Cyber 2.0

UNIFIED CYBER SECURITY SOLUTION

SOLUTION DOCUMENT

Cyber 2.0-Introduction

Cyber 2.0 is a first of kind unified cyber security technology that packs in the combined power of Zero Trust, Network Access Control, Network Obscurement, EDR/XDR functionalities & SOC/forensic capabilities and offers holistic protection and prevention in its true sense for enterprise networks

As against the traditional security solutions that are based on biological models that are in some way vulnerable, Cyber 2.0's 9 unique patents are conceived on the Mathematical Chaos Model that form the core of the solution. These patents work in cohesive synergy to render a state of complete network control and creates an organization specific scrambled network that is impenetrable.

Cyber 2.0 Integrated AV/EDR/XDR/MTD

Unlike the standard defence systems, Cyber 2.0 works is an integrated solution that acts as a Reverse EDR with Xtended detection and prevention capabilities with built in default features of a Next Gen AV.

The Cyber 2.0 system defines and marks, in the initial stage, only the software that are allowed to route around the network and make use of network resources (about 100 out of thousands of software available on the organization's computers)

Software that was not defined as allowed to route around the network (including any new and unknown software, whether it is malicious or not, including any new virus) will be blocked by the Cyber 2.0 system.

In other words, it do not need to detect malware.

In addition, Cyber 2.0 deploys its MOVING TARGET DEFENSE capabilities by constantly shifting and changing the incoming and outgoing ports using Chaos mathematics, thereby effectively obscures the correct access ports of any attempt to assault them, causing any such attempt to result in a failure.

Cyber 2.0 is the worlds most unique, defense grade cyber security technology built on 9 different patents to deliver the most powerful and unparalleled Protection & Containment capability that currently exists.

CYBER 2.0 TECHNOLOGY

1. MATHEMATICAL MODEL:

Cyber 2.0 is the first of its kind technology which is conceived based on the MATHEMATICAL CHAOS THEORY that cannot be breached.

2. NETWORK SCRAMBLING

Cyber 2.0 synergize's its CHAOS ALGORITHM, UNIQUE SCRAMBLING SYSTEM, REVERSE TRACKING MECHANISM and other patents to create an organization specific scrambled network that creates an impenetrable chaos barrier, which stops all attacks. Additionally it deploys its Unique Containment Engine that stops the spreading of an attack, if any, into the organization from the infected computer.

3. INTEGRATED SUITE

Cyber 2.0 is the Most Powerful Technology that harnesses the combined power of ZERO TRUST, NAC, NETWORK OBSCUREMENT & EDR.

4. LEGACY SYSTEM PROTECTION

Cyber 2.0's offers the same level of protection to legacy and unsupported OS that are most vulnerable due to end of life support issues.

5. OT & IOT DEVICE PROTECTION

Cyber 2.0 has the unique capability of protecting the entire suite of IT,OT and IOT devices under a single eco-system. Its Vortex Gateway is specially designed for OT and IOT environments that is not required to be installed over the Controller and works in unconnected environments. It does not require any updates, does not slow down the network and is easy to operate.

6. WFH COMPLIANT

Cyber 2.0 offers similar superlative protection of prevention plus containment to the systems of employees working from home that are relatively less protected and hence easier targets for malicious intruders

7. MINIMAL OPERATIONAL LOAD

Cyber 2.0 is a self sustaining agent that does not need any internet connection or updates or patches, that drastically reduces the operational load on the IT team on a day to day basis.

8. GDPR COMPLIANT

Cyber 2.0 is Fully Compliant with the Data Protection framework of GDPR. No Private information or identification is stored or analysed

9. PROVEN TECHNOLOGY

Cyber 2.0 is the only technology that remains Un-compromised even after 4 years of Consecutive Global Hackathons and 4 million+ attacks by 5500+ hackers from over 30+ countries with an open bug bounty of 1,00,000 USD

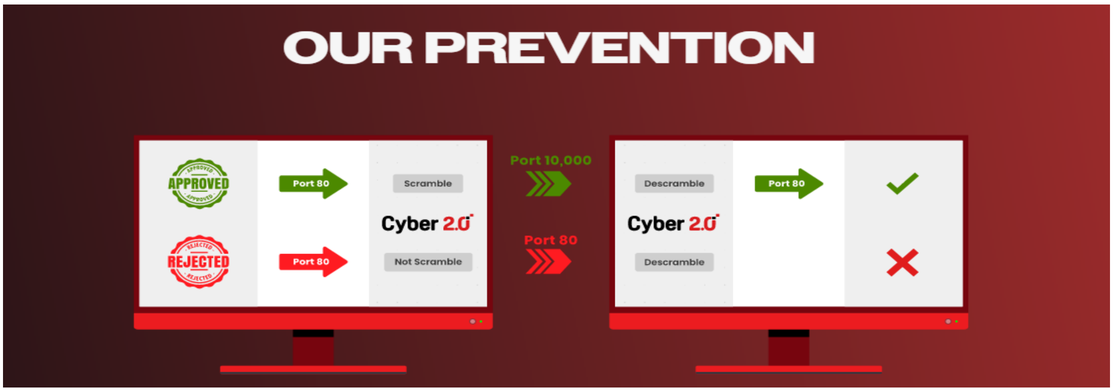
10. MULTI ENVIRONMENT SUPPORT

With a simple one click installation, Cyber 2.0 lends complete flexibility in terms of True ON PREM as well as Cloud Deployment models with OS support covering traditional IT as well as OT & IOT environments on a single dashboard instead of multiple dashboards and vendors.

11. OPTIMUM ROI

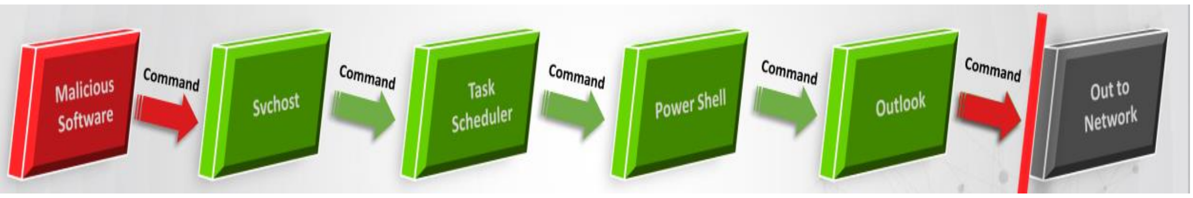
With Cyber 2.0, organizations will no longer be required to invest on additional security software's like Next Gen AV, IDS, IPS, Internal Firewall, NAC, BYOD, PW Acceleration, Honey Pots etc ensuring OPTIMUM Return on Investment(ROI).

Unique Scrambling Mechanism based on Mathematical Chaos



Cyber 2.0's Reverse Tracking Mechanism - Superlative Zero Day Protection

Cyber 2.0's Reverse Tracking Patent allows the system to check every process that comes up on the computer and ascertain by MD5, by size and by SHA, whether the file is authentic and is approved to route around the network. The information is saved in the form of flow instead of individual packets enabling efficient and rapid reading of the information.

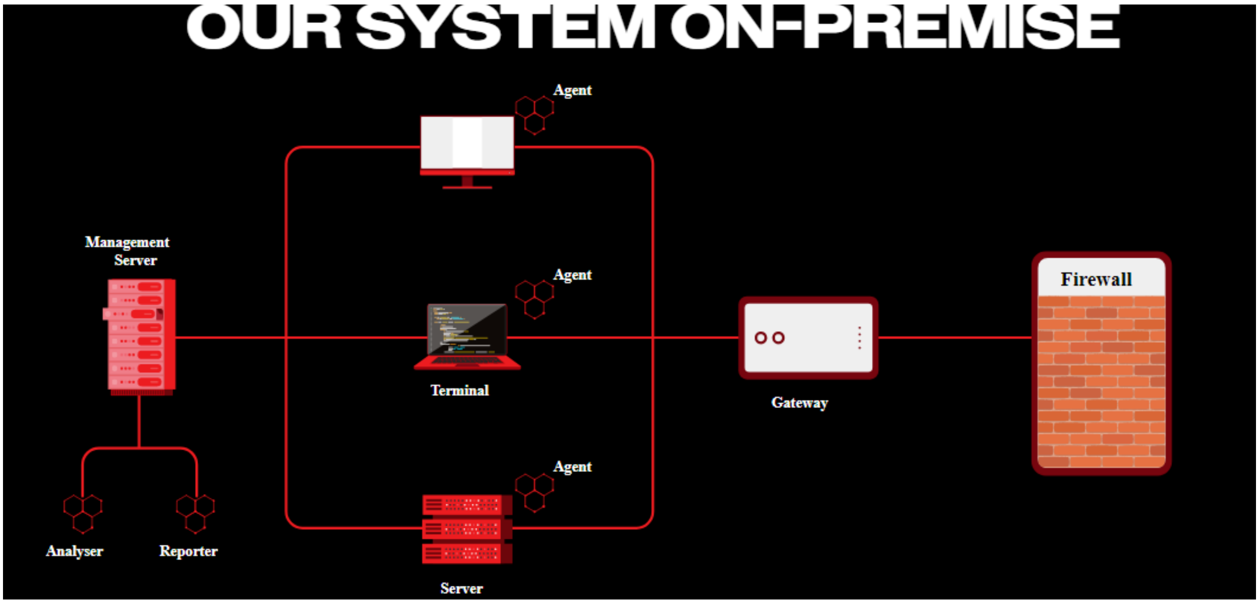


The system monitors all active software and all active processes on the monitored computers. The knowledge stored by the system allows it to make an inventory of all the software and processes that exist. The system displays every software and version of the software according to the computer on which they are installed. The Cyber 2.0 system monitors all incoming and outgoing traffic from the protected components.

This allows Cyber 2.0 to protect even against **Zero Day attacks** as the **REVERSE TRACKING MECHANISM** tracks the chain all the way back and blocks even the legitimate application from going out of the network.

Cyber 2.0 is designed in such a way, that even if it is attacked or removed from the infected computer, it can still protect the organization from spreading cyber-attacks from the infected computer into the organization.

Cyber 2.0 On Premise Deployment-Network Schematic



QUICK & EASY DEPLOYMENT

The deployment can be done with Full On Prem of Cloud

STAGE 1- POC

The agent can be installed on a pre defined no of systems

And within 14 days the system is ready to present the analysis, a list of every software that is recognized as malicious and every unknow software

STAGE 2- MONITOR MODE

This is the initial mode of the system, that Creates a comprehensive inventory of every process or file that has been active since the system was installed.

It is designed to gather and analyse information about the network it is installed on.

It presents all software that are Supposed to be blocked by Cyber 2.0, when its deployed in Défense Mode.

STAGE 3- DEFENSE MODE

Défense Mode is designed to bring the most cutting-edge defence into your organization. It creates an unpassable chaos barrier between the computer of a specific network and does not allow any unknown or unwanted application to traverse the network.

Any attempt by malicious software to bypass or deactivate the mechanism will cause the offending software to get locked on the original computer, while the allowed programs keep working unhindered.

Network Intrusion Prevention System (NIPS)

Cyber 2.0’s AI Based patented Chaos Engine works on the network layer. Every packet that traverses the network in or out of the computer, passes through the Cyber 2.0 Chaos Engine, and is being logged, and the logs are sent to a central controlling server (local or cloud).

The information is organized and analysed by the central server and the user can view the following data:

- Network -one single flow instead of hundreds of packets per connection
- The source and destination of the flow
- The source and destination ports
- The user that initiates the network flow
- The application or process name
- The application or process #md5
- The path of the running application
- In case of a file system access, instead of a port there will be the destination path and accessed files or doc
- Incoming dropped packages
- Incoming Broadcasts
- Any application that was part of the chain of activation of that network flow

Since Cyber 2.0 uses Network Control instead of application control, creating a complete Zero Trust network becomes viable and easy and once activated, it creates a barrier between the network computers, allowing only approved applications to travel between network resources, effectively creating a Network control state.

Host Intrusion Prevention System (HIPS)

The Reverse tracking mechanism works on the application layer. Every time an application is opened or an application, uses accesses, sends data, communicates or does any sort of interaction with another app or process, it is registered, being logged, and sent to a central controlling server (local or cloud).

The information is organized and analysed by the central server and the user can view the following data:

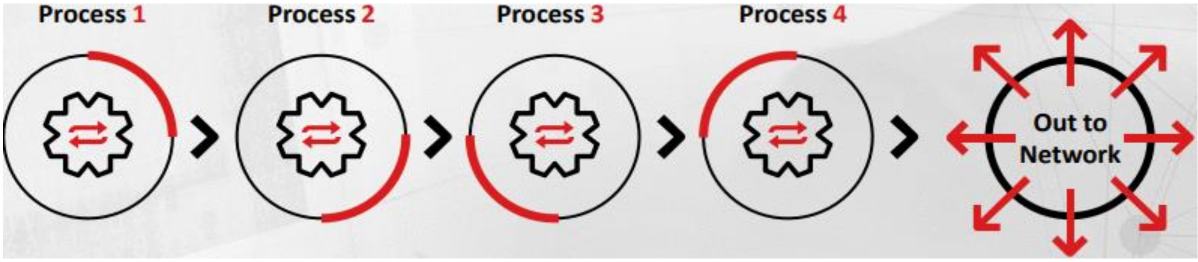
- Any file or process that has been running on any computer
- Display name and true name of the process or file - (when applicable – not all processes and files have a true version)
- The version of each file or process (when applicable – not all processes and files have a true version)
- The #md5
- Allow the Chaos engine to display the chain of networks flows

Patented Reverse Tracking Mechanism Flow

-Every Process and library file that loads is recorded

-The system captures their MD5 and SHA signature

-Every access of another process is recorded



All attempts of unauthorized, unknown or malicious applications to bypass or disable the chaos mechanism, will cause it to become unbalanced, and will lock that application in its origin computer.

BUBBLES: The MINI SOC (Real Time Threat Monitoring & Risk Posture)

Cyber 2,0 has offers a real time Network Traffic Monitoring System that visually depicts the live Network Traffic of an organization with real time changes as they happen in the network and identifies live threats across the network. This serves as a mini-SOC for organizations to monitor their network risk posture and align their security strategy accordingly.

With this strikingly visual and powerful tool, organizations will be able to monitor the live network traffic from across their locations and will be able to understand the risk posture at any given point in time and take appropriate actions accordingly.

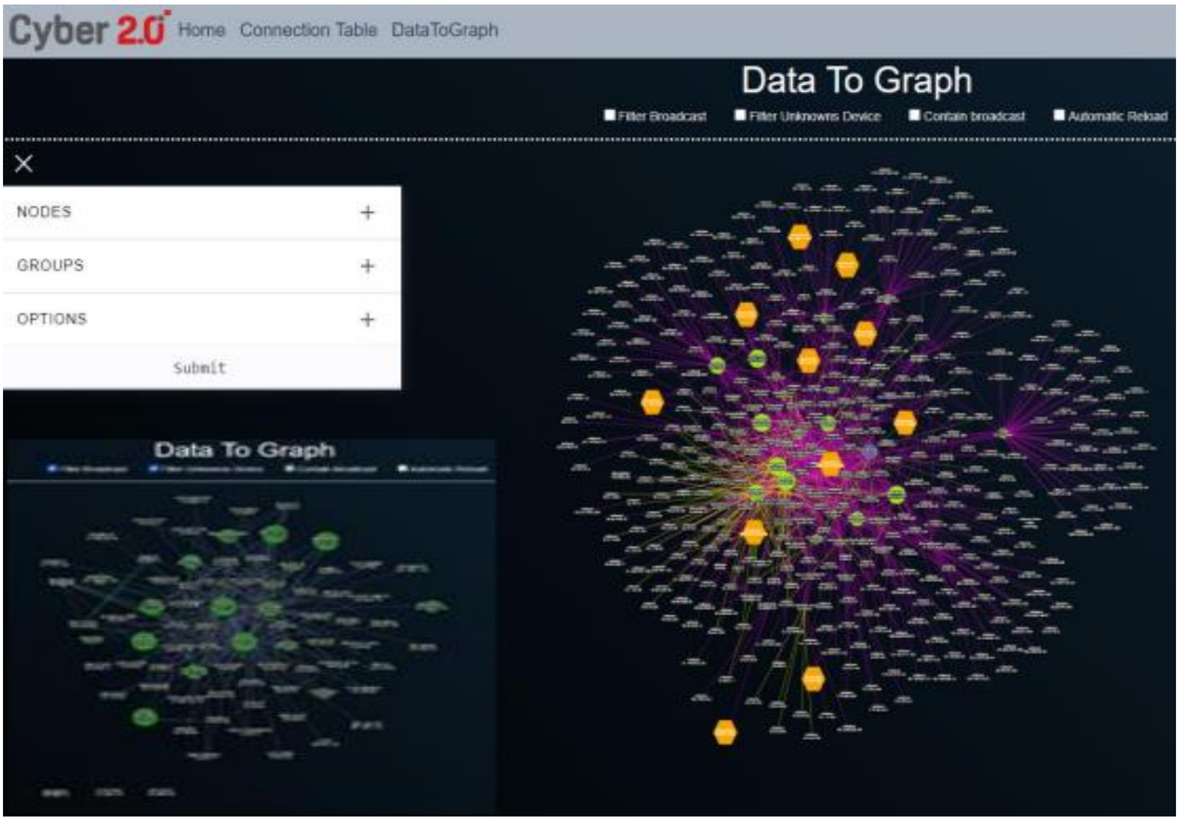
The platform visually displays the entire network in the form of nodes and arcs by extracting information of the communication between the organizations computers and outside of it.

The default colour of the nodes and arcs is determined by the group it belongs to and displays the station name and the IP address.

The platform has the functionality to display 4 levels of information:

1. **Filter Unknown Devices:** Communication between devices that do not the Cyber 2.0 agent deployed or external communication
2. **Filter Broadcast:** Filters all broadcast calls
3. **Contain Broadcast:** Combines all the nodes defines as broadcast into one single node.
4. **Automatic Reload:** The Platform updates and reloads automatically every 10 minutes thereby vividly illustrating the live state of the network

The platform is feature rich and has powerful and comprehensive monitoring, inventory and forensic capabilities.

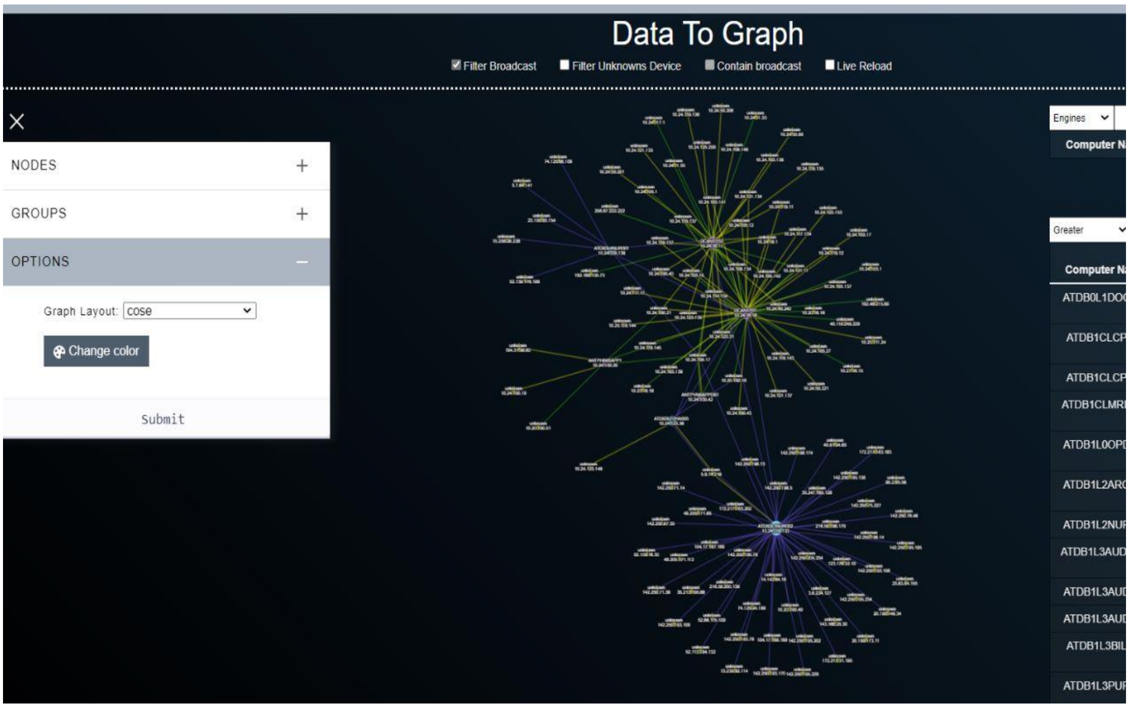


Upon tap on the bow, it displays all the relevant bow in terms of its

- IP Address & exit port of the source device
- IP Address & Entry point of the destination device,
- Process name &
- Status.

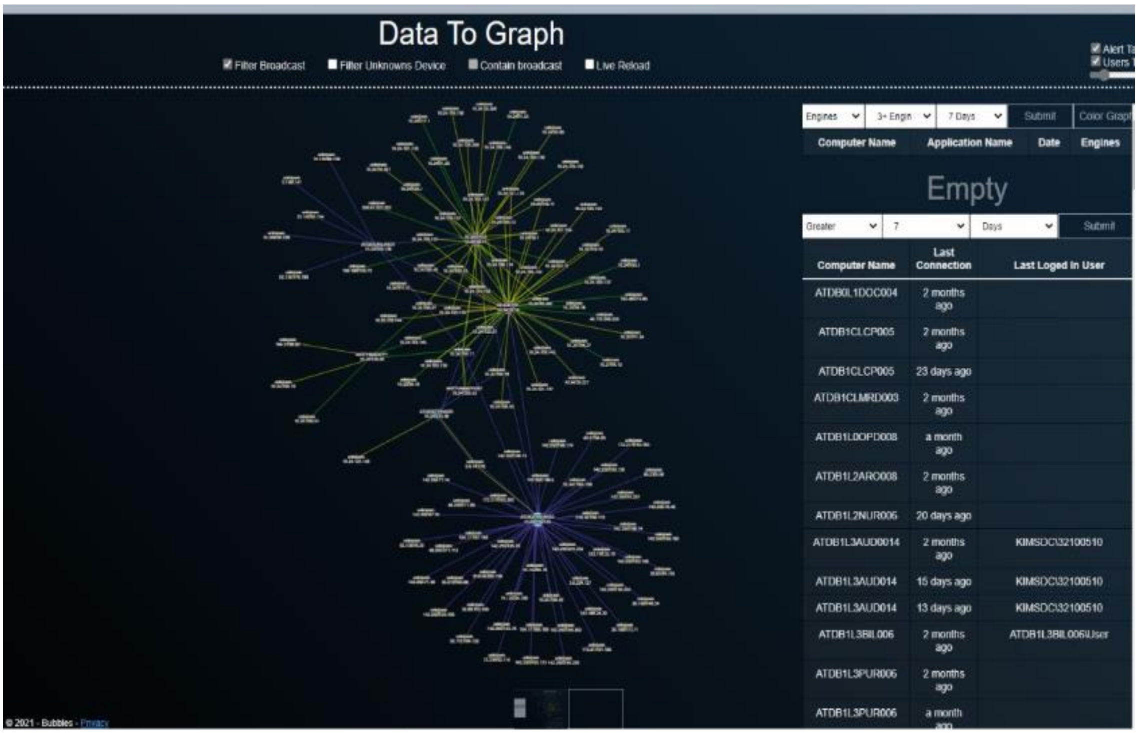
And upon tab on the node, it platform displays a detailed information table containing all communication attempts made by the device with the following fields:

- User Name
- IP Address & exit port of the source device
- IP Address & Entry point of the destination device
- Process Name &
- Status.



Data To Graph

☑ Filter Broadcast ☐ Filter Unknowns Device ☐ Contain broadcast ☐ Live Reload



Data To Graph

☑ Filter Broadcast ☐ Filter Unknowns Device ☐ Contain broadcast ☐ Live Reload

☑ Alert Ta
☑ Users T

Computer Name	Application Name	Date	Engines

Empty

Computer Name	Last Connection	Last Loged In User
ATDB0L1DOC004	2 months ago	
ATDB1CLCP005	2 months ago	
ATDB1CLCP005	23 days ago	
ATDB1CLMRD003	2 months ago	
ATDB1L0OPD008	a month ago	
ATDB1L2ARC008	2 months ago	
ATDB1L2NUR006	20 days ago	
ATDB1L3AUD0014	2 months ago	KIMSDC\32100510
ATDB1L3AUD014	15 days ago	KIMSDC\32100510
ATDB1L3AUD014	13 days ago	KIMSDC\32100510
ATDB1L3BIL006	2 months ago	ATDB1L3BIL006\User
ATDB1L3PUR006	2 months ago	
ATDB1L3PUR006	a month ago	

© 2021 - Bubbles - Privacy

Cyber 2.0 is currently the only system that offers the integrated stack of an EDR/MDR/XDR/NAC & SOC with powerful and comprehensive Forensic capabilities based on the Mathematical Chaos Model that renders the power of real time Threat Monitoring & Blocking to enterprises.

ON PREMISE DEPLOYMENT: VIRTUAL/PHYSICAL SERVER REQUIREMENTS

- Hardware server minimum requirements:

CORE	HD	Memory	Quantity of computers
I7	500G SSD	32G	500 Until
I7	256G SSD	64G	500-1000
	1T SSD		
I7	256G SSD	128G	1000 and above
	1T SSD		

Software server requirements:

- OS windows server 2016 or 2019 standard edition fully updated

Stages of the pilot

Stage 1 - Presetting

Set up a management server according to the requirements mentioned below – R**esponsibility of Customer**.

- IT recommended to Add an exclude to the following paths in Antivirus on the endpoints**:**

C:\Program Files\Cyber 2.0\Cyber 2.0 Agent
C:\Users\Public\Cyber 2.0
C:\ProgramData\Cyber20Agent

- Windows 7 or Windows server 2008 R2, Requires installation of update KB3033929 and .net Framework 4.5
- Windows 8 or Windows 8.1., Requires installation of the .net Framework 4.5 on

Stage 2 – Deploying Cyber 2.0 in monitor mode

- Installing Cyber 2.0 Agent on endpoints.
- Inventory of programs and processes that use the network.
- Building and distributing first dynamic list to the endpoints.
- Short Training on the following Cyber 2.0 tools
  - Cyber 2.0 Analyzer
  - Cyber 2.0 Log Reader
  - Cyber 2.0 End Point

Purpose of the stage:

- Distribution, computer forensics and proper interaction with other systems in the organization.
- Monitoring workspace and obtaining information about existing threats.

Approximate Working time: 1-2 hours.

Approximate Training time: 1 hour

Estimated duration of the stage: 2 weeks.

Stage 3 – Displaying POC Results:

- Generating a Report from the Cyber 2.0 Analyzer tool
- Setting a meeting to discuss the finding from and the POC results

Approximate Working time: 1-2 hours.

End of Document