CYREBRO SOLUTION OVERVIEW

WELCOME TO CYREBRO

CYREBRO pioneered the first online, managed Security Operations Center (SOC) Infrastructure with the mission of bringing enterprise-grade cybersecurity to businesses of all sizes, ensuring fast and efficient responses to cyber threats and their mitigation. End customers benefit from a first-of-its-kind, complete SOC Infrastructure offering with advanced 24/7/365 capabilities, including threat intelligence and hunting, forensic investigation, and incident response.

SOLUTION OVERVIEW

To provide a state-level, managed SOC Infrastructure, CYREBRO utilizes the knowledge and expertise of Israeli cyber experts, and the ongoing wisdom of the masses to teach and operate the ML-based detection, investigation, and response that is the "CYREBRO Brain".

All of this is delivered using CYREBRO's online, interactive SOC Platform. The SOC Platform integrates all your security, network, infrastructure, and cloud logs into one central command, and provides complete clarity, insights, and real-time actionable steps to mitigate and remediate cyber threats.

THE OFFERING

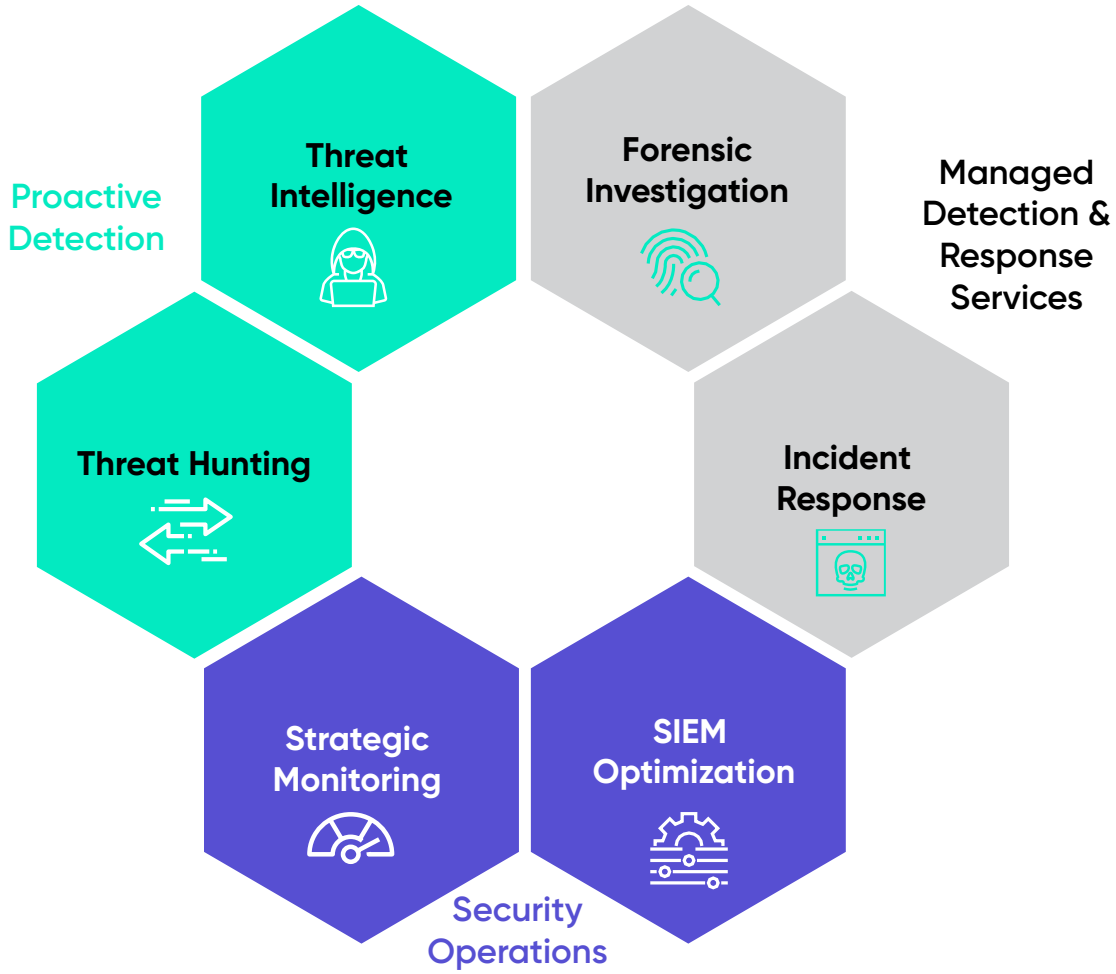
- Data lake and correlation engine capabilities
- Over 1,500 ready-made, unique and proprietary detection algorithms, written, tested, and executed over years of real cyber operation and detection experience
- Next-generation SIEM
- In-house automation and orchestration capabilities
- In-house cyber threat research
- In-house cyber threat intelligence
- Log collection
    - We support log collection across multiple platforms and environments covering hundreds of leading log types and supporting systems
- Proactive threat hunting
- Data ingestion validation and enhancement*

Additionally, CYREBRO empowers the client's security teams by providing 24/7/365:

- Advanced monitoring and investigation capabilities
- Digital forensics and incident response

** CYREBRO does not provide "hands-on" integration support. For any integration requirements, please see the "CYREBRO certified integrator" list. Only official and certified integrators will be supported by CYREBRO Labs*

SOC CAPABILITIES



SECURITY OPERATIONS

STRATEGIC MONITORING & DETECTION

CYREBRO's approach to monitoring, detecting, and responding, is based on continuously learning, improving, and evolving our detection algorithms. It involves the continuous 24/7 live monitoring of organizational assets, networks, and systems, while constantly learning the evolving threat landscape and understating risks and their use cases across the globe in near real-time. This works in parallel to constantly adapting to clear and relevant alerts. CYREBRO is specifically designed to utilize ML and internal cyber experts across the millions of machines connected to it, to assist clients in mitigating security risks and effectively operating their security infrastructure.

The goal is to provide the organization with a clear, analyzed, and real-time view of its security posture, enabling it to make informed data driven decisions about risk management and resource allocation.

OPTIMIZATION

This refers to the process of ever improving the effectiveness and efficiency of CYREBRO's SOC Platform. This involves fine-tuning the system to ensure that it is collecting the right data, analyzing it effectively, and providing actionable insights.

The goal of the optimization is to improve the accuracy and speed of threat detection, reduce false positives, and enable faster incident response times.
This is the live, ongoing process within the "CYREBRO Brain", based on a combination of ML capabilities, statistics, correlations, and trends with a highly skilled, highly experienced cyber team.

Optimization includes:

- Refining alerts / rules: By fine-tuning alert rules, organizations can reduce the number of false positives generated while ensuring that important security events are not missed.
- Reducing noise: By filtering out unnecessary data, such as known benign traffic or redundant log entries, CYREBRO can focus on the events that are most relevant to security.
- Increasing data visibility: By collecting and analyzing a broader range of relevant event data, including data from cloud environments and endpoints.
- Automating response: By automating incident response workflows, CYREBRO reduces response times and improves the efficiency of the teams.
- Regular tuning and maintenance: Including updating correlation rules, ensuring data ingestion is in accordance with the updated scheme and patching core infrastructure.

PROACTIVE DETECTION

THREAT INTELLIGENCE

The role of the threat intelligence element within CYREBRO is to provide relevant and actionable intelligence related to potential security threats, and to constantly correlate relevant indicators and potential threats, within every relevant technology connected to CYREBRO.

Primary responsibilities include the following:

- Collection of threat data: Collecting information from various sources such as internal security logs, external threat intelligence feeds, and open-source intelligence.

- Analysis of threat data: Analyzing the collected data to identify potential threats, attack patterns, and indicators of compromise (IOCs).

- Enhancing threat data: A process of enrichment of the data pool in-order to add context, relevance and actionable items for each IOC.

- Sharing threat intelligence: CYREBRO disseminates the threat intelligence reports, alerts, and advisories to the appropriate stakeholders within CYREBRO, including the incident response team and security analysts.

THREAT HUNTING

CYREBRO's threat hunting process is a proactive approach to identifying potential cyber security threats which involves searching for indicators of compromise (IOCs) and other anomalous activity that may have otherwise gone unnoticed by traditional security measures.

It encompasses the "wisdom of the crowd", lessons learned, derived from past and ongoing cases together with vast experience which was accumulated over the many years of operation in both the private as well as the governmental sectors.

The process of threat hunting involves processing vast amounts of data from various sources. The data is then analyzed to identify patterns, anomalies, and potential IOCs that may indicate the presence of a security threat. This process is often conducted or guided by skilled security analysts who have in-depth knowledge of the attack life cycle and methods of operation.

By proactively identifying potential security threats, CYREBRO's threat hunting capability enables organizations to respond quickly and effectively to security incidents, reducing the risk of data loss, financial damage, and reputational harm. It also allows organizations to gain a deeper understanding of their security posture and identify areas where additional security measures may be necessary.

Overall, CYREBRO's threat hunting capability provides a proactive approach to cybersecurity that goes beyond traditional security measures, helping to ensure that potential threats are identified and neutralized before they can cause harm.

MANAGED DETECTION AND RESPONSE SERVICES

INCIDENT RESPONSE

CYREBRO's incident response provides organizations with a structured and efficient approach to managing security incidents. Our unique teams of experienced incident responders, with state and private level experience, have conducted hundreds of IR cases across the globe, of all shapes, sizes, and level of complexity. CYREBRO follows a well-defined process that involves preparation, identification, containment, analysis, eradication, and recovery in-order to achieve optimal results in a timely manner and a forensically sound fashion.

CYREBRO, in consultation with the customer, will classify the incident following the severity levels. If appropriate, the IR team will establish and provide to the client a communications protocol that limits communications related to an incident to the appropriate group, provides for proper labeling of documents and provides for inclusion:

- Determining, developing, and implementing, an appropriate strategy for responding to an incident
- CYREBRO will lead efforts to investigate, contain, and resolve the incident
- Conducting the post-incident analysis
- Participating in the review and closure of an incident
- Facilitating the creation of operational procedures
- Reviewing and updating the customer IRP as needed

In the case of an immediate threat, such as an ongoing live cyberattack on the organization, the response team is available 24/7 to lead in blocking, containment, and remediation of the event.

- Each IR activation will include a full "postmortem" detailed report on the event
- CYREBRO will conduct first response online and will manage the incident with client's POC until closing of the incident

DIGITAL FORENSICS

CYREBRO's digital forensics provides organizations with a thorough and efficient approach to investigating and analyzing digital evidence related to cybersecurity incidents. In our process, expert digital forensics analysts follow a rigorous procedure that involves acquisition, preservation, analysis, and reporting which remains "forensically sound".

In the acquisition stage, CYREBRO uses advanced tools and techniques to gather digital evidence from various sources while taking steps to preserve the integrity of the evidence to ensure that it is admissible in court, if necessary.

Once the evidence has been acquired and preserved, CYREBRO analyzes it to determine the cause and extent of the security incident. CYREBRO uses a range of forensic techniques, including data carving, memory analysis, and timeline analysis, to identify potential indicators of compromise and reconstruct the sequence of events leading up to the incident.

CYREBRO prepares a detailed report outlining the findings of the investigation, including a description of the incident, the methods used to acquire and analyze the evidence, and any potential legal or regulatory implications. We also provide recommendations for improving the organization's security posture and preventing similar incidents from occurring in the future.

Overall, CYREBRO's digital forensics provides organizations with a reliable and effective way to investigate security incidents, preserve digital evidence, and analyze data to identify potential threats.

HOW DOES IT WORK?

CYREBRO SOC PLATFORM

Watch a walkthrough of the CYREBRO SOC Platform here.

WATCH NOW

CYREBRO ALERT LIFECYCLE

1

Collectors are data gateways that gather data (logs sources from cloud, on-prem, endpoints, machines, etc) from clients' environments and send it to CYREBRO.

2

The data is then parsed on the SIEM, a dedicated cloud environment. Meaning the data is broken down into a readable format, ie the source IP and destination IP.

3

The data then enters the data lake where it is mapped and normalized. This is to better understand what the data is telling us based on parsing (i.e. failed log-in attempts). Here, CYREBRO begins looking at "events of interest" from all of the data received.

4

The "rule engine." AI detections kick inby continuing to look at the parsed data to identify "events of interest". This uses a combination of AI technology, rules, and correlations. Events are then correlated to create corresponding offenses.

5

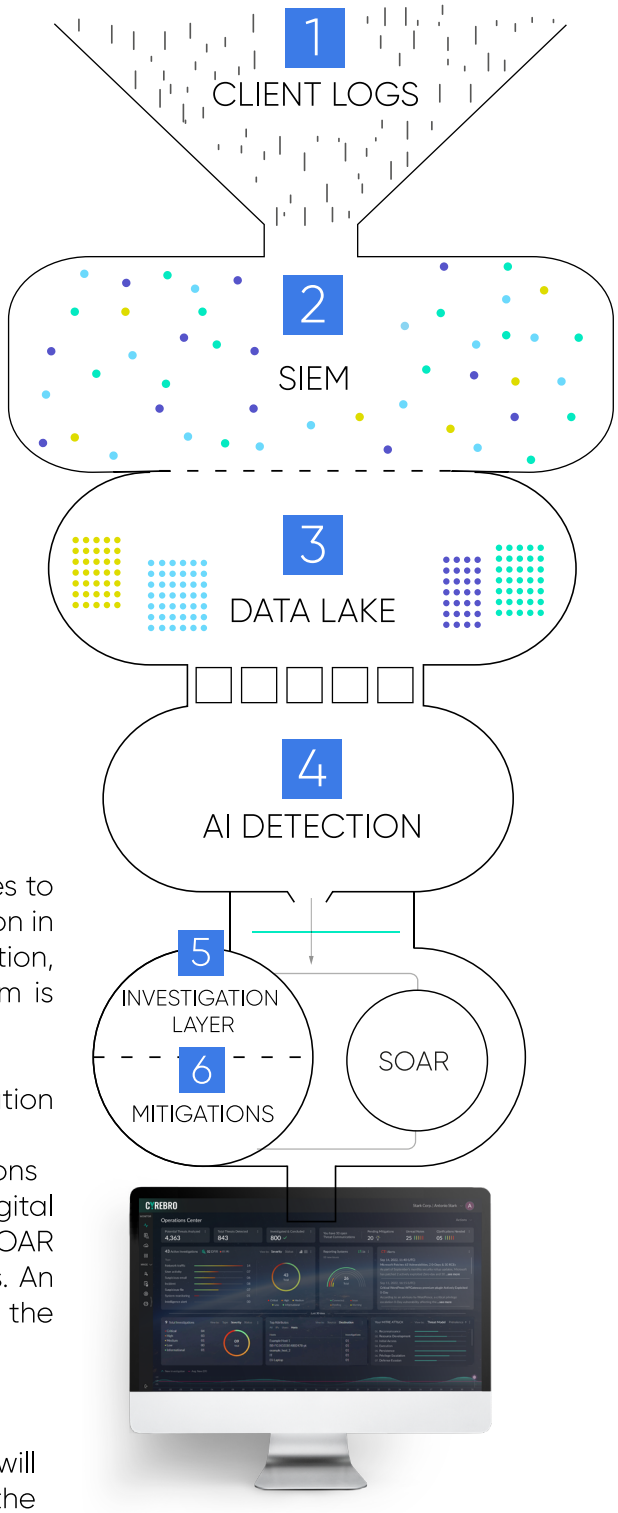
Next, the SOAR correlates and aggregates the offenses to determine the attack story, and creates an investigation in the CYREBRO Platform. Throughout the detection, investigation, and mitigation stages, the SOAR system is responsible for:

- Creating an attack story
- Automatically enriching the data (i.e., geolocation resolving for IP addresses, known bad IPs, etc.)
- Automatically investigating and closing investigations

The strategic monitoring, incident response, and digital forensics teams work in conjunction with the SOAR technology to review, close, or escalate investigations. An alert is generated in the CYREBRO Platform for the end-user (client) with detailed information

6

After investigating, the monitoring and DFIR teams will deliver mitigation steps to the client directly in the CYREBRO Platform. These steps come in the form of recommended remediation steps and actions required from the client to mitigate the incident.



MONITORING AND DETECTION

WHAT DOES CYREBRO MONITOR & DETECT?

CYREBRO monitors all your business systems and security tools, collects, and analyzes the data, and interprets suspicious events with an attacker's mindset. Strategic monitoring and detection are achieved through a combination of proprietary detection and response algorithms, plus our team's extensive knowledge of various monitoring methodologies.

CYREBRO creates its own custom, proprietary rules, instead of using generic, out-of-the-box rules. Detection and response algorithms are created based on specific attributes, not specific systems, so CYREBRO is able to detect a wide range of threats, covering the attack landscape. Detection attributes are based on the MITRE framework, CYREBRO incident response cases, and our threat research.

CYREBRO clients benefit from the "wisdom of the crowd," meaning that the rules created for a single client incident will be applied proactively to the entire client base.

CYREBRO DETECTION

Rule Logic

Rules are created to ingest two different data streams. The first are raw events coming from non-security tools and critical assets, and the second are alerts sent by security tools. All types of rules created fall into these categories:

- Single event rule (based on an alert from one system)
- Aggregation rule (multiple events from one system)
- Correlation rule (multiple events from multiple systems)
- Machine learning and AI rules – Conclusions reached by the machine after learning mass data and solidifying statistics and outcomes

CYREBRO MONITORING

CYRBERO has three categories of alerts:

1. Hunting leads - alerts created for the threat hunting team to proactively detect threats

2. High fidelity alerts - high risk, high severity alerts that trigger CYREBRO investigation

3. Attack stories - a chain of behavior aggregated by hunting leads and/high-fidelity alerts

CYREBRO monitors and responds to all alert types, but the alerts that are visible in the SOC Platform consist of high-fidelity alerts and attack stories. Instead of escalating every benign alert, CYREBRO shows you what needs to be dealt with, and how our security analysts are dealing with it, instead of overwhelming you with countless harmless alerts. System and network activity can occur as part of normal network or as adversarial activity. Therefore, events and alerts should not be viewed in isolation, but as part of a chain of behavior that can lead to other activities, based on the information obtained.

GETTING STARTED

PLATFORM INTEGRATIONS

Event collectors are deployed to collect event data. Systems and log sources must be integrated only by a certified CYREBRO integrator. CYREBRO will provide a list of certified integrators to work with.

The following is an online list of integration types that CYREBRO supports - https://www.cyrebro.io/integrations/. It may be amended from time to time.

Platform integration is performed by a third-party certified CYREBRO Integrator.

**Customized plugins may be developed per request.*

Machine Requirements: A lightweight machine is required to serve as an event collector.

ADDITIONAL SERVICES

Managed EDR

CYREBRO offers managed EDR solutions, whereby CYREBRO configures, maintains, and manages the policy of the EDR, and it is accessible to clients through the CYREBRO Platform.

This solution includes:

Deliverable	Description
24x7x365 Monitoring & Response	Real-time monitoring and active threat hunting to detect and respond to security incidents.
Threat Intelligence	Both manual and automated processes of threat intelligence covering countless sources and knowledge bases including CYREBRO's knowledge of the crowd aggregation.
Forensic Investigation & Malware Analysis	In-depth analysis of security incidents to track an attack's origin and methods and identify the specific type of malware used.
Fleet Management	Easy management and monitoring of the entire fleet of endpoints, including the ability to deploy, configure, and update agents and perform remote actions to contain and remediate security incidents.
Policy Management	Configuration and enforcement of security policies across the entire fleet of endpoints, including creating and managing custom policies, assigning different policies to different groups of endpoints, and monitoring compliance in real time.
Users & Roles Management	Management and monitoring network access, including creating and managing custom roles, assigning different roles to different users, and monitoring user activity in real time.
Agent High-level Troubleshooting	Diagnosis and resolution of issues with agents, including the ability to review agent logs, troubleshoot common issues and perform remote actions to resolve issues.

Allow / Block List Management	Management and monitoring network access, including creating and managing custom allow/ block lists, assigning different lists to different groups of endpoints, and monitoring compliance in real time.
Device Control	Ability to set USB rules to control which devices can access the network, including the ability to block or allow specific devices based on their type and set rules for different groups of endpoints.
Version Updates	Automatic deployment of updates and patches to all endpoints, ensuring that the organization's endpoints are always protected against the latest threats.
Support	Access to a dedicated support team that can answer any questions and provide assistance with any issues that may arise, as well as a comprehensive knowledge base and documentation.

Cold Storage

- CYREBRO offers the option to extend the default Log storage of the SIEM in a "cold storage format) at a minimum cost.

Custom Rule Creation

- Should a client require specific customized rules, a "custom rule package" can be added. To clarify, exclusion of existing rules and exceptions to the CYREBRO rule base – do not fall under the "Customized rules", and do not bear a cost to them.

Plugin Creation

- CYREBRO supports all log types and sources as stipulated online in our list of integrations: https://www.cyrebro.io/integrations/ - CYREBRO can develop a customized Plugin (That does not exist in our current list) per clients request, at a cost.