



Conference Session Proposal:
NMCI Industry Symposium, June 20-23, New Orleans Marriott

Speaker POC:

Tom Resau, PR Manager, Public Sector
703-668-8743
thomas_resau@symantec.com

Topic concentration:

“Security and NMCI”

Session title:

“From Information Overload to Actionable Alerts: Threat Intelligence for Critical IT Systems”

Session Presenter:

Jason Shupp, Principal Security Consultant, Symantec Corporation

Presenter background:

Mr. Shupp is an expert on information security technologies and strategies. He currently serves as an on-site security consultant at Navy-Marine Corps Intranet (NMCI) operations centers, where he assists U.S. Department of Defense (DOD) authorities with security management across a large enterprise environment. In addition to consulting resources, Symantec Corporation provides NMCI with a broad range of security solutions across firewall, intrusion protection, content filtering, enterprise administration and virus protection technologies.

Session description:

Gathering intelligence on security threats likely to target enterprise networks and IT assets is a prime requirement for effective information assurance strategies. Novel intrusion attempts, malicious code variants and ever-increasing software vulnerability disclosures create a vast landscape of risk for sensitive information. The promise of threat intelligence is to strengthen existing security devices by providing accurate, timely assessments of a threat, its associated effects and mitigating strategies. This session outlines requirements, best practices and evaluation criteria for intelligence systems.

Leveraging a current U.S. Defense Department implementation case, this session will study the integration of a commercial threat intelligence capability with existing military intelligence assets to create a “360-degree” view of continuously updated global threat data. Specific NMCI intelligence needs and threat assessments will also be included.

Maintaining “situational awareness” on the unconventional Internet battlefield is a painstaking, yet critical task. According to Symantec Corporation surveys, the average information security practitioner spends more than two hours each day sifting through new and old security data – patch releases, vulnerability posts, internal reports – simply to ascertain the “status” of the network versus perceived risks. This equation determines whether prioritized actions should be taken. This manual mode of intelligence collection is inherently time-consuming, error-prone and often results in overdue advisories and after-the-fact analysis.

Today there is an urgent need for intelligence systems to aid limited IT staff as they combat increasingly swift and sophisticated attacks against diverse system platforms and environments. To be effective, intelligence must be specific, according to IT assets deployed in your network. It must be detailed, with information on the makeup of the threat and examples of vulnerable systems. The information must also be immediately “pushed” to managers in a clear, uniform manner.

Establishing a centralized intelligence collection/analysis capability within NMCI will help the enterprise wring further performance from its deployed security technologies, and discern threat activity impacting military systems versus activities facing industry and academia around the globe. Achieving this multi-dimensional view of vulnerability exploits and introductions of novel attack techniques will yield more strategic planning and execution within NMCI information assurance programs.