SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Countering the Advanced Persistent Threat

Facilitator: Michele Moss, Booz Allen Hamilton

for Tom Millar, US CERT

March 2, 2011

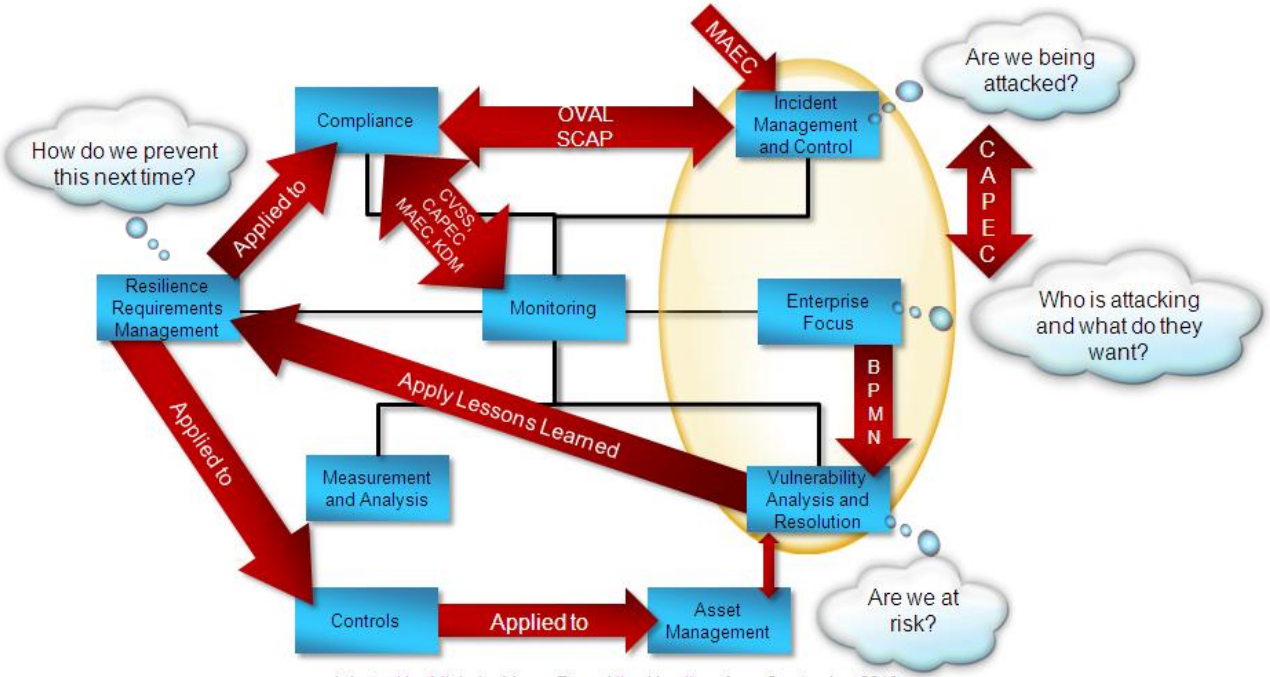
Homeland Security

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Countering the Advanced Persistent Threat

Objective: Provide insights into the advancement, opportunities, and challenges of leveraging incidents and forensics information to inform development and sustainment of trusted technology



Adapted by Michele Moss, Booz Allen Hamilton from September 2010 SwA Forum, CERT RMM for Assurance , Lisa Young, SEI

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Speakers

- ***Sean Barnum, Mitre***
  - Sean Barnum is a Software Assurance Principal at The MITRE Corporation where he acts as a thought leader and senior advisor on software assurance and cyber security topics to a wide variety of government sponsors throughout the national security, intelligence community and civil domains. He is very active in the software assurance community and is involved in numerous knowledge standards-defining efforts including CWE, CAPEC, SAFES, and MAEC.
- ***Ryan Kazanciyan , Mandiant***
  - Ryan Kazanciyan is a Principal Consultant with MANDIANT and has specialized in incident response, forensics, application security, and penetration testing for eight years. He has conducted intrusion investigations and response efforts for organizations in the defense industrial base, technology, financial services, and energy sectors. He also has extensive experience performing application security assessments, internal and external penetration testing, and red-team exercises in both federal and corporate environments. In addition to consulting, Mr. Kazanciyan has led training sessions for audiences in law enforcement, government, and corporate security groups.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Speakers

- ***Stephen Windsor, Booz Allen***
  - Steve Windsor is a Senior Associate at Booz Allen Hamilton. With extensive experience in the field of digital forensics he manages the firm's Advanced Persistent Threat, Digital Forensics, Incident Response, and Proactive Threat Identification service offerings.
- ***Rick Doten, Lockheed Martin***
  - Rick Doten is Chief Scientist for the Lockheed Martin's Center for Cyber Security Innovation. Rick spent the last 10 years managing penetration testing, forensics, incident response, and risk assessment teams for commercial and government customers. Today, Rick works with Lockheed business units to provide guidance to build and maintain trusted systems for our customers. Current trends and focus areas are Advanced Persistent Threat (APT) defense, Smart Grid Security, Application Security, and Insider Threat.

Questions?

Questions

- One of our biggest obstacles in reaching the Development and Acquisition communities is Creating the NEED for SwA.

  There is a perception that it does not apply to “Me” because
  - No one would maliciously attack my software
  - No one would attack my enterprise

- In hindsight, what would have helped organizations dealing with incidents understand the need to address the risk in development, acquisition, and sustainment prior to an incident?