SANS

SUMMIT SERIES 2008

WHAT WORKS

Incident Response and Forensic Solutions

Cyber Threats • Data Breaches

TABLE OF CONTENTS

SANS SUMMIT SERIES 2008 WHAT WORKS

Incident Response and Forensic Solutions

Cyber Threats • Data Breaches

Expert Briefing: The Forensic and IR Counterinsurgency Field Manual
Rob Lee, SANS Fellow

Expert Briefing: Upping the "Anti": Using Memory Analysis to Fight Malware
Aaron Walters, Volatile Systems

IR/Forensic Team Tactics Panel - The best incident response and forensic techniques while responding to a data breach
Harlan Carvey, IBM ISS; Kris Harms, Mandiant; Ken Bradley, Mandiant; Chris Novak, Verizon Cybertrust; Stan Kang, Verizon Cybertrust; Mike Poor, Intelguardians; Tom Liston, Intelguardians

Expert Briefing: iPhone Forensics
Steve Whalen, Forward Discovery

Government and Defense Industrial Branch Panel - Successful strategies in responding and mitigating enterprise level intrusion investigations
Ovie Carroll, DOJ; Monty McDougal, Raytheon; George Bakos, Northrop Grumman; Michael Cloppert, Lockheed Martin; Jennifer Kolde, FBI; Kevin Rivera, DC3; Henri Vangoethem, Mantech

Solution Provider and Vendor Panel: Demonstrations of the latest enterprise and host response and forensic tools to combat sophisticated threats

Expert Briefing: "Slaying the Red Dragon: Countering the China Cyber Threat"
Ken Bradley, Mandiant; Wendi Rafferty, Mandiant

Expert Briefing: Law Enforcement Trends and the Future of Computer Forensics and Incident Response
Ovie Carroll, DOJ

IR/Forensic Team Strategy Panel - Incidents Gone Wrong! How can you prepare better for potential compromise? Case studies of organizational best/worst practices
Harlan Carvey, IBM ISS; Kris Harms, Mandiant; Ken Bradley, Mandiant; Chris Novak, Verizon Cybertrust; Stan Kang, Verizon Cybertrust; Mike Poor, Intelguardians; Tom Liston, Intelguardians; Brett Padres, Stroz Friedberg LLC

Expert Briefing: "Applying Security Intelligence to Drive Incident-Handling"
Bryan Sartin, Verizon Cybertrust

Expert Briefing: Using the Home Advantage: Combating Anti-Forensics and Linkage Blindness
Eoghan Casey, Handbook of Computer Crime Investigation, Johns Hopkins University Information Security Institute; Chris Daywalt, CSC

Secrets of Registry Analysis Revealed
Harlan Carvey, IBM ISS author of Windows Forensic Analysis

Vendor Panel: Tools Shootout. Vendors discuss and compare capabilities to investigate and analyze enterprise threats in an open forum where audience participation leads the discussion.

Presentations released for publication and not found on this CD may be accessed at: http://files.sans.org/summit/forensics08/