

Key Elements of a Threat and Vulnerability Management Program

John P. Pironti, CISA, CISM, CISSP

Enterprise Solution Architect / Security Consultant
Unisys Corporation

UNISYS

Imagine it. Done.

INTEROP[®]

Agenda

- Threat and Vulnerability Management Programs
- Asset Identification
- Key Elements of Threat Analysis
 - Who, What, When, Where, Why, and How
 - OSI+ Layers
- Threat Level Assignment
- Vulnerability Management Concepts
- Final Thoughts

Why Is Security So Difficult?

- Adversaries have extraordinary resources
- Adversaries need to master only one attack
- Defenders constrained by ethics and laws
- Defenders must serve business goals
- Defenders must win all the time



Threat and Vulnerability Management Programs

- Proactive approach to information security
- Provides a business impact view of information security threats to the organization
- Assist in regulatory compliance (i.e. GLBA)
- Integral part of the information security program



Asset Identification

- All assets associated with solution need to be identified prior to threat analysis activity
- Both physical and logical assets need to be identified
- Third party elements need to be accounted for
 - Risks associated with these elements need to be documented



Threat Analysis Concept Overview

- Threat Analysis is an activity which models a particular solution against attack scenarios and known vulnerabilities to evaluate its ability to repel attacks
- The output of a threat analysis should produce information to create appropriate identification and countermeasure plans for identified attack scenarios
- Threat Analysis should also quantify risk of identified threat to organization
 - Likelihood of occurrence
 - Impact on organization

Threat Analysis Required Information

- Threat analysis activities require significant information from organization to be accurate and effective
 - Value to the organization
 - Regulatory and legal constraints
 - Sensitivity of data included in solution
 - Impact on third party activities
- Appropriate risk management decisions cannot be made without these considerations



Threat Analysis Methodology Overview

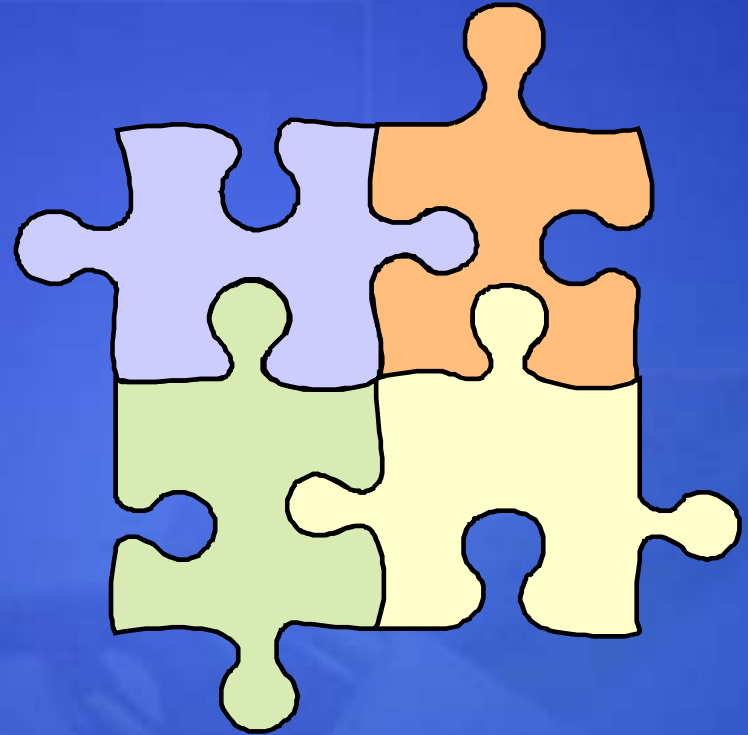
OSI+ Threat Assessment Methodology

- Overview
- Who, What, When, Where, Why, and How
- Countermeasure Plans
- Threat Level Assignment



OSI+ Methodology Overview

- Skilled adversaries will use a combination of skills and techniques to attempt to compromise a solution
 - Technological attacks are not the only way an adversary will attack a solution
- The OSI+ model provides a framework for analyzing how an adversary can attack a solution
 - Identifies weaknesses in current solution
 - Systematic way to evaluate a solution
- Each element needs to be analyzed but not elements will be relevant for each solution



Threat Analysis – Who

Attacker Profiles

■ **Newbies**

- Beginners, Download Tools from Internet

■ **Script Kiddies**

- Basic Programming Skills
- Customize Downloaded Tools

■ **Coders**

- Advanced Programming Skills
- Write Tools for Newbies and Script Kiddies

■ **Professionals**

- Privately Funded Research
- Advanced Capabilities and high levels of access to technology
- Highly dedicated and resourceful

■ **Spooks**

- Government Agents
- Unlimited Resources and Capabilities



Threat Analysis – Who

Competency Models

- Understanding of current and future capabilities of the adversary community
- Research of current education and knowledge programs for computer science and computer security
- Profiling of backgrounds and lifestyles of potential adversaries
- Profiling of adversaries required skills, knowledge, and tools

Threat Analysis

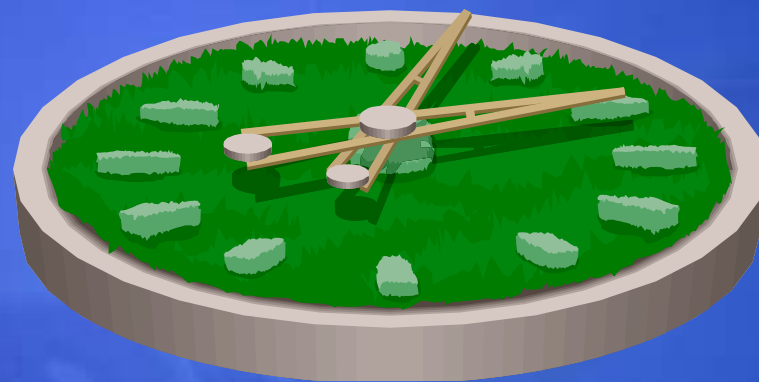
What

- Identification of the portion of the solution which the adversary will most likely attack
 - Typically area most easily accessible from external access point or with highest perceived value
- Skilled adversaries usually attack highest value solutions
- General adversaries will attack solutions which they have highest levels of access to
 - Web Access
 - Remote Access



Threat Analysis When

- Identification of most likely time an adversary will attack
 - Time of day when defenses at weakest
 - Time of year when defenses are at their weakest
- Skilled adversaries will attempt to attack when they believe security staff is distracted with other events
 - Business continuity and disaster recovery events
 - Recovery from known virus infections



Threat Analysis Where

- Identification of the most likely points of attack of a solution
 - Remote access points
 - Third party access points
 - Web environments (HTTP attacks)
- Skilled adversaries will attempt to identify systems whose value is perceived to be low and will most likely have minimum security attributes
 - Print Servers
 - Backup Servers



Threat Analysis

Why

- What is the benefit to the of a successful attack to an adversary?
 - Financial
 - Political
 - Personal
 - Status Seeking
- Understanding of motivations will assist in the creation of appropriate countermeasures and risk identification



Threat Analysis

How

- Analysis of the tools and techniques an adversary will use to attack a solution and the solutions ability to counteract these tools and techniques
- Information will be required from multiple sources
 - Web sites
 - News feeds
 - IRC message boards
 - Intelligence activities
- OSI+ Methodology is one way to analyze how an adversary can compromise a solution
 - Aligns with Open Systems Interface (OSI) Model
 - Adds critical element of people, policy, process, and procedure to model



OSI+ - How Layers

Policy, Process, and Procedure
Application
Presentation
Session
Transport
Network
Data
Physical
People

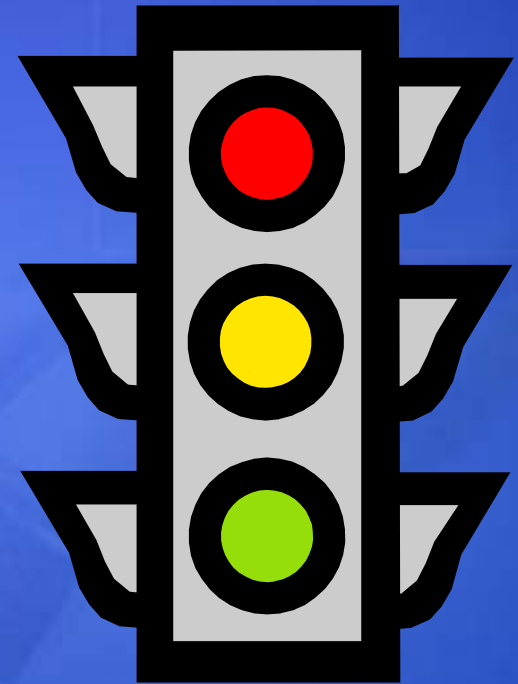
Threat Models – *Attack Trees*

- Attack trees are graphical depictions of how an adversary could compromise a solution
 - Identifies roadmap of adversaries activities
- Useful in understanding system view of attack sequence and impact
- Provide valuable data to incident response and operations teams in identification and remediation of attacks



Threat Level Assignment

- Output of threat analysis should include threat level assignment
 - Required for risk management decisions by management teams
 - Should be communicated to all individuals with security responsibilities
- Threat levels need to be simple and easily understood
 - Red, Yellow, Green & 1 -5 designations work well
 - Simple designations allow for better awareness throughout organization
- Each designation needs to be defined from a business impact perspective



Vulnerability Management Countermeasure Plans

- Once threat analysis has been completed countermeasure plans should be created for identified scenarios
 - Threat identification
 - Procedures for threat and attack mitigation
 - Recognition of attack completion and successful mitigation



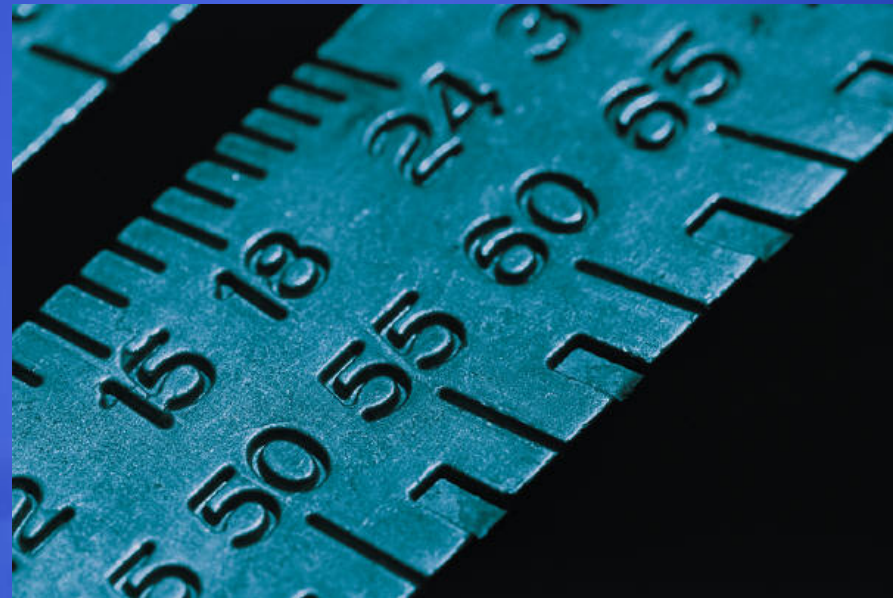
Vulnerability Management Controls

- Risk mitigation concept or technique
 - Can be technological or business process oriented
- Developed as a result of threat analysis activity
- Introduced at risk points within business process or operation



Vulnerability Management Metrics and Measures

- Based on information from threat analysis activities
- Provide insight to success or failure of risk mitigation strategy and controls
- Required for maturity modeling and program development
 - Provide statistical data points for business and technical analysis



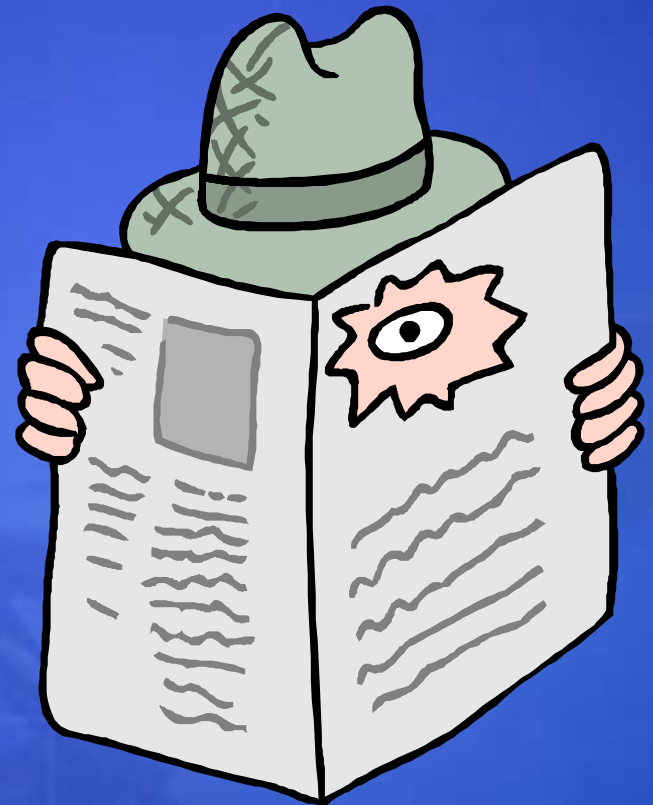
Vulnerability Management Countermeasure Plans

- Incident response personnel should produce countermeasure plans
 - Input from Threat Analysis
- Operations teams need to be briefed on identification of threat activity
- Management needs to be briefed and endorse resource requirements prior to plans being finalized



Vulnerability Management Intelligence

- Important to understand current trends and capabilities of attackers
- Knowledge base of known attacks and attackers should be created
- Trend analysis should be performed to be able to project future attacks and attack methods



Final Thoughts

- Threat Analysis activities are an essential tool in risk management programs
- Before you can solve a problem you must understand the problem
- Threat analysis is only a module in a overall security program
 - Does not solve the overall security problem
 - Require incident management and operations integration to be successful
- Vulnerability management drives proactive security activities



Thank You For Your Time!

Contact Information...



John P. Pironti, CISA, CISM, CISSP
01-781-238-1375
John.pironti@unisys.com