Lepide

Mapping the Lepide Data Security Platform to **NIST Cybersecurity Framework (CSF)**

Key Activity	Control Text	Technology Alignment
Access Control	ID.AM-4: External information systems are catalogued. ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value. PR.AC-1: Identities and credentials are managed for authorized devices and users PR.AC-3: Remote access is managed PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	Lepide Identify (Data Discovery and Classification) Lepide Trust (Access Governance) Lepide Insight (User and Entity Behavioural Analytics)
Logging, Monitoring and Alerting	PR.DS-4: Adequate capacity to ensure availability is maintained PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy DE.CM-1: The network is monitored to detect potential cybersecurity events DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events 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 DE.DP-2: Detection activities comply with all applicable requirements DE.DP-4: Event detection information is communicated to appropriate parties	Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)

Key Activity	Control Text	Technology Alignment
Logging, Monitoring and Alerting (continued)	DE.DP-5: Detection processes are continuously improved RS.AN-1: Notifications from detection systems are investigated	Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)
Systems Security	PR.DS-5: Protections against data leaks are implemented PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained PR.IP-3: Configuration change control processes are in place PR.PT-4: Communications and control networks are protected DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)
Incident Response	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed 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 RS.RP-1: Response plan is executed during or after an event RS.CO-2: Events are reported consistent with established criteria RS.CO-3: Information is shared consistent with response plans RS.AN-2: The impact of the incident is understood	Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)

Key Activity	Control Text	Technology Alignment
Incident Response (continued)	RS.AN-3: Forensics are performed RS.AN-4: Incidents are categorized consistent with response plans RS.MI-1: Incidents are contained RS.MI-2: Incidents are mitigated RS.IM-1: Response plans incorporate lessons learned RS.IM-2: Response strategies are updated RC.RP-1: Recovery plan is executed during or after an event RC.IM-1: Recovery plans incorporate lessons learned RC.IM-2: Recovery strategies are updated RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)
Risk Analysis and Management	ID.RA-1: Asset vulnerabilities are identified and documented ID.RA-3: Threats, both internal and external, are identified and documented ID.RA-4: Potential business impacts and likelihoods are identified ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties PR.IP-12: A vulnerability management plan is developed and implemented RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	Lepide Identify (Data Discovery and Classification) Lepide Trust (Access Governance) Lepide Insight (User and Entity Behavioural Analytics) Lepide Detect (Threat Detection and Response)

Lepide Data Security Platform

Core Capabilities

Lepide Identify

(Data Discovery and Classification)

- Discover and classify data in real-time.
- Tag data.
- Data valuation.
- Identify data most at risk.

Lepide Trust

(Access Governance)

- Analyse permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Change permissions.

Lepide Insight

(User and Entity Behavior Analytics)

- View interactions with data.
- View interactions with systems governing access to data.
- Employee audit logs.
- Investigate incidents and breach scenarios.

Lepide Detect

(Threat Detection and Response)

- Detect threats in real-time.
- Baseline/profile employee behaviour.
- Identify anomalous employee behaviour.
- Alert and respond to threats in real-time.

Start a free trial

Get a demo

Get a free risk assessment