SANS What Works in Cyber Threat Intelligence Summit

March 22, 2013
Washington, DC

The Cyber Threat Intelligence Summit strives to bring you the most up-to-date thinking on the hottest topics.
As a result, the agenda is dynamic and subject to change. Please check back for updates.

Time	
7:00am - 8:00am	**Registration**
8:20am - 8:30am	**Welcome and Introduction** Mike Cloppert & Rob Lee – Summit Co-Chairs Cyber Threat Intelligence is generally understood to be the collection of information about external threat actors and active external threats.
8:30am - 9:30am	**Keynote** **The Evolution of Cyber Threats and Cyber Threat Intelligence** The presentation will address the history of our understanding of the cyber threat landscape and provide perspective on the role of cyber threat intelligence in addressing ever evolving cyber threats. The presentation will address the role of tactical threat intelligence in response to threats and the challenges of relating threats to operational risks and conducting strategic estimative intelligence. The presentation will highlight the value of cyber threat intelligence for enterprises and how to leverage intelligence to improve cyber defense. The attendees will learn why intelligence is a crucial part of cyber defense at all levels. **Speaker:** Greg Rattray, Chief Executive Officer, **Delta Risk LLC** **Presenter Biography:** As CEO and founding partner in Delta Risk, Dr. Rattray brings an exceptional record in establishing strategies for cyber security and risk management for clients across both the government and private sectors. He also serves as the Senior Security Advisor for BITS/The Financial Services Roundtable. During his 23 year Air Force career, he served as the Director for Cyber Security on the National Security Council staff in the White House where he was a key contributor to the President's *National Strategy to Secure Cyberspace*, initiated the first national cyber security exercise program involving government and the private sector, and coordinated the interagency activities related to international engagement on cyber security issues. Greg also commanded the Operations Group of the AF Information Warfare Center and served in other command and staff positions. In this role, he was initiated AF and DOD programs for collaboration with defense industrial base partners related to advanced persistent cyber threats and established the AF network warfare training, cyber security tactics and cyber exercise programs. He also served from 2007-2010 as the Chief Security Advisor to Internet Corporation for Assigned Names and Numbers (ICANN) establishing the ICANN strategy for enhancing security and resiliency of the domain name system. He was the driving force in the establishment of the Cyber Conflict Studies Association founded to ensure U.S. and international cyber security thinking are guided by a deeper well of intellectual capital involving private industry, think tanks, government and academia and serves as the Association's President. Dr. Rattray is a Full Member of the Council on Foreign Relations. He received his Bachelor's Degree in Political Science and Military History from the U.S. Air Force Academy; a Master of Public Policy from the John F. Kennedy School of Government, Harvard University; and his Doctor of Philosophy in International Affairs from the Fletcher School of Law and Diplomacy, Tufts University. He is the author of the seminal book *Strategic Warfare in Cyberspace* as well as numerous other books and articles related to cyber and national security.

9:30am - 10:30am	**If It Bleeds, We Can Kill It: Leveraging Cyber Threat Intelligence to Take the Fight to the Adversary** In perhaps the greatest film ever made, Arnold Schwarzenegger's elite team of Special Forces operators is pitted against an alien adversary who outmatches them in nearly every encounter. Hopelessly outmatched, Dutch must change his tactics to ultimately defeat the Predator. Enterprises are at a similar point; one look at the headlines makes this painfully clear. Cyber Threat Intelligence (CTI) has emerged as a new capability that enterprises can leverage to become proactive in protecting their environments. This timely and fast-paced talk will cover: • Why you might not be ready for CTI • Building versus buying CTI capabilities • The vendor landscape for CTI • Intelligence sharing and operational security **Speaker:** Rick Holland, Senior Analyst, **Forrester Research** **Presenter Biography:** Rick Holland is a Sr. Analyst at Forrester Research where he serves security and risk professionals. Rick works with information security leadership providing strategic guidance on security architecture, operations and data privacy. His research focuses on incident response, threat intelligence, email and web content security as well as virtualization security. Prior to joining Forrester, he was a Solutions Engineer where he architected enterprise security solutions. Previously, he worked in both higher education and the home building industry, where he focused on intrusion detection, incident handling and forensics. He is regularly quoted in the media and is a frequent guest lecturer at the UT Dallas. Rick holds a B.S. in Business Administration from UT Dallas.
10:30am -10:50am	**Networking Break**
10:50am – 11:50am	**Expert CTI User Panel: Best Practices in creating, delivering, and utilizing Cyber Threat Intelligence for your organization** We've pulled together some of the key, thought leading analysts that have years of experience supporting some of the world's biggest enterprise networks, the US Department of Defense, and Intelligence communities in detecting and defending against sophisticated, nation-state caliber adversaries. Many of the panelists have been respected colleagues of mine for years, and although you may not have ever met or heard of them, they have each played an instrumental role in ensuring the security of our country's economic, military, and geopolitical interests. Their collective past and present experiences in using CTI will draw from past and present experiences with the DoD Cybercrime Center (DC3), the DoD's Joint Task Force for Global Network Operations (JTF-GNO), General Electric, Google, and various organizations within the intelligence community. I can't wait fo you to hear what they have to share with you about creating, delivering, and utilizing CTI. --Michael Cloppert **Moderator:** Michael Cloppert, **Lockheed Martin** **Panelists:** Rich Barger, Chief Intelligence Officer, **CyberSquared** Chris Sperry**, Lockheed Martin** Shane Huntley, Threat Analysis Group, **Google** Andre Ludwig, **Neustar** Aaron Wade, Senior Team Leader – GE Cyber Intelligence, **General Electric Co.**
11:50am- 1:00pm	**Lunch Break**
1:00pm – 2:00pm	**Building and Operating a Cyber Threat Intelligence Team**

	Building a response capability to Advanced Persistent Threats involves integration of people, process, technology acquisition and development, organizational structure, communications, and partnerships in a way that enables even large enterprises to be agile and responsive in order to leverage intelligence for effective computer network defense. Although all of these elements may exist in a conventional incident response team, Lockheed Martin's threat-oriented focus causes these elements to manifest differently in what is largely an intelligence operation. In this talk, participants will hear how each of these elements is shaped by cyber threat intelligence, and how their careful orchestration is achieved, by the Senior Manager charged with protecting the world's largest defense contractor from computer network exploitation. Also discussed will be methods to evaluate the maturity of one's own threat intelligence organization, and paths for quick evolution to counter sophisticated adversaries. **Speaker:** Mike Gordon, CIRT Senior Manager, **Lockheed Martin** **Presenter Biography:** Mr. Gordon has over thirteen years of experience in the information security field supporting the Defense Industrial Base, and has also been a security consultant for Public, Health and Financial sectors. Mike is currently the Senior Manager of the Computer Incident Response Team (CIRT) for Lockheed Martin Corporation. The CIRT is responsible for all protection, detection and response capabilities used in the defense of Lockheed Martin networks enterprise-wide. The team's scope of work includes coordination and collaboration with the government and industry partners to handle a wide variety of events related to security intelligence, incident response, intrusion detection, risk mitigation, and digital forensics support. Mike joined Lockheed Martin in 1997 and has since held multiple positions within the Corporation supporting the Aeronautics Business Area and Corporate Information Security. Mike has received the Lockheed Martin NOVA Award, the corporation's high recognition in 2010 and 2011 for Cyber Security programs.
2:00pm – 3:00pm	**Creating Threat Intelligence: Tools to Manage and Leverage Active Threat Intelligence** Presenting raw data in a way that makes relevant connections obvious and easy to follow has been a major challenge in cyber threat intelligence. Too often, important details find themselves buried in unstructured and unsearchable formats where analysts cannot effectively use them. This talk will discuss two tools - Chopshop and CRITs - that attack this problem and how analysts use them to understand and track sophisticated cyber threats. **Speaker:** Reid Gilman, Senior Cyber Security Engineer, **MITRE Threat Intelligence Team** **Presenter Biography:** Reid Gilman works on cyber threat intelligence operations and research at The MITRE Corporation. He has experience in malware analysis, cyber threat intelligence and network traffic analysis and DPI and is a team lead in MITRE's Cyber Threat Analysis Cell. Reid has a B.A. from Carleton College and an M.S. from Northeastern University, both in computer science.
3:00pm – 3:20pm	**Networking Break**
3:20pm - 4:20pm	**Expert CTI Solutions Panel: Delivering Actionable Cyber Threat Intelligence as a Solution – What Works, Pitfalls, Costs, and Skills** Threat and vulnerability feeds by themselves do not produce Cyber Threat Intelligence – let alone create effective, affordable or actionable security advice. Creating an enduring "CTI as a Service" capability can enable a proactive approach to security but it takes a mixture of processes, tools, automation and architecture to assure security (and business) benefit. In this panel we will ask leading experts from firms that have been creating and delivering

	CTI services to their customers for years to provide detailed lessons learned with a "What Works" perspective. Come hear their advice and take home the knowledge to ensure success of your own CTI initiatives. **Moderator:** John Pescatore, Director of Emerging Security Trends, **SANS Institute** Panelists: Richard Bejtlich, **Mandiant** Rocky DeStefano, **Visible Risk** Adam Meyers, **CrowdStrike** John Ramsey, **SecureWorks**
4:20pm - 5:20pm	**Cyber Threat Intelligence SANS360** In one hour, 10 experts will discuss the Cyber Threat Intelligence and how they use it in their organizations. 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 experts within one hour, instead of the standard one Speaker 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. **360 Talks:** ▪ **Attribution: The Holy Grail or Waste of Time?** Billy Leonard, Security Engineer, Google ▪ **Cybersecurity at the NSA** Dave Hogue, Operations Lead, National Security Agency's NSA/CSS Threat Operations Center (NTOC) ▪ **Intelligence Driven Security In Action** Seth Geftic, Associate Director, Security Management & Compliance Group RSA, The Security Division of EMC ▪ **The Product of Intelligence** Sean Coyne, Security Solutions Director, Verizon/Terremark ▪ **Intelligence-Led Incident Response** Sean Catlett, VP – Operations, iSIGHT Partners ▪ **Exercising Analytic Discipline to Make Your Mission Relevant** Patton Adams, Senior Strategic & Counterintelligence Analyst, Northrop Grumman ▪ **Communication Between Teams for CTI** Enoch Long, Principal Security Strategist, Splunk ▪ **Crowdsourcing Threat Intelligence** Adam Vincent, Founder & CEO, Cyber Squared ▪ **Curating Indicators: Bringing Smarts to Intel** Douglas Wilson, Manager – Threat Indicators Team, Mandiant ▪ **Battlefield Intelligence - Turning Your Adversary's *Thwarted* Attacks into Attribution Gold** Anup Ghosh, PhD, Founder & CEO**,** Invincea ▪ **The Detection Timeline** Julie J.C.H. Ryan, Associate Professor, George Washington University

	Summary & Closing Remarks – Mike Cloppert & Rob Lee