HongKe 虹科

启用指南

# 启用LEPIDE为

# 防范内部威胁

# 目录

# 1. 导言

威胁检测仍然是当今企业面临的巨大挑战--黑客敏捷、快速、聪明。当我们在这里使用威胁一词时，我们指的是恶意软件或某种形式的外部暴力攻击。尽管许多 "传统 "供应商声称威胁检测率很高，但没有一家安全供应商能 100% 检测到威胁，只要有一个威胁被攻破，整个网络就会受到攻击。

大多数安全供应商对活动目录和 Windows 文件系统的内部运作知之甚少或一无所知，这限制了他们在检测和调查企业网络中传播的威胁时的价值。

99% 的安全威胁都会利用活动目录作为其在网络中传播的手段，如果黑客的目的是窃取、泄漏或以某种方式限制对企业数据的访问，大多数安全供应商在这方面几乎不提供任何背景信息。大多数安全供应商无法提供任何有关 敏感数据或受威胁影响的数据的背景信息，这使得调查工作影响较小、速度较慢且效率较低。

# 2. 针对内部威胁调整 Lepide

要检测、预防、调查和应对威胁，您需要能够回答一些关键问题。

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 |
| --- | --- | --- |
| 检测 | 检测员工是否做出了违反常规的行为 | 所有环境变化报告 (Lepide 审计)<br>异常发现 (Lepide 检测)<br>大规模删除行为(OU)威胁模型 (Lepide 检测)<br>海量删除行为(用户)威胁模型 (Lepide 检测) |

| | | |
|---|---|---|
| | | 海量删除行为(计算机)威胁模型 (Lepide 检测)<br>批量删除行为(组)威胁模型 (Lepide 检测)<br>大量删除行为(FS)模型 (Lepide 检测)<br>海量数据复制威胁模式 (Lepide 检测)<br>潜在数据泄漏威胁模型 (Lepide 检测)<br>潜在业务中断威胁模型 (Lepide 检测)<br>权限升级(组)威胁模型 (Lepide 检测)<br>权限升级(文件)威胁模型 (Lepide 检测)<br>权限升级(文件夹)威胁模型 (Lepide 检测)<br>潜在密码威胁模型 (Lepide 检测) |
| | 检测是否存在可能是受损用户帐户症状的操作 | 所有环境变化报告 (Lepide 审计)<br>异常发现 (Lepide 检测)<br>按用户报表划分权限 (Lepide 信任)<br>任何威胁模型 (Lepide 检测) |

| | | |
|---|---|---|
| | | 权限升级(组)威胁模型 (Lepide 检测)<br>权限升级(文件)威胁模式 (Lepide 检测)<br>权限升级(文件夹)威胁模型 (Lepide 检测)<br>按用户报告的过多权限 (Lepide 信任)<br>具有管理权限的用户报告 (Lepide 信任)<br>权限修改报告 (Lepide 信任)<br>Active Directory安全组修改报告 (Lepide 信任)<br>Azure AD的组修改报告 (Lepide 信任)<br>历史权限报表 (Lepide 信任)<br>所有组策略修改报告 (Lepide 信任)<br>按邮箱报告的交换权限 (Lepide 信任) |
| | 确定何时复制敏感数据 | 文件复制报告 (Lepide 审计)<br>海量数据复制(FS)威胁模型 (Lepide 检测)<br>文件服务器报告中的所有修改 (Lepide 审计)<br>敏感数据分类 (Lepide 识别) |

| | | |
|---|---|---|
| | 确保Active Directory管理员没有进行可能导致风险的更改 | Active Directory报告中的所有修改(Lepide 审计)<br>Active Directory权限修改报告(Lepide 信任)<br>所有组策略修改报告(Lepide 信任)<br>所有环境变化报告(Lepide 审计)<br>触发任何威胁模型(Lepide 检测) |
| | 查看敏感数据何时通过电子邮件，OneDrive, MS Teams共享 | 外部数据共享O365报表(Lepide 审计)<br>实时警报(Lepide 检测)<br>文档修改报告(Lepide 审计)<br>所有邮箱访问报表(Lepide 审计)<br>潜在数据泄漏威胁模型(Lepide 检测) |
| 调查 | 在一个简单的报告中查看员工正在移动、修改和访问哪些数据 | 所有环境变化报告(Lepide 审计) |
| | 回答人力资源团队关于员工如何处理数据的要求 | 所有环境变化报告(Lepide 审计)<br>权限过高报告(Lepide 信任)<br>按用户报表划分权限(Lepide 信任)<br>具有管理员权限的用户报告(Lepide 信任)<br>公开资源报告 (Lepide 信任) |

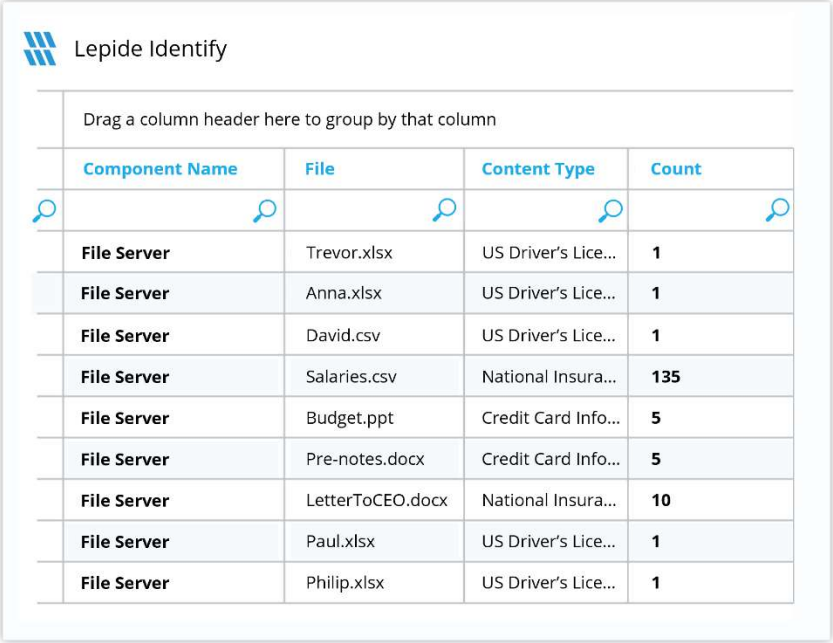
| | | |
|---|---|---|
| | | 数据分类 (Lepide 识别)<br>文件服务器修改报表 (Lepide 审计)<br>SharePoint在线修改报表 (Lepide 审计)<br>OneDrive修改报告 (Lepide 审计)<br>MS团队修改报告 (Lepide 审计)<br>外部数据共享O365报表 (Lepide 审计)<br>非所有者访问邮箱报告 (Lepide 审计) |
| | 确定特定员工一直在处理的数据以及他们对这些数据做了什么 | 所有环境变化报告 (Lepide 审计)<br>按用户报表划分权限 (Lepide 信任)<br>具有管理员权限的用户报告 (Lepide 信任)<br>公开资源报告 (Lepide 信任)<br>数据分类 (Lepide 识别)<br>文件服务器修改报表 (Lepide 审计)<br>SharePoint在线修改报表 (Lepide 审计)<br>OneDrive修改报告 (Lepide 审计)<br>MS团队修改报告 (Lepide 审计)<br>外部数据共享O365报表 (Lepide 审计) |

| | | |
|---|---|---|
| | | 非所有者访问邮箱报告 (Lepide 审计) |
| 预防 | 减少员工可以访问的敏感数据量，以降低风险 | 非活跃用户报告 (Lepide 审计)<br>按用户划分的过度权限报告 (Lepide 信任)<br>按对象报告的过度权限 (Lepide 信任)<br>P按用户报表划分权限 (Lepide 信任)<br>具有管理员权限的用户报告 (Lepide 信任)<br>公开资源报告 (Lepide 信任)<br>数据分类 (Lepide 识别)<br>增加威胁表面积威胁模型 (Lepide 检测)<br>权限升级(组)威胁模型 (Lepide 检测)<br>权限升级(文件)威胁模型 (Lepide 检测)<br>权限升级(文件夹)威胁模型 (Lepide 检测) |
| 响应 | 应对内部威胁 | 触发任何威胁模型 (Lepide 检测) |

# 3. Lepide 核心能力

## 3.1. - Lepide Identify

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。

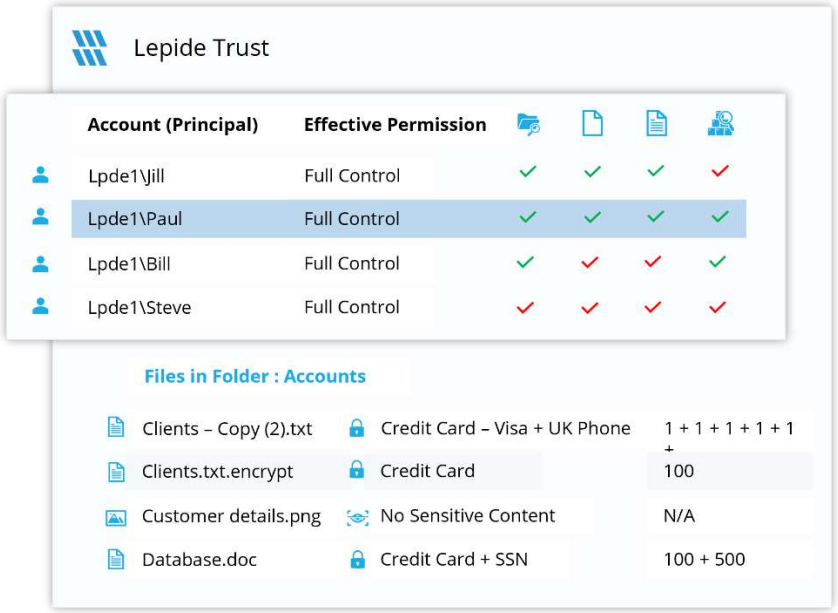



**总之：**

- 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。

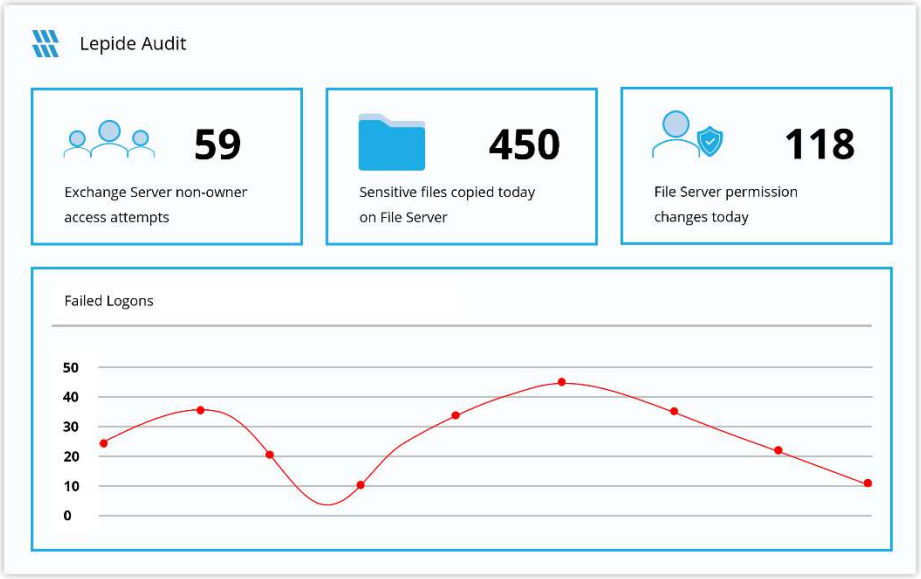



**总之：**

- 分析权限。
- 识别特权过大的员工（最小特权）。
- 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。

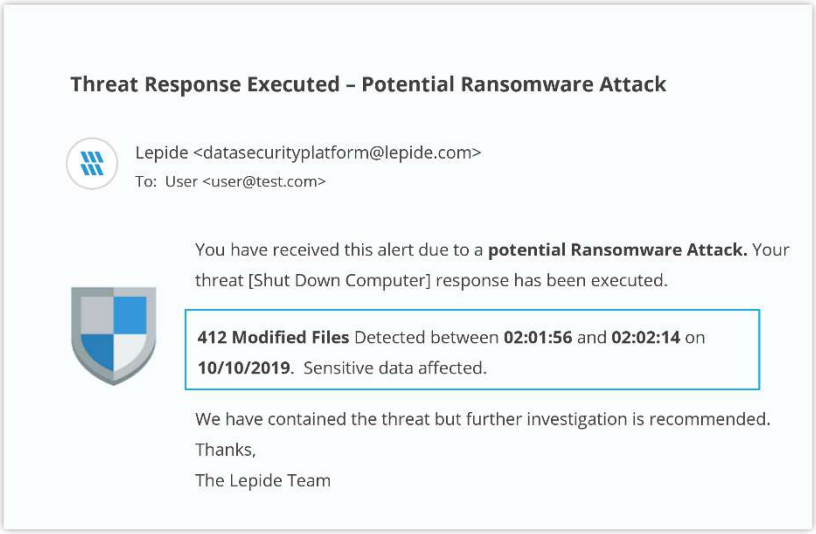



**总之：**

- 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。
- 实时预警和应对威胁。

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