censys

Censys for Compliance

NIST 2.0 Cybersecurity Framework

The NIST Cybersecurity Framework (CSF), particularly its latest release, NIST CSF 2.0, sets the standard for robust cybersecurity programs. It underscores the importance for organizations of all sizes and industries to manage and mitigate cybersecurity risks proactively, enhancing security posture against advanced threats. The framework extends responsibility for an organization's security across all levels, from executives to practitioners, and is organized into six core functions for clear understanding by a diverse audience.

- **Identify** - Establishes a foundation for an effective cybersecurity program by understanding managing risks to systems, people, assets, data, and capabilities.
- **Protect** - Focuses on implementing appropriate safeguards to ensure delivery of critical services, encompassing aspects like access control and data security.
- **Detect** - Involves the development and implementation of appropriate activities to identify the occurrence of a cybersecurity event promptly.
- **Respond** - Addresses how to take action during or after the detection of a cybersecurity incident, including response planning and communications.
- **Recover** - Involves developing and implementing activities to restore any capabilities or services impaired due to a cybersecurity incident.
- **Govern** - Newly added in CSF 2.0, this function emphasizes the importance of governance in managing cybersecurity risk, encompassing policies, processes, and strategies.

Effectively applying the NIST CSF's six functions is crucial for strengthening cybersecurity defenses. These functions should be addressed simultaneously, ensuring continuous and concurrent activities that support: Identify, Protect, Detect, and Govern, while maintaining readiness for Respond and Recover functions in case of incidents.

Although the NIST CSF does not specify exact outcomes or methods, a thorough understanding of the framework, coupled with appropriate tools and technologies, is essential. The Censys Internet Intelligence Platform provides the necessary support and capabilities to effectively implement and enhance the NIST CSF.

See details on the categories Censys supports below:

Function	Category	How Censys Helps
Govern (GV)	**Cybersecurity Supply Chain Risk Management (GV.SC):** Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders	Censys streamlines the assessment of supply chain partners or 3rd party vendors effortlessly with no deployment or configuration required.
		Censys continuously crawls internet data sources such as Certificate Transparency (CT) logs, passive DNS sinks, and internet scans to uncover assets that you own. So you can understand your critical exposures and mitigate risks, while embedding best practice monitoring into your security operations.
Identity (ID)	**Asset Management (ID.AM):** Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy	Censys helps organizations understand what external-facing assets (Hosts, Certificates, Web Entities, Domains, Storage Buckets, and Software) belong to their organization. Censys also provides information on exposed ports, services, and protocols in addition to many other pertinent facts about the discovered assets so an organization can understand their risks associated with these systems.
	Risk Assessment (ID.RA): The cybersecurity risk to the organization, assets, and individuals is understood by the organization	Censys identifies and provides valuable context on risks associated with cloud misconfiguration, device exposure, evidence of compromise, information leakage, name infrastructure or service misconfiguration, service or interface exposure, software or web app security vulnerabilities, and exposed services, ports, protocols, and instances of end of life (EOL) software.
Protect (PR)	**Platform Security (PR.PS):** The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability	Censys protects your organization's digital footprint with a comprehensive profile of all internet facing assets to continuously monitor for unauthorized services, matching more than 1,433 software fingerprints and identifying end-of-life (EOL) software versions.
	Technology Infrastructure Resilience (PR.IR): Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience	Censys provides the most comprehensive and up-to-date visibility of hosts and services on the global internet, discovering 65% more attack surface than leading competitors. This allows security teams to efficiently track changes within their network, thoroughly investigate risks, and proactively respond to emerging threats.

Function	Category	How Censys Helps
Detect (DE)	**Continuous Monitoring (DE.CM):** Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events	Censys conducts daily comprehensive scans of the top 100+ ports with proprietary machine-learning based discovery across all 65k ports, discovering services six times faster than the nearest competitor. With daily refreshes on all 3b+ services in our dataset, we significantly reduce false positives for precise asset monitoring.
	Adverse Event Analysis (DE.AE): Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents	Censys Integrations and mature API enable organizations to send event data downstream to correlate new asset discovery and risk identification with other security event sources.
Respond (RS)	**Incident Management (RS.MA):** Responses to detected cybersecurity incidents are managed	Censys automates the assessment of each asset against 400+ risk fingerprints, facilitating the determination of severity based on impact, exploitability, and likelihood, offering precise remediation guidance and detailed insights into recommended mitigation steps.
	Incident Mitigation (RS.MI): Activities are performed to prevent expansion of an event and mitigate its effects	Censys enables organizations to quickly prioritize, remediate, and rescan on-demand to validate the risk has been mitigated or to accept a risk with documented business reason.