Lepide 如何检测含有敏感数据的电子邮件已被发送

Lepide 如何检测含有敏感数据的电子邮件已被发送
- 概述
- 交换服务器
- Lepide解决方案
- 潜在数据泄漏威胁模型
- 先决条件机密邮件报告
- 先决条件运行机密邮件报告过滤报表

概述

数据泄露对任何组织都是一个严重的威胁，需要采取措施将其发生的风险降至最低。Lepide的重点是为您的数据提供可见性，通过可见性，您可以采取必要的措施来降低风险并保持合规。

交换服务器

电子邮件是几乎所有类型的组织中所有业务流程的基本元素，Exchange Server是用于与同事、客户和合作伙伴联系以制定业务决策和共享信息的标准。

然而，电子邮件数据的机密性和完整性是安全策略的基本要素，与Active Directory和Windows Server一样至关重要。

了解Exchange Server上正在发生的活动是确保数据安全并保持合规的关键。一旦发现敏感数据被不当共享，就会触发警报，并立即采取措施来降低风险并减少进一步的损害。

但是，如果没有合适的解决方案，跟踪发送的内容、发送者以及发送时间可能是一项复杂的任务。

Lepide解决方案

Lepide数据安全平台通过潜在数据泄漏威胁模型和分类电子邮件报告为这种复杂性提供了解决方案。

一旦敏感数据通过电子邮件发送，威胁模型就会触发警报。该报告提供了所有包含敏感数据的电子邮件的详细信息。

潜在数据泄漏威胁模型

配置后，当敏感数据泄露或通过电子邮件交换与其他用户共享时，潜在数据泄漏威胁模型将生成警报。

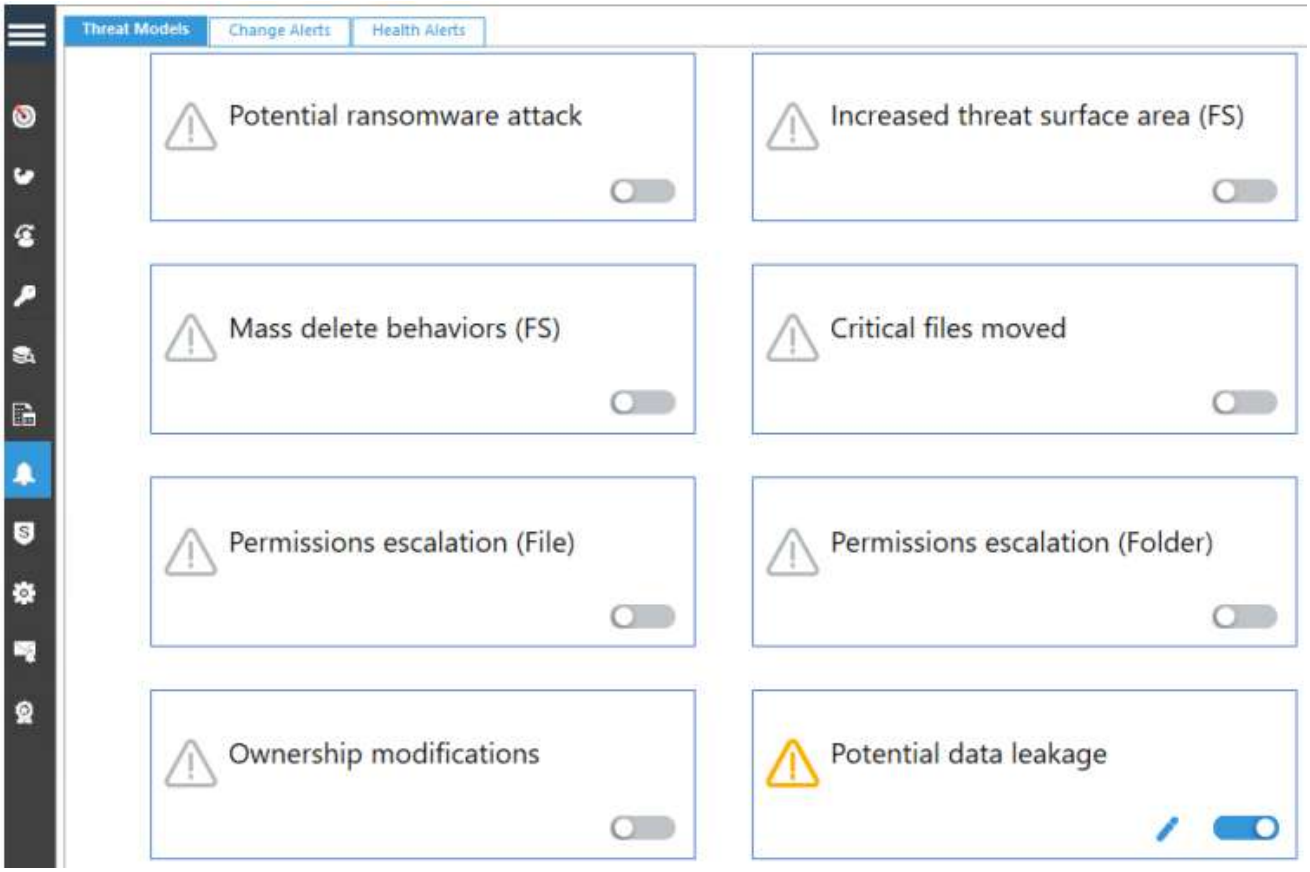
先决条件

在配置潜在数据泄漏威胁模型之前，您需要为Exchange Online配置数据发现和分类，并选择On the Fly分类。有关如何做到这一点的说明，请参阅我们的数据发现和分类配置指南。

建立潜在资料外泄威胁模型：

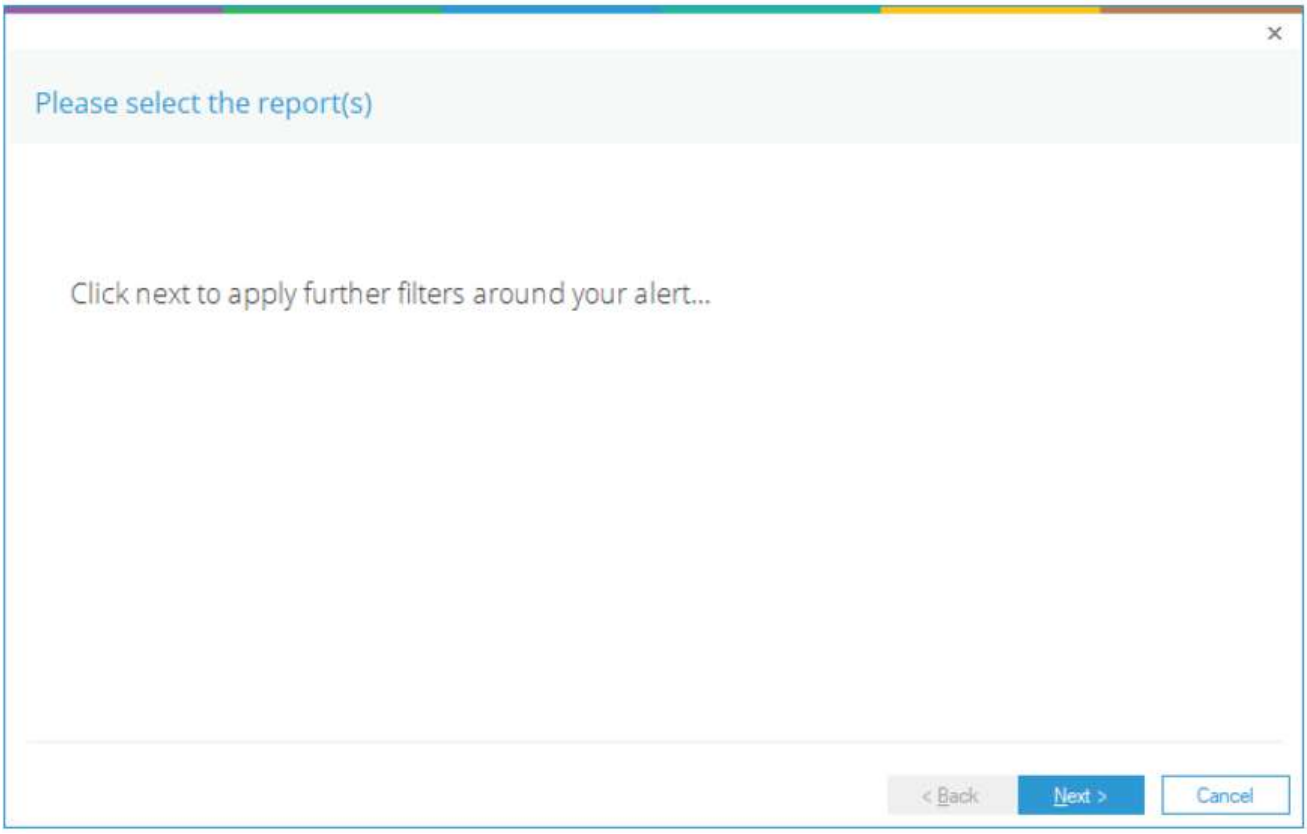
• 单击左侧工具栏中的警报图标，显示所有可用的威胁模型。

• 若要启用潜在数据泄漏威胁模型，请向右移动滑动开关，如下所示：

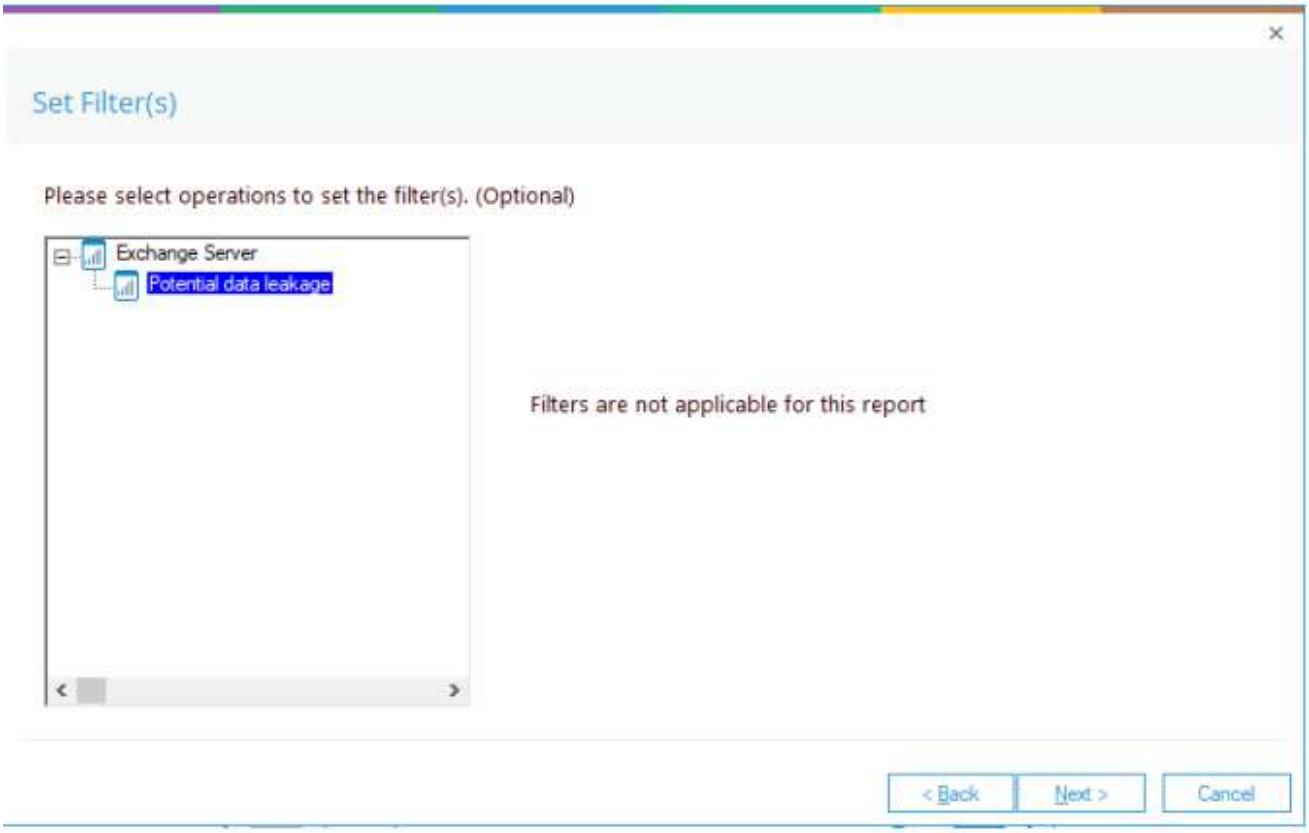


• 单击图标以配置所需的警报和响应。

这将启动一个向导：

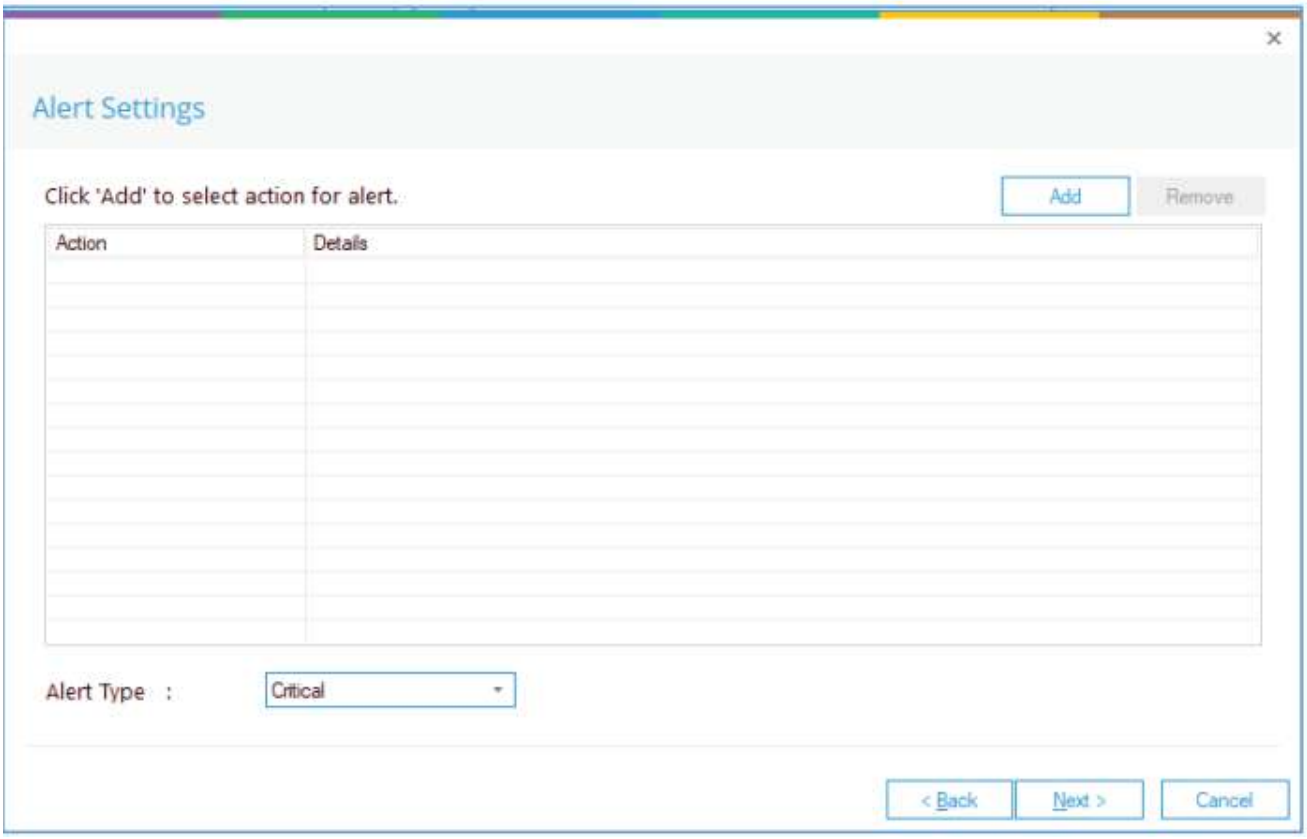


• 单击Next以显示Set Filter(s)对话框：



• 此报告不需要过滤器，因此单击Next继续。

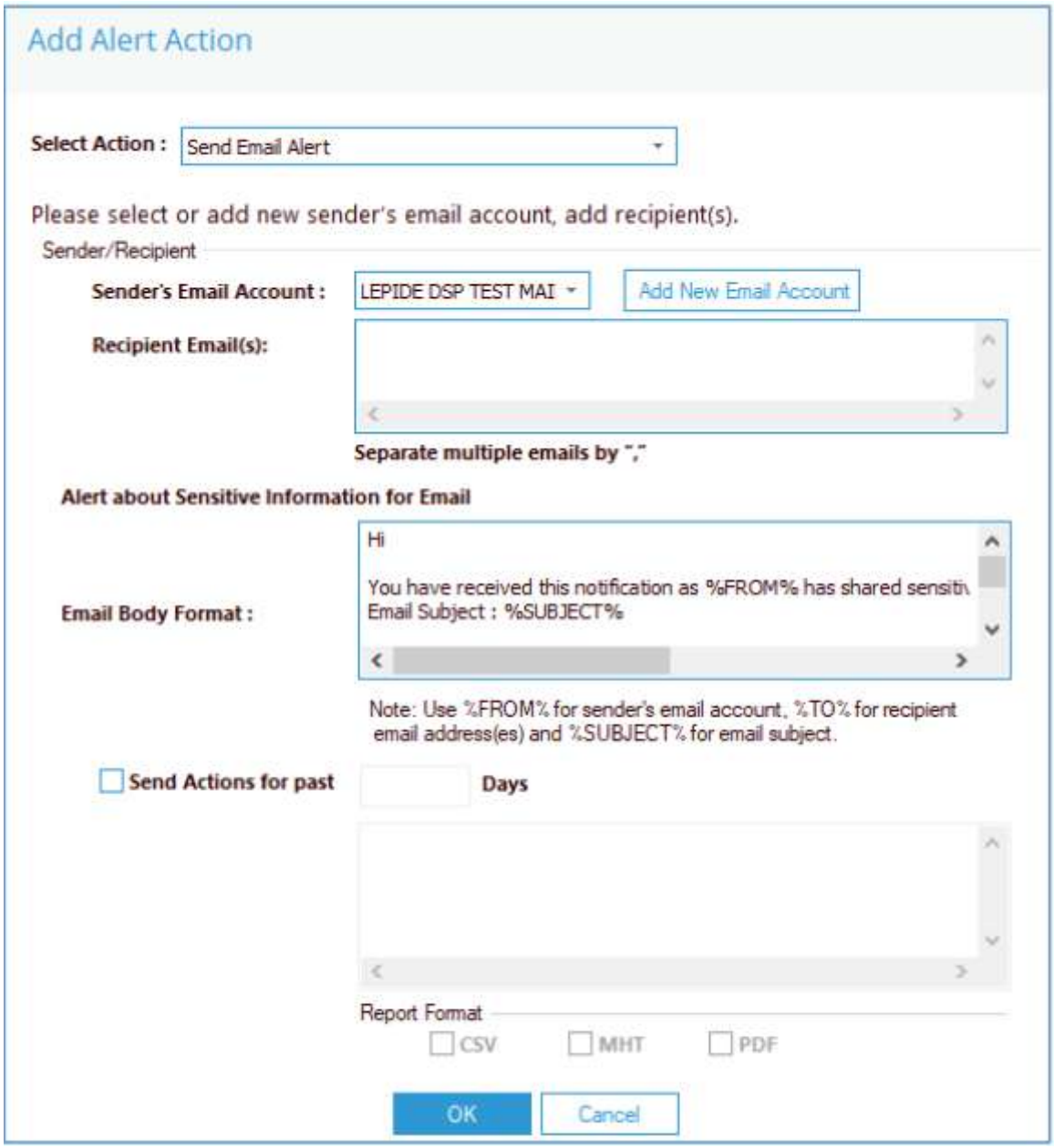
系统弹出"告警设置"对话框：



此对话框允许您设置在触发警报时发生的响应，并显示已设置的任何现有响应。您也可以更改警报类型。

• 要创建对警报的新响应，请单击Add按钮。

系统弹出“Add Alert Action”对话框。



此选项允许您在触发警报后发送电子邮件。对话框的元素如下:

发件人的电子邮件帐户：如果选择了发件人的电子邮件帐户，则在此处显示发件人的电子邮件帐户。单击"添加新电子邮件帐户"以输入新的发件人电子邮件帐户

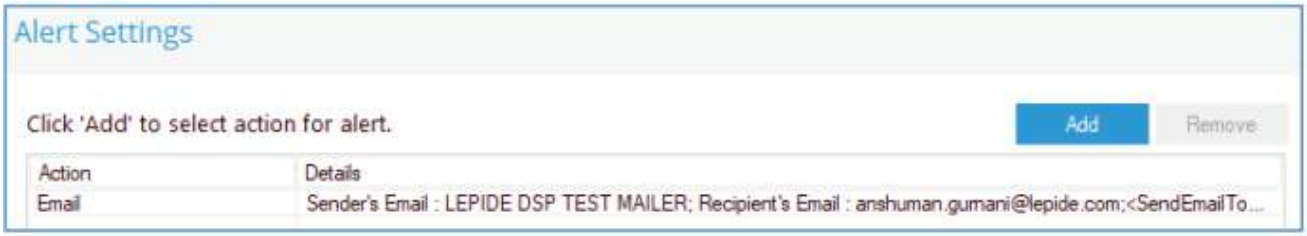
收件人电子邮件：通过在框中键入电子邮件地址来添加收件人电子邮件。如果有多个邮箱地址。

用"发送过去xx天的操作"分隔它们：此选项允许您查看该用户在过去指定天数内所做的所有操作。例如，如果因为发送了包含敏感数据的电子邮件而触发警报，您可能希望查看该帐户还发生了什么。选中此框并指定天数，将发送一封电子邮件，其中包含一个附件，列出用户在指定天数内所做的所有事情。

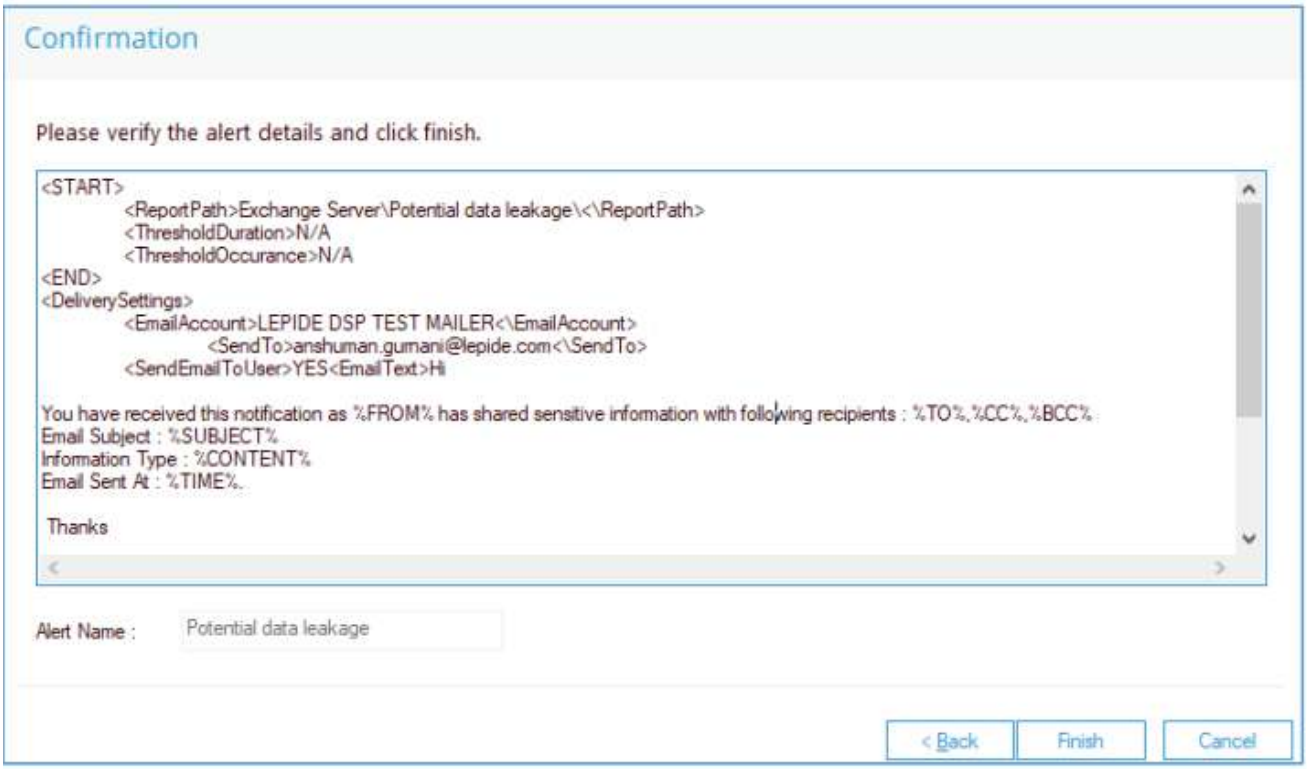
附件将包含一份报告，可以通过选中相关框来指定格式。格式为CSV、MHT和PDF。

• 单击"确定"，保存告警操作。

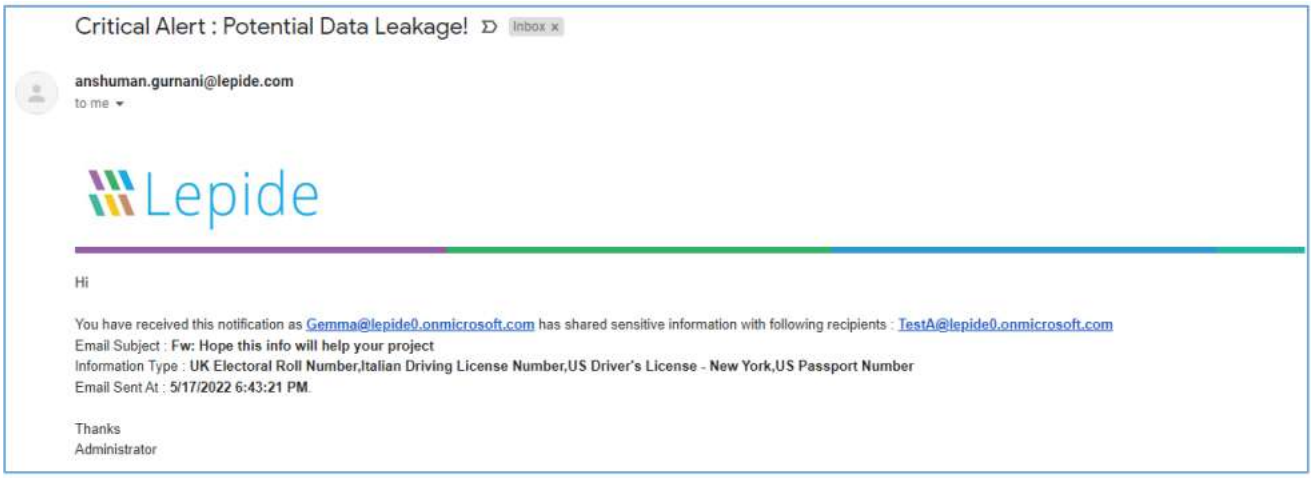
您将返回到"警报设置"对话框，您设置的警报现在将显示在这里:



• 单击下一步



警报现在设置好了。一旦发生电子邮件交换，Lepide数据安全平台将调用警报设置并发送电子邮件给收件人，如下所示：

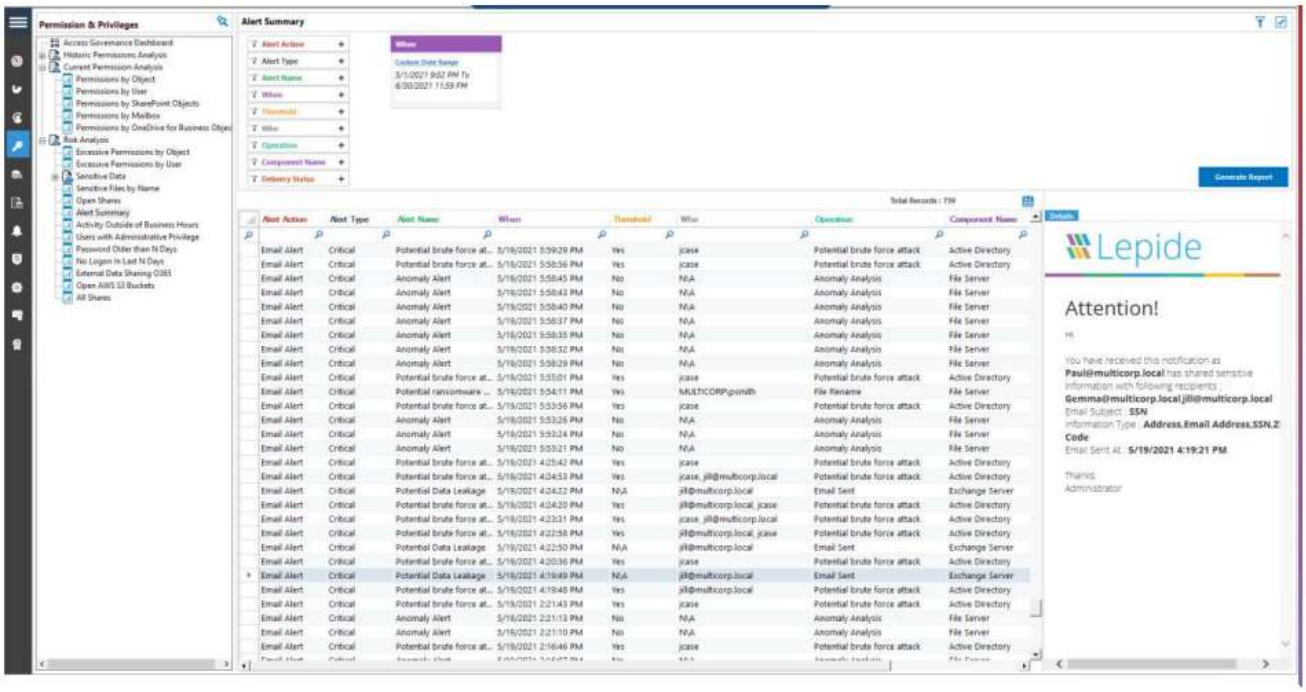


警报通知也可以在警报摘要报告中看到。

• 单击Permissions & Privileges图标

• 展开Risk Analysis（从树形结构到屏幕左侧）

• 单击Alert Summary以显示Alert Summary Report



当您单击某一行时，它将在屏幕右侧的详细信息窗口中显示提醒电子邮件的内容。

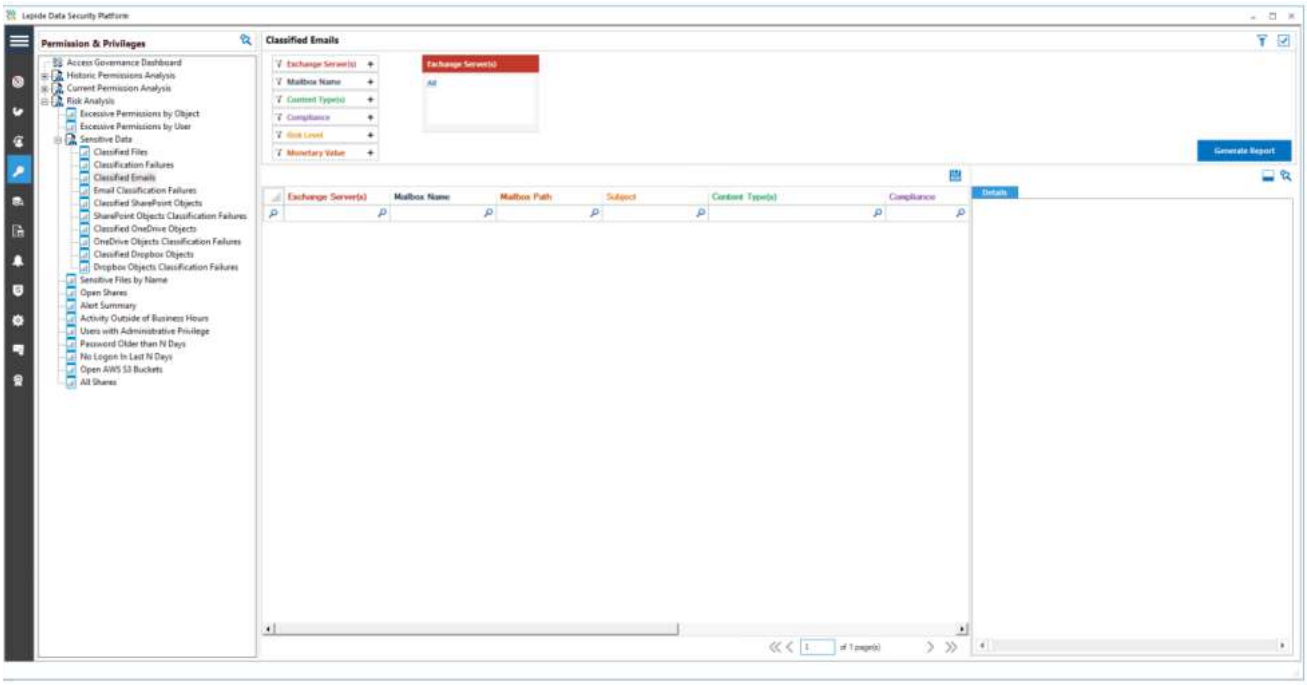
机密邮件报告

先决条件

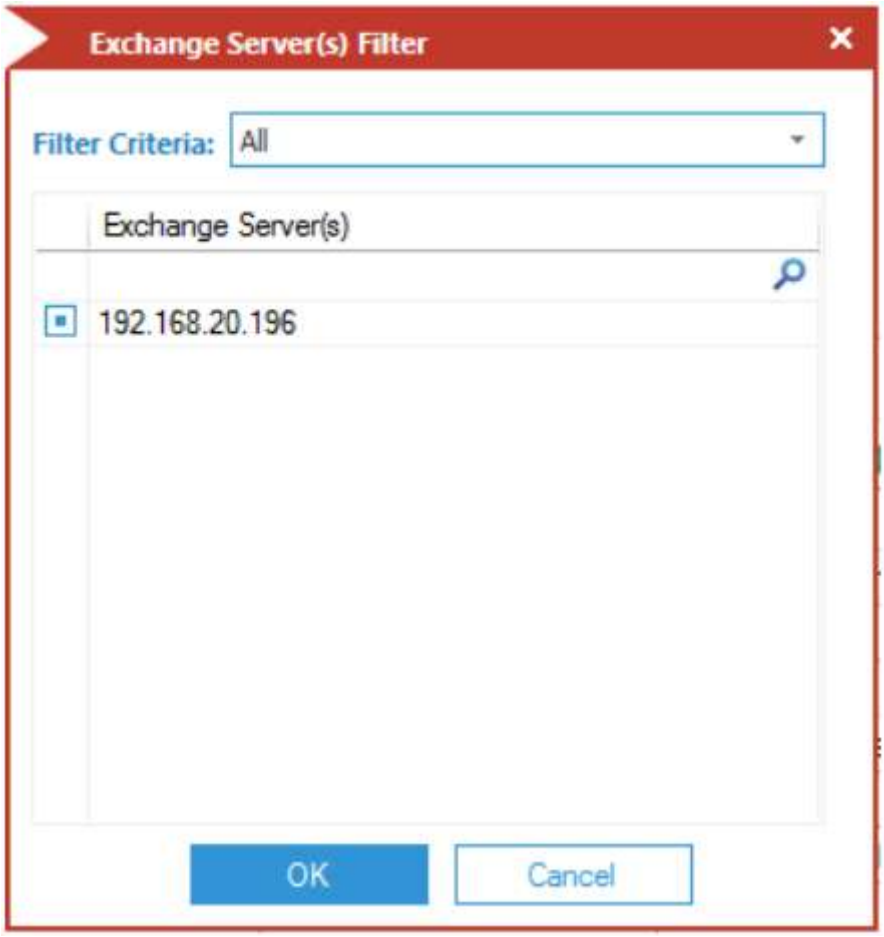
在运行分类电子邮件报告之前，您需要为Exchange Online配置数据发现和分类。有关如何做到这一点的信息，请参阅数据发现和分类配置指南。

运行机密邮件报告

- 点击权限和特权图标
- 展开风险分析(从树状结构到屏幕左侧)
- 展开敏感数据
- 点击分类邮件显示分类邮件报告：

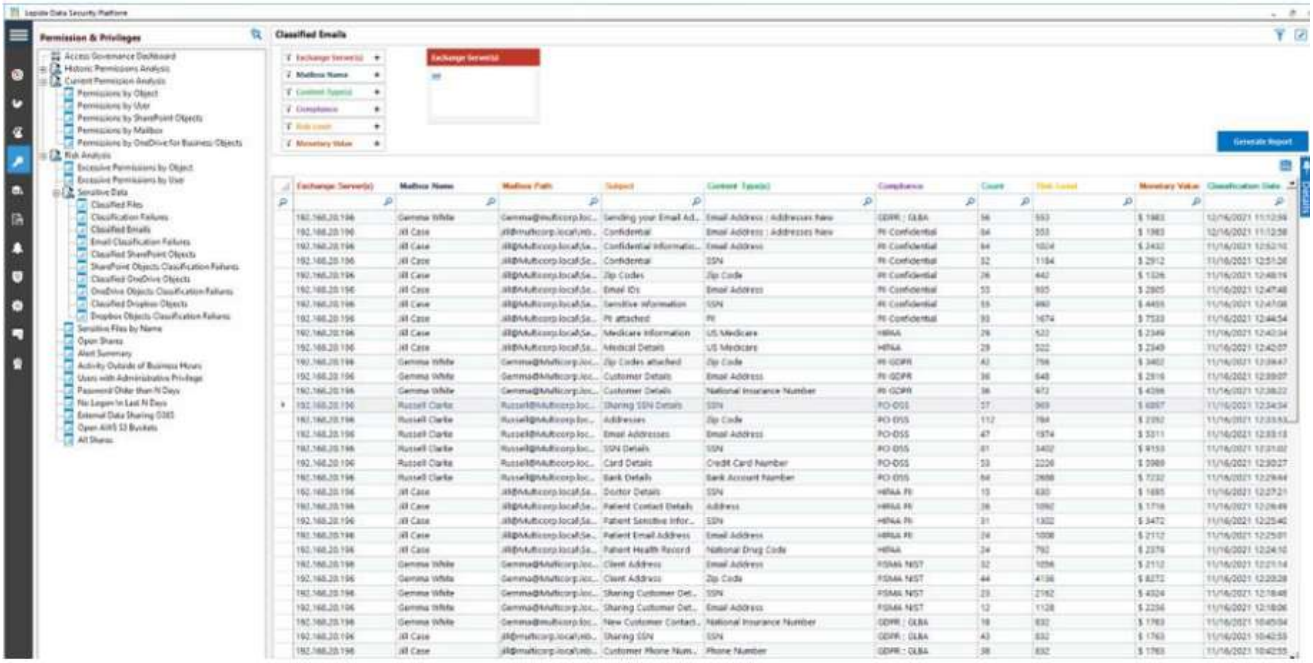


• 在屏幕顶部的Exchange Server(s)下，单击以选择所需的Exchange Server：



• 单击Generate Report

在选定的交换服务器中，任何用户或其邮箱之间的任何敏感电子邮件交换都将在报告中列出。



• 报告显示哪些邮箱、电子邮件主题和内容类型是包含敏感数据的电子邮件交换的一部分。

• 在本报告的右侧，您将能够在合规性栏中看到更多详细信息，显示哪些数据安全合规性已被破坏，作为此电子邮件交换的一部分。

• 所构成的风险水平，其计数和货币价值也被报告。这可能是管理员用来采取行动以阻止进一步损害的关键信息。

• 报告还显示相同的电子邮件是否被转发给其他用户，可以在主题栏中看到。

Received Time列可用于了解在此由电子邮件引起的敏感数据泄露事件中，哪个数据源（或邮箱）充当源。这为进一步调查提供了必要的信息。

• 请注意，您不需要在Lepide数据安全平台的审计模块中添加相同的Exchange在线服务器。只需完成Data Discovery & Classification的设置就足以生成这个一次性报告。

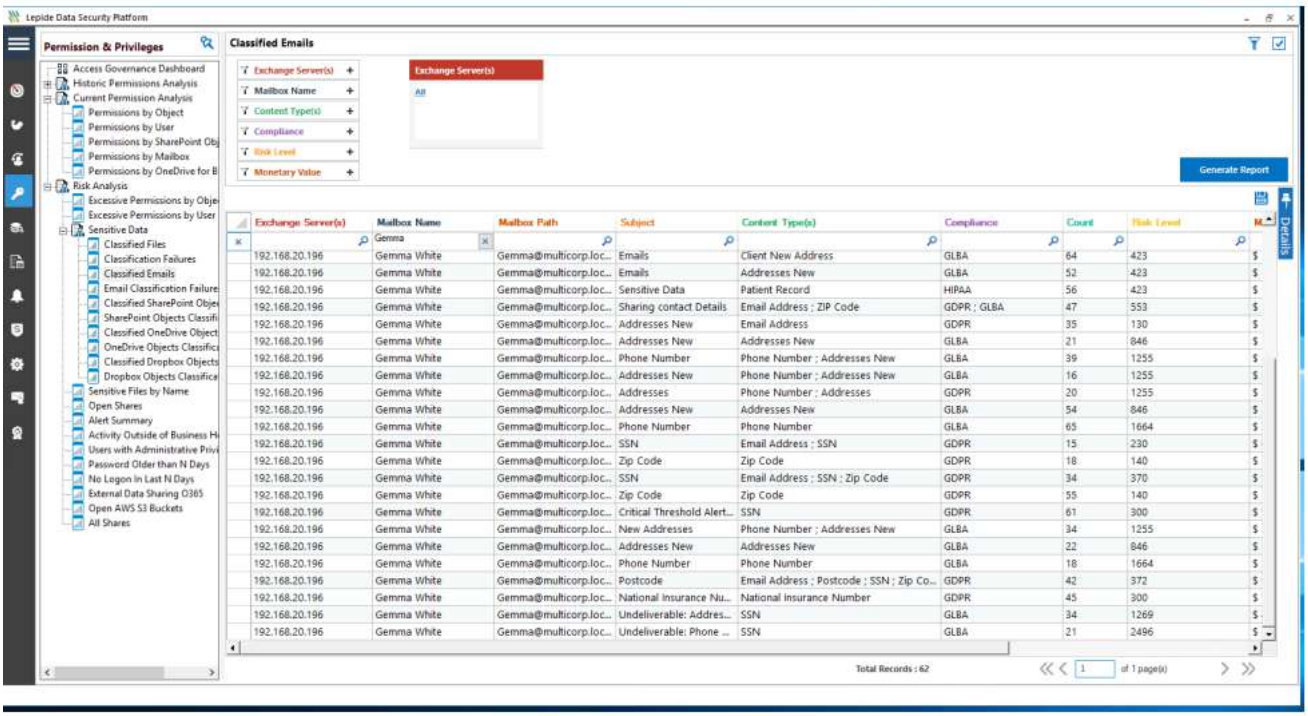
• 但是，如果您希望实时生成相同的报告，那么您需要在数据发现和分类配置期间选择分类服务器向导上的On the Fly Classification选项。

过滤报表

•若要为数据添加过滤器，请单击相关列上方的过滤器区域，并键入您想要查看的信息。

例如，您可能希望查看特定邮箱名称的数据-因此单击"邮箱名称"列顶部并键入要过滤的名称：

在下面的示例中，报告已被过滤以显示Gemma的数据:



报表支持调度、保存和导出。

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