HOW LEPIDE IS HELPING SECURE ACTIVE DIRECTORY

Our client is a large bank in the USA. We have happily accommodated their request for anonymity.

CASE STUDY

DISCOVERY

THREAT SURFACE AREA

The Company's Active Directory was identified as being in a bad state, with a high threat surface area.

RESPONSE

The company had no way to automate their detection of and response to attacks targeted at their Active Directory.

NOISE

The company were overly reliant on noisy Windows Event logs that lacked visibility and context.

ACTION

DEPLOYMENT

The Company chose to deploy Lepide Data Security platform and undergo a complimentary risk assessment.

SUPPORT

The Lepide support team did all the heavy lifting configuring the solution to the Company's exact requirements.

ALIGNMENT

Lepide set up the solution with the required reports, threat models, and dashboards configured for their Active Directory security.

OUTCOME

Lepide identified stale data, inactive users, open shares, and users with excessive permissions. Threat models were configured to detect and react to security threats like ransomware, privilege abuse and more. Lepide maintains a complete history of AD events with advanced searching so that the Company can perform easy, intelligent security investigations. As a result, the Company chose to become a customer of Lepide, and with ongoing support, are able to demonstrate reduced risk in terms of threats to Active Directory.

Launch Interactive Demo