ManageEngine
AD360

The NIST Cybersecurity Framework:

5 core functions and how to align with them

www.manageengine.com/active-directory-360/

Table of contents

What is the **NIST Cybersecurity** Framework?

The National Institute of Science and Technology (NIST) Cybersecurity Framework (CSF) is a security framework that helps organizations manage their cybersecurity risks by assessing and improving their abilities to prevent, detect, and respond to cybersecurity incidents. Many organizations around the world and across different industries have adopted the NIST CSF and made their cybersecurity more resilient.

The **five core functions** of the NIST CSF

The NIST CSF is organized into five core functions as below:

- **Identify (ID**) - What processes and assets need protection?
- **Protect (PR)** - What safeguards are available?
- **Detect (DE)** - What techniques can be used to identify incidents?
- **Respond (RS)** - What techniques can be used to contain impacts of incidents?
- **Recover (RC)** - What techniques can restore capabilities?

In the following sections, we will look at what these core functions are and how AD360, a web-based identity and access management (IAM) solution, can help you adhere to them.

1. Identify (ID)

What the NIST says:

> *Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.*

How can AD360 help?

AD360's reports offer administrators a thorough overview of their Active Directory, Exchange server, and Office 365 environments. With over 1000 pre-configured reports, they can increase the visibility of the activities performed within their IT infrastructure. These reports give IT administrators actionable insights on their environments, helping them identify their vulnerable areas and prioritize their security efforts accordingly.

2.

Protect
(PR)

What the NIST says:

> *Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.*

How can AD360 help?

In a Windows environment, Active Directory serves as the identity and access governance system and controls the resource and data access for all critical Windows infrastructure. Ensuring the safety of your AD user accounts could go a long way in securing your AD infrastructure as they act as the basis of authentication and initial access to your network. AD360 adds an extra layer of security with MFA for Windows, macOS, and Linux logons along with various applications by forcing users to establish their identity through various authentication methods such as Google Authenticator, Duo Security, biometrics and more, in addition to using their login credentials. AD360 also ensures data confidentiality by empowering IT administrators to enforce the principle of least privilege (PoLP). Using AD360, IT administrators can safeguard their business critical data by giving users only the bare minimum access required. This significantly reduces the possibilities of data leaks.

3. Detect (DE)

What the NIST says:

> *Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event*

How can AD360 help?

Using AD360's real-time change auditing and alerting feature for on-premises AD and Azure AD, you can identify cybersecurity incidents at their early stages, helping you identify cybersecurity attacks at their early stages, helping you to contain them and thereby reduce the damage. For instance, say a disgruntled employee attempts to steal proprietary data to sell it to a competitor, and hence accesses an unusual amount of documents. Using user behavior analytics (UBA), AD360 can spot this abnormality and trigger an alert to the administrator in real-time.

4. Respond (RS)

What the NIST says:

> *Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.*

How can AD360 help?

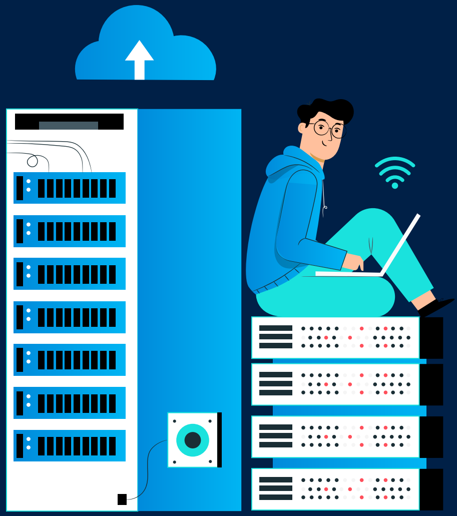
Using AD360 you can configure automatic workflows (execution of batch files) that tries to mitigate the suspicious security incident.

For example, when multiple login attempts are made to log into an AD user account during non-business hours, it indicates that the account might be on the verge of being compromised and hence, need immediate attention. In such cases, you can configure the tool to instantly respond with counter-measures— in this case, disabling the AD user account under attack.

This way you can effectively automate responses to cybersecurity events, and can therefore remediate, contain, and recover quickly.

5.

Recover (RC)



What the NIST says:

> *Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event*

How can AD360 help?

AD360 takes care of all your AD, Exchange Server, and Office 365 backup and recovery needs. Using AD360, you can back up all of your AD objects and restore them either partially or completely; back up and restore all items in your Exchange Online tenant and Exchange server; back up Office 365 files, folders, sites, etc., and perform item-level or attribute-level restorations to any previous version effortlessly.

Conclusion

These five functions are further separated into 22 categories and then divided into 98 subcategories. Aligning with all these categories is no easy task. However, aligning with the fundamental core functions of the NIST CSF is a great place to start and can help organizations significantly improve their cyber resilience.