cybereason | PRODUCT BRIEF

HISTORICAL DATA LAKE

Expand threat hunting capabilities against historical endpoint and mobile data

The Challenge

Targeted cyber attacks are increasingly difficult to identify across a large, complex enterprise network. This trend equates to woefully long dwell times for embedded cyber threats, meaning attackers are allowed to engage in command and control activities that escalate access to sensitive data.

Lack of visibility

In-house data storage has limits and is costly to expand

Lack of full visibility into attacks means security teams are unable to identify root cause and the scope of the threat

Threat hunting often involves complicated queries and tools

Tier III expertise is often required to successfully threat-hunt and build complex, GREP-based queries, leaving Tier I and II analysts underutilized.

Constrained SOC resources and skill sets

Most security teams struggle with a lack of Tier III expertise on staff; organizations require solutions that can augment SOC team capabilities to improve efficacy.

Full visibility in the entire attack sequence is vital to complete remediation of a cyber attack

End cyber attacks

To counter lengthy dwell times, it's essential that information security teams have the capability in place to proactively threat-hunt against historical endpoint data. Adversaries can obfuscate their activities and hide in the "noise" of log-based security alerts, but the aggregation of endpoint data that can be queried over time to uncover the anomalous chains of behavior that are indicative of a developing attack at the earliest stages. The ability to effectively query large historical data sets is essential to detecting earlier and remediating faster.

How it works

Historical Data Lake is available as an add-on package to Cybereason EDR. Endpoint data that is used to generate the high-fidelity detections is stored for a designated period of time, allowing security teams access to telemetry and threat data for either multi-month or multi-year terms. This expanded historical visibility allows security teams to proactively threat-hunt against endpoint telemetry data for deeper detection insights.

Multi-month data retention

30 Days

Ideal for small to midsize enterprises with a less-complex network and implemented controls

Less mature security programs likely have limited staff to support advanced threat hunting. The Cybereason UI enables Tier I analysts to perform Tier II and Tier III level activities with guided threat hunting and intuitive workflows for a duration of 30 days.

60-90 Days

Ideal for large enterprises and government agencies with complex networks and demanding threat hunting requirements

Maturing security teams with a dedicated SOC and Tier III staff benefit from a 60-90 day view of stored endpoint data for threat hunting use cases so the can proactively run queries to identify advanced malicious operations active in the environment.

Multi-year data retention

Full access to all endpoint data with no filtering for longer-term retention needs

Large network environments are fruitful ground for cyber adversaries to operate due to their complexity. Cyber attacks often slowly unfold over time, requiring the ability to view all threat activities over a period of years as opposed to days, weeks or months. Multi-year retention allows analysts to query threat data and endpoint telemetry against everything collected by the Cybereason sensor over that time period allowing analysts to uncover advanced threats and quickly respond.

Benefits:

- **Uncover latent threats** based on historical indicators of behavior
- Confidence in threat detection with the **best data retention in the industry**
- **Investigate and respond** over a longer retention period
- Threat hunt against richly **contextualized threat data** with the Cybereason platform
- **Understand the entire attack**, not just sporadic and unconnected alerts
- **Boost the scale** of current threat hunting operations

Cybereason Historical Data Lake offers a "search wide" and "go deep" approach to threat detection and response. Security teams can threat-hunt over a lengthy history, many assets, and a large amount of data. Once threats are identified, teams can focus resources into the in-depth investigation and response.