HongKe 虹科

启用指南

使用 LEPIDE 用于

防止数据泄露

Table of Contents

1. 导言 3
2. 针对数据泄露调整 Lepide 3
3. Lepide 核心能力 6
   3.1. - Lepide 识别 6
   3.2. - Lepide 信任 7
   3.3. - Lepide 审计 8
   3.4. - Lepide 检测 9
4. 支持 10
5. 商标 10

1. 导言

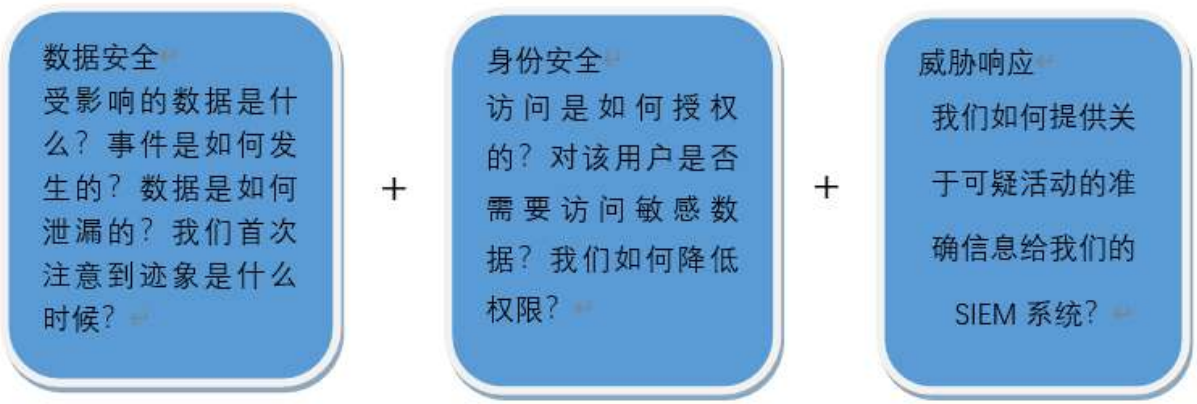
数据泄露是指敏感数据、受保护数据或机密数据被未经授权的人复制、传输、查看、窃取或使用的安全违规行为，即无意或不适当地泄露公司数据。

2021 年，有 5,250 起经确认的数据泄露报告，但这可能只占总数的 10%，因为大多数数据泄露都没有报告。数据泄露平均会给企业带来 460 万美元的罚款，更不用说对声誉或品牌造成的无形损害。

许多数据泄露都是可以预防的，与其他安全供应商相比，Lepide 这样的解决方案使企业能够更快地采取措施预防 、检测和应对数据泄露。

2. 针对数据泄露调整 Lepide

要确保数据安全、识别和应对数据泄露，您需要能够回答一些关键问题。



questions: 在下表中，我们将 Lepide 技术与这些问题进行了对比：

类别	应采取的行动	实施技术
数据安全	确定哪些敏感数据受到事件或漏洞的影响	文件服务器报告中的所有修改 (Lepide 审计) 文件重命名报告 (Lepide 审计) 读取失败报告 (Lepide 审计)

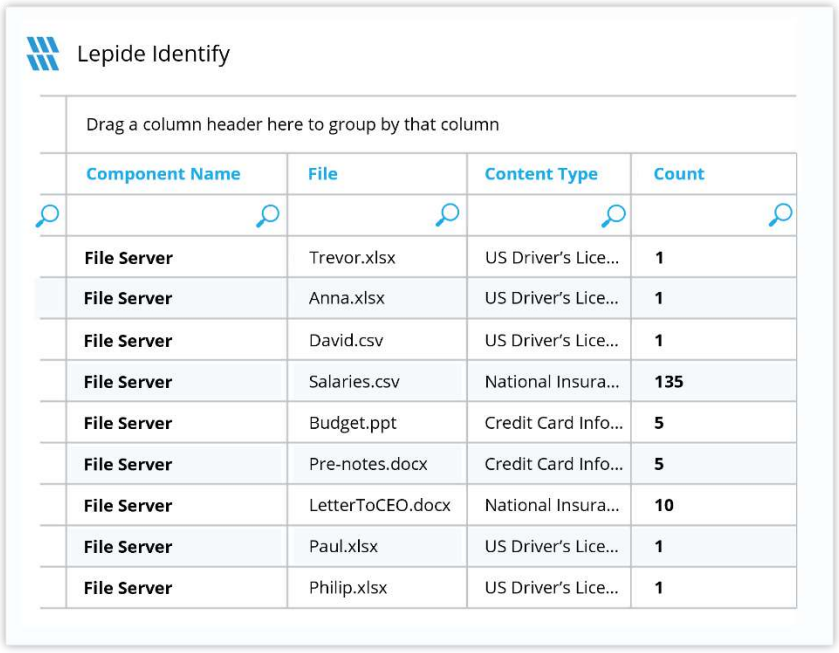
		所有环境变化报告 (Lepide 审计) 敏感数据分类 (Lepide 识别)
	确定数据是如何共享或泄露的	外部数据共享0365报告 (Lepide 审计) 文件复制报告(Lepide 审计) 机密邮件报告 (Lepide 审计) 非所有者访问邮箱报告 (Lepide 审计)
	发现可能导致漏洞的事件的第一个迹象	文件服务器报告中的所有修改 (Lepide 审计) 异常检测(Lepide 检测) 任何威胁模型触发 (Lepide 检测)
	确定事件是如何开始以及如何传播的	文件服务器报告中的所有修改 (Lepide 审计) 潜在勒索软件攻击威胁模型 (Lepide 检测) 文件重命名报告 (Lepide 审计) 读取失败报告 (Lepide 审计) 所有权限修改报告 (Lepide 信任)
身份安全	确定入侵源是如何获得访问权限的	所有环境变化报告 (Lepide 识别) 用户权限报告 (Lepide 信任)

	减少对敏感数据的权限，以减少泄露的影响	非活跃用户报告 (Lepide 审计) 用户过度权限报告 (Lepide 信任) 用户权限报告 (Lepide 信任) 用户管理权限报告 (Lepide 信任) 公开股票报告 (Lepide 信任 数据分类 (Lepide 识别)
	确定哪些用户在事件中受到了损害。看看他们还能接触到什么	权限按对象报告 (Lepide 信任) 用户权限报告 (Lepide 信任)
	确定数据泄露是由于人为错误、用户帐户受损还是恶意员工造成的	文件服务器报告中的所有修改 (Lepide 审计) 用户权限报告 (Lepide 信任)
响应	向SIEM提供有关可疑活动的准确信息	SIEM集成 (Lepide 检测)

3. Lepide 核心能力

3.1. - Lepide 识别

在创建时自动扫描、发现数据并进行分类，帮助您随时掌握敏感数据的位置。利用近距离扫描技术消除误报。与大多数分类解决方案相比，这有助于进一步提高准确性。根据合规性、风险、发生率、货币价值等因素对数据进行分类和评分，随时掌握最敏感的数据。

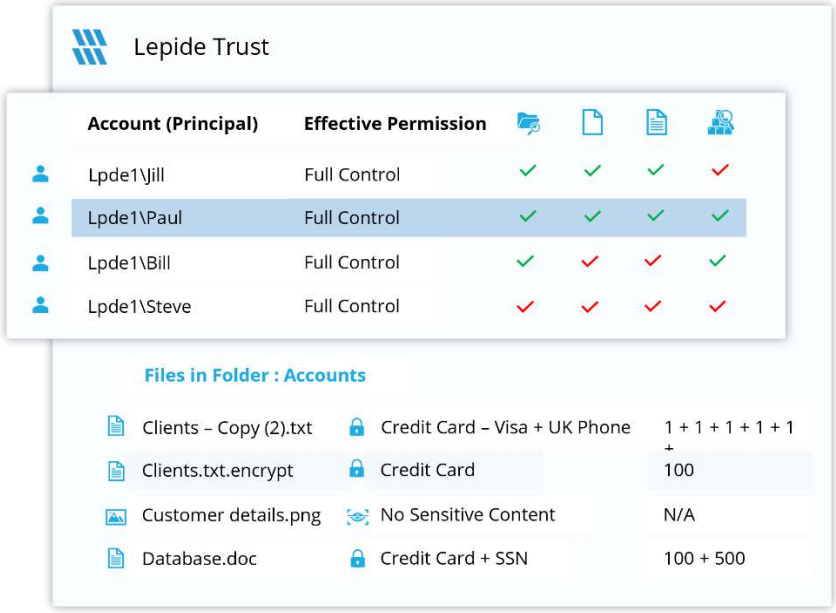


总之:

- 在真实 Tag 数据中发现数据并对其进行分类。
- 数据估值。
- 识别风险最大的数据。

3.2. - Lepide 信任

报告谁可以访问最敏感的数据，以及他们是如何被授予访问权限的。针对权限过大的用户的特定报告能让你发现哪些用户最有可能成为内部威胁。在权限发生变化时及时发现并逆转，从而维护零信任策略。

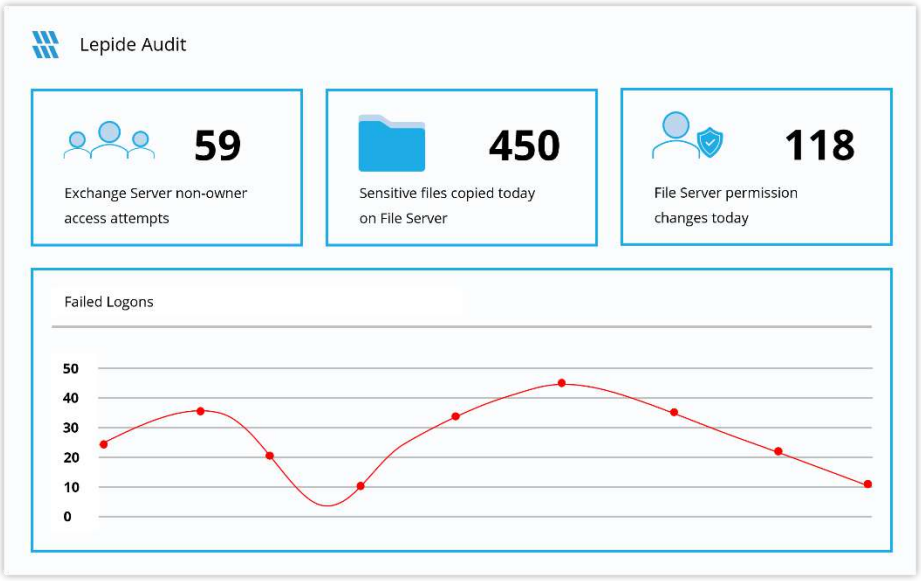


总之:

- 分析权限。
- 识别权限过大的员工（权限最小）。
- 查看历史许可。
- 跟踪权限更改。

3.3. - Lepide 审计

对敏感数据和混合环境所做的更改进行审计、报告和警报。回滚不需要的更改并恢复已删除的对象，以维护系统的完整性。跟踪用户对关键文件和文件夹所做的任何更改和修改。

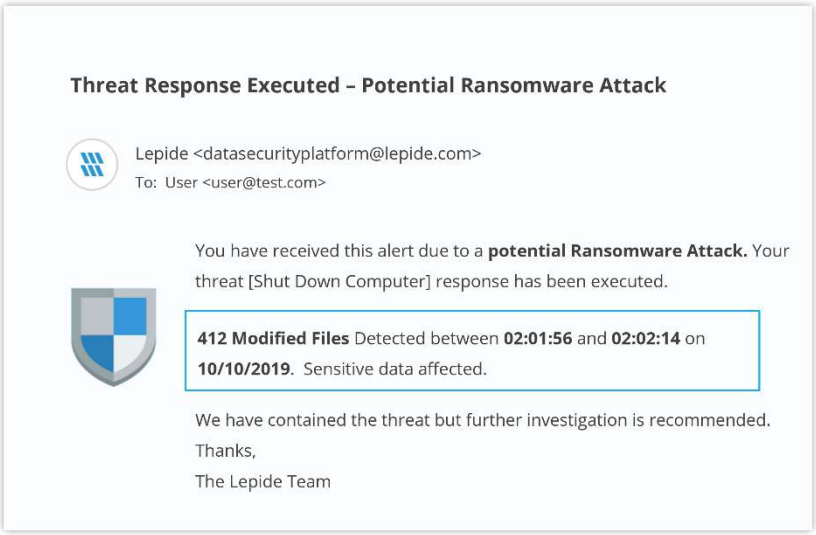


总之:

- 查看与数据的交互。
- 查看与管理数据访问的系统之间的互动。
- 员工审计日志。
- 调查事故和违规情况。

3.4. - Lepide 检测

机器学习支持的异常点发现技术可让您确定用户何时成为内部威胁。针对特定数据安全威胁定制的数百种威胁模型可在数据安全受到威胁时生成实时警报。可触发自动威胁响应，执行威胁缓解措施，如关闭受影响的计算机或服务器。



总之:

- 利用预定义的威胁模型实时检测威胁。
- 员工行为基准/档案。
- 识别异常员工行为。
- 实 时警报并应对威胁。

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 - 23/09/07

联系我们

获取更多资料

haocst.com