Expert advice

AVENGR

Executive Summary

United States Federal Government agencies are continually faced with the challenge of meeting Federal Information Security Management Act (FISMA) requirements. One of the primary challenges is successfully and efficiently performing and understanding Information Assurance vulnerability assessments. These assessments typically uncover several thousand vulnerabilities and other threats in the form of non-compliance with Cybersecurity controls. Organizations must remain aware of these threats and vulnerabilities as a part of an overall risk assessment. This is a monumental task, often requiring significant manual and tedious work by Information Security professionals. Athena Consulting Group, LLC has developed the Automated Vulnerability Enumerator for Numeric and Graphical Reporting (AVENGR) suite, iAVENGR and eAVENGR, to enhance the Security Test and Evaluation (ST&E) process by introducing automation into the historically manual task of analyzing and documenting results. The AVENGR suite aggregates, sorts, and graphically displays many thousands of lines of data within minutes of the data being captured/imported. This allows for near instantaneous visibility into the results of a vulnerability assessment versus the test and wait for results model of years past. Another key feature, and time saver, is the ability to automatically generate a FISMA compliant plan of action and milestones (POA&M). The AVENGR suite is a great compliment to existing risk assessment processes, saving time and resources

Background

FISMA is part of the E-Government Act of 2002. It imposes stringent requirements to develop, document, and implement an agency-wide program to secure government information and information systems that support the operations and assets of the agency and holds federal government agencies accountable for their success or failure in meeting those requirements. FISMA tasked the National Institute of Standards and Technologies (NIST) to create and manage technical standards for compliance.

Determining compliance and reporting on FISMA has been a challenge for all agencies. Government leaders facing budget cuts would benefit from gaining efficiencies in the FISMA reporting process, while also gaining improvements on their security posture, by automating a labor intensive component of the Systems Certification[1] requirement.

The Challenge of Meeting FISMA Reporting Requirements

FISMA requirements are extensive and continue to be increasingly critical to the protection of information assets throughout all US Government organizations. Many years of real-world experience have taught us that a thorough Information Assurance Vulnerability Assessment will produce a voluminous amount of data. The output from the wide array of scanning tools and manual checklists used to detect security vulnerabilities for various devices and platforms must be analyzed and condensed before a realistic picture can be painted of an organization's security posture.

Although effective, these tools require expertise, continual support, and report formats vary. These tools may include an automated vulnerability assessment tool, Gold Disk and Security Content Automation Protocol (SCAP) Compliance Checker (SCC), Security Technical Implementation Guide (STIG) Checklists, amongst others. ACG's Information Assurance Vulnerability Assessment teams have recognized the data burden inherently produced by these test tools, and therefore took the initiative to develop the Independent AVENGR (iAVENGR) tool kit to speed up the assessment and delivery of test results.

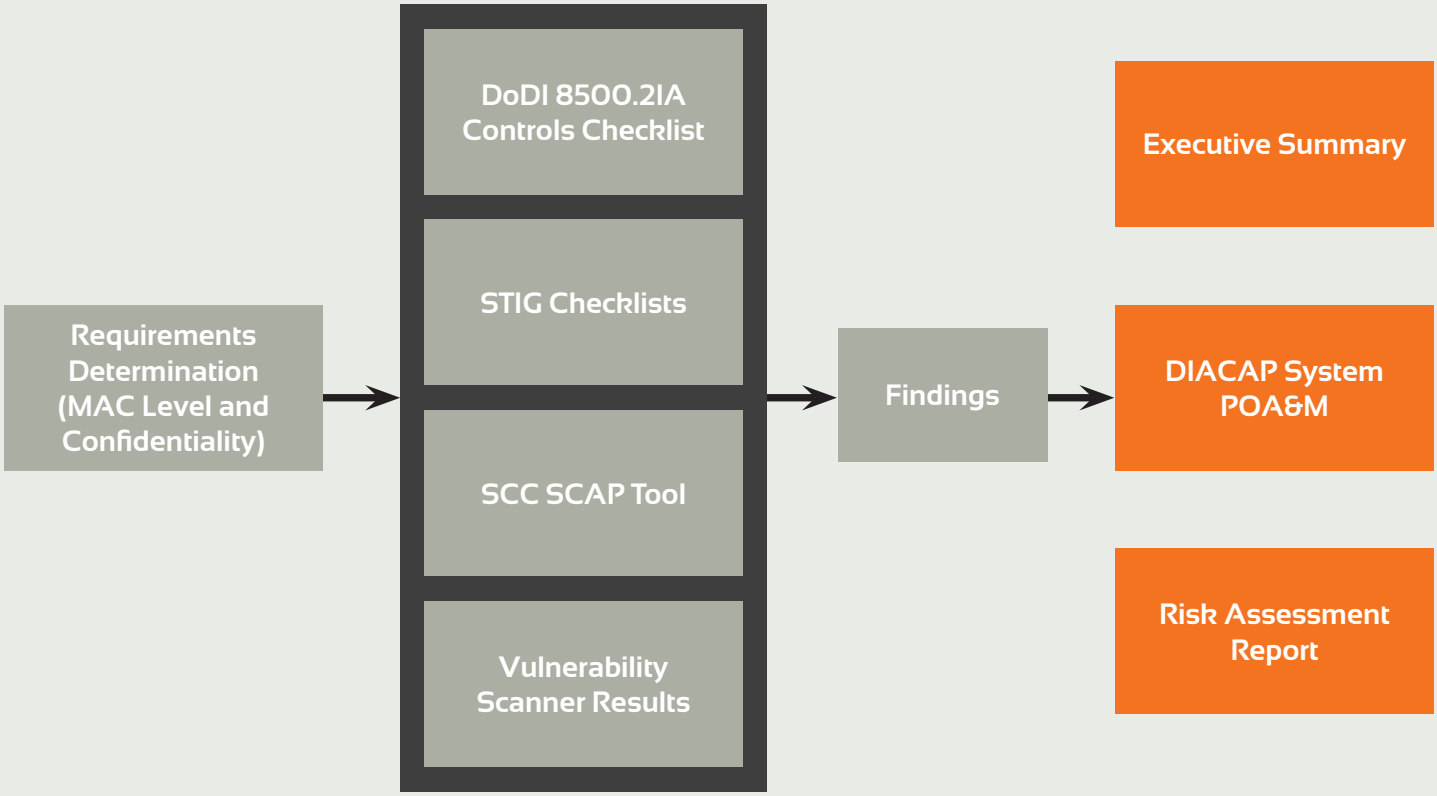
ACG employees have completed hundreds of information assurance vulnerability assessments over the past several years at Government locations across the globe. A typical organization may face approximately 200,000 lines of vulnerability data to manually assess or compile. It is this data that must be distilled and manually entered into a FISMA compliant POA&M to be resolved based on priority. From this POA&M, leadership would be able to determine the site's risk posture. Currently, the tools, manpower, and technology are not consistent between sites and result in cumbersome manual steps which contribute to errors in the results. Errors in results translate to undetected vulnerabilities at worst, or wasted time and effort at best as well as the lack of visibility that is essential to assess risks, much less to provide specific guidance needed to mitigate those risks. iAVENGR greatly assists in this manual process by producing the results via an automated means, saving valuable resources.

Making the Process of Vulnerability Assessment More Efficient

To be effective, a solution was needed to allow the rapid packaging and interpretation of data from the IA tool set. Data Aggregation is key and becomes the single largest issue once tools and manpower are applied. It is at this point that the need for technology insertion is realized.

ACG has developed a technology that is able to handle a multi-data format in the form of an IA tool base. This data aggregator handles, sorts, and graphically displays many thousands of lines of data within minutes of the data being captured/imported. This product then produces a FISMA

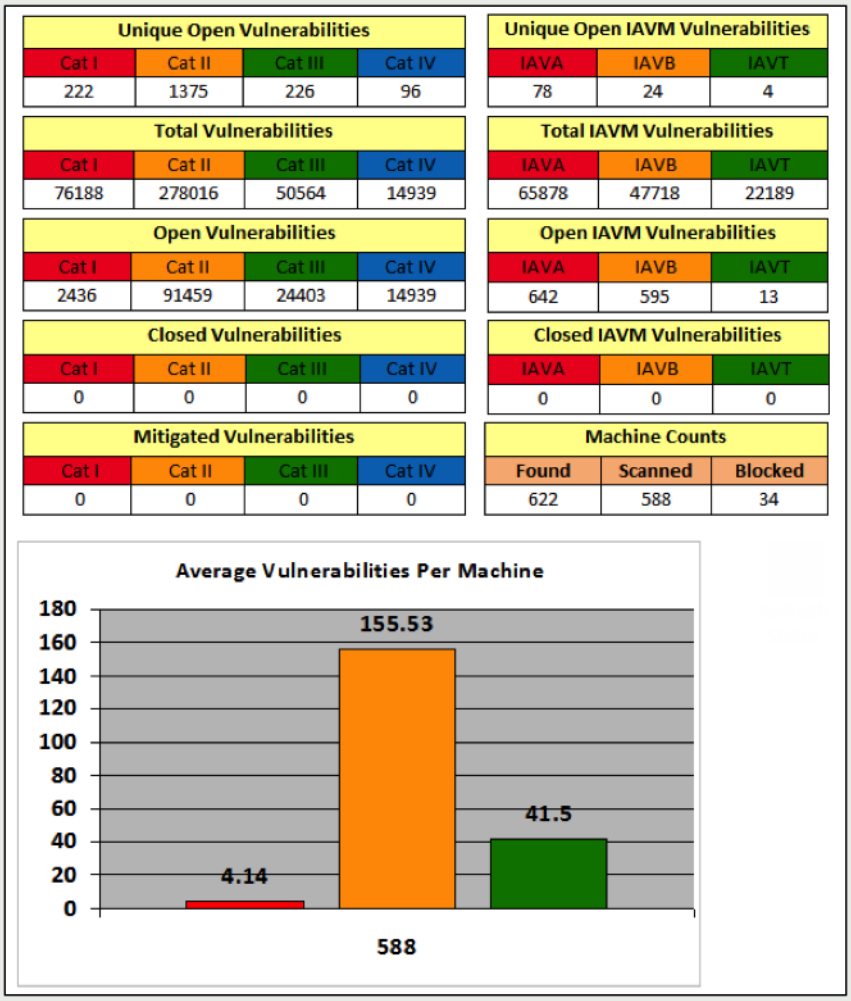
DIACAP POA&M which can be used by IA staff throughout the chain-of-command. Resource prioritization, tracking, and resolution of vulnerabilities through this POA&M is now actualized and a holistic compliance view of a site or multi-site Enterprise can be provided.



The data aggregator tool, known as iAVENGR can be used by site support staff to perform this function.

iAVENGR can:

- Condense and combine reports from multiple information assurance scanning tools
  - Eliminate multiple counts for the same vulnerability
  - Quickly incorporate results from all sources to help prioritize remediation
- Streamline POA&M generation and maintenance
  - Generate an accurate POA&M within minutes of finalizing all platform scans
  - Simplify POA&M maintenance during re-scan for lifecycle IAVM
- Reduce both human error and labor hours by automating aggregation of all scan results



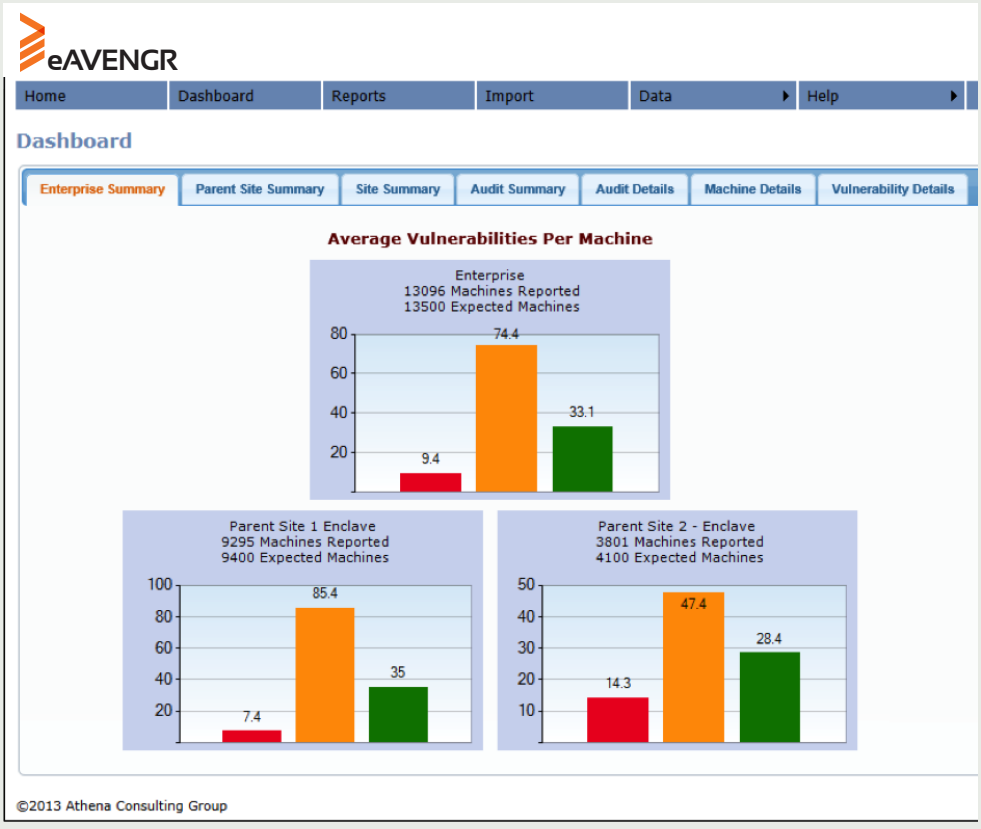
iAVENGR Dashboard

eAVENGR

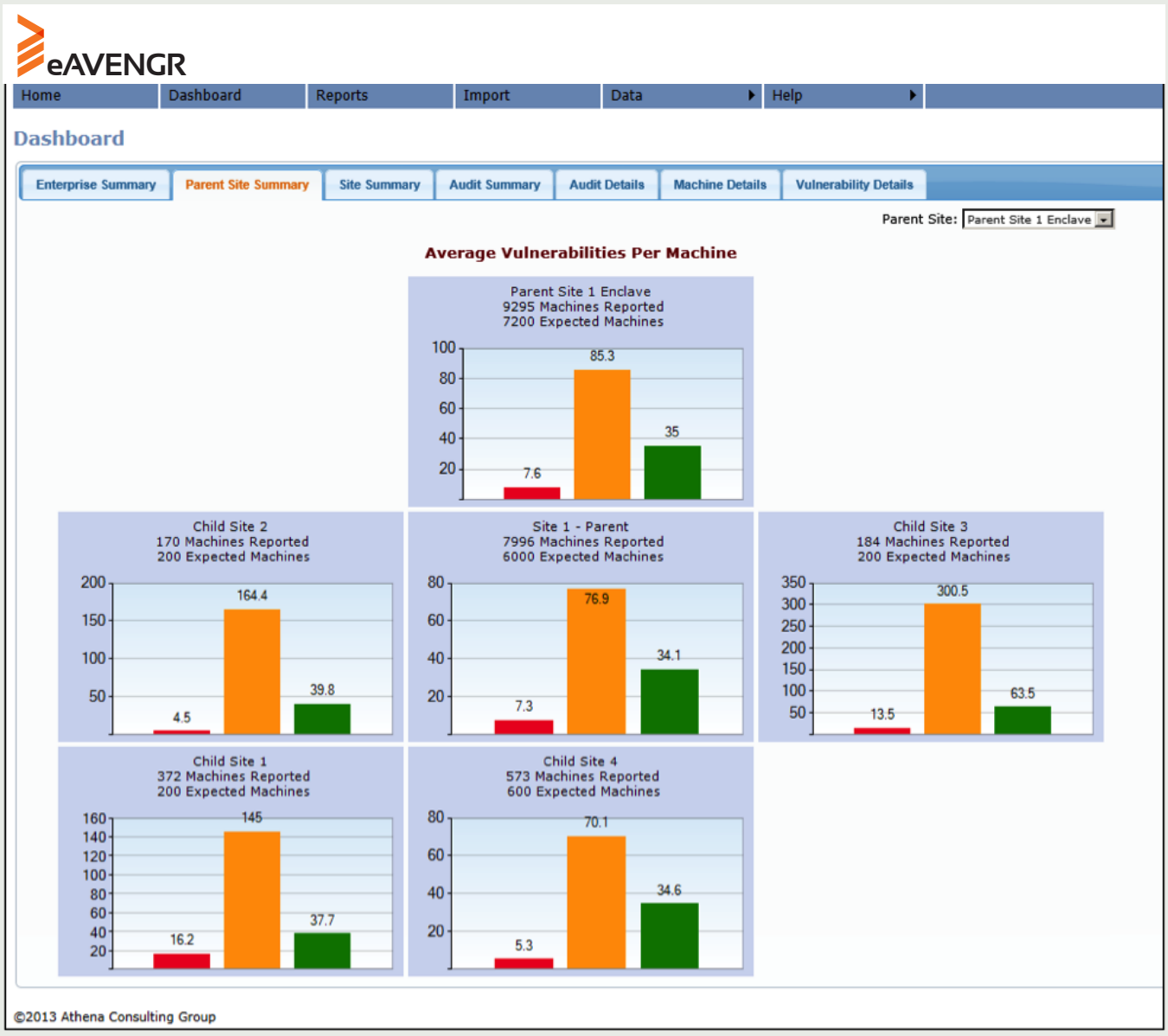
For multi-site organizations, correlated results can be obtained through the use of Enterprise AVENGR (eAVENGR) which produces a combined Enterprise assessment.

eAVENGR can:

- Aggregate data from multiple sites and
  - Present an Enterprise view of vulnerability counts from Parent Sites
  - Rollup multiple child sites to present a Parent Summary of vulnerability counts
- Detailed Vulnerability Count view for each Child Site
- Show Audit Summaries for each Child Site
- Show a detailed view of each machine and its associated Audits
- Show Vulnerability Details for each machine/component

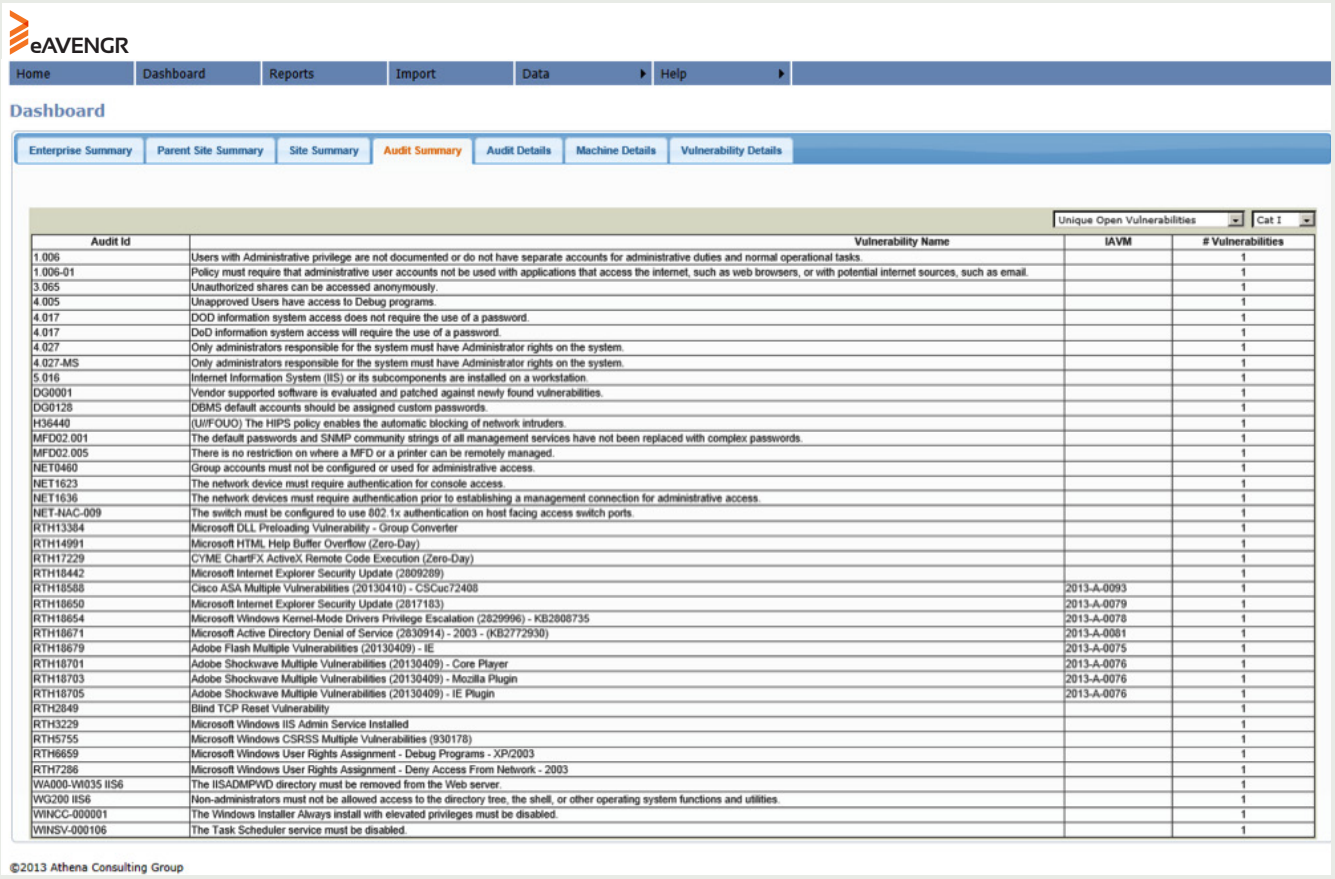


eAVENGR Enterprise Dashboard

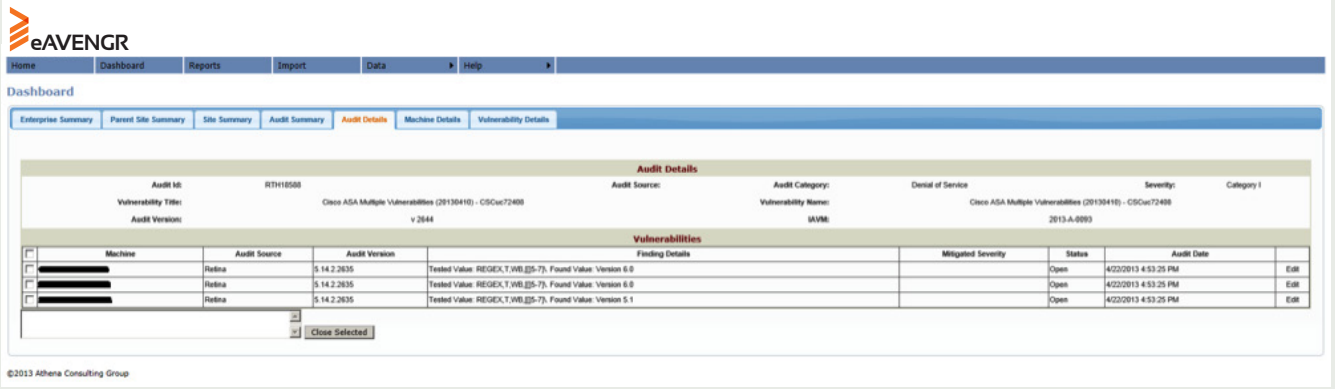


eAVENGR Parent Site Summary Dashboard

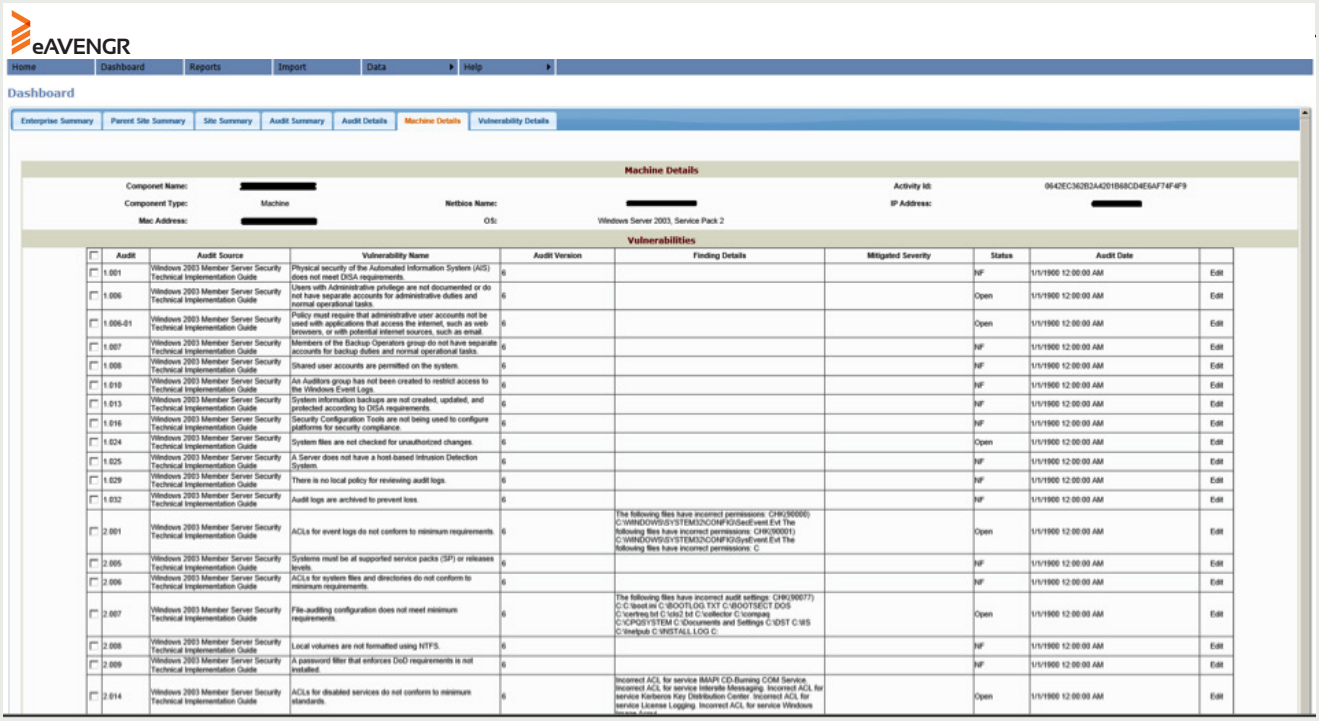
eAVENGR Child Site Summary Dashboard



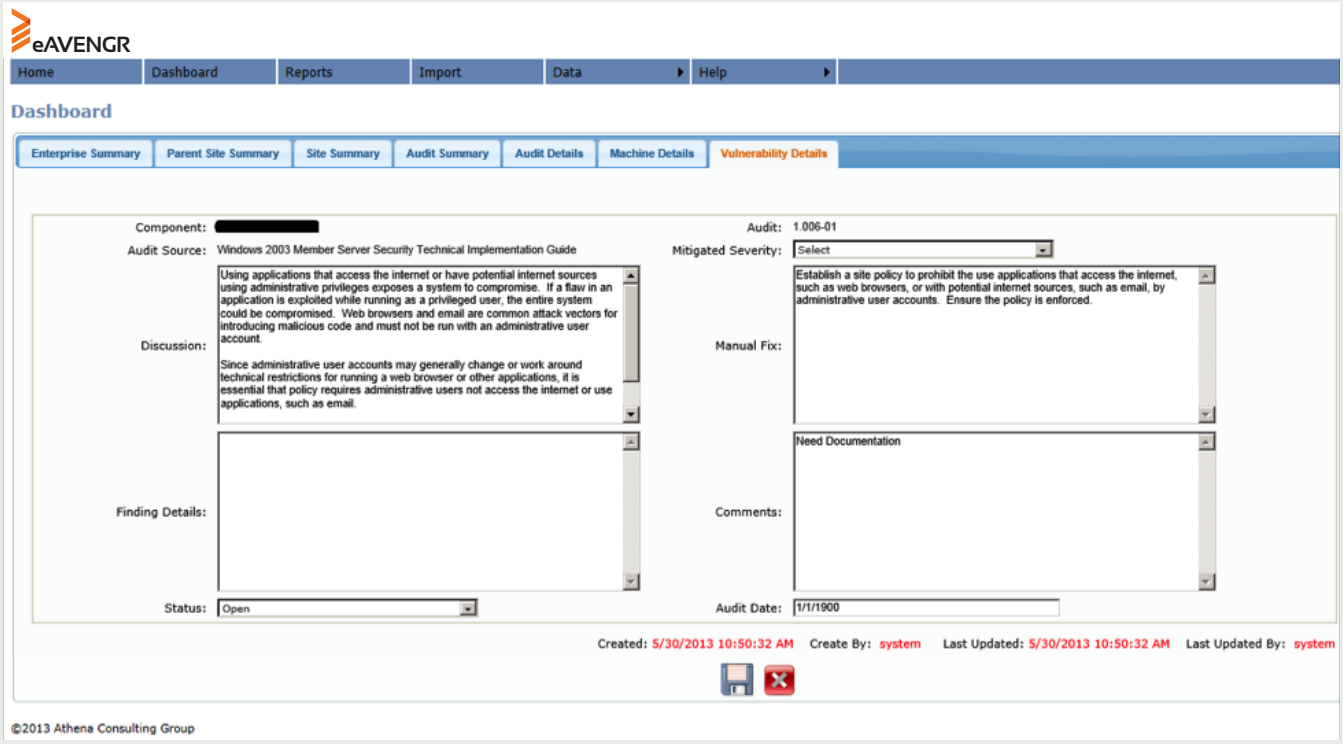
eAVENGR Audit Summary



eAVENGR Audit Details



eAVENGR Machine Details



eAVENGR Vulnerability Details

Benefits

The benefits of iAVENGR and eAVENGR are:

- Streamlined reporting occurs, whereas before reporting received could not be used, or was significantly delayed, due to volume and was error prone.
- As a result, sites have a quicker turnaround between vulnerability scan and the start of the repair process, enhancing their ability to maintain and comply with FISMA requirements.
- Centralized POA&M management gives leadership near real-time awareness of their Enterprise vulnerability status
- Enables leadership continued automated updates and visibility into the Enterprise to better understand their risk posture.
- These tools provide relevant vulnerability reporting to all levels of command from leadership (site and enterprise), to the IA workforce (IAMs, PMs, IAOs, Technicians, Administrators), and Testers.

Whether providing an enterprise or site view for leadership, or details on specific systems or even individual machines, iAVENGR and eAVENGR provide personnel with a comprehensive, useable view of open security problems and a clear understanding of the risks facing the command/enterprise so that they can use their resources in the most effective manner, fixing those problems that will have the biggest impact first, and those lesser issues later.

A Path to a More Effective IA Process

Current processes being used at sites across the enterprise are subject to inaccurate information due to the manually intensive nature of data capture/collation. As errors are inserted into the site vulnerability status, inaccurate POA&Ms are created that waste valuable resources and focus on areas that may not exist at the levels indicated.

Athena created iAVENGR and eAVENGR tools which are able to handle, sort, and graphically display data that will provide the site and leadership with real-time vulnerability counts and POA&Ms which can be used by IA staff throughout the chain-of-command.

[1] Systems Certification: This requirement calls for the periodic testing and evaluation of information security controls and techniques to ensure they have been effectively implemented. Security evaluation processes have been employed by government agencies to meet requirements of this type as part of the system authorization process, which requires reaccreditation every three years, or when significant changes to information systems are proposed. Guidance for performing testing and evaluation activities is provided in NIST SP 800-37, 800-53, and 800-53A.

Get in touch

Athena Consulting Group, LLC

4995 LaCross Rd, Suite 1250
North Charleston SC 29406
USA

Phone +1 843 375 5438
Fax +1 843 789 4894

Email AVENGR@athenaconsultinggroup.com

AVENGR