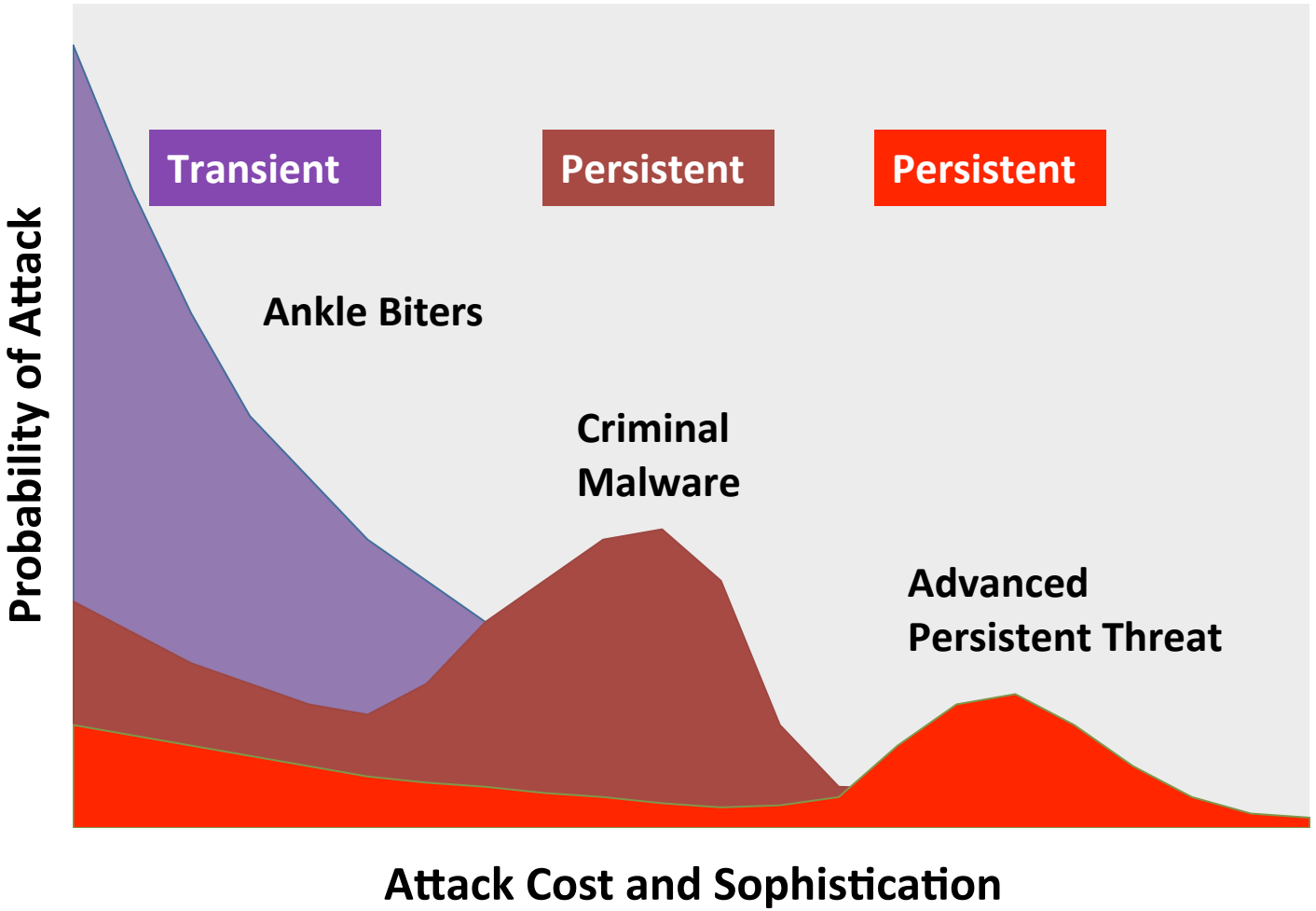
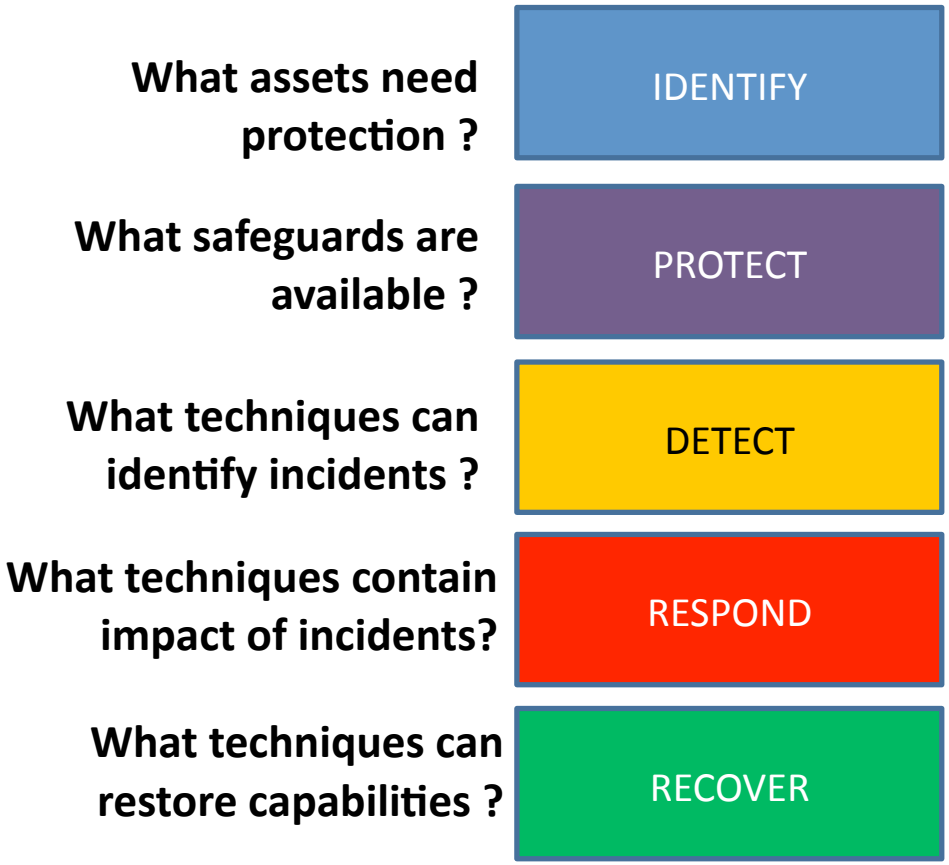
Software Assurance
Secure Environments

Arun Sood
Professor Computer Science, Director International Cyber Center
George Mason University
Founder, SCIT Labs

Threat Landscape



NIST Cyber Security Framework



Issues

- What is the role of time?
- Are these steps sequential?
- What if Detect & Prevent are not perfect?
- What about tactical environments?
- Cyber Resilience? Recovery?

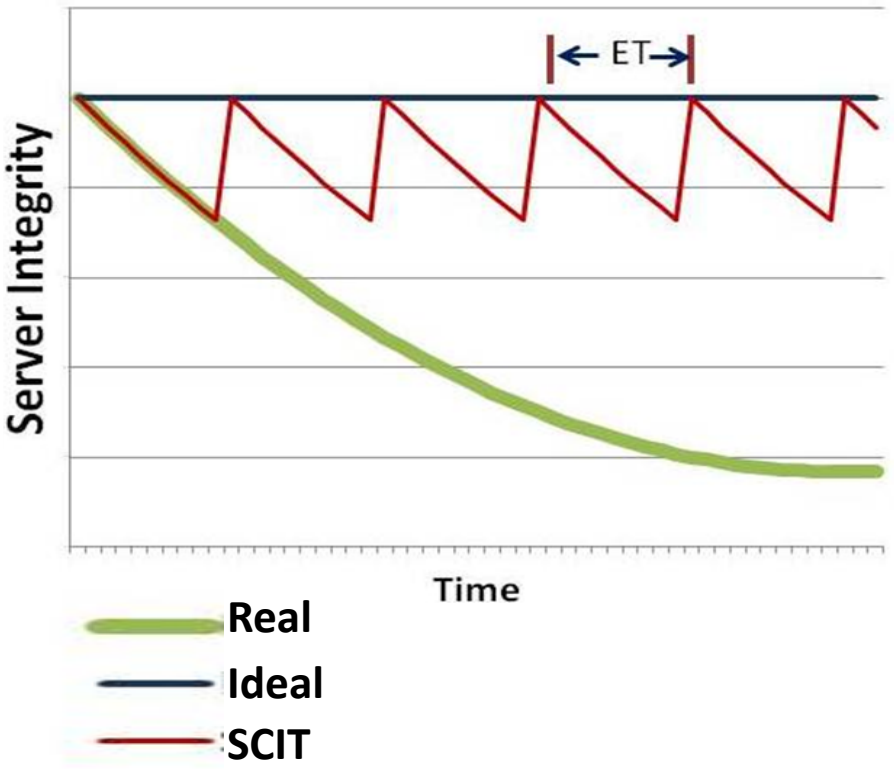
Cyber Resilience

- All intrusions cannot be prevented
- Intruders persist for long periods
- Cyber Resilience solutions should emphasize response and recovery
- Speed and automation of response and recovery processes is essential

Self Cleansing Intrusion Tolerance (SCIT)

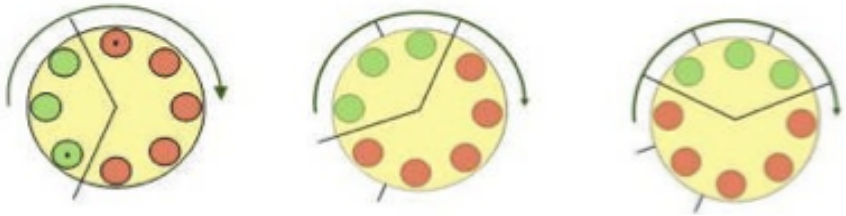
Resilience through Recovery

Restore Server Integrity



How SCIT Works

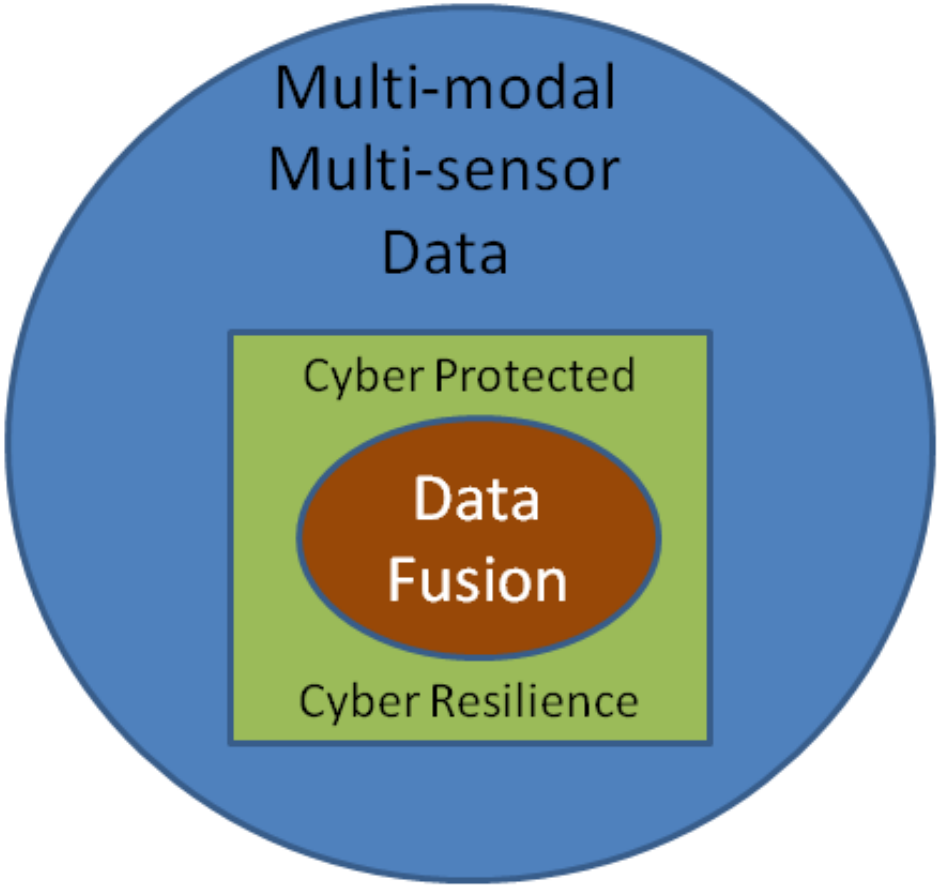
- **Online servers are assumed to be compromised**
- **Offline servers are restored to pristine state**



SCIT Goal: Reduce Compromise to Restoration time to 1 minute without requiring threat detection.

SPAWAR: Tactical Cyber Attack Deterrence

Data Fusion in Future Tactical Environments



- Restores VMs to uncontaminated (pristine) base image every minute
- Attacker is forced to make multiple attempts
- Forensics step enables comparison with base image
- Extend to deployable microservers

Questions ?

Arun Sood

asood@gmu.edu

arun_sood@scitlabs.com