At-A-Glance

Enable the Cybersecurity Conversation

Security conversations should happen at all levels of an organization. But what happens when cybersecurity professionals and senior leadership don't speak the same language?

The NIST Cybersecurity Framework can help facilitate this communication. NIST says one of its most frequently cited benefits is that it provides a common cyber risk management language that allows more efficient discussions to take place—up, down, and across an agency's management structure, with auditors, or between supply chain partners.*

It's also being used as a basis for security-oriented discussions and decision-making in corporate boardrooms, the C-Suite, and among line managers and staff with cyber responsibilities.

Learn more about the NIST Cybersecurity Framework.

**Newsletter Update on the Cybersecurity Framework,* NIST, July 1, 2015

Cisco Cybersecurity for Federal Agencies

Today's dynamic cyber threat landscape raises the stakes for defenders to ensure the confidentiality, availability, and integrity of today's sensitive information and mission-critical data. Sophisticated attacks and massive data breaches happen almost every day. How can federal agencies and organizations approach security differently?

Adopt a Threat-Centric Approach to Security

Traditional defenses that rely exclusively on detection and blocking for protection are no longer adequate. A new security approach is needed that covers the entire attack continuum—before, during, and after the attack. The new cybersecurity best-practices framework from the National Institute of Standards and Technology (NIST) shows agencies and organizations of all sizes how to apply such a model.

The Problem

Managing Cybersecurity Risk

From the largest government agencies to the smallest, nearly every federal organization struggles with cost-effective cybersecurity risk management against the backdrop of today's advanced threats, the shortage of skilled cybersecurity talent, and countless compliance regulations and security mandates.

The Solution

NIST Cybersecurity Framework

It's a simple, best-practices approach to cybersecurity that leverages the specific standards that are already working well throughout the world today. It includes five core functions that improve overall cybersecurity risk management and provide a common language with which to discuss cybersecurity risk both internally and externally.

NIST Cybersecurity Framework Core Functions

Identify	Protect	Detect	Respond	Recover

The Cybersecurity Framework has five core functions that provide the set of activities, desired outcomes, and applicable references that are common and working well across all sectors today.

© 2015 Cisco and/or its affiliates. All rights reserved.

At-A-Glance

What Is NIST?

The National Institute of Standards and Technology (NIST) is part of the U.S. Department of Commerce. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology across a broad spectrum of subject areas.* Its IT projects and programs include the Cybersecurity Framework, and the Computer Security Resource Center, among others.

* Source: http://www.nist.gov/public_affairs/general_information.cfm

Why Cisco?

Cisco Enables Framework Adoption

Cisco communicates cybersecurity risk management and related solutions in the NIST Framework context, enabling all federal organizations to adopt the Framework and improve their cybersecurity profiles. Our threat-centric security model addresses the entire attack continuum: before, during, and after an attack.

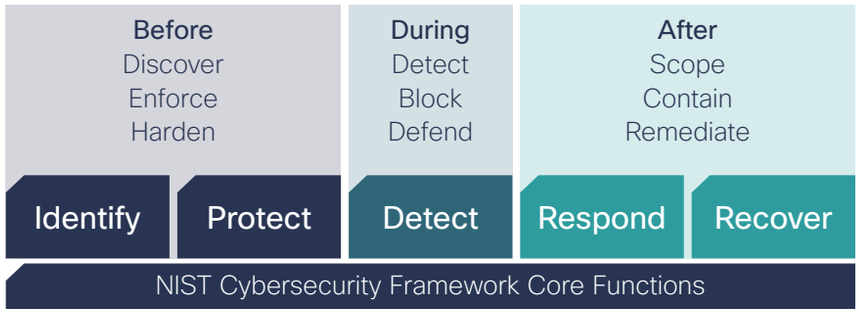
Cisco Threat-Centric Security Model Alignment with NIST Cybersecurity Framework

The Cisco® threat-centric security model includes three phases that align with the NIST Cybersecurity Framework five core functions (Figure 1). The first Cisco phase—before—includes the capabilities necessary to discover (NIST Identify function) what's on the network because it can be difficult to protect what you don't know you have. This phase also includes the essential capabilities to enforce and harden (NIST Protect function) your mission-critical systems and sensitive information.

The next phase's—during—capabilities detect, block, and defend against an attack once it is already underway (NIST Detect function).

Our last phase—after—includes capabilities that scope the extent of the breach or attack and contain the damage to minimize impact (NIST Respond function). Lastly, our approach includes essential remediate capabilities to quickly restore operations, recover from the attack, and prevent recurrence in the future (NIST Recover function).

Figure 1: How the Cisco Threat-Centric Security Approach Aligns with NIST Cybersecurity Framework



More Information

Learn about today's cybersecurity challenge in the Cisco Security Report at cisco.com/go/securityreport

Get more information on the NIST Cybersecurity Framework at nist.gov/cyberframework

Discover the Cisco threat-centric security model at cisco.com/go/security

© 2015 Cisco and/or its affiliates. All rights reserved.