www.thei3p.org

Institute for Information Infrastructure Protection

Selected I3P Process Control Systems Research

Robert Cunningham, MIT LL
Team: MITRE, PNNL, SRI, UIUC, U. Tulsa

Presentation to the Process Control System Forum
June 7, 2006

This work was supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

I3P Addresses Federal Cyber Security Needs

Mission: **To help protect the information infrastructure of the US by**

- **Coordinating the development of a comprehensive, prioritized R&D agenda for cyber security, and**
- **Promoting collaboration and information sharing among academia, industry, and government**

Homeland Security

- Funding through the Department of Homeland Security and the National Institute of Standards and Technology

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.

- Managed by Dartmouth College

Dartmouth founded 1769

I3P Research Draws from Academia, FFRDCs, National Laboratories, and Nonprofit Organizations

- Academic Research Institutions

CERIAS, Purdue University
Center for Information Security, U. of Tulsa
Computer Security Lab, UC, Davis
Cornell University
Critical Infrastructure Protection Project, George Mason University
Georgia Tech Information Security Center
Heinz School of Public Policy and Management, Carnegie Mellon University
Information Security Lab, Oregon State U.
Information Technology and Operations Center, United States Military Academy
Information Trust Institute, University of Illinois at Urbana-Champaign
Institute for Civil Infrastructure Systems, NYU
Institute for Security Technology Studies, Dartmouth College
Johns Hopkins University Information Security Institute
Stanford University
University of California, Berkeley
University of Virginia

- National Laboratories
  - Lawrence Berkeley National Lab
  - Los Alamos National Laboratory
  - Pacific Northwest National Lab
  - Sandia National Labs
- FFRDCs
  - MIT Lincoln Laboratory
  - The MITRE Corporation
  - Software Engineering Institute at CMU
- Nonprofit Organizations
  - Mitretek Systems
  - The RAND Corporation
  - SRI International

Research Problem: Develop tools to design, verify and configure secure PCSs

- Support Secure Operations
  - Risk management for configuration and deployment
  - Assess architectural security vulnerabilities
  - Model and monitor correct behavior
- Enable Secure Components
  - Application software
  - Protocols and protocol stacks
  - Operating systems

- Lead – MIT/LL – Rob Cunningham
- Team members – MIT/LL, SRI, University of Illinois, MITRE, PNNL, Tulsa

Why Security is Hard: The Attacker has the Advantage

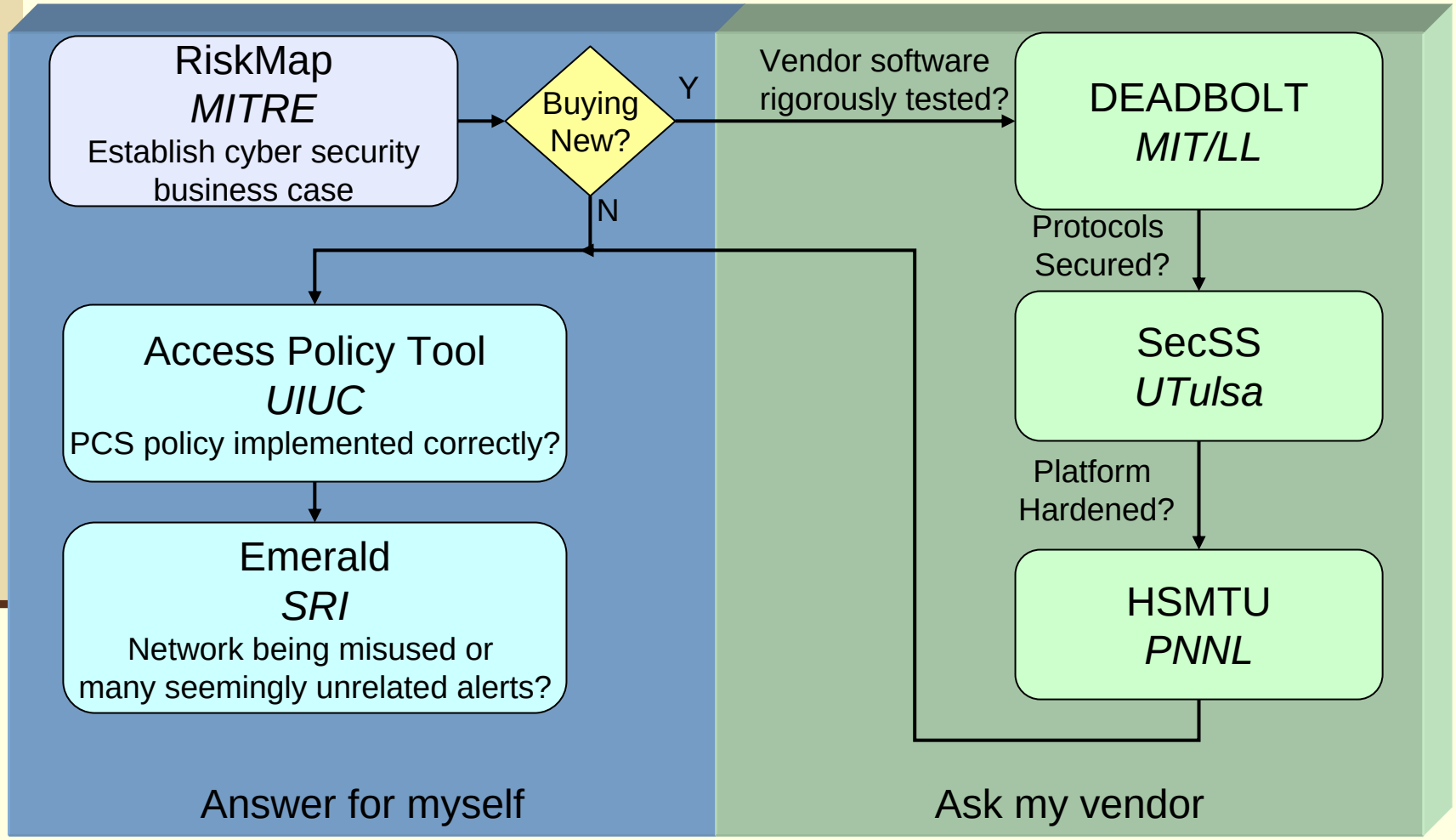
- The defender must defend all input points
- The defender must defend at all times
- The defender must limit defense to legal approaches
- The defender can defend only against known attacks

- The attacker can choose the weakest point
- The attacker can choose the weakest time
- The attacker can use approaches that are illegal
- The attacker can probe for unknown vulnerabilities

Solution: Proactive security development where the defender thinks like an attacker, then limits possible attacks

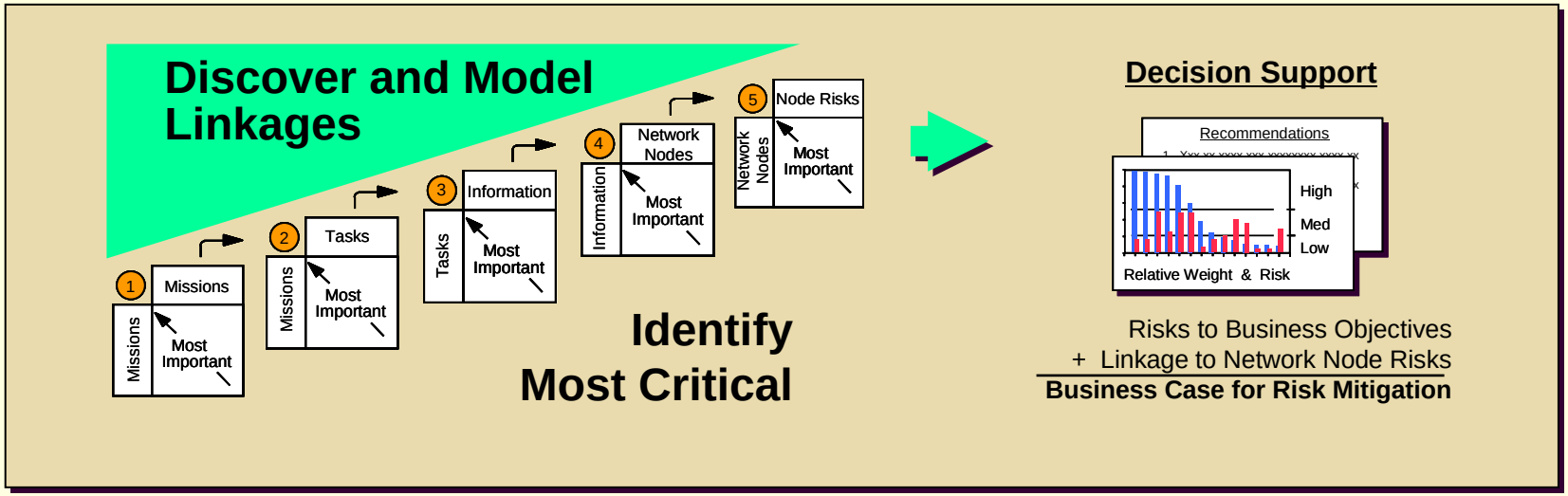
Derived from Howard and LeBlanc, "Writing Secure Code 2nd ed.," 2003

Tool Relationship: An Operator's View



Note: This is only the dominant activity of each performer

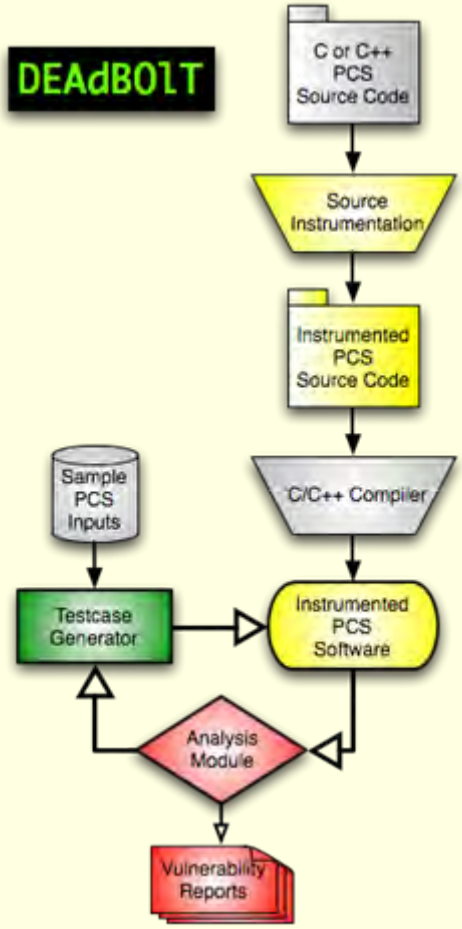
Assess Security Risks in Business Context



RiskMap

- RiskMap model for Ergon refinery delivered & in use
- Generalized RiskMap template for Oil sector in work
- Template for Natural Gas sector is next

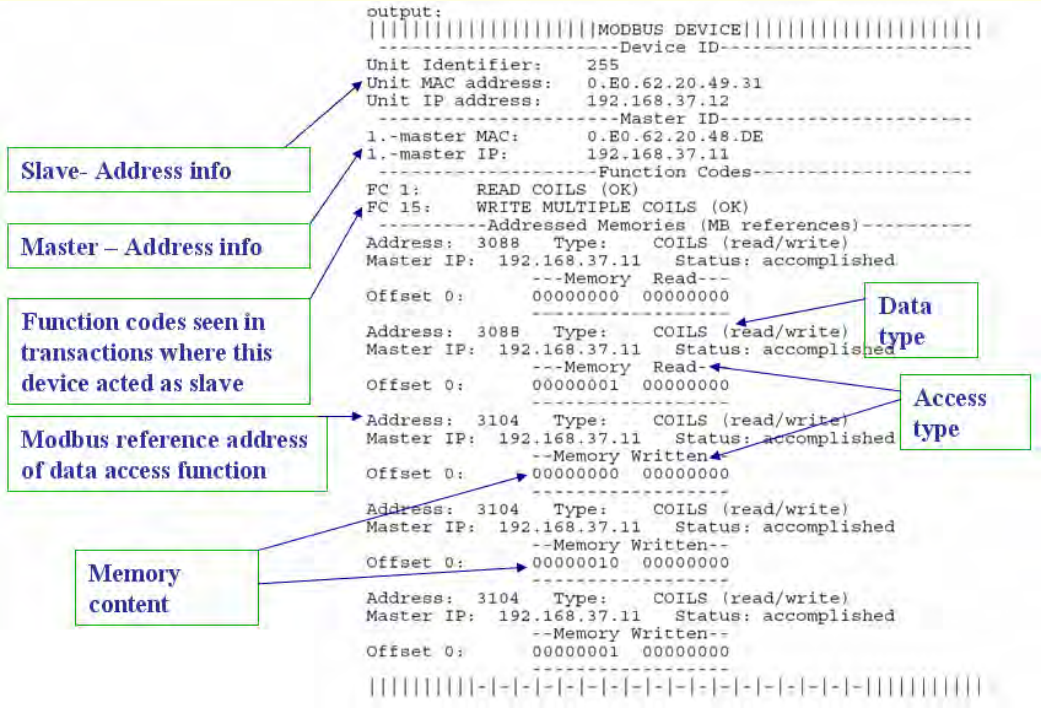
Improve Security of PCS Software



- DEADBOLT is designed for securing real-time PCS software during testing
  - Approach will work with most compliant C++ environments
  - Automatically tests for most important class of cyber attacks
- Established a partnership with Emerson Process
  - Emerson provides: PCS expertise, next-generation software
  - Lincoln provides: Cyber security expertise

Secure PCS Protocols via Security Service Suite (SecSS)

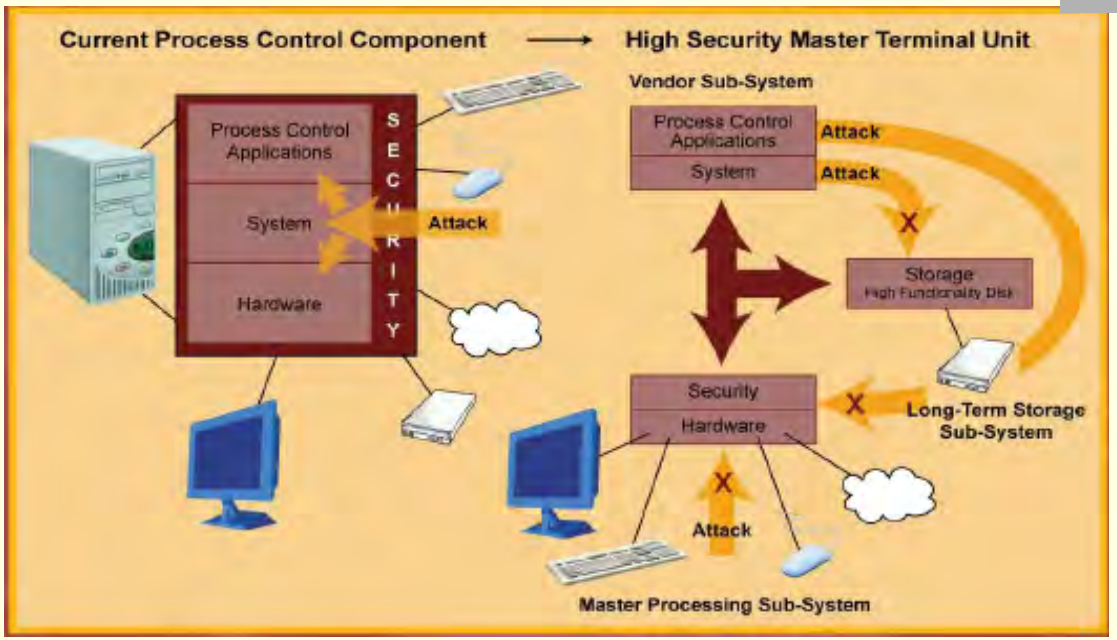
- Supports
  - RTU monitoring
    - Operating
    - Address config
  - System integrity
    - Presence of rogue masters/slaves
  - Detect changes in structure and availability
    - Operations
    - Data transfers
- Approach
  - Use standard PCS protocols (more than IP)
  - Reduce risk of RTUs tha do not respond well to certain TCP/IP messages



Example Output –

Passive Modbus Network Scanner

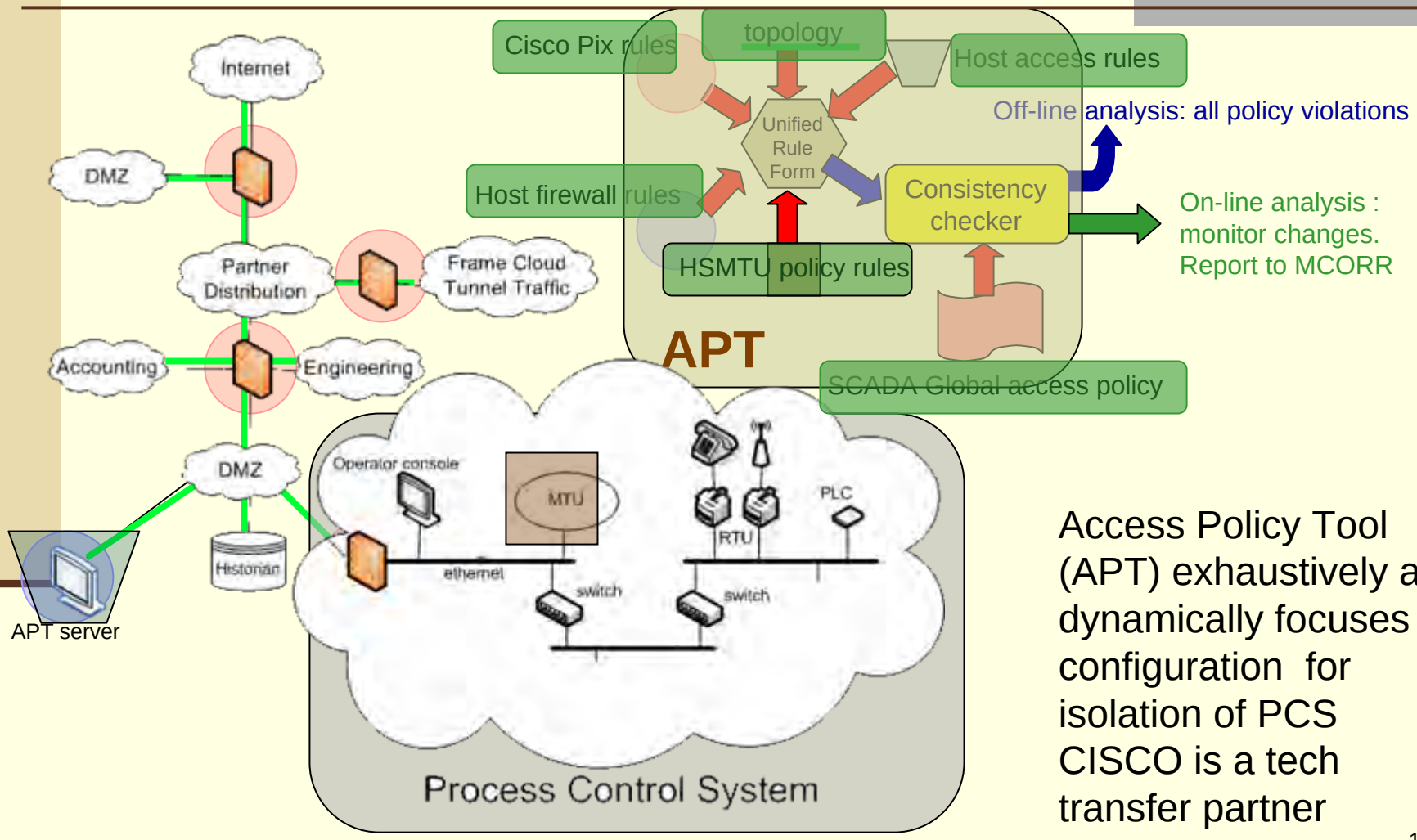
Secure the host with the High Security Master Terminal Unit



HSMTU

- Logically replaces a standard open-source based process control component with three high performance (open-source) commodity systems that:
  - Reduce possibility of privilege escalation
  - Detects tampering and takes evasive action where possible
  - Controls and protects local fixed and removable storage media from insider threats.

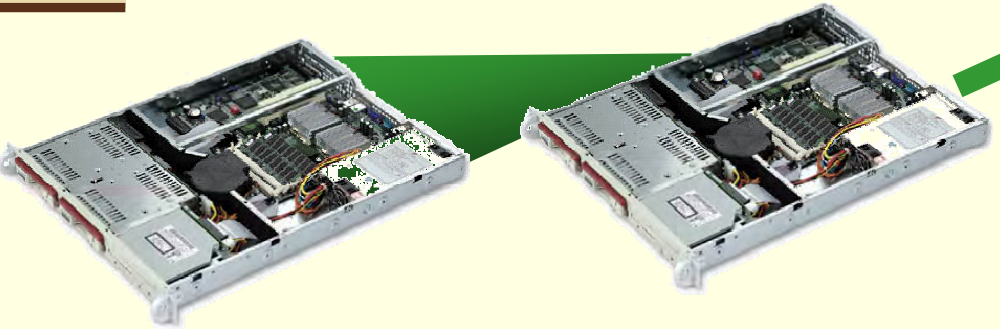
Assess PCS Access Policy Implementation

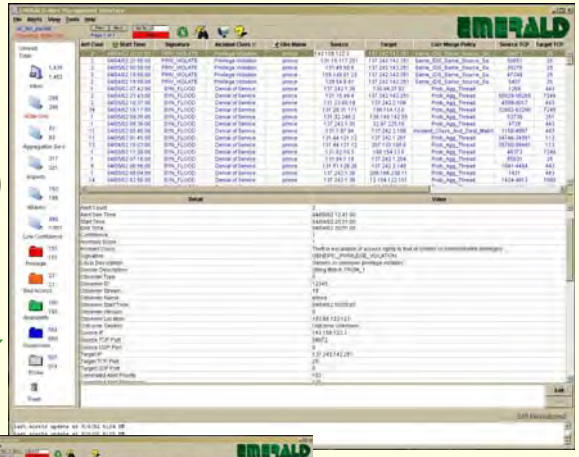


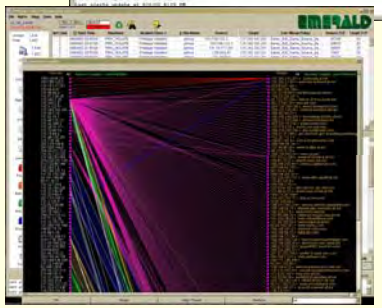
Access Policy Tool (APT) exhaustively and dynamically focuses on configuration for isolation of PCS CISCO is a tech transfer partner

EMERALD IDS for PCS

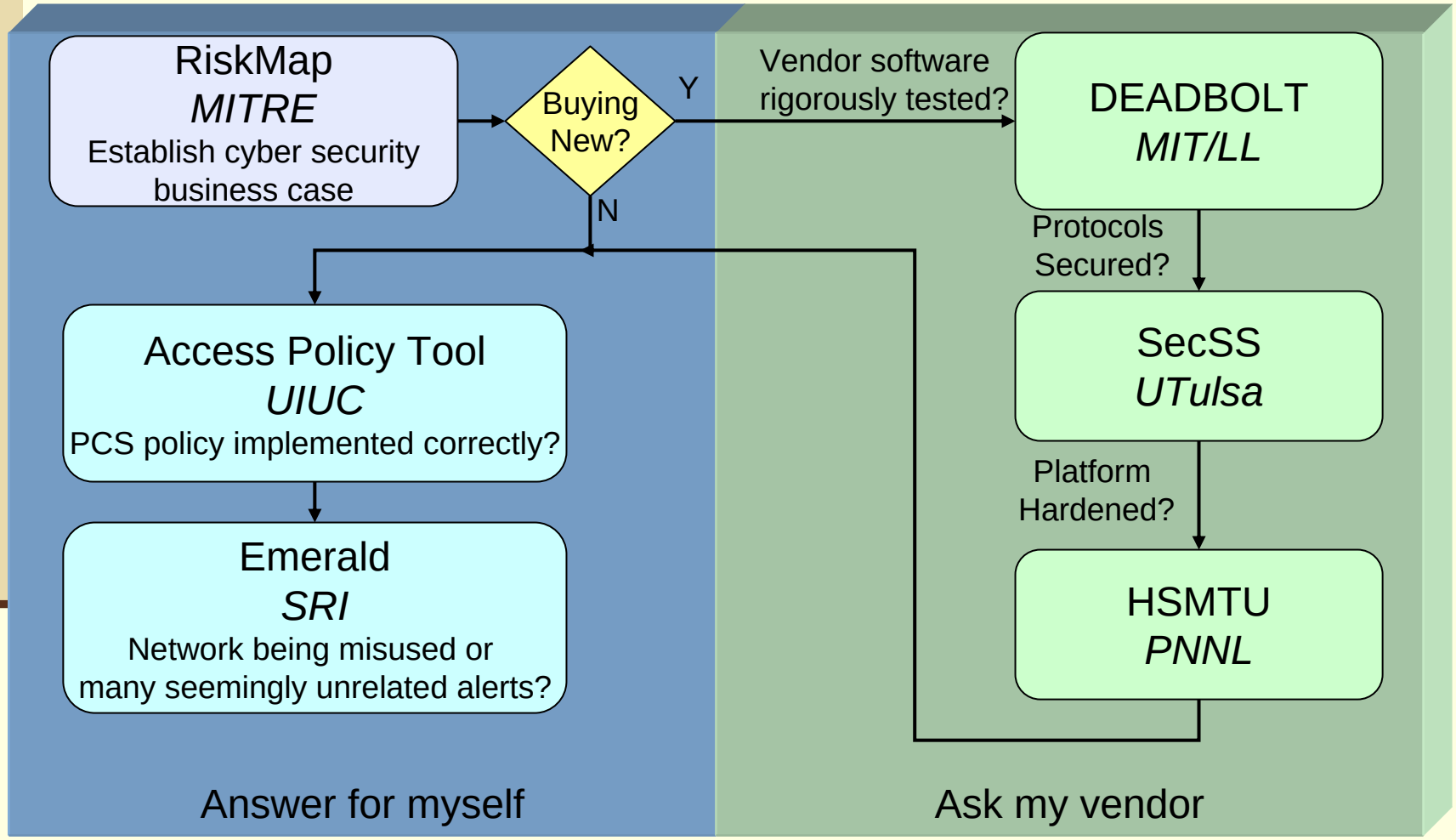
- Multi-algorithm IDS appliance
  - Bayes analysis o TCP headers
  - Stateful protocol eXperts
  - Complemented by custom ruleset SNORT
- Digital Bond PCS rule set
- Additional SRI rule set allows specification of allowed connections
- Alerts (potentially from multiple IDS appliances) forwarded to correlation framework







Tool Relationship: An Operator's View



Note: This is only the dominant activity of each performer

2nd Industry Workshop June 8, 2006

- Focused on presentation and demonstration of research results in action-ready format

Understanding The Problems
- Vulnerabilities
- Metrics
- Interdependencies
- Risk Analysis

Understanding The Solutions
- Secure Design
- Security Monitoring
- Information Sharing
- Future Trends

- We will collect stakeholder feedback

I3P Workshop: Thursday, June 8
My session attendees will learn…

- What a buffer overflow is, why it can cause a problem, and what a vendor could do about it (DEADBOLT)
- What the principle of least privilege is, why it's important to limit the privileges of programs and personnel, and how one could do this on a single host (HSMTU) and across a network (APT)
- What "defense in depth" is and how can the use of these three programs protect a PCS network

➔ **In this and other sessions, see working demonstrations of all tools described today!**