cybereason

Cybereason Detection and Response Platform

The Cybereason real-time attack detection and response platform brings military-grade defense to enterprises, providing automated detection, complete situational awareness and a deep understanding of attacker activities.

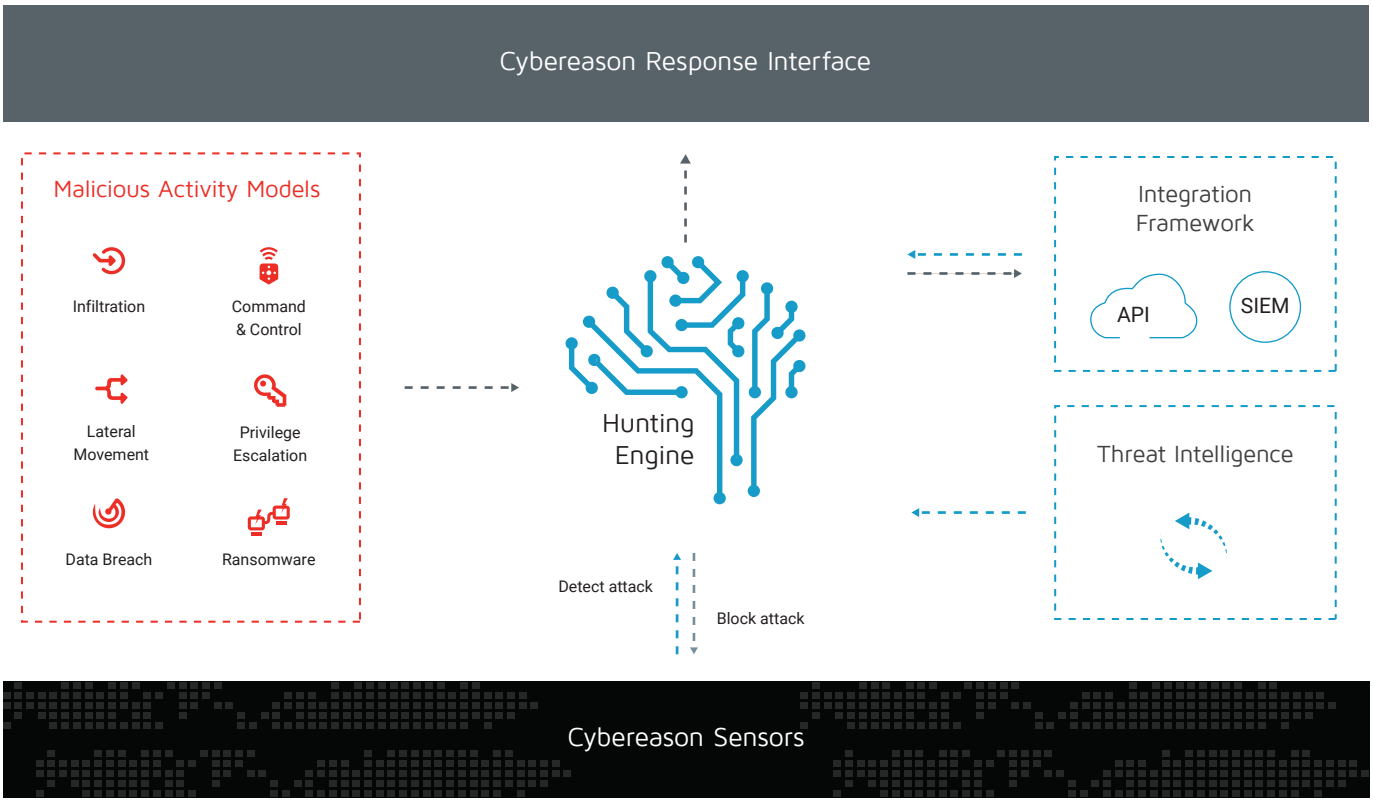
Automatically detects attack campaigns

Provides detailed attack information

Empowers security teams to be elite defenders

Cybereason automatically detects malicious activity and presents it in an intuitive way, provides end-to-end context of an attack campaign and deploys easily with minimal organizational impact. Organizations are able to deploy and can start detecting within 24-48 hours.

With continuous 24/7 monitoring, Cybereason provides complete situational awareness across your entire IT environment, allowing you to answer the question, at any given moment, “am I under attack?”



Gain an end-to-end view of malicious activities

Cybereason Sensors continuously collect detailed information from all end user machines and servers across an enterprise. The Hunting Engine then performs centralized, in-memory analysis to identify all malicious activity, such as the initial infiltration, command and control, privilege escalation and lateral movement.

The Cybereason Response Interface graphically represents the timeline of these activities and provides visibility into the root cause, affected endpoints and users, related communication and the tools used. Cybereason then makes the information available for search and investigation by security analysts.

Cybereason Sensors

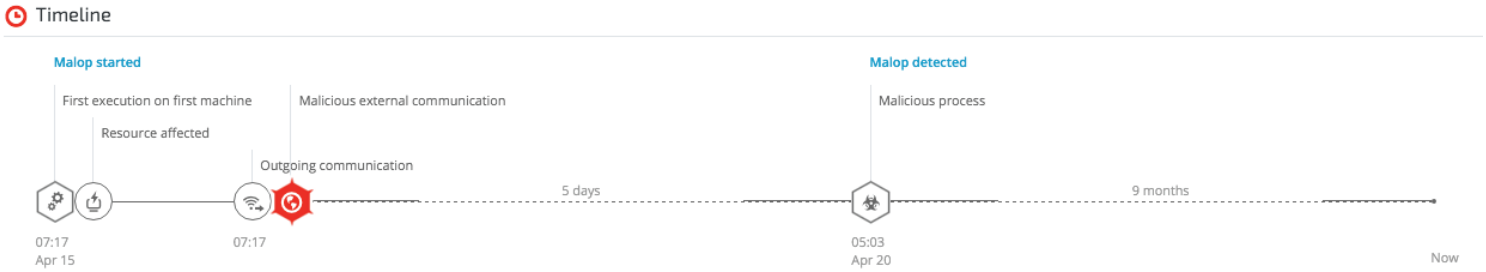
Cybereason Sensors, our unique data-gathering agents, are deployed on endpoints and servers and collect data from across your environment. The Sensors deploy with zero impact on productivity. The Cybereason Sensors' unique technology runs continuously in user space, making it impossible to crash the system, while providing full visibility into all activities.

The Hunting Engine

The Hunting Engine comes pre-built with a wide range of detection models designed to identify known and unknown elements of an attack and new attack techniques, with no up-front configuration or tuning. This means that you can start detecting and responding to security threats as soon as the Hunting Engine receives data from the Sensors.

Malicious Activity Models

Cybereason comes preconfigured with a library of models that look for malicious activities and tools, tactics and procedures 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 cover the entire attack lifecycle, allowing detection of **infiltration, command and control, lateral movement, privilege escalation and damage**.



Cybereason Response Interface

The Cybereason Response Interface uses the information collected by the platform to tell an easy-to-understand visual attack story. The Cybereason Response Interface incorporates:

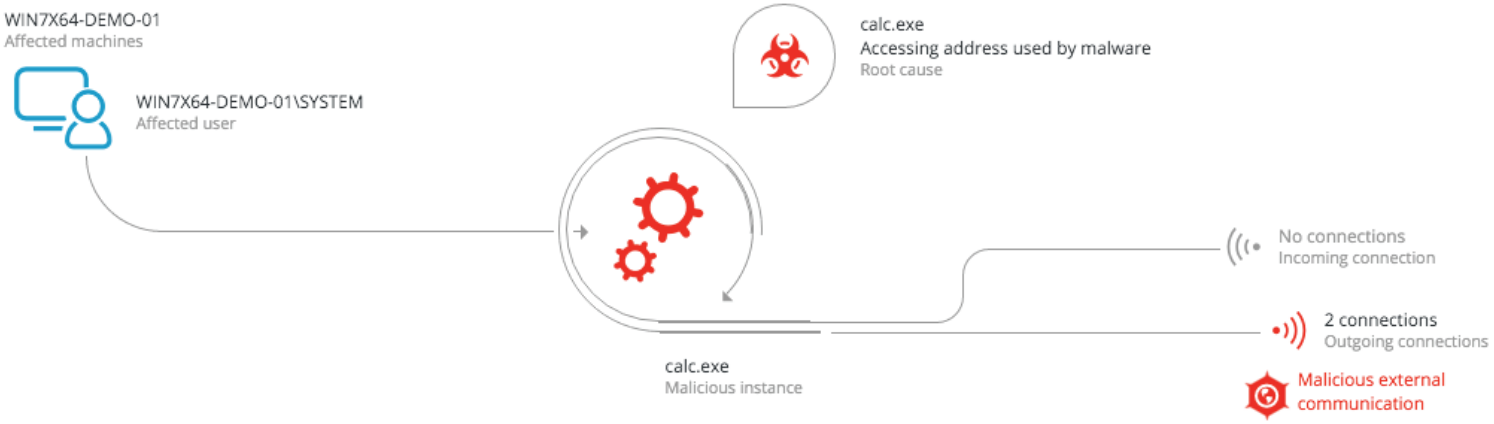
Malicious Operations Dashboard Helps you understand the state of your environment at a glance. Provides insight into what active malicious operations are underway and how pervasive they are. Allows exporting of attack information to communicate with executives.

Malop Visualizer Automatically visualizes connected malicious activities detected by Cybereason in real time. Showcases the attack's scope, the timeline of what happened and the picture of the evolving situation.

Investigation Workbench Provides a detailed attack context of the adversary's operation for investigators and researchers. Allows you to pivot across affected users, network connections, machines and processes to track the attacker's activities, tools and techniques.

Single-Click Guided Remediator Automates the process of containing and eradicating threats, allowing you to kill processes, quarantine files and delete registry keys.

Attack Blocker Stops threats from causing damage to your business by automatically blocking process execution and preventing network communication.



Cybereason Live Threat Intelligence

Cybereason Live Intelligence creates actionable intelligence that is built into the platform to automatically detect malicious operations. The expert team monitors adversary activities across the globe to get early warning of imminent danger.

Cybereason's unique behavioral approach to identifying malicious operations means that rather than a binary "blacklisting" and "whitelisting", Cybereason uses threat intelligence as just one factor in evaluating whether activities are malicious enough to investigate.

Cybereason Active Monitoring Team

Cybereason has assembled a corps of military-grade security experts from a range of military, academic and commercial backgrounds. The team has decades of first-hand experience dealing with some of the world's most sophisticated attacks. Collectively, they have built security operations centers for Fortune 500 companies, and developed the incident response plan for one of the Big Four professional services organizations. The team has extensive experience developing and delivering security training for hundreds of organizations, ranging from small security teams to the largest international organizations.

Get specific, actionable notifications from the Cybereason Active Monitoring Team. We can provide your team with:

Active monitoring Cybereason experts monitor and analyze malicious activity in your environment. When confirmed malicious activity occurs, Cybereason notifies you and tells you how to eliminate the threat.

In-depth investigation For potentially serious issues, Cybereason experts will drill into the data and give you independent advice on whether to declare an incident and develop a response plan.

Your security team also gets full access to the Cybereason platform, enabling validation and additional investigation of Cybereason's findings. This gives you the expertise of managed monitoring, while maintaining full control of your platform and data.

Cybereason was founded in 2012 by a team of ex-military cyber security experts to revolutionize detection and response to cyber attacks.

Cybereason is privately held and headquartered in Boston, MA with offices in Tel Aviv, Israel and Tokyo, Japan.

cybereason