SQUIRREL
COMPLIANCY SOLUTIONS

1.833.477.8477
sales@squirrelcompliancy.com
www.squirrelcompliancy.com
3434 Kildaire Farm Road
Suite 135 PMB 536
Cary, NC 27518

Solution Overview

Automated Network Compliance for DISA STIGs

Cyber Defense Enforcement

- Continuous monitoring of your compliance status
- Know your security posture awareness at any moment

Operational Benefits

- Reduced level of effort (LOE) required to maintain your environment saving thousands of personnel hours per audit which can be redirected to mission critical, higher value added activities

Know your security posture and risks before they become issues

NAICS:
519190, 541310, 541330, 541511, 541512, 541513, 541519, 541690, 611420, 511210

DUNS: 080982289

CAGE: 8OEX3

Challenges of Operating a Secure Network Environment

The level of effort required to assess and maintain network infrastructure is a significant barrier to operating secure environments. The estimated time to assess compliance with DISA STIGs is **one personnel hour per device per audit[1]. Our service enables assessment of a device in under 7.5 seconds[2].**

The U.S. DoD is continuously implementing new methods to ensure communications security. The Defense Information Systems Agency (DISA) releases Security Technical Implementation Guides (STIG) to assist with the protection and defense for the systems that support military readiness and operations. The STIGs are a key element in implementation of the Risk Management Framework (RMF) security controls.

Command Cyber Readiness Inspections (CCRI) are performed to assess defensive posture as it relates to DISA STIG best practices.

Our service automates the tedious manual process of determining if network devices are configured in accordance with the appropriate DISA STIGs and RMF security controls.

Our service can save you thousands of personnel hours and millions of dollars per year.

Numbers of Device	Hours for 52 manual audits	Hours for 52 automated audits	Estimated cost for 52 manual audits[3]
500	19,500	13 hrs	$1.17M
2,500	97,500	65 hrs	$5.85M
5,000	195,000	130 hrs	$11.7M
10,000	390,000	260 hrs	$23.4M

[1] Based on assessing all appropriate regulatory standards for all appropriate components of each device

[2] Performance can vary between customer environments based on the number of interfaces and server resource.

[3] Effort estimate based on 45 minutes per device per audit at GS12 Step 6 pay

Squirrel's Automated Network Compliance for DISA improves security posture quickly and efficiently

Our Automated Network Compliance for DISA STIGs (ANCDS) solution provides visibility into your network infrastructure security posture at a glance. The solution can be utilized across any network classification thus ensuring communication security for any environment.

Our solution mirrors the requirements outlined in the DISA network infrastructure STIGs to determine the security posture. The audit information allows determination of operational risks using the DISA STIG vulnerability ranking classification system.

Know your network better than your adversaries

Built-in Remediation

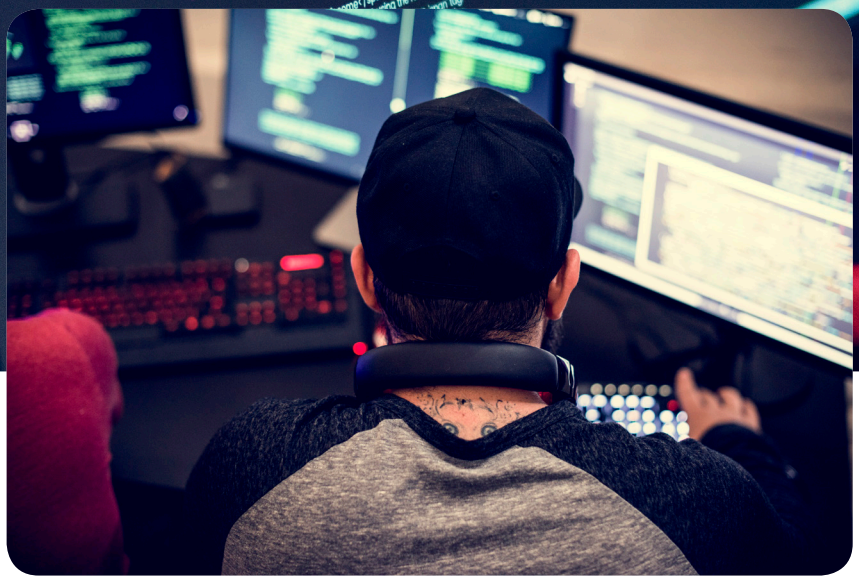
Our solution provides interactive remediation to automate the implementation of security controls. This capability further decreases the time for vulnerabilities to be corrected and reduces your attack surface.

Continuous Compliance Monitoring

Our service allows you to audit your environment daily (or more often) to improve situational awareness of your security and RMF posture.

Improve Staff Efficiency

By automating time-consuming audits, we allow your staff to increase focus on the mission and operating your organizations network infrastructure.



Solution Benefits

- Annual subscription and tiered pricing structure to meet your organization's needs
- Risk scoring for software and configuration vulnerabilities using NIST and DISA classification standards
- Analysis and reporting of out-of-support device operating systems, chassis hardware and hardware modules
- DISA STIG/SRG configuration vulnerabilities analysis and reporting
- Automated remediation of user selected DISA STIG configuration vulnerabilities to further decrease level of effort
- Minimizes the staff workload and operational overhead
- Remote support and vulnerability consulting included for the solution
- Ad-hoc audits to address out-of-cycle or zero-day software vulnerabilities reporting
- No sampling; all devices and interfaces are inspected ensuring thorough compliance
- On-site support included in the cost of the subscription
- 100% on-premises - no information leaves your site