Session 12C: Future SATOPS Planning and Enterprise Ground Architecting (EGA) – Achieving Resiliency for Increased Commercial Multi Mission Support

Chairs:

- Roberta Ewart, USAF AFSPC SMC Chief Scientist
- Joseph Betser, The Aerospace Corporation

Speakers:

- Maj. Michael Molesworth, USAF SMC
- LTC Matthew Kimsal, USAF SMC
- Wayne Wheeler, The Aerospace Corporation

GSAW 2015, Los Angeles, CA, March 2015

**** This briefing represents the opinion of the presenters. It is not the official position of the US Government or that of the Aerospace Corporation***

AEROSPACE
Assuring Space Mission Success

Enhanced Cyber Resilience for EGA Architectures

Factors Driving Cyber Threats to Ground

- **Ground systems are distributed networks of COTS[1], and can share vulnerabilities with any commercial infrastructure**
  - Aging ground infrastructure can be less secure that current commercial systems (no remediation for emerging threats)
- **"100% closed systems" assumptions for space systems are not realistic, in light of Advanced Persistent Threats**
  - APTs- highly resourced and motivated attackers
  - Supply chain, FOSS[2] or commercial software, upgrades, links to other systems, and insider threats are potential attack vectors
- **Threats development has moved up from "hackers" to organized crime and resourced State actors**
  - Computing power amplifies asymmetric power
- **Potential adversaries are known to be developing (and are sometimes demonstrating) sophisticated cyber attack capabilities against space systems**

[1] Commercial-of-the-Shelf
[2] Free-and-open-source software

The Advanced Persistent Threat (APT)

The highly resourced and motivated adversary

- **The Cyber Threat is active and evolving**
  - Ground Segments must be resilient to the persistent probing, penetration and exploitation attempts
- **Ground Architectures must be cyber resilient to all types of threats**
  - "Known" Cyber Threats
    - Identified "in the wild" as a known vulnerability
    - Usually similar to previous malware
  - "Unknown" Cyber Threats
    - Only identified after exploit
    - Zero-day attacks

Defensive Cyber Capabilities

Known
Identified Vulnerabilities

- Available technologies
- Global industry response
- Best-practices
  - ✓ Defense-in-Depth
  - ✓ Network Segmentation
  - ✓ Layer 3 Firewalls
  - ✓ Aggressive Patch Management
  - ✓ Boundary Enforcement
  - ✓ IDPS
  - ✓ 7x24 Top-tier Security Ops Center
  - ✓ Current Software/Hardware

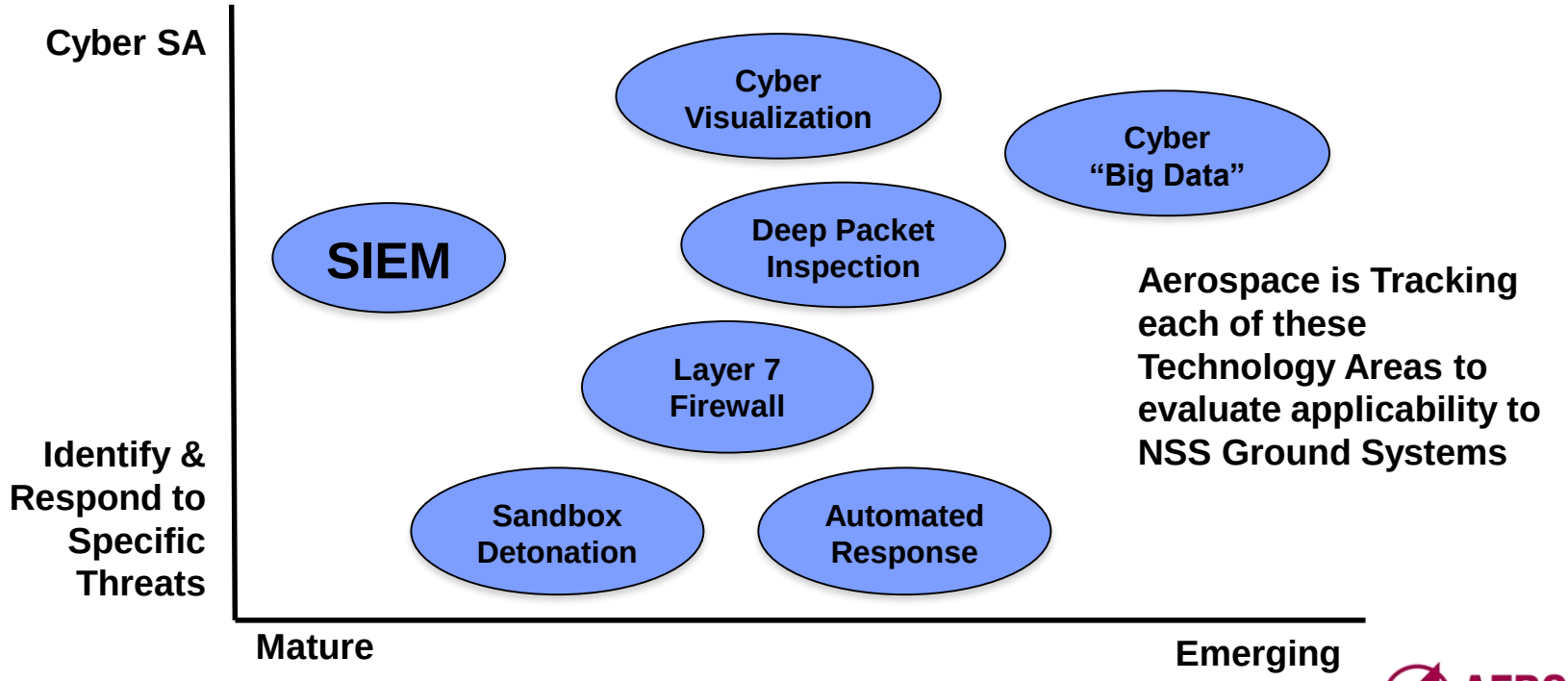
Unknown
Zero Day, APT

- Emerging technologies
- Industry struggling to respond
- Cyber Analytic Tools
  - ✓ Layer 7 Firewalls
  - ✓ SIEM
  - ✓ Virtualization Sandbox
  - ✓ Cyber Visualization
  - ✓ Auto respond systems
- Ineffective without development and Ops expertise
  - Significant costs for start-up Ops

Zero Day- Cyber exploit not previously seen
APT- Advanced Persistent Threat
DPDS- Intrusion Detection & Prevention
SIEM- Security Information & Event Management

Cyber Analytic Tools for Advanced Threats

- Industry has developed various real-time cyber analytic tools to identify and respond to advanced threats
- Instrumentation highlights patterns of a cyber attack – subtle changes in state on a number of systems can be correlated to facilitate early discovery of an attack
- Data-Driven Security- emerging capabilities such and Big Data cyber analytics and cyber visualization may enable automated analysis and response to advanced threats



Summary

- The cyber threat to ground systems will continue to evolve with increasing capabilities for potential attackers
- **Cyber Situational Awareness** is critical for all segments of a space system (space, ground networks, ops centers, user terminals)
  - *Required to identify, mitigate, and attribute advanced cyber attacks*
- **Cyber Analytics Tools** can provide significant insight into cyber situational awareness
  - *Instrument the network*
  - *Implement analytics to support security team*
  - *Must develop (our contract for) expertise necessary to integrate and operate cyber analytic tools*
- Cyber Analytic solutions are evolving— resources must be provided for an “evergreen” refresh approach to cyber security

Discussion