Organizations are facing a rise of multi-technique and multi-wave threats from financially-motivated criminals and nation-state actors. Once breached, attackers can linger in your network for anywhere from minutes to months. While real-time detection is critical, it often fails to correlate different parts of an attack, leading to gaps in detection. Similarly, when new threat intelligence is received, correlation is limited. Answering the question, "Were we ever exposed?" is akin to finding the proverbial needle in a haystack - forcing companies to tackle big data challenges rather than focus on the business. Cybereason Threat Hunting lets you and your analysts turn the tide on attackers with syntax-free threat hunting, revolutionary data retention, and more.

**HUNT THREATS INTUITIVELY**

Your analysts need the tools to quickly stop and easily hunt for threats. Cybereason's intuitive user interface gives analysts a syntax-free tool to investigate events and free-form, hypothesis-driven hunting. By eliminating the need for complex query building and debugging, SOCs are able to shrink query development time. With Cybereason Threat Hunting, L1/L2 analysts are able to perform advanced analysis that's typically only done by L3s. Analysts can easily filter and pivot between query responses to bring malicious behavior into full focus. The user interface is designed with a highly visual approach to facilitate faster exploration and resolution of hypotheses.

**DATA RETENTION REVOLUTIONIZED**

Attackers spend an average of 197 days in the network before being detected. To counter this, effective security tools must support varied investigation time periods. With Cybereason Threat Hunting, analysts can perform automated and proactive threat hunting across time periods for an unmatched ability to discover and analyze threats.

Cybereason delivers industry-leading data retention for any custom time period on Windows, Mac, and Linux endpoints. Your team can analyze security data over large periods of time - days, months, or even all data ever collected.

**CYBEREASON EDR**

Cybereason EDR uses advanced behavioral analysis and machine learning techniques to recognize relationships between multiple events and determine if they are part of a single attack. The full attack scope is automatically correlated into a single threat package, called a malicious operation or Malop™.
THE MALOP

Malops give analysts a unified view of the triggering event, detection category, root cause, affected endpoints, related processes, and the connections between endpoints. They are contextualized with a timeline of all events, benign or malicious, and shorten time-to-triage from hours to minutes. Analysts can easily make additional queries with Cybereason’s syntax-free approach to investigation. L1 analysts are empowered to perform L2/L3 tasks, including recommended response actions for safe remediation. Analysts can perform investigation on all data, (processes, connections, etc.), malicious or benign, that surrounds a Malop looking back over 30 days. All Malop details are retained for one year.

SUPPORTED VERSIONS

EDR
MALOP INVESTIGATION & AUTOMATED THREAT HUNTING
30 days for all data related to a malicious operation;
12 month malicious data

HUNTER
PROACTIVE, ADVANCED, THREAT HUNTING
Retain all data for 7, 15, 30, 60 or 90 days

INFINITY
HISTORICAL ANALYSIS & AUDITING
Retain all data access for up to 3 years

CYBEREASON HUNTER

Cybereason Hunter takes it a step further with an unparalleled proactive threat hunting experience that serves as the foundation of a SOC’s evolution to a proactive threat hunting approach. Cybereason delivers easy-to-master, real-time access to every raw data point collected, with a retention span ranging from 7 to 90 days.

With options to customize and automate, Cybereason Hunter maximizes the ability to integrate threat hunting into the overall workflow of your SOC team, regardless of size or maturity.

CYBEREASON INFINITY

With Cybereason Infinity, your SOC obtains a unique level of security and insurance. Cybereason Infinity supports analysts querying historical data and, if necessary, replaying events with infinite retention. Infinity opens up a completely new cyber security vantage point to common-yet-challenging problems like audits, insider threats, and validating simple or complex IOCs. Analysts can go back in time to answer key questions like:

» Did this threat ever exist in our environment?
» What actions occurred on this machine in that time period?
» Has this behavior occurred before in our environment?

Cybereason Infinity is offered in levels, each enabling a larger number of historical queries and replays.