Lepide

Datasheet

CJIS Compliance

CJIS Compliance

CJIS applies to any organization that receives information from or submits information to FBI CJIS systems or services. Failing a CJIS audit can be incredibly costly, including, in some cases, federal criminal penalties. Lepide Data Security Platform can help you avoid this.

Find Exposed CJI Data

Discover and classify criminal justice information so that you can spot over-exposed, at risk, data.

Govern Access to CJIS Data

Discover and classify criminal justice information so that you can spot over-exposed, at risk, data.

Detect Threats to CJI Data

Analyze user behavior, spot anomalies and detect/react to threats to the security of CJI data.

Prepare your organization for a Criminal justice Information Services (CJIS) audit with Lepide. Lepide Data Security Platform is a complete CJIS compliance audit solution, providing numerous pre-defined audit reports to help your organization avoid non-compliance fines.

4.2.2.

Proper Access, Use, and Dissemination of NCIC Restricted Files Information

4.2.4.

Storage

4.3.

Personally Identifiable Information (PII)

5.3.1

Reporting Security Events

5.3.2.1.

Incident Handling

5.3.2.2

Collection of Evidence

5.3.4

Incident Monitoring

Criminal Justice Information and PII

This section essentially deals with ensuring that you can properly identify where your CJI and PII is located and that you are applying the appropriate access controls.

With Lepide, you can scan your on-premise and cloud data stores for PII and CJI, see who has access to it, get alerts when permissions and configurations change, and revoke excessive permissions where appropriate.

Incident Response

In this section, Lepide is able to provide the level of visibility, reporting, alerting and automated response actions to ensure you are covered.

Anomaly spotting, threshold alerting, and threat models ensure that you are able to detect potential security threats and incidents in real time.

Once potential incidents are spotted, Lepide can execute custom threat responses to ensure that you can shut down the potential threat. Pre-defined reports can also be generated to help with collection of evidence and threat investigations.

Auditing and Accountability

The two main ways that Lepide helps you to address this section of CJIS is through access controls and detailed change auditing.

Lepide helps you determine who has access to which sensitive data and you can even report on which of your users have excessive permissions and revoke those permissions from within the solution itself. This will help you ensure that only the appropriate users have access to sensitive or covered data.

Lepide also provides detailed auditing of events and content and allows you to analyze user behavior and generate pre-defined audit reports. The Lepide audit reports come complete with all key audit information for compliance requirements, including who, what, when and where details – all accessible from one, easy-to-view window.

5.4.1.
Auditable Events and Content

5.4.2.
Response to Audit Process Failures

5.4.3.
Audit Monitoring, Analysis and Reporting

5.4.5.
Protection of Audit Information

5.4.6.
Audit Record Retention

Access Control

Lepide helps govern access to sensitive data by implementing least privilege. Easily identify users with excessive permissions and revoke access from within the solution.

Get real time alerts and pre-defined reports on all permission and configuration changes, as well as successful and unsuccessful login attempts.

5.5.1.
Account Management

5.5.2.
Access Enforcement

5.5.3.
Unsuccessful Login Attempts

5.12.2.

Personnel Termination

Personnel Security

Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI.

With Lepide, you can easily see what that user had access to, and how that access was granted, so you can easily revoke all permissions to CJI and PII.