



Unifying STIG Compliance Across Separate NIPR and University Environments

CHALLENGE: Relieving the manual effort involved in managing two separate environments

Organizations operating in two or more distinct environments face unique compliance challenges. Each environment has different security requirements, yet both must maintain rigorous hardening standards, continuous monitoring and audit readiness. This can cause great strain on the manhours, timelines and costs it takes to comply with Security Technical Implementation Guides (STIGs) and stay compliant.

In 2013, an organization that fosters education and collaboration for a more secure Pacific region faced that exact dilemma. Their team needed to maintain Authorization to Operate (ATO) requirements while supporting Cybersecurity Risk Management Construct (CSRMC) / Risk Management Framework (RMF) processes, eMASS reporting, quarterly vulnerability scans and ongoing remediation across separate NIPR and University environments.

The team's compliance activities relied heavily on manual processes. They used multiple tools to help streamline their efforts, including Evaluate STIG, Group Policy Objects (GPOs), Microsoft Intune and other point solutions to help scan, harden and remediate their Windows systems.

While these tools addressed portions of the compliance process, they lacked the automation necessary to efficiently manage nearly 500 endpoints spread across their NIPR and University environments. More than that, however, the incompatibility issues of using disparate tools created more work and frustration.

Manual remediation created several operational challenges that couldn't be solved using the tools they were using:

- ✓ Once scanned, STIG remediation required significant hands-on effort
- ✓ GPO management became increasingly complex, particularly when application compatibility issues occurred
- ✓ Separate toolsets were required for different environments, increasing administrative overhead
- ✓ Broken applications added to their already extensive remediation efforts
- ✓ Quarterly scans and reporting demanded substantial staff time
- ✓ Cybersecurity personnel were spending valuable hours on repetitive compliance tasks rather than higher-value security initiatives

To relieve the amount of effort involved, along with its accompanying frustration, the organization started searching for a single, agent-based solution capable of automating STIG hardening, while also supporting separate NIPR and University environments without increasing infrastructure complexity.

SOLUTION: Uniting efforts and environments through a unified automation solution

After a thorough review, the organization chose SteelCloud's ConfigOS MPO, a unified automation solution, purpose built to scan, remediate, verify and report from the same platform based on STIG and/or CIS Benchmarks requirements. As a single solution, it delivered the automation, integration, flexibility and comprehensive features that existing tools could not provide, as well as customization capabilities for policies and the differing requirements of securing both a NIPR and University environment.

ConfigOS delivered an agent-based approach to automated STIG hardening and continuous compliance management across both environments. The deployment included:

- ✓ 480 Windows workstations (150 in University space and 330 in NIPR)
- ✓ 27 Windows servers
- ✓ Two iterations of the ConfigOS policy workbench, one for University policy and another for NIPR policy

By replacing manual remediation workflows with automated policy enforcement, the organization significantly simplified its compliance operations, dramatically reducing the time, effort and cost of compliance; improving accuracy; and enabling effortless continuous compliance.

Key capabilities included:

- ✓ Automated STIG hardening *and* remediation
- ✓ Agent-based enforcement where endpoints continuously apply and maintain approved configurations locally
- ✓ Continuous monitoring profiles supporting quarterly compliance activities
- ✓ RMF/CSRMC and eMASS reporting support
- ✓ Improved readiness for ATO renewals and security audits
- ✓ Centralized management across separate NIPR and University environments
- ✓ Reduced dependence on GPO-based remediation

The organization was among ConfigOS' earliest adopters and became the first implementation across two separate network environments, demonstrating the platform's flexibility in complex operational settings.

RESULTS: Transforming compliance processes and delivering better security

With ConfigOS, the organization no longer needs to juggle disparate tools that weren't built to be used with each other. Instead, they have a single solution offering all the functionality they need to simplify compliance across two domains from a single dashboard.

The organization immediately realized many other meaningful operational improvements, such as:

- ✓ **Streamlined Compliance Operations.** ConfigOS' automation has dramatically reduced the amount of manual effort required to maintain STIG compliance, allowing hardening, remediation and continuous monitoring to become repeatable and consistent processes rather than labor-intensive projects.
- ✓ **Improved Audit Readiness.** By automating compliance workflows and supporting RMF/CSRMC and eMASS reporting requirements, the organization is better prepared for ATO renewals, quarterly assessments and potential audits.
- ✓ **Greater Operational Efficiency.** Instead of spending significant time manually scanning systems, troubleshooting GPOs and performing repetitive remediation tasks, cybersecurity personnel can focus on mission-critical security initiatives that deliver greater organizational value.
- ✓ **Increased Customization.** With ConfigOS, the organization can create, manage and deploy custom policies; tailor their solution to different environments; and create custom security controls.
- ✓ **Simplified Management Across Multiple Environments.** ConfigOS enables the organization to manage both its NIPR and University environments using a consistent automation strategy while still meeting the distinct requirements of each network.

For organizations managing multiple security environments with limited cybersecurity resources, automated compliance can transform STIG hardening from an ongoing administrative burden into a sustainable, repeatable process that strengthens security while reducing operational workload.