The CIS Security Metrics & Benchmarking Service

Clint Kreitner
The Center for Internet Security

the CENTER for INTERNET SECURITY

The Center for Internet Security (CIS)

- **Formed** - October 2000
  - As a not-for-profit public-private partnership
- **The mission** – produce security guidance to:
  - Help users **harden** their systems against IT vulnerabilities
  - Enable IT buyers to use their **purchasing leverage** so they can buy systems with **security built-in**
  - Support the higher level standards/regulations with unambiguous **operational-level "how-to" detail**
- **The method**
  - Security configuration benchmarks **built by consensus teams** of security experts
- **The impact** – downloaded **over 1,000,000 times / year**

Current reality – info security

- Focus is on compliance with *practices/processes* with inadequate attention to *outcomes*
- Security investment decisions being made on an intuitive basis
- Using methods like risk assessment & CMM which lack a feedback/learning loop
- Lawmakers and executives asking questions that pose a threat to security's funding support

Security Metrics Initiative

- Sponsored by the Center for Internet Security
  - Community consensus group
- Practical approaches to security management
  - Focus first on outcome metrics
- Why outcomes?
  - An unacceptable outcome usually suggests the processes producing the outcome need improvement
- The ultimate cybersecurity outcome
  - A cyber infrastructure that functions as needed and is available when needed by anyone who wants to use it—the same way we view the highway infrastructure

Consensus team members

- **Corporations and Organizations**
  - Small & Fortune 50 organizations, non-profit and commercial, many industry verticals, **especially banking and financial**
- **Industry Experts**
  - Mathematicians, statisticians, actuaries, CISO's, security managers
- **Government**
  - Federal, state, and local
- **Vendors**
  - Security product, solution and consulting firms
- **Universities and Researchers**
  - Well know institutions that specialize in information security

Goals

- Reach consensus on an initial small set (<10) of unambiguous security metrics
  - Facilitate widespread adoption among CIS Members
- Launch an operational benchmarking service that enables:
  - Communication of internal security status over time
  - Inter-enterprise benchmarking of security status
  - Development of a database from which *security practice/ outcome correlations* can be derived to better inform future security investment decisions

Example of how a metric evolves through the consensus process

- Starter set stage
  - # of security incidents
- Survey stage
  - # of security incidents that impacted info C, I, or A
  - # hrs elapsed between incidents that impacted C,I or A
- Current stage
  - Mean time between security incidents
  - Mean time to recover from a security incident
    - security incident defined as an event for which a trouble ticket is produced

Current status – conceptual metrics

- Outcome metrics
  - Mean time between security incidents
  - Mean time to recover from security incidents
- Process/practice/diagnostic metrics
  - % of systems configured to approved standards
  - % of systems patched to policy
  - % of systems with anti-virus
  - % of business applications that had a risk assessment
  - % of business applications that had a penetration or vulnerability assessment
  - % of application code that had a security assessment, threat model analysis, or code review prior to deployment

Milestones

- Reach consensus on an initial set of metrics – Completed
- Reach consensus on final definitions and conform them to the consensus schema – 9/1/08
- Complete development of the benchmarking technology platform – 9/30/08
- Launch CIS Security Metrics & Benchmarking Service – 10/08
- CIS Members contributing data and producing reports – 11/08

Summary

- Leverage CIS community efforts and experience to
  - Implement a few consensus metrics within the community
  - Launch a proof-of-concept inter-enterprise benchmarking database service

- We invite you to participate
  - Please contact Steven Piliero at spiliero@cisecurity.org

http//:www.cisecurity.org

ckreitner@cisecurity.org
540-459-1861

spiliero@cisecurity.org
818-425-6129

CIS Security Benchmarks are:

- Available at http://www.cisecurity.org
  - free-of-charge in .pdf format to everyone
  - in tool-readable XML format to CIS Members for use with configuration auditing/monitoring tools
- Used worldwide as
  - the basis for enterprise configuration standards
  - the recognized standard against which to compare
    - Downloaded >1,000,000 times/year