Lepide

Datasheet

Threat Detection and Response

Intelligent incident detection and automated response

Our anomaly detection technology allows you to spot and react to anomalous or unique user behavior. Generate real time alerts when one of our threat model templates picks up on a potential data security threat. Once a threat is detected, automate your response to shut down the threat before it manifests as a breach of compliance.

AI-Backed Anomaly Detection

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.

Alert on Potential Threats

Receive real time alerts whenever a potential threat is detected. Deploy one of our hundreds of pre-defined threat models for a wide variety of security threats.

Automate Threat Response

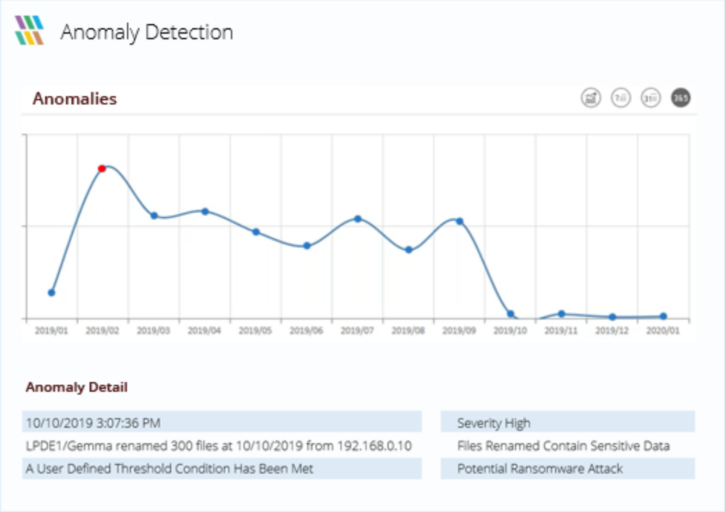
Execute custom scripts automatically to shut down threats as they are detected in real time - ensuring the security of your data and your compliance posture.

Identify When Privileged Users Become Threats

Our data classification technology will allow you to classify files on a persistent basis to enable you to keep track of your most sensitive data.

With real time alerting and predefined reports, you can detect threats to this data and take the required steps to mitigate them before they manifest as data breaches.

Machine learning enables you to establish a baseline for normal user behavior and receive alerts whenever behavior deviates from this norm. Our anomaly spotting technology can even detect single point anomalies.



Anomaly Detection

Anomalies

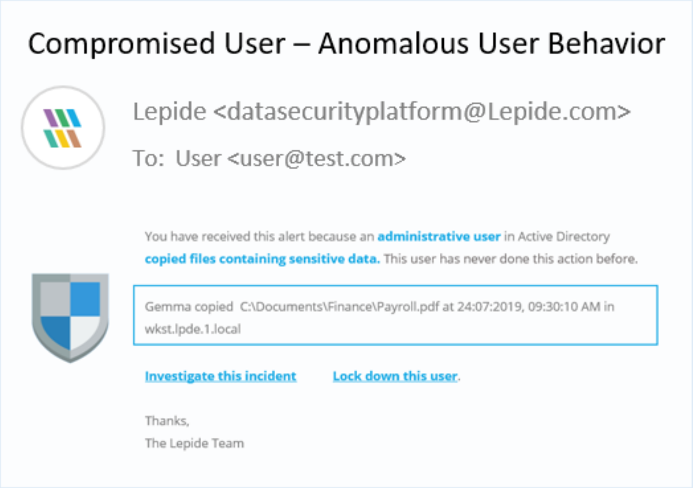
Anomaly Detail

10/10/2019 3:07:36 PM	Severity High
LPDE1/Gemma renamed 300 files at 10/10/2019 from 192.168.0.10	Files Renamed Contain Sensitive Data
A User Defined Threshold Condition Has Been Met	Potential Ransomware Attack

Detect the Symptoms of Malware in Your Environment

Using Lepide, you can set threshold alerts to help you identify the symptoms of malware in your key data stores. For example, if you experience a large number of file renames or failed access attempts in a very short period time, our solution can notify you of a potential ransomware attack in motion.

Automated responses to these alerts can be executed to speed up response time and address threats. Using custom script execution, you can shut down users, servers and take other actions to prevent malware from spreading.



Compromised User – Anomalous User Behavior

Lepide <datasecurityplatform@Lepide.com>

To: User <user@test.com>

You have received this alert because an **administrative user** in Active Directory **copied files containing sensitive data.** This user has never done this action before.

Gemma copied C:\Documents\Finance\Payroll.pdf at 24:07:2019, 09:30:10 AM in wkst.lpde.1.local

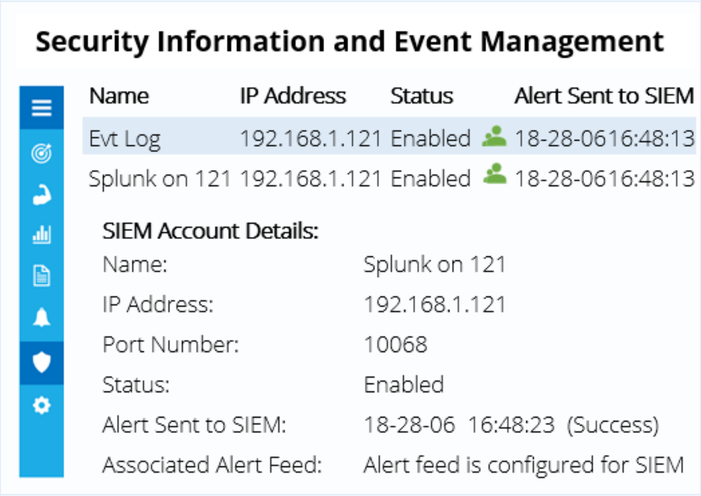
Thanks,
The Lepide Team

Improve Incident Response and Integrate with Your SIEM

Using our custom script execution you can automatically detect and respond to potential threats to your data security.

Lepide Data Security Platform can integrate with any SIEM solution to simplify your data breach response. Configure Lepide to send specific events to your SIEM and give more context to the raw audit data.

With a detailed and complete audit trail of all changes being made to your data, permissions and systems, Lepide can provide your Security Operations team with the information they need to investigate incidents faster and more efficiently.



Security Information and Event Management

Name	IP Address	Status	Alert Sent to SIEM
Evt Log	192.168.1.121	Enabled	18-28-0616:48:13
Splunk on 121	192.168.1.121	Enabled	18-28-0616:48:13

SIEM Account Details:

Name:	Splunk on 121
IP Address:	192.168.1.121
Port Number:	10068
Status:	Enabled
Alert Sent to SIEM:	18-28-06 16:48:23 (Success)
Associated Alert Feed:	Alert feed is configured for SIEM