Threat Hunting & Incident Response
SANS DFIR | Summit & Training
New Orleans, LA
SUMMIT: Sep 30 – Oct 1 TRAINING: Oct 2-7
LEARN MORE

Monday, September 30	
9:00-9:15 am	*Welcome & Opening Remarks* **Matt Bromiley @mbromileyDFIR, Summit Co-Chair, SANS Institute** **Phil Hagen @philhagen, Summit Co-Chair, SANS Institute**
9:15-10:00 am	*Keynote* **Play Like a Kid, Protect Like a Champion: A Reservist Model** **Chris Cochran, @chriscochran_io, Threat Intelligence & Operations Lead, Netflix** Research has shown that play is crucial to the development of skills for children. This concept also applies to Olympic-caliber athletes, high-functioning military units, and cutting-edge cybersecurity programs. What if there was a way to simultaneously inject play/training into your security program, execute advanced cybersecurity functions (threat hunting, red teaming, and threat intelligence),and identify and close gaps in visibility and security posture? This talk will explore the Netflix framework to accomplish these goals. Netflix strives to find high-leverage activities that solve multiple challenges. For example, Netflix uses a reservist model to supplement crisis management and incident response with great success. This year, Netflix implemented a similar model to establish a purple team – a matrixed team of reservists to support threat hunting, red teaming, and intelligence operations. This presentation will explore how Netflix executes hunting via the red and intelligence teams, lessons learned, and steps you can start implementing today. It’s time to play, have some fun, and develop championship-level security programs!
10:05-10:40 am	**Evolving the Hunt: A Case Study in Improving a Mature Hunt Program** **David J. Bianco, @davidjbianco, Principal Engineer - Cybersecurity, Target** **Cat Self @coolestcatiknow, Lead Information Security Engineer, Target** As a major U.S. retailer with a strong cybersecurity focus, Target has long had a functional, mature threat hunting program. When David Bianco took over responsibility for the hunting program in early 2019, leadership’s key question was “How can we do even better?” But what does “better” mean for a hunting

	program, and how do you get from where you are now to where you want to be? In this presentation, we'll talk about coming into an existing threat hunting program, prioritizing areas for improvement, and then implementing those improvements to make a great hunting program even better. Attendees will learn the key functions of a threat hunting program and how to evaluate the current hunting program maturity level, set an appropriate maturity improvement goal, identify and prioritize possible program changes to support the desired improvements, and understand how and why these efforts work (or don't work!).
10:40-11:20 am	**Networking Break**
11:20-11:55 am	**My "Aha!" Moment** **John Stoner @stonerpsu, Principal Security Strategist, Splunk** This presentation is designed as a personal journey through threat hunting to inspire others to embrace certain methods, tips, and lessons learned. When John Stoner joined this Splunk team in 2017, the team started working on the second version of what it called "Boss of the SOC" (BOTS). John will share his team's journey in threat hunting as it attempted to figure out where to start, at times found itself getting tangled in the data, and overcame distractions encountered during the hunting process. He'll cover how the team was able to conduct hunts, and he'll share some thoughts on gap analysis and operationalizing these findings. The presentation will also include some cautionary tales to help the threat hunting community assist security operations with operationalizing hunt data and not take all the great work that is out there and oversimplify it in such a way that it loses its impact. Attendees will come away with a better understanding of how to create a hunting hypothesis, build "guard rails" into your hunt to stay focused, and take hunting output and operationalize it. We'll also examine the importance of conducting gap analysis as part of the hunting activity to support the efforts of operations. Attendees will receive a data set and instructional application that they can take home and play with!
Noon-12:35 pm	**Well, What Had Happened Was…** **Todd Mesick @tmesick1, Lead Forensic Analyst, Precision CastParts** **Brian Moran @brianjmoran, Digital Strategy Consulting, BriMor Labs** This presentation will cover the details and lessons learned from a cybersecurity incident involving a nation-state adversary that occurred in 2013. The nation-state threat actor group was named in an October 2018 indictment, so it can finally be discussed in a public forum. We will also present additional information that was not seen in this specific incident, but was part of a strategic operation that was traced all the way back to 2010. It is not often that a presentation can include not only the entire digital life cycle of an attack, from

	first infection method to last-ditch attempted persistence, but also insider threats, physical security, and more!
12:35-1:40 pm	**Lunch & Learn Sessions**
1:45-2:20 pm	**Who's that CARBANA King at My Door? Hunting for Malicious Application Compatibility Shims** **Benjamin Wiley @benwiley, Associate Consultant, Mandiant** If an attacker clearly had backdoor access to a system, yet no malware can be found on disk and there is no sign of how the malware was loaded into memory, how would you even begin your forensic investigation? This was the obstacle Mandiant consultants faced while responding to an intrusion attributed to FIN7 in 2017. FIN7, a financially-motivated threat group, was able to stealthily use the CARBANAK backdoor as well as point-of-sale malware to steal thousands of payment card numbers. FIN7 remained undetected for months by using application compatibility shims to hide and execute its malware, a methodology that had rarely been seen prior to this intrusion. This presentation will recount that investigation from the perspective of the incident responders and share techniques for detecting and hunting malicious application compatibility shims in your own network. The number of threat actors using application shim persistence will likely continue to rise in the years ahead as network defenders become more effective at detecting traditional persistence mechanisms and more attackers are forced to take FIN7's lead. Raising industry awareness of this attacker methodology is critical before its use becomes prevalent. Attendees will come away with a technical understanding of how Microsoft uses shims to provide applications with backwards compatibility against the ever-changing Windows codebase, and how attackers have abused shim functionality to covertly execute malware and ways they will expand this abuse in the near future. Be prepared to come away locked and loaded, ready to hunt down malicious application compatibility shims that are likely already on your networks!
2:25-3:00 pm	**Threat Hunting in the Enterprise with Winlogbeat, Sysmon, and ELK** **David Bernal Michelena @d4v3c0d3r, Lead Security Researcher, Scitum** **Patricio Sánchez, Head of SCILabs, Scitum** While threat prevention is critical to reduce an organization's security risk, it is not enough. Blue teamers must assume that at some point a threat is going to evade defenses and get an initial foothold in the organization. So it is important to have the means to detect those attacks at an early stage to contain the threat and reduce its impact. Defenders also need to perform retrospective investigations and do enterprise-wide searches, analyzing information of multiples devices at once. This presentation will show how to enhance endpoint visibility by using free tools such as Sysmon, Winlogbeat, and ELK. By using

	ATT&CK as a reference model, blue teamers can create detections for several attack techniques based on the endpoint events. By targeting threat behavior, defenders can more effectively detect adversaries, even when they change their artifacts or infrastructure. Several examples will show how the system can be used to detect various attack techniques such as live-off-the-land attacks (attackers using tools available on the endpoints such as wmic, cscript, net, PowerShell, net scripts); fileless attacks through PowerShell scripts (detections for PowerShell Empire and Unicorn will be shown); lateral movement (PSEXEC, wmic); password spraying attacks (based on Windows' successful and failed logins visualization in Kibana); persistence creation via the Windows registry, new services, and other techniques; command and control callbacks; actions on objective, such as looking for passwords on the file system and Windows registry for lateral movement and privilege escalation, in addition to Kibana, elasticsearch, and ELK API; and known threats based on specific functions used in code (TTP), rather than file hash, IP address, or domain, which allows for better detection and is harder for attackers to evade. While the human analyst is focusing on detecting TTPs, ELK API allows analysts to automate the search for indicators of compromise such as IP addresses, domains, and hashes to programmatically detect known evil. We will also show how to integrate this solution with the MISP Threat Intelligence Platform through API for automatic detection of Indicators of Compromise.
3:05-3:40 pm	**Networking Break**
3:45-4:20 pm	**Once Upon a Time in the West: A Story on DNS Attacks** **Ruth Esmeralda Barbacil, Cyber Intelligence Analyst, Deloitte** **Valentina Palacin, Cyber Intelligence Analyst, Deloitte** Just like in movies about the Old West, we are going through a land riddled with well-known gunmen – OceanLotus, DNSpionage, and OilRig, among others – who roam at ease while the security cowboys sleep. This presentation will uncover the toolset and techniques used by these gunmen, taking a closer look at their big guns and behavioral patterns. We will explore the attacks involving DNS that took place during the last decade to examine the latest techniques discovered to improve detection and dodge the bullets the bad guys are firing in our direction.
4:25-5:00 pm	**BZAR – Hunting Adversary Behaviors with Zeek and ATT&CK** **Mark Fernandez, Lead Cybersecurity Engineer, The MITRE Corporation** **John Wunder @jwunder, Principal Cybersecurity Engineer, The MITRE Corporation**

	Lately, threat hunters have been obsessed with endpoint data, and for good reason. Endpoint sensing is great for finding behaviors that happen exclusively on a single host. It has traditionally been neglected, yet it is a critical part of any threat hunter's arsenal. At the same time, adversaries need to move around the internal network. Whether via SMB, RDP, or something other method, moving laterally is a critical part of most adversaries' attacks. Adversaries can also use mechanisms like RPC to execute code, evade defenses, and access credentials. This means that internal network monitoring can also be a valuable asset for a threat hunter. This presentation will first describe what adversaries do that is visible via internal network monitoring. This will be framed using the ATT&CK knowledge base: which techniques are always, usually, or sometimes visible in network traffic? As an example, Windows Admin Shares will almost always be visible in network traffic, while Scheduled Task creation might sometimes be visible when done in a certain way. The presentation will describe BZAR (Bro/Zeek ATT&CK-Based Analytics and Reporting), a set of Bro/Zeek scripts utilizing the Server Message Block (SMB), and Remote Procedure Call (RPC) protocol analyzers to detect post-exploit adversary behaviors. We'll focus not just on what BZAR can do, but also on how it works, how to deploy network sensors that can feed it, and lessons learned in building it out. We'll also examine another approach to BZAR-style analytics. Rather than doing analytics in Zeek directly, they can be implemented in a SIEM by sending the relevant Zeek logs to the SIEM and implementing analytics there. BZAR has the advantage of detecting events in real time with less ingest into the SIEM, and the SIEM has the advantage of being able to correlate events after the fact, across network and endpoint events, and across larger time frames.
6:00-8:00 pm	**Summit Night Out** Take a 10-minute walk to Barcadia (@barcadianola) for food, drinks, networking, and vintage arcade games. (Tron! Galaga! MS. PAC MAN!) Barcadia is located at 601 Tchoupitalas.

Tuesday, October 1	
9:00-9:05 am	*Day 2 Opening Remarks* **Matt Bromiley @mbromileyDFIR, Summit Co-Chair, SANS Institute** **Phil Hagen @philhagen, Summit Co-Chair, SANS Institute**
9:05-9:50 am	*Keynote* Classifying Evil: Lessons from Hunting Human Traffickers **Sherrie Caltagirone, Executive Director, Global Emancipation Network @GblEmancipation** Global Emancipation Network is the leading data analytics and intelligence nonprofit dedicated to countering all forms of human trafficking across the globe. We track children across the web and international borders. We monitor and reconstruct timelines of trafficker's online personas and real-world locational data. We develop and provide cutting-edge tools to counter-trafficking stakeholders to disrupt international criminal organizations. Join us as we explore the parallels between hunting human traffickers and cyber criminals from aggregating siloed data to adapting to changing adversary tradecraft to the latest efforts in image analysis and open source intelligence.
9:50-10:25 am	**Jupyter Notebooks and Pre-recorded Datasets for Threat Hunting** **Roberto Rodriguez @Cyb3rWard0g, Security Researcher** **Jose Luis Rodriguez, Security Researcher** How many times have you thought about a more efficient, intuitive, or creative way to analyze the security events your organization collects, but feel limited to the capabilities of a one language-dependent search bar with basic Boolean search capabilities? In addition, how much time do you usually spend preparing for the simulation of specific adversarial techniques? What if you could expedite the process to validate the detection of those techniques in a more efficient and affordable way? In this talk, we will introduce the concept of utilizing Jupyter Notebooks for a more dynamic, flexible, and language-agnostic way to analyze security events, and at the same time help your team document, standardize, and share detection playbooks. We will go over the architecture, deployment, and capabilities of Jupyter Notebooks and present a few use cases covering multiple techniques to analyze data while performing research. In addition, we will show how to use pre-recorded datasets from a new open-source project named Mordor to expedite simulation of adversarial techniques and validation of data analytics. The final part of the presentation will cover a methodology used to collect and consume pre-recorded security events in a controlled lab environment with specific security log auditing configurations that can also be used to identify gaps and provide recommendations for data collection strategies in production environments.

10:25-10:55 am	**Networking Break**
11:00-11:35 am	**Don’t Miss the Forest for the Trees: How to Translate Too Much Data from Too Many Intrusions into Strategic Hunting Value** **Karl Scheuerman, @KarlScheuerman, Senior Strategic Intrusion Analyst, CrowdStrike** **Piotr Wojtyla, Senior Researcher, CrowdStrike** The global pace of targeted intrusion activity is as rapid as ever, but improvements in monitoring, detection, and forensics technologies currently provide threat hunters with unprecedented visibility. How can we manage the seemingly exponential growth in the number of breaches and amount of relevant intrusion data even as we still have to develop a useful strategic threat picture over time? This talk will provide insights from an industry-leading threat hunting team on ways to approach this problem. Recommendations will include ways to effectively capture the most relevant takeaways from intrusions to help analysts create better hunting leads and build threat assessments with robust context. Armed with these foundations, threat hunters can better partner with their threat intelligence counterparts to harness tactical data when building strategic assessments of adversaries. The talk will also present unique strategic trends and threat hunting findings identified using these methods.
11:40 am-12:15 pm	**Open the Pod Bay Doors Please, HAL** **Gunter Ollmann @gollmann, Chief Security Officer, Microsoft** Modern threat hunting has focused on tooling that enables hunters to be more efficient in finding correlated events and bringing the relevant data to their fingertips. As data volumes have increased – with new logs, alerts, telemetry, and intelligence blossoming at rates that make Moore’s Law look quaint – machine learning and machine intelligence systems have taken over the bulk of the “business as usual” and anomaly hunts. At the same time, the first generation of cloud SIEM complete with automated threat hunting and incident response capabilities has only just been launched. Subsequent generations will evolve both rapidly and in a way that will force organizations into rethinking their hunting and response requirements. This session looks at where “cloud effects” will be leveraged by cloud SIEM, how automation will default to autonomous, why machine intelligence will visibly succeed, and how the role of the threat hunter will evolve over the next few years.
12:15-1:25 pm	**Networking Lunch & Vendor Expo**

1:30-2:05 pm	**Live Debates!** **Referee: Matt Bromiley @mbromileyDFIR, Summit Co-Chair, SANS Institute** Back by popular demand! This fast-paced, fun session pits friends and colleagues against one another in a (mostly) friendly competition with a twist: debaters don't know the topics – or whether they're pro or con – until they get on stage. Laugh along with them as they're put on the spot to defend their positions on a variety of hunting and IR topics.
2:10-2:45 pm	**Remote Access Tools: The Hidden Threats inside Your Network** **David Pearson @davidp0508, Head of Threat Research, Awake Security** Many remote access tools are used legitimately and not considered malware. However, these tools actively bypass network controls, obscuring which parties are communicating, when, and how. This ability to fly under the radar is attractive to malicious insiders and outside attackers alike. This presentation will discuss common techniques these tools use and how security teams can find and understand them.
2:50-3:25 pm	**Worm Charming: Harvesting Malware Lures for Fun and Profit** **Will MacArthur @Anti_Expl0it, Threat Research & Intelligence Lead, InQuest.net** Client-side attacks are a common source of compromise for many organizations. Web browser and e-mail-borne malware campaigns target users by way of phishing, social engineering, and exploitation. Office suites from vendors such as Adobe and Microsoft are ubiquitous and provide a rich and ever-changing attack surface. Poor user awareness and clever social engineering tactics frequently result in users consenting to the execution of malicious embedded logic such as macros, JavaScript, ActionScript, and Java applets. In this talk, we'll explore a mechanism for harvesting a variety of these malware lures for purposes of dissection and detection: worm charming (also known as grunting or fiddling). Worm charming is an increasingly rare real-world skill used to attract earthworms from the ground. A competitive sport in East Texas, it uses methods that involve vibration of the soil, which encourages the worms to surface. In our context, we'll apply a series of YARA rules to charm interesting samples to the surface from the nearly 1 million files uploaded to Virus Total daily. Once the samples are aggregated, we'll explore mechanisms for clustering and identifying "interesting" samples. Specifically, we're on the hunt for malware lures that can provide a heads-up to defenders on upcoming campaigns as adversaries frequently test their lures against anti-virus consensus.
3:25-3:45 pm	**Networking Break**
3:50-4:25 pm	**Hunting Is Sacred, But We Never Do It for Sport!**

	Ashraf M. Abdalhalim, Incident Response and Forensics, Senior Consultant, FireEye "Hunting is sacred, little brother. It's our right, but we never do it for sport!" Bagheera teaches Mowgli that jungle law during a hunt. Predators have to FIND preys and KILL in order to survive, and they do it instinctually. Threat Hunting and Incident Response (THIR) practitioners also have to do both effectively in order to survive. In cybersecurity, threat hunting (FIND) and incident response (KILL) practices are interrelated but at the same time distinct in nature. When a hunt sortie identifies a threat (prey) in the environment, it has to be followed by an effective incident response. Sounds straightforward, but the details and the overlooked seams between the two practices are underestimated and may lead to failure. Are the two THIR practices conducted by one team? Or two different teams? Internal or external? When do you switch from TH to IR? Does the first true positive come from the TH? How are the new injects from the TH cycle integrated into an already running IR cycle? How do you synchronize and integrate the two practices? We have good models and practices to run and manage THIR, but for the most part separately. We need to do more to seamlessly integrate the two practices and mend the seams between them. In this session we'll present examples when THIR has failed due to the overlooked seams between the two practices. Attendees will learn how to run the two practices seamlessly as one process – that is, stitch the seams between the two practices – as well as how the original Kill Chain (F2T2EA) model can be used to run an effective THIR.
4:30-5:05 pm	**There's an Actor in My Pocket!** **Jennifer Chavarria, Threat Hunting Analyst, Shell Oil** **Daniel Garcia, Threat Hunting Analyst, Shell Oil** Did you ever have the feeling there's a WASKET in your BASKET? Or an actor in your logs? Threat hunting is a human-driven approach to taking hunches like these and tracking them down to find threat actors lurking in your environment. A well-structured hunt includes inputs (for example, a hunch, internal incident learnings, threat intel), outcomes, and hypotheses to avoid going down rabbit holes when exploring large datasets. Join this session as we walk through multiple hunting examples with varying outcomes – from uncovering an incident to nothing – and share queries that you can use to hunt down bad guys in your own environment. We'll examine the tools and data sources used in threat hunting, including log aggregators (for example, SIEM) that create a playing ground for hunters to correlate events across data sources. And we'll also look at the rules or queries that are used to make sense of the data and help prove or disprove a hypothesis.
5:05-5:15 pm	*Wrap-Up* **Matt Bromiley @mbromileyDFIR,** Summit Co-Chair, SANS Institute **Phil Hagen @philhagen**, Summit Co-Chair, SANS Institute

Speaker Biographies

Ashraf M. Abdalhalim, Incident Response and Forensics, Senior Consultant, FireEye
Ashraf M Abdalhalim (a.k.a Tango) is incident response senior consultant. Tango has spent the past 5+ years on the frontlines of the cyber battle field, responding to security incidents that matter. Tango is always interested in researching ideas and concepts from other disciplines that could apply to cybersecurity and address its challenges.

Pedram Amini, @pedramamini, CTO, InQuest.net
Pedram is a security researcher, software developer, published author, serial entrepreneur, investor, advisor, and hacker of all things. His background is in reverse engineering and creative problem-solving skills He is the CTO of InQuest.net, a threat discovery and prevention company focused on mitigating malicious and unauthorized data-in-transit and data-at-rest. His specialties include reverse engineering, software engineering, management, public speaking, cloud architecture, and amazing ping pong and foosball skills. He is fluent in a variety of languages including Python, C, C++, x86-64 Assembly, PHP, Perl, Lisp, and SQL.

Ruth Esmeralda Barbacil, Cyber Intelligence Analyst, Deloitte
Ruth is an information systems engineering student from the Universidad Tecnológica Nacional (UTN). She has been working at Deloitte's Argentina Cyber Threat Intelligence area as the Threat Library Team Leader. She has gained experience related to Tactics, Techniques and Procedures (TTPs) investigation, Advanced Persistent Threats (APTs), Campaigns, Incidents and Tools to help mitigation and defense.

David J. Bianco **@davidjbianco,** Principal Engineer - Cybersecurity, Target
David has more than 20 years of experience in the information security field, with a particular focus on incident detection and response. He is active in the DFIR and Threat Hunting community, speaking and writing on the subjects of detection planning, threat intelligence, and threat hunting.

Sherrie Caltagirone, Executive Director, Global Emancipation Network @GblEmancipation
Sherrie Caltagirone is the founder and Executive Director of Global Emancipation Network (GEN), the leading data analytics and intelligence nonprofit dedicated to countering human trafficking. Prior to starting GEN, she served as a policy advisor for Orphan Secure, a global human trafficking rescue nonprofit, and began her anti-trafficking career with the Protection Project at the Johns Hopkins University. She currently serves as a Distinguished Research Scholar at North Carolina State University and is driven by research on the use of data analytics and mathematical models to combat trafficking, measuring criminal economies and polycriminality. She received her degree in international relations summa cum laude from American University.

Jennifer Chavarria, Threat Hunting Analyst, Shell Oil
Jennifer coded her first program in high school, a game of Pong. Looking to make a career out of it, she graduated from the University of Texas at Austin, and began working in IT for the oil and gas Industry. She has held roles from system administration to project management – experience she deems invaluable to finding her niche in security. An oil downturn, and several roles and companies later, she is now a threat hunter for the Shell CyberDefence team, where she delves into various efforts including providing support to industrial control system (ICS) asset owners. She also served as an advisor for the SANS ICS Summit in 2019. Offline, Jennifer enjoys running with her fur babies, cooking for friends, and spending weekends at the lake with her husband.

Chris Cochran, @chriscochran_io**,** Threat Intelligence & Operations Lead, Netflix
Chris is former active duty U.S. Marine in intelligence who had dedicated his career to building advanced cybersecurity and intelligence capabilities for national-level governments and the private sector. He has led intelligence programs at the National Security Agency, U.S. Cyber Command, U.S. House of Representatives, and financial and high-tech sector companies. He currently leads the threat intelligence and operations program at Netflix. He has made it his personal mission to motivate and empower cybersecurity professionals and teams through coaching, his podcast, and speaking engagements.

Mark Fernandez, Lead Cybersecurity Engineer, The MITRE Corporation
Mark has done a variety of open-source projects with the Zeek Network Security Monitor tool.

Daniel Garcia, Threat Hunting Analyst, Shell Oil
Daniel's interests have always been in Information Technology, whether dissembling his first PC to see how components worked in order to later build his own, or learning about intrusion techniques and how to detect and respond to better secure enterprise environments. He's been a blue teamer since 2013, performing roles in Incident Response, Malware Analysis, Threat Hunting and Intelligence, and he has occasionally dipped his toes into the red team's pool. An avid gamer, reader, pop culture collector, and foreign language enthusiast, his mantra is continuous learning and enjoyment.

Phil Hagen @philhagen, Summit Co-Chair, SANS Institute
Phil engages with the Digital Forensic and Incident Response (DFIR) community to ensure Red Canary's endpoint security solution fits into DFIR processes at organizations of all sizes. Phil is a SANS Senior Instructor and course lead for SANS FOR572: Advanced Network Forensics. He has held several previous positions at ManTech CFIA and worked as a communications officer in the U.S. Air Force. He lives with his amazing wife and two kids in coastal Delaware, where he enjoys the local craft beer scene and is often found riding a OneWheel wherever he can.

Will MacArthur @Anti_Expl0it, Threat Research & Intelligence Lead, InQuest.net
Bio to Come

Todd Mesick @tmesick1, Lead Forensic Analyst, Precision CastParts
Todd's 19-year IT career started as a help desk technician and then expanded to administration of networks and systems in both heavy Microsoft and UNIX environments. he has spent the past five years focusing on DFIR. Todd obtained a masters' degree in digital forensic science, focusing on scaled Incident Response, from Champlain College and holds the GCFE, GCFA, GNFA, GREM, and several Splunk certifications.

David Bernal Michelena @d4v3c0d3r, Lead Security Researcher, Scitum
David has 10 years of experience in information security and holds a bachelor's degree in computer engineering from the National Autonomous University of Mexico (UNAM). Since June 2015 he has served as Lead Security Researcher for SCILabs, the Cyber Security Team at Scitum. David is a SANS Mentor in Mexico City and holds multiple industry certifications. He enjoys exercising and playing the piano.

Brian Moran @brianjmoran, Digital Strategy Consulting, BriMor Labs
Brian is a digital forensic analyst with nearly 20 years of experience in the cybersecurity field, both in the U.S. Air Force and the private sector. His initial exposure to DFIR came about during an all-expenses-paid tour in 2004 in Mosul, Iraq, where he served on a team that provided mobile device analytics in support of tactical military operations. He also possesses some sweet Photoshop skills.

Gunter Ollmann @gollmann, Chief Security Officer, Microsoft
Gunter drives the cross-pillar strategy for the Cloud and AI Security groups at Microsoft. He has over three decades of information security experience in an array of cybersecurity consulting and research roles. Before joining Microsoft, Gunter served as CSO at Vectra AI driving new R&D into ML and AI-based threat detection of insider threats.

Valentina Palacin, Cyber Intelligence Analyst, Deloitte
Valentina is a Deloitte Threat Intelligence Senior Analyst, specializing in tracking APTs worldwide and using the ATT&CK Framework to analyze their tools, tactics and techniques. She is a self-taught developer with a degree in Translation and Interpretation from the Universidad de Málaga (UMA), and a Cyber Security Diploma from the Universidad Tecnológica Nacional (UTN).

David Pearson @davidp0508, Head of Threat Research, Awake Security
Having used Wireshark ever since it was Ethereal, David has been analyzing network traffic for well over a decade. He has spent most of his professional career understanding how networks and applications work, currently as Head of Threat Research for Awake Security. David holds computer security degrees from the Rochester Institute of Technology (BS) and Carnegie Mellon University (MS).

Jose Luis Rodriguez, Researcher
Bio to Come

Roberto Rodriguez @Cyb3rWard0g, Security Researcher,
Roberto is a senior threat hunter and researcher specializing in the development of data analytics to detect advanced adversarial techniques. He is also the author of several open-source projects, such as the Threat Hunter Playbook and HELK, that help the community develop techniques and tooling for hunting campaigns. His blog is at https://medium.com/@Cyb3rWard0g

Patricio Sanchez, CTO, InQuest.net
Patricio is a cybersecurity enthusiast with experience in creating and leading highly specialized teams related to advanced security monitoring, threat hunting, penetration testing, DFIR, malware analysis, cyber intelligence, threat intelligence, and security architectures. Currently he is the Head Scitum CyberIntelligence Laboratories , Professor of CyberSecurity at LaSalle University, and a founding member of BSIDECDMX. He holds the GCIH, GWAPT, CISSP®, and CISM certifications.

Karl Scheuerman, **@KarlScheuerman**, Senior Strategic Intrusion Analyst, CrowdStrike
Karl is a Senior Strategic Intrusion Analyst on CrowdStrike's OverWatch threat hunting team. He holds multiple SANS certifications and lives in Richland, WA with his beautiful wife and three daughters.

Cat Self @coolestcatiknow, Lead Information Security Engineer, Target
Cat started her career as a developer implementing and designing a metric to evaluate the security posture of technology products, known as the Product Intelligence Score (patent pending). She transitioned to the red team, implementing APT techniques and learning the value of being offensive. She now works as a threat hunter at Target, continuing to specialize in offensive security. She previously served in Military Intelligence with the U.S. Army, including two combat deployments.

John Stoner @stonerpsu, Principal Security Strategist, Splunk
As a Principal Security Strategist at Splunk, John enjoys blogging, problem-solving, and building content. During the fall and winter, you can find him driving his boys to hockey rinks all over the northeast.

Benjamin Wiley @benwiley, Associate Consultant, Mandiant
Ben is an associate consultant in Mandiant's Denver, CO office as part of its Incident Response team. He provides emergency services to clients when a security breach occurs. Ben has been a part of the Information Security community for more than three years, spending much of that time as a Security Operations Center analyst in the energy industry. In his free time, he enjoys spending time outdoors with his wife and dog.

Piotr Wojtyla, Senior Researcher, CrowdStrike
Piotr has 10 years of experience in security and has presented at a number of leading conferences. Piotr is experienced working on Security Operations Centers, Incident Response, and threat hunting teams.

John Wunder @jwunder, Principal Cybersecurity Engineer, The MITRE Corporation
At The MITRE Corporation, John works on defensive operations and ATT&CK, maintains the Cyber Analytics Repository (CAR), and works across MITRE's sponsors building out hunt programs and capabilities.