



DON'T LET THE CORONAVIRUS IMPACT YOUR BUSINESS CONTINUITY

Aegean Experts and Kreston, IL understand that the Coronavirus has a real impact on your business continuity and working from home brings new security challenges. While you protect the health of your employees and stability of your business, let us and our partners CyberHat defend your network security and machines. Enjoy a 45-days free trial of CYREBRO managed SOC.

Time to Be Proactive -

Let CyberHat experts help manage and control all your security remotely.

CyberHat provides a cohesive cyber security platform (CYREBRO managed SOC). It offers a Platform that enables your organization to leverage existing IT security investments (Anti-Virus, Firewalls, Web Proxy, Email Security, etc.). Its teams monitor and detect suspicious activity in real time. Through its unique methodologies, technology integration, and smart automation, CyberHat manages the overwhelming security logs and reduce the workload on understaffed teams, enabling increased productivity and a stronger security presence.

CyberHat offers 45 days
FREE trial including



A FULLY LICENSED SIEM

PROPRIETARY END POINT AGENTS

24/7 MONITORING

THREAT INTELLIGENCE AND INCIDENT
RESPONSE TEAMS

Don't let hackers exploit the situation and gain access to your critical infrastructure.
Contact us today: pvalantassis@aegeanexperts.gr

CYREBRO Online SOC platform

*Free 45-day Corona Cyber protection
Proposal
For Aegean Experts and Kreston clients*



*All your security systems operated in one place.
Managed and operated by experts, for you.*

March 2020

Our Goal

Help your organization control and operate their cybersecurity remotely. Providing an organizational cyber and IT security professional center, active, accessible and learning 24/7

One, highly advanced, Online security operation center, acting 24/7 to enable the organization to better, defend, identify and respond to a cyber and IT security incident.

The Offering

CyberHat proposes to provide a managed SOC solution through a unique online platform, designed to utilize the existing security sources and systems in the company, this includes the required technology (A SIEM and end point collection agents), 24/7 Monitoring, investigation and response service, Cyber threat intelligence and a professional Incident Response team on call. All managed, presented and operated through CYREBRO online Platform

Fully operated and managed by CyberHat, Providing the organization with an online solution for monitoring and identification across their network as detailed in the offering.

CYREBRO platform not only offers “Clients” a managed Security Operation Center but a real ability to see and operate the organization’s security remotely and in the most effective and tactical manner

Following, is the detailed proposal and scoping.



Smart SOC Platform

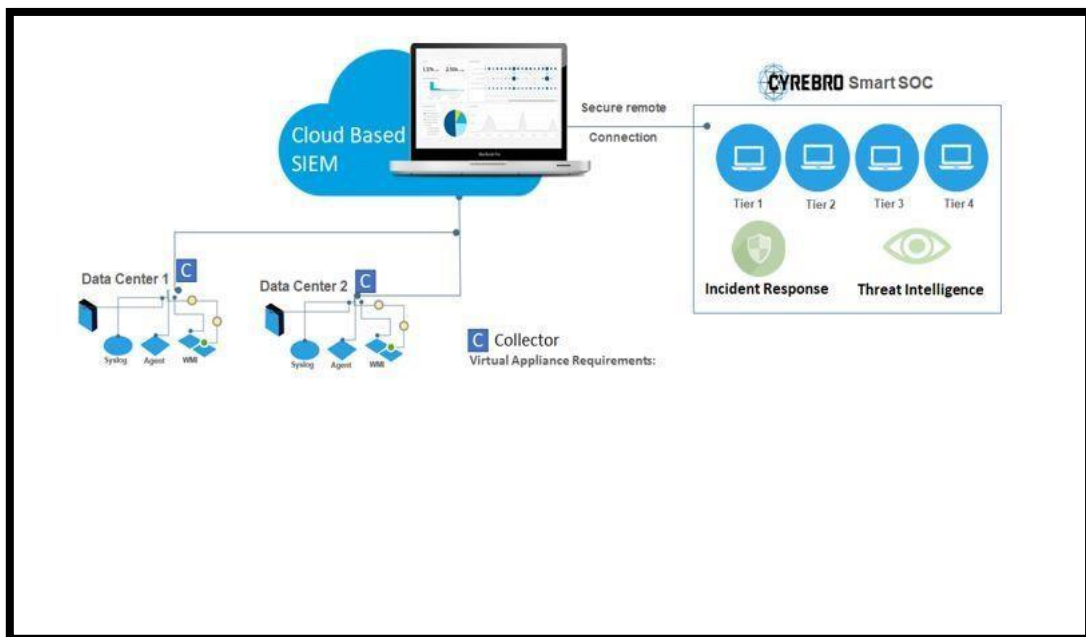
CYREBRO provides a cohesive cyber security platform for organizations looking to maximize their cyber security capabilities. Developed by CyberHat, a leading cyber security firm, CYREBRO is a managed Security Operation Center solution comprised of industry-leading analysts. These experts monitor and optimize your defenses and respond to cyber-threats to provide you a fully managed cyber security operation.

The image shows a computer monitor displaying a complex dashboard with various charts, graphs, and data points, representing the Smart SOC Platform. The dashboard includes several circular gauges and data tables, all set against a dark background with blue and green highlights.

Coverage Scope

Technological Scope

The following proposal is for our CYREBRO solution, a technological and expert based SOC solution including the SIEM technology and 24/7 experts cyber monitoring and detection. The solution covers specific log sources as detailed below, and a proprietary collection agent per machine, CYREBRO-X for end points



The following Virtual Hardware must be supplied by Client

- CPU – 8 cores
- RAM - 16 GB
- HDD – minimum 1TB
- 300 MB/s data transfer rate

*The following HD requirements may vary from time to time

** Collector environment requirements - VMWare / Hyper V / AWS / Azure

Log sources

The monitoring plan in scope will include the following (if applicable):

- Antivirus / Endpoint protection
- Perimeter inbound - FW
- Mail relay O365 / Gsuite Log Sources
- Authentication- Active Directory/LDAP
- VPN/Citrix/VDI – Authentication

A proprietary end point collection agent “CYREBRO-X”

Technical prerequisites for the X agent per machine

Windows:

- Windows 2008 R2, Windows 8.1 and above which include: Windows 10, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 X Supports Linux

Ubuntu 16.04, Ubuntu 18.04 Ubuntu 19.04, Ubuntu 18.04.2LTS.

24/7 ResponseTeam

In case of an immediate threat such as an ongoing live Cyber-attack on the organization, the response team is available 24/7 (SLA applies) to lead in blocking, containment and remediation of the event

- The team will conduct first response online and will manage the incident with client's POC until closing of the incident
- Up to Three (3) activated hours for the period of 45 days for Incident Response.
- Note: In the event that an active incident requires more than 3 hours/45 days, the additional hours will be billed at \$150 an hour
- The IR hours cannot be accumulated.

The Incident response team is committed to the following SLA for real time incidents:

- 24/7 availability for "phone and email" trigger of report
- 1 hour maximum – first response, IR team member begin handling
- 4 hours maximum – initial update

The response team can only be triggered by SOC management / Client pre-defined POC and will be priced by the hour if required to execute.



Price & Proposal Consideration

Service	100 EPS
One Time Setup	<u>\$0</u>
CYREBRO: <ul style="list-style-type: none"> Fully licensed SIEM technology 24/7 coverage of Tiers 1-4 Analysts 24/7 Incident Response Threat Intelligence Feeds 	\$0 per month For 45 days
CYREBRO X end point agent	First 100 agents – Free for 45 days

- **Prices above are for a 45-day trial period**

Terms and Conditions:

- Support for a single cloud based SIEM instance only.
- Integration of Threat Intelligence feeds (IOC).
- The prices above cover a SIEM license of up to 100 EPSs.
- Prices include up to 100 CYREBRO-X agents.