SANS Forensics and Incident Response SUMMIT

AUSTIN, TEXAS

July 9-10, 2013

PROGRAM GUIDE

Agenda

All joint Summit Sessions will be held in Lone Star (unless noted).

All approved presentations will be available online following the Summit at ***http://computer-forensics.sans.org/community/summits****.*
An e-mail will be sent out within 5 business days once the presentations are posted.

Monday, July 8

6:00pm-8:00pm

Registration – *Location: The Atrium*

6:00pm-8:00pm

Welcome Reception – *Location: The Atrium*

Sponsored by

Tuesday, July 9

7:00am-8:00am

Registration – *Location: 2nd Floor Foyer*

8:00am-8:10am

Welcome and Introduction to the 2013 Digital Forensics and Incident Response Summit

Rob Lee *&* ***Alissa Torres*** *– Summit Chairs, Digital Forensics and Incident Response Summit*

8:10am-9:10am

Autopsy 3: Extensible Open Source Forensics

Autopsy 3.0 is an open source, end-to-end digital forensics platform based on The Sleuth Kit. It is a complete rewrite from Autopsy 2.0 and was designed to be an extensible platform with modules that are open or closed source and free or commercial. This talk covers the exciting new features of this system, including multi-threaded frameworks, triage, embedded databases, web artifact analysis, and indexed keyword search. This talk is targeted towards both users and developers. Users will learn about the tool, and how they can use it. Developers will learn the basics of where they can incorporate their tools into the Autopsy workflow as modules.

Brian Carrier *- VP of Digital Forensics, Basis Technology*

9:10am-10:10am

TRACK 1 – CAPITAL BALLROOM A

File system journaling forensics theory, procedures and analysis impacts

Journaled file systems have been a part of modern file systems for years but the science of computer forensics has only been approaching them mainly as a method of recovering deleted files. In this talk we will outline the three major file systems in use today that utilize journaling (NTFS, EXT3/4, HFS+) and explain what is stored and its impact on your investigations. We will demonstrate tools for NTFS and EXT3/4 that allow us to:

- Recover data hidden or destroyed by anti-forensics
- Recover previously unrecoverable artifacts
- Trace all file system movements and actions of malware
- The possibility of entirely new analysis techniques

Ending with a review of HFS+ and the future of file system forensics in relations to journals and new file systems such as ReFS.

David Cowen *with* ***Matthew Seyer****, G-C Partners, LLC*

TRACK 2 – CAPITAL BALLROOM B

Mining for Evil

Microsoft's System Center Configuration Manager (SCCM), formerly Systems Management Server (SMS), can be a gold mine when hunting for evil. During a response it can provide valuable information of what was executed on the host system. This presentation will provide an understanding of SCCM, host artifacts, scripts and tips to find targeted threats in your enterprise. Although this presentation details SCCM, the concepts can be used on similar configuration-management platforms.

The second part of this presentation will delve into the finer points of Windows log file analysis. Properly configured Windows logging can provide a wealth of information, making the jobs of both proactive intrusion detection and reactive incident response faster and more effective. We'll discuss a number of tips and techniques for implementing a strong logging policy and for analyzing the resulting logs for evidence of compromise.

John McLeod *- Manager, Incident Response Team*
Mike Pilkington *- Senior Consultant, Incident Response Team*

10:10am-10:30am

Networking Break and Vendor Expo – *Location: Capital Ballroom Foyer*

10:30am-11:30am

TRACK 1 – CAPITAL BALLROOM A

The "Trusted" Insider Theft of Intellectual Property and Trade Secrets

As company downsizing becomes more prevalent in today's economic downturn, business are increasingly vulnerable to the pirating of Intellectual Property by current and former employees. Learn how to mitigate these risks as one of the former lead investigators of the "Comtriad" investigation shares the story for this discussion. See how Warren Kruse, George Wade, and Michael Barba became aware of a potential issue, developed a strategic approach, assessed potential damages, and developed leads using forensic and network technologies which led to the arrest of three foreign nationals attempting to appropriate Intellectual Property which was valued to be in excess of one billion dollars. This investigation garnered worldwide attention and has received the High Tech Criminal Investigative Association's (HTCIA) Case of the Year award.

Hear how computer and network forensics, along with current technologies and with a little luck, aided this investigation.

Warren G. Kruse II *- VP, Altep, Inc.*
Michael Barba *- Managing Director, BDO*
George Wade *– Security Solutions Architect, HP Enterprise Security Service (ESS)*

TRACK 2 – CAPITAL BALLROOM B

Volatile IOCs for Fast Incident Response

Incident response against malware infection generally takes long time for memory forensics, disk forensics and malware analysis. It's desirable to find and identify malware at an early stage performing memory forensics, but it requires expert knowledge about malware.

In this session, I show "volatile IOCs (Indicators of Compromise)" to detect some famous malware (e.g., ZeuS, SpyEye, Poison Ivy) from physical memory images. By using the IOCs, everyone can pinpoint the type of malware without disk forensics and malware analysis. Audiences can also grasp the techniques of fast malware triage.

Specifically, I explain how to define volatile IOCs using OpenIOC that is an extensible XML schema for describing technical characteristics of known threats. Some IOCs are already available on the Internet, but most of them are difficult to reuse and need non-volatile information such as file hash values and file names. Volatile IOCs introduced in this session can identify malware including its variants based on only volatile evidences like header signatures of data structures, deobfuscated strings and a sign of code injection in memory space.

Takahiro Haruyama*, Forensic Investigator, Internet Initiative Japan Inc.*

11:30am-12:30pm

TRACK 1 – CAPITAL BALLROOM A

Johnny AppCompatCache: the Ring of Malware

In 2012, MANDIANT investigators determined that a registry key, AppCompatCache, maintained a list of executable files. The structure also contained date and timestamps. Researching the structure indicated that it belonged to the Windows Application Compatibility Database. The structure itself contains full file paths, date and time information, file sizes, and in some versions of Windows, an execution flag. A MANDIANT consultant, Andrew Davis, wrote a python script that is able to extract the information from the various versions of the Application Compatibility Database. With this tool and knowledge, MANDIANT has been able to enhance their investigations by determining that executable files were on a system and putting time or chronological context to the investigation where none had existed before.

This paper and discussion will examine the structure of the database across the various versions of Windows, will discuss why many Windows registry analysis tools fail to see the structure's data, and will provide examples of case work that illustrate why the analysis of the Application Compatibility Cache have become a regular process in MANDIANT investigations.

Brice Daniels *- Senior Consultant, MANDIANT*
Mary Singh *- Senior Consultant, MANDIANT*

TRACK 2 – CAPITAL BALLROOM B

"My name is Hunter, Ponmocup Hunter"

In early 2011 we discovered some botnet malware infected systems in our network. Starting from one A/V event we discovered several host- and network-based indicators to identify and confirm several infections. A brief high-level overview of the security architecture will help you understand how the indicators could be found and searched for. With a one-strike remediation all infected systems were quarantined and cleaned. A few weeks later the sinkholing of several known C&C domains showed the botnet was very big (several million bots). Quickly I got obsessed with analyzing and hunting this malware, which could infect fully patched systems without using exploits (only social engineering) and protected by firewalls, IPS and multi-layered A/V. The malware got some visibility and media attention in June 2012 with titles such as "printer virus", "printer bomb" or "Trojan. Milicenso: A Paper Salesman's Dream Come True". This was likely due to an unwanted side-effect or "mistake" by the bot-master and probably didn't happen to all infected hosts or networks.

You'll learn:

- how the malware was discovered, what indicators were derived
- how all infected hosts were identified and how remediation was done
- how this malware spreads and how to defend against it
- how to detect infected systems (host & network indicators)
- how to find infected web servers used to spread it
- what malware functionalities are known and currently still unknown

Tom Ueltschi *- Security Officer, Swiss Post*

12:30pm-1:45pm

Lunch & Learn – *Location: Lone Star*

Presented by

cellebrite
delivering mobile expertise

Using Data Analytics to Focus and Streamline Forensic Exams

"Give me everything on the phone" is a phrase most digital forensic examiners have grown familiar with -- and come to dread. With smartphones, gigabytes of data including thousands of text messages, images and videos, and other content can quickly consume a lab's resources past the point of inefficiency.

Helping investigators understand what is most relevant to their case is critical. This is where data analytics can work to your advantage. With the tools available through mobile forensic solutions such as UFED Physical Analyzer and UFED Link Analysis, show investigators how they may not need "everything" when they can visualize only the most important context from call logs, text messages, email and app data. This can give investigators more meaningful leads that they can put to work right away in an investigation, often within the first "golden hour" that it starts.

***Lee Papathanasiou**, Technical & Sales Engineer, Cellebrite*

1:45pm-2:45pm

TRACK 1 - CAPITAL BALLROOM A

(Mostly) Open Source DFIR – A Toolkit for End-to-End Investigations

We are entering a "golden age" of incident response investigations. After many years of being outgunned and depending mostly on expensive tools to fight back, a wide range of open source tools and powerful low cost applications are coming on line. Look at the Collective Intelligence Framework, Google's Rapid Response, Malformity, foorep, and plaso to name a few.

We will spend most of the session taking a close look at some significant tools and how they contribute to a well-run incident response effort. We will close with a quick run through a number of other tools that you might want to investigate.

- Google Rapid Response – We heard about GRR at the Summit last year. Is it ready for prime time? How can you instrument, monitor and investigate a global enterprise with an open source tool?
- Maltego with Malformity – Using Maltego to conduct open source investigations of malware, network indicators, and threat actors. There are some very interesting transforms coming out to help shape Maltego for incident response.
- Foorep – You need to organize, categorize, and share your evidence. Foorep handles a lot of the static analysis, presents the results well, enables the analyst to annotate the samples, and facilitates sharing of samples and intel.
- Yara/OpenIOC/Stix – You've got a piece of malware, great. Now, how do you find it in the wild? Or, find things like it? Or find things that behave like it? Despite claims to the contrary, signatures and IOCs provide a lot of IR value, even if you're just using them to share intel.
- Collective Intelligence Framework – "A framework for warehousing intelligence bits." So you've got your malware all tidied up in a malware zoo. What about the rest of your data? CIF doesn't get it all, but it goes a long way to collect, normalize, and report on threat intel from a variety of feeds.

At the end of the session you should have enough information to go home and stand up a pretty impressive incident response toolkit capable of meeting many needs in a large enterprise at the cost of your time and some hardware.

***David Kovar** - Manager, Advisory Center of Excellence, Ernst & Young*

TRACK 2 - CAPITAL BALLROOM B

Offense informs Defense, or does it?

This presentation will look at various highly publicized attack campaigns like (CVE-2011-0609,CVE-2012-1535 & CVE-2012-4792) and reveal behavioral characteristics found in each one, attack methodologies and defensive measures will be explored in the malware, the memory artifacts and network traffic signatures. The idea is to enumerate features of the attacks to supplement defensive operations and this can only be accomplished through intelligence derived from the campaigns. Open source intelligence can be a great source of data on present day attacks which can yields volumes of threat data in a timely fashion. All of these facets will be combined and fused into a process that can make it more difficult for the attacker to succeed and help defenders elevate their awareness.

***Jeff Brown** - Director of Cyber Operations, Cyber Clarity*

TRACK 1 – CAPITAL BALLROOM A

Open Source Threat Intelligence

Organizations can no longer rely purely on general, preventive controls. Instead, defenders must continually adapt to their adversaries, including using threat intelligence as appropriate. This talk will examine a number of tools and sources of "open source" intelligence (OSINT) focusing on network indicators, malware, and threat actor tracking. We will also look at how to extend and integrate these tools and sources with existing common technologies for already-stressed incident response teams.

Kyle Maxwell *- Senior Analyst, Verizon Business*

TRACK 2 – CAPITAL BALLROOM B

Cyber Nightmares: Red October & Shamoon

The presentation will cover potential delivery methods used to infect the victim hosts and networks of the two most recent malware attacks—Shamoon and Red October. The presentation will also explore some of the implementation and obfuscation techniques that might explain how the malware used in the Red October operation was reportedly undetected for several years. During the live analysis of these pieces of malware, the attendees will be exposed to a series of tools used for malware analysis together with suggestions on report writing.

Harold Rodriguez*- Malware Reverse Engineer, General Dynamics Fidelis Cybersecurity Solutions*

3:45pm-4:05pm

Networking Break and Vendor Expo *– Location: Capital Ballroom Foyer*

4:05pm-5:00pm

Solutions Session *– Location: Lone Star*

Presented by

FireEye
Next-Generation Threat Protection

Advanced Malware Analysis for Effective Incident Response

According to a recently released ISMG Incident Response survey, 60% of respondents rate their IR program as "reasonably" effective. Clearly, there is a fundamental disconnect between the advanced, evolving threat landscape and the traditional security defenses in which organizations have invested in and come to rely on. The reality is, despite huge investments in people and technology to deploy defense-in-depth, layered security, breach prevention typically fails – causing enterprises to suffer major system downtime, significant theft of data, or even measurable financial loss. Supplementing traditional security defenses with advanced technology that provides greater insight, timeliness and accuracy, the FireEye Advanced Threat Protection Platform creates a comprehensive incident response methodology that delivers key benefits across the entire incident response lifecycle. Don't settle for reasonably effective. Ensure you have the right tools and forensics to achieve "very effective" IR.

Ron Nguyen*, Managing Principal Consultant, FireEye Labs, FireEye, Inc.*

5:00pm-6:00pm

TRACK 1 – CAPITAL BALLROOM A

Hunting Attackers with Network Audit Trails

Sophisticated, targeted attacks have become increasing difficult to detect and analyze. Attackers can employ 0day vulnerabilities and exploit obfuscation techniques to evade detection systems and "fly under the radar" for long periods of time. Reports cataloging trends in data breaches reveal a systematic problem in our ability to detect that they ever occurred. Gartner estimates 85% of breaches go completely undetected and 92% of the detected breaches are reported by third parties. New strategies for identifying network attack activity are needed.

The purpose of the session is to review how network logging technologies such as NetFlow and IPFIX can be applied to the problem of detecting sophisticated, targeted attacks. These technologies can be used to create an audit trail of network activity that can be analyzed, both automatically and by skilled investigators, to uncover anomalous traffic. We will demonstrate how to these records can be used to discover active attacks in each phase of the attacker's "kill chain." We will also cover how these records can be utilized to determine the scope of successful breaches and document the timeline of the attacks.

The session will demonstrate these processes and techniques in both open source and commercial solutions.

Tom Cross - *Security Researcher, Lancope*
Charles Herring - *Security Researcher, Lancope*

TRACK 2 – CAPITAL BALLROOM B

Panel: Women in DFIR

This panel focuses on *"Solutions That Work For Getting More Women Into DFIR"*, bringing together four highly accomplished professionals to share their insights into "what works" and "what doesn't" in bringing more women into our field. Spanning diverse sectors of the digital forensics community, from consulting services to federal and law enforcement communities, our panelists bring unique perspectives to a complex, long-standing issue.

Alissa Torres*, SANS Institute (Moderator)*
Stacey Edwards*, Forensic Analyst, The Sylint Group*
Sarah Edwards*, Digital Forensics Analyst, Harris Corporation*
Detective Cindy Murphy*, City of Madison, WI*
Wendi Rafferty*, VP – Professional Services, CrowdStrike*

6:00pm-6:30pm

Forensic 4Cast Awards – *Location: Lone Star*

This lively awards presentation recognizes excellence and leadership in forensics, as voted upon by the readers of the popular Forensic 4cast blog. Categories include:

- Computer Forensic Hardware Tool of the Year
- Digital Forensic Article of the Year
- Phone Forensic Software Tool of the Year
- Digital Forensic Podcast of the Year
- Digital Forensics Book of the Year
- Computer Forensic Software Tool of the Year
- Digital Forensic Blog of the Year
- Phone Forensic Hardware Tool of the Year
- Digital Forensic Organization of the Year
- Digital Forensic Examiner of the Year

Lee Whitfield - *Director of Forensics at Digital Discovery - http://forensic4cast.com*

6:30pm-8:30pm

Networking Reception – *Location: The Atrium*

Presented by

FireEye
Next-Generation Threat Protection

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

Wednesday, July 10

7:00am-8:30am

Registration – *Location: 2nd Floor Foyer*

8:30am-9:30am

Finding Malware Like Iron Man

When confronted with a system impacted by unknown malware time is of the essence. Triage needs to be done, information technology units need guidance, and the business needs to get back up and running. Questions have to be answered quickly: is the system infected, what malware is involved, and how did the infection occur in the first place. The available triage options all take time: scanning with antivirus, dumping and analyzing memory, performing live analysis, or performing a full post mortem examination. Mass malware makes triage even more challenging with new variants being released at a pace faster than signatures and IOCs are generated.

This presentation discusses how to perform triage on a system infected with malware in three examination steps. Within minutes not only can the majority of malware be detected but the initial infection vector can be identified as well. Topics will include: malware indicators, program execution artifacts, auto-start extensibility points (ASEPs) artifacts, and NTFS artifacts and then there will be a mock case study tying everything together.

Corey Harrell *- IT Specialist III, New York Office of the State Comptroller*

9:30am-10:30am

TRACK 1 – CAPITAL BALLROOM A

Detecting data loss from cloud synchronization applications

Cloud backup solutions, such as Dropbox, provide a convenient way for users to synchronize files between user devices. These services are particularly attractive to users, who always want the most current version of critical files in each location. Many of these applications "install" into the user's profile directory and the synchronization processes are placed in the user's registry hive (HKCU). Users without administrative privileges can use these applications without so much as popping a UAC dialog. This freedom makes illicit installations of these applications all the more likely. Cloud backup providers are marketing directly to corporate executives offering services that will "increase employee productivity" or "provide virtual teaming opportunities." Offers such as these make it more likely than ever that any given corporate environment has some cloud backup solutions installed.

Jake Williams *- Principal Consultant, CSRgroup Computer Security*

TRACK 2 – CAPITAL BALLROOM B

A Day in the Life of a Cyber Tool Developer

As the density of digital media continues to grow, the forensic investigator will see massive amounts of data during any acquisition phase or computer analysis. Timely reduction and processing of large, disjointed datasets will be extremely important for those investigative shops that face more work than the number of available, qualified people doing the analysis. This means automating the workflow process to ensure consistent, accurate reporting which will in turn translate into more revenue for the investigator. To aid in this, forensic development shops will need to use and/or create toolsets that are flexible and scalable to assist in any automation transition.

This talk will focus on how TZWorks takes on the challenge of developing a tool to aid in this automation process. The discussion will be centered on a TBD tool that has been developed in the past. It will include:(a) the step by step process used in the development and where key decision points were made, (b) the research that was involved when identifying critical data structures, and (c) how it was decided which data will be presented to the end user and which data will not. This discussion will be from a developer's perspective.

Jonathan Tomczak *– Chief Information Officer, TZWorks, LLC*

10:30am-11:00am

Networking Break and Vendor Expo – *Location: Capital Ballroom Foyer*

11:00am-12:00pm

TRACK 1 – CAPITAL BALLROOM A

Proactive Defense

By nature, computer network defenders tend to be very reactive - an IDS alert triggers and they take action. This can quickly cause a defense team to become overwhelmed with things they need to react to, causing them to miss key indicators. Proactive network defense allows defenders to look at the threat landscape to proactively anticipate where the adversary will be in-order to defend against an attack before it happens. Today we collect large volumes of data on our enterprises. This massive amount of data, coupled with defenders who are focusing on technical analysis and typically do not have the background or experience in traditional intelligence discipline, inhibits thinking proactively.

This presentation is tailored towards technical analysts who want to learn about intelligence collection and analysis and how to couple it with technical analysis in-order to mine the myriad of data to extract powerful information about the adversary such as their Tools, Techniques, and Practices (TTP). As this data is extracted, the audience will learn to start asking proactive questions about the data so that they may anticipate the adversary's next move and begin the defense in advance. This presentation will provide background on intelligence collection, intelligence analysis, building a collection, and introduce some powerful tools to mine intelligence.

***Jason Geffner**, Senior Security Researcher, CrowdStrike, Inc.*

TRACK 2 – CAPITAL BALLROOM B

The 7 Sins of Malware Analysis

In this presentation, I will discuss the common mistakes that analysts make when working with malicious code. Each of these 'sins' will be presented along with their corollary 'what to do instead'. I hope to give new analysts a head start so they don't make some of the newbie mistakes that can happen, as well as remind experienced analysts of some of the important characteristics that make for good analysis.

***Dominique Kilman**, Malware Analyst, KPMG LLP*

12:00pm-1:20pm

Lunch & Learn – *Location: Lone Star*

Presented by

GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

Large Scale Breach Investigations- Lessons Learned

Come and join Vice President of Cybersecurity Services Jim Jaeger to learn about trends that have been identified in recent breach investigations involving financial institutions and the payment card industry. Jim will be discussing evolving attack techniques employed in financial breaches and how to guard your network against advanced threats.

***Jim Jaeger**, Vice President of Cybersecurity Services*

1:20pm-2:10pm

TRACK 1 – CAPITAL BALLROOM A

Plaso– Reinventing the Super Timeline

Timeline analysis has really grown in the past few years with new tools that can automate the correlation between multiple data sources into a single timeline. This analysis technique has provided the analyst with a completely new and unprecedented view of the data that lies on the drive.

And with the introduction of the new log2timeline engine called plaso things are even changing more. The next generation of log2timeline produces more structured data with more features, which in turns opens up new ways of analyzing the massive dataset the tool extracts from any given drive.

The goal of this presentation is to introduce the audience to timeline analysis in a practical way, showing how to use the tool in a simple malware intrusion investigation as well as to show how to expand the tool to parse new datasets in a simple way.

Kristinn Gudjonsson *– Senior Security Engineer, Google*

TRACK 2 – CAPITAL BALLROOM B

Facilitating Fluffy Forensics (a.k.a. Considerations for Cloud Forensics)

Cloud computing enables the rapid deployment of servers and applications, dynamic scalability of system resources, and helps businesses get products to market faster than ever before. Most organizations are aware of the benefits of adopting cloud architectures and many are becoming aware of the potential security risks. The majority of organizations, however, don't realize the numerous challenges of conducting incident response (IR) activities and forensic investigations across public, private, and hybrid cloud environments.

It's not all doom and gloom, however. The consumption model of cloud architectures actually lends itself to helping investigators conduct forensic and IR exercises faster and more efficiently than on a single workstation. For this to happen, however, the tools and techniques employed must evolve.

In this session, CloudPassage Chief Evangelist Andrew Hay will address the forensic and IR challenges of investigating servers and applications in cloud environments in addition to the opportunities that cloud presents to help expedite forensic investigations. Topics that will be discussed include:

- Traditional forensics and IR
- Cloud architectural challenges for responders
- Chain-of-custody and legal issues across architectures and regions
- How existing forensics/IR tools can help - and what they can do better
- Advantages of conducting forensics/IR in cloud environments

Andrew Hay *- Chief Evangelist, CloudPassage, Inc.*

2:10pm-3:00pm

TRACK 1 – CAPITAL BALLROOM A

Timeline creation and review, GUI style!

Timeline analysis is a concept used by Digital Forensic and Incident Response practitioners to normalize event data by time and present it in chronological order for review. This sequence of data is used to tell a narrative "story" of events over a period of time. Furthermore, it can be used to put events into context, interpret complex data and identify anomalies or patterns.

Thanks to tools like log2timeline the creation of timeline data is easy, however the review process can be challenged by gigabytes and millions of rows of events. This presentation will focus on making the creation of timeline data even EASIER and challenges of reviewing large timeline data sets using a FREE tool called, l2t_R, a cross-platform GUI solution specifically designed for reviewing timeline data.

David Nides*, Manager, Forensic Technology Services KPMG LLP*

TRACK 2 – CAPITAL BALLROOM B

Building, Maturing, and Rocking a Security Operations Center

I will discuss key items around building a security operations center and maturing it. Initially working through points on the importance of process and procedures, how to document and options to store and actively use documentation. I will discuss hiring, on-boarding and training analysts and monitoring technology and data feed on-boarding. After having a SOC in place, there are items you start to discuss around maturing the processes, incident response within the SOC and the interactions with internal and external organizations. The last section will cover incident response, daily reactions to users, noise, etc and a "rocking" example of one of our responses to a virus outbreak – going from detection, impact and a hack back response the SOC analysts used to shut it down. I will use the SANS Incident Response Model walking through the steps and how we made decisions and handled the issue. The reason I have chosen this virus outbreak is because, while dealing with the big things (intruders, etc) end up involving a lot of folks and get the visibility, sometimes the nuisance things are the hardest to get visibility internally from other groups but the security teams have to address regardless and offers an example of how to handle things when other groups aren't as invested.

Brandie Anderson *- Manager, Security Operations Center and Security Delivery Operations, Hewlett-Packard*

3:00pm-3:20pm

Networking Break and Vendor Expo – *Location: Capital Ballroom Foyer*

3:20pm-4:10pm

TRACK 1 – CAPITAL BALLROOM A

ICS, SCADA, and Non-Traditional Incident Response

INTRODUCTION:

With the attack landscape constantly changing, new focus has been placed on industrial control systems (ICS) and SCADA systems. This talk aims to show not only a high level overview of ICS and SCADA systems, but also shows how to effectively perform incident response in these often times remote systems.

CORE CONCEPTS:

Core concepts that will be covered include, but are not limited to:

- How ICS/SCADA systems differ than normal systems.
- Core overview of ICS/SCADA overview. (Common uses for these systems)
- Reasons behind ICS/SCADA systems.
- How ICS/SCADA differs in terms of incident response.
- How to effectively perform incident response on ICS/SCADA systems.

GOALS:

Goals that are included, but are not limited include:

- Help conference goers understand core incident response subjects.
- Help conference goers understand what ICS/SCADA systems are used for.
- Help conference goers be able to differentiate between ICS/SCADA incident response and traditional incident response.
- Help conference goers leave the conference with core notes on being able to easily perform incident response on ICS/SCADA systems.

Kyle Wilhoit *- Threat Researcher, Trend Micro*

TRACK 2 – CAPITAL BALLROOM B

Restoring Credential Integrity after an Enterprise Intrusion

One of the most important, and most overlooked, steps of running an enterprise APT intrusion investigation involves the rapid identification of risk factors that enabled the threat actors to establish an enterprise presence in that environment. One of these risk factors is related to Active Directory and local system user credentials. Investigators must rapidly determine the status of these factors from an investigative perspective to eventually help the organization restore credential integrity with a hard password reset. We will discuss how to rapidly determine which user, admin, and service accounts have active or historical LanManager password hashes, which user accounts share credentials, which domain administrators share credentials between their standard and privileged accounts, and other factors related to user credential risk. We will demonstrate the tools and techniques we currently use, identify common pitfalls, and will include a couple of enterprise hard password reset case studies

James Perry *- Lead Associate, Booz Allen Hamilton*

Anuj Soni *- Lead Associate, Booz Allen Hamilton*

4:10pm-5:10pm

DFIR SANS360

In one hour, 10 Digital Forensics and Incident Response experts will discuss the coolest forensic technique, plugin, tool, command line, or script they used in the last year that really changed the outcome of a case they were working. If you have never been to a lightning talk it is an eye opening experience. Each speaker has 360 seconds (6 minutes) to deliver their message. This format allows SANS to present 10-12 experts within one hour, instead of the standard one presenter per hour. The compressed format gives you a clear and condensed message eliminating the fluff. If the topic isn't engaging, a new topic is just 6 minutes away.

- ***Don't Be a Script Kiddie*** *- Kyle Maxwell, Verizon*
- ***Incident Readiness - Top 10 Keys to a Successful Forensic Investigation*** *- J Jewitt*
- ***Social Media Forensics*** *- Brian Lockrey*
- ***Finding Evil Everywhere: Combining Host-Based and Network Indicators*** *- Alex Bond*
- ***Chasing Malware, Not Rainbows*** *- Frank McClain*
- ***Raising Hacker Kids*** *- Joseph Shaw*
- ***Fighting Your Dragons*** *- Hal Pomeranz*
- ***A Decade of Trends in Large-Scale Financial Cyber Breaches*** *- Jim Jaeger*
- ***Reconstructing Reconnaissance*** *- Mike Sconzo*
- ***Advanced Procurement Triage*** *- Michael Ahrendt*

5:10pm-5:30pm

Summary & Closing Remarks

Rob Lee *&* ***Alissa Torres*** *– Summit Co-Chairs, Digital Forensics and Incident Response Summit*

Thank you for attending the Digital Forensics & Incident Response Summit.

Please remember to complete your speaker evaluation for today.

You may leave completed surveys at your seat or turn them in to the SANS registration desk.

Exhibitors

Austin HTCIA

The High Technology Crime Investigation Association (HTCIA) was formed to provide education and collaboration to our global members for the prevention and investigation of high tech crimes. The Austin Chapter of the HTCIA was formed in 1996. The headquarters for this Chapter is Austin; however, members are located throughout Texas.

Access Data

130,000+ users rely on AccessData, the maker of FTK, SilentRunner and the CIRT platform. CIRT integrates computer, network and malware analysis, data auditing, and remediation into a single solution. It integrates with SIEM/SIM tools to enable automated rapid response and also allows you to detect threats your alerting tools miss. **www.accessdata.com**

Cellebrite

Since 2007, the Cellebrite UFED has provided mobile forensics solutions to investigative professionals worldwide. The UFED enables extraction, decoding and analysis of data and passwords from thousands of legacy and feature phones, smartphones, portable GPS devices, and tablets. Visit the Cellebrite exhibit or online at **www.ufedseries.com** to learn more.

Crowd Strike

CrowdStrike is a security technology company focused on identifying and preventing damage from targeted attacks. Utilizing Big-Data technologies and Active Defense, we have technology, intelligence, and services offerings to solve today's most demanding cyber-security challenges. Our core mission is to fundamentally change how organizations implement and manage security in their environment.

FireEye

FireEye® has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection against the next generation of cyber attacks. The FireEye platform provides real-time, dynamic threat protection without the use of signatures to protect across the primary threat vectors, including web, email, and files.

General Dynamics Fidelis Cybersecurity Solutions

General Dynamics Fidelis Cybersecurity Solutions provides organizations with a robust, comprehensive portfolio of products, services, and expertise to combat today's sophisticated advanced threats and prevent data breaches. Our customers can face advanced threats with confidence through use of our Network Defense and Forensics Services and Fidelis XPS™ Advanced Threat Defense Products.

Guidance Software

Guidance Software is the worldwide leader in digital investigations. Government agencies and Fortune 100 corporations use EnCase® Enterprise for network-wide digital investigations. Built on EnCase Enterprise are EnCase® eDiscovery, EnCase® Analytics, and EnCase® Cybersecurity, helping organizations with e-discovery, security intelligence, and rapid incident response. For more information, visit **www.guidancesoftware.com**.

Trend Micro

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our solutions for consumers, businesses and governments provide layered data security to protect information on mobile devices, endpoints, gateway, servers and the cloud. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. All of our solutions are powered by a cloud-based global threat intelligence data mining framework, the Trend Micro™ Smart Protection Network™ infrastructure, and are supported by over 1,200 threat experts around the globe. For more information, visit **TrendMicro.com**.

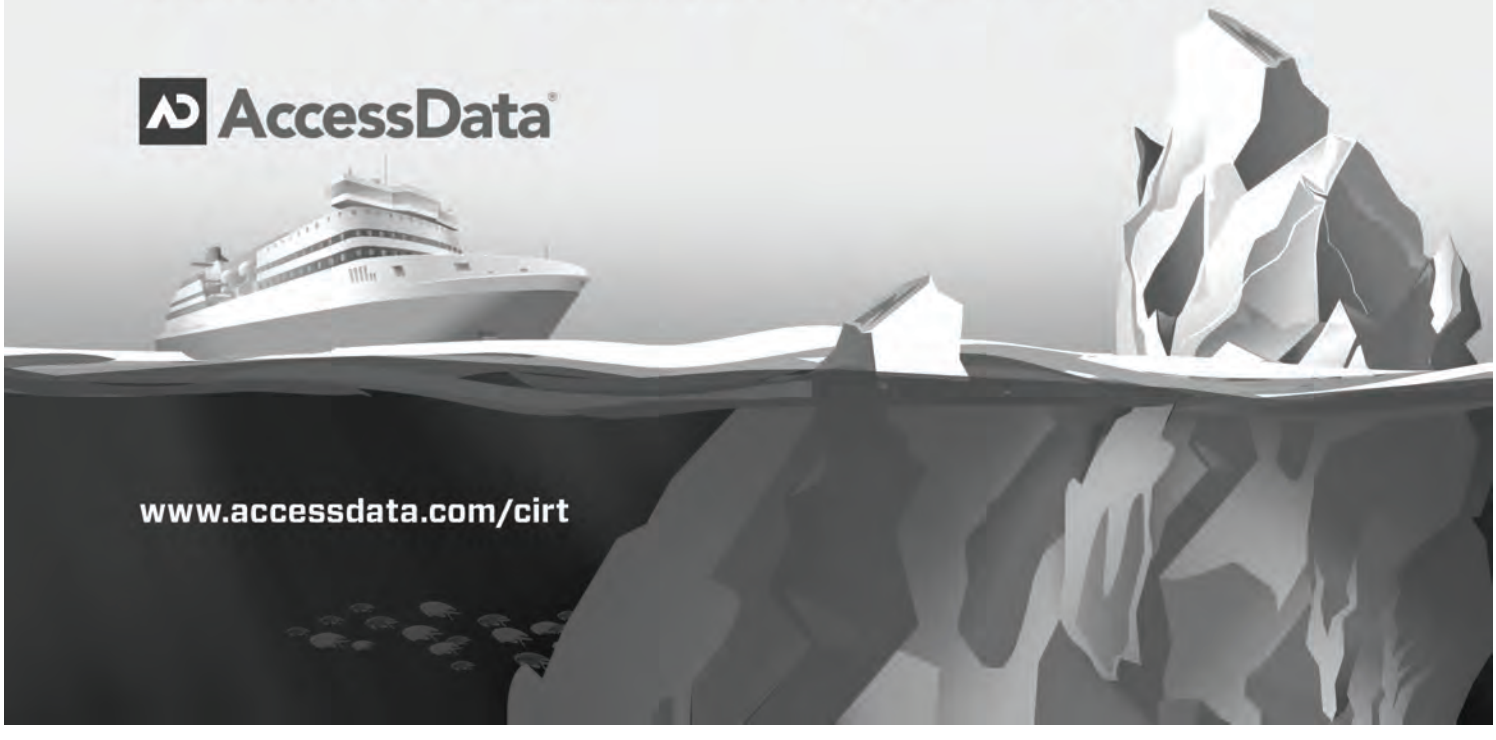
WHAT YOU DON'T KNOW
CAN HURT YOU.

The traditional cyber security infrastructure is riddled with blind spots... resulting in threats you can't see, because the tools you're relying on can't see them. Cyber Intelligence & Response Technology (CIRT) is designed to eliminate your blind spots, allowing you to catch the data leakage your DLP misses, detect the new malware your IDS and antivirus don't recognize, and even monitor Internet activity of employees when they are not logged into your network.

Integrating computer, network and malware analysis, large-scale data auditing and remediation, the CIRT platform fills the detection, analysis and remediation gaps that currently exist in the typical information security architecture. With CIRT you're able to see all critical analysis through a single pane of glass, perform batch remediation to stop the bleeding at the first sign of a breach, and create threat profiles to prevent threat recurrence. Furthermore, it's a virtual war room, in which multiple cyber security teams can collaborate in real time.

Eliminate Your Cyber Security Blind Spots

AccessData®



www.accessdata.com/cirt

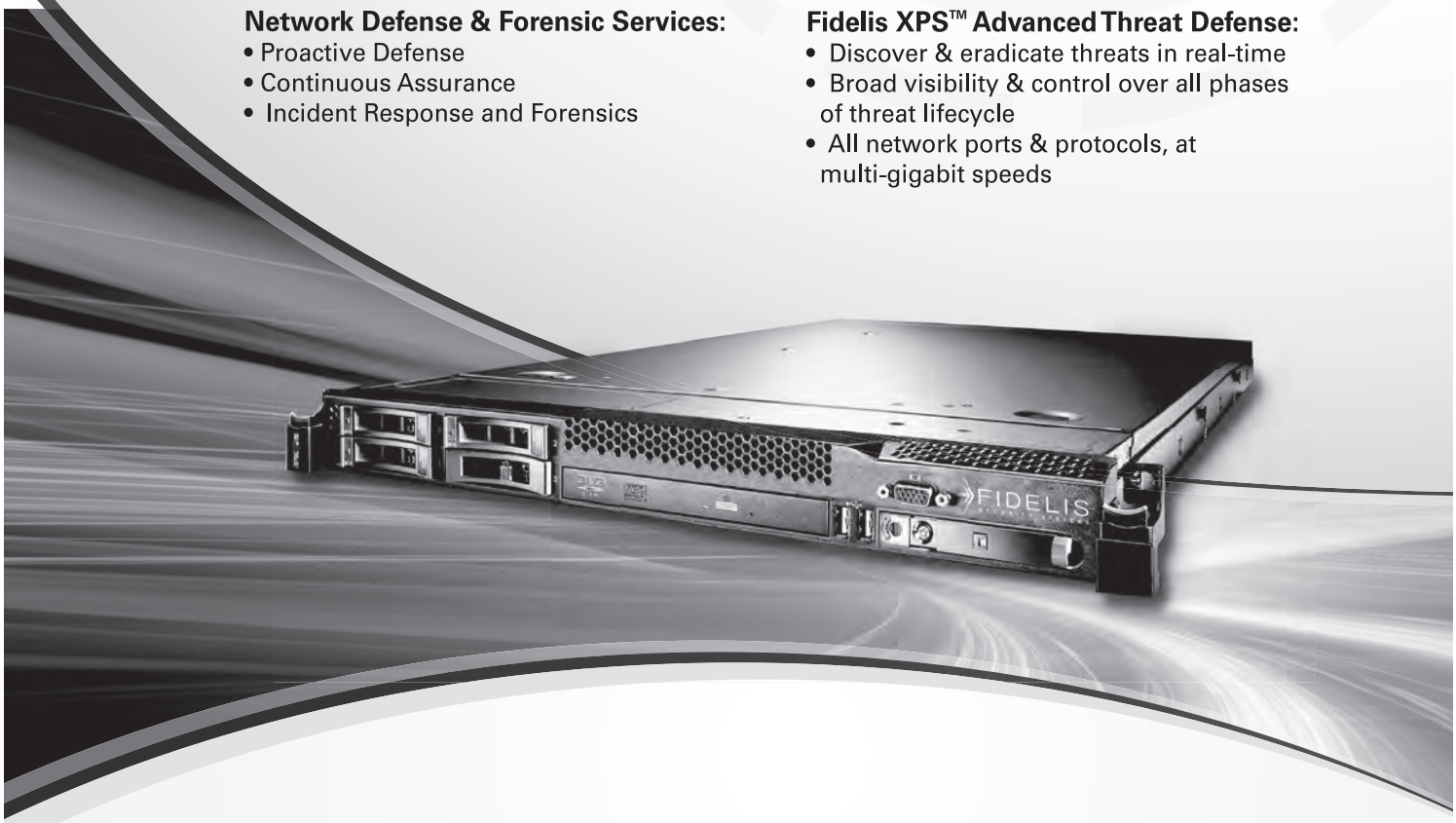
GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

Face Advanced Threats with Confidence

A powerful combination of Products, Services, and Expertise to combat today's sophisticated advanced threats

Network Defense & Forensic Services:
- Proactive Defense
- Continuous Assurance
- Incident Response and Forensics

Fidelis XPS™ Advanced Threat Defense:
- Discover & eradicate threats in real-time
- Broad visibility & control over all phases of threat lifecycle
- All network ports & protocols, at multi-gigabit speeds



FIDELIS XPS

CROWDSTRIKE FALCON PLATFORM

Adversary Intelligence Subscription

In today's threat environment, adversaries are constantly profiling and attacking your corporate infrastructure to access and collect your intellectual property, proprietary data, and trade secrets. CrowdStrike Intelligence provides your organization with detailed technical and strategic analysis of adversary capabilities, indicators and tradecraft, attribution and intentions.

Combat targeted attacks and advanced adversaries with actionable security-driven intelligence.

- CrowdStrike Intelligence Reporting
- Actionable Intelligence Feeds and Indicator Data
- Malware Identification
- Flash Reporting
- CrowdStrike Adversary Profile Library
- Quarterly Executive Intelligence Briefings
- Expert Support

DOWNLOAD A SAMPLE REPORT NOW!
www.crowdstrike.com/deeppanda

CROWDSTRIKE

YOU DON'T HAVE A MALWARE PROBLEM, YOU HAVE AN ADVERSARY PROBLEM.™

Are you up to the challenge?

01000011011011110110110001101100011000010110001001101111011100100110000101110100011001010010111000100000010010110110111001101111011101110110110001100100011001000111011101101001011001000110010100101110000011010000101001000010011001010110001101101111011010110011010000000110000100100000011010110010101101101011000100110010101110010001000000111010001101111011001000011000010111100100101110000011010000101001

http://www.htcia.org/

UPCOMING SUMMITS & TRAINING COURSES

2013

Industrial Control Systems Security Training
Washington, DC | August 12-16

Critical Security Controls Summit
Washington, DC | August 12-18

Digital Forensics and Incident Response Summit & Training
Prague, Czech Republic | October 6-12

Securing the Internet of Things Summit
San Francisco, CA | October 22

Healthcare Summit
San Francisco, CA | October 22-23

Pen Test Hackfest Summit & Training
Washington, DC | November 7-14

Asia Pacific ICS Security Summit
Singapore | December 2-7

2014

AppSec Summit & Training
Austin, TX | February 3-8

Industrial Control Systems Security Summit & Training
Orlando, FL | March 12-18

Digital Forensics & Incident Response Summit & Training
Austin, TX | June 3-10

For more information on speaking at an upcoming summit or sponsorship opportunities, e-mail SANS at **summit@sans.org**.
Visit **www.sans.org/summit** for detailed summit agendas as they become available.

Save the Date!

SANS Forensics and Incident Response SUMMIT

AUSTIN, TEXAS

June 3-10, 2014

COURSES OFFERED:

FOR408
Computer Forensic Investigations – Windows In-Depth
GIAC CERT: GCFE

FOR508
Advanced Computer Forensic Analysis & Incident Response
GIAC CERT: GCFA

FOR526
Windows Memory Forensics In-Depth

LEARN R.E.M.

FOR610
Reverse-Engineering Malware: Malware Analysis Tools and Techniques
GIAC CERT: GREM

AND MORE!