

# 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:

	Threat Models Change Alerts Health Alerts	
0	Potential ransomware attack	Increased threat surface area (FS)
e		
۲ ه	Mass delete behaviors (FS)	Critical files moved
B		0
5 \$	Permissions escalation (File)	Permissions escalation (Folder)
-		
Q	Ownership modifications	Potential data leakage

• 单击图标以配置所需的警报和响应。

这将启动一个向导:

		×
Please select the report(s)		
Click next to apply further filters around your alert		
	< <u>B</u> ack <u>N</u> ext > Ca	incel

• 单击Next以显示Set Filter(s)对话框:

						×
Set Filter(s)						
Please select operations to s	et the filter(s). (O	ptional)				
Exchange Server	į.					
		e76				
		Filters are not	applicable for this	report		
¢	>					
				< Back	Next >	Cancel

•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:

lort Sottings		
iert settings		
Click 'Add' to se	lect action for alert.	Add Remove
Action	Details	
lert Type :	Critical -	
		< Back Next > Cancel

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。

elect Action : Send Email Alert	<b>*</b>	
lease select or add new sen	der's email account, add recipient(s).	
Sender/Recipient		
Sender's Email Account :	LEPIDE DSP TEST MAI * Add New Email Acc	ount
Recipient Email(s):		~
	c .	>
	Separate multiple emails by ","	
Alert about Sensitive Informat	tion for Email	
	Hi	
	You have received this patification as IV ED OMIN h	as shared coorts
Email Body Format :	Email Subject : %SUBJECT%	as shared sensiol
	•	
	Note: Use %FROM% for sender's email account, %	TO% for recipient
	email address(es) and %30000001 % for email subje	<b>u</b> t.
Send Actions for past	Days	
		2
		~
	1	2
	<	· · · · ·

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:

Alert Settings			
Click 'Add' to sel	ect action for alert.	Add	Remove
Action	Details		
Email	Sender's Email : LEPIDE DSP TEST MAILER; Recipient's Email	iil : anshuman.gumani@lepide.com;<	SendEmailTo

•单击下一步

Please verif	fy the alert details and click finish.		
<start> <r <ti< th=""><th>eportPath&gt;Exchange Server\Potential data leakage\&lt;\ReportPat hresholdDuration&gt;N/A</th><th>th&gt;</th><th>^</th></ti<></r </start>	eportPath>Exchange Server\Potential data leakage\<\ReportPat hresholdDuration>N/A	th>	^
<ti< th=""><th>hresholdOccurance&gt;N/A</th><th></th><th></th></ti<>	hresholdOccurance>N/A		
<deliverysett< th=""><th>lings&gt;</th><th></th><th></th></deliverysett<>	lings>		
<b< th=""><th>mailAccount&gt;LEPIDE DSP TEST MAILER&lt;\EmailAccount&gt; <sendto>anshuman.gumani@lepide.com&lt;\SendTo&gt;</sendto></th><th></th><th></th></b<>	mailAccount>LEPIDE DSP TEST MAILER<\EmailAccount> <sendto>anshuman.gumani@lepide.com&lt;\SendTo&gt;</sendto>		
-			
<s< th=""><th>endEmailToUser&gt;YES<emailtext>Hi</emailtext></th><th></th><th></th></s<>	endEmailToUser>YES <emailtext>Hi</emailtext>		
<si You have rec</si 	endEmail I oUser>YES <email ext="" i="">Hi selved this notification as %FROM% has shared sensitive informations to the sensitive information of the sensitive informatio</email>	on with following recipients : %TO%,%CC%,%BCC%	
You have rec Email Subject Information T	endEmail IoUser>YES <email iext="">Hi ceived this notification as %FROM% has shared sensitive information t : %SUBJECT% ype : %CENT% + %TIME%</email>	on with following recipients : %TO%,%CC%,%BCC%	
You have rec Email Subject Information T Email Sent At	endEmail IoUser>YES <email ext="" i="">Hi selved this notification as %FROM% has shared sensitive information : : %SUBJECT% ype : %CONTENT% : : %TIME%.</email>	on with following recipients : %TO%,%CC%,%BCC%	
<s You have rec Email Subject Information T Email Sent At Thanks</s 	endEmail IoUser>YES <email ext="" i="">Hi beived this notification as %FROM% has shared sensitive information t : %SUBJECT% ype : %CONTENT% t : %TIME%.</email>	on with following recipients : %TO%,%CC%,%BCC%	~
<si You have rec Email Subject Information T Email Sent At Thanks</si 	endEmail I oUser>YES <email ext="" i="">Hi ceived this notification as %FROM% has shared sensitive information t : %SUBJECT% ype : %CONTENT% t : %TIME%.</email>	on with following recipients : %TO%,%CC%,%BCC%	*
<si You have rec Email Subject Information T Email Sent At Thanks Alert Name :</si 	endEmail I oUser>YES <email ext="" i="">Hi ceived this notification as %FROM% has shared sensitive information t : %SUBJECT% ype : %CONTENT% t : %TIME%. Potential data leakage</email>	on with following recipients : %TO%,%CC%,%BCC%	¢

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:

Critical Alert : Potential Data Leakage! D Inbox x
anshuman.gurnani@lepide.com to me ▼
<pre>WLepide</pre>
HE
You have received this notification as <u>Gemma@lepide0.onmicrosoft.com</u> has shared sensitive information with following recipients : <u>TestA@lepide0.onmicrosoft.com</u> Email Subject : Fw: Hope this info will help your project Information Type : UK Electoral Roll Number,Italian Driving License Number,US Driver's License - New York,US Passport Number Email Sent At : 5/17/2022 6:43:21 PM.
Thanks
Administrator

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

Permission & Privileges	Alert Summary								Ť
- ## Access Governance Dashboard	7 Ainet Action		Wites						
# Philastic Permission: Analysis	7 Alert Type		Carlos Dete Sanje						
Permission Analysis	7 Ainet Barne		5/5/2021 9:02 PM Te						
Permissions by User	7 Wilson		6/30/2021 11:59 FM						
Permissions by SkarePoint Objects	A. House								
Permanent by Maiber	¥ Characteristic	•							
Permissions by Conditive for Business Object	T the								
Entertaine Permanent by Obart	T Careation								
Excessive Permissions by User	7 Congrowed No.	• •							
🛞 🔀 Sensitive Data	7 Delivery Malas	+							Generate Repre
Senative Files by fileme							Total Rev		
Alert Summary	A Ant Artes	Aint Tane	Alex Barry	Where	Barrhold	We	Owner	Concept Name *	Detate
Activity Cutside of Business Hours	D	8	0 0			0	8	0 0	and a second second
Researched Diday than Is Days	Frank Main	Painted .	Reported house factor of		1100	Sec. 1	Reducted Dates forms attack	Autor Directory	. enide
The Learn In Last N Days	Email Alart	Critical	Detected broke force at	EVELOTIN SAME PAR	1000	in the second se	Retential bride force starts	Active Developy	m Lepiue
External Data Sharing 0365	Email Alert	Critical	According Light	5/16/2021 5:58.45 PM	No	104	Anomaly Analytic	File Server	
Open AWS 53 Buckets	Email Alert	Critical	Anomaly Alert	5719/2021 5-58-43 PM	No	NA	Anomaly Analysis	file Server	
- [d] All Shans	Fittail Alert	Critical	Anomaly Alert	S/15/2011 Sishiat PM	No	16.6	depende analysis	File Server	Attention
	Email Alert	Critical	Anomaly Alert	1/19/2021 5:58:37 PM	No	NA	Anomaly Analysis	File Server	Allention
	Email Alert	Critical	Anomaly Alert	3/10/2021 5:58:35 PM	No	N/A	Anomaly Analysis	File Server	H
	Email Alert	Critical	Anomely Alert	5/19/2021 5/38/32 PM	No	NOA.	Anomaly Analysis	File Server	
	Email Alert	Critical	Anomaly Alert	5/18/2021 5:58:29 PM	No	MA	Anomaly Analysis	His Seiver	You have received this notification as
	Email Alert	Critical	Potential brute force at.	5/19/2021 5:55:01 PM	Ves	jcase	Potential brute force attack	Active Directory	Paul@multicorp.local has shared sensitive
	Email Alert	CHENCIAL	Potential ransommare	5/19/2021 5:54:11 PM	1945	MULTICORPIperville	File Rename	File Server	information with following recipients .
	Email Alert	Critical	Potential brute force at.	5/15/2021 5:53:56 PM	Yes	jcase	Potential brute force attack	Active Directory	Email Schuert CON
	Email Alert	Critical	Anomaly Alert	5/19/2021 5:53:26 PM	NO.	NA	Ahomaly Analysis	File Server	information Type Address Email Address \$57
	Email Alert	Critical	Anomaly Aiert	5/10/2021 5:53124 PM	No	NA	Amomaly Analysis	File Server	Code
	Email Alert	Critical	Anomaly Alert	3/18/2021 5/55/21 PM	140	NOA	Anomaly Analysis	File Server	Email Sent AL: 5/19/2021 4:19:21 PM.
	Email Alert	Critical	Potential brate force at.	. 5/18/2021 4/25/42 PM	Yes	icase	Potential brute force attack	Active Directory	
	Ernail Alert	Critical	Potential brute force at.	5/18/2021 4/34:53 PM	Ves.	jcase, jil@muticorp.local	Potential brute force attack	Active Directory	TRACKS
	Email Alert	CHEICH	Potential Data Leakage	5/19/2021 4/24:22 PM	10,0	#I@multicorp.tocal	Email Sert	Exchange Server	Administration
	Email Alert	Critical	Potential brute fonce at.	5/19/2021 4/24/20 PM	Yes	jili@multicorp.local, jcase	Potential brute force attack	Active Delectory	
	Email Alert	Critical	Potential brute force at.	. 5/19/2021 4/23/31 PM	TEL	icase, pli@muticorp.local	Potential brute force attack.	Adive Delectory	
	Email Alert	critical	Potential brute force at.	1/19/2021 4/22/58 PM	THE	yitemuticorplocal joine	Potential brute force attack	Active Devectory	
	Email Alert	Critical	Potential builts Leakage	5/19/2021 4/22/50 PM	TRUA	internuticorp.ioca	Emple Sent	Exchange server	
	A Email diart	Collector	Detectial Cata Lankage	STREET ALCOUNT AND BUT	165	ilitheuiticon bool	Final Cast	Autore perform	
	Email Alart	Critical	Potential Prote from al.	5/10/0011 #10/40 PM	No.	all multicore local	Victorial brate force attack	Active Direction	
	Final Alert	Critical	Potential brute force at	5/19/021 22145 844	Tes	17214	Potential brute force attack	Active Deactory	
	Email Alert	Critical	Anomaly Alert	5/18/2021 2/21/13 PM	Ráp	10.4	Anomaly Analytic	file Server	
	truel diert	critical	Anomaly alert	3/19/2021 2/21/10 PM	740	NA	Anomaly Analysis	File Server	
	Email Alert	critical	Potential brute force at.	5/19/2021 2:16/46 PM	Vet	Kate	Potential brute force attack	Active Directory	
	Panel Mart	making!	Annal the sheet		also.	48.5	tananahi tantula y	Pli Palate	

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:

Lepide Data Security Platform		(a) (B) (
Permission & Privileges 🔍	Classified Emails	7 🖸
Excess Genemance Darbitrand     Excess Genemance Darbitrand     Excess Genemance Darbitrand     Excess Permission Andrysis     Excess Permission by Diget     Excess Permission by Use     Excess Permission by Use     Excess Permission by Use     Excess Permission by Use	V     boxbases     finitume       V     Matheway None     Ad       T     Comptions     +       V     Monotacy Vole     +	Generate Neport
Classified Emails		
Cleastied SharePoint Objects	Escharge Server(s) Malbox Name Malbox Path Saleect Content Type(s) Carelance Malbox Path	
Constant Open Construction dates Constant Open Construction Constant Open Construction Constant Open Construction Constant Open Construction Constant Open Construction Constant Open Construction Constant Open Construction Cons		

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

	Exchange Server(s) Filter	×
Filte	r Criteria: All	*
	Exchange Server(s)	
	192.168.20.196	٩
	ОК	Cancel

• 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。

The Legisle Data Security Matterne										
Permission & Privileges	Classified Emails									¥ G
Action Sciences Published     Homore Providence Advisor     Homore Providence Advisor     Providence Advisor	4 Facturer Serverbil 4 Mollina Same 4 Complement 4 Complement 5 Solid compl 4 Moneticy Male	• Extense 0	er wetta							Generate Report
Exception Parentations by Object										
CA BIA Serutive Data	d Eastwarge Server(a)	Madisca Name	Madines Path	Subpact .	Genere Typels()	Compliance	Court	The Loted	Monetary Votos	Geeficaten Sele
CinsRed Files	P	P	P P	P		2	P	P	p J	P
Ciscification Fallows	182,165,30,196	Centrals Trifular	Canmagnutteerp.loc.	Sending your Email Ad.,	Email Address / Addresses him	CERT : FARA	56	-853	\$ 1962	12/16/2071 11:12:58
Email Classification Failure	192,188,20,199	JRI Calle	alignmentions locations	Confidential.	Email Address ( Addresses New	PE Confidential	- 84	25.8	1 1943	12/16/2021 11:12:58
Clauffert Sharefront Olevers	192.168.278.196	INT CALE	imps.aticcep.local.(a.,	Confidential Information.	Creat Address	PE Confidential	84	1004	\$ 2432	11/16/0821128238
Durafished Objects Cassification Failures	192.166.25.156	JRI Cape	stable corp local Se.	Confidential	25%	R Confidential	32	1184	\$ 2912	11/10/2021 12:51:26
Claufed Orighter Objects	192,768,20,795	III Case	stpts.temp.toc45e_	70 Codes	The Code	PE Confidential	28	642	\$ 1128	11/16/2021 12:48:19
Družske Objects Cassification Failures	192,148,28,196	141 Case	allforuteerplocation.	Emer IDs	Dear Address	TI CUINDERNI	- 53	805	3 2905	11/10/2021 12:47:48
Caroling Drawing Objects	192,195,252,198	III Celle	algeball corp. local (a.,	Lendbe Mormation	1324	#E Costfidential	85	4962	8.4455	11/16/2021 12:41:08
Compared white the second second	192.166.20.196	THI CEER	alightering local 34	PE attached		HE CONTINUES	90	19674	\$ 7533	11/10/2021 12:44:54
Copyr Plants	142,188,20,10	IN Case	and American Construction of the	Medicare information	US Medicare	1994	28	100	\$ 2349	11/16/2021 12:42:34
Alart Surrary	192.105.28110	141 CELE	INDAMACIP IOCH/SE	Antidical Details	US MIGGIN	HETAA	29	544	3 2349	11/16/2021 12:42:07
Activity Outside of Business Hours	197,186,26,199	Centime trible	Carning Multicip Jos.	The Codes attached	Cly Code	an ocean	AU.	198	5.0402	11/16/0021 12/0647
Quers with Administrative Privilege	192,198,23,196	Gening white	Service deviation drafes	Customer petales	Ender Address	10.0004	198	040	5 2019	11/14/2021 12/39/27
His Lessen in Last N Parts	192,194,25,195	Carriente Utilitar	Canana guate or pro-	Californier Decem	Autoria Insulance Number	10 (2,24)	100	100	5 4258	11/16/00/11/23822
Esternal Data Sharing 0385	<ul> <li>192,166,20,790</li> </ul>	Ruther Carts	Rutter Bank Batter Dic.	DAVING SEV CIESING	1004	10.000	- 27 /	003	1.0207	11/16/2023 12:34:34
Open Ailth S3 Busilets	192,186,72,796	Partiel Corte	norse igneration in the	Addresses.	ap cade	10.055	1114	1000	18 2250	through transford
Alt Shares	182.198.20.199	Autory Carte	Hatter Broke Corp Roc.	Empri Appresses	Dealer Address	PCPUSS		1274	3 2011	10/10/2021 12:8818
	102 102 10 100	Parties Carlo	Harter groups of pro-	Circl Details	County County & Look on	20.005	140	1000	8 8150	NUMBER OF STREET
	192,796,200 199	Harper Carts	Resident Resident	Card Details	Credit Carlo Nancer	101000	- 28	1000	1 2000	11/16/2021 12:30:27
	167 168 30 156	and Chara	USEA & Roman Incid Co.	Sara Ortago	COM	10000	12	1000	8 1485	11/16/2023 12/2018
	THE REAL OF THE	di Care	sheet a Recent bound to	Report Control Databa	1.55		11	1000	1 1 1 1 1	The second states as
	and here the odd.	10.000	shifts Broom bread to	Preteral Communities	TTN:	and a fit	144	14400	6.1477	11002/0012 (3/25.40
	102 102 20 108	10 Cale	ill that disease local fa	Report Local Address	Imal Millard	10000 00	14	1000	4 1414	11/16/0001 12/20/00
	107.108 10.108	al Case	all first Barney Incid Sa	Report Marin Record	Automatic Prove Cardy	with a	14	1941	4 1010	11004000111005440
	107 100 10 100	Camera White	Cammadd Addition Inc.	Class Address	Terrar Address	COLDAN MANY	147	and a	8.2412	11/14/0011 10/2114
	192 165 33 194	Garnesa Within	Genma@indicion.icc	Clare Address	Zin Cada	ROMA NOT	44	14130	\$ 6172	11/16/2021 12:29:38
	1411100.00.000	Genture White	Cerrma@htuticrem.inc	Sharing Customer Det	59N	PSAN NOT	29	2162	5 4324	11/16/3071 12:18:49
	192 168 30 106	Gamma tribita	Cermadito/fump.loc	Sharing Customer Oat	Email Address	ROLAS NOT	12	1128	\$ 2254	11/16/2021 12:18:06
	107.100.75.144	Genture White	Cennadmultisso inc	New Cutomer Codart.	National Insurance Number	CONT CARA	14	837	\$ 1763	11/10/0621 10/00/04
	102 148 30 194	All Case	alderselecter and and	Thirng Silv	SSN .	CENT CANA	43	832	4 (743	10/14/2021 10:42-55
			the second se							

•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:

)	Mailbox Name		Mailbox Path
Q	Gemma	×	
	Gemma White	- Personal Personal Person Per	Gemma@mult
	Gemma White		Gemma@mult
	Commo White		Gomma@mult



报表支持调度、保存和导出。



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





haocst.com

获取更多资料