IP FABRIC

NIST ANALYSIS

Report Introduction

The **NIST Cybersecurity Framework (CSF) v2.0** is a comprehensive and flexible framework designed to help organizations of all sizes and sectors manage and reduce cybersecurity risks. It is structured around six core functions:

GV: Govern

ID: Identify

PR: Protect

DE: Detect

RS: Respond

RC: Recover

which collectively provide a taxonomy of high-level cybersecurity outcomes. These functions guide organizations in understanding their current cybersecurity posture, identifying gaps, prioritizing actions, and improving risk management practices. The framework emphasizes governance and strategic alignment with organizational objectives, while being adaptable to unique risks, technologies, and missions. It also integrates with other standards and frameworks, making it a globally recognized tool for enhancing cybersecurity resilience.

Relationship Between NIST CSF v2.0 and NIST 800-53

NIST 800-53: Provides a catalog of security and privacy controls specifically for federal information systems. It is a detailed, prescriptive framework aimed at ensuring the confidentiality, integrity, and availability of federal systems.

Organizations can use **NIST 800-53** controls to implement the outcomes defined in the CSF core functions. For example, the CSF provides high-level guidance on managing risks, while NIST 800-53 offers specific technical controls to achieve those outcomes

Feature	NIST CSF v2.0	NIST SP 800-53
Purpose	High-level guidance for managing risks	Technical controls for secure federal systems
Applicability	Flexible; voluntary for most organizations	Mandatory for federal agencies
Focus	Risk management and governance	Prescriptive security controls
Integration	Maps outcomes to other frameworks like 800-53	Provides technical implementation details
Governance Emphasis	Strategic alignment with business goals	Operational security measures

IP Fabric assists organizations in aligning with the NIST CSF v2.0 by leveraging its platform's 160+ default intent checks (and many more custom checks!) to immediately identify risks and issues across network and cloud infrastructures. Through automated discovery, intent-based verification, and real-time analysis, IP Fabric enables organizations to rapidly assess basic compliance with many of the NIST CSF's core functions.

Snapshot Data Summary

IP Fabric URL	https://marketing.ipf.cx/api/v7.0/
IP Fabric Version	7.2.7+0
Snapshot Name	Day 1
Snapshot ID	97ad7c58-341a-4e93-9612-8dd259d41672
Network sites/groups	4
Network devices	25

1 Device Inventory Breakdown by Site

Sites (14)	Ratio (%)	Device Count
0X	6.45%	6
1X	12.9%	12
2X	3.23%	3
3X	12.9%	12
4X	9.68%	9
5X	4.3%	4
6X	5.38%	5
AWS:418295684712/eu-central-1	2.15%	2
AWS:418295684712/eu-west-1	5.38%	5
AWS:418295684712/eu-west-3	4.3%	4
AWS:890561831523/eu-central-1	17.2%	16
AWS:890561831523/eu-west-1	9.68%	9
AWS:890561831523/eu-west-3	5.38%	5
unknown	1.08%	1

Total Device Count: 93

Ref: NIST ID.AM Identify.Asset Management

2 Devices with Telnet Protocol Enabled

Device Name	Site	Login IP	Additional Login Type	Version	Uptime (secs)
s5xr01	5X	10.194.56.108	ssh	15.6(2)T	3960
s5xr02	5X	10.194.56.109	ssh	15.6(2)T	3960
d3xr02	3X	10.194.56.87	ssh	15.6(2)T	4260
s5xr05	5X	10.194.56.112	ssh	15.6(2)T	3960
d1xr02	1X	10.194.56.70	ssh	15.6(2)T	4620
d1xr01	1X	10.194.56.69	ssh	15.6(2)T	4620
d3xr01	3X	10.194.56.86	ssh	15.6(2)T	4260
d5xr01	5X	10.194.56.107	ssh	15.6(2)T	3900
d4xr02	4X	10.194.56.98	ssh	15.6(2)T	3900
d4xr01	4X	10.194.56.97	ssh	15.6(2)T	3960

Total Device Count: 10

Ref: NIST PR.DS Protect.Data Security