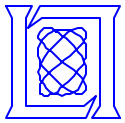
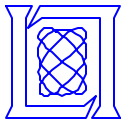


Proposed 1999 DARPA Off-line Intrusion Detection Evaluation Plans

Richard Lippmann

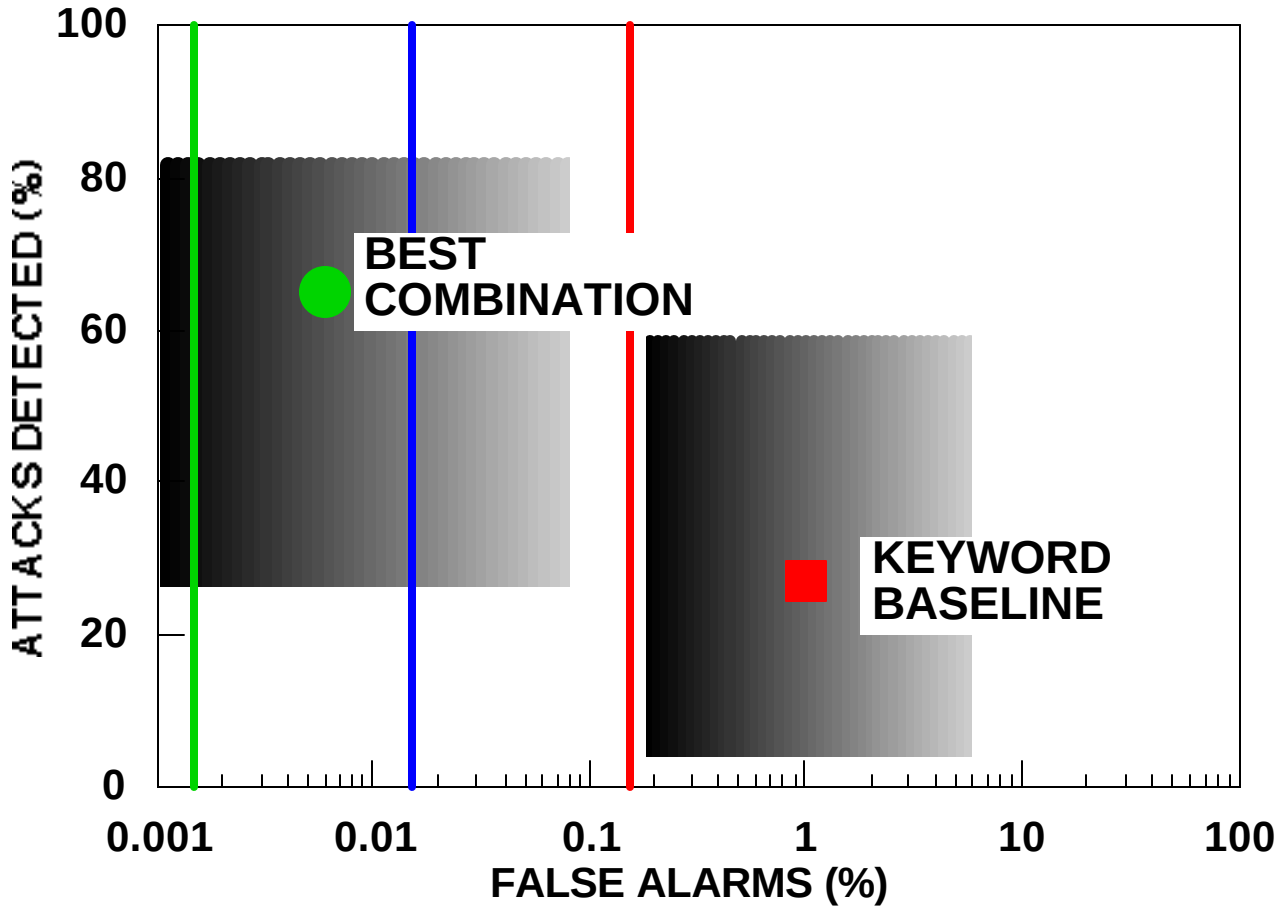
MIT Lincoln Laboratory



Overview of Last Year's 1998 Evaluation

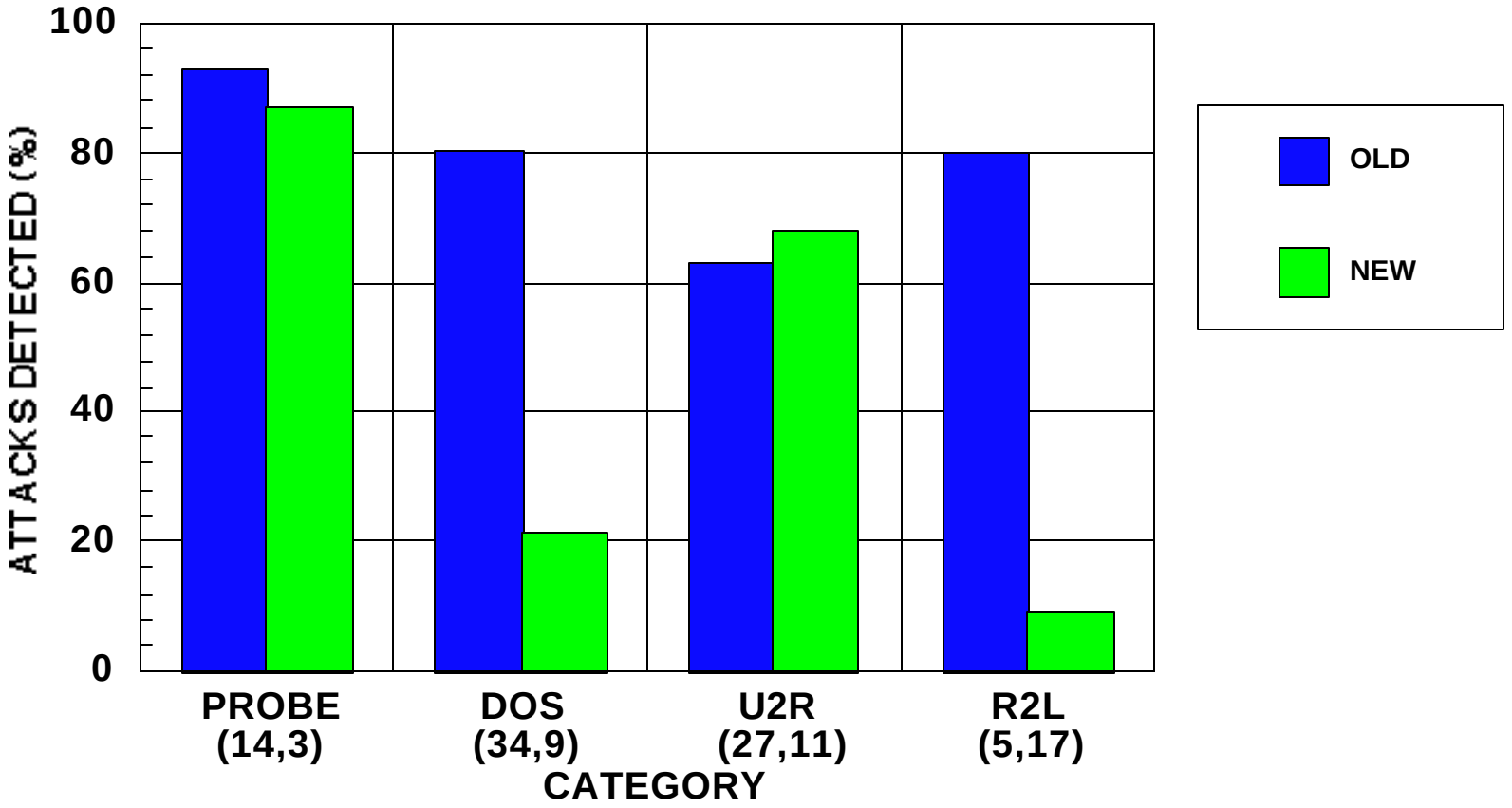
- **Last Year's 1998 Evaluation Was The First Comprehensive Realistic Evaluation of Intrusion Detection Systems**
- **Extremely Successful**
  - **Results Focused Research, and Highlighted Current Capabilities and Recent Advances**
  - **Procedures Worked Well, Many Successful Participants using Different Approaches**
  - **We now have the first large baseline corpus of background traffic and attacks for algorithm development and testing**
- **Only Minor Procedural Changes are Necessary for 1999**

Best Combination System from 1998 Evaluation Compared to Keyword Baseline

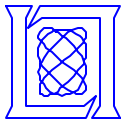


- More Than Two Orders of Magnitude Reduction in False Alarm Rate With Improved Detection Accuracy, Most Errors are in New Attacks
- Keyword Baseline Performance Similar to That of Commercial and Government Keyword-Based Systems

Best Systems in 1998 Evaluation Didn't Accurately Detect New Attacks



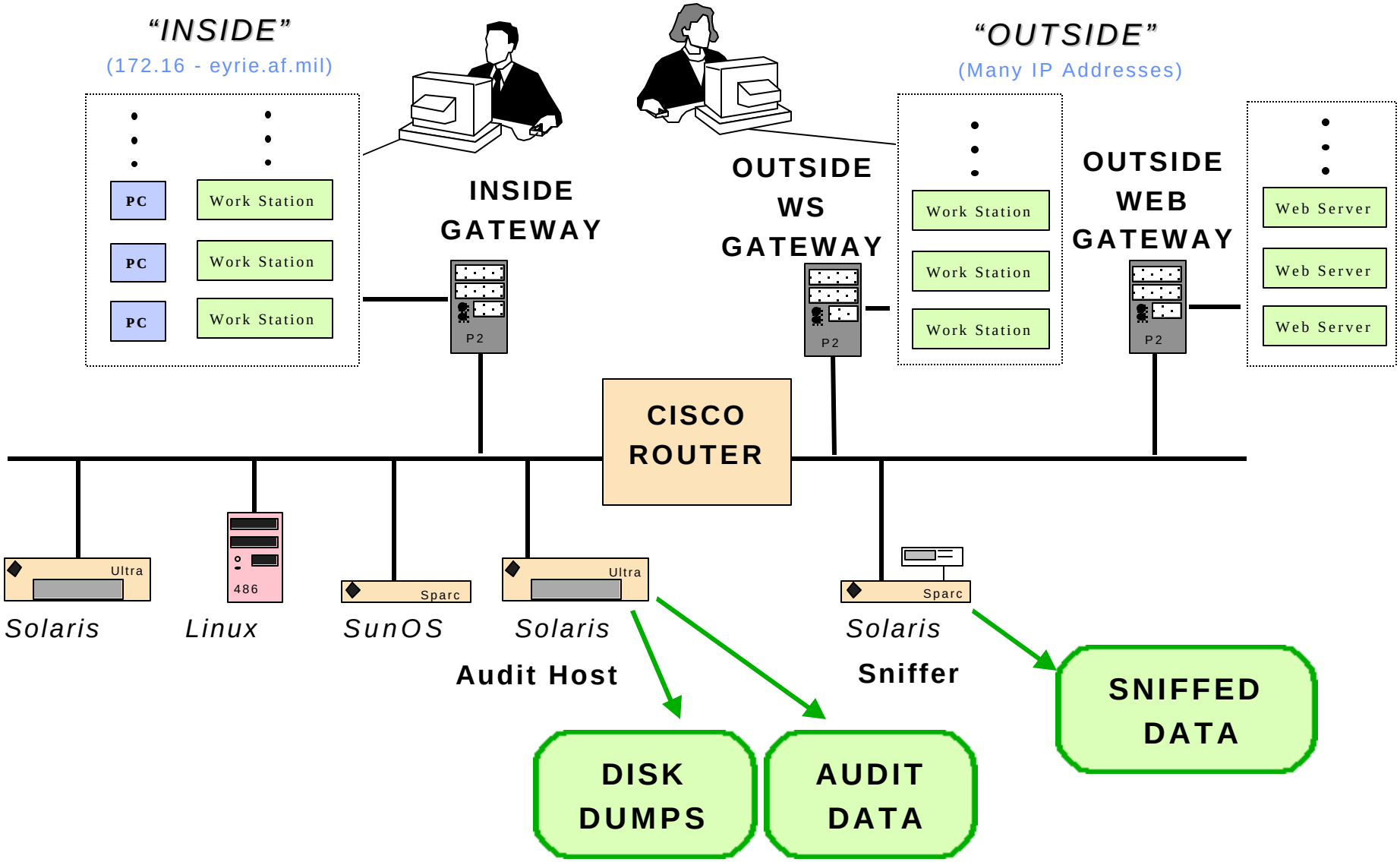
- Systems Generalize Well to New Probe and User to Root Attacks, but Miss New Denial of Service and Remote to Local Attacks
- Basic Detection Accuracy for Old Attacks Must Also Improve



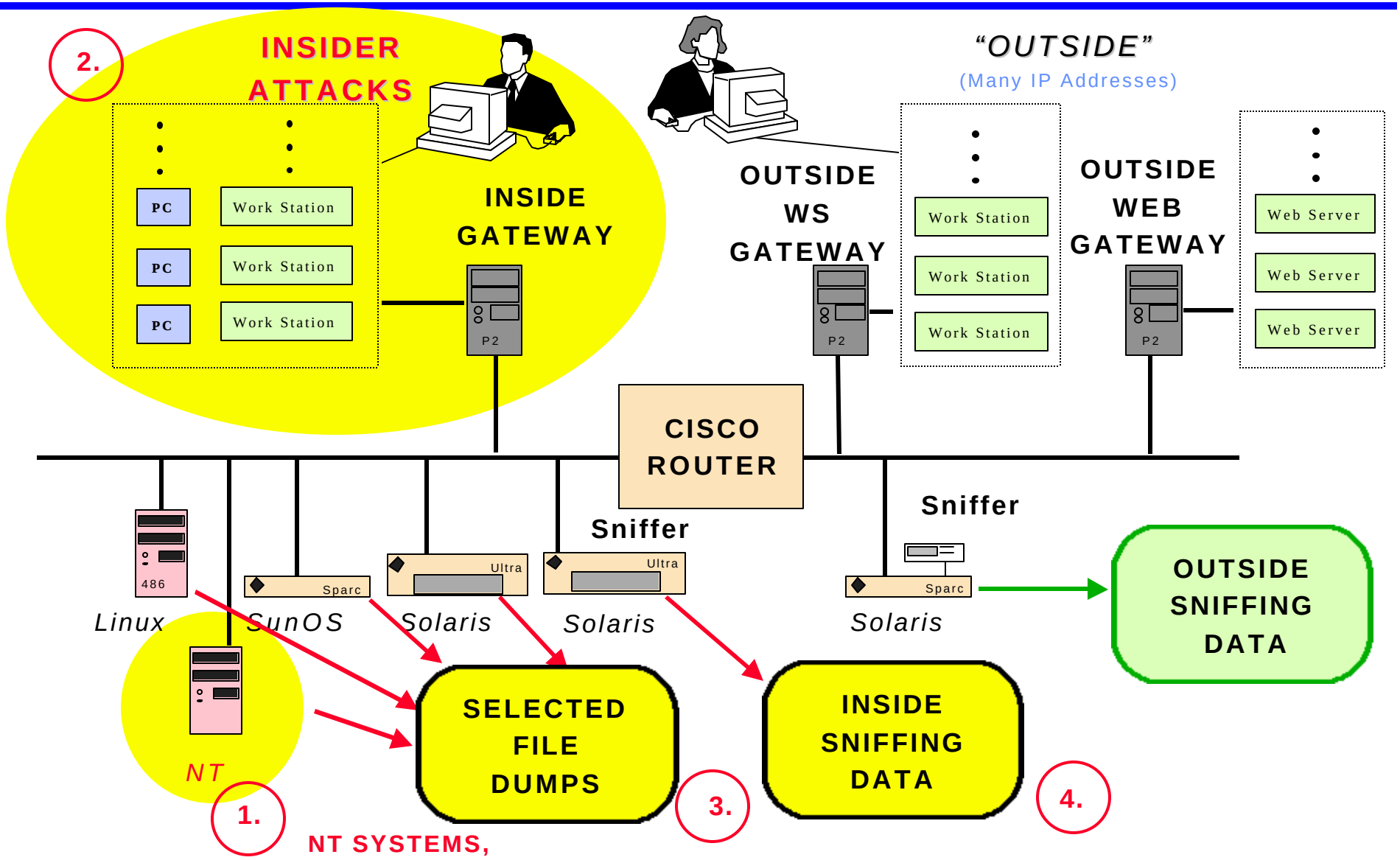
Goals of 1999 Evaluation

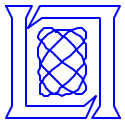
- Measure Ability of Intrusion Detection Systems to Detect New Attacks
  - Extend Beyond Signature-Based Approaches
  - This Requires Many New Attacks
- Add NT Workstation Victim to the Simulation Net
  - NT Traffic and Attacks
- Add Insider Attacks
- Provide Selected File System Dumps
  - Provide Important Components from File Systems of Five Victims Each Night (Includes NT Audit Logs)
- Provide Inside Sniffing Data

Last Year's 1998 Simulation Network



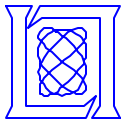
New Features in 1999 Evaluation





Major New Features for 1999

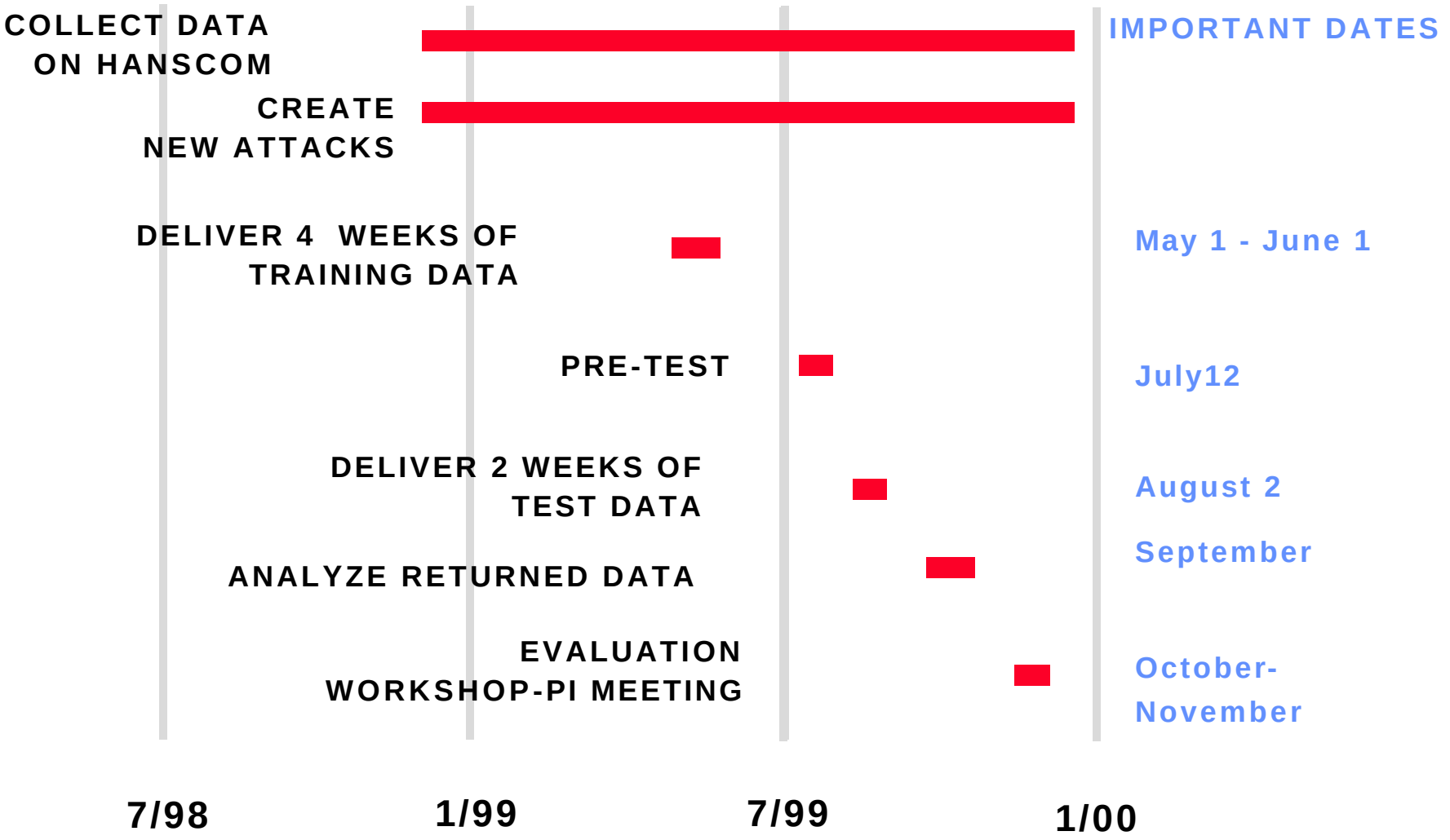
- NT Workstation
  - NT Traffic and Attacks
- Insider Attacks
- Selected File System Dumps
  - Provide Important Components from File Systems of Five Victims Each Night (Includes NT Audit Logs)
  - We Will No Longer Provide Complete File System Dumps
- Provide Inside Sniffing Data

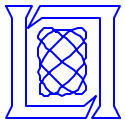


Minor Changes for 1999

- Simplify Scoring Procedure
  - No Longer Use List Files
  - Evaluate Attack Detection and Identification Separately
- Add a New Attack Category “Data Compromise”
- Last Week of Training Data Contains No Attacks to Assist Training Anomaly Detectors
- No Longer Provide ASCII Praudit BSM Audit Data
- No Longer Provide psmonitor output
- Provide Security Policy for Eyrie Air Force Base
- Fewer Overlapping Attacks in Training/Test Data

Proposed Time Line for 1999 Evaluation





Provide Feedback and Suggestions

- Send Email to jhaines@sst.ll.mit.edu
- For More Information Look at the Lincoln Laboratory Intrusion Detection Evaluation Web Site
  - ADDRESS: ideval.ll.mit.edu
  - USER: ideval
  - PASSWORD: daRpa98!