Patton Adams, Senior Strategic and Counterintelligence Analyst, Northrop Grumman
Patton Adams comes to cyber threat intelligence analysis by way of studies in Foreign Service, ancient Cambodian epigraphy, library science, and various languages both human and machine; and through work in France, Taiwan, Indonesia, China, in the U.S. Army, and at his present company where he has engaged in intelligence and computer network defense for critically sensitive networks for close to fifteen years. His certifications include CISSP and GCFE.

Rich Barger, Chief Intelligence Office, Cyber Squared
Mr. Barger has over 15 years' experience supporting the Department of Defense and Intelligence Community. He currently supports Computer Network Operations community as a Senior Cyber Intelligence Strategist. Mr. Barger is also a founding member of The Center for Cyber Intelligence Analysis and Threat Research (cciatr.org) a 501c6 non-profit organization, which seeks to demonstrate leadership by developing common standards that promote cyber analytic methodologies and tradecraft for all practitioners, participant organizations and the community. Prior to Cyber Squared, Mr. Barger was a Senior Principal Consultant with Symantec Federal Consulting, Cyber Threat Analyst Program (CTAP). He is alumni of the Joint Task Force Global Network Operations, and the U.S. Army 1st Information Operations Command.

Richard Bejtlick, Chief Security Officer, Mandiant
Richard Bejtlich is Chief Security Officer at Mandiant. He was previously Director of Incident Response for General Electric, where he built and led the 40-member GE Computer Incident Response Team (GE-CIRT). Prior to GE, he operated TaoSecurity LLC as an independent consultant, protected national security interests for ManTech Corporation's Computer Forensics and Intrusion Analysis division, investigated intrusions as part of Foundstone's incident response team, and monitored client networks for Ball Corporation. Richard began his digital security career as a military intelligence officer in 1997 at the Air Force Computer Emergency Response Team (AFCERT), Air Force Information Warfare Center (AFIWC), and Air Intelligence Agency (AIA). Richard is a graduate of Harvard University and the United States Air Force Academy. He wrote "The Tao of Network Security Monitoring" and "Extrusion Detection," and co-authored "Real Digital Forensics." He also writes for his blog (taosecurity.blogspot.com) and Twitter (@taosecurity).

Sean Catlett, VP- Operations, iSIGHT Partners
Sean is the Vice President of iSIGHT Partners, Inc. running their commercial threat intelligence and cyber risk management business. Previous to that he was the CISO at Betfair in London, the world's biggest online betting community and one of the fastest and most resilient trading platforms available on the internet, where he rebuilt their security capability and helped the company manage a severe and now public cyber-attack. Sean joined Betfair from Barclays PLC where he was Global Head of Threat and Vulnerability Management for the Barclays Global Retail and Commercial bank. In that role he transformed the function by creating strategies and new capabilities in data loss prevention, information security and privacy incident response and security assessment. Prior to joining Barclays Sean was a Senior Vice President at Bank of America leading their global Security Monitoring and Response team.

Sean built a creative and innovative security R&D team which delivered millions of dollars in customer value year over year through detection of electronic fraud and attacks. Prior to financial services, he worked as the VP of Technology at Streamwaves, Inc. where he created a streaming music delivery system responsible for the world's first legal delivery of on-demand subscription streamed music from all 5 major record labels. Sean graduated with honors from University of Texas at Dallas with a B.S. in Business Administration.

Mike Cloppert, Chief Research Analyst, Lockhead Martin & Community Instructor, SANS Institute
Michael is the Chief Research Analyst for Lockheed Martin's CIRT (LM-CIRT), charged with collecting and managing intelligence on adversaries intent on stealing the organization's intellectual property, and development of new detection and analysis techniques. Michael has worked as a security analyst in various sectors including the Financial, Federal Government, and Defense industries. He has an undergraduate degree in Computer Engineering from the University of Dayton, an MS in Computer Science, and is currently pursuing a PhD in Systems Engineering from The George Washington University. Mike has received a variety of industry certifications including SANS GCIA, GREM, and GCFA, is a SANS Forensics and IR blog contributor, a SANS FOR610 instructor, and co-author of a seminal paper on Intelligence-driven Computer Network Defense.

Sean Coyne, Security Solutions Director, Verizon/Terremark
Sean Coyne(CCNA, Sec+, GWAPT, GPEN, RSA/CSE) is a Security Solutions Director with Verizon/Terremark, where he advises Federal customers on issues around cyber security. Over his career Sean has spent time penetrating networks, instructing federal agents, and performing forensic investigations for government and commercial clients. Prior to this he has worked for an elite handful of security and consulting firms serving intelligence & defense clients here and overseas. Sean was one of the first graduates of Penn State's Information Assurance program and has recently completed his graduate studies in the field of Cyber Intelligence.

Rocky DeStefano, CEO, VisibleRisk
Rocky DeStefano is an internationally respected security professional with 20 years of leadership in intelligence and security operations. He has led Enterprise Security, IncidentResponse and Intelligence Operations for multiple fortune 500 companies and US government agencies. Rocky has held key positions in several extremely successful security start-ups, including ArcSight, Decurity and NetWitness. He is currently the Founder and CEO of VisibleRisk, a growing Information Security company based out of Austin, TX.

Anup Ghosh, Ph.D., Founder & CEO, Invincea
Anup Ghosh, Ph.D., is Founder and CEO at Invincea. Prior to founding Invincea, he was a Program Manager at the Defense Advanced Research Projects Agency (DARPA) where he created and managed an extensive portfolio of cyber security programs. He has previously held roles as Chief Scientist in the Center for Secure Information Systems at George Mason University and as Vice President of Research at Cigital, Inc. Anup has published more than 40 peer-reviewed articles in cyber security journals. He is a frequent on-air contributor to CNN, CNBC, NPR and Bloomberg TV. A number of major media oultets carry his commentaries on cyber security issues including the Wall Street Journal, New York Times, Forbes, Associated Press, FoxNews and USA Today. He was awarded the NSA's Frank Rowlett Trophy for Individual Contributions in 2005 and the Secretary of Defense Medal for Exceptional Public Service for his contributions while at DARPA. He is currently a member of the Naval Studies Board and the Air Force Scientific Advisory Board, informing the future of American cyber-defenses.

Mike Gordon, CISSP, IAM/IEM, Senior Manager – CIRT, Lockheed Martin Corporation
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 Manger 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.

Prior to taking this position, Mike served as the Chief Security Architect for the Enhanced Security Initiative (ESI) and program manager for the Information Assurance - Baseline Security Program. In 2007 he received the Lockheed Martin Enterprise Operations Pinnacle Award for Technical Excellence for his work to reduce the impact of Advanced Persistent Threats on LM infrastructures. He also has experience as an IT consultant with Cap Gemini where he developed security architectures for multiple clients.

Mike represents Lockheed Martin to the Network Security Information Exchange (NSIE), and serves as the Vice-Chairman of the Board for the Defense Security Information Exchange (DSIE). He actively participates in the DoD/DIB Cyber Task Force Working Groups and is responsible for managing the corporation's relationship with the DC3 DoD/DIB Collaborative Information Sharing Environment (DCISE). Mike has been engaging in ongoing activities with the governments of the United Kingdom and Australia to facilitate multilateral, cross-sector information sharing.

Mike holds an undergraduate degree in Engineering Physics and Masters in Technical Management from Embry-Riddle Aeronautical University as well an MBA and Masters of Information Assurance degrees from the University of Dallas.

Rick Holland, Senior Analyst, Forrester Research
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 University of Texas at Dallas. Rick holds a B.S. in Business Administration MIS from UT Dallas. Rick is also a GIAC Certified Incident Handler (GCIH).

Dave Hogue, Operations Lead – NSA/CSS Threat Operations Center, National Security Agency
Dave Hogue represents the National Security Agency's NSA/CSS Threat Operations Center (NTOC), with experience in both the defensive and offensive cyber missions of NSA. He is slated to serve as a Director of Cybersecurity Operations (DCO) this summer in the NTOC's Operations Center, where he will lead a dynamic, national level 24*7*365 response element that defends against malicious cyber threats on the Department of Defense's Global Information Grid (GIG). Dave started his career as an incident handler

for the US Cyber Command predecessor, Joint Task Force Global Network Operations (JTF-GNO), ascending to the JTF-GNO Embedded Analyst to NTOC, and then transitioning four years ago to NTOC, where he has held multiple technical leadership positions and been at the forefront of NTOC's inter-agency efforts to protect DoD and USG networks from cyber threats.

Billy Leonard, Security Engineer, Google
Billy is currently a security engineer at Google in the Threat Analysis Group. Prior to Google, Billy spent 6 years with various parts of the US Government - the first few months on the pre-fail side of security and the remainder on the post-fail side (it's way more fun on this side).

Enoch Long, Principal Security Strategist, Splunk
Long worked as the Manager for Northrop Grumman's Cyber Security Operations Center (CSOC). In this role, he worked to build/protect secure environments for all aspects in network security for Northrop Grumman internal networks and its clients highly classified networks/assets. Currently he is a Principal Security Strategist for Splunk.

Adam Meyers, Director of Intelligence, CrowdStrike
Adam Meyers has over a decade of experience within the information security industry. He has authored numerous papers that have appeared at peer-reviewed industry venues and has received awards for his dedication to the field. At CrowdStrike Adam serves as the Director of Intelligence. Within this role it is Adam's responsibility to oversee all of CrowdStrike's intelligence gathering and cyber-adversarial monitoring activities. Adam's intelligence team supports both the Product and Services divisions at CrowdStrike and Adam manages these endeavors and expectations. Prior to joining CrowdStrike, Adam was the Director of Cyber Security Intelligence with the National Products and Offerings Division of SRA International. He served as a senior subject matter expert for cyber threat and cyber security matters for a variety of SRA projects including on site at Department of State. He also provided both technical expertise at the tactical level and strategic guidance on overall security program objectives. During his tenure at SRA International Adam also served as the Product Manager for SRA's dynamic malware analysis platform called Cyberlock. Adam supported various law enforcement agents as a technical resource, regarding malware and criminal investigation.

Julie J.C.H. Ryan, Associate Professor, George Washington University
Julie J.C.H. Ryan received her D.Sc. from The George Washington University (GWU) in Engineering Management and Systems Engineering. She holds an M.L.S. in Interdisciplinary Studies from Eastern Michigan University and a B.S. from the United States Air Force Academy. She is currently an Associate Professor at GWU. Her research interests include information security, knowledge management, international relations, and information warfare. She worked for 18 years as an information security specialist, systems engineer, intelligence data analyst, and policy consultant prior joining academia in 2001. She is the co-author of "Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves" (2000, McGraw-Hill).

Chris Sperry, Senior Cyber Intelligence Analyst, Lockheed Martin
Mr. Sperry has over 15 years of demonstrated experience in cyber intelligence, penetration testing, vulnerability assessment, security engineering, information assurance and courseware development within those fields. He has worked in a number of contract and civilian positions within the US government to include the Departments of Defense, Energy and Justice.

Adam Vincent, Founder & CEO, Cyber Squared
Mr. Vincent is an cyber security visionary and entrepreneur. Prior to founding Cyber Squared Inc., Mr. Vincent was a founder and Chief Technology Officer (CTO) for the Public Sector Division at Layer 7 Technologies a Cyber Security & Cloud Company. While at Layer 7, Mr. Vincent was responsible for exponential growth of the federal division and was recognized for his strategic leadership & direction to the company across the government sector – Worldwide. Prior to Layer 7, Mr. Vincent was a Sr. Information Security Engineer with The MITRE Corporation. Mr. Vincent holds an MS in computer science with a graduate certificate in computer security & information assurance from George Washington University. Mr. Vincent is an active blogger in the area of cyber security and a sought-after speaker at security industry conferences and events.

Aaron Wade, Senior Team Leader – GE Cyber Intelligence, General Electric Company
Aaron is a senior member of GE's Cyber Intelligence organization where he works with a dedicated and tenacious group of analysts focused on advanced threats. While at GE he has helped develop and shape the core capabilities, methodologies and processes of an intelligence program in a global enterprise. Prior to GE, he spent many years in environments developing novel methods and creative solutions on shoestring budgets.

Doug Wilson, Manager – Threat Indicators Team, Mandiant
Doug Wilson is the Manager of the Mandiant Threat Indicators Team, a part of the Mandiant Threat Intelligence Unit. Doug has worked in various fields of Information Security since 1999, with previous specializations in Incident Response, Multi-tiered Application Architecture, and Web Hosting. Doug has also supported several government customers during his career as a consultant, both civilian and DoD.

In his role at Mandiant, Doug has been an advocate for the standardized, automated sharing of Threat Intelligence, and has often presented about Mandiant's OpenIOC standard, which was released as Open Source in late 2011. His team works to improve the lifecycle and quality of Indicators of Compromise (IOCs) used by Mandiant and their customers, integrating an ever increasing tide of intelligence sources into a practical IOC creation workflow. Doug also runs the downtown DC social meetup for Infosec practitioners, CapSec DC.