

**2012 DHS S&T/ASD(R&E)  
CYBER SECURITY SBIR WORKSHOP**



Homeland  
Security  
Science and Technology



# Grabbing Security By the Roots

## *APT Detection & Response*

Clear Hat Consulting, Inc.  
Sparks, Sherri



# Agenda



- Company Overview
- Capabilities
- Current SBIR Projects
- Questions

# Company Overview



- Founded in 2007 by S. Sparks and S. Embleton
- Located in downtown Orlando, FL
- Mission Statement
  - “To research and develop proactive, innovative solutions to cutting edge cyber security problems”

# Capabilities



- Threat Assessment
- Reverse Engineering
- Custom Research & Development
- Training



# Current SBIR Projects

- **OSD09-IA1:** Real-time Adversarial Characterization and Adaptive Protection Countermeasures (Phase 2)
- **OSD09-IA2 :** Countermeasures to Covert Access Methods to Reduce Attack Susceptibility and Ensure Trust (Phase 2)
- **OSD10-IA1:** Countermeasures to Malicious Hardware to Improve Software Protection Systems (Phase 2)

# OSD09-IA1 & OSD09-IA2



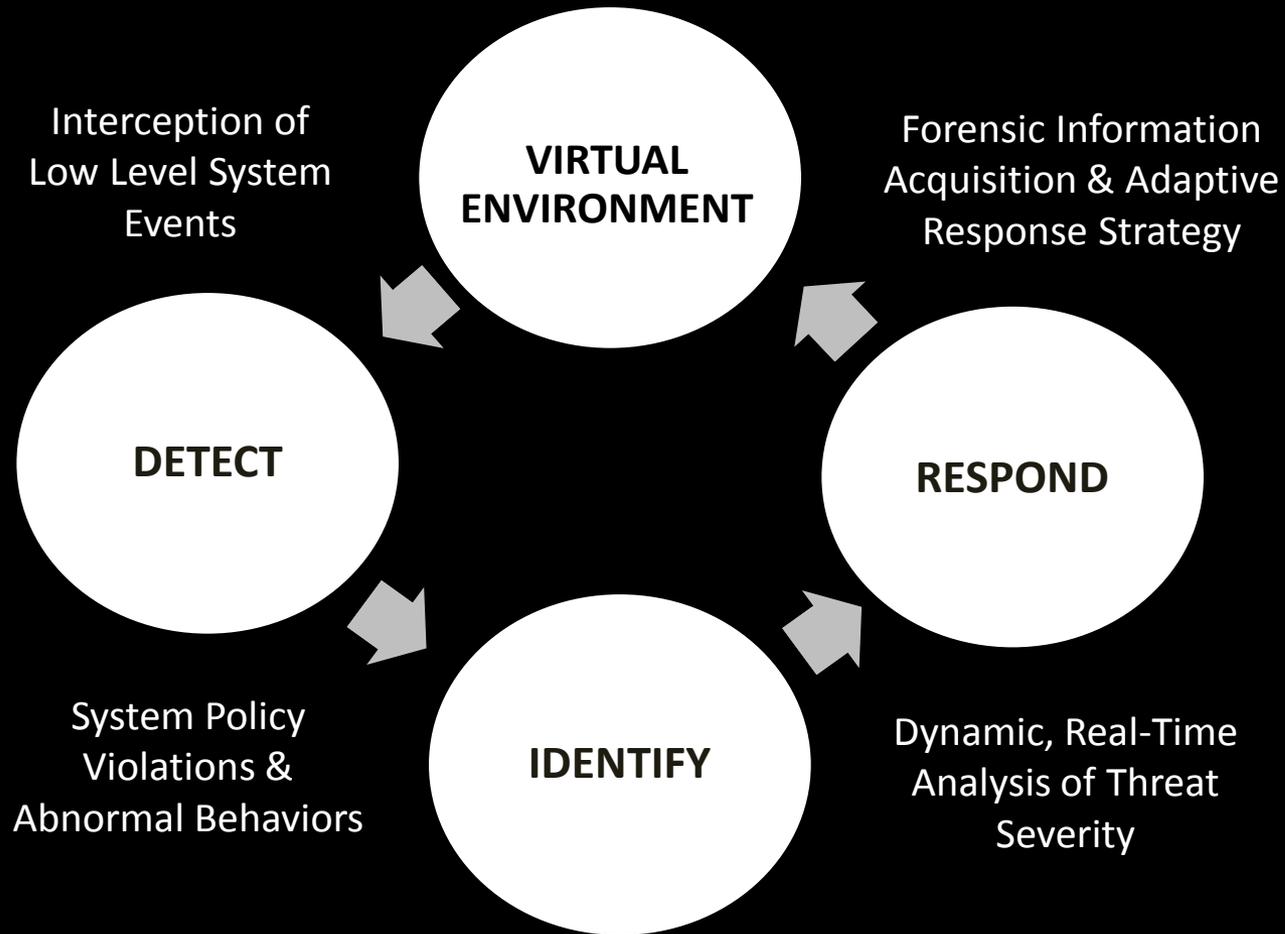
- We are developing an APT detection and response product
- Our product uses a bare metal hypervisor to detect and respond to OS independent threats that misuse low level CPU and chipset resources to compromise security



# Exploitable Resources

- Virtual Memory Configuration
- System Management Mode (SMM)
- Active Management Technology (AMT)
- Advanced Configuration & Power Interface (ACPI)
- Direct Memory Access (DMA)
- Peripheral Hardware (Disk, Video, Network, etc.)
- Processor Caches
- Virtualization Extensions
- PCI Expansion ROM's
- BIOS
- CPU Microcode
- Local & I/O APIC's

# System Architecture



# Applications



- Advanced malware detection
  - Early detection of sophisticated attacks or zero-day attacks that target low-level CPU and chipset resources
- Advanced incident response
  - Provide a sequential trace of anomalous system behaviors or policy violations
  - Capture valuable information about attacks:
    - Attack origin
    - Resource types targeted by the attack

# OSD10-IA1



- **Topic:** Countermeasures to Malicious Hardware to Improve Software Protection Systems
- **Objective:** Develop innovative countermeasures to malicious hardware / firmware modifications in COTS devices for the purposes of developing trusted software protection systems
- **Approach:** Because of the size and diversity of the COTS attack surface, we have focused our research on countermeasures for disk based firmware threats

# Phase 1 Results

- At the conclusion of our Phase 1 effort, we were successful in:
  - Dumping and disassembling a significant number of firmware routines in a popular COTS hard drive
  - Locating critical data structures in the drive firmware
  - Identifying the firmware ATA command handling routines
  - Identifying where the drive's data buffers are stored
  - Developing a proof of concept test case
  - Identifying countermeasures for disk based threats

# Phase II Objectives



- To facilitate a greater understanding of the COTS peripheral component attack surface
- To research and develop a host oriented protection to improve the ability of critical software assets to carry out their missions even when they are operating in hostile hardware environments.
- To research and develop disk based firmware introspection tools and technologies

# The CHC Advantage



“hacker”  
mindset  
+  
technical  
expertise

