Metrics Management

GENI Workshop
26 June 2009

Elizabeth A. Nichols, CTO for Metrics, PlexLogic LLC

Introduction

- Betsy Nichols
  - Academia: Mathematics
  - Industry: Apollo, War Gaming, Process Control, NSM + Agents, Metrics Automation
- GENI Relevant Work
  - Instrumentation Frameworks: CMIS/CMIP, SNMP, CIM, WEBM, JMX, CAIDA
  - hyperPlex: Grid, WebServices, P2P, Service Orchestration, Distributed Programmability
  - MetricsCenter: Acquision(less), Analysis (more)

Presentation

- Terminology
- Metrics Management: Two Layers
- Example Metric Layer Requirement
- Thoughts on GENI
- References

Terminology

- **Instrumentation**: Generates raw observations
  - **Sensor = Listens to Instrumentation and produces ...**
  - **Measures = Quantitative value**
- Dimension
  - Usually not quantitative: ex: protocol, owner, criticality, time
  - Captures context: technical, location, business, policy, ...
- Metric
  - Derived via analysis applied to measures and dimensions
  - Can cross sensor boundaries
- Key Goal Indicator & Key Performance Indicator
  - Characterize target levels and goal attainment

Metrics Management: Two Layers

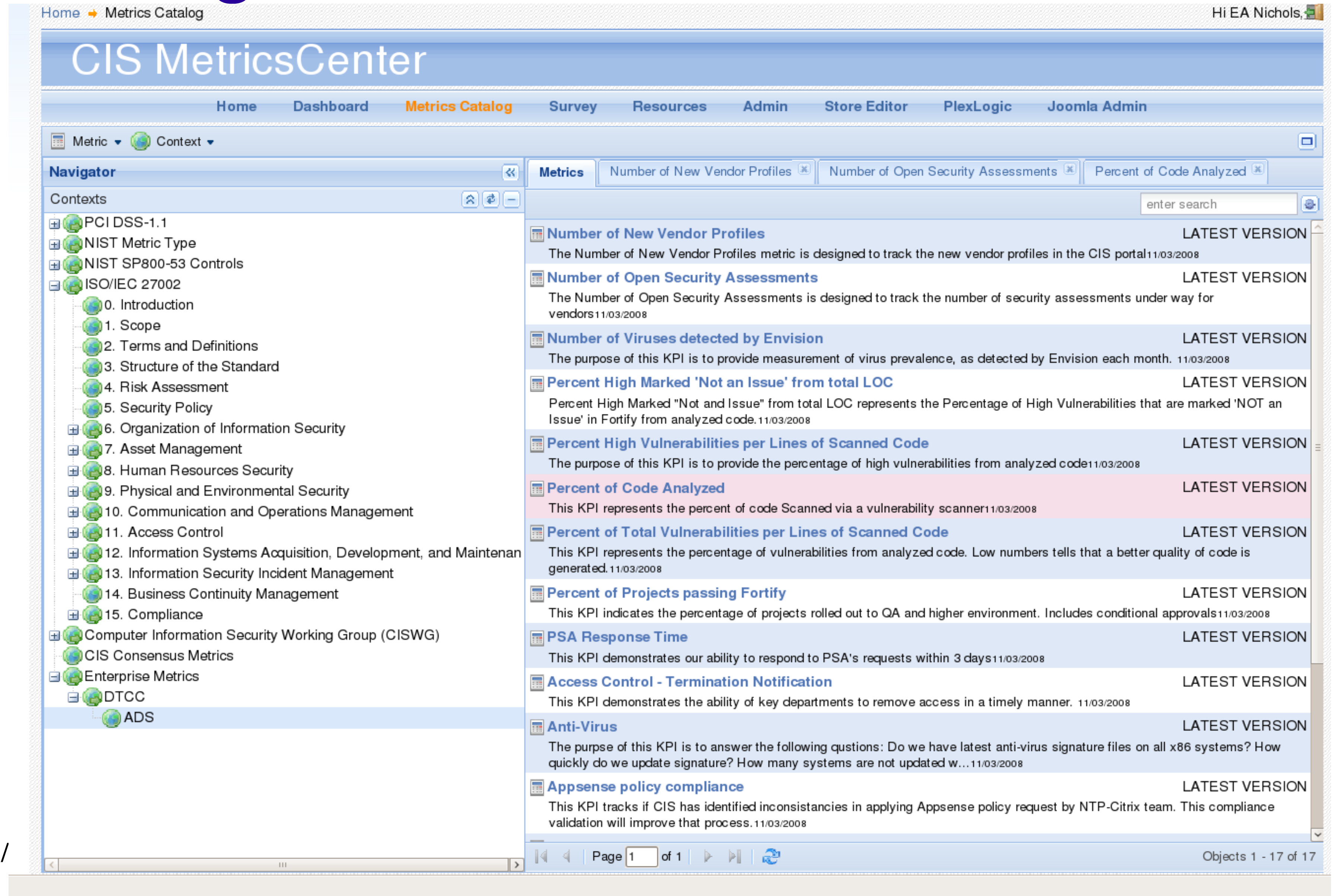
- Instrumentation Layer
  - Heterogeneous and dispersed silos
  - Localized data quality control
  - Anonymization
  - Persistence
- Metric Layer
  - Life Cycle: Design+Deploy+Deliver
  - Specialized Services + Object Models
  - Privacy + Re-Identification

Metric Design Phase

- What question does this metric answer?
- What data does it need?
- What terminology needs definition?
- What analysis (and assumptions) does it use?
- What results will it produce?
- What contexts does it map to?
- How should results be published?
- What revisions have occurred ?
- How do users rate its effectiveness ?

Deliverable: Catalog

Catalog: One Embodiment



- PCI DSS-1.1
- NIST Metric Type
- NIST SP800-53 Controls
- ISO/IEC 27002
  - 0. Introduction
  - 1. Scope
  - 2. Terms and Definitions
  - 3. Structure of the Standard
  - 4. Risk Assessment
  - 5. Security Policy
  - 6. Organization of Information Security
  - 7. Asset Management
  - 8. Human Resources Security
  - 9. Physical and Environmental Security
  - 10. Communication and Operations Management
  - 11. Access Control
  - 12. Information Systems Acquisition, Development, and Maintenan
  - 13. Information Security Incident Management
  - 14. Business Continuity Management
  - 15. Compliance
- Computer Information Security Working Group (CISWG)
- CIS Consensus Metrics
- Enterprise Metrics
  - DTCC
    - ADS

Number of New Vendor Profiles LATEST VERSION
The Number of New Vendor Profiles metric is designed to track the new vendor profiles in the CIS portal11/03/2008

Number of Open Security Assessments LATEST VERSION
The Number of Open Security Assessments is designed to track the number of security assessments under way for vendors11/03/2008

Number of Viruses detected by Envision LATEST VERSION
The purpose of this KPI is to provide measurement of virus prevalence, as detected by Envision each month. 11/03/2008

Percent High Marked 'Not an Issue' from total LOC LATEST VERSION
Percent High Marked "Not and Issue" from total LOC represents the Percentage of High Vulnerabilities that are marked 'NOT an Issue' in Fortify from analyzed code.11/03/2008

Percent High Vulnerabilities per Lines of Scanned Code LATEST VERSION
The purpose of this KPI is to provide the percentage of high vulnerabilities from analyzed code11/03/2008

Percent of Code Analyzed LATEST VERSION
This KPI represents the percent of code Scanned via a vulnerability scanner11/03/2008

Percent of Total Vulnerabilities per Lines of Scanned Code LATEST VERSION
This KPI represents the percentage of vulnerabilities from analyzed code. Low numbers tells that a better quality of code is generated.11/03/2008

Percent of Projects passing Fortify LATEST VERSION
This KPI indicates the percentage of projects rolled out to QA and higher environment. Includes conditional approvals11/03/2008

PSA Response Time LATEST VERSION
This KPI demonstrates our ability to respond to PSA's requests within 3 days11/03/2008

Access Control - Termination Notification LATEST VERSION
This KPI demonstrates the ability of key departments to remove access in a timely manner. 11/03/2008

Anti-Virus LATEST VERSION
The purpse of this KPI is to answer the following qustions: Do we have latest anti-virus signature files on all x86 systems? How quickly do we update signature? How many systems are not updated w...11/03/2008

Appsense policy compliance LATEST VERSION
This KPI tracks if CIS has identified inconsistanciesin applying Appsense policy request by NTP-Citrix team. This compliance validation will improve that process.11/03/2008

Thoughts about GENI

- A Metrics Layer for GENI delivers
  - User Context
  - Better Business Decision Support
  - Enhanced Transparency & Trust
- GENI Metrics Layer could be:
  - A “long running” experiment
  - Instrumented and Managed by GENI O&M

Metrics Layer Resources

- http://www.MetricsCenter.org - Go to the resources page for pointers to lots of additional resources
- http://www.SecurityMetrics.org
- http://www.cert.org/podcast - Several podcasts on metrics have been produced by CERT and are published here
- http://www.itpmi.org - The IT Metrics and Process Institute
- http://www.qop-workshop.org - The Quality of Protection web site
- http://www.itpi.org - The IT Process Institute web site
- http://cisecurity.org - The Center for Internet Security will be publishing consensus metrics soon

Contact Info

Elizabeth A. Nichols
CTO, PlexLogic
betsy.nichols@plexlogic.com
703.963-7202