THREAT ANALYSIS & MANAGEMENT

Deeper Knowledge for InfoSec Teams

By: Brent Huston, Security Evangelist & CEO

MSI
MICROSOLVED,INC.

DO YOU KNOW THE ENEMY?

- Who are your threat agents?
- What are their capabilities?
- What are this risks that your organization faces?
- What are the specific risks of a specific application or operation?
- ***Goal: Help you use real-world threat models for insight and analysis of real-world risk.***

META-FACTORS

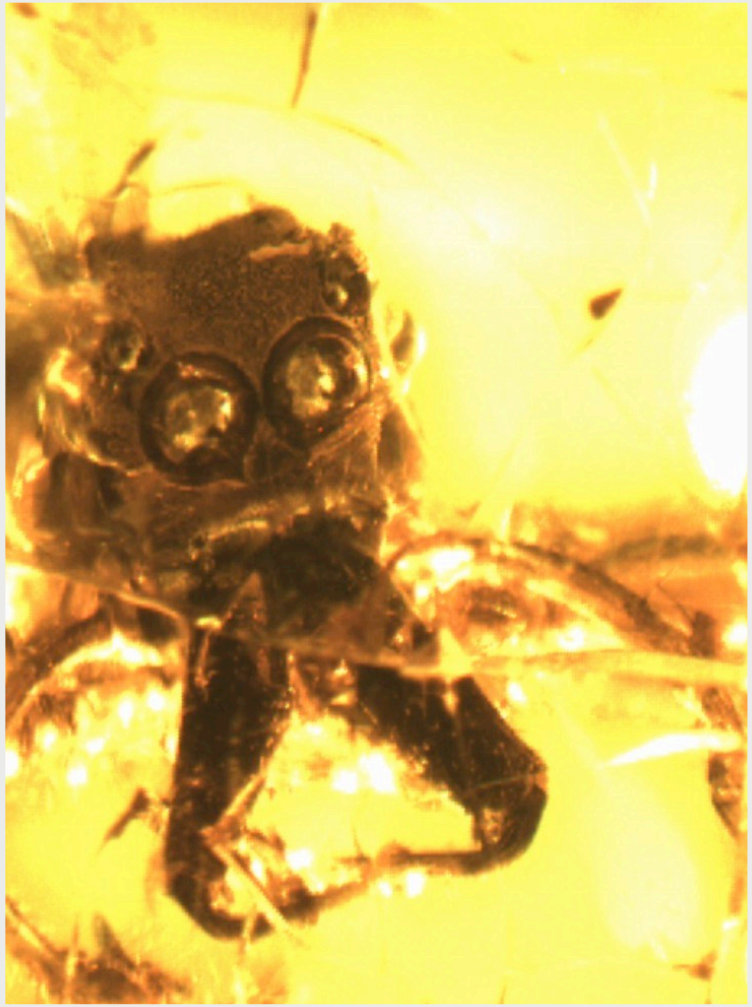
- Frequency
- Capabilities
  - Automated Threats vs Human Threats
- Guess vs Modeling...
- **"Rational Knowledge Prevents Panic"**

BUILDING A MODEL

- Determine Goal
- Create the Model
- Deploy the Model
- Monitor & Measure
- Remove
- Analysis

LEVERAGE LIH TECHNOLOGIES**

- Low Interaction Honeypots
  - Emulate Basic Services & Deployments
  - Capture Attacker Interaction (FREQUENCY)
  - Give Insight into CAPABILITY
    - Not full, deep knowledge - But more than current
    - Little real risk

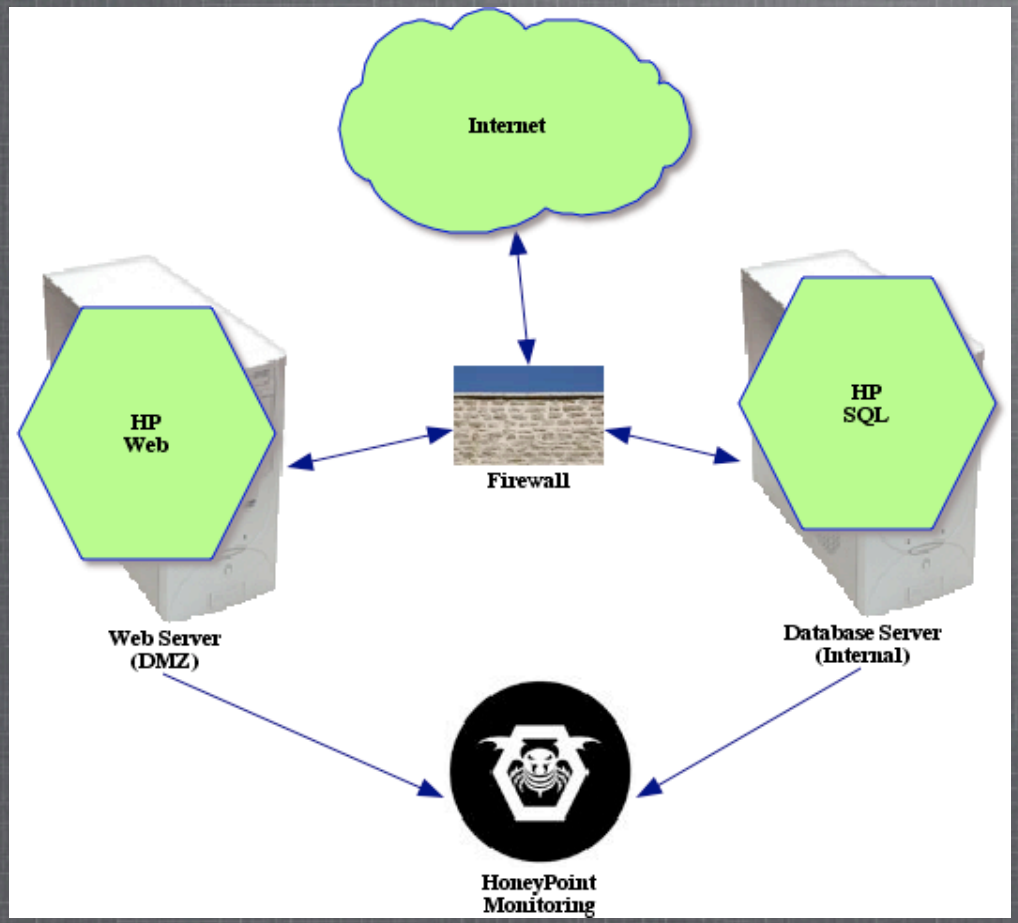


** ***Disclaimer: MSI Makes an LIH Product!!!***

WHAT TO MODEL

- Smaller scope is better
- Deep emulation is not needed to gather what you need
- Examples:
  - SSH exposures to the Internet
  - Web applications with login
  - Use your imagination

WHAT CAN YOU GET?



- Contact with Services
- Contact with Controls
- Contact with Emulated Vulnerabilities
- Human vs Software
- Intent
- Random vs Focused - Routine eliminated!!!
- Even Multi-components with Multi-presences (EX: complete PCI web site, check scanning, system, etc.)

THE HOW OF MODELING

- Emulate ports/services
- Emulate applications only as far as needed
- KISS
- Our Example: SSH / Inet

WHERE & HOW LONG

- Remember the goals!
- Longer = More Accurate = More Work
- Attackers Tend to Cycle
- Maybe # of Attackers vs Time?
- Internal, DMZ, External

IDEAS FOR MODELING

*Pre-measure Firewall Exposures
*Prove Controls ROI
*End to End Business Processes
*Research Potential Impacts
*Identify Current Attacker Focus
& More!!!

USING MODEL DATA

- Determine attack frequency, local & global:
  - SSH: US ~1.5 hrs, South America ~5.25 hrs
- Real metrics = ***THE TRUTH***
- Correlation, Intent (Focused vs Wide, etc.) & Capability, Changes in Threat Levels - ***Manage Risk***
- ***Plug right into ERM & methodologies (FAIR, etc.)***

EVOLUTION: CCI

- Proactive Security
- Threat Management
- ***We CAN Influence & Modify Threat Agent Behavior!***
  - HoneyPoint Trojans
  - HornetPoints

THANKS, MORE INFO, Q&A

- More Information:
  - www.microsolved.com
  - bhuston@microsolved.com
  - (614) 351-1237
- HoneyPoint: www.microsolved.com/honeypoint/
- Blog: www.stateofsecurity.com