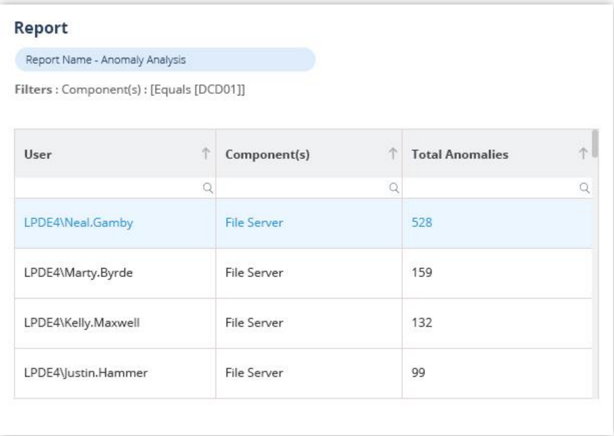
Lepide

Lepide Detect

Pre-defined threat models, and automated threat response, mean you can detect the signs of a compromise or security incident, and react in real time before it causes significant damage.



Report

Report Name - Anomaly Analysis

Filters : Component(s) : [Equals [DCD01]]

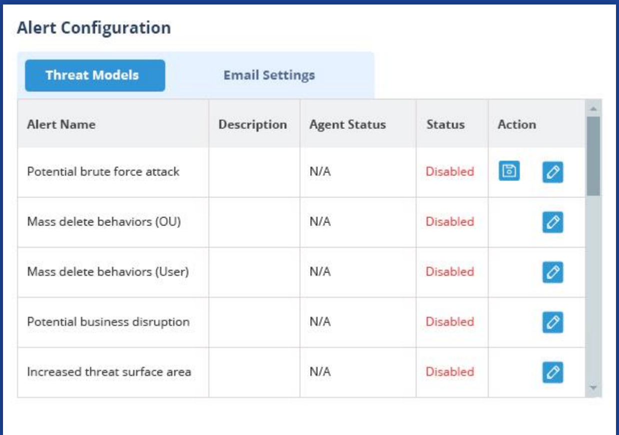
User	Component(s)	Total Anomalies
LPDE4\Neal.Gamby	File Server	528
LPDE4\Marty.Byrde	File Server	159
LPDE4\Kelly.Maxwell	File Server	132
LPDE4\Justin.Hammer	File Server	99

Detect anomalies in user behavior.

Lepide will automatically detect anomalies in user behavior, whether it is copying files with sensitive data, logging into the server out of hours, or simply acting strangely based on learned behavior. The solution learns what the normal behavior of your users looks like, and then can generate real time alerts whenever that behavior changes.

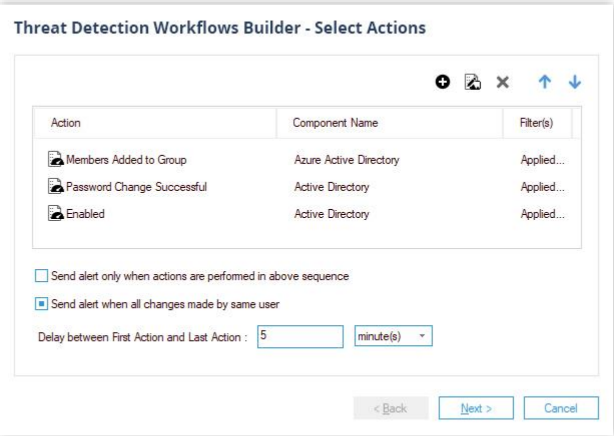
Deploy pre-defined threat models.

Pre-defined threat models detect a wide range of known security threats and will alert you in real time the instant a threat has been detected in your critical systems. Simply activate the threat model, and our solution will work in the background to ensure that no security threat goes unnoticed by your team.



Alert Configuration

Alert Name	Description	Agent Status	Status	Action
Potential brute force attack		N/A	Disabled	💾 ✎
Mass delete behaviors (OU)		N/A	Disabled	✎
Mass delete behaviors (User)		N/A	Disabled	✎
Potential business disruption		N/A	Disabled	✎
Increased threat surface area		N/A	Disabled	✎


Threat Detection Workflows Builder - Select Actions

Action	Component Name	Filter(s)
Members Added to Group	Azure Active Directory	Applied...
Password Change Successful	Active Directory	Applied...
Enabled	Active Directory	Applied...

□ Send alert only when actions are performed in above sequence

☑ Send alert when all changes made by same user

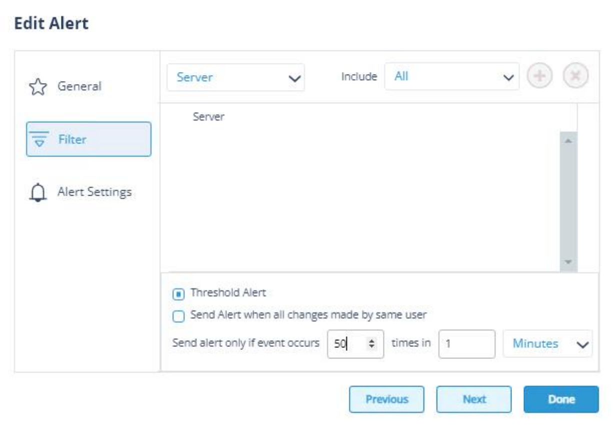
Delay between First Action and Last Action : 5 minute(s)

Advanced threat detection workflows.

Lepide Detect will allow you to chain events together across multiple systems / data stores to identify threats based upon certain attack paths. By doing this, you can configure threat detection workflows for specific known threats that follow the same pattern of events across your systems and data stores. This will drastically improve the effectiveness of your overall threat detection and response strategy.

Real time and threshold alerts.

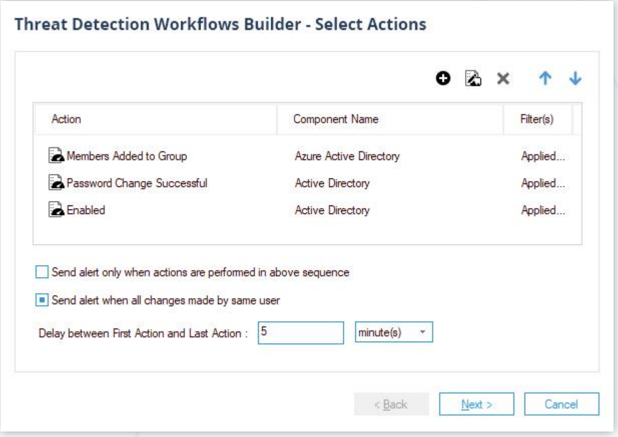
Receive real time alerts for anomalous user behavior, threats detected through threat models/workflows or for any custom event you want. Alerts can also be triggered on the basis of a threshold condition being met, such as a large number of file copy events over a small time period. This drastically helps to speed up your threat response and security investigations.


Edit Alert

☑ Threshold Alert

□ Send Alert when all changes made by same user

Send alert only if event occurs 50 times in 1 Minutes


Threat Detection Workflows Builder - Select Actions

Action	Component Name	Filter(s)
Members Added to Group	Azure Active Directory	Applied...
Password Change Successful	Active Directory	Applied...
Enabled	Active Directory	Applied...

□ Send alert only when actions are performed in above sequence

☑ Send alert when all changes made by same user

Delay between First Action and Last Action : 5 minute(s)

Automate threat response.

Execute pre-defined threat models/ workflows automatically to take whatever action you need to contain threats when they are detected. Ensure that your data remains protected, and your compliance posture remains in-tact. Our pre-defined threat models can take a number of actions to contain a threat, including shutting down the compromised user account, computer, or server.

Ready to test-drive Lepide? Visit lepide.com/in-browser-demo/