:55

Why can't we be friends? (Ask a Fed & the EFF.)

Ground1234!, Wednesday, 17:00–17:55

co-presenting

Kurt Opsahl is the Deputy Executive Director and General Counsel of the Electronic Frontier Foundation. In addition to representing clients on civil liberties, free speech and privacy law, Opsahl counsels on EFF projects and initiatives. Opsahl is the lead attorney on the Coders' Rights Project, and is representing several companies who are challenging National Security Letters. Before joining EFF, Opsahl worked at Perkins Coie, where he represented technology clients with respect to intellectual property, privacy, defamation, and other online liability matters.

John Orleans

DLP Sucks and Why You Should Use It

Common Ground, Tuesday, 11:30–12:25

When he's not busy crashing bikes or sampling tiki drinks, John runs the threat modelling, application security, data retention, and privacy regulations functions for Mesirow Financial, an independent financial services firm in Chicago, IL. He has over 20 years' experience breaking systems and getting them fixed before the next workday. He is a CISSP and proud owner of several lapsed certifications.

Davi Ottenheimer

AIs Wide Open—Making Bots Safer Than Completely $#%cking Unsafe

I Am The Cavalry, Tuesday, 14:30–14:55

AIs Wide Open—Making Bots Safer Than Completely #$%cking Unsafe

Public Ground, Tuesday, 16:00–17:55

flyingpenguins, Cyberwar History, Threat Intel, Hunt, Active Defense, Cyber Letters of Marque, Cloudy Virtualization Container Security, Adversarial Machine Learning, Data Integrity and Ethics in Machine Learning (Formerly Known as Realities of Securing Big Data). Davi works at MongoDB and is author of the book, "The Realities of Securing Big Data" (Wiley 2019).

Suchi Pahi

Cover Your A**

Proving Ground, Wednesday, 15:00–15:55

MENTOR: Clint Gibler

Suchi is a data privacy and cybersecurity lawyer (@SuchiPahi). She was supposed to be a doctor, but went rogue and wound up in law school arguing about the CFAA. After 4 years of working on some of the most incredible incidents as a cybersecurity lawyer and of helping companies of all sizes set up privacy and security practices, she decided to leave the law firm life so that she could do more tech law things. She currently lives in DC, where she is Director of Privacy and Business Affairs at Rally Health, Inc.

Robert Paul

Enterprise Overflow: How Breached Credentials Impact Us All

Ground1234!, Tuesday, 15:00–15:55

Robert Paul is the Director of Research & Development for NuID, an authentication and cyber security company. At NuID, Robert studies the identity landscape from a security perspective and looks to uncover real-world threats in authentication and other identity technologies. Robert is a seasoned white hat hacker and red-teamer, with experience on the security teams at Microsoft, Ericsson, and McAfee. Before NuID, he most recently held a position at Microsoft working on the cryptographic libraries for Azure. Robert is CISSP and OSCP certified.

Will Pearce

Scheming with Machines: Using ML to Support Offensive Teams

Ground Truth, Wednesday, 15:00–15:55

Will Pearce is Senior Security Consultant/ Researcher at Silent Break Security. His work involves security consulting, red team operations, and offensive research. He has presented

"Dark Side Ops" course series for blackhat and other groups. His research is focused primarily on malware development, windows techniques, and exploring the intersection of machine learning and offensive operations.

David Pearson

Knowing the Unknown: Using PCAP to Break Down Application-Layer Protocols

Training Ground, Tuesday, 08:00-11:55

Having used Wireshark ever since it was Ethereal, David has been analyzing network traffic for well over a decade. He has spent the majority of his professional career understanding how networks and applications work, currently as Principal Threat Researcher for Awake Security, which enables rapid, iterative, conclusive investigations & threat hunting by placing context at security teams' fingertips. David holds computer security degrees from the Rochester Institute of Technology (BS) and Carnegie Mellon University (MS).

Katherine Pratt

Reverse Engineering the Cyber Policy API

Public Ground, Tuesday, 10:00-11:55

co-presenting

Dr Katherine Pratt received her B.S. in aerospace engineering from MIT in 2008, and her PhD in Electrical and Computer Engineering (ECE) from the University of Washington (UW) in 2019. During undergrad she completed several internships with the private space venture Blue Origin, working in systems and propulsion engineering. She has served four years in the United States Air Force, working primarily as an operational flight test engineer on the F-35 Joint Strike Fighter. Her doctoral dissertation focused on the privacy, ethics, and policy of information derived from elicited neural signals. She was the recipient of a NSF Graduate Research Fellowship and the 2018-19 UW ECE Irene Peden Endowed Fellowship. During graduate school she interned with the ACLU of Washington through the Speech, Privacy, and Technology Project. She also completed a six month fellowship as the first Congressional Innovation Scholar through Tech Congress where she crafted technology policy and legislation.

Gregory Price

Virtual Breakpoints for x86_64

Breaking Ground, Wednesday, 14:00-14:55

With nearly 20 years of experience in the cyber-security industry, Guy held various positions in both corporates and start-ups

Matteo Rebeschini

Finding Evil with Mitre ATT&CK and the Elastic Stack

Training Ground, Wednesday, 14:00-17:55

Matteo Rebeschini is a Principal Solutions Architect and Security Specialist at Elastic, where he works with customers on architecting real-time security analytics solutions using the Elastic Stack. Matteo has 18+ years of experience in the cybersecurity industry covering various roles, from software engineering to technical product management and more recently consulting and solutions architecture.

Vanessa Redman

The drunk colonel and the flipped stone: Game Theory for a Defensive Strategic Advantage

Proving Ground, Wednesday, 12:00-12:25

MENTOR: Allan Friedman

Vanessa Redman has been fully immersed in the Cybersecurity industry for the last 4 years, but has been involved with computers since getting a Commodore Vic-20 in the late 1980s. She currently teaches Cyber Operations fundamentals. Vanessa has also worked for a certified Red Team, and as such, is always playing the Devil's Advocate and looking for assumptions to disprove. She is also studying Algorithmic Game Theory for use in Cyber Threat Intelligence and Attack Detection.

Joshua Reynolds

From EK to DEK: An Analysis of Modern Document Exploit Kits

Breaking Ground, Wednesday, 11:00-11:55

https://meliorsec.com

Michael Rich

Loki: Add a little chaos to your USB drive

Breaking Ground, Wednesday, 10:00-10:55

Kris Rides, Tiro Security

Behind the Recruiting Curtain: What Do Recruiters Really Say and Do [SPONSORED]

Hire Ground, Tuesday, 17:30-17:55

co-presenting

Chris Roberts

Now that you hacked the plane, what are you going to do about your career?

Hire Ground, Tuesday, 11:30-11:55

Roberts has led or been involved in information security assessments and engagements for the better part of 20 years, and has a wealth of experience with regulations such as GLBA, HIPAA, HITECH, FISMA, and NERC/FERC. He has also worked with government, state and federal authorities on standards such as CMS, ISO, and NIST. And worst case, to jog the memory, Chris was the researcher who gained global attention in 2015 for demonstrating the linkage between various aviation systems, both on the ground and while in the air that allowed the exploitation of attacks against flight control system. Most importantly, Chris has shared several commentaries on career development and job search in our community. He will share his thoughts on what participants need to take full advantage of while at BSidesLV for their career development.

Pedro Rodriguez

The Contemplator Approach: Data Enrichment Through Elastic Stack

Common Ground, Tuesday, 15:00-15:55

co-presenting

Graduated from the Costa Rican Institute of Technology with a BS in Computer Science in 2017. Started working as an intern in National Instruments, getting a full-time position later as a Information Security Analyst. Currently in charge of managing the logs throughout the Elastic Stack platform, incident response and also testing new tools related to security, he is currently pursuing a certification as a Cloud Security specialist and architect.

Nick Rosario

MENTOR to Chrissy Morgan

Breaking the Bodyguards

Proving Ground, Wednesday, 14:30-14:55

Nick "MasterChen" Rosario started as an amateur phone phreak and branched out into VoIP Security, Surveillance, Social Engineering, and Data Analytics. He has been speaking at BSidesLV and DEF CON since 2014. He is currently the secretary of SYNShop, the Las Vegas Valley Hackerspace, where he hosts a weekly Information Security podcast called GreyNoise.

Yolan Romailler

Have You Distributed Randomness?

Common Ground, Wednesday, 15:00–15:55

Yolan is a security researcher at Kudelski Security delving into (and dwelling on) cryptography, crypto coding, blockchains technologies and other fun things. He has spoken at Black Hat USA, BSidesLV, NorthSec, Cryptovillage and DEF CON, on topics including cryptography, public keys vulnerabilities, or vulnerability research, and presented at FDTC the first known practical fault attack against the EdDSA signature scheme. Yolan tweets as @anomalroil.

Mathieu Saulnier

The SOC Counter ATT&CK

Proving Ground, Wednesday, 11:30–11:55

MENTOR: Ethan Gregory Dodge

Mathieu Saulnier is a "Security Enthusiast" @h3xstream. He has held numerous positions as a consultant within several of Quebec's largest institutions. For the last 6 years he has been focused on putting in place a few SOC and has specialized in detection (Blue Team), content creation and mentorship. He currently holds the title of "Senior Security Architect" and acts as "Adversary Detection Team Lead" and "Threat Hunting Team Lead" for Bell Canada, one of Canada's largest carriers. In the last decade, he has taken two separate sabbaticals to travel Africa and Asia.

Ben D Sawyer

Neurosecurity: where Infosec meets Brain-machine Interface

Breaking Ground, Tuesday, 18:00–18:55

Ben D. Sawyer is an applied neuroscientist and human factors engineer known for using brainwaves, eye movements, and mathematical theory to build better human-machine teams. His models and algorithms power trustworthy machines that work with their human partners. His design recommendations are leveraged by Fortune 500 companies. His work has been covered by Forbes, Reuters, Fast Company, and The BBC. With the US Air Force, he studied the mathematical underpinnings of attention in cyberdefense. At MIT his work focused upon designing superior connections between humans and machines. At UCF, where he is Faculty in Industrial Engineering and Director of LabX, he works to optimize, or disrupt, these connections.

Ty Sbano

Startup Security Leadership: Lessons to Level Up from Fortune 100 to Tech Startup

Hire Ground, Wednesday, 14:00–14:25

Ty Sbano is an Information Security leader with over 13 years of experience, mainly in Financial Technology organizations. Currently, Ty is the Cloud Chief Information Security Officer at Sisense, who acquired Periscope Data in May 2019. Ty's career has been focused on developing application and product security programs for Capital One, JPMorgan Chase, LendingClub, and Target. Key areas of knowledge include developing security champions, threat modeling, secure code training, static code analysis, component analysis, dynamic analysis, penetration testing and red teaming. Ty's security mentality has been concentrated on enabling engineering and product teams to securely move at the speed of the business to make it a competitive advantage. Ty graduated from Penn State University with a B.S. in Information Science & Technology and from Norwich University with a M.S. in Information Assurance. He currently holds a CISSP, CEH, CCSK and CPT. To learn more, please visit—tysbano.com

Mike Sconzo

All that glitters isn't Chrome: Hunting for suspicious browser extensions

Ground Truth, Wednesday, 17:30–17:55

Mike Sconzo has been around the Security Industry for quite some time, and is interested in creating and implementing new methods of detecting unknown and suspicious network activity as well as different approaches for file/malware analysis. This includes looking for protocol anomalies, patterns of network traffic, and various forms of static and dynamic file analysis. He works on reversing malware, tool creation for analysis, and threat intelligence. Currently a lot of his time is spent doing data exploration and tinkering with statistical analysis and machine learning to solve detection and threat intelligence related problems.

David Seidman

Noobs: Training the Next Generation of Security Engineers

Hire Ground, Wednesday, 13:30–13:55

David (they/them) joined Google's Detection & Response team in Kirkland 3 years ago as a Security Engineering Manager. They manage several teams related to detection in Google Cloud, as well as the ATC team that is the subject of this presentation. Prior to Google they led the Microsoft security incident response team in responding to incidents such as Heartbleed and Stuxnet. They are a Quora Top Writer on topics such as security, management, and the tech industry. In their free time, they enjoy playing with their kids, hiking, climbing, camping, sailing, chess, and homebrewing beer. Quora profile: https://www.quora.com/profile/David-Seidman

John Seymour

Reducing Inactionable Alerts via Policy Layer

Ground Truth, Tuesday, 18:00–18:25

MENTOR to Anna Skelton

Deepfakes, Deep Trouble: Addressing Potential Market Manipulation Caused by Deepfakes

Proving Ground, Wednesday, 17:00–17:25

John is a Senior Data Scientist on the Detection and Response team at Salesforce, which focuses on aggregating all security logs at Salesforce, applying rules and models to obtain high fidelity alerts, and sharing those results with other pertinent Security teams. In particular, John performs machine learning on security logs to alert to new attacks, to improve our existing alerts and rules, and to find/make new contextual data to help in investigations. He previously performed data science at a startup focused on social media security. He has presented at several security cons, including Black Hat, DEF CON, and SecTor.

Shay Shavit

At Your Service—Abusing the Service Workers Web API

Breaking Ground, Wednesday, 17:00–17:55

co-presenting

Shay is a Senior Security Researcher on Akamai's Threat Research Team where he focuses on bot detection and web application attacks research for Akamai's cloud security solutions all together. In addition to working with Akamai, Shay is active in many bug bounty programs and is part of the Bugcrowd Researcher Council.

Tyler Shields

MENTOR to Abdessamad Temmar

Securing Fast (and Furious) DevOps pipelines

Proving Ground, Wednesday, 18:00–18:25

I've spoken at most major conferences over the last decade or more. This includes RSA, Blackhat, RSA EU, Blackhat EU, InfoSec EU, AppSecUSA, and many others. I spoke at well over 20 events in one year as an analyst at Forrester research covering the mobile, application, and IoT security markets. I have also spoken on topics including rootkit detection, antidebugging techniques, and other advanced RCE technologies. I speak business as well as geek and can easily translate between the two.

Nathan Shepard

Ask the EFF

Underground, Tuesday, 18:00–18:55

co-presenting

As EFF's Grassroots Advocacy Organizer, Nash works directly with community members and organizations to take advantage of the full range of tools provided by access to tech, while engaging in empowering action toward the maintenance of digital privacy and information security.

Erica Schneider, Valimail

Behind the Recruiting Curtain: What Do Recruiters Really Say and Do [SPONSORED]

Hire Ground, Tuesday, 17:30–17:55

co-presenting

Toru Shimanaka

**Cyber Deception after Detection:
Safe observation environment using
Software Defined Networking**

Proving Ground, Wednesday, 15:30–15:55

MENTOR: Claus Houmann

Toru Shimanaka is a Security Researcher at Fujitsu System Integration Laboratories. Toru has over 20 years of experience developing workstations, routers and network switches as a software engineer. His interests over the past five years are cyber range and cyber deception. Toru has gave presentation in HICSS-52 and BSides Sendai in the past.

Sibusiso Sishi

**An investigation of the security of
passwords derived from African languages**

Ground1234!, Wednesday, 11:00–11:55

Sibusiso is a former professional athlete that has represented his country at the highest sporting level, the Olympic games. After retiring from the athletics he transitioned into cyber security and has been doing penetration testing for the past five years. Sibusiso co-founded a majority black owned cyber security company called Ironsky Pty Ltd in South Africa where he serves as a technical director and penetration tester. Sibusiso has always had an interest for passwords and how users create and use passwords within the organisation.

Anna Skelton

**Deepfakes, Deep Trouble: Addressing
Potential Market Manipulation
Caused by Deepfakes**

Proving Ground, Wednesday, 17:00–17:25

MENTOR: John Seymour

Hailing from a town where the wifi infrastructure hasn't been upgraded since 2004, I got my collegiate footing in global security but have since fallen victim to the slippery slope of information security. Now I spend my days using the tools of vendors whose parties I went to at my first DefCon in 2017 (hint: less champagne). I'm hoping to expand my InfoSec horizons and please my research-loving brain by partnering with a mentor to present on a topic I'm incredibly passionate about—China.

Serenity Smile

**The Resilient Hacker: Growth Mindset,
Health Hacks & Powerful Help to
Navigate Personal Challenges**

Proving Ground, Tuesday, 17:30–17:55

MENTOR: Nathaniel Davis

Serenity Smile is a SANS Diversity Cybertalent Immersion Academy Graduate. She holds the GIAC GSEC (GIAC Security Essentials), GIAC GCIH (GIAC Certified Incident Handler), and GIAC GCIA (GIAC Certified Intrusion Analyst) Certifications. Additionally, she's earned five different yoga and meditation teaching certifications and is a health and wellness consultant. She also co-directs Women Who Code in her city and is an avid cybersecurity researcher, chair of an Arboretum Board, a Coursera Beta-Tester, and an avid lifelong learner.

Arnaud Soullie

Pentesting ICS 102

Training Ground, Wednesday, 14:00–17:55

co-presenting

Arnaud Soullie is a manager at Wavestone, performing security audits and leading R&D projects. He has a specific interest in Active Directory security as well as ICS, two subjects that tend to collide nowadays. He teaches ICS security and pentests workshops at security conferences (BlackHat Europe 2014, BSides Las Vegas 2015/2016, Brucon 2015/2017, DEFCON 24, DEFCON 26) as well as full trainings (Hack In Paris 2015 and 2018, BlackHat Asia 2019).

Nimrod Stoler

Prisoner Number Six

Common Ground, Wednesday, 11:00–11:55

Nimrod Stoler is a cybersecurity researcher at CyberArk Labs where he focuses on researching the latest attack techniques and applying lessons learned to improve cyber defenses. Nimrod's primary research areas are network defense, DevOps analysis and security and Linux containers. Prior to CyberArk, Nimrod served in several high-technology roles doing research and development of software and hardware. Nimrod holds an LLB in law and BA in economics.

Maddie Stone

MENTOR to Alon Weinberg

Please inject me, a x64 code injection

Proving Ground, Wednesday, 18:30–18:55

Maddie Stone (@maddiestone) is a Senior Security Engineer on the Android Security team at Google where she reverses all the bytes to keep malware off the phones of Android users. She has spent many years deep in the circuitry and firmware of embedded devices including 8051, ARM, C166, MIPS, PowerPC, BlackFin, the many flavors of Renesas, and more. Maddie has previously spoken at conferences including Blackhat USA, REcon Montreal, OffensiveCon, KasperskySAS and more.

John Stoner

Cyber Threat Intel & APTs 101

Ground Floor, Wednesday, 17:00–17:55

Mr. Stoner has over 18 years of experience in the national security sector working a variety of roles, including most recently as a Cyber Threat Analyst, Cyber Counterintelligence Analyst and Instructor. His work experience includes IT, instruction and course design, cyber exercise and testing, intelligence collection, threat support, SIGINT (Signals Intelligence), and Cyber Operations. He holds A+, Net+, CEH, CHFI, CEI, CISD, CASP and CISSP certifications. He loves soccer and is an avid coach and fan. He is currently the Chief of Analytics, in DCISE at DC3.

Lakshmi Sudheer

Who dis? The Right Way To Authenticate

Ground1234!, Wednesday, 14:00–14:55

Lakshmi Sudheer is a Security Researcher at Adobe. She holds a Master of Science in Information Security and has been in the security industry for about four years now. At Adobe, she works on reviewing architectures and providing security guidelines to various product teams. Prior to Adobe, she was at a startup doing all things Application Security and has experience with security consulting at Bishop Fox. She has also spoken about her open source projects at security conferences like RSA 2018, Appsec USA & AppSec Cali.

Eli Sugarman

Why we need a Cyber Peace Institute

Public Ground, Wednesday, 16:00–17:55

Eli Sugarman is a Program Officer at the William and Flora Hewlett Foundation. He manages the Cyber Initiative, a ten-year, $130 million grant-making effort that aims to build a more robust cybersecurity field and improve policy-making. Previously, he was a consultant and strategist to private sector and nonprofit leaders. He has served as a foreign affairs officer at the U.S. Department of State, where he focused on international security issues. A San Diego native and graduate of Middlebury College, he holds a J.D. from Stanford University Law School.

Luke Szczutowski

Getting CVSS, NVD, and CVEs to Work for You: Standardizing and Scaling Your Vulnerability Risk Analysis

Common Ground, Wednesday, 14:30–14:55

co-presenting

Luke is an Offensive Security Certified Professional and a professionally trained digital forensic analyst regularly involved in local and national cybersecurity events, including competing yearly at DEF CON. Luke currently works as a Security Analyst on the Azure team at Microsoft, applying his passion for offensive security to provide expert-level risk analysis. He has previously led penetration tests as a part of 3PAO engagements for clients pursuing FedRAMP accreditation, and he has extensive experience driving vulnerability management in hyperscale cloud environments and scoring risks using CVSS.

Abdessamad Temmar

Securing Fast (and Furious) DevOps pipelines

Proving Ground, Wednesday, 18:00–18:25

MENTOR: Tyler Shields

Abdessamad Temmar is an information security consultant and App Sec Engineer. He worked through a variety of sources to provide security professional services to clients. Abdessamad is also a member of the OWASP Proactive controls Project, where he contributes in the update of his Top-Ten document, and also a co-author of the Mobile Security Testing guide.

SJ Terp

Applying Information Security Paradigms to Misinformation Campaigns: A Multidisciplinary Approach

Ground Truth, Tuesday, 11:30–12:25

co-presenting

Sara-Jayne "SJ" Terp is a data scientist, strategist, old-school AI researcher and community builder who focuses on complex business and social problems. She's currently working on the Global Disinformation Index (an independent disinformation rating system), and running a Credibility Coalition working group on the application of information security principles to misinformation; her previous work covers belief systems and situation awareness across many disciplines (including autonomous systems,intelligence analysis, crisis data, journalism, online advertising and political data science).

Pete Thurston

Salesforce Data Governance What dark secrets lurk in your instance??

Proving Ground, Tuesday, 14:00–14:25

MENTOR: Wendy Knox Everette

Pete has spent over 15 years at the intersection of Business and Technology. Understanding the complexities of enterprise business as well as the intricacies of running a small company is something he prides himself in. He has worn many hats (often at the same time) throughout his career including Data Analyst, Product Owner, Business Analyst, Software Engineer, Team Leader, QA Engineer and probably several others he's forgotten. Out of all of this, he's discovered his passion is really in identifying simple and effective applications of technology to the problems all businesses face. This has driven his leadership of the technology team at RevCult since day one and has proven to be enjoyable, sustainable and productive for the company.

David Tomaschik

CTFs for Fun and Profit: Playing Games to Build your Skills

Ground Floor, Wednesday, 10:00–10:55

David (@Matir) is a Red Team engineer for a major internet company and a security researcher focusing on IoT and embedded devices. When not working on these things, he likes to build CTFs for BSidesSF and BSidesLV, and occasionally still finds time to play in a CTF. He also sometimes builds electronic things just for fun.

Jen Tong

Why FIDO Security Keys & WebAuthn are Awesome

Ground1234!, Tuesday, 18:00–18:55

Jen is a Security Advocate on Google Cloud. In this role she helps software developers and IT professionals stay out of trouble while getting the most out of cloud computing. Previously she worked in a wide variety of engineering roles from robotics at NASA, to developer advocacy for Google Glass. She is passionate about education, especially on the subjects of technology and science. If she's away from her laptop, she's probably playing ice hockey, or running a D&D game.

Alexandrine Torrents

Pentesting ICS 102

Training Ground, Wednesday, 14:00–17:55

Alexandrine Torrents is a cybersecurity consultant at Wavestone, a French consulting company. She is specialized in penetration testing, and performed several security assessment on ICS. She worked on a few ICS models to demonstrate attacks on PLCs and she developed a particular tool to request Siemens PLCs. Moreover, she is also working at securing ICS, in the scope of the French military law, enforcing companies offering a vital service to the nation to comply to security rules.

Katie Trimble

What's Next in Coordinating Vulnerability Disclosures

Public Ground, Tuesday, 14:00–15:55

Kathleen "Katie" Trimble currently serves as the Section Chief of the Vulnerability Management and Coordination section of the Cyber Threat & Risk Analysis (CTRA) branch of the NCCIC of DHS, where she leads the Department's primary operations arm for coordination of the responsible disclosure and mitigation of identified cyber vulnerabilities in control systems and enterprise hardware and software used in the 16 critical infrastructure sectors and all levels of U.S. government organizations.

Previous to this position, within the Department, she served as the Senior Communications Infrastructure Sector Analyst in the Office of Cyber and Infrastructure Analysis (OCIA), in this capacity, she operated as the focal point for efforts related to wired and wireless communications between interagency government partners, DHS components, and Private Industry stakeholders in response to National Security Council requirements.

Pavel Tsakalidis

BEEMKA / Electron Post-Exploitation When The Land Is Dry

Breaking Ground, Tuesday, 11:30–12:25

Maurice Turner

Reverse Engineering the Cyber Policy API

Public Ground, Tuesday, 10:00–11:55

Free and Fair Elections in an Internet Era

Public Ground, Wednesday, 09:00–09:55

Maurice Turner is Senior Technologist at the Center for Democracy & Technology, a Washington, DC-based non-profit advocacy organization dedicated to ensuring the internet remains open, innovative and free. Supporting work across all of CDT's programmatic areas, Turner focuses on the Election Security and Privacy Project identifying and updating election cybersecurity practices and infrastructure, and working through potential remedies. Turner brings a unique mix of formal education and practical work experience in technology and local, regional, and national policymaking to the Internet Architecture team. After receiving a bachelor's in political science from Cal State Fullerton, he went on to earn a master's in public administration from the University of Southern California focusing on emerging communication technologies, privacy, and civic engagement. In addition, he holds a graduate certificate in cybersecurity strategy from Georgetown University, and has nearly a decade of municipal management experience complemented by numerous private-sector technology positions, fellowships, and internships.

Martin Vigo

From email address to phone number

Breaking Ground, Wednesday, 12:00–12:25

Martin Vigo is a red teamer and researcher with a background in product security and software engineering. He previously focused on Mobile security, Identity and Authentication, helping keep "the cloud" secure. Since then, he has shifted to pure offensive security work, putting on the black hat to catch the bad guys. Martin is also involved in educating developers on security essentials and best practices. Martin has presented several topics including accounts takeover by voicemail cracking, breaking password managers, exploiting Apple's Facetime to create a spy program and mobile app development best practices. These were given at conferences such as DEF CON, Blackhat EU, Ekoparty, BSides Las Vegas, Kaspersky Security Analyst Summit and Shakacon. Outside the office, Martin enjoys research, bug bounties, gin tonics and scuba diving.

Mitch Wasson

(Im)proper Database Authentication

Ground1234!, Wednesday, 12:00–12:25

Mitch Wasson is currently working as a software engineer on Cisco's Advanced Malware Protection (AMP) for Endpoints data engineering team. Aside from merging bugs into master, he creates detection platforms and middleware that support millions of endpoints. Mitch also holds a master's degree in computer engineering from the University of Toronto. Outside of tech, he enjoys most winter sports—like skiing in the Canadian Rockies.

Roy Wattanasin

How to Fail Well (In Order to be Successful)—From IT to Infosec & More

Hire Ground, Tuesday, 17:00–17:25

Roy Wattanasin @wr0 is a healthcare information security professional and a faculty member of over 10+ years. He has experience in many industries and spends most of his time developing information security programs, teaching students and helping to build the local communities. Roy is also a member of multiple advisory groups including OWASP Boston etc. He was an adjunct instructor at Brandeis University as part of the Health and Medical Informatics and Information Security Master's degree programs. He is also co-founder of the Health & Medical Informatics program and credited for bringing back Security BSides Boston many years ago.

Alon Weinberg

Please inject me, a x64 code injection

Proving Ground, Wednesday, 18:30–18:55

MENTOR: Maddie Stone

Alon Weinberg is a security researcher at Deep Instinct. Before Alon joined Deep Instinct two years ago, he served in the IDF for 4.5 years in an elite cyber unit as a security researcher. As part of his role in Deep Instinct, Alon is in charge of finding new ways to enhance protection and defense mechanisms. Alon leverages his cyber-offense experience and OS internals knowledge to conduct malware analysis and RE, explore attack surfaces in Windows and macOS, and research existing or new attack vectors and evasion techniques. Alon is addicted to cross-fit and enjoys riding his motorcycle during his free time.

Bill Weiss

MENTOR to Kenny Jansson

Making your website vulnerable for fun and security awareness

Proving Ground, Wednesday, 10:00–10:25

Currently a pointy-haired boss to hackers, Bill came up in fantastic (despite his presence) red and blue teams working for the .gov, moved into DevOps in the financial services industry, and spent a minute working for a large automation tooling vendor herding sysops and then starting their product security group. He loves organizing community events like BSides and DevOpsDays, as well as attending them. Give him a great cup of coffee and a team interested in doing great work and he'll be happy.

Veronica Weiss

Is This Magikarp a Gyarados?: Using Machine Learning for Phishing Detection

Ground Truth, Wednesday, 11:00–11:55

Veronica Weiss is currently a security analyst in the financial industry. She is a data science researcher in her personal time, and is very passionate about gradient boosting algorithms and has recently been focusing on cloud security. Veronica is also an undergraduate college student studying Computer Science and Statistics at Skidmore College, and can be found playing Capture the Flag (CTF) competitions with RPISEC.

Justin Whitehead

Hacking the STORM

Training Ground, Wednesday, 08:00–17:55

Justin sits at the intersection of hacker and maker. His passion for knowing how things work as lead him into research of IoT devices, Drones, and RFID. Justin has worked on many Raspberry Pi projects including two Debian based distros; Vap0r, and RedSkyz for which he was the main contributor. He has spoken and taught at a multitude of security conferences and enjoys sharing his knowledge and learning from others around him.

Justin also has experience in external and internal penetration testing across a wide range of sectors (e.g. government, healthcare, financial, aerospace, automotive). He is the Founder and CEO of Digital Silence.

Jamie Williams

ATT&CKing Your Adversaries—Operationalizing cyber intelligence in your own environment for better sleep and a safer tomorrow.

Ground Floor, Wednesday, 15:00–15:55

Jamie Williams is a Cyber Adversarial Engineer for The MITRE Corporation where he works on various efforts involving security operations and research. He is also a member of both the MITRE ATT&CKing and ATT&CK Evaluations teams. Before joining MITRE, Jamie received his M.S. in Information Systems Engineering from Johns Hopkins University and his B.S. in Information Systems from the University of Maryland, Baltimore County (UMBC).

Elizabeth Wilson

Satellite Vulnerabilities 101

Proving Ground, Tuesday, 19:00–19:25

MENTOR: Philip Young

Elizabeth is currently wrapping up her International Master in Intelligence, Security, and Strategic Studies with a concentration in Security & Technology—a degree jointly awarded by the University of Glasgow in Scotland, Dublin City University in Ireland, and Charles University in the Czech Republic. Her thesis concentrates on the intersection of Artificial Intelligence and Human Security. She is a recipient of the fully funded Erasmus Mundus scholarship for her studies. Before that, she was a self-taught software developer after her undergraduate studies in International Business with a concentration in Russian language and culture. In her free time, Elizabeth is a hobby photographer, training aerialist, musician, and gamer.

Beau Woods

I Am The Cavalry Track Welcome and Overview (co-presenting)

I Am The Cavalry, Tuesday, 11:30–11:55

Saving Lives Through Security Research

I Am The Cavalry, Wednesday, 18:30–18:55

Beau Woods is a Cyber Safety Innovation Fellow with the Atlantic Council, a leader with the I Am The Cavalry grassroots initiative, and Founder/CEO of Stratigos Security. His work bridges the gap between the security research and public policy communities, to ensure connected technology that can impact life and safety is worthy of our trust. He formerly served as Entrepreneur in Residence with the US FDA, and Managing Principal Consultant at Dell SecureWorks. Over the past several years in this capacity, he has consulted with the energy, healthcare, automotive, aviation, rail, and IoT industries, as well as cyber security researchers, US and international policy makers, and the White House. Beau is a published author, frequent public speaker, often quoted in media, and is often engaged for public or private speaking venues.

Michael Wylie

Using Wireshark for Incident Response and Threat Hunting

Training Ground, Wednesday, 08:00–17:55

Michael Wylie, MBA, CISSP is the Director of Cybersecurity Services at Richey May Technology Solutions. In his role, Michael is responsible for delivering information assurance by means of vulnerability assessments, cloud security, penetration tests, risk management, and training. Michael has developed and taught numerous courses for the U.S. Department of Defense, Moorpark College, California State Universities, and clients around the country. Michael holds the following credentials: CISSP, CCNA R&S, CCNA CyberOps, GPEN, TPN, CEH, CEI, VCP-DCV, CHPA, PenTest+, Security+, Project+, and more. Michael is responsible for identifying four zero-day vulnerabilities in major tax software in 2018. Twitter: @TheMikeWylie

Udi Yavo

Meltdown's Aftermath: Leveraging KVA Shadow To Bypass Security Protections

Breaking Ground, Tuesday, 17:00–17:55

co-presenting

Udi Yavo has more than 15 years of experience in cyber-security with a proven track record in leading cutting edge cyber-security R&D projects. Prior to enSilo, Udi spearheaded the direction of the cyber-security unit at the National Electronic Warfare Research & Simulation Center of Rafael Advanced Defense System and served as its CTO. Additionally, he developed and led Rafael's cyber training programs. Udi's achievements at Rafael have been recognized, winning him excellence and innovation awards on complex security projects. Prior to Rafael, Udi served as a system architect at the IDF. He holds a BA in Computer Science from the Open University. Udi is a past speaker in Blackhat, RSA conference and BSidesLV.

Sarah Yoder

ATT&CKing Your Adversaries—Operationalizing cyber intelligence in your own environment for better sleep and a safer tomorrow.

Ground Floor, Wednesday, 15:00–15:55

co-presenting

Sarah Yoder is a Cyber Security Engineer for the MITRE Corporation. She enjoys furthering her red team skills and applying cyber threat intelligence to ATT&CKing. Prior to joining MITRE, Sarah worked as an Exploit Analyst with the Department of Defense. Sarah received her M.P.A. in Public Administration and B.S. in Cybersecurity from California State University, San Bernardino (CSUSB).

Nir Yosha

My quest for (privileged) identity to own your domain

Ground1234!, Tuesday, 14:00–14:55

Nir started his career as a squad leader in the Israeli Intelligence Corps. He helped with gathering intelligence tracking the growth of terrorist organizations. Nir has over 15 years of experience in identity management, user behavior and insider threat analysis. Currently, Nir is a Principal Solutions Engineer for Preempt. Nir publishes his posts on LinkedIn and speaks occasionally at security conferences.

Philip Young

MENTOR to Elizabeth Wilson

Satellite Vulnerabilities 101

Proving Ground, Tuesday, 19:00–19:25

Soldier of FORTRAN is a mainframe hacker with over 20 years in the infosec space. He's spoken at Shmoocon, DEFCON, Skytalks, RSA, BlackHat, Thotcon, BSidesLV (since 2013). He's keynoted SHARE (twice) and MSITAC. He also teaches a mainframe hacking class at Derbycon as well as workshops at BSidesLV. His current job puts him in charge of pentesting odd areas like mainframes, datalakes, telephony systems. On top of this he's contributed to projects like the mainframe enumeration project, nmap and metasploit. He got his first speaking opportunity being a mentee at BSidesLV in 2013 and now returns the favor by being a mentor ever since.

Sarah Young

Addressing non-linear InfoSec career paths

Hire Ground, Tuesday, 12:00–12:25

Sarah is a security professional and has worked in tech for about a decade now, but she had a not-so standard start into the IT industry, and eventually found her way into security. In this talk, Sarah shares how—as a contrary teenager—she definitely didn't do what everyone will tell you to do career-wise but still managed to build a successful security career, and how we need to embrace individuals with non-linear careers to address the skills shortage in cyber.

Tomer Zait

Hidden Networks Pivoting: Redefining DNS Rebinding Attack

Ground Floor, Wednesday, 11:00–11:55

Tomer Zait (Principal Security Researcher at F5Networks) worked in a range of professions in the security industry (Web Application Firewall Integrator, Penetration Tester, Application Security Engineer, Security Researcher, Etc.). During this time, he developed open-source projects (most of them are security tools). His projects include: x64dbgpy; PyMultitor (Presented In BlackHat Arsenal ASIA/US/EU 2017); SubDomain-Analyzer; AutoBrowser; phantom-requests, and more. Tomer writes regularly for online security magazines and is a 4-time winner of the Israeli Cyber Challenge (CTF).

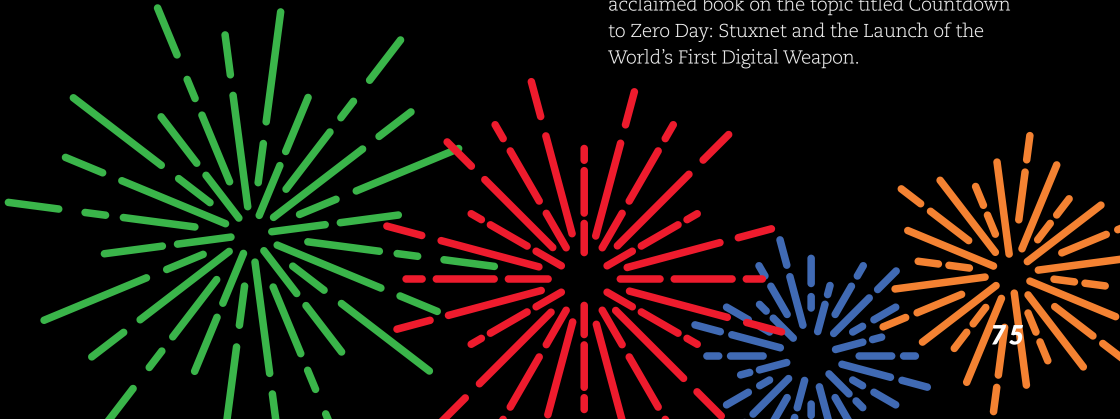
Kim Zetter

Why journalists and hackers need each other (a panel discussion with infosec reporters)

I Am The Cavalry, Wednesday, 15:00–15:55

co-presenting

Kim Zetter is an award-winning investigative journalist and book author who covers security, cybercrime, digital warfare, surveillance and civil liberties. She has been covering computer security and the hacking underground since 1999, first for PC World magazine, and more recently for WIRED, where she began writing in 2003. In 2004, long before fears of Russia hacking US presidential elections became an issue, she wrote a series of award-winning investigative pieces about the security problems with electronic voting machines and their susceptibility to hacking. She was among the first journalists to cover Stuxnet, and in 2014, Crown/Random House published her widely acclaimed book on the topic titled Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.



BSides Las Vegas Staff

Presenting BSides Las Vegas to you requires the love and dedication of a year-round staff. The people listed here have some of the biggest hearts, brightest minds, and best laughs in all of InfoSec (and beyond)! We are a family, and we thoroughly enjoy the work we do to present BSides Las Vegas to you each year. We're proud of this team.

General Officers

Kelly "nous" Gardner, Chief Operations Officer / Executive Producer (@nousie)
Rob Carson, Chief Security Officer (@robcarson05)
Steve Ragan, Chief Media Officer (@SteveD3)

Board of Directors

Iftach Ian Amit, President (@iiamit)
Cindy Jones, Vice President (@SinderzNAshes)
Jack Daniel, Treasurer, Assistant Secretary (@jack_daniel)
Justin Tibbs, Secretary (@JMP_EBP)
Dave Lewis, General Director (@gattaca)
Jessica Archer, General Director (@j3ssa)
Russ Rogers, General Director (@v3rtig0)
Charles Nwatu, General Director (@charles_nwatu)

A special thanks to the 250 volunteers who help us before, during, and after the show. Without your support, we'd be nowhere.

Staff

Assistants to the COO: @hushedfeet and @magen_wu

Assistant to the Executive Producer: @leanrum

CFP Program Directors: @daemontamer and @mortman

Breaking Ground Directors: @mainframed767 and @daemontamer

Common Ground Directors: @allanfriedman and @mortman

Proving Ground Directors: @guy_mcdudefella and @sa3nder

Ground Truth Directors: @gdbassett and @urbansec

Ground1234! Directors: @jmgosney and @baybedoll_doll

Underground Directors: @daemontamer and @mortman

I Am The Cavalry Directors: @beauwoods and @joshcorman

Hire Ground Director: @yesitskathleen

Public Ground Directors: @beauwoods and @infosecjen

A/V: @sciaticnerd and @jnitterauer

Contests and Events: @randominterrupt, @jackassplus, and @knarphie

Lockpick Village: @thesweetkat and @wendyck

Pros vs. Joes CTF: @dichotomy1

Silent Auction & Raffle: @wintr and @Xanadu2600

OSINT CTF: @tracelabs

Hacker Summer Camp Hacker Stand-up Comedy: @joshjaycomedy, @dakacki, and @5urv1va7rix

Design: @1dark0ne

InfoBooth: @telecon and @rossja

Las Vegas Logistics: @fuzzy_l0gic

NOC: @jack_daniel, @lickitysplitted, and @securethisnow

Photographer: @ladymerlin

Press Operations: @steved3 and @ladyerisian

Quartermasters: @esp_09, @VanillaGranilla, @aj7o2, and @x_mycroft_x

Registration: @sinderznashes, @momiekins09, and @surferdave_sec

Room Hosts Coordinators: @ngree_h0bit and @mrglass

Safety Operations: Rob Carson, Brad Stine, @tkrabec, and @edwardprevost

Speaker Operations: @coolacid and @nickinfosec

Sponsor Coordinators: @J_ai_Ho and @storm_of_ethics

T-Shirts: @TessSchrodinger

Training Operations: @RaynManMD

Volunteer Operations: @paulby, and @mr0x20wednesday

Webmasters and Social Media: @MisterGlass and @fl3uryz

CFP Committee Members: @beajammingh, @buffaloparks, @davbatz, @sirspamsalot, @__muscles, @seric, @wendynather, @spacerog, John Liu, @fsmontenegro, @lil_lost, @JMP_EBP, Sarah Connor, Thing One, @falcondarkstar, @ussjoin, @clintgibler, @straithe, and @pink_tangent

BSides Las Vegas 2020 Announcements

Thanks for helping us celebrate our 10th anniversary of BSidesLV!

We hope to see you again next year. Here are a few dates of note:

The 2020 Sponsor Prospectus will be released on **October 25, 2019**	Donor Drive will open on **April 1, 2020** and run until it's sold out—No Foolin'!	BSides Las Vegas 2020 will be held **July 28–29, 2020**
The General Call for Papers will open on **March 1, 2020** and close on **April 15, 2020**	**SAVE THESE DATES**	Acceptance and rejection letters for General CFP go out on **May 13, 2020**
Proving Ground Call for Mentors will open on **January 1, 2020** and close on **February 29, 2020**	Proving Ground Call for Papers will open on **February 1, 2020** and close on **February 29, 2020**	All this information and more will be updated at **bsideslv.org**

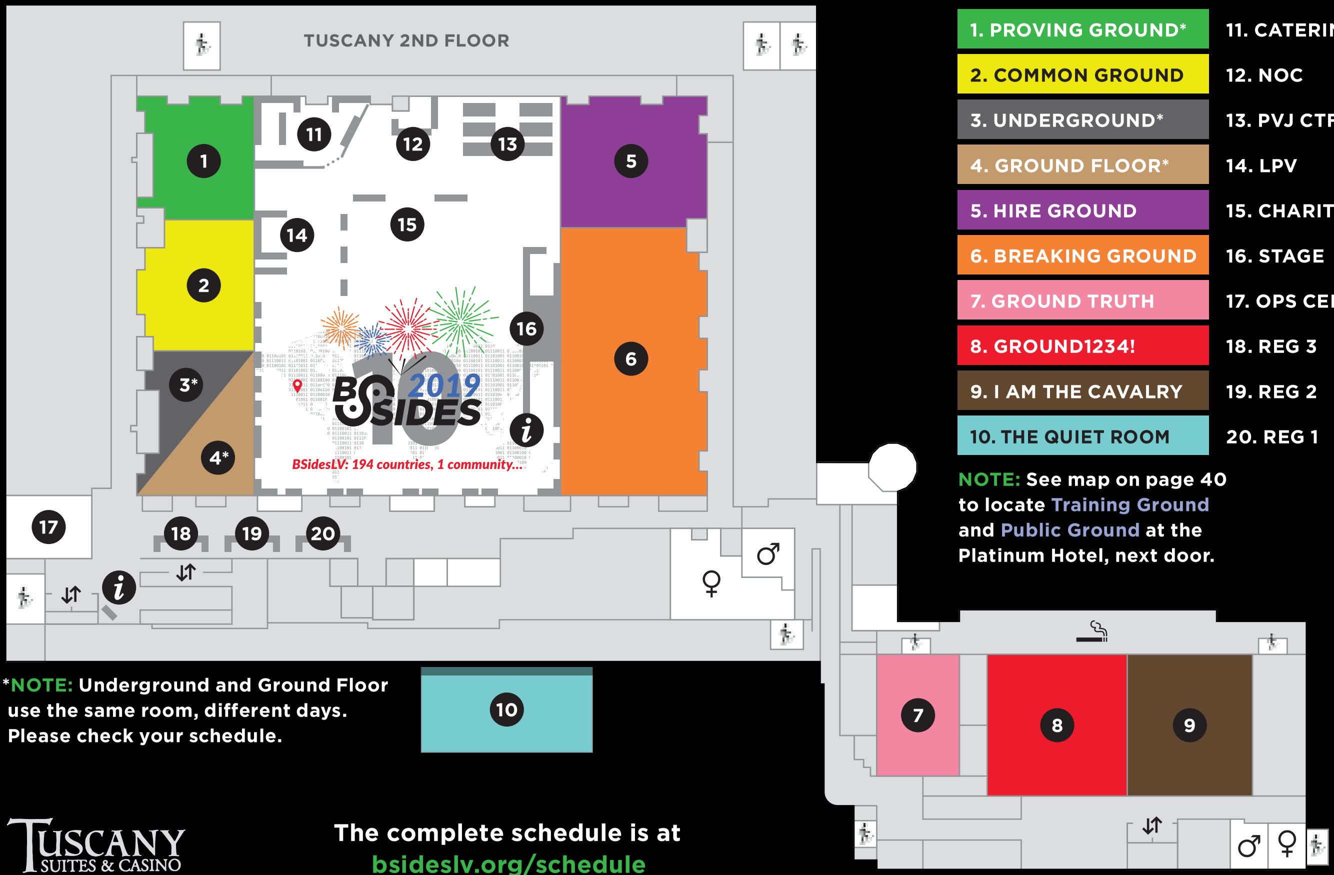
PLAN AHEAD FOR NEXT YEAR. You must register in advance to get a badge. There will be NO on-site registration or walk-ins. FAQ: bsideslv.org/registration-faq

Follow us on Twitter 🐦 **@bsideslv**

Thank Our Sponsors

Because of our sponsors, BSides Las Vegas is able to provide a vendor-neutral, free as in beer, free as in speech event year after year.

Please take a moment to thank them for their support. You can find them at the sponsor tables in Middle Ground, in Hire Ground, and throughout the conference with Gold badges. Or give them a shout-out on social media with #BSidesLV #Sponsors.



1. PROVING GROUND*	11. CATERING
2. COMMON GROUND	12. NOC
3. UNDERGROUND*	13. PVJ CTF
4. GROUND FLOOR*	14. LPV
5. HIRE GROUND	15. CHARITIES
6. BREAKING GROUND	16. STAGE
7. GROUND TRUTH	17. OPS CENTER
8. GROUND1234!	18. REG 3
9. I AM THE CAVALRY	19. REG 2
10. THE QUIET ROOM	20. REG 1

NOTE: See map on page 40 to locate **Training Ground** and **Public Ground** at the Platinum Hotel, next door.

***NOTE:** Underground and Ground Floor use the same room, different days. Please check your schedule.

TUSCANY SUITES & CASINO

The complete schedule is at bsideslv.org/schedule

We regret to inform you that **DEF CON has been canceled**. Thank you for attending BSides Las Vegas.