

TRAINING

Through lab-based Mu-4000 analyzer training, carriers, critical infrastructure, government agencies and product developers are learning how to minimize their product or service attack surface. Mu Dynamics is already helping both end-users and their product developers use a process-oriented, proactive approach to security and robustness analysis as well as vulnerability isolation throughout their respective product development and end-user deployment lifecycles. Hands-on use of the Mu-4000 provides unbiased metrics for real management of security and robustness for the first time, and greatly expedites fault remediation.

Product Developers

Theory and labs demonstrate how to use the Mu-4000 analyzer's customized, process-oriented approach to build security and robustness analysis into the product development lifecycle. QA teams and Lab Managers discover how to quickly isolate and reproduce faults in their local environment before adversely impacting their end-user customers.

Students will become familiar with the export and use of actionable remediation tools and reports that help accelerate the process of eliminating a flaw. Developers learn how to use regression to verify that fixes are effective as well as to ensure that no previously discovered fault ever creeps back into a product.

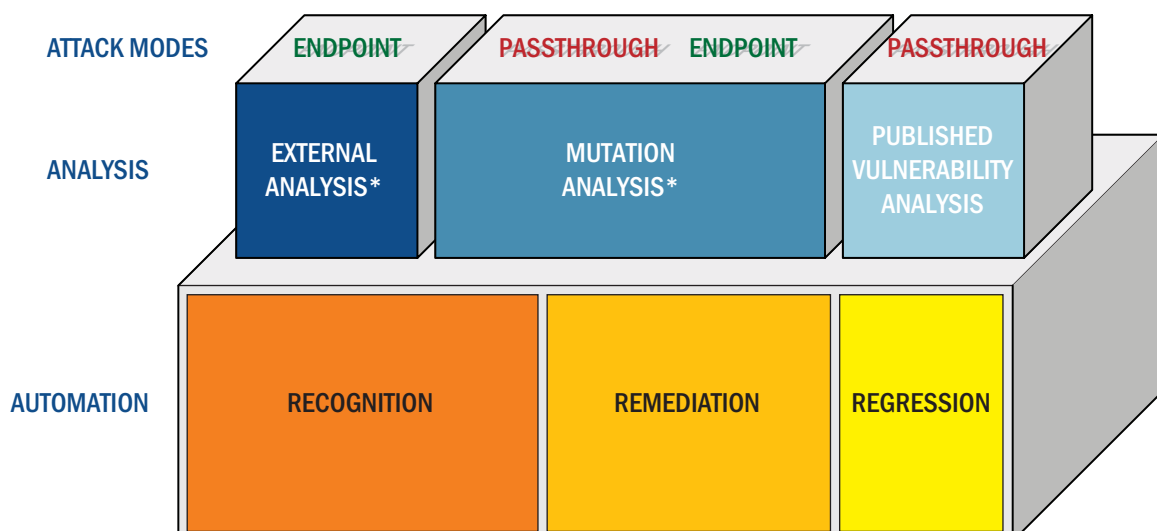
Service Provider, Critical Infrastructure and Enterprise End Users

Through hands-on training, end-users learn how the Mu-4000 analyzer plays a critical role in their product deployment lifecycle. Unprecedented and unbiased security and robustness metrics allow Security Engineers to better evaluate products.

Operations executives learn how early identification of their unique attack surfaces and respective disruptive vulnerabilities can prevent costly service downtime, revenue loss and ultimately customer turnover. Customers will learn how to provide effective remediation tools to developers that reduce the "mean time to repair" and use regression to easily validate vendor fixes once they are released.

Additional Training Topics

Training topics include three types of analysis (Mutation Analysis, Published Vulnerability Analysis, and External Analysis) and attack modes (Endpoint and Passthrough). Specific details of Mu Dynamics' automation foundation, analysis process and attack modes all covered within training are detailed [online](#).



* Supports Adaptive Analysis

Training Class Breakout

Introduction to Mu Dynamics

- Pre-emptive Hacking
- Attack Surface Analysis
- Target Configuration Options

Setup and Administration

- Getting Started
- Updating and Securing the Platform

Analysis Options

- Mutation Analysis Theory
- Instrumentation, Monitors, and External Vectors

Licensing and Support

- Mu-4000 Platform Capabilities
- Protocol Mutations, Published Vulnerabilities and External Analysis
- Getting Help

Advanced Analysis

- Protocol Spidering
- Regression Analysis
- Endpoint and Passthrough Analysis

Regression and Remediation

- Fault Management
- Best Practices

Participants learn to:

- Set up the Mu-4000 hardware and user accounts
- Apply protocol and feature updates and manage platform licenses
- Use contextual, online, and live help resources
- Configure Instrumentation and Monitors for a target
- Discover and replicate 0-day security and robustness issues
- Drive third-party toolsets with External Analysis
- Validate software and hardware products using 3+ years of Published Vulnerabilities
- Use regression analysis to validate new releases/patches
- Research vulnerabilities with built-in expert analysis and create detailed reports
- Export trace files and other tools to help remediate the fault
- Apply security analysis to every phase of the product lifecycle



web: www.mudynamics.com | email: info@mudynamics.com
address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA
phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317