Continuous Monitoring in a Cloud Environment

Kent Landfield
Director, Content Strategy, Architecture and Standards
So Automated Continuous Monitoring?

• Continuous review of the security posture of your critical facilities or networks

• Discovery and knowledge of devices attached to the network

• Validation of configurations, assuring they are as they should be

• Verification of critical system and operational files to assure they are not modified without knowledge of the proper owners

• Provide visibility of what is happening to the critical facilities your organization depends on
So where are we?

- In the middle of a transition from paperwork exercise, to electronic reporting, to the visibility provided by a near real time monitoring infrastructure.

- In some cases still working to get to electronic reporting.

- Need to determine what the metrics are that are important to us

- Need to create thresholds where action is required and understand what those actions would be
  - Lots of talk about continuous monitoring but to what end?

- Monitoring for the sake of monitoring yields little
Service Models

• Software as a Service (SaaS)
  – Use provider’s applications over a network

• Platform as a Service (PaaS)
  – Deploy customer-created applications

• Infrastructure as a Service (IaaS)
  – Rent fundamental computing resources (Storage, processing, bandwidth support, etc.)
4 Cloud Deployment Models

• Private cloud
  – enterprise owned or leased
• Community cloud
  – shared infrastructure for specific community
• Public cloud
  – Sold to the public, mega-scale infrastructure
• Hybrid cloud
  – composition of two or more clouds
Issues with Continuous Monitoring Cloud Services

• Determining the right level to monitor
  – What aspects do you monitor?
  – The service you are using? The infrastructure owned by the provider?

• Lack of ownership and physical control over the facilities providing the services
  – Trusting provider’s security model and staff
  – Customer inability to respond to findings
  – Provider proprietary implementations can’t be examined

• May have to be yet another service offered by the cloud provider

• Where is the line drawn?