cybereason

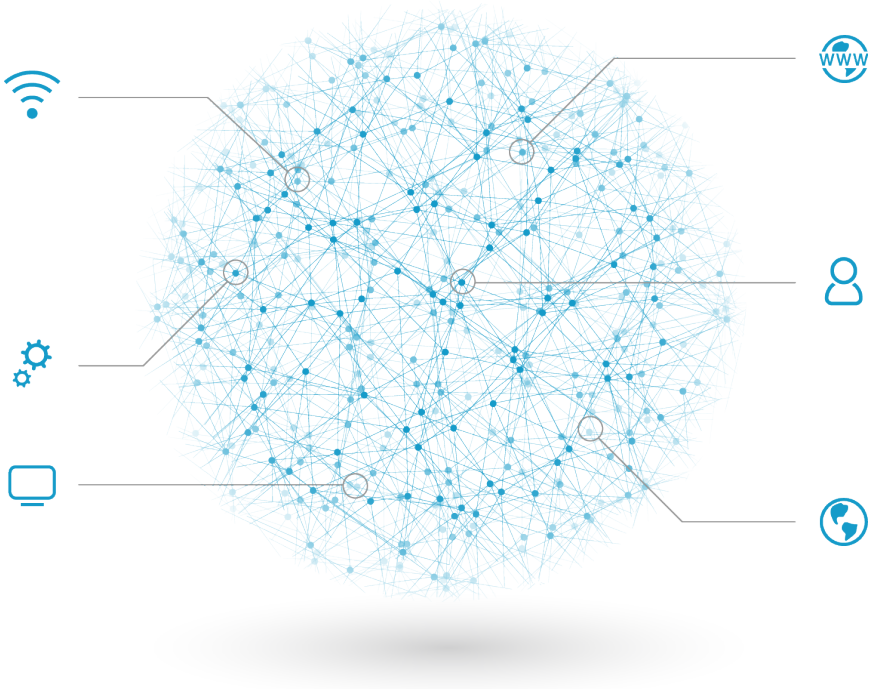
THE TECHNOLOGY BEHIND THE HUNTING ENGINE

Defending a complex IT ecosystem, means understanding the activities, relationships and roles of an ever—growing and diverse set of people and things—knowing what is good and identifying what is bad—protecting what you can, detecting attacks as they occur and responding before the damage is done.

GROUP DEFENSE: COMPLETE PROTECTION AGAINST ATTACKS

The Cybereason Hunting Engine is a purpose built, in-memory data store that performs streaming, adaptive entity correlation. The Hunting Engine pulls in millions of pieces of data every second, and maintains tens of millions of relationships between the data.

The Hunting Engine is a fast, scalable graph database. A graph uses nodes, edges (or links) and properties to represent data and the relationships between them. It runs in-memory rather than retrieving data from disk. Operations in memory happen thousands of times faster than disk requests, which allows the Hunting Engine to answer queries much more quickly. Modern computing also makes large amounts of memory available cost effectively, so that large environments can be represented in the graph on a single machine, and multiple machines can work together to establish and represent cross-database relationships. This allows the Hunting Engine to scale to the largest of environments.



DETECTING AND VISUALIZING MALICIOUS ACTIVITY

The Hunting Engine continuously adapts and asks tens of thousands of questions every second about the data it receives to keep an ever-evolving, in-memory, real-time picture of your environment.

For example, every element that Cybereason collects—all the users, machines, processes, network connections, auto-runs and more—is fed into the Hunting Engine. The relationships between the elements are represented in the Hunting Engine using a link (or an edge). These nodes are continuously added as more and more data is fed into the Hunting Engine, and more relationships are established.

If you want to understand all the processes a particular user has executed, the Hunting Engine makes it easy, since there is a link between that user and every process the user has run. Similarly, if we want to understand all the connections made by a particular process, this is also simple because there is a link between the processes and all its network connections.

Past technologies have struggled to meet this challenge due to scalability issues. Relational databases in particular have proven to be inadequate, and many have made attempts to solve the problem using technologies like Hadoop®, columnar databases and other NoSQL engines. In each case, these approaches did not scale due to issues with data ingestion, analytic power and storage retrieval.

The Hunting Engine is the first technology that can ingest, organize and analyze data in a way that identifies malicious activity and visualizes it in a coherent way—to scale.

The Hunting Engine does not simply store collected data. It uses preconfigured detection models to hunt for malicious activities and tools, tactics and procedures (TTPs) attackers use while executing their hacking campaigns. You don't need to spend weeks configuring and tuning rules. You can start detecting threats immediately.

CYBEREASON MALICIOUS ACTIVITY MODELS

The models cover the entire attack lifecycle, allowing detection of infiltration, command and control, lateral movement, privilege escalation and damage. In order to detect incidents most effectively, Cybereason defines and organizes the data it collects and analyzes:

Facts are the raw information collected by the Cybereason Sensors. Facts are detailed telemetry information used to determine changes in processes, users, machines, memory, registry and any other events.

Evidence is a collection of facts that the Cybereason Hunting Engine categorizes as interesting, anomalous, or suggesting that an attack is underway. Without additional incriminating data, though, evidence does not justify further investigation.

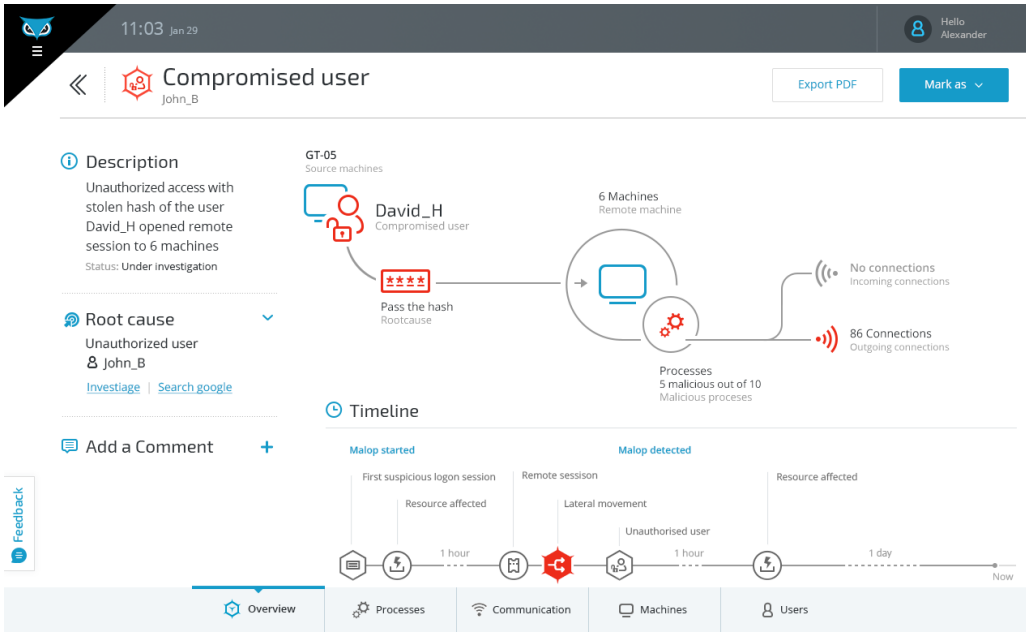
Suspicions are activities that the Hunting Engine identifies as more likely to be malicious. Sometimes these are activities that are independently suspicious, other times they are caused by aggregating multiple related pieces of evidence. The threshold for evidence to become a suspicion is deliberately low to minimize the likelihood of missing an attack.

A Malicious Operation or "Malop" is a complete story of a cyber attack: the full context analysts need to identify a security incident in their organization. A Malop is a collection of related suspicious activities that are very likely part of a security incident. A Malop is designed to minimize the time analysts spend on investigating benign activities or false positives.

PROVIDING IMMEDIATE, FULL ATTACK CONTEXT FOR INVESTIGATION

Because the Hunting Engine maintains relationships between all the pieces of data it collects, a Malop combines, in one view, all the related data elements an analyst can drill down into to determine exactly what happened before and after the Malop triggered an alert. Alternatively, if analysts are investigating an alert from another tool, and searches for a given user, machine, process or network session, they can quickly build a full picture to understand whether a suspected issue is truly malicious or benign. If the activity really is malicious, analysts can build a picture of all related elements.

If the attacker triggers a single alert, the Hunting Engine creates the full story of what happened and when, at all stages of the attack lifecycle.



DISRUPT

THE ADVERSARY

LET THE HUNT BEGIN

Cybereason was founded in 2012 by a team of ex-military cyber security experts to revolutionize detection and response to cyber attacks. The Cybereason Malop Hunting Engine identifies signature and non-signature based attacks using big data, behavioral analytics, and machine learning. The Incident Response console provides security teams with an at-your-fingertip view of the complete attack story, including the attack timeline, root cause, adversarial activity and tools, inbound and outbound communication used by the hackers, as well as affected endpoints and users. This eliminates the need for manual investigation and radically reduces response time for security teams. The platform is available as an on premise solution or a cloud-based service. Cybereason is privately held and headquartered in Boston, MA with offices in Tel Aviv and Tokyo.