Global Cutting Edge Approaches in the Defense of Cyber Intelligence Threats

David E. Luzzi

Northeastern University

Boston, USA

The Global Cyber Battlespace is Expanding and Becoming Dangerous

- Attacks on national economies & defense
  - Largest theft of Intellectual Property in history
    - Private and Nation-State activities
    - Measurable negative impact on national economy
  - Largest theft of military system design information
    - Strong evidence of Nation-State sponsorship
    - Profound impact on global security
- Attacks on national & international systems
  - Direct efforts to influence US presidential election
  - Efforts to undermine international and Olympic Sports governance

All Organizations must develop

- Cyber Situational Awareness (SA)
- Advanced multi-level protections
- Resilient systems and strategies
  - Withstand
  - Maintain essential core functionality
  - Recover rapidly

Cutting Edge Approach - 1

- 

- Corporate partnership
  - Original 5 – BAE, Boeing, LMCO, Raytheon, Rolls-Royce
- System for supply chain vetting, communication, management
- Drives superior cyber security practice across the supply chain
- Aides compliance with NIST and DFAR cybersecurity standards

Northeastern University

- Institute for Information Assurance
- Cybersecurity & Privacy Institute
- Kostas Research Institute for Homeland Security
  - Cybersecurity at the Tactical Edge
- US National Security Agency / Dept of Homeland Security triple Center of Excellence
  - Information Assurance
  - Cyber Defense
  - Cyber Operations
- US National GeoSpatial Intelligence Agency
  - Geospatial Intelligence Systems Center of Excellence

Cutting Edge Approach - 2

- Northeastern University Spinout Company
  - With UCSB

- NSS Labs - Top rated company for Breach Detection
  - Announced RedHat 2016
- Founders also developed
  - ISecLab – International Secure Systems Laboratory
    - Meta-Laboratory
  - Anubis
  - Wepawet

- https://Lastline.com

Cutting Edge Approach - 3

- Current Northeastern Research
- Addressing scourge of ransomware
- UNVEIL© - ransomware detection scheme
  - Captures ransomware behavioral signatures
  - **Avoids detection by malware as a sandbox**
- Recent test results
  - Detected 13,637 randsomware samples from 148,223 recent general malware
  - 0% false positives
  - Detected “SilentCrypt” ransomware which defeated all known commercial techniques
- http://www.ccs.neu.edu/home/mkharraz/publications/unveil-USENIX.pdf

Thanks for listening

Questions?