HongKe 虹科

数据表
符合 CJIS 标准

CJIS合规

CJIS适用于从FBI CJIS系统或服务接收信息或向其提交信息的任何组织。没有通过CJIS的审计可能会付出难以置信的代价，在某些情况下，包括联邦刑事处罚。leide数据安全平台可以帮助您避免这种情况。

找到暴露的CJI数据

发现和分类刑事司法信息，以便您可以发现过度暴露，处于危险中的数据。

管理对CJIS数据的访问

发现和分类刑事司法信息，以便您可以发现过度暴露，处于危险中的数据。

检测威胁到CJI数据

分析用户行为，发现异常，检测/应对CJI数据安全威胁。

准备您的组织为刑事司法信息服务(CJIS)审计与莱德。

Leide数据安全平台是一个完整的CJIS合规性审计解决方案，提供大量预定义的审计报告，以帮助您的组织避免违规罚款。

4.2.2.
正确的访问，使用和传播
NCIC限制文件信息

4.2.4.
存储

4.3.
个人身份资料(PII)

5.3.1
报告安全事件

5.3.2.1.
事件处理

5.3.2.2
证据收集

5.3.4
事件监控

刑事司法信息和个人信息

本节主要处理确保您能够正确识别CJI和PII所在的位置，以及您正在应用适当的访问控制。

使用leide，您可以扫描本地和云数据存储中的PII和CJI，查看谁有权访问它，在权限和配置更改时获得警报，并在适当的时候撤销过多的权限。

事件响应

在本节中，leide能够提供可见性、报告、警报和自动响应操作的级别，以确保您得到覆盖。

异常发现、阈值警报和威胁模型确保您能够实时检测潜在的安全威胁和事件。

一旦发现潜在的事件，leide可以执行自定义的威胁响应，以确保您可以关闭潜在的威胁。还可以生成预定义的报告，以帮助收集证据和调查威胁。

审计及问责

Lepide帮助您解决这部分CJIS的两种主要方法是通过访问控制和详细的变更审计

Lepide可以帮助您确定谁可以访问哪些敏感数据，您甚至可以报告哪些用户拥有过多的权限，并从解决方案本身撤销这些权限。这将帮助您确保只有适当的用户才能访问敏感或覆盖的数据。

Lepide还提供对事件和内容的详细审计，并允许您分析用户行为并生成预定义的审计报告。leide审计报告包含所有符合合规性要求的关键审计信息，包括人员、内容、时间和地点的详细信息——所有这些都可以从一个易于查看的窗口访问。

访问控制

Lepide通过实现最小特权来帮助管理对敏感数据的访问。轻松识别具有过多权限的用户，并从解决方案中撤销访问权限。

获取所有权限和配置更改的实时警报和预定义报告，以及成功和不成功的登录尝试

5.4.1.
可审计的事件和内容

5.4.2.
对审计过程失败的响应

5.4.3.
审计监控、分析和报告

5.4.5.
审计信息的保护

5.4.6.
审计记录保留

5.5.1.
账户管理

5.5.2.
访问执行

5.5.3.
登录失败

5.12.2.

人员终止

人员的安全

接口机构解聘人员后，该机构应立即终止与CJI有联系的当地代理系统的访问。

使用Lepide, 您可以很容易地看到该用户拥有哪些访问权限，以及如何授予该访问权限，因此您可以很容易地撤销对CJI和PII的所有权限。

HongKe 虹科

虹科电子科技有限公司

www.haocst.com
network@hkaco.com

广州市黄埔区开泰大道30号佳都PCI科技园6号楼1-7层

T (+86) 400 - 999 - 3848
M (+86) 135 3349 1614

各分部：广州 | 成都 | 上海 | 苏州 | 西安 | 北京 | 台湾 | 香港 | 日本 | 韩国 | 美国硅谷

版本：V1.0 - 23/09/10

联系我们　获取更多资料　haocst.com