DuroSuite™

an agile DEFENSE® solution

STIG Automation | Audit + Remediation

API Integration | Artifacts

@agiledefense www.durosuite.com DuroSuite@agile-defense.com

Agile Defense's DuroSuite

Mitigating Cybersecurity Risks with Security Technical Implementation Guide (STIG) Automation

Key Features

Remediation

Agentless

Automated

Current Artifacts

Scalable

The Department of Defense and Federal Agencies need to prevent advanced persistent threat actors from gaining unauthorized access to their systems and infrastructure. However, this presents a contentious and continuous challenge with repetitive checks and audits. Agile Defense's STIG automation tool offers a solid and validated solution to perform ad-hoc systems audits, remediate, and provide current state artifacts using an immutable automated approach that leverages the advantages and cost savings of automation.

Overview

Security Technical Implementation Guides (STIGs) have been in use for many years to help protect our Information Technology systems and infrastructure. As technology evolves, cybersecurity threats advance at an unprecedented pace. In a Government Accountability Office (GAO) Cyber Security report (GAO-23-105084), it was reported that entities that provide goods or services critical to meeting U.S. military requirements continue to be the target of cyber attacks. The solution to preventing these attacks is DuroSuite! As of September 2023, DuroSuite received an official authority to operate (ATO). The assess only ATO was officially granted following months of rigorous review to ensure the tool is safe, secure, and approved for U.S. Government systems.

Continued the next page.

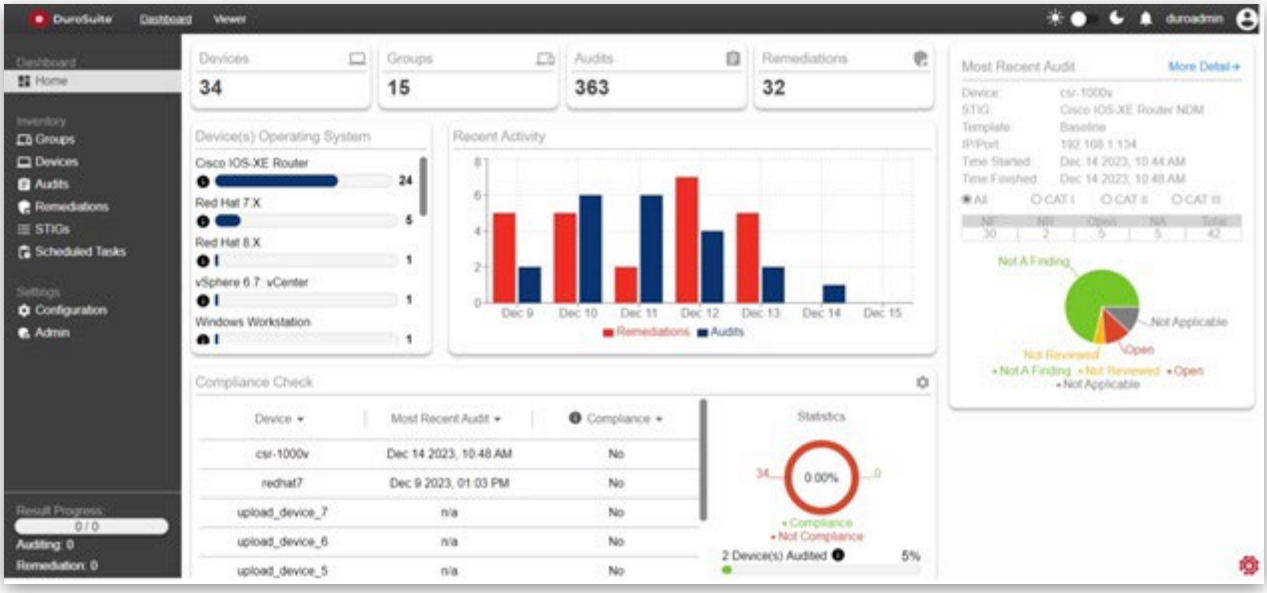
Overview (cont.)

Agile Defense's DuroSuite employs flexible and scalable automation applicable to an extensive set of systems and use cases. DuroSuite can be used for on-prem, air-gapped, or cloud infrastructures. Users can utilize the Graphical User Interface (GUI) or the Application Programming Interface (API) to access tool functionality. Our solution is critical to align agencies towards operational consistency and repeatable processes as a single solution across the enterprise infrastructure.

A key differentiator of DuroSuite is its ability to produce artifacts guaranteeing that STIGs are completed and that systems comply with Information Assurance (IA) standards and the DISA Security Requirements Guide (SRG). In addition, our solution is designed to evolve and adapt to the ever-changing IT landscape and business practices. DuroSuite has the capability to scale flexibly and to perform audits on any system that can be accessed via Secure Shell Protocol, Windows Remote Management Protocols or Systems Manager.

Agile Defense brings over 25 years of experience as an integrator to programmatically automate and remediate systems security vulnerabilities. Within minutes, DuroSuite can perform security configuration audits, remediation, and provide artifacts to demonstrate that STIGs have been completed. For one customer, the time to remediate a 24-port switch went from four hours down to 30 minutes. For their 50-switch environment, the total time to remediate went from 200 hours to five hours, a savings of 97%! This time reduction freed up staff to work on other initiatives and higher priorities.

We have demonstrated the success of our DuroSuite solution in supporting various government agencies. Leave behind the panic that typically accompanies audit preparation. Getting ready for a CCRI or CCORI audit is a breeze when using DuroSuite. Agile Defense is paving the way for government and federal agencies to adopt automation in their day-to-day operations.



www.agile-defense.com | www.durosuite.com

@agiledefense