IT2775 Operations Security

InfoSecurity Continuous Monitoring (ISCM)

NANYANG POLYTECHNIC

Objectives

- What is ISCM?
- Approaches (3)
- Capability Levels (6)

What is ISCM?

- InfoSec Continuous Monitoring (ISCM)
  - risk management approach to cyber security
  - maintains an accurate picture of an organization's information security risks
  - provides visibility into assets
  - leverages the use of automated data feeds to
    - quantify risk
    - ensure effectiveness of security controls
    - implement prioritized remedies/responses

ISCM Approaches

1. Customise ISCM solution from multiple vendors
   - Integrate vendor components => ISCM capability
   - Duplicate work and repeat mistakes of others
2. Buy integrated ISCM solution from vendor
   - Lock into a solution with strength and weaknesses
   - Difficult to compare vendor products
   - E.g. Tripwire VIA
3. Leverage an ISCM technical reference architecture and standards (CAESARS, SCAP)
   - Best of breed solutions
   - Use existing security products

ISCM Capability Levels

	Level 0 Manual Assess	Level 1 Auto Scan	Level 2 Standard Measure	Level 3 Continuous Monitor	Level 4 Adaptable ISCM	Level 5 Continuous Manage
Focus	Manual Assess	Auto Assess, not centralized	Standard data	Centralized, consolidated data ->risk	Plug and play components	Risk -> remedy
Interface	Not defined	Unused	Unused	Non-standard	Standard	Standard
Data Format	Non-standard	Non-standard	Partly standard	Partly Standard	Standard	Standard
Report	Ad hoc	Non-standard, no integration	Non-standard, no integration	Partly standard, basic integration	Standard integration	Standard integration
Remedy	Manual	Non-standard/ manual	Non-standard/ manual	Non-standard/ manual	Non-standard/ manual	Standard automation

ISCM Capability Levels

0. Manual Assessment
   - No automated solutions for security assessment.
1. Automated Scanning
   - Automate generation of scanned data
   - Decentralized use of automated scanning.
   - Automation crucial to ISCM
     - For some technologies, partial automation may be the best arrangement. E.g. log analysis
   - Need to consider how data is propagated to the relevant system and end user.

ISCM Capability Levels

2. Standardised Measurement
   - Standardise data to facilitate:
     - Exchange of info accurately among systems
     - Fast/accurate correlation of multiple data sources
     - CVE – Common Vulnerabilities and Exposure
       - Unique identifiers to identify vulnerabilities
     - CCE – Common Configuration Enumeration
       - Unique identifiers for system configuration issues
     - USGCB – US Govt Configuration Baseline
       - Standardized security configuration baselines for IT products widely deployed across the US Govt

ISCM Capability Levels

3. Continuous Monitoring
   - Generate risk level from standardised data.
   - Centralized control of automated scanning tools.
   - Facilitate large scale collection of distributed data.
   - Organization-wide security measurements consolidated into risk scores
   - Comparative risk scoring displayed on a dashboard for management oversight.

ISCM Capability Levels

4. Adaptable Continuous Monitoring
   - Standardise ISCM architecture
   - Allows for plug-and-play ISCM components.
   - Standardized message formats and interfaces.
   - ISCM components can be acquired or re-deployed according to organizational needs.
5. Continuous Management
   - Activate remedy actions based on risk level.
   - Risk remedy capabilities added.
   - Integrate mitigation and remediation processes.
   - If possible, implement automated remediation.

ISCM Capability Levels

	Level 0 Manual Assess	Level 1 Auto Scan	Level 2 Standard Measure	Level 3 Continuous Monitor	Level 4 Adaptable ISCM	Level 5 Continuous Manage
Focus	Manual Assess	Auto Assess, not centralized	Standard data	Centralized, consolidated data ->risk	Plug and play components	Risk -> remedy
Interface	Not defined	Unused	Unused	Non-standard	Standard	Standard
Data Format	Non-standard	Non-standard	Partly standard	Partly Standard	Standard	Standard
Report	Ad hoc	Non-standard, no integration	Non-standard, no integration	Partly standard, basic integration	Standard integration	Standard integration
Remedy	Manual	Non-standard/ manual	Non-standard/ manual	Non-standard/ manual	Non-standard/ manual	Standard automation

Summary

- What is ISCM?
- Approaches (3)
- Capability Levels (6)

Additional References: Current Trends

- There exists great momentum surrounding ISCM (both management and working levels)
  - Dashboards, “big easy” buttons, aggregated reporting of technical metrics
- Companies can leverage their existing security tools to evolve towards an automated ISCM solution
- The long term vision will take time and effort, but significant gains are achievable today.