

Assure CORA compliance by finding and fixing your exposure to critical threats

Close critical vulnerabilities and misconfigurations in routers, switches, firewalls and wireless access points before the Cyber Operational Readiness Assessment (CORA) assessors arrive, with Nipper Resilience, a standalone solution for assessing network configuration and pinpointing security risks.



Gain clear insights into device compliance posture, so you can prioritize fixes and track your progress in addressing Key Indicators of Risk (KIORs).



Designed for CORA – includes analysis against latest Security Technical Implementation Guide (STIG) releases



Rapid point-in-time assessment with device-specific insights



Standalone solution: analyze network config files on an offline laptop



Guides post-CORA remediation and can form the basis of ongoing security audits



Based on technology **trusted within the defense sector**

The CORA challenge

Since it was introduced in March 2024, CORA has changed the rules for how cyber readiness is assessed across the defense landscape. Instead of tick-list compliance, CORA challenges Department of Defense (DoD) organizations to focus on the highest risks: the mission-critical systems and most significant vulnerabilities, as determined by current threat intelligence and MITRE ATT&CK data at the time of each assessment.

Why you can't afford to fail

While the process has changed, the consequences of failing CORA are not the same as the old Command Cyber Readiness Inspection (CCRIs).

Responsible officers will be held to account, given a timescale for remediation and potentially face scrutiny by a Risk Review Board – as well as increased likelihood of repeat assessments.

Compliance aside, failing CORA indicates there are critical vulnerabilities and misconfigurations in your infrastructure that could be targeted by bad actors. In short, **every red flag on a CORA-style assessment is an issue that needs urgent resolution to protect your operations and missions.**




How Nipper Resilience can help

Nipper Resilience empowers your network team to identify misconfigurations and vulnerabilities and prioritize remedial actions, before you are assessed.

Working as a standalone solution that doesn't require direct connectivity to your devices or the Internet, Nipper Resilience analyzes config files for routers, switches, firewalls and wireless access points to pinpoint any non-compliance with the latest STIGs.

And it does it fast: audit times are typically reduced by 80%. Even if you have thousands of devices, you can get a comprehensive and actionable report within a matter of hours that **shows every KIOR on every device assessed.**

Take steps to address the issues, then re-run the analysis to confirm you've shut down the vulnerabilities – giving confidence ahead of CORA assessors arriving and (more importantly) before attackers can exploit them.



Audit times are
typically reduced by

80%



How it works

Nipper Resilience is designed to be straightforward to use for CORA assessment:

- 1 Download Nipper Resilience onto a laptop or local server.
- 2 Extract config files for each device to be assessed and store the files in a configuration repository. There's guidance at <https://docs.titania.com/device-guides> on how to do this for all major network device vendors.
- 3 Drag and drop the configuration files into Nipper Resilience.
- 4 Perform a one-off STIG assessment.
- 5 View visualizations of findings and access device-specific reports through the built-in dashboard.

View an instant picture of your current CORA status.





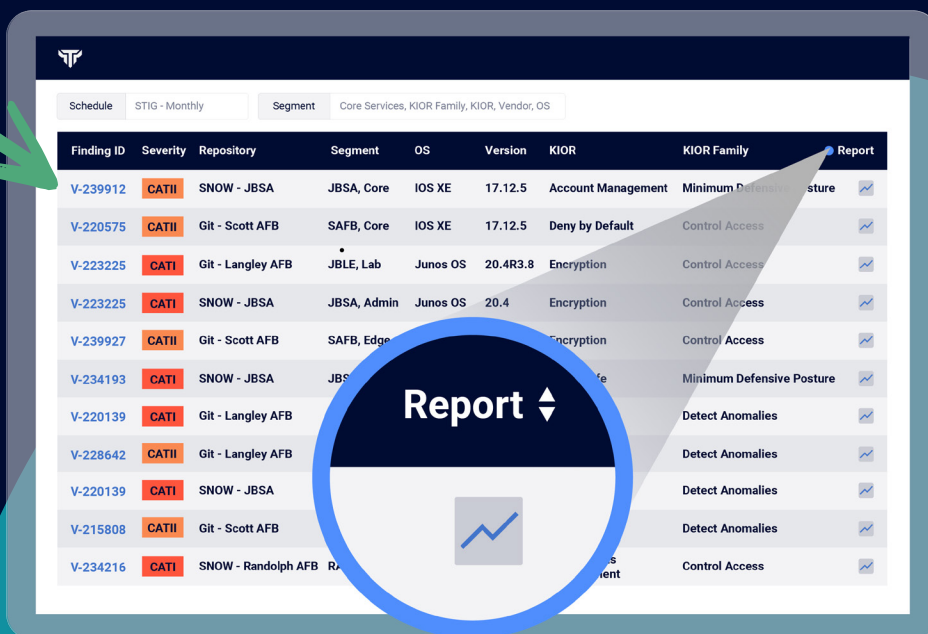
Gain insights into KIORs by severity, vendor, operating system or other categories.

View findings on either a device-by-device or issue-by-issue basis to understand whether there is a single misconfigured device or network-wide issue that needs a group response.

Schedule: STIG - Monthly Segment: Core Services, KIOR Family, KIOR, Vendor, OS							
Device	KIOR Score	KIORs	Repository	Segment	OS	Version	
JBSA-RTR-OT	3	Account Management, End of Life, Log Review	SNOW - JBSA	JBSA, OT	IOS XE	15.5(3)M	
JBSA-SW-CORE	2	Account Management, Deny by Default	SNOW - JBSA	JBSA, Core	ASA	17.12.5	
RAFB-RTR-OT	2	Encryption, Permissions Management	SNOW - Randolph AFB	RAFB, OT	Junos OS	20.4	
JBLE-RTR-EDGE	1	Account Management	Git - Langley AFB	JBLE, Edge	IOS XE	17.12.5	
JBLE-RTR-Lab	1	Deny by Default	Git - Langley AFB	JBLE, Lab	Junos OS	20.4R3.8	
SAFB-SW-CORE	1	Deny by Default	Git - Scott AFB	SAFB, Core	IOS XE	17.12.5	
JBSA-FW-ADMIN	1	Encryption	SNOW - JBSA	JBSA, Admin	FortiOS	7.6.3	
SAFB-FW-EDGE	1	Encryption	Git - Scott AFB	SAFB, Edge	ASA	9.20.3	
JBLE-FW-ADMIN	1	Log Review	Git - Langley AFB	JBLE, Admin	PAN-OS	11.2	
JBSA-RTR-EDGE	1	Log Review	SNOW - JBSA	JBSA, Edge	IOS XR	6.3.1	
SAFB-SW-CORE	1	Log Review	Git - Scott AFB	SAFB, Core	NX-OS	9.3	

Identify the actions required per device to support prioritization.

Once you have completed the recommended remediations, perform another assessment to confirm success.



The screenshot displays the Nipper Resilience dashboard. At the top, there are filters for 'Schedule' (STIG - Monthly) and 'Segment' (Core Services, KIOR Family, KIOR, Vendor, OS). Below the filters is a table with columns: Finding ID, Severity, Repository, Segment, OS, Version, KIOR, KIOR Family, and Report. A green arrow points to the 'Report' column header. A blue circle with the word 'Report' and a line graph icon is overlaid on the table. The table contains 12 rows of findings.

Finding ID	Severity	Repository	Segment	OS	Version	KIOR	KIOR Family	Report
V-239912	CATII	SNOW - JBSA	JBSA, Core	IOS XE	17.12.5	Account Management	Minimum Defensive Posture	
V-220575	CATII	Git - Scott AFB	SAFB, Core	IOS XE	17.12.5	Deny by Default	Control Access	
V-223225	CATI	Git - Langley AFB	JBLE, Lab	Junos OS	20.4R3.8	Encryption	Control Access	
V-223225	CATI	SNOW - JBSA	JBSA, Admin	Junos OS	20.4	Encryption	Control Access	
V-239927	CATII	Git - Scott AFB	SAFB, Edge			Encryption	Control Access	
V-234193	CATI	SNOW - JBSA	JBSA, Core				Minimum Defensive Posture	
V-220139	CATI	Git - Langley AFB					Detect Anomalies	
V-228642	CATII	Git - Langley AFB					Detect Anomalies	
V-220139	CATI	SNOW - JBSA					Detect Anomalies	
V-215808	CATII	Git - Scott AFB					Detect Anomalies	
V-234216	CATI	SNOW - Randolph AFB	RAFB, Core				Control Access	

A trusted solution for rapid deployment

Nipper Resilience is powered by Nipper, which has been granted authority to operate as part of the US Air Force's Cybersecurity Vulnerability Assessment / Hunt (CVA/H) weapon system and is used by a growing number of DoD cyber operators.

Operating without requiring a network connection, Nipper Resilience can be deployed swiftly and without risk. The vulnerability reports and dashboard are only visible locally to your team.

Seeing is believing

**We'd love to show you how Nipper Resilience works in practice.
Arrange a demo or speak to one of our experts.**

USA

2451 Crystal Dr, Suite 600
Arlington, VA 22202
enquiries@titania.com

UK

167-169 Great Portland Street,
London, England, W1W 5PF
enquiries@titania.com

About Nipper Resilience

The Nipper Resilience platform enables network security teams to proactively identify and fix critical vulnerabilities and misconfigurations in routers, switches, firewalls and wireless access points before attackers exploit them. It supports scheduled and continuous monitoring for up to 250,000 devices. Titania Nipper solutions are trusted by elite cybersecurity organizations and deployed across 100+ critical infrastructure providers, departments of defense, interior ministries and federal agencies globally, as well as major financial institutions, telecommunications providers, and leading oil and gas companies.

Find out more about our experience working with the military at
titania.com/solutions/industries/military