SANS

THREAT HUNTING & INCIDENT RESPONSE

SUMMIT & TRAINING

Program Guide

Advisory Partner

CARBON BLACK

ARM YOUR ENDPOINTS

@sansforensics #ThreatHuntingSummit

Welcome to the **Threat Hunting & Incident Response Summit!** I'm so excited that SANS Institute and our advisory partner Carbon Black have come together to create an event dedicated to in-depth discussions on this critical topic in the security landscape. Over the next two days, we will focus on specific hunting and incident response techniques and capabilities that can be used to identify, contain, and eliminate adversaries targeting your networks. Our goal is for you to be able to take what you learn here and use it to better secure your organization.

We have nearly 300 members of the information security community in attendance. Take this opportunity to introduce yourself to those sitting around you, join one of the many conversations during the networking breaks, and soak up some local culture with fellow attendees and Summit speakers at the House of Blues on Tuesday, April 12. Attendees tell us time and again that the greatest value of a Summit is the plethora of newly forged or deepened industry connections made during their time with us.

Finally, let's have fun! Engage with our expert speakers during the breaks, ask questions during the Q&A sessions, and weigh in on twitter **#ThreatHuntingSummit**. Your participation is what makes the Summit a truly wonderful and unique event.

Sincerely,

Rob Lee,
Summit Chair & Fellow, SANS Institute

Agenda

All Summit Sessions will be held in the International Ballroom – 16th Floor (unless noted).

All approved presentations will be available online following the Summit at
https://digital-forensics.sans.org/community/summits
An e-mail will be sent out as soon as the presentations are posted, typically within 5 business days of the event.

Tuesday, April 12	
8:00-9:00am	**Registration & Coffee** (LOCATION: CRESCENT A/B – 16TH FLOOR)
9:00-9:20am	***Opening Remarks*** ***Rob Lee**, Fellow, SANS Institute*
9:20-10:00am	***Threat Hunting, Defined*** Our cyber adversaries continue to change, modify, and evolve their tactics. Cyber Defense teams are broadening their own capabilities to detect and respond to these new attacks. While everyone agrees the process of threat hunting is a valuable tool in the Cyber Defense quiver, putting a definition around threat hunting tends to create heated debate. Is there a defensible definition of threat hunting the entire community can accept? ***Bamm (Robert) Visscher**, CIRT Manager, Cyber Defense, Information Technology, General Motors*
10:00-10:30am	**Networking Break and Vendor Expo** (LOCATION: CRESCENT A/B – 16TH FLOOR)
10:30-11:15am	***Hunting on the Cheap*** For organizations and individuals with limited security budgets, successfully hunting for cyber adversaries can be a daunting challenge. Threat Intelligence can be expensive and sometimes nothing more than IoCs or blacklists. In this talk, Endgame's threat research team will present a series of techniques that can enable organizations to leverage free or almost-free sources of data and open-source tools to "hunt on the cheap." They'll explain how to: retrieve attackers' tools from globally distributed honeynets that look like your organization or a juicy launching point to attackers; enrich the data past basic file/tool hashes to identify malicious command and control IPs/domains through automated binary analysis using open-source sandboxes and tools; and use passive DNS data to identify active infections and enrich existing data sets. Attendees will learn how to apply these three techniques to hunt for adversaries within their own networks. They will also learn about the various open-source solutions available, such as graph databases, that make these techniques inexpensive and within the scope of many organizations. ***Anjum Ahuja**, Senior Threat Researcher, Endgame* ***Jamie Butler**, Chief Scientist, Endgame* ***Andrew Morris**, Threat Researcher, Endgame*

Tuesday, April 12

11:15-12:05pm

Hunting Your Memory

The POS malware used in the Target hack of 2013 was a great example of how adversaries are looking for sensitive data in memory. Why not allow our hunters to do the same? What if the threat you're hunting is resident only in memory? Advanced introspection of memory at scale, on demand, can provide a unique view into the operations of your adversaries. Whether you are doing ad-hoc hunting for unknown unknowns, hunts for known IOCs during an incident, or regularly scanning for suspicious activity, advanced introspection of memory at scale can provide a unique view into the operations of your adversaries. Using entirely open-source tools, this talk will cover some current (and upcoming) capabilities and techniques to hunt on the cheap.

***Heather Adkins**, Information Security Manager, Google*

12:05-1:15pm

Lunch & Learn Presentation (LOCATION: INTERNATIONAL BALLROOM – 16TH FLOOR)

The Most Dangerous Game: Evolving Threat Hunting to Keep Up with Skilled Adversaries

The focus of cybersecurity is often on stopping malware, but advanced threats are orchestrated by skilled operators. Rather than pit technology solutions against malicious code, the modern defense requires security teams to evolve a hunting function, pitting human beings against other human beings that are hiding in their environment. Our speakers share insight into what skills and tools you need to hunt effectively, how the security team can unite to collectively defend against bad actors and share insight into the returns your team will get from honing the craft of threat hunting.

***Ryan Cason**, Senior Technical Account Manager, Carbon Black*
Marc Brawner, Associate Managing Director, Kroll

1:15-2:05pm

Using Open Tools to Convert Threat Intelligence into Practical Defenses

Threat actors are not magic and there is not an unlimited, unique list of threats for every organization. Enterprises face similar threats from similar threat sources and threat actors – so why does every organization need to perform completely unique risk assessments and prioritized control decisions? This presentation will show how specific, community-driven threat models can be used to prioritize an organization's defenses – without all the confusion. In this presentation James Tarala will present a new, open, community-driven threat model that can be used by any industry to evaluate the risk that faces them. Then he will show how to practically use this model to prioritize enterprise defense and map to existing compliance requirements facing organizations today. Whether you are in the Department of Defense or work for a small mom-and-pop retailer, you will be able to use this model to specifically determine a prioritized defense for your organization.

***James Tarala**, Principal Consultant, Enclave Security; Senior Instructor, SANS Institute*

Tuesday, April 12

2:05-2:50pm

The Remediation Ballet: Performing the Delicate Dance of Clean Up

The security industry focuses a great deal on defense, detection and investigation of advanced threats, but the red team always wins in the end. Once an attacker is on your network, it's imperative to have a formal and repeatable plan to quickly get them back out! This talk explores the difficulties involved in remediation such as when to kick-out, whether to clean up or rebuild, and suggests some methods by which IR teams can engage with ops and admins to more professionally accomplish remediation and return servers and networks to a known-trusted state.

Matt Linton*, Chaos Specialist, Google*

2:50-3:10pm

Train Like You Fight

Too often, incident response talks are filled with glib advice: "assume compromise," "build a baseline," with little or no practical advice to offer. Our organization pursues aggressive testing and drills for our analysts and administrators, using real adversarial tactics and tool sets. We test our own environment with the intent to be caught and discovered. This is the best way to train your teams. These tests are cross-functional and have been proven highly effective. Your teams will learn what to look for, how these tools work, where their gaps are. From this talk you will come away with actual tactics and tools that you can use to mimic adversarial actions. We will explore how to conduct tests and counter-adversary operations with your teams. We'll explore what artifacts credential theft leaves on a system, and what command and control traffic looks like? The hope is that you will begin to train like you fight, to be ready to face the real threats.

Casey Smith*, Threat Intelligence Analyst, FirstBank*

3:10-3:40pm **Networking Break and Vendor Expo** (LOCATION: CRESCENT A/B – 16TH FLOOR)

3:40-4:00pm

Collecting and Hunting for Indications of Compromise with Gusto and Style!

In this session, SANS instructor Ismael Valenzuela will explain the methods and techniques used by world-class IR teams to leverage the power of open-source tools like Yara and Bro to do IOC hunting when reacting to emergency incidents. State-of-the-art techniques will be presented along with a new open-source tool called **rastrea2r**, designed to assist with collecting and hunting for IOCs with gusto and style!

Ismael Valenzuela*, Lead IR/Forensics Technical Practice Manager, Intel Security;*
Community Instructor, SANS Institute

Tuesday, April 12

4:00-4:45pm

Must Collect IOCs... Now What?!

Indicators of Compromise(IOCs) are hot commodities nowadays. Most of us have a metric ton of IOCs from a plethora of sources, but what do we do with them? After struggling to drink from the IOC firehose, we developed Overlord, an open source project designed to provide automated searching and alerting on IOCs in a scaleable and robust manner, to help us stay on top of the influx. In this talk, Phillips will examine how to utilize the Overlord Project to bridge the gap between IOC repositories and searching infrastructure.. After getting a fresh IOC, besides the usual vetting, we would like to know about this IOC in our environment, ideally on an ongoing basis. Overlord allows us to achieve by this allowing each of its primary components to be modified or completely rewritten for each use case, while still remaining easy to use.

Williams M. Phillips IV*, Security Researcher, Salesforce*

4:45-6:00pm **Networking Reception and Vendor Expo** (LOCATION: CRESCENT A/B – 16TH FLOOR)

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat
or turn them in to the SANS registration desk.

6:30-8:30pm

THIR in NOLA

We're taking this show on the road!
Join fellow attendees, Summit speakers,
and sponsors for networking and live music
at the iconic House of Blues.

HOUSE OF BLUES®
NEW ORLEANS

CARBON BLACK
ARM YOUR ENDPOINTS

ARBOR® NETWORKS
The Security Division of NETSCOUT

DOMAINTOOLS®

sqrrl
Target. Hunt. Disrupt.

Wednesday, April 13

8:00-9:00am

Networking Breakfast (LOCATION: MADEWOOD A/B – 2ND FLOOR)

HOSTED BY ARBOR® NETWORKS

9:00-9:45am

Hunting as a Culture (HaaC): Moving Your Cyber Defenses Towards an Aggressive, Proactive Style

Cybersecurity is hard. Bombardment of attacks is paired with bombardment of data. The surface area is growing, the perimeter deteriorating, and few organizations can hire enough defenders to adequately staff their ranks. But all is not lost. It's time to automate, it's time to orchestrate, and it's time to unite man and machine to enable team search-and-destroy missions to move closer to clean environments. 2016 is the year that hunting establishes itself as a first-class cyber defense strategy, and we will explore how to get you there.

***Ben Johnson**, Chief Security Strategist, Carbon Black*

9:45-10:30am

Casting A Big Net: Hunting Threats at Scale

One of the biggest differentiators between a mature incident response team and one that is less experienced is the ability to triage hundreds to thousands of endpoints at once. The classic approach is to analyze one host at a time, attempt to connect the dots and determine patient zero. This approach is time-consuming and leaves victims vulnerable while attackers are active in their network.

A much faster and more agile process is to collect, process, and analyze artifacts from all endpoints simultaneously. Known by various monikers such as sweeping, hunting, or stacking, being able to collect live response data quickly from endpoints is a crucial capability.

This talk will demonstrate methods similar to those used by CrowdStrike's incident response consultants using a free tool, CrowdResponse, for collection and a free Splunk application for analysis at scale. Using real-world examples, we will show how to parse artifacts and identify anomalies from the registry, services, events, tasks, and file system at scale. Attendees will receive both the tools and expertise to put them on the fast track to identifying and ejecting adversaries from their network.

***Paul D. Jaramillo**, Principal Consultant, CrowdStrike*
***Reed Pochron**, Senior Consultant, CrowdStrike*

10:30-11:00am

Networking Break and Vendor Expo (LOCATION: CRESCENT A/B – 16TH FLOOR)

11:00-11:45am

Hunting and Dissecting the Weevely Web Shell

Weevley (version 3) is an extendable PHP web shell that provides attackers a wide range of backdoor functionality via standard HTTP requests.This talk walks through techniques to find Weevely based on network analysis and, once located, how to dissect the host and network based artifacts.This process includes reversing the custom command and control encryption used by Weevely. Once done, the analysis allows determining what actions where taken by the attacker, and what data was exfiltrated via the web shell.The PCAP from a simulated attack, host-based artifacts, and custom Python scripts used during the analysis will be made available afterwards.

***Kiel Wadner**, Information Security Analyst - Red Team, Blue Coat Systems*

Wednesday, April 13

11:45am-12:05pm

SANS Threat Hunting Survey Results

The results of SANS' first-ever Threat Hunting Survey will be released in a two-part webcast on April 14th and April 15th, but Summit attendees will get an exclusive sneak peek at the results. Included will be data and feedback on the tools organizations are using for threat hunting; the top skills hunters need to succeed; and how threat hunting affects and is affected by security budgets.

***Rob Lee**, Fellow, SANS Institute*

12:05-1:15pm

Lunch & Learn Presentations

LUNCH & LEARN
(LOC: ROSEDOWN – 2ND FLOOR)

Presented by

ARBOR NETWORKS®

The True Clues That Only Traffic Reveals

***Paul Bowen**, Principal Security Technologist, Arbor Networks*

Stealthy attackers are brilliant at covering their tracks with misdirection and obfuscation. Fortunately network traffic never lies, and understanding flows and packets can provide the high-fidelity clues needed to find and disrupt attack campaigns in just minutes. Join Arbor's Paul Bowen to learn how senior responders, mid-level analysis and novice specialists can quickly use network traffic to gain an unfair advantage.

LUNCH & LEARN
(LOC: MADEWOOD A – 2ND FLOOR)

Presented by

DOMAINTOOLS®

Threat Hunting with DNS & Domain Profiles

***Mark Kendrick**, Director of Solution Engineering, DomainTools*

"I Have the IOCs – Now What?" The best threat hunters know attribution can be a proxy for risk. Even when you don't know who's behind an attack, simply knowing what's linked to it can give you tremendous insight. This session will explore specific techniques for enumerating an attacker's online infrastructure and revealing patterns in the history of their domain names and IP addresses. You'll see first-hand the value of a domain-focused, actor-centric investigative model.

LUNCH & LEARN
(LOC: MADEWOOD B – 2ND FLOOR)

Presented by

ENDGAME.

Think Offense: Hunt Smarter, Live Low

***Mike Nichols**, Prinicipal Product Manager*

Defense strategies have run their course. The traditional security stack no longer provides the mission assurance enterprises need. "Search based" strategies that depend on short-lived indicators of compromise are ineffective for identifying polymorphic adversaries. Enterprises must add an "offense" approach to their security programs to detect adversaries that have never been seen before. Attend this talk to learn how Endgame's "Automate the Hunt" offense strategy is essential to detect never-before-seen adversaries that bypass the traditional security stack.

LUNCH & LEARN
(LOC: SHADOWS – 2ND FLOOR)

Presented by

LogRhythm®

Please visit LogRhythm at the Vendor Expo to hear about their Lunch & Learn topic!

1:15-2:05pm

To Catch an APT: YARA

It's time to reclaim your networks and start hunting, armed with the open-source tool called YARA. Learn how to author YARA rule signatures with techniques used by malware researchers to mercilessly hunt down the elusive adversary of advanced threat actors, and how to apply those signatures in your organization or investigations using YARA-friendly tools. We will look at real-world case examples of PlugX and other favorite APT tools to show beginner to advanced YARA rules. Already familiar with YARA? Come learn how to improve rule signatures to catch different malware variants, all the while keeping false positives to a minimum. Arm yourself with the knowledge to go from hunted to hunter.

***Jay DiMartino**, Sr. Cyber Threat Researcher, Fidelis Cybersecurity*

Wednesday, April 13

2:05-2:50pm

Detecting & Responding to Pandas and Bears

30% of incident response investigations conducted by our team over the past two years have had multiple attack groups operating at the same time within the same organization, and this number is likely to increase in the future. Do you know how to identify and remove multiple attackers within your environment?

This presentation focuses on a recent investigation where the victim was simultaneously under attack by two separate attack groups, each with varying goals and TTPs. We'll demonstrate the critical role played by threat intelligence in identifying the attackers and how using this information allows responders and security teams to tailor their remediation tactics and implementation for success. We'll share approaches you can use and when to apply them. Attendees will also learn how to conduct adversary-based hunting operations using existing technology within your organization; improve authentication credential protection during live IR, and prepare for detection of future attacks.

Christopher Scott*, Director, CrowdStrike Services*
Wendi Whitmore*, Former VP, CrowdStrike*

2:50-3:10pm

Threat Intelligence Isn't Automatic

Watching people struggle to determine which of their many sources had the *correct* threat intelligence was one of the motivations for building the ThreatExchange platform. The world is a complicated place and there is no one right answer, no matter what your vendor may tell you. But it is possible to maximize the value of that information by sharing context and experience with a trusted community. This talk will describe how ThreatExchange sharing works, how you can use the information shared with you, and how to make sense of all of that data.

Jesse Kornblum*, Security Engineer, Facebook*

3:10-3:40pm **Networking Break and Vendor Expo** (LOCATION: CRESCENT A/B – 16TH FLOOR)

3:40-4:00pm

Proactive APT Hunting Style

One of the biggest challenges for enterprises today is to have the capabilities available to determine and identify if a security incident has occurred and what systems that have already been compromised.

The majority of enterprise's network defense is reactive and heavily dependent on detection through mistakes by adversaries or benevolent 3rd parties alerting organizations to breaches within their network. This approach to detection is simply inexcusable and leads to attackers having control of a network for months or years before they are noticed.

This presentation will introduce a tool, developed by Advanced Security Center at EY, named "APT Hunter," can be used to remotely collect large-scale system artifacts via Windows Management Instrumentation (WMI) and potentially identify existing threat for enterprise. In addition, we will show some real cases where we used this tool to discover data breach incidents. APT Hunter is an open-source tool and will be made available to Summit attendees after the event.

Joshua Theimer*, Manager, EY*
Hao Wang*, Senior Penetration Tester & Incident Responder, EY*

Wednesday, April 13

4:00-4:20pm

DIY DNS DFIR: You're Doing it WRONG

DNS is one of those protocols that we, as DFIR practitioners, take for granted. Operationally, if DNS resolution is working properly, we're happy. Many organizations, however, fail to utilize DNS logs and associated intelligence within their response and investigative activities. This is in part due to the perceived lack of value associated with DNS logs and its associated features, such as name server, WHOIS, and hosting information, and more often due to the unavailability of the logs. This talk will present several tools (both commercial and open source) to help manage the deluge of information on even the smallest of budgets. We will also discuss how to enrich your data with valuable intelligence from freely available sources. Finally, this talk will highlight some real-world investigative techniques where DNS and its associated features were used to add clarity to DFIR investigations.

***Andrew Hay**, CISO, DataGravity, Inc.*

4:20-4:40pm

A Longitudinal Study of the Little Endian that Could

The 9002 malware, first seen during Operation Aurora in 2009, is a family of malware seen in use by threat actors based in China. What makes 9002 interesting is that over the last six years, the development of this malware has not been linear. Different threat groups have taken 9002 and customized it to suit their own needs, creating multiple, parallel development branches. By understanding the differences between these development branches we can gain an insight into the adversary's development process, allowing the creation of better criteria for detection for both current and future threats.

This presentation will provide an overview of the 9002 malware, how the different development branches can be distinguished, how the development goals of the groups behind each branch differ, and how all of this information can be combined to better detect and respond to an intrusion.

***Andrew White**, Senior Security Researcher, Dell Secureworks*

4:35-4:45pm

Closing Remarks

***Rob Lee**, Fellow, SANS Institute*

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat
or turn them in to the SANS registration desk.

THIR SUMMIT SPEAKERS

Heather Adkins *Google* @argvee

Heather Adkins is a founding member of the Google Security Team. As Manager of Information Security, she has built a global team responsible for maintaining the security of Google's networks, systems and applications. The Google Security Team is involved in every facet of the business, including building security infrastructure, responding to security threats, and evangelism.

Anjum Ahuja

Endgame

Anjum Ahuja is a Threat Researcher at Endgame, working on problems related to network security, malwares, and large-scale data analysis. He is currently focused on building threat detection systems based on network fingerprints of malwares, their infrastructures, and global traffic patterns. He has a background in computer networks, routing and IOT security, and holds multiple patents in these fields.

Jamie Butler

Endgame @jamierbutler

Jamie Butler is the Chief Technology Officer and Chief Scientist at Endgame, where he leads Endgame's research on advanced threats, vulnerabilities and attack patterns. He has directed research teams at some of the most prominent and successful security companies of the last decade.

Jay DiMartino

Fidelis Cybersecurity

Jay DiMartino is a Sr. Cyber Threat Researcher for Fidelis Cybersecurity. He has been doing Malware Reverse Engineering for over five years and also has several industry certifications including the GREM and GCFA.

Andrew Hay

DataGravity, Inc. @andrewsmhay

Andrew Hay is the CISO at DataGravity where he is responsible for the development and delivery of the company's comprehensive information security strategy. Prior to that, Andrew was the Director of Research at OpenDNS (acquired by Cisco) and was the Director of Applied Security Research and Chief Evangelist at CloudPassage.

Paul D. Jaramillo

CrowdStrike @DFIR_Janitor

Paul is a Principal Consultant with CrowdStrike and previously worked in the government, energy, manufacturing and telecommunication sectors. Career highlights include breaking into a 2FA VPN as a pentester, successfully investigating an insider threat case across the globe as a forensics examiner, and ejecting nation state adversaries from corporate networks.

Ben Johnson

Carbon Black @chicagoben

Ben Johnson is cofounder and chief security strategist for Carbon Black. In that role, he spends a lot of time strategizing with customers to improve cyber defenses across the stack. Ben worked in cyber at NSA and at a defense contractor and has two computer science degrees.

Jesse Kornblum

Facebook @jessekornblum

Jesse Kornblum is a network security engineer on the Threat Infrastructure team at Facebook. He currently works on the ThreatExchange platform which enables organizations to share threat information with trusted partners within a vetted community. Previously, Kornblum was a computer forensics researcher and practitioner, writing tools such as ssdeep and md5deep. He is also a former Special Agent for the Air Force Office of Special Investigations.

Rob Lee

SANS Instititute @robtlee @sansforensics

Rob is currently the curriculum lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response.

Matt Linton *Google* @0xMatt

Matt is an incident responder with experience throughout the security process, from architecture through penetration. He is formally trained in disaster management and specializes in rapid response, remediation and hardening of compromised environments.

Andrew Morris

Endgame @Andrew_Morris

Andrew Morris works on the Research and Development team at Endgame, specializing in developing cutting-edge security technologies and researching advanced adversary techniques. Prior to Endgame, Andrew spent several years consulting to various Fortune 100 companies, government agencies, and military customers providing red team support, penetration testing, and adversary emulation services.

William M. Phillips IV *Salesforce*

William Phillips is a recent graduate of Brown University and currently a Security Researcher for the Salesforce Threat Intelligence team where one of his projects is Overlord. Areas of interest include OS X forensics, iOS security, and Network Forensics.

THIR SUMMIT SPEAKERS

Reed Pochron

CrowdStrike @rpochron

Reed Pochron has over 5 years of experience in intrusion investigations, conducting incident response, and enterprise security operations. As a Senior Consultant with CrowdStrike out of the Saint Louis office, Reed participates in customer engagements ranging from breach response to proactive compromise and maturity assessments. Reed currently holds his CISSP, GCFA, GCFE, and GCIH certification.

Christopher Scott

CrowdStrike Services

Christopher Scott has 18 years of Fortune 500/DoD/DIB business proficiency, including more than eight years of targeted threat detection and prevention expertise. Christopher supports a variety of engagements at CrowdStrike that include: proactive and reactive security services, incident response, data loss prevention, business continuity and disaster recovery processes.

Casey Smith

FirstBank @subTee

Casey Smith is a Threat Intelligence Analyst in the Financial Industry. He has a passion for understanding and testing defensive systems.

James Tarala

Enclave Security @isaudit

James Tarala is a founder and principal consultant with Enclave Security and a senior instructor with the SANS Institute. James presently serves as a technical editor for the Center for Internet Security's Critical Security Controls and the Open Threat Taxonomy projects.

Joshua Theimer

Ernst & Young

Joshua Theimer is a manager in EY's cybersecurity advisory practice where he evaluates and implements sustainable enterprise information security programs for the Fortune 500. He has experience responding to, investigating, and remediating compromised environments and leads a wide range of client engagements focused on assessing enterprise breach resiliency.

Ismael Valenzuela

Intel Security @aboutsecurity

Ismael Valenzuela (SANS Instructor & GSE #132), has 15+ years of international experience in cybersecurity consulting, teaching and public speaking. He currently works as Practice Manager at Intel Security, leading the delivery of SOC, Incident Response, Forensics and Threat Research services for major public and private organizations in North America.

Bamm Visscher

General Motors

Bamm Visscher is the CIRT Manager at General Motors where his team is responsible for detecting and responding to threats targeting the company's information assets. He has been performing CIRT functions since 1997 with experience in the USAF, Fortune 500, and Fortune 10 companies. Bamm contributes to the infosec community as the author of Sguil, an open source tool for performing network security monitoring.

Kiel Wadner

Blue Coat Systems @kielwadner

Kiel works on an internal Red Team at Blue Coat Systems evaluating products and internal networks. Previously he was a security researcher on Blue Coat's Global Intelligence Network building back-end detection systems and tracking threats. He is a graduate of the SANS Technology Institute and holds numerous GIAC certifications.

Hao Wang

Ernst & Young

Hao Wang is a senior in Ernst & Young's Advanced Security Center. Hao joined Ernst & Young after he graduated from Information Security Institute of Johns Hopkins. Hao is currently responsible for performing Attack & Penetration assessments involving internal as well as external network assessments, and Incident Response involving both network- and host-based forensics, and threat hunting.

Andrew White

Dell Secureworks

Andrew White, Ph.D. is a senior security researcher at Dell Secureworks with over five years of experience in digital forensics research. When not responding to targeted intrusions, Andrew performs research into memory forensics, targeted malware, credential theft and malware-less intrusions. Current holder of the DFIR Netwars high-score record.

Wendi Whitmore

@wendilou2

Wendi Whitmore has over 15 years of experience in the computer security industry responding to critical security breaches and providing customers with solutions to complex adversary problems.