TITANIA NIPPER

NIPPER ENTERPRISE

NIST 800-53 Mapping Document

Accurately automate the assessment of up to 52 NIST 800-53 network controls

NIST 800-53 Mapping Document

Titania Nipper is trusted by the US DoD and civilian federal agencies to accurately automate network security and compliance assessments for firewalls, routers and switches against (i) trusted security benchmarks (e.g., DISA STIGs – NDM, RTR and VPN) and (ii) trusted control and risk management frameworks (e.g., NIST 800-53).

By virtually modelling device configurations as single entities to consider overlapping rules, Nipper achieves an accuracy advantage in detecting configuration drift that that is proven to reduce assessment times by up to 80% by not wasting time investigating false positives.

Nipper prioritizes vulnerabilities it identifies according to network criticality and provides remediation guidance, improving both the MTTD and MTTR. Additionally, Nipper's security and compliance reports provide evidence of both passes and failures.

Nipper Enterprise is capable of assessing the security and compliance posture of up to 250,000 network devices every day. Through integrations with (i) CMDBs/config repositories and (ii) with SIEMs/GRC platforms, Nipper Enterprise can provide evidence to support:

1. **DoD Control Cyber Readiness Inspection (CCRI)** assurance;
2. **Zero Trust** policy assurance, by evidencing (i) networks are segmented with deny all/permit by exception rules and (ii) devices are managed and compliant to IT security policies;
3. **Continuous RMF** and **Continuous Diagnostics and Mitigation (CDM) assurance;** and
4. **Attack Surface Management (ASM)** assurance**,** by using NIST/MITRE-approved mapping of NIST 800-53 controls onto 10 of the 11 MITRE ATT&CK Tactics for Network Infrastructure.

NIST 800-53 Mapping Document

Using DISA STIG Control Correlation Identifiers (CCIs), Nipper and Nipper Enterprise automate the accurate assessment of up to 37 NIST 800-53 controls. This can be extended up to 52 controls, across the following 12 control families, by leveraging Titania's existing NVD, Security Audit and SIEM reporting capabilities:

- Access Control – *see page 4*
- Audit & Accountability – *see page 5*
- Security Assessment & Authorization – *see page 6*
- Configuration Management – *see page 6*
- Contingency Planning – *see page 7*
- Identification & Authentication – *see page 7*
- Maintenance – *see page 8*
- Risk Assessment – *see page 8*
- System & Services Acquisition – *see page 9*
- System & Communications Protection – *see page 9*
- System & Information Integrity – *see page 10*
- Supply Chain Risk Management – *see page 10*

Access Control

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Check Automated with Nipper Audit	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Access Control (AC)	AC-2	Account Management	AC-2 (a)	AC-2 (4,7a)	STIG Audit	✓	✓	✓
	AC-4	Information Flow Enforcement		AC-4 (8,17)	STIG Audit		✓	✓
	AC-6	Least Privilege		AC-6 (9)	STIG Audit		✓	✓
	AC-7	Unsuccessful Logon Attempts	AC-7 (a)		STIG Audit	✓	✓	✓
	AC-8	System Use Notification	AC-8 (a)	AC-2 (4,7a)	STIG Audit	✓	✓	✓
	AC-10	Concurrent Session Control			STIG Audit			✓
	AC-11	Device Lock			Security Audit		✓	✓
	AC-12	Session Termination			STIG Audit		✓	✓
	AC-17	Remote Access		AC-17 (2)	STIG Audit	✓	✓	✓
	AC-18	Wireless Access	AC-18 (b)	AC-18 (1)	Security Audit	✓	✓	✓

Audit and Accountability

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Check Automated with Nipper Audit	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Audit & Accountability (AU)	AU-2	Event Logging	AU-2 (a,b,c)		Nipper + SIEM Integration	✓	✓	✓
	AU-3	Content Of Audit Records		AU-3 (1,3)	STIG Audit Nipper + SIEM Integration	✓	✓	✓
	AU-4	Audit Log Storage Capacity		AU-4 (1)	STIG Audit	✓	✓	✓
	AU-5	Response To Audit Logging Process Failures	AC-5 (a,b)	AU-5 (2,4)	STIG Audit	✓	✓	✓
	AU-6	Audit Record Review, Analysis, & Reporting	AC-6 (a,c)	AC-6 (1,3,4,5)	Nipper + SIEM Integration	✓	✓	✓
	AU-7	Audit Record Reduction & Report Generation			Nipper + SIEM Integration		✓	✓
	AU-8	Time Stamps	AC-8 (b)		STIG Audit	✓	✓	✓
	AU-9	Protection Of Audit Information		AC-17 (2)	STIG Audit	✓	✓	✓
	AU-10	Non-Repudiation			STIG Audit			✓
	AU-11	Audit Record Retention		AC-11 (1)	Nipper + SIEM Integration	✓	✓	✓
	AU-12	Audit Record Generation	AU-12 (a,b,c)	AC-12 (1,2)	STIG Audit	✓	✓	✓
	AU-14	Session Audit		AU-14(3)	STIG Audit Nipper + SIEM Integration			

Security Assessment & Authorization

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Check Automated with Nipper Audit	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Security Assessment & Authorization (CA)	CA-2	Security Assessments	CA-2 (d,e)	CA-2(2)	Security Audit	✓	✓	✓
	CA-7	Continuous Monitoring	CA-7 (c,e)	CA-7(3,4,6)	Nipper + SIEM Integration	✓	✓	✓

Configuration Management

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Check Automated with Nipper Audit	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Configuration Management (CM)	CM-2	Baseline Configuration	CM-2 (b)		Raw Change Tracking	✓	✓	✓
	CM-5	Access Restrictions For Change		CM-5 (6)	STIG Audit	✓	✓	✓
	CM-6	Configuration Settings	CM-6 (b)	CM-6 (1)	STIG Audit	✓	✓	✓
	CM-7	Least Functionality	CM-7 (a,b)		STIG Audit	✓	✓	✓
	CM-8	Information System Component Inventory		CM-8 (1)	Configuration Report	✓	✓	✓

Contingency Planning

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Check Automated with Nipper Audit	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Contingency Planning (CP)	CP-9	System Backup	CP-9(b)		STIG Audit	✓	✓	✓

Identification & Authentication

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Check Automated with Nipper Audit	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Identification & Authentication (IA)	IA-2	Identification & Authentication (Organizational Users)		IA-2 (8)	STIG Audit	✓	✓	✓
	IA-3	Device Identification & Authentication		IA-3 (1)	STIG Audit		✓	✓
	IA-5	Authenticator Management		IA-5 (1a,b,c),(2a,c)	STIG Audit	✓	✓	✓
	IA-7	Cryptographic Module Authentication			STIG Audit	✓	✓	✓
	IA-11	Re-Authentication			STIG Audit	✓	✓	✓

Maintenance

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Check Automated with Nipper Audit	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Maintenance (MA)	MA-4	Nonlocal Maintenance	MA-4 (e)	MA-4 (6)	STIG Audit	✓	✓	✓

Risk Assessment

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Check Automated with Nipper Audit	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Risk Assessment (RA)	RA-3	Risk Assessment	RA-3 (a)		Security Audit Vulnerability Audit	✓	✓	✓
	RA-5	Vulnerability Monitoring & Scanning	RA-5 (a,b,c,f)	RA-5 (2,3,5,6,8,10)	Nipper + SIEM Integration	✓	✓	✓

System & Services Acquisition

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Check Automated with Nipper Audit	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
System & Services Acquisition (SA)	SA-4	Acquisition Process		SA-4 (5)	Security Audit STIG Audit SIEM Integration			✓

System & Communications Protection

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Check Automated with Nipper Audit	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
System & Communications Protection (SC)	SC-5	Denial-Of-Service Protection		SC-5 (2)	STIG Audit	✓	✓	✓
	SC-7	Boundary Protection	SC-7 (a)	SC-7 (5,11)	STIG Audit	✓	✓	✓
	SC-10	Network Disconnect			STIG Audit		✓	✓
	SC-13	Cryptographic Protection			STIG Audit	✓	✓	✓
	SC-17	Public Key Infrastructure Certificates			STIG Audit		✓	✓
	SC-23	Session Authenticity		SC-23 (3)	STIG Audit		✓	✓
	SC-45	System Time Synchronization		SC-45(1,2)	Security Audit			

System & Information Integrity

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Check Automated with Nipper Audit	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
System & Information Integrity (SI)	SI-2	Flaw Remediation	SI-2 (c)		STIG Audit	✓	✓	✓
	SI-4	System Monitoring	SI-4 (d,e)	SI-4 (2,3,5,16,17)	STIG Audit Nipper + SIEM Integration	✓	✓	✓
	SI-5	Security Alerts, Advisories, & Directives		SI-5(1)	Nipper + SIEM Integration	✓	✓	✓
	SI-11	Error Handling	SI-11(b)		STIG Audit		✓	✓
	SI-13	Predictable Failure Prevention		SI-13 (4b)	STIG Audit			

Supply Chain Risk Management

Control Family	Control #	Control	Main Control Supported	Control Enhancement	Check Automated with Nipper Audit	Low Impact Information Systems	Moderate Impact Information Systems	High Impact Information Systems
Supply Chain Risk Management (SR)	SR-6	Supplier Assessments & Reviews		SR-6 (1)	Vulnerability Audit		✓	✓

TITANIA NIPPER

NIPPER ENTERPRISE

Get a live demo of Nipper Enterprise

titania.com/try/demo/nipper-enterprise

Get in touch to arrange a demonstration of Titania's continuous accurate and evidentiary NIST 800-53 compliance assurance reporting to meet your continuous RMF and CDM compliance requirements for network infrastructure.

+44 (0) 1905 888785 | enquiries@titania.com

Titania, Security House, Barbourne Road, Worcester, WR1 1RS

Titania, Suite 426, 2011 Crystal Dr, Crystal City, Arlington, VA 22202

January 2023