Continuous Monitoring
Federal Information Systems

Earnest Neal – Atlantic Systems Group, Inc.
Steve Johnston – Tripwire, Inc.
Continuous Monitoring is...

...more than just watching data
Continuous Monitoring

Agenda

• Overview of Continuous Monitoring Basics
• CAESARS architecture and SP 800-137
• Case Study Automated vs. Manual
• ASG and Tripwire Continuous Monitoring Solution
  – Finding the Events of Interest
  – Maintaining a Secure Configuration State
  – Providing actionable results
Continuous Monitoring  Basic Overview

• Technical and business process development to support a Agency
  – Technical development follows the Continuous Asset Evaluation, Situational Awareness and Risk Scoring (CAESAR) Reference Architecture

• Strategy Development
  – Clear understanding of Agencies' risk tolerance helping to identify priorities
  – Meaningful metrics illustrating security posture
  – Continuous evaluation of the effectiveness of security controls
  – Compliance validation
  – Security status visible to all organizations to maintain vigilance
  – Awareness of threats and vulnerabilities
Continuous Monitoring Basic Overview

- Establishing Agency’s Information Security Continuous Monitoring (ISCM)
  - Define Agency-ISCM strategy
  - Establish the Agency-ISCM program
  - Develop the Agency-ISCM Reference Architecture
  - Analyze data and report findings
  - Respond to findings
  - Review and update the Agency-ISCM strategy and program

1. Categorize Information System
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize Information System
6. Monitor Security Controls
Benefits of Continuous Monitoring

- Moves the focus back to Security
- Provides staff (management/operational) access to real-time security information
- Leads to improved security posture
- Creates better awareness of threats and vulnerabilities
- Automates manual processes wherever possible
- Enables prioritization of remediation
- Remediation costs move to daily operations
Continuous Monitoring Challenges

• Identifying existing capabilities
  – Prevent unnecessary work in areas already developing
  – Increase effort to leverage those capabilities

• Participation
  – Ensure sufficient involvement to create a Agency-wide view of CM to capture the organizations core missions and business functions

• Developing the risk thresholds/tolerance levels
  – Capturing information and facilitating data driven management decisions

• Automation development
  – Engineering components of sub-systems not already in-place
Case Study

• VA
  – In 2005 300 systems were assessed with the average reporting time of 200 hours per system. In 2007 all 650+ systems were assessed, over 5 million individual tests, and the average reporting time was reduced to 4 hours... for QA review.

<table>
<thead>
<tr>
<th>Year</th>
<th>Hours</th>
<th>Cost</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>200</td>
<td>$125.00</td>
<td>$25,000.00</td>
</tr>
<tr>
<td>2007</td>
<td>4</td>
<td>$125.00</td>
<td>$500.00</td>
</tr>
</tbody>
</table>

• Legislative Branch Auditing Organization
  – 2009/10 this organization needed to meet aggressive C&A deadlines that were costing millions. They had Limited Resources, Budget Constraints, Outsourcing C&A processes were too costly
  – Saved 600K within first year and an estimated 1.8 million through the current C&A Period
Continuous Monitoring – Reference Architecture
Continuous Monitoring Security Alerts

- Find complex risks
- Faster discovery
- Enhance SIEMs
- Less False Positives

Broad coverage

Continuous Monitoring Feeds

- Config. Policy Failures
- Found Vulnerabilities
- Change Auth. Failures
- Missing Patches
- Change Policy Failures

Actionable Security Alerts!
Configuration Changes of Interest: Analyze / Filter Change

- Detect → Analyze → Filter

Changes of Interest!
- Config. Policy Failures
- Change Policy Failures
- Change Auth. Failures

Broad coverage
The Worst Problems Are Often Most Difficult To Discover

- Logging turned off
- FTP event to foreign IP
- New user added
- Login successful
- FTP enabled
- DLL modified by new user
- 10 failed logins
Vulnerability, Change and Configuration Assessment cannot make these types alerts. **Change intelligence is required.**
Detecting Log Security Events Alone IS Not Enough

Login successful

10 failed logins

Log management alone cannot alert on these events—SIEM is required.
Relating Configuration Modification to Log Events Is Required

Continuous Monitoring

Events of Interest

- Logging turned off
- FTP event to foreign IP
- New user added
- FTP enabled
- DLL modified by new user
- Login successful
- 10 failed logins
Continuous Monitoring

Example Feedback to the Authorized Official

Respond on Critical Control and Change Information
Continuous Monitoring

Example Feedback to the Authorized Official

Provide actionable data

Respond to Critical Events
Get visibility into Cyber Threats

Know the system settings that need to be secured
IA² - Continuous Monitoring Program (CMP)
Questions and Answers
## Complete Security & Compliance Solution

<table>
<thead>
<tr>
<th>Tripwire Solution</th>
<th>Benefits</th>
</tr>
</thead>
</table>
| **Security Intelligence**  | • Arm CISOs with the data they need  
• Have business context (risk) to help prioritize & make better decisions  
• Improve analytics                                                                  |
| **Security Hardening**     | • Reduce attack surface  
• Harden systems through secure configurations  
• Understand the security and risk posture                                             |
| **Continuous Monitoring**  | • Make cost-effective, risk based decisions  
• Continuous controls-based visibility of state, policy & events  
• Meet NIST 800-137 guidelines and go beyond the compliance checkbox                 |
| **Threat Response**        | • Detect real-time evidence of potential data compromise, misuse, tampering  
• Reduce the breach-to-detection time gap                                              |
| **Operationalize Security**| • Quick deployments of new datacenters, infrastructure and business services  
• Find and fix security breaches & weaknesses in defenses  
• Manage planned and unplanned changes to production systems                           |
| **Forensics/Investigation**| • Quickly extract actionable information from critical systems  
• Quickly identify root cause of incident & problem management  
• Have historical proof to simplify compliance                                         |
| **Continuous Compliance**  | • Satisfy compliance requirements for security assurance  
• Make compliance a by-product of being secure continuously  
• Be compliant at lowest cost                                                          |
| **Compliance Auditing**    | • Avoid fines, audit failures and penalties  
• Proactively manage compliance  
• Easily prove compliance on-demand at lowest possible cost                             |