WHITE PAPER

Daily Federal Compliance and Continuous Cybersecurity Monitoring

solarwinds federal

Introduction

Governments have a critical need for information security. The many agencies that comprise government require and amass great quantities of information. Much of this information is vital to national, economic, and security interests, and must be vigorously defended from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction. Therefore, government agencies must comply with strict standards and controls designed to offer these protections.

Defense Information Systems Agency (DISA) is a combat support agency that provides, operates, and ensures command and control, information-sharing capabilities, and a globally-accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of its operations. DISA-managed IT supports some of the most critical programs in the U.S. government, and therefore requires the highest levels of confidentiality and availability.

To achieve its operational objectives, DISA has developed the Security Technical Implementation Guides (STIGs) for securing information and systems under its control. The STIGs are specific to operational and device-level technical controls and how to configure those controls on specific hardware. For example, a STIG for a Cisco® router will not only mandate using passwords to restrict router access, but also provide iOS® configuration instructions for how to properly configure password authentication.

The Department of Defense (DoD), through adoption of the DISA STIGs, was doing a reasonable job of IT security in 2002. However, Congress decided that the civilian agencies were not taking IT security seriously enough, so they created the Federal Information Security Management Act (FISMA) to help the civilian agencies secure their IT systems.

FISMA requires each federal agency to implement information security safeguards, audit these safeguards annually, and make an accounting to the Office of Management and Budget (OMB). The OMB, in turn prepares an annual compliance report for Congress. FISMA standards and guidelines are developed by the National Institute of Standards and Technology (NIST).

FISMA requires every U.S. federal agency to adopt the following process:

1. Categorize information and systems according to confidentiality and availability
2. Design operational and technical controls based on categorization
3. Construct policies mandating what systems and information assets are to be protected using specified controls

4. Verify that controls and policy mitigate risks
5. Implement policies and controls and maintain compliance through regular certification
6. Continuously monitor systems and controls to prevent compliance drift and to update operating and technical controls

Implementing FISMA required NIST to produce several key security standards and guidelines. These publications include FIPS 199, FIPS 200, and NIST Special Publications such as 800-53. These documents provide standards for categorizing IT systems by mission impact, establish minimum security standards for data and IT systems, and institute baseline security controls.

NIST has continued to take a leadership role by working with DoD and other agencies to establish a unified information security framework for the federal government. In 2010, NIST introduced the Risk Management Framework (RMF), a six-step process that includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. As described in the background section of the publication, "The intent of this common framework is to improve information security, strengthen risk management processes, and encourage reciprocity among federal agencies." (Section 1.1; SP 800-37)

RMF provides a framework that combines IT security and risk management into the systems development lifecycle to enable a more dynamic approach to managing agency risk. RMF is transforming the traditional certification and accreditation (C&A) process agencies use to ensure security requirements are met.

THE PROBLEM

There are a number of challenges that government agencies face to achieve and maintain FISMA, DISA STIG, and RMF compliance, especially in the area of network security. Some of these are:

- Routers and switches are complex devices that require many commands to properly configure. Routinely examining these configurations and verifying all required technical controls are present and properly implemented (such as DISA STIGs in the case of DoD protected systems) can be daunting.
- Even when technical controls are initially implemented, unless the operational controls are also in place, vulnerabilities will soon appear. IT systems are dynamic and constantly changing, as are the methods attackers use to breach defenses. Therefore, there must be strict management controls in place to manage inevitable change. Unfortunately, there are few specialized tools to help network managers adequately manage operational controls.

THE CONSEQUENCES

The consequences of noncompliance far exceed the threat of simple inconvenience or sanctions. While punitive sanctions are undesirable, the true cost of loss is often measured in human lives, weakening of national security, interruption of crucial services to citizens, or significant economic losses.

Cybersecurity remains the top priority of federal CIOs, and that's not surprising, given the findings in the Verizon 2018 Data Breach Investigations Report, which found that there were 304 breaches and 22,788 security incidents in the public sector. Additional public sector findings included that 44% of the breaches were motivated by espionage, attacks usually involve phishing or installation and use of backdoors, and that personal data is being targeted in addition to state secrets.

Everyone should be familiar with high-profile breaches such as those involving the Office of Personnel Management (OPM) and Edward Snowden.

The OPM breach compromised the personal and sensitive data of millions of Americans. A congressional report found that prior data breaches in 2014 were likely associated with the 2015 data breach. Additional findings were that the breach was preventable, but OPM leadership failed to prioritize resources for cybersecurity.

Snowden, by using his knowledge of the NSA's poor control over its SSH and private keys and self-certificates, was able to turn those security assets against the NSA and steal valuable and top secret information. The need for continuous monitoring to stay compliant with information assurance standards like FISMA and the DISA STIGs has never been greater.

Fortunately, even seemingly small measures can have a significant impact. Sustained attacks always rely on finding holes in the defenses. The FISMA/RMF guidelines and DISA STIGs serve to close those avenues for easy exploit and greater access.

SOLUTION

A recent SolarWinds federal cybersecurity survey showed that:

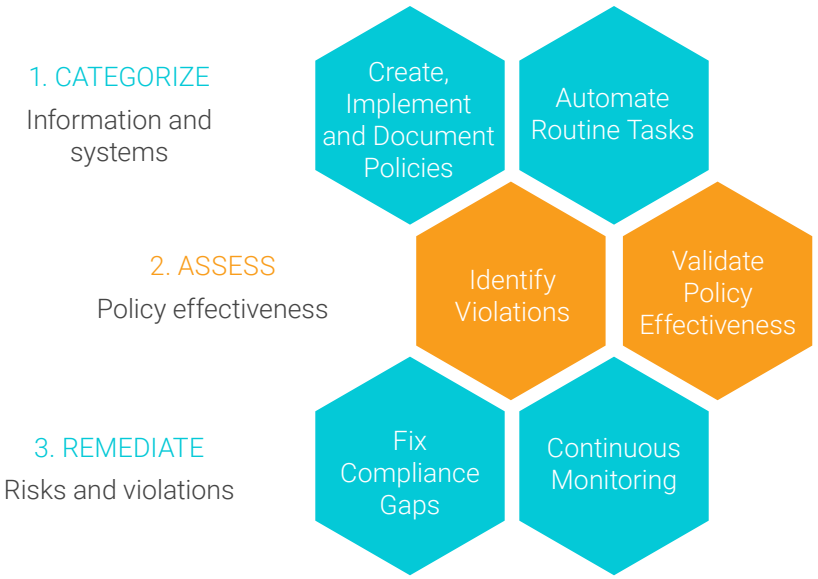
- 54% of respondents said that careless/untrained insiders are first to blame for cybersecurity breaches. Foreign governments and the general hacking community were other leading sources of security threats, as reported by 48% and 38% of respondents respectively. Threats are coming from all directions.
- As a source of threats, malicious insiders have seen significant increases; from 2014 to 2017, surveys results nearly doubled from 17% to 29%.

DISA STIGs and FISMA/RMF standards require each federal government agency to develop minimally-acceptable system configuration requirements and ensure compliance. Systems with secure configurations are less vulnerable and better able to thwart network attacks.

The exploitation of vulnerabilities must be evaluated at the level of the network device being reviewed. A router, for example, is a standalone device for some purposes and part of a larger system or network for others. All these risk factors are to be considered when developing mitigation strategies at the device and system level:

- Risks to the device
- Risks to the device in its environment
- Risks presented by the device to the environment

CATEGORIZING, ASSESSING, AND REMEDIATING SECURITY RISKS



SolarWinds recommended steps in the process of categorizing, assessing, and remediating security risks in accordance with the DISA STIGs and FISMA/RMF standards.

Enhancing compliance for your network can be achieved through three simple steps.

1. Categorize information systems
2. Assess policy effectiveness
3. Remediate risks and violations

Let us examine in detail the tasks involved in each step, its significance, and best practices for execution.

INFORMATION SYSTEMS

The first step in this process is to review and inventory all devices in the network. Then, assess compliance requirements and devices that need to be brought into compliance.

For those devices out of compliance, make the required changes and bring them under regulatory controls. Clearly document the applied policies and steps taken to comply with regulatory controls. This is helpful for audit proofs and to maintain an audit trail of what changes were made to the network and when.

Next, automate routine tasks like bulk password changes, perimeter device hardening, configuration backup and archival, configuration changes (e.g., SNMP configuration, VLAN configuration, access control list changes), or even interface configuration changes.

Automation helps reduce human error and systematically conduct routine tasks required to maintain compliance. Network administrators—especially those handling very large networks with hundreds of devices—are finding it increasingly difficult to carry out these repetitive but important tasks manually. Yet, ignoring these everyday jobs or putting them off for extended periods of time can be disastrous to your network.

ASSESS POLICY EFFECTIVENESS

Once security controls are in place, it is important to ensure that they are enforced and followed. Devices need to be continuously monitored and changes tracked. Any new device configuration or change in configuration must conform with internal and external policies documented for the agency.

Continuous compliance, requires regular audits to assess and identify violations. Validate policy effectiveness separately through analysis and by conducting penetration tests.

Compliance assessment can also be automated with the use of tools that run reports and list policy violations.

Despite the tedium of these tasks, it's very important that they be carried out regularly and effectively. Some steps that help administrators improve compliance include:

1. Establish baseline configurations so that they can be used in the case of a configuration issue.
2. Generate compliance reports that can help verify compliance and point out policy violations.
3. Ensure that security and risk management controls are exercised and practiced.

REMEDIATE RISKS AND VIOLATIONS

Once assessment is complete and security gaps and policy violations listed, the next and most important step is to close these vulnerabilities that put the network at risk.

This is called remediation, and all steps taken need to be documented. All proposed changes must be reviewed and approved by authorized personnel. This helps reduce the chance of errors or misconfigurations.

Use of a tool can help automate the change management approval process with the help of role-based controls. It also provides an audit trail that tracks users who uploaded configurations so the right people can be involved in fixing problems.

The use of an automated tool also simplifies configuration management and can save hours of troubleshooting. In a given scenario, an administrator makes changes to a router one evening and runs through the test plan where all looks fine. However, the next day, the help desk is swamped with phone calls related to a problem caused by that change. So, remediation also includes the provision to be able to quickly roll back a bad or unauthorized change.

Finally, continuously monitor devices to know whenever device configurations are changed, even if changes are made directly on the device. This eliminates the problem of mystery changes that haven't been approved and aren't discovered right away, which can reduce downtime.

In short, continuous monitoring encourages timely awareness of vulnerabilities, allows faster detection of a possible security incident, helps ensure latest compliance guidelines are in place, and provides clear visibility into compliance status on the network.

Let's not forget that new vulnerabilities get reported frequently. Configuration management tools should be able to get updates on emerging threats and help determine agency impacts. Device configurations and firmware that are vulnerable must be remediated.

Along with increasing requirements from regulatory agencies and a growing awareness of security risks of nonconformity, agencies now implement compliance as an integrated part of their daily operations. To do so successfully, they need the support of easy-to-use technology.

BENEFITS AND SUMMARY

Manual execution is certainly not advisable to carry out the above compliance tasks. It is recommended that you invest in an automated solution that offers a single interface to manage all the devices in your multivendor environment. A previously-conducted study by Market Connections and SolarWinds indicates that IT pros are using continuous monitoring tools to detect network issues and vulnerabilities within minutes.

Time to Detect and Analyze Compliance

	Time taken	Total respondents	Continuous monitoring user	Continuous monitoring non-user
How long does it typically take your organization to detect and/or analyze network device configurations out of compliance?	Within minutes	20.0%	24.0%	13.3%
	Within hours	28.0%	27.2%	29.3%
	Within one day	21.0%	23.2%	17.3%
	More than one day	17.0%	14.4%	21.3%
	No ability to detect	1.5%	0%	4.0%
	Don't know/unsure	12.5%	11.2%	14.7%

Twenty percent of federal IT pros are able to detect noncompliant configurations within minutes ; responses also varied based on use of continuous monitoring. Source: SolarWinds 2014 Cybersecurity Survey

Continuous monitoring users, significantly more than non-users of automated tools, point out that most practices and technologies are essential and warrant priority investments.

IMPORTANCE OF SECURITY TO CONTINUOUS MONITORING USERS

	Continuous monitoring user	Continuous monitoring non-user
Firewall configuration and security continuous monitoring	53%	33%
Intrusion detection and prevention	52%	31%
Improving system defenses e.g. anti-virus, HIPS	46%	32%
Network configuration security compliance continuous monitoring	46%	31%
Database security	44%	17%
Vulnerability management	41%	25%
Technologies and processes to monitor and block use of removable media (USB, etc.)	37%	23%
Secure remote system administration	36%	20%
Security information and event management	34%	20%
Patch management	33%	19%

= statistically significiant difference

Users of continuous monitoring consider compliance and vulnerability management more essential than do non-users. Source: SolarWinds 2014 Cybersecurity Survey

Compliance policies and controls can be implemented at any time. However, to enforce them, you need specialized tools to help manage device configurations according to FISMA, RMF, and STIG guidelines.

The survey results above illustrate the importance of using automation for continuous monitoring. Consider consolidating the management of tasks with configuration backup, configuration change, device inventory, and compliance checks through a single automated solution.

SolarWinds Network Configuration Manager (NCM) saves time and improves network reliability and security by managing configurations, changes, and compliance for routers, switches, and other network devices. Use of tools such as NCM for continuous monitoring helps improve agency detection and response times.

With NCM you can:

- Easily download and back up network device configurations
- Create baselines and automatically compare configurations
- Audit device configs for compliance and obtain reports on violations
- View graphs on compliance details for each device
- Leverage user-tested STIG and FISMA policy templates
- Automatically identify IOS devices with newly reported vulnerabilities
- Take advantage of options designed to help with immediate compliance remediation

The cost of noncompliance can be high. If vulnerabilities are present, unwarranted entities can penetrate and gain access to confidential data, putting essential agency missions and lives in danger. Don't let a security threat or breach put you or your agency in jeopardy.

ABOUT SOLARWINDS

SolarWinds provides powerful and affordable IT management software to customers worldwide, from Fortune 500® enterprises to small businesses, managed service providers (MSPs), government agencies, and educational institutions. We are committed to focusing exclusively on IT, MSP, and DevOps professionals, and strive to eliminate the complexity that our customers have been forced to accept from traditional enterprise software vendors. Regardless of where the IT asset or user sits, SolarWinds delivers products that are easy to find, buy, use, maintain, and scale while providing the power to address key areas of the infrastructure from on-premises to the cloud. This focus and commitment to excellence in end-to-end hybrid IT performance management has established SolarWinds as the worldwide leader in both network management software and MSP solutions, and is driving similar growth across the full spectrum of IT management software. Our solutions are rooted in our deep connection to our user base, which interacts in our THWACK® online community to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at www.solarwinds.com.

FEDERAL
Phone: 877.946.3751
Email: federalsales@solarwinds.com
www.solarwinds.com/federal

NATIONAL GOVERNMENT
Phone: +353 21 2330440
Email: nationalgovtsales@solarwinds.com
www.solarwinds.com/nationalgovernment