cybereason
malops protection

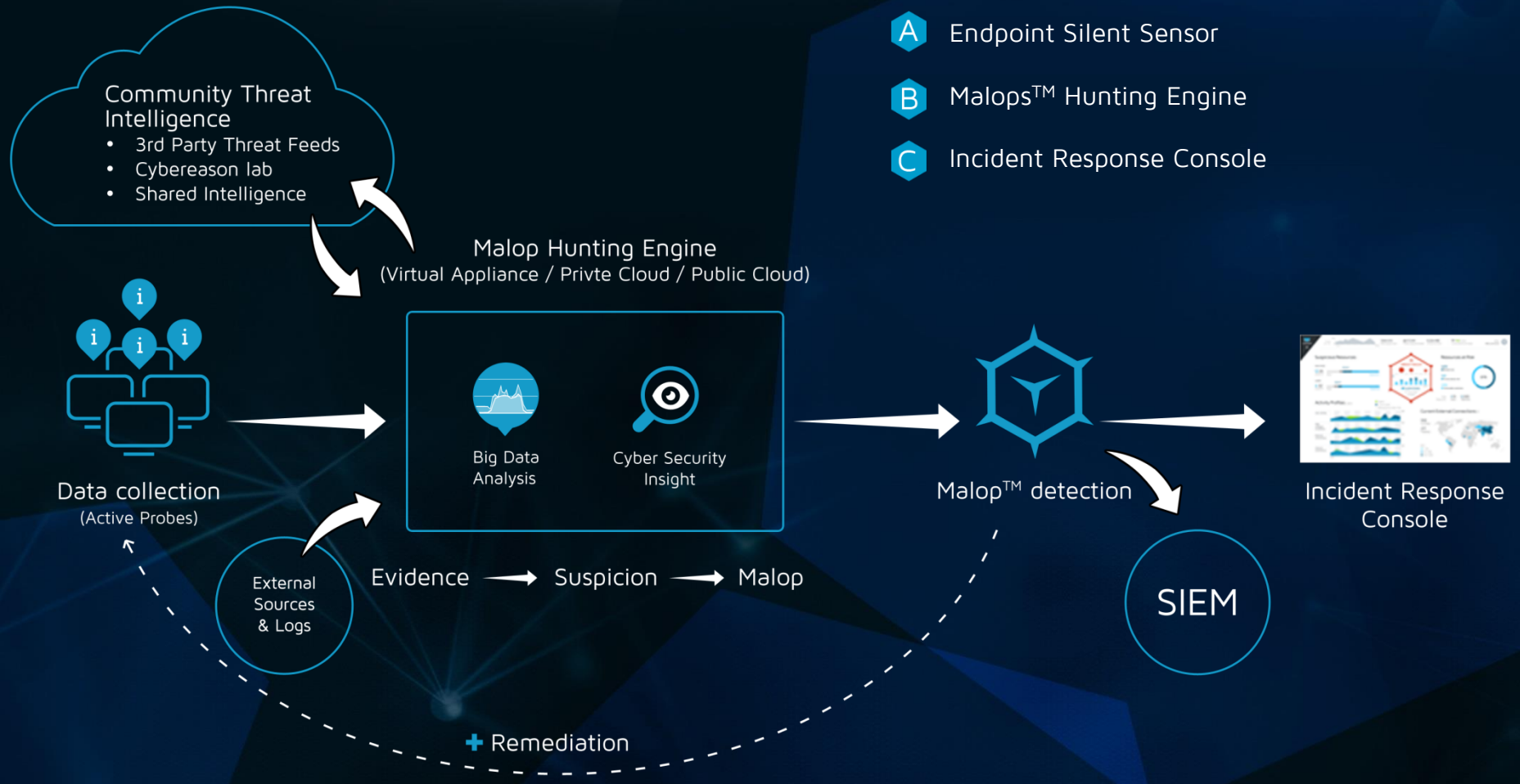
Cybereason Platform Architecture

Overview

Cybereason's Endpoint Detection and Response platform reveals cyber-attacks in real time and accelerates investigation and response.

Cybereason Platform is comprised of three components:

- A Endpoint Silent Sensor
- B Malops™ Hunting Engine
- C Incident Response Console



cybereason
malops protection

A

Endpoint
Silent Sensor

Cybereason Endpoint Silent Sensor enables accurate and broad data collection while maintaining business continuity.

The Silent Sensor collection includes:

- Process actions
- File access information
- Network events
- Configuration changes
- User information and behavior, and more.

Cybereason's Silent Sensor runs as a service in the user space of the operating system, leveraging multiple existing and custom-built mechanisms of the operating system to discover events and collect them. Contrary to kernel-level endpoint deployment, Cybereason's silent sensor maintains user experience, machine stability and network bandwidth.

Zero Interference with User Experience

100%	2%	50m	1mb	0
User Experience Maintained	CPU Consumption	Memory Usage	Per day per endpoint	System Crashes

B

Malops™
Hunting Engine

Cybereason platforms hunts for malicious operations, Malops, through a unique set of analytics aimed to identify signature -based, known attacks as well as unknown attacks.
Malops are identified based on behavioral as well as community -sourced indications of compromise and threat feeds.

COMMUNITY INTELLIGENCE SERVER

The Community Intelligence Server is Cybereason's cloud-based aggregation of community threat intelligence. The Community Intelligence Server consumes multiple types of information:

- 3rd party threat intelligence feeds
- Security intelligence originated from Cybereason labs
- Cross-customer profiling of emerging threats

Each data point, collected by the sensors, is profiled and reviewed by the community intelligence server in real time. This enables an immediate identification of known malicious activities and also implicates other activities that have not yet been identified as a known threat.

CONTINOUS MONITORING and RESEARCH

Data received from the endpoint sensors is signed and stored for continuous research and analysis. The data then flows through the in-memory graph where behavioral models based on machine learning search for anomalies and identified risks.

cybereason
malops protection

IN MEMORY GRAPH

The Malops Hunting Engine's patent pending in-memory graph processes 8 million events per second and builds an accurate picture of a cyber-attack in real time.
It analyzes key elements (processes, machines, memory users, network, files, registry, etc.), reviews the elements' profile (e.g. known benign, known malicious, unknown, etc), looks for anomalies and hunts for indicators of malicious operation.

LINKING TOGETHER MALICIOUS ACTIVITIES

The Malops Hunting Engine looks for interconnected anomalies and risk indicators (collectively, "evidence"). When sufficient evidence is found, Cybereason reports the detection of a malicious operation: a Malop.

Incident Response Console

All Malicious operations, Malops, are visually presented in Cybereason's Incident Response Console, specifically designed to portray the storyboard of a detected cyber-attack. The console also facilitates communication between security teams and management for effective decision making.

SIEM Integration

Malops detected by Cybereason can be sent to a SIEM or any event management system.

Technical Specifications

Cybereason is a software solution delivered as an on premise virtual appliance to your data center or as a private or public cloud implementation.

On the backend, the server uses MongoDB as a NoSQL big-data data store. The innovative implementation of this in-memory graph allows a single CPU core to handle up to 5000 Silent Sensors. Therefore, an 8-cpu (32 cores) server can handle 80,000 Sensors on a single machine.

About Cybereason

Founded in 2012 by elite members of the Israeli intelligence Corps specializing in cyber security, Cybereason's mission is to help organizations deal with the growing problem of complex hacking operations. Cybereason's team of experts in cyber security and data science brings a new detection and response approach to security.