Lepide

ALIGNMENT GUIDE

ALIGNING LEPIDE FOR

INSIDER

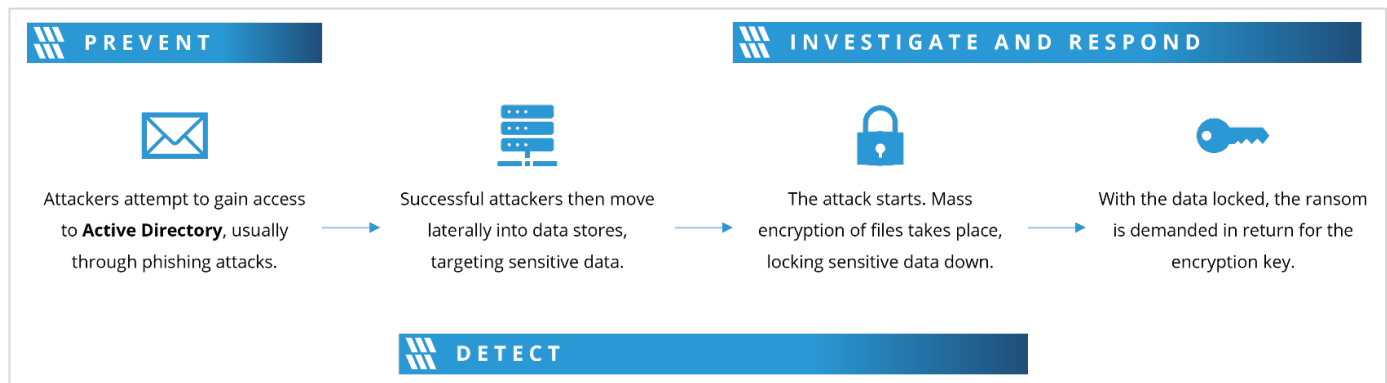# THREATS

Table of Contents

1. Introduction

Threat detection is still a huge challenge for organizations today – hackers are agile, fast and smart. When we use the term threat here, we're referring to malware or some form of external brute force attack. While many 'traditional' vendors claim high threat detection rates not one security vendor out there can detect 100% of threats and it only takes one threat to break through and then the whole network is vulnerable.

Most security vendors have little or no understanding as to the inner workings of Active Directory, Windows File Systems which limit their value when trying to detect and investigate threats as they propagate across the corporate network. 99% of all security threats will utilize Active Directory as their means of spreading across the network, and if the objective of the hacker is to steal, leak or in some way restrict access to corporate data most security vendors offer little or no context in this area. Most security vendors can't provide any context as to what sensitive data is or what was affected by the threat which makes investigations less impactful, slower and less efficient.

2. Aligning Lepide for Insider Threats

There are a number of key questions that you need to be able to answer to be able to detect, prevent, investigate and respond to threats.

PREVENT

Attackers attempt to gain access to **Active Directory**, usually through phishing attacks.

Successful attackers then move laterally into data stores, targeting sensitive data.

INVESTIGATE AND RESPOND

The attack starts. Mass encryption of files takes place, locking sensitive data down.

With the data locked, the ransom is demanded in return for the encryption key.

DETECT

In the table below, we align Lepide technology to these questions:

Category	Actions to Take	Technology to implement
Detect	Detect when an employee goes rogue and acts in a way that they don't normally act	All Environment Changes Report (Lepide Audit) Anomaly Spotting (Lepide Detect)

		Mass Delete Behaviors (OU) Threat Model ([Lepide Detect](#))
		Mass Delete Behaviors (User) Threat Model ([Lepide Detect](#))
		Mass Delete Behaviors (Computer) Threat Model ([Lepide Detect](#))
		Mass Delete Behaviors (Group) Threat Model ([Lepide Detect](#))
		Mass Delete Behaviors (FS) Threat Model ([Lepide Detect](#))
		Mass Data Copy Threat Model ([Lepide Detect](#))
		Potential Data Leakage Threat Model ([Lepide Detect](#))
		Potential Business Disruption Threat Model ([Lepide Detect](#))
		Permissions Escalation (Groups) Threat Model ([Lepide Detect](#))
		Permissions Escalation (File) Threat Model ([Lepide Detect](#))
		Permissions Escalation (Folder) Threat Model ([Lepide Detect](#))
		Potential Password Compromises Threat Model ([Lepide Detect](#))
	Detect if there were actions that could be symptomatic of a compromised user account.	All Environment Changes Report ([Lepide Audit](#))
		Anomaly Spotting ([Lepide Detect](#))

		Permissions by User Report (Lepide Trust)
		Any Threat Model (Lepide Detect)
		Permissions Escalation (Groups) Threat Model (Lepide Detect)
		Permissions Escalation (File) Threat Model (Lepide Detect)
		Permissions Escalation (Folder) Threat Model (Lepide Detect)
		Excessive Permissions by User Report (Lepide Trust)
		Users with Admin Privileges Report (Lepide Trust)
		Permissions Modifications Reports (Lepide Trust)
		Security Group Modifications Report for Active Directory (Lepide Trust)
		Group Modifications Report for Azure AD (Lepide Trust)
		Historical Permissions Reports (Lepide Trust)
		All Group Policy Modifications Reports (Lepide Trust)
		Exchange Permissions by Mailbox Report (Lepide Trust)

	Determine when sensitive data is being copied.	File Copied Report ([Lepide Audit](#))
		Mass Data Copy (FS) Threat Model ([Lepide Detect](#))
		All Modifications in File Server Report ([Lepide Audit](#))
		Sensitive Data Classification ([Lepide Identify](#))
	Ensure Active Directory administrators are not making changes that could lead to risk.	All Modifications in Active Directory Report ([Lepide Audit](#))
		Active Directory Permissions Modifications Reports ([Lepide Trust](#))
		All Group Policy Modifications Reports ([Lepide Trust](#))
		All Environment Changes Report ([Lepide Audit](#))
		Any Threat Model Triggered ([Lepide Detect](#))
	See when sensitive data is being shared via Email, OneDrive, MS Teams.	External Data Sharing O365 Report ([Lepide Audit](#))
		Real Time Alert ([Lepide Detect](#))
		Document Modification Reports ([Lepide Audit](#))
		All Mailbox Access Reports ([Lepide Audit](#))
		Potential Data Leakage Threat Model ([Lepide Detect](#))
Investigate	See what data employees are moving, modifying, accessing in a simple report	All Environment Changes Report ([Lepide Audit](#))

	Answer requests from our HR Team around how employees are engaging with data.	All Environment Changes Report (Lepide Audit)
		Excessive Permissions Report (Lepide Trust)
		Permissions by User Report (Lepide Trust)
		Users with Admin Privileges Report (Lepide Trust)
		Open Shares Report (Lepide Trust)
		Data Classification (Lepide Identify)
		File Server Modification Reports (Lepide Audit)
		SharePoint Online Modification Reports (Lepide Audit)
		OneDrive Modification Reports (Lepide Audit)
		MS Teams Modification Reports (Lepide Audit)
		External Data Sharing O365 Report (Lepide Audit)
		Mailbox Accessed by Non Owners Report (Lepide Audit)
	Identify the data that a specific employee has been handling and what they have done with it.	All Environment Changes Report (Lepide Audit)
		Permissions by User Report (Lepide Trust)
		Users with Admin Privileges Report (Lepide Trust)
		Open Shares Report (Lepide Trust)
		Data Classification (Lepide Identify)

		File Server Modification Reports (Lepide Audit)
		SharePoint Online Modification Reports (Lepide Audit)
		OneDrive Modification Reports (Lepide Audit)
		MS Teams Modification Reports (Lepide Audit)
		External Data Sharing O365 Report (Lepide Audit)
		Mailbox Accessed by Non Owners Report (Lepide Audit
Prevent	Reduce the amount of sensitive data employees have access to, to reduce risk.	Inactive Users Report (Lepide Audit)
		Excessive Permissions by User Report (Lepide Trust)
		Excessive Permissions by Object Report (Lepide Trust)
		Permissions by User Report (Lepide Trust)
		Users with Admin Privileges Report (Lepide Trust)
		Open Shares Report (Lepide Trust)
		Data Classification (Lepide Identify)
		Increased Threat Surface Area Threat Model (Lepide Detect)
		Permissions Escalation (Groups) Threat Model (Lepide Detect)
		Permissions Escalation (File) Threat Model (Lepide Detect)

		Permissions Escalation (Folder) Threat Model ([Lepide Detect](#)) Permissions Remediation [(Lepide Protect)](#) Remove Inactive Users [(Lepide Protect)](#)
Respond	Respond to insider threats.	Any Threat Model Triggered ([Lepide Detect](#))

3.   Lepide Core Capabilities

3.1. - Lepide Identify

Automatically scan, discover and classify data at the point of creation to help you stay on top of where your sensitive data is located. Remove false positives with proximity scanning technology. This helps to improve the accuracy even further than most classification solutions. Categorize and score data based on compliance, risk, occurrence, monetary value, and more to stay on top of your most sensitive data.

In Summary:

- Discover and classify data in real Tag data.

- Data valuation.

- Identify data most at risk.

For More Information:

https://www.lepide.com/lepide-identify/

3.2. - Lepide Trust

Report on who has access to your most sensitive data and how they were granted that access. Specific reports for users with excessive permissions enable you to spot which users are most likely to be insider threats. Maintain your zero-trust policy by spotting when permissions change and reversing them.

In Summary:

- Analyse permissions.
- Identify over privileged employees (least privilege).
- View historic permissions.
- Track permission changes.

For More Information:

https://www.lepide.com/lepide-trust/

3.3. - Lepide Audit

Audit, report and alert on changes being made to sensitive data and your hybrid environment. Roll back unwanted changes and restore deleted objects to maintain system integrity. Track any changes and modifications users are making to critical files and folders.

In Summary:

- View interactions with data.

- View interactions with systems governing access to data.

- Employee audit logs.

- Investigate incidents and breach scenarios.

For More Information:

https://www.lepide.com/lepideauditor/

3.4. - Lepide Detect

Machine Learning backed anomaly spotting technology will allow you to determine when one of your users becomes an insider threat. Hundreds of threat models, tailored to specific data security threats, generate real time alerts when the security of your data is in jeopardy. Automated threat responses can be triggered to perform threat mitigations, such as shutting down an affected computer or server.

In Summary:

- Detect threats in real time with pre-defined threat models.
- Baseline/profile employee behavior.
- Identify anomalous employee behavior.
- Alert and respond to threats in real time.

For More Information:

https://www.lepide.com/lepide-detect/

3.5. - Lepide Protect

Reduce the complexity of managing user permissions. The permissions management system within Lepide Protect provides a straightforward and efficient way to manage permissions over all shared locations. It provides clear visibility as to who has access to what, including identifying excessive permissions. Once identified, excessive permissions can be revoked, and inactive users removed; permissions policies can be used to do this automatically.
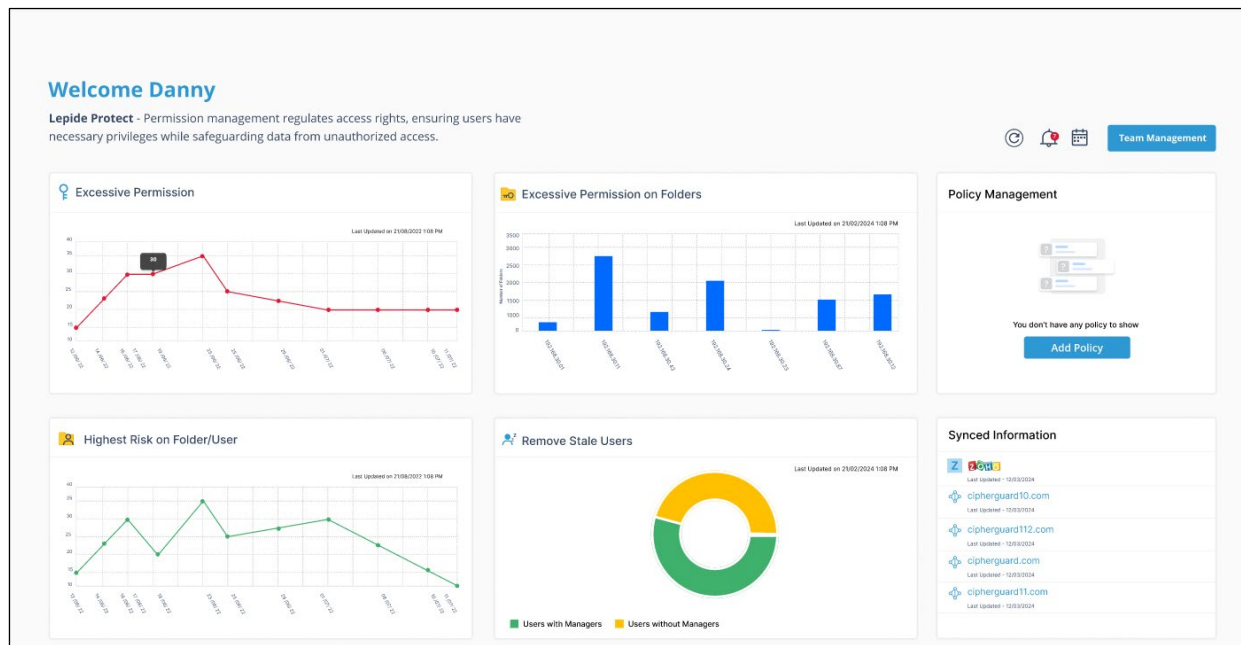
In Summary:

- Identify and revoke excessive permissions.
- Remove inactive users to reduce your threat surface.
- Delegate permissions management to team leaders.
- Use policy management to automatically revoke permissions.

For More Information:

https://www.lepide.com/lepide-protect/

4. Support

If you are facing any issues whilst installing, configuring, or using the solution, you can connect with our team using the contact information below.

Product Experts

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91 (0) -991-004-9028

Technical Gurus

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91(0)-991-085-4291

Alternatively, visit https://www.lepide.com/contactus.html to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com

support@Lepide.com

To read more about the solution, visit https://www.lepide.com/data-security-platform/.

5. Trademarks

Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform Logon/Logoff Audit Module, Lepide Data Security Platform for Active Directory, Lepide Data Security Platform for Group Policy Object, Lepide Data Security Platform for Exchange Server, Lepide Data Security Platform for SQL Server, Lepide Data Security Platform SharePoint, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only.

Microsoft®, Active Directory®, Group Policy Object®, Exchange Server®, Exchange Online®, SharePoint®, and SQL Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetApp® is a trademark of NetApp, Inc., registered in the U.S. and/or other countries.