SANS

# Data Breach Investigation Summit

Dallas, TX | Mon, Sep 21 - Sat, Sep 26, 2015

The following sessions are included with the course registration fee.  We hope that by providing these additional talks, you'll have a chance to learn from some of the leading experts in the field and get in some valuable networking with fellow attendees.

| **Tuesday, September 22nd** | | |
|---|---|---|
| 12:30-1:15 pm | **Going Right to the Data: Incorporating SQL Artifacts into Your Forensic Investigation**<br>When we are investigating a breach, one question rises up above them all: How much data walked out the door? We can examine a wide range of artifacts to try and figure out what left, or we can go right to the database, and ask! In this session, we will examine artifacts and data from one of the world's most popular database solutions: Microsoft SQL Server. Attendees will learn about volatile and non-volatile artifacts, where they are located, how to examine them, and how they may be integral to understanding the actions of an attacker. We will also look at how to go beyond what's in front of us, carving memory for SQL records. This session will display new research into SQL artifacts, as well as offer open source tools for forensic professionals to apply that knowledge on their next investigation.<br>**Matt Bromiley, Senior Consultant, Mandiant** | **Network Security Monitoring for the Masses**<br>The saying "prevention is ideal, but detection is a must" is as true today as ever before.  While most organizations are bolstering their security budgets and improving their defenses, it remains nearly impossible to completely prevent a determined attacker from compromising their intended target. Therefore, we must remain vigilant in our monitoring and outfit our networks with tools that provide visibility and agility when responding to the inevitable breaches that will occur.<br>In this talk, Mike Pilkington will discuss and demonstrate the relative ease of deploying powerful network security monitoring with free software on commodity hardware.  This can be done for a small home or office, all the way to a global enterprise network with thousands of users—all with relative ease and minimal expense.  The demonstrations will focus on Security Onion, a software distribution particularly well-suited for comprehensive network security monitoring in environments large and small. This talk will arm you with the information you need to keep a keen |

| | | |
|---|---|---|
| | | eye on your valuable assets.<br>**Mike Pilkington, Technical Incident Response Lead, Fortune 500 Oil & Gas Company & Certified Instructor, SANS Institute** |
| **Wednesday, September 23rd** | | |
| 12:30-1:15 pm | **Current Legal Issues in Computer Search and Seizure**<br>This talk will be a review of current federal cases that impact on search and seizure of electronic devices and current legal issues relating to computer forensics and testifying as an expert witness in computer forensics.<br>**Howard Cox, Former Assistant Inspector General for Investigations, Central Intelligence Agency** | **Turning Your Caseload into Threat Intelligence**<br>No external intelligence source can ever provide information more relevant than an organization's own internal information. By looking at what your incident response team already has investigated, you can get an view into the intentions and capabilities of attackers that present a confirmed threat to your information. This talk will focus on how to structure your reporting and analyze your case load in such a way as to produce valuable strategic, operational, and tactical intelligence that can be applied at all levels of your information security program. Attendees will be able to go back and immediately begin extracting information that will help guide their ongoing breach detection and incident response efforts.<br>Kyle Maxwell**, Senior Researcher, Verisign** |
| **Thursday, September 24th** | | |
| 12:30-1:15 pm | **Identifying Historical Attacker Actions via Journal Analysis**<br>File system journal forensic analysis is a relatively new sub discipline of DFIR. While most people are coming into it thinking about traditional host based forensics it can also be applied in cybercrime investigations. In this session learn how to find historical IOCs, locate past attacker toolkits loaded and deleted before you responded and identify possible exfil.<br>**David Cowen, Partner, G-C Partners** | **Walk Softly and Carry 26 Trillion Sticks**<br>Malware research community has long spent their expertise in dissecting malware binaries, examining footprints on victims' systems. Instead of studying the diseases themselves, however, at OpenDNS we study the collective behavior of victims (patients) and the behavior of bad actors (diseases).<br>At OpenDNS Andrew has the privilege of using roughly 71 Billion DNS queries per day (~26 Trillion per year) with which to track bad guys, predict malware |

| | | |
|---|---|---|
| | | outbreaks, and determine opportunistic or campaign-specific botnet infrastructures. In this talk, Andrew will explore some of the key findings in 2014 based on this massive corpus of data. Visualization techniques for assigning attribution based on co-occurring domains and infrastructure will also be discussed.<br>**Andrew Hay, Director of Research, OpenDNS Inc.** |
| **Friday, September 25th** | | |
| 12:30-1:15 pm | **Hardware Keylogger Case Study**<br>Hardware keyloggers were identified in a client environment. Upon analysis identified the mass storage volume associated with the hardware key logger data was not accessible due password protection at hardware level. Using a teensy (USB-based microcontroller development system) created a hardware based brute force device which was used to emulate a dictionary of keystrokes. Ultimately this device exposed the password for the keylogger allowing sufficient analysis. Upon analysis of the device was able to tie the keylogger back to a hostname and user name with unique and surprising artifacts. Demo of teensy will be provided.<br>**Steve Gibson, Director, KPMG** | |