OD/ITAO
NIHRFC0055
Category: Brick Retirement

Joe Klosky
OD
January 2010

Event Monitoring Brick Retirement
V1.0

Status of this Memo

This document proposes the retirement of a standard for the National Institutes of Health (NIH) and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Table of Contents

1 Introduction

This document initiates the retirement of the NIH Technical Architecture Standards Brick for Event Monitoring Analysis for the NIH community.

2 Description

Vulnerability Analysis. Internet-based attack tools are becoming increasingly sophisticated and increasingly easy to use. NIH's network could contain vulnerabilities that attackers can exploit to gain access, even when NIH has secured the network perimeter with firewalls and intrusion detection systems. In order to proactively find and plug such holes NIH will require the use of both vulnerability assessment products and vulnerability assessment services.

System Monitoring and Logging. Identifying and reacting to security incidents in real-time requires comprehensive system and network monitoring, Furthermore the ability to aggregate alarms and other information from disparate systems is necessary to correlate events and identify an incident.

3 Justification for Retirement

The 2003 brick entitled Event Monitoring and Analysis Brick is nearly identical to the 2004 brick entitled Event Management Brick. As the 2004 brick is more comprehensive, it is recommended that the Event Monitoring and Analysis Brick be deleted.

1 – Event Monitoring Analysis Brick

Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)
■ None	■ None
Retirement (Technology to eliminate)	**Containment (No new deployments)**
■ None	■ None
Baseline Environment (As of last review)	**Emerging (Technology to track)**
■ Event Monitoring ■ Computer Associates TNG ■ DeepMetrix ipMonitor ■ Fluke OptiView ■ Fluke Link Analyzer ■ Fluke Network Inspector ■ HP OpenView ■ HP ITO ■ Ipswitch WhatsUpGold ■ NetIQ ■ OpenNMS ■ Quest Software Big Brother ■ Log Monitoring ■ Microsoft Operations Manager ■ Log Analysis ■ Central Syslog Facility ■ Envision ■ Microsoft Operations Manager ■ OS Logging ■ Remote syslog ■ Router/switch logging	■ Event Correlation
Comments	
■ Tactical and strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated retirement and containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected tactical and strategic products.	

Table 2 - Event Management Brick

Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)
■ CA Unicenter ■ HP OpenView ■ Micromuse ■ Nagios	■ Either HP OpenView or CA Unicenter
Retirement (Technology to eliminate)	**Containment (No new deployments)**
■ None	■ None
Baseline Environment (As of last review)	**Emerging (Technology to track)**
■ CA Unicenter ■ HP OpenView ■ Micromuse ■ Nagios	■ Other leading or innovative vendors of Event Management tools, such as: ■ Auto RCA ■ CA Neugent Technology ■ HP Event Correlation ■ Managed Objects ■ Mercury Interactive Topaz
Comments	
■ NIH needs to choose either the HP Openview or CA Unicenter framework as the MOM. ■ Tactical and strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs of new products. ■ Some baseline products have been designated retirement and containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as the selected tactical and strategic products. ■	

4 Contact

To contact the NIHRFC Editor, send an email message to EnterpriseArchitecture@mail.nih.gov

5 Changes

Version	Date	Change	Authority	Author of Change
0.1	1/8/2010	Initiation of retirement		Joe Klosky
0.2	2/9/2010	Minor formatting	NIHRFC0001	Kiley Ohlson

		changes		
0.3	2/17/2010	Updated the structure of the brick to match the website		Anja Holovac
1.0	4/27/2010	ARB approved NIHRFC	ARB	Kiley Ohlson

6 Author's Address

Helen Schmitz / Joe Klosky
OD/Office of the Chief IT Architect, NIH
10401 Fernwood Road, Room 3NW10B
Bethesda, Maryland 20817-4800
Phone: 301-496-2328
Email: schmitzh@mail.nih.gov
Email: joe.klosky@nih.gov