Commercial Practices in IA Testing Panel

March 22, 2001
Albuquerque, New Mexico

First Information Assurance Testing Conference

Sponsored by:

Director, Operational Test and Evaluation

WINDERMERE

Panel Members

- **Dr. Myron L. Cramer**
  - » Executive Director, Information Assurance Division, Windermere
- **Lori Ericson**
  - » interAmerica Analytics
- **Matthew Devost**
  - » Director of Operations, Security Design International (SDI)
- **Samuel Nitzberg**
  - » Senior Scientist, New Jersey Operations, Windermere

Objectives

WINDERMERE

- To share commercial practices in the area of IA Testing, emphasizing topics with high relevance to DoD
- The speakers will each share their perspectives and will participate in Group Wrap-up

Discussion Topics

WINDERMERE

Presentations will address he following topics as they relate to IA testing.

- **Test Objectives**
  - » What things are commercial testers trying to accomplish?
  - » How are these objectives incorporated into test planning?
- **Threats**
  - » How does the commercial world characterize its threats?
  - » What are threat motives, capabilities?
  - » What kind of intelligence gathering is done on the threat?
  - » To what extent does the threat drive a system design?
  - » How is this incorporated in testing?

continued

Discussion Topics (cont)

- **Metrics**
  - » What is the current commercial thinking on test metrics?
  - » How do they measure success?
- **Test Methods**
  - » What are the roles for vulnerability scanning, penetration testing, blind testing, insider testing?
- **Reports**
  - » What kind of documentation is produced?
  - » How does it get used?
  - » Who uses test reports?

Agenda

Time	Topic	Speaker
8:30 – 9:05	Commercial Testing Introduction & Overview	Myron Cramer
9:05 – 9:45	Perspectives on the Threat	Lori Ericson
9:45 – 10:15	Break	
10:15 – 11:00	Hacker Methods & Penetration Testing	Matthew Devost
11:00 – 11:40	New York e-Commerce Testing Activities	Samuel Nitzberg
11:40 – 12:00	Panel Discussions Questions & Answers	All

Role of Testing

- Testing plays an integral part of development process even in the most streamlined processes
- Information security is recognized as a standard requirement for e-Commerce and part of a system's transition from development to production
- Information security testing of operational systems is also regularly performed

Test Objectives

- **What things are commercial testers trying to accomplish?**
  - » Verify design implementation, configuration, integration, operation
  - » Assess exposures
  - » Satisfy audit responsibilities
- **How are these objectives incorporated into test planning?**
  - » Identify system security requirements
  - » Allocate security requirements within security architecture
  - » Develop test plan

Challenges for Enterprises

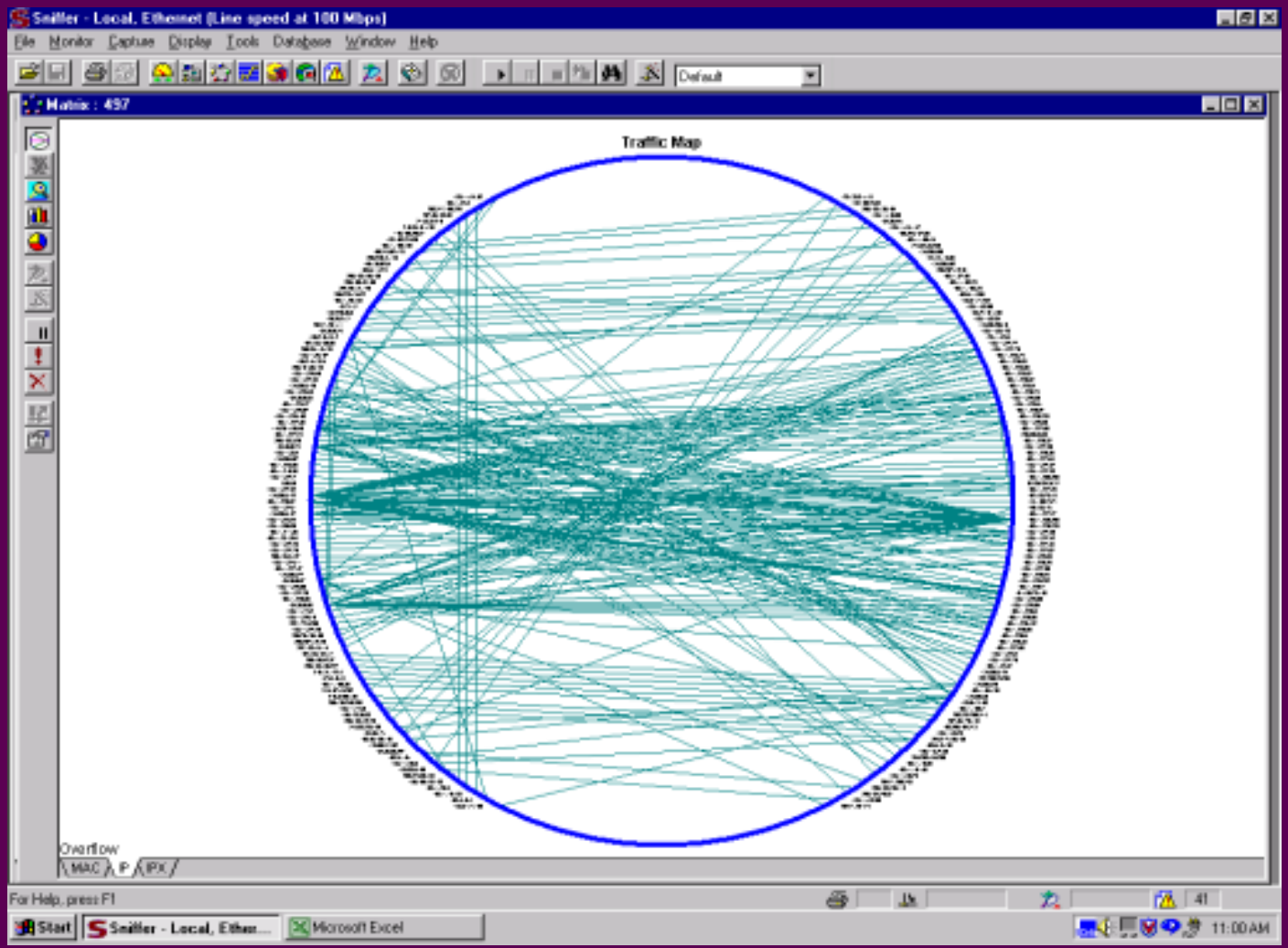
- **Landscape Discovery**
  - » Network topology
  - » Role of legacy systems, services and users
  - » Constraints of communications infrastructure
- **Dealing with Change**
  - » Maintaining compatibility
  - » Data center versus distributed computing base
- **Controlling Access**
  - » Enabling extranet operations
  - » Sharing information with partners and customers
  - » Protecting intranet
- **Scalability**
  - » Implementing security across a large enterprise
  - » Supporting required user services
  - » Maintaining cost-effective operations

Landscape Discovery

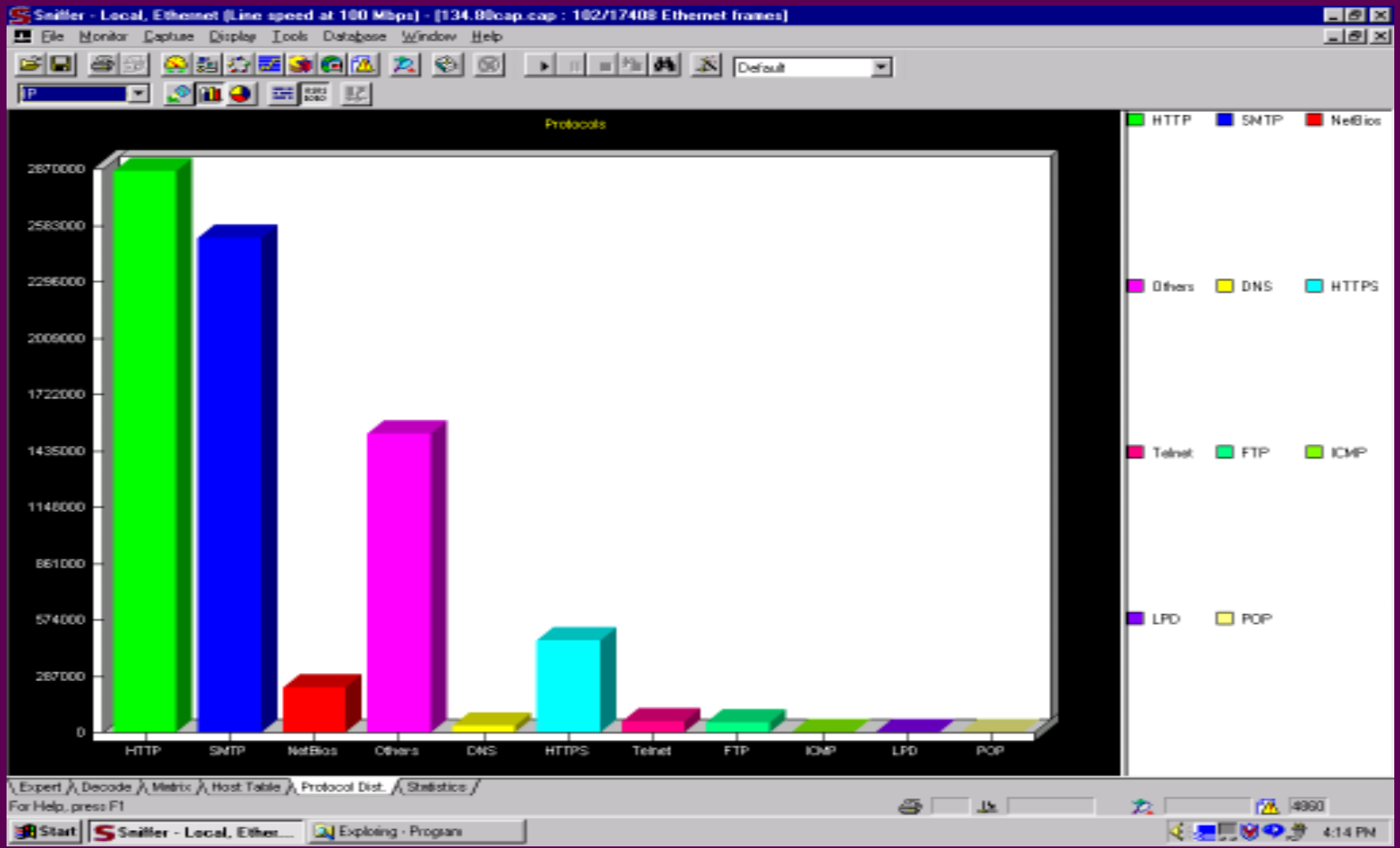
- **Scanning and assessment**
  - » Networks, servers, protocols, protections
- **Interviews**
  - » Nature of the information
  - » Sensitivity
  - » Risks
  - » Information organization
- **Picture of existing architecture**
  - » Networks, servers, applications
  - » Users
  - » Information, value, and data sensitivity

Network Discovery

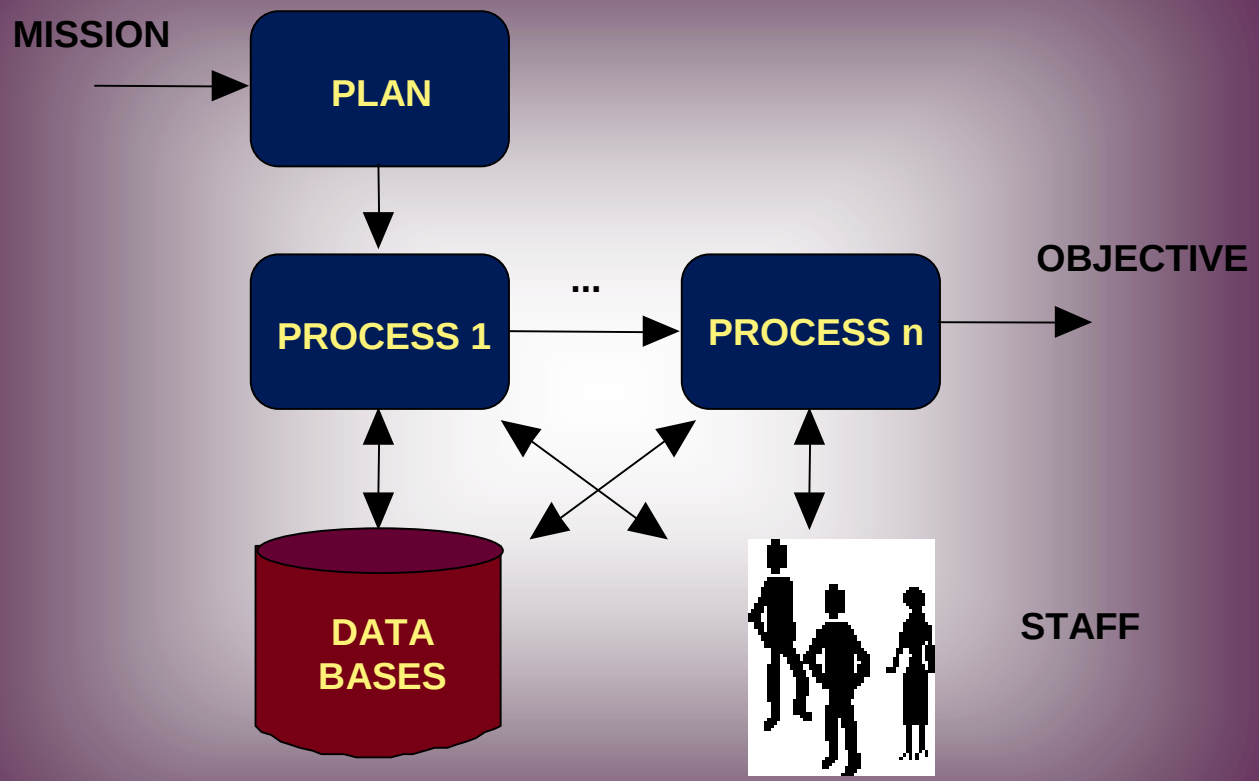
WINDERMERE



Protocol Distribution



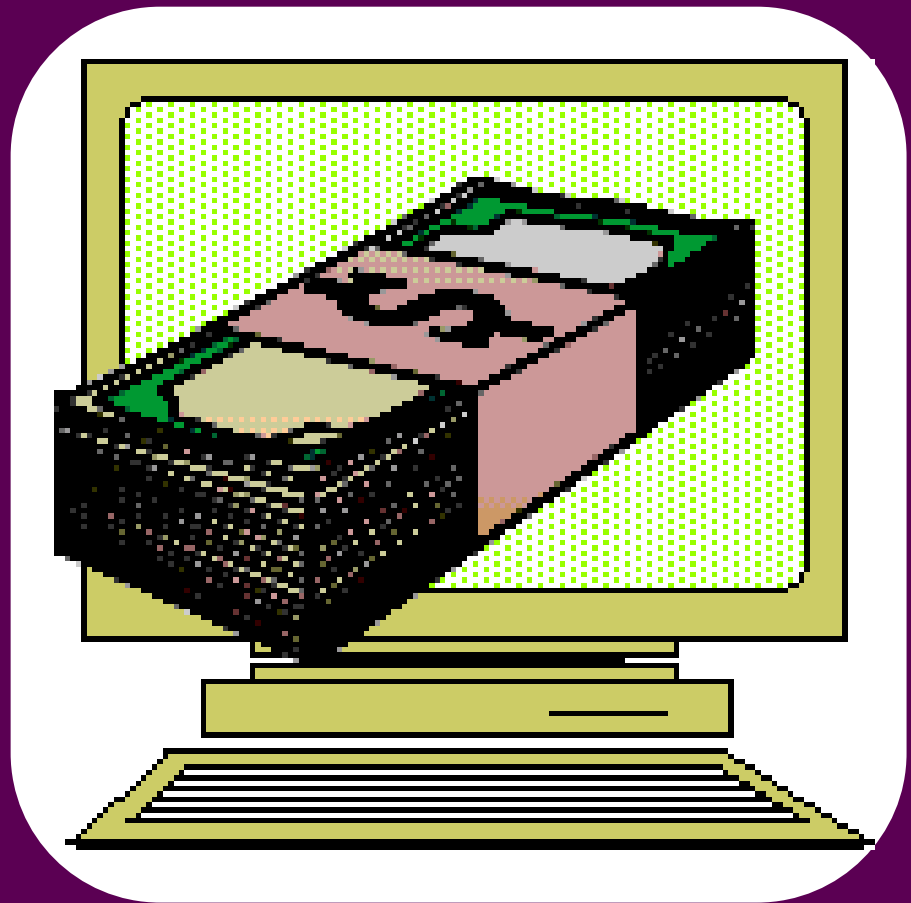
Types of Information



Value of Information

WINDERMERE

- There are different types of organizational information
- These face different threats and have different security issues

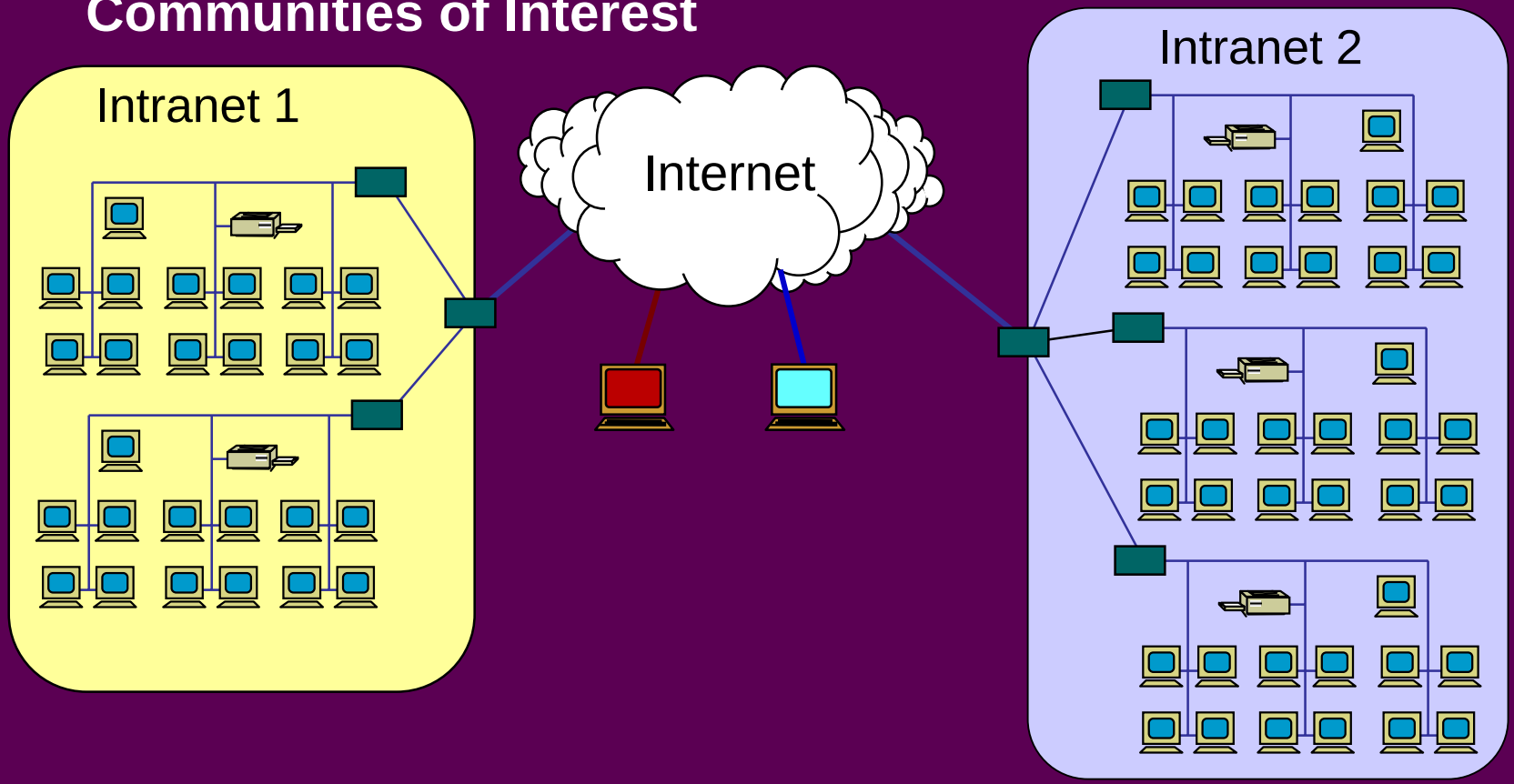


Dealing with Change

- **Requires new approaches and new technologies**
  - » New Computing Model
  - » Transition from Data Center to Distributed Computing
  - » Internet connections and services
- **Introduces new exposures**

Controlling Access

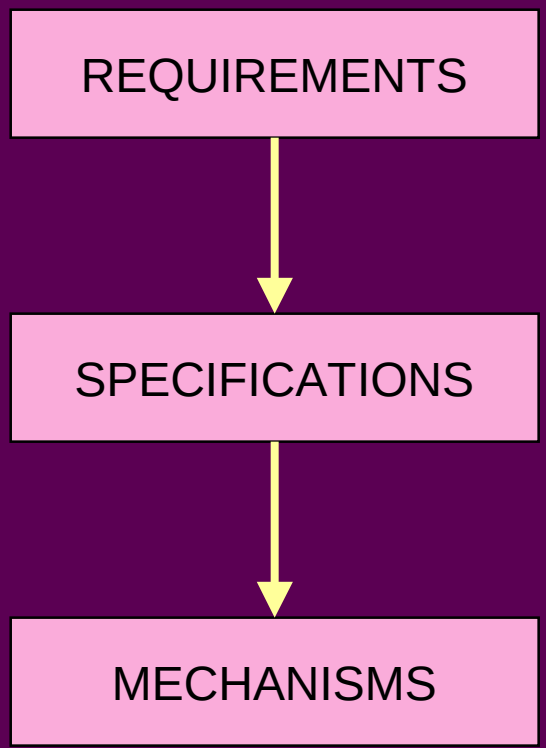
- **Supporting collaboration over multiple overlapping Communities of Interest**



Scalability

- **Network-based components**
  - » Leverage network to distribute services to all connected users
- **Host-based components**
  - » Where visibility and access is required to individual workstations
  - » Requires administration of client configurations
- **Managed Services**
  - » Outsourced operational support solutions

Security Architecture & Engineering

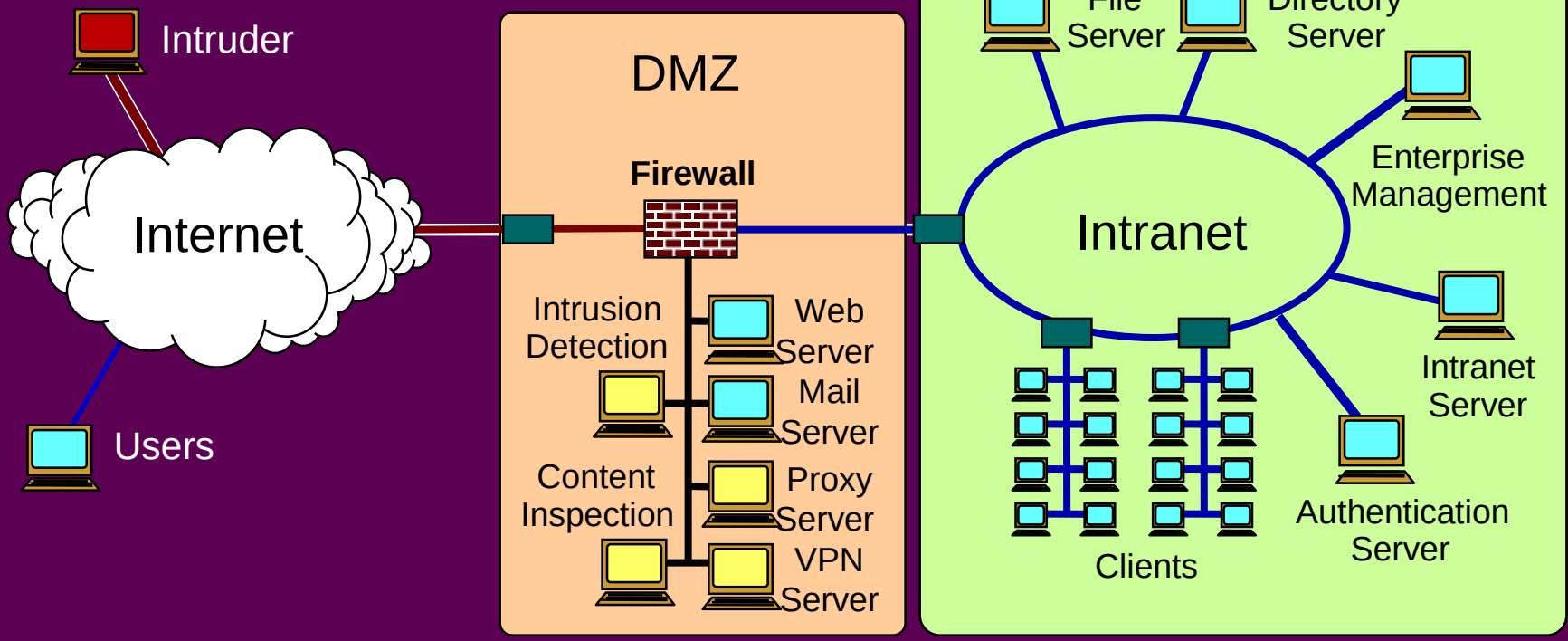


- **Policy**
  - » Business Plan
  - » International, Federal, State Law
  - » Intercompany Agreements
- **Requirements Translation**
  - » Operational Environment
  - » Risk Exposures
  - » User Communities
  - » Information Administration
  - » Security Specifications
- **Design**
  - » Architectural Implementation
  - » Product Performance Specification
  - » Components Selection and Configurations

Security Architecture

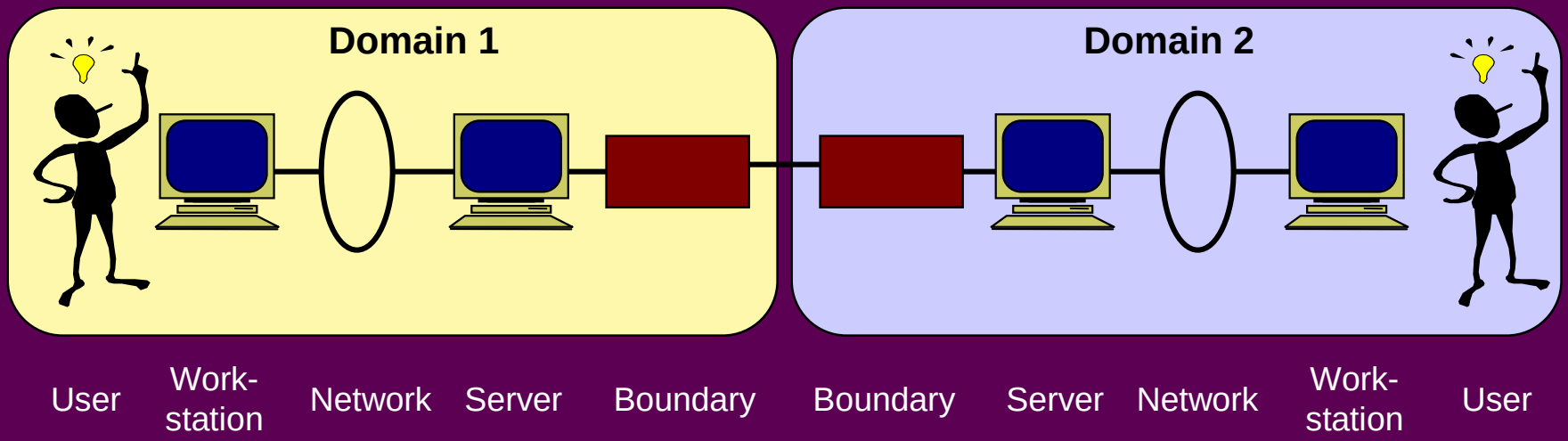
Protect Enforces separation Applies Least Privilege Enforcement Principles	Anti-Virus Firewalls Proxy Server VPN Content Inspection Host access controls Application access controls
Measure Determines the condition of an information system	Network Mapping Vulnerability Assessment Intrusion Detection
Support Provides enabling and infrastructure services	Authentication Directory Incident Response Enterprise Management

Security Architecture

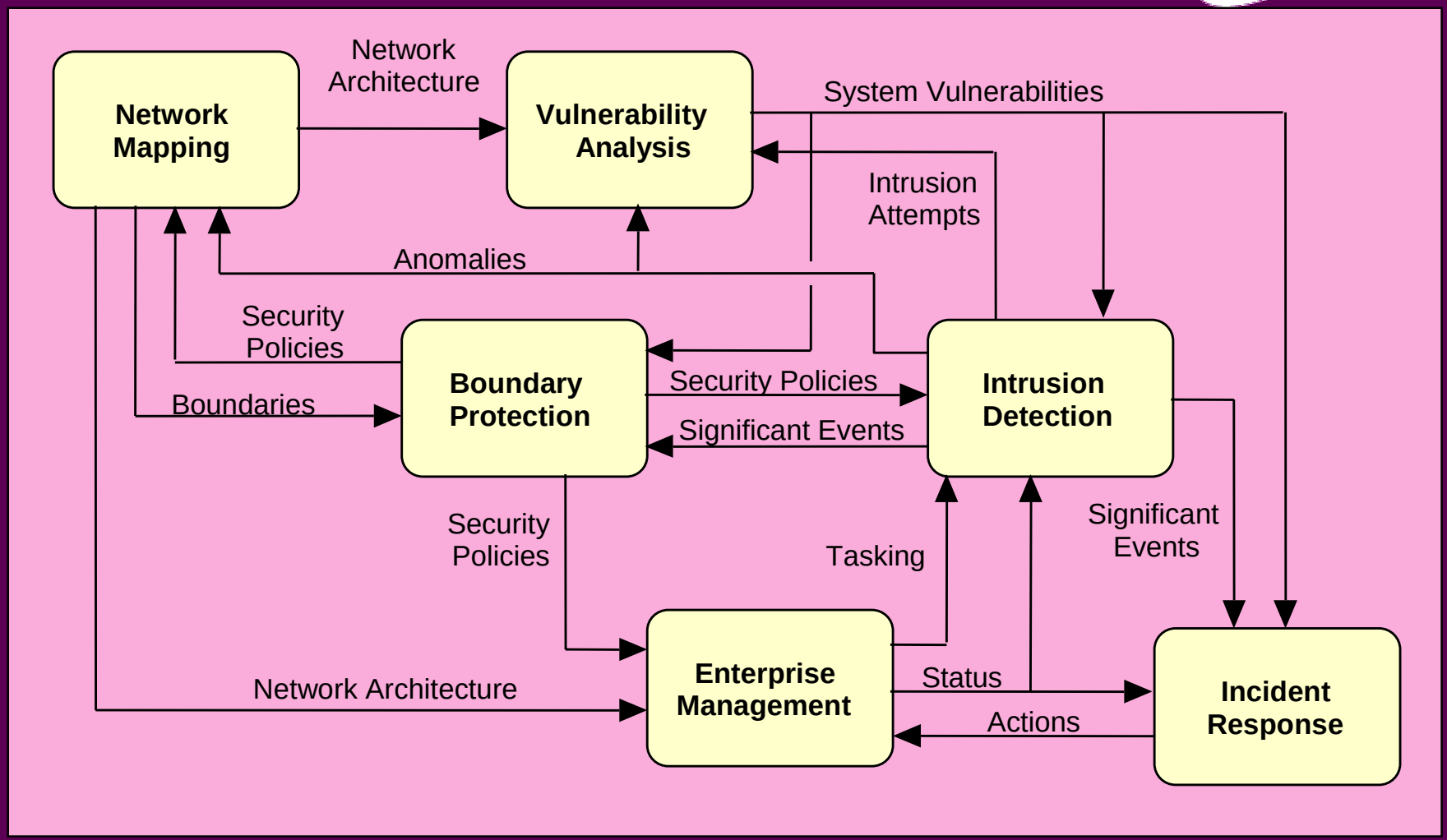


Domain Model

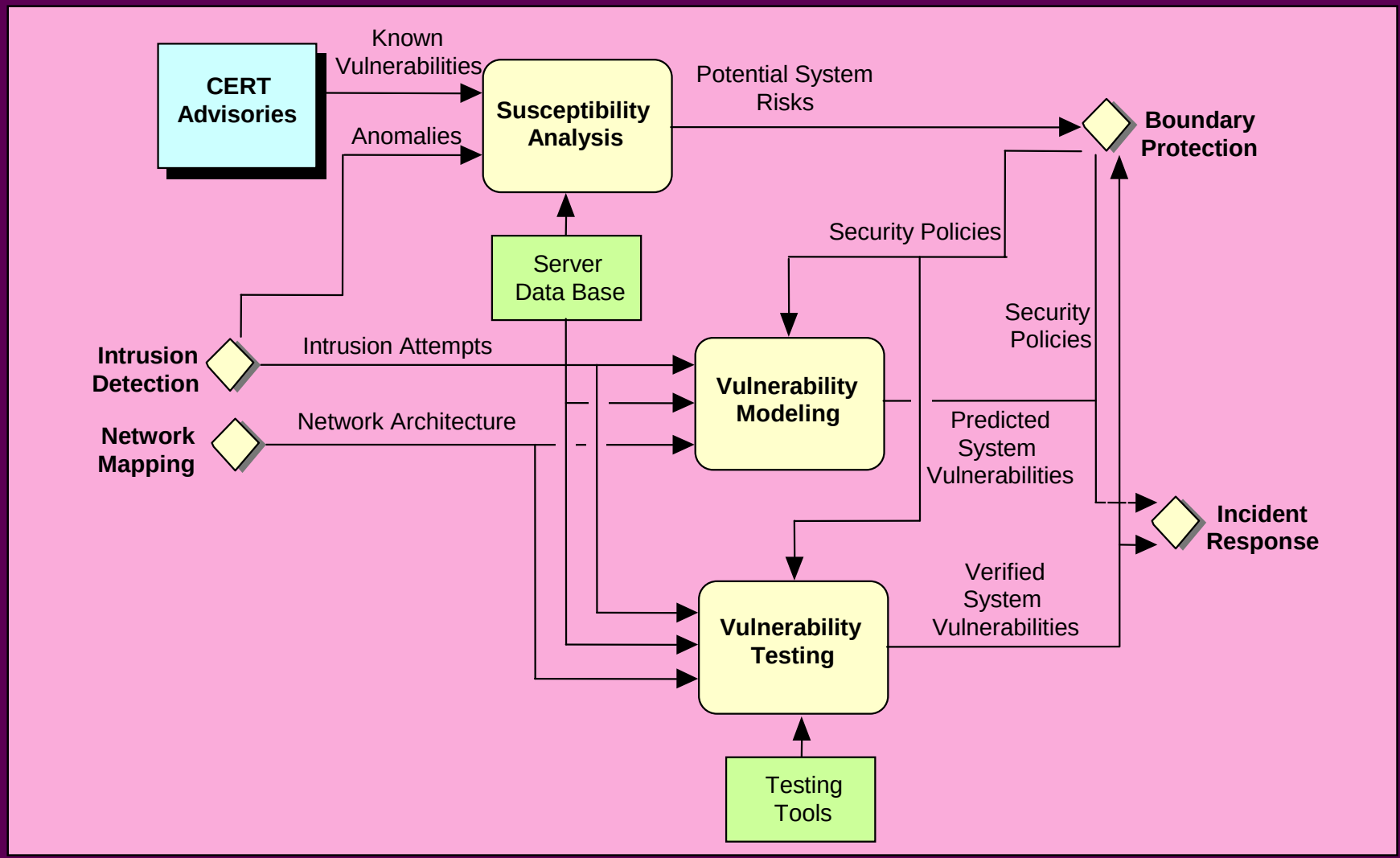
- **Shares security responsibility among each component in functional regions**



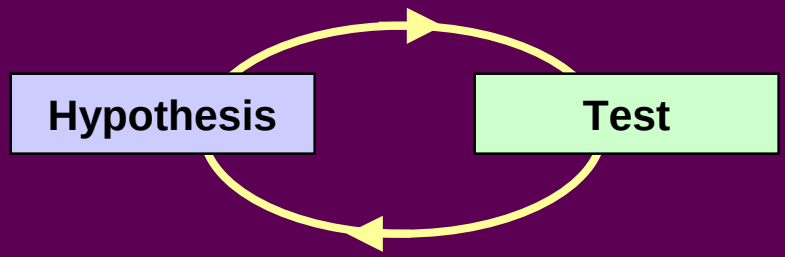
IA Context

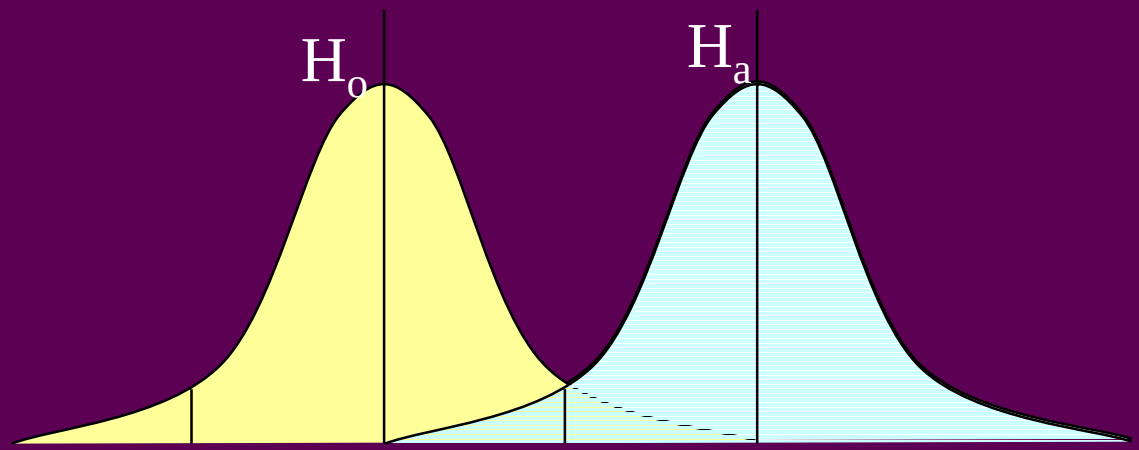

Network Mapping
Network Architecture
Vulnerability Analysis
System Vulnerabilities
Intrusion Attempts
Anomalies
Security Policies
Boundaries
Boundary Protection
Security Policies
Significant Events
Intrusion Detection
Security Policies
Tasking
Significant Events
Network Architecture
Enterprise Management
Status
Actions
Incident Response

Vulnerability Analysis

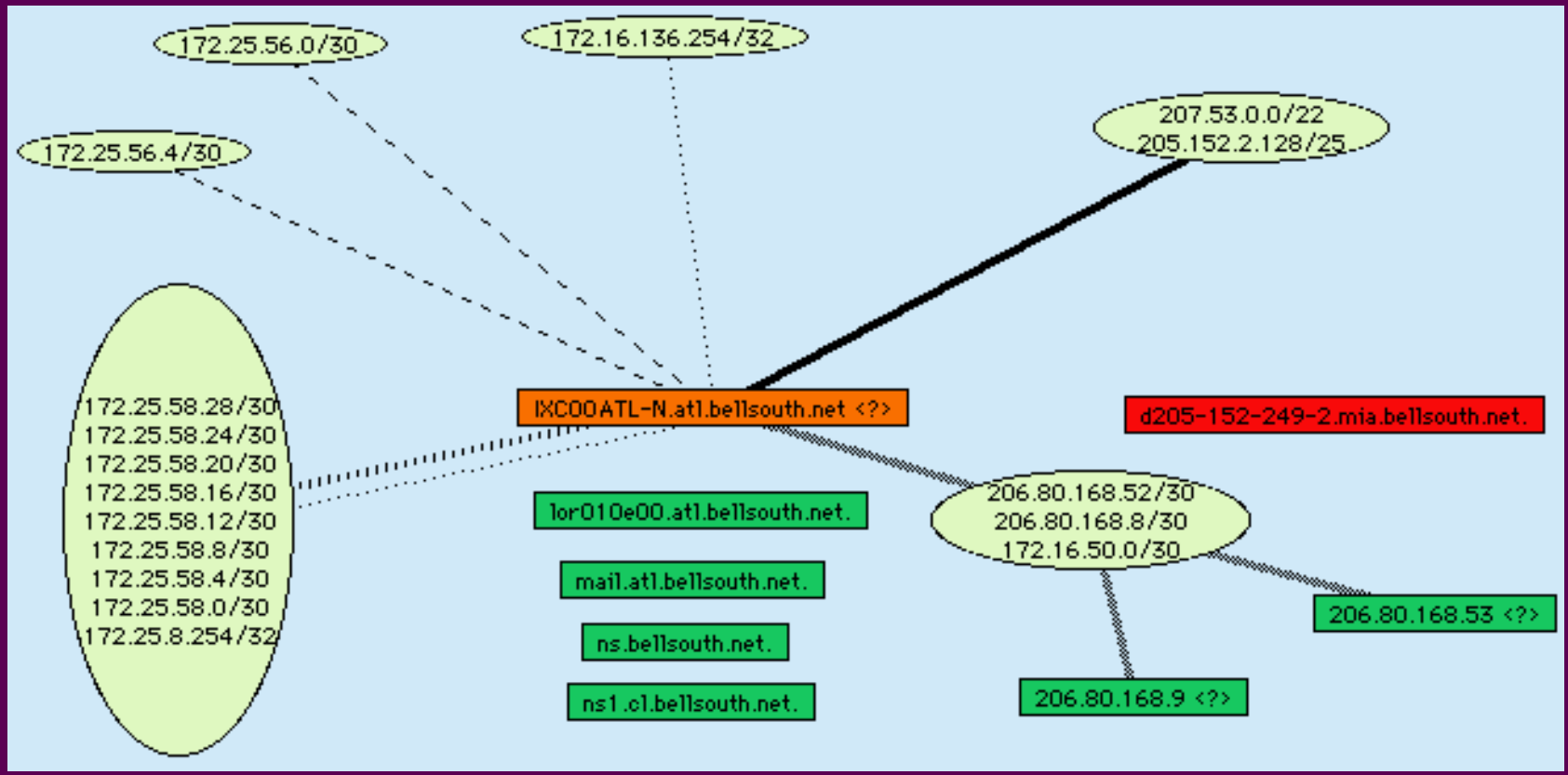


Scientific Method





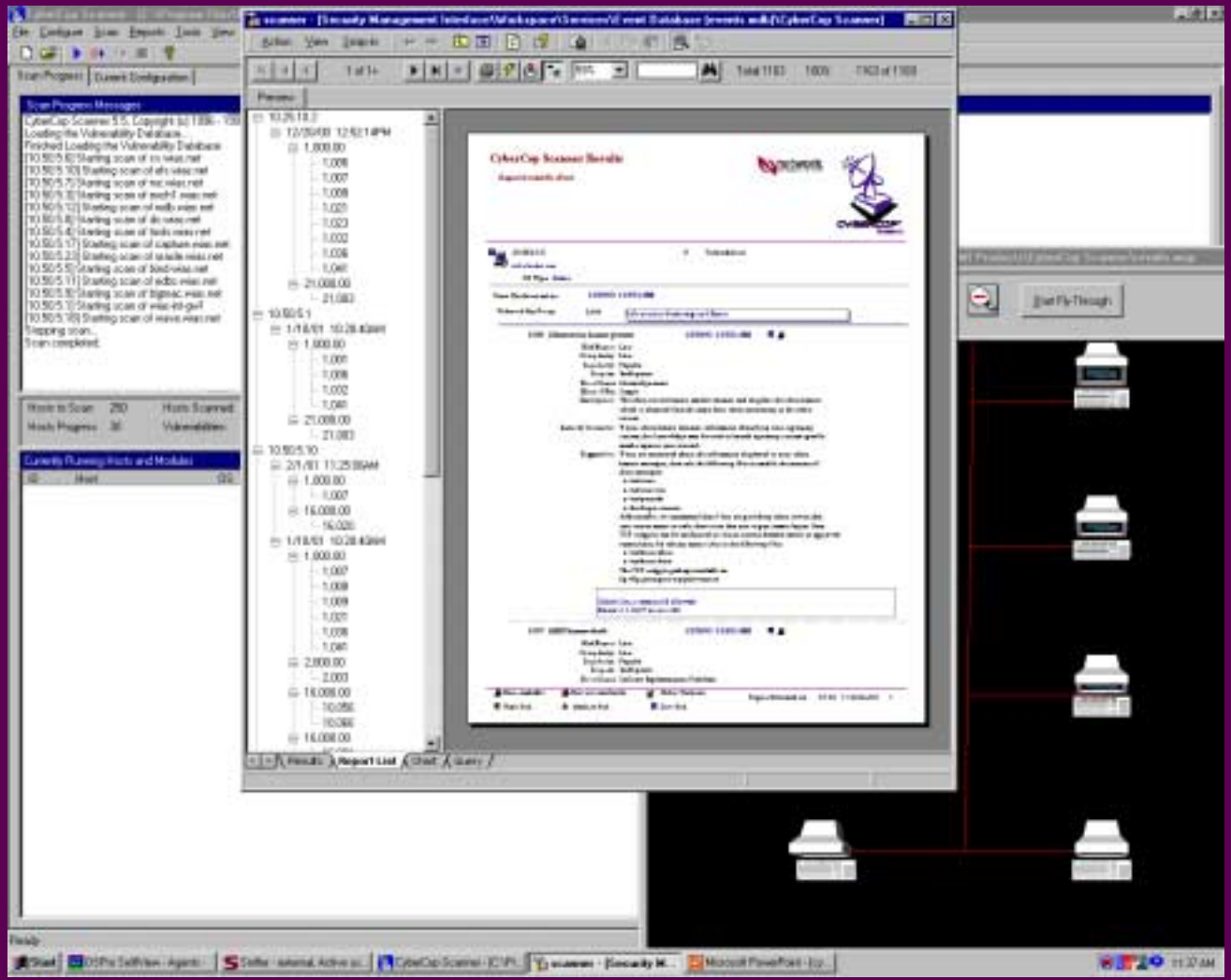
Architecture Testing



System Functional Testing

Host Scanning

WINDERMERE



Intrusion Detection Operations

Contact Information

Dr. Myron L. Cramer

410-266-1900

mcramer@wias.net

http://www.wias.net

Windermere Information Technology Systems

Information Assurance Division

401 Defense Highway

Annapolis, Maryland 21401