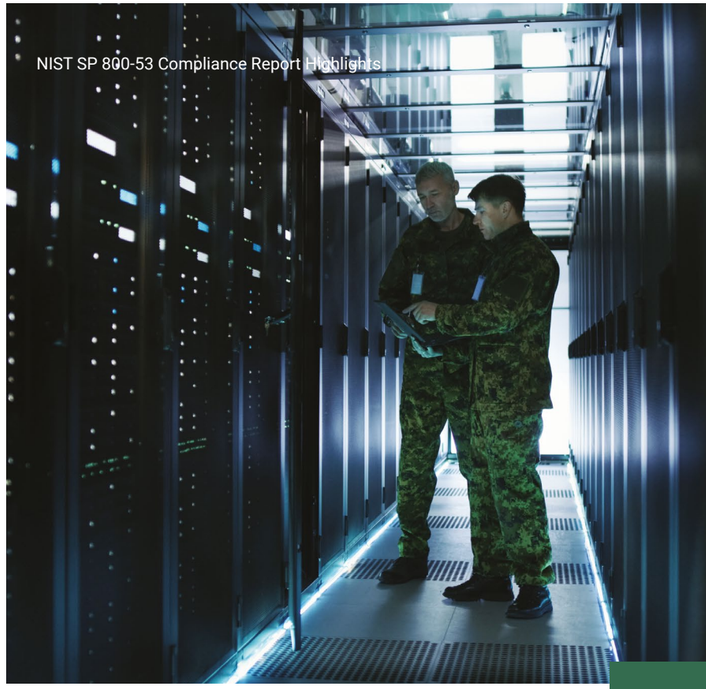
TITANIA

NIST SP 800-53 compliance reporting made easy

Your guide to the innovative new features in Nipper's dedicated NIST SP 800-53 Compliance Report

NIST SP 800-53 Compliance Report Highlights



Nipper InfraSight automatically analyzes NIST SP 800-53 non-compliances that it identifies, to reveal the risk to the network if the misconfiguration is exploited.

Validate NIST SP 800-53 compliance using trusted pathways

Demonstrating compliance with the NIST SP 800-53 framework has typically involved manually mapping network infrastructure device checks to requirements – a process which is inherently time-consuming.

The new NIST SP 800-53 compliance report from Titania changes all this. Using trusted pathways of validation, Nipper software now provides an automated way to embed the risk focus, evidence and best practice required to deliver security from compliance with the framework.

Cybersecurity teams can:

- Assess network compliance with NIST SP 800-53,
- Validate compliance with evidence, and
- Prioritize non-compliances for remediation.

Risk Focus | Evidence | Best Practice

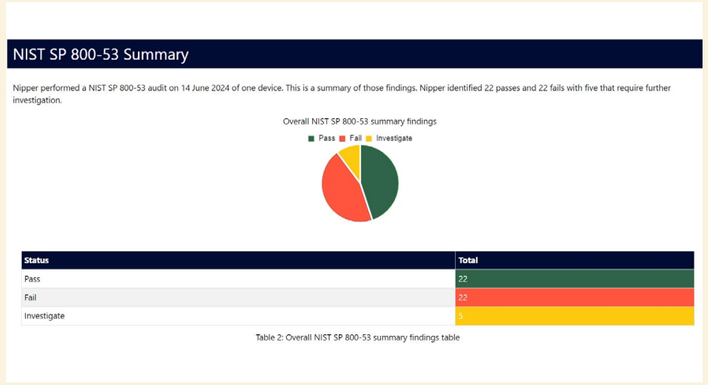
Cybersecurity teams that are mandated to evaluate and report their compliance will benefit from:

- **Automated requirements mapping of NIST SP 800-53 network controls with drill down to testing procedures.**
- **An assessor-ready report providing evidence for both passed and failed checks.**
- **Risk-prioritized findings where misconfigurations are prioritized based on STIG CAT I, CAT II, CAT III ratings.**

Established best practice, automated with precision

Nipper InfraSight automatically analyzes NIST SP 800-53 non-compliances it identifies, to reveal the risk to the network if the misconfiguration is exploited, providing an easy way to categorize risks and helping to inform remediation workflows.

And now, Nipper OmniSight provides this capability on an enterprise scale – leveraging the precision of Nipper InfraSight to assess routers, switches and firewalls to assure NIST SP 800-53 compliance on an up-to-hourly basis, or whenever configuration changes are detected.



NIST SP 800-53 Summary

Nipper performed a NIST SP 800-53 audit on 14 June 2024 of one device. This is a summary of those findings. Nipper identified 22 passes and 22 fails with five that require further investigation.

Overall NIST SP 800-53 summary findings

Status	Total
Pass	22
Fail	22
Investigate	5

Table 2: Overall NIST SP 800-53 summary findings table

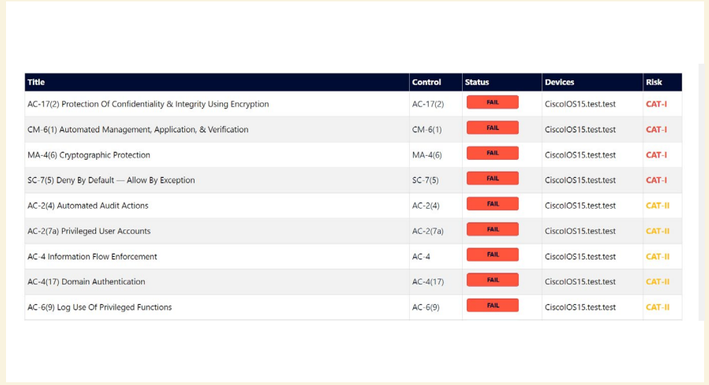
1. At-a-glance compliance posture

Innovation

- Nipper InfraSight checks are automatically mapped to NIST SP 800-53 requirements.
- The assessment findings are summarized to provide visibility of the compliance posture of devices.

Benefit

Get a high-level overview of the NIST SP 800-53 assessment results, summarizing passes, fails, and any findings that require further investigation, as well as checks that are not applicable.



Title	Control	Status	Devices	Risk
AC-17(2) Protection Of Confidentiality & Integrity Using Encryption	AC-17(2)	FAIL	CiscoIOS15.test.test	CAT-I
CM-6(1) Automated Management, Application, & Verification	CM-6(1)	FAIL	CiscoIOS15.test.test	CAT-I
MA-4(6) Cryptographic Protection	MA-4(6)	FAIL	CiscoIOS15.test.test	CAT-I
SC-7(5) Deny By Default — Allow By Exception	SC-7(5)	FAIL	CiscoIOS15.test.test	CAT-I
AC-2(4) Automated Audit Actions	AC-2(4)	FAIL	CiscoIOS15.test.test	CAT-II
AC-2(7a) Privileged User Accounts	AC-2(7a)	FAIL	CiscoIOS15.test.test	CAT-II
AC-4 Information Flow Enforcement	AC-4	FAIL	CiscoIOS15.test.test	CAT-II
AC-4(17) Domain Authentication	AC-4(17)	FAIL	CiscoIOS15.test.test	CAT-II
AC-6(9) Log Use Of Privileged Functions	AC-6(9)	FAIL	CiscoIOS15.test.test	CAT-II

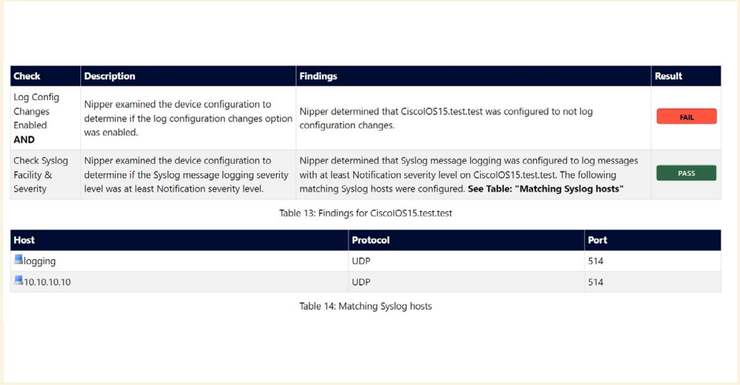
2. Potential impact summary

Innovation

- The solution prioritizes non-compliances according to STIG CAT I, CAT II, and CAT III status, reflecting risk criticality.
- It identifies the specific devices affected that carry a non-compliance risk and require remediating action.

Benefit

Drill down to passes and failures, to understand the potential impact of non-compliances as well as determining which checks need to be performed manually.



Check	Description	Findings	Result
Log Config Changes Enabled **AND**	Nipper examined the device configuration to determine if the log configuration changes option was enabled.	Nipper determined that CiscoIOS15.test.test was configured to not log configuration changes.	FAIL
Check Syslog Facility & Severity	Nipper examined the device configuration to determine if the Syslog message logging severity level was at least Notification severity level.	Nipper determined that Syslog message logging was configured to log messages with at least Notification severity level on CiscoIOS15.test.test. The following matching Syslog hosts were configured. **See Table: "Matching Syslog hosts"**	PASS

Table 13: Findings for CiscoIOS15.test.test

Host	Protocol	Port
logging	UDP	514
10.10.10.10	UDP	514

Table 14: Matching Syslog hosts

3. Risk-prioritized evidence

Innovation

- Automated analysis of each 'passed' check provides the evidence required to show compliance, whilst detailed risk information about any failures helps inform remediation workflows.

Benefit

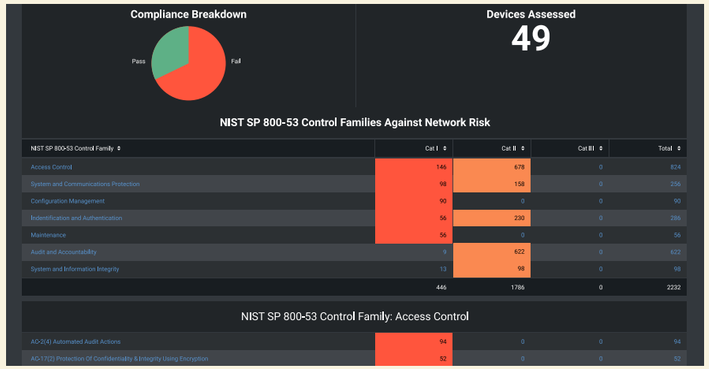
- For each device - see findings against applicable NIST SP 800-53 requirements, with an explanation of the testing procedure.

Five innovative new report features

Streamlining compliance reporting so you can focus on improving network security posture.

Delivering so much more than accurate compliance reporting, Titania's new NIST SP 800-53 report is packed with powerful insights to help embed the risk focus, evidence and best practice required to deliver security from compliance.

Here's your guide to risk prioritizing non-compliances for remediation, tracking changes between audits, and driving further investigation into whether drift was accidental or deliberate.



Compliance Breakdown

Devices Assessed
49

NIST SP 800-53 Control Families Against Network Risk

NIST SP 800-53 Control Family	Cat I	Cat II	Cat III	Total
Access Control	146	678	0	824
System and Communications Protection	98	158	0	256
Configuration Management	90	0	0	90
Identification and Authentication	56	230	0	286
Maintenance	56	0	0	56
Audit and Accountability	0	622	0	622
System and Information Integrity	13	98	0	98
	445	1786	0	2232

NIST SP 800-53 Control Family: Access Control

AO-2(4) Automated Audit Actions	94	0	0	94
AC-17(2) Protection Of Confidentiality & Integrity Using Encryption	52	0	0	52

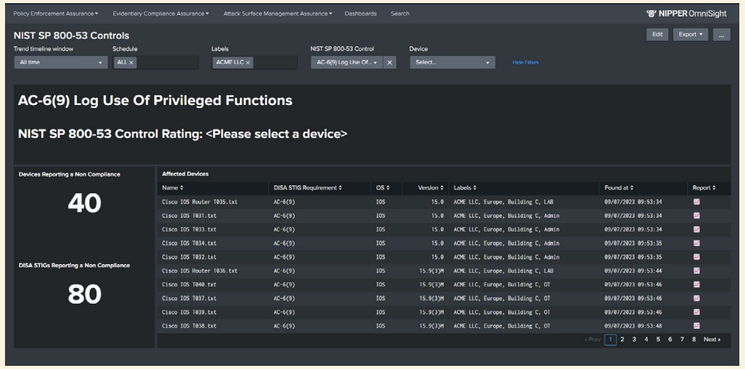
4. Continuous assurance

Innovation

- Nipper OmniSight provides immediate awareness of any device configuration changes, providing assurance that planned network changes have not created new vulnerabilities, as well as alerting network owners to any unplanned changes.

Benefit

- Effectively manage configuration drift with NIST SP 800-53 assessments of every router, switch and firewall, on an up-to-hourly basis with Nipper OmniSight.



5. Augmented compliance evidence

Innovation

- Nipper OmniSight leverages the precision of Nipper InfraSight assessments and applies a range of lenses through which to view - and improve - network security and compliance posture.

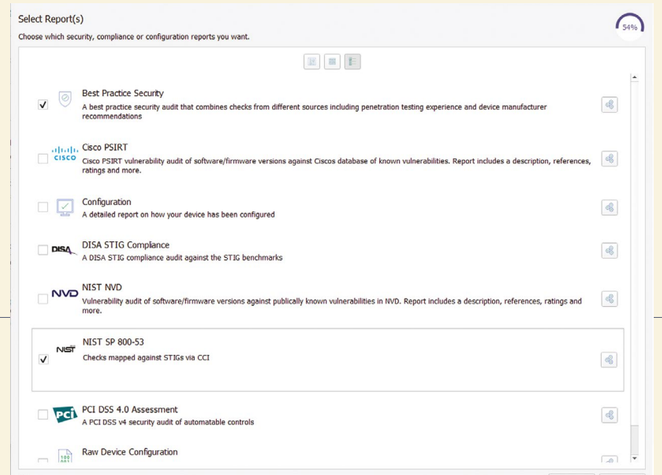
Benefit

- Drill down to a range of underlying Nipper reports (including Security Audit and STIG reports) to augment NIST SP 800-53 compliance evidence.

Whether you are a federal agency looking for continuous assurance, or non-federal organization that needs to evidence NIST SP 800-53 compliance, there is a Nipper solution for you.

On-demand security and compliance with Nipper InfraSight

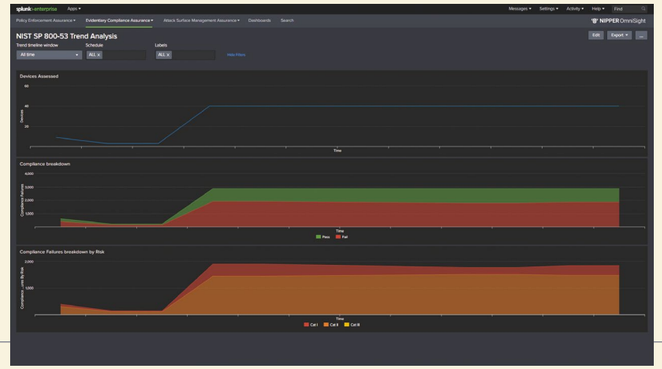
Auditors and external assessors choose Nipper InfraSight to quickly verify configurations are secure and/or meet regulatory compliance standards, reducing their audit times by up to 80%.



Nipper InfraSight interface showing NIST SP 800-53 report

Continuous security and compliance assurance with Nipper OmniSight

Deployed by SOCs to assure the security and compliance posture of network infrastructure, Nipper OmniSight also adds a transformative proactive security layer to the NOC tech stack. Nipper OmniSight integrates with SIEM, SOAR, GRC and trouble-ticketing solutions.



Splunk dashboard visualizing Nipper OmniSight's NIST SP 800-53 trend analysis

Request a demo to see for yourself how Nipper solutions will be of value to you. **titania.com/try/demo**

NIST SP 800-53 Compliance Report Highlights

Leaders in proactive security and compliance assurance for network infrastructure

Titania is a world leader in continuous configuration drift analysis for routers, switches and firewalls, helping NOCs and SOCs around the world build configuration confidence in their network infrastructure. Automating an inside-out view of security and compliance vulnerabilities across the network, Nipper solutions enable risk-prioritized remediation to shut down attack vectors that pose real-world threats to the enterprise. And now, for the first time, the solutions automate evidence-based NIST SP 800-53 compliance reporting against DoD Control Cyber Readiness Inspection (CCRI) and Cyber Operational Readiness Assessment (CORA) criteria.

Why Titania

Used by more than 30 federal agencies and throughout the US Department of Defense, for over 10 years elite cyber teams have complemented their vulnerability analysis with Titania's accurate network configuration software – Nipper InfraSight.

And now Nipper OmniSight extends this pentester-accurate automation to enable customers to establish a defendable network with continuous risk detection and remediation at scale.

USA
Suite 6500, 2451 Crystal Dr, 6th Floor,
Arlington, VA 22202

UK
167-169 Great Portland Street,
London, England, W1W 5PF

TITANIA
titania.com