

Product Review: Cenizic Hailstorm Enterprise ARC 5.7

http://searchSecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1344755,00.html

by: [Phoram Mehta](#)

Issue: [Jan 2009](#)

WEB APPLICATION SECURITY

Cenizic Hailstorm Enterprise ARC 5.7 REVIEWED BY PHORAM MEHTA

[Cenizic](#)

Price: \$26,000



Web application security has moved from a nice-to-have to a must-have requirement, for data protection and compliance. Cenizic's Hailstorm, which we last reviewed in 2005, reflects the growth in the depth and maturity of Web application vulnerability assessment software.

Installation

B

Enterprise ARC includes a management server/console; database for checks, assessments and results; ARC Execution Engine (AEE); distributed scanners that run scans with the Web application to run in different parts of the network and the standalone enterprise desktop

scanner.

These components can be installed on one or more machines. The only combination that might be a little tricky is the AEE and desktop software on the same box. In this scenario, you have to stop the AEE service before you can run the desktop client.

Use the desktop application for applications needing some manual interaction and constant monitoring during the assessment, and use AEE for assessments that can be completely automated.

The installation wizard is straightforward and walks you through the various options, including setting the network port and passwords for communicating with the database.

Configuration

B+

Hailstorm offers three methods to add applications: Users can run an auto-discovery scan on Web application ports, add applications manually, or import a CSV file. You can assign a risk factor, and group applications for better management. Running and scheduling assessments is as simple as it gets.

The desktop application allows custom assessments that are a combination of checks from best practices (OWASP), regulatory standards, and custom attacks created in-house. We selected the OWASP and best practices assessments against a classic ASP/MS SQL and a Joomla (LAMP) Web application, respectively.

Hailstorm offers by far the best attack customization and new attack creation capability in the industry. To offer flexibility, Cenizic has added features such as interactive assessments, where the user navigates through the website manually.

Effectiveness

A

The two areas enterprises spend the most time on when using a vulnerability scanner are the home page/central display and the results/reports. Cenizic has remarkable

interactive dashboard that shows trends and activities. During the review assessments, we were able to watch the findings and graphs updated as vulnerabilities were discovered. The details on each finding were available instantly, along with the HTTP request/response, complete explanation of how the attack was executed and remediation recommendations.

One feature that sets Hailstorm apart is the Hailstorm Application Risk Metric score, which incorporates the risk factor assigned to each application and the severity of the vulnerabilities discovered. This helps you focus remediation efforts and determine which vulnerabilities present the most risk. It also measures if risk is decreasing and if remediation is effective over time.

Reporting

B+

Reporting is by far the most improved module. The reporting engine is a powerful tool to monitor progress, manage compliance and distribute relevant information in a timely manner. The Crystal Reports viewer can export reports in many formats.

Verdict

Enterprise ARC 5.7 is a true enterprise-class solution for managing Web application vulnerabilities.

Testing methodology: We installed the server, database and desktop client on a Windows 2003 Server and used a Windows XP machine as an execution engine and tested against several Web applications.

Information Security Magazine is a part of the [TechTarget](#) portfolio of enterprise IT-focused media. Copyright 2000 - 2009, TechTarget. All Rights Reserved.