

Archer® Continuous Monitoring

Use Case for Public Sector Solutions

The Challenge

Security controls are infrequently and ineffectively assessed using tools from different vendors, with proprietary data formats and limited data sharing. There are typically more findings than the available staff can manage and remediation of findings is not prioritized using all available contextual data.

Continuous monitoring (CM) is a combination of manual and automated assessments. While vendors who produce automated scanner or sensor tools market their product as “continuous monitoring solutions,” they do not provide for manual assessments and typically check for only one defect type (vulnerability or misconfiguration). Updates to Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) guidance create pressure to move CM planning forward, but lack of precedent leaves organizations guessing about finer implementation details.

Lack of CM in the public sector means defects and vulnerabilities remain open for long periods of time. It is also difficult to share data or the “big picture” of risk due to the disparity of tools and incomplete and outdated assessment results. Staffing is insufficient to perform all assessments and remediate all findings. Lack of business context and visibility means the most critical defects are not always remediated first. Most organizations do not have the insight and metrics to perform defect rankings, especially with consideration for information system criticality.

Overview

Archer® Continuous Monitoring serves as a hub for many types of scanners and sensors, allowing organizations to build an aggregate risk view at any level of the enterprise. At the lowest end, individual defects can be monitored and scored. Defects are aggregated at each level of the hierarchy, from the individual device up to the department level. In this way, a risk score can be designated at any level and the amount of relative risk introduced can be measured. This allows resources to be focused on the remediation efforts that will provide the greatest benefit.

Archer Continuous Monitoring enables faster, more targeted response to emerging risks. Staff can mitigate findings in the order in which they will most reduce risk. When used in tandem with the RSA Archer Assessment & Authorization use case, Archer Continuous Monitoring enhances your FISMA, OMB and other regulatory compliance activities by verifying that information systems are abiding by authorization agreements and operating within acceptable levels of risk. This provides a more secure environment and more insight to make better, more informed risk decisions.

Key Features

- Current authoritative hardware and software inventories.
- Current defect libraries.
- Integration of scanners and sensors into a common environment, in a common format.
- Scoring and ranking algorithms for each defect, device and layer of the organizational hierarchy.
- Defect tracking and remediation.

Key Benefits

With Archer Continuous Monitoring, organizations can:

- Reduce exposure time.
- Reduce risk overall.
- Increase visibility/better decision-making.
- Access current risk data.
- Increase assurance and confidence based on current data.

ISSO CM OVERVIEW

My Vulnerability Scan Results

Scan Result ID	Category	Severity	Title
VSR-00003	Windows	High	TCP/IP Vulnerabilities on Windows Could Allow Remote Code Execution (MS08-001)
VSR-00005	Database	High	Microsoft Jet Database Engine Could Allow Remote Code Execution (95927)
VSR-00006	Windows	Medium	Enabled Guest Access to System Log
VSR-00008	Web server	High	Microsoft IIS 4.0/5.0 File Permission Canonicalization Vulnerability
VSR-00009	Windows	High	Windows TCP/IP Denial of Service Vulnerability (MS08-004)
VSR-00011	Information Gathering	Medium	Remote User List Disclosure Using NetBIOS
VSR-00012	Local	High	Mozilla Firefox, Thunderbird, SeaMonkey Multiple Vulnerabilities February 2008

My Vulnerable Devices

Hardware Name	Type	Description	Number of Vulnerabilities	Hardware Owner	Scan Result ID	Title	Severity	Remediation Status
APPSSRV005	Application Server	Supports multiple applications used by the NDC.	5		VSR-00003	TCP/IP Vulnerabilities on Windows Could Allow Remote Code Execution (MS08-001)	High	Not Started
					VSR-00009	Windows TCP/IP Denial of Service Vulnerability (MS08-004)	High	N/A
					VSR-00012	Microsoft Windows Server Service Could Allow Remote	High	N/A

Vulnerability Alerts with Systems Affected

Vulnerability Alerts with Systems Affected

Title	CVE(s)	Severity	Type	Technologies Reference(s)	Version Name	Hardware Name	Hardware Owner
00000000-nb0u-n Moodle 2.1.x before 2.1.10, 2.2.x before 2.2.7, 2.3.x before 2.3.4, and 2.4.x before 2.4.1 continues to provide a local XSS feed after logging in, disabled, which allows remote attackers to obtain sensitive information	CVE-2012-0105	High		Moodle	2.1		
				Moodle	2.1.1		
				Moodle	2.1.2		
				Moodle	2.1.3		
				Moodle	2.1.4		
				Moodle	2.1.5		

Misconfigurations by Severity

Severity	Percentage
Severe	44.44%
High	16.67%
Medium	16.67%
Low	5.56%
Minimal	5.56%
Informational	5.56%

Misconfigurations by Scan Date

Misconfigurations by Week

Week	Count of Date of Scan
Week 40 - 2014 (1)	3
Week 40 - 2014 (2)	5
Week 40 - 2014 (3)	6
Week 40 - 2014 (4)	3

Scanner/Sensor Results by Hardware Type

Hardware Type	Count
Application Server	14
Database Server	1
Firewall	3



Discover More

Archer, an RSA company, is a leader in providing integrated risk management solutions that enable customers to improve strategic decision making and operational resiliency. As true pioneers in GRC software, Archer remains solely dedicated to helping customers understand risk holistically by engaging stakeholders, leveraging a modern platform that spans key domains of risk and supports analysis driven by both business and IT impacts. The Archer customer base represents one of the largest pure risk management communities globally, with over 1,500 deployments including more than 90 of the Fortune 100.