Remediation Reference Implementation

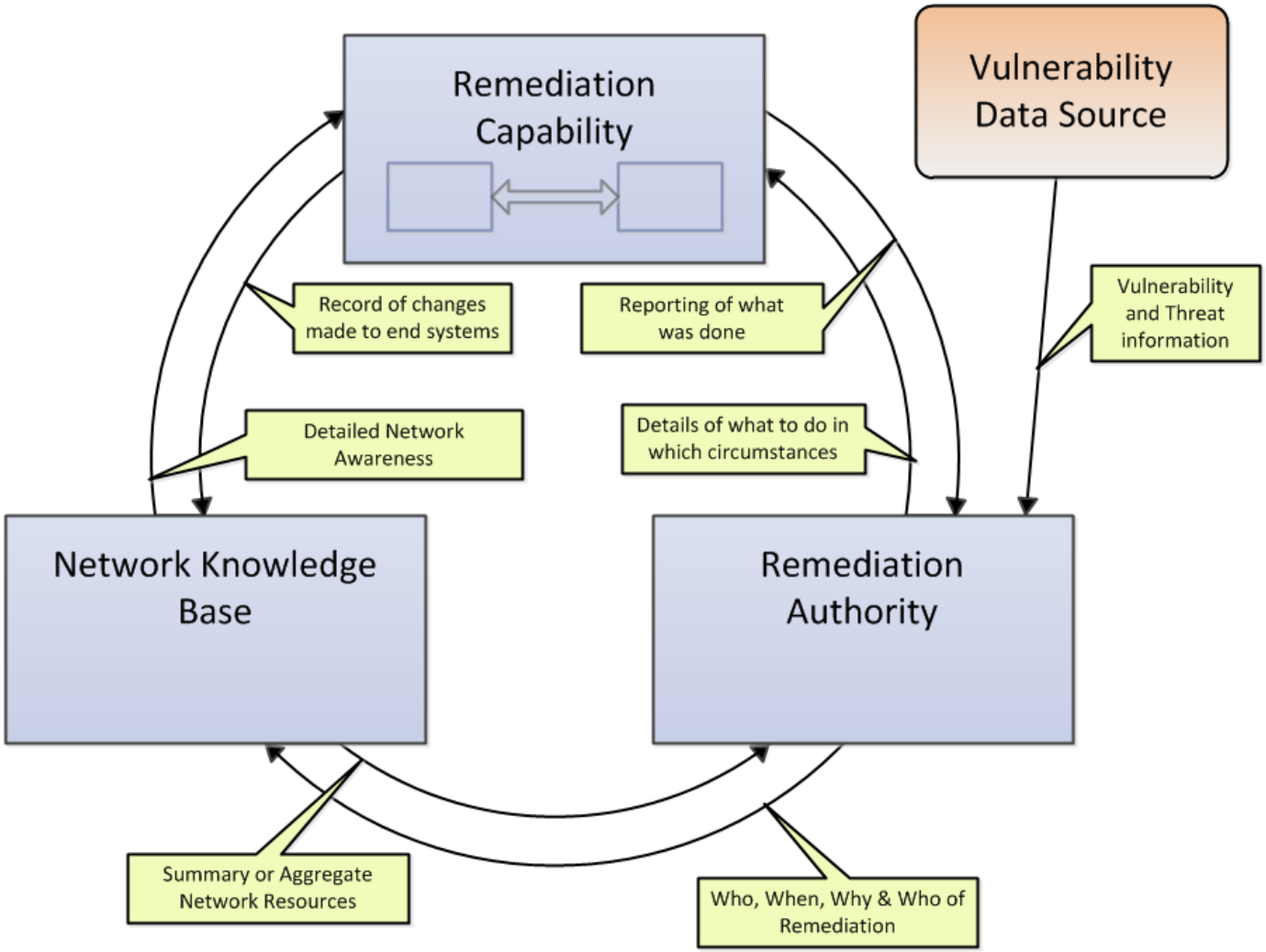
24 March 2011

MITRE

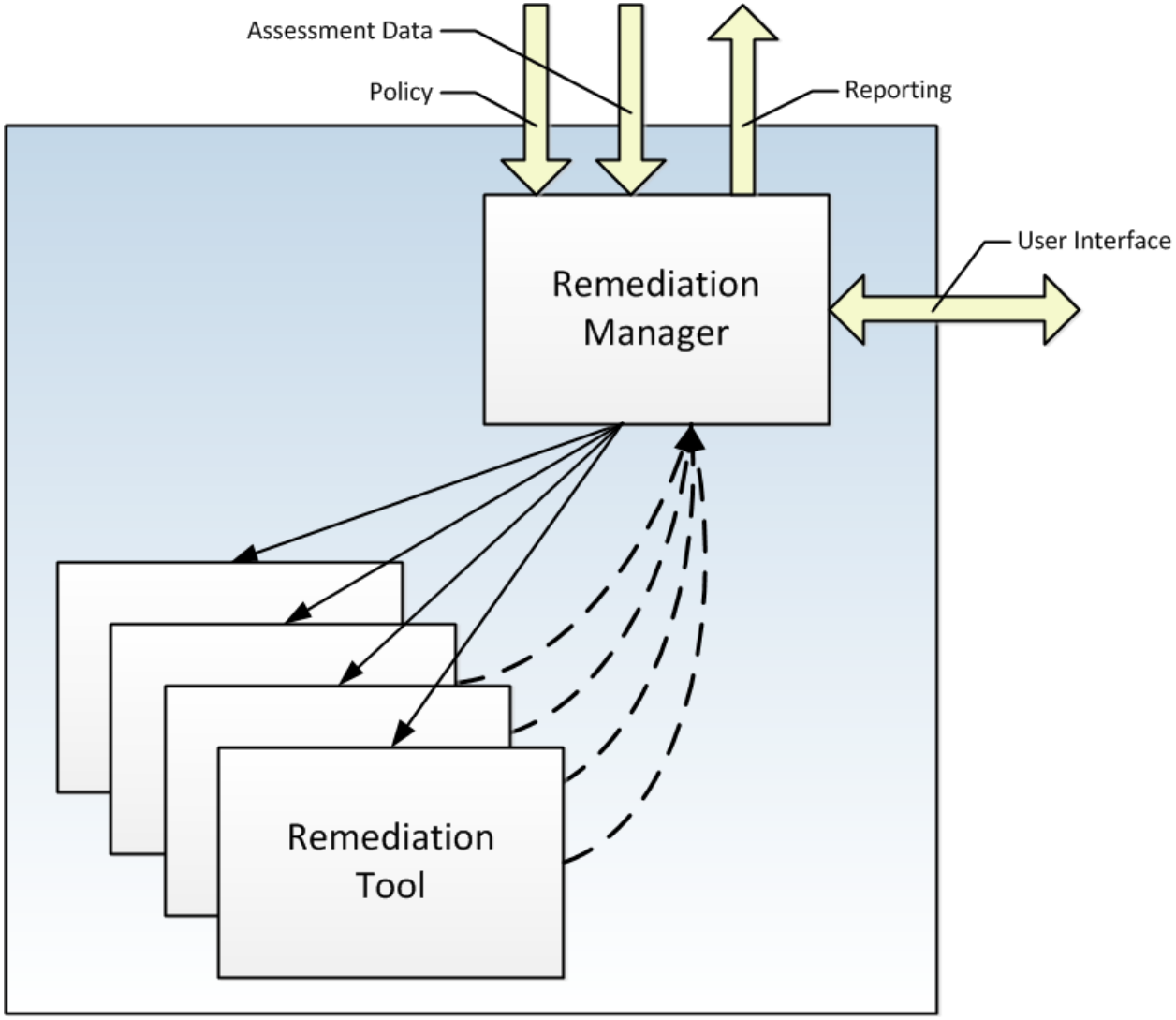
Remediation Standards: Background

- Goal: Interoperability of IT Remediation activities
  - "Remediation" defined as any security-motivated change
- Approach: Develop a set of open remediation standards
  - Establishing consensus through open community discussions
  - Supported by research and development, prototyping tools and content
- Identified use cases include:
  - Scan and remediate, configuration compliance, targeted remediation
- Requirements include:
  - Integrate with SCAP assessment
  - Map well onto existing commercial remediation capabilities
  - Accommodate legacy tools

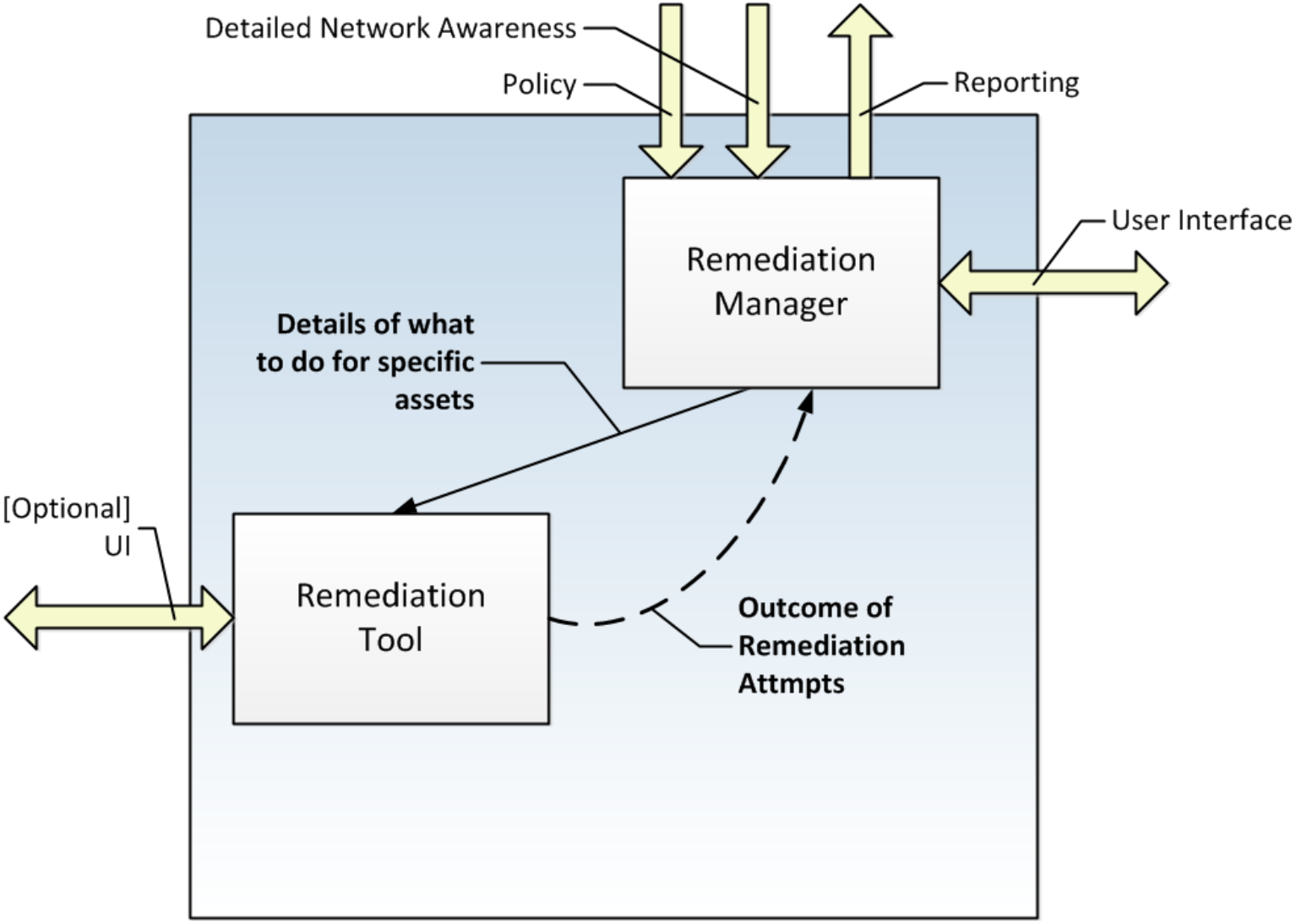
High Level Operational Concept



Remediation Capability: Detailed View



Remediation Capability: Detailed View



Key Remediation Standards Under Development

- **CRE (Common Remediation Enumeration)**
  - **Unique IDs and human-oriented descriptions of remediations**
- **Remediation Policy Language**
  - **Document allowed or required remediation actions (CREs) by host type**
  - **Simple case: link a CRE and a parameter value with a CCE**
  - **Similar to XCCDF's role in assessment**
- **Remediation Tasking Language**
  - **Machine-readable input to remediation tool**
  - **"Perform <CRE list>, with <options>, on <target list>"**

Single System Remediation Capability