National Institute of Standards and Technology’s (NIST) Framework

Lepide Data Security Platform

On February 12, 2014, the National Institute of Standards and Technology (NIST) released the first version of their Framework for Improving Critical Infrastructure Cybersecurity. The Framework was created as a collaboration between technology experts and governmental bodies to collect and standardize guidelines and best practices for the protection of critical infrastructure. By implement the NIST Framework organizations can manage cybersecurity-related risk to their critical infrastructure and data.

Whilst going through this mapping guide, bear in mind that the Framework is an overall structure that can be addressed by different security standards, including NIST 800-53, NIST 800-171, ISO 270001 and more.

Mapping Lepide Data Security Platform to the NIST Framework

The following table is an explanation of how you can use the Lepide Data Security Platform to reduce risk to security and protect your critical infrastructure:

NIST Framework	Description	Lepide DSP
	ID.AM-3: Organizational communication and data flows are mapped	Lepide shows all directory and file share contents mapping users to data and vice versa.
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	Lepide allows you to classify data based on the contents, the associated risk, business value and sensitivity.
Identify: Business Environment The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.		Lepide allows you to implement proper access controls and ensure that users have access to only the data and systems they need to perform their job roles. Understand the data in your systems to help govern access.

Identify: Governance The policies, procedures, and processes to manage and monitor the organization’s regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.		Use Lepide to help govern access to your most sensitive data and identify where the areas of risk are as they arise. Spot excessive permissions and implement a policy of least privilege.
Identity: Risk Assessment The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals		Using Lepide you can reduce the risk to your critical assets by implementing a zero-trust policy.
Identity: Risk Management Strategy The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	Using Lepide, you can spot risks to your critical infrastructure (file systems, Active Directory, SharePoint and more) quickly and easily.
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	
	ID.RM-3: The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	Spot data that is over-exposed (such as through open shares) as well as users with excessive permissions.
Protect: Access Control Access to assets and associated	PR.AC-1: Identities and credentials are managed for authorized devices and users	Lepide helps manage access controls by providing visibility over

facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.		who has access to what and when permissions are changed.
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Lepide helps organizations implement least privilege by detecting excessive permissions, permission changes and more.
Protect: Awareness and Training The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.		Lepide offer professional services to help ensure that Lepide solutions are being used to their full security potential. Lepide also provides a range of datasheets, documentation, guides and blogs to educate and inform.
Protect: Data Security Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-1: Data-at-rest is protected	Ensure that your sensitive data remains confidential and unpublished by classifying data within your systems, determining who has access and monitoring anomalous user behavior. Lepide can also ensure the success and ease of audits and demonstrate the effectiveness of security through audit trails, detailed reporting and an interactive search.

	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	Using Lepide, you can identify stale data, inactive users/groups and other key identifiers of data in need of management/deletion.
Protect: Information Protection Processes and Procedures Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	Lepide provides real time alerts whenever permissions are changed, or users receive excessive permissions. Lepide establishes a baseline for normal user behavior and can alert users when behavior deviates from the norm.
Protect: Maintenance Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Lepide provides users with the ability to carry out a full data entitlement review. Report on user current permissions to data, and compare with historical permissions to spot over-exposed data.
Protect: Protective Technology Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	The pre-defined reports and real time alerts in Lepide help organizations to identify the use of privileged access accounts and ensure the appropriate segregation of duties. Lepide can be configured to alert users whenever elevated accounts have been used or when permissions escalate.

Detect: Anomalies and Events Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Lepide helps you to detect anomalous events that may be indicative of data breaches. Real time monitoring and alerting of file activity, permission changes and changes to critical infrastructure, enable you to detect potential data breaches as they happen. Our anomaly spotting technology measures user behavior and sends real time alerts when user behavior is deemed to be anomalous (even spotting single point anomalies).
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	
	DE.AE-4: Impact of events is determined	
	DE.AE-5: Incident alert thresholds are established	
Detect: Security Continuous Monitoring The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events	Lepide can be used in a variety of different ways to help identify and respond to cybersecurity events. For example, Lepide can be used to detect and react to ransomware through threshold alerting. Some ransomware strains, like WannaCry, work by changing file extensions. So, using Lepide, you can spot whenever there are large numbers of file modifications over a small period of time. Upon detection of this threat, you can execute a script to shut it down.
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	
	DE.CM-4: Malicious code is detected	
	DE.CM-5: Unauthorized mobile code is detected	
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	

	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	There are hundreds of use cases for Lepide, including insider threats, ransomware, data breaches, malware and data leakage. Contact Lepide for more information on how to address these threats.
	DE.CM-8: Vulnerability scans are performed	
Respond: Communications Response activities are coordinated with internal and external stakeholders, as appropriate, to include external	RS.CO-2: Events are reported consistent with established criteria	Lepide provides detailed pre-defined reports on a number of security issues, including file activity, user activity, permissions and more.

If you would like more information about how Lepide Data Security Platform can be used to implement and adhere to the NIST Cybersecurity Framework, contact our team:

support@lepide.com

+1(0)-800-814-0578

Alternatively, if you would like to see our solution in action, schedule a demo with one of our engineers: https://www.lepide.com/demorequest.html