CYBER2OT/IOT

Protection of OT SCADA and IOT networks

Cyber 2.0

WWW.CYBER20.COM

The Cyber 2.0 system is built on a mathematical model of chaos theory and based on 9 different patents.

The protection capabilities of the system

In the event of a cyber-attack on various water systems, Cyber 2.0's SOC system has the ability (at the push of a button) to transfer all water systems, including their computers and networks, from monitoring mode to protection mode, thus blocking any possibility of another attack on the rest of the entities that have not yet been attacked.

The protection includes

- Blocking cyber-attacks in real time
- Isolation of computers or specific systems
- Preventing cyber-attacks on computers or protected systems
- Absolute prevention of attacks on the infrastructure systems (OT) using our Gateway devices.

The Cyber 2.0 solution for OT and SCADA systems

While developing the product for the IT world, we also developed a complete solution for the OT world. We started implementation in this area, and today we support several water systems in the State of Israel and have proposed to the Water Authority that Cyber 2.0 will manage a SOC system for them. Concurrently, we are now providing solutions to factories and municipalities in Israel and around the world.

The advantage of Cyber 2.0 is that one system, can simultaneously protect the computers in the organization, provide a full response to workers from home, and completely protect important facilities and infrastructures. This technology has already been tried and proven and has recognized success in its performance.

The Monitoring Capabilities

The monitoring capabilities of the active software is derived from its reverse tracking capability. The system monitors all active software and all active processes on the computers

The received information includes

- The version no. of the process or application
- The hash (#) of the process or of the application
- The name of the process or application
- Any information regarding the time when it was first discovered
- The information regarding the computer or processes or application that have been detected
- The registered name of the process or application

The dynamic inventory system

The knowledge stored by the system enables it to create an inventory of all the programs and processes that exist in the monitored devices.
The system enables searching different sections according to all the parameters collected in the monitoring.
The system displays each software and its software version, according to the computer where they are installed.

Monitoring the network movement

Monitoring the network movement is derived from the chaos capabilities of the system: The Cyber 2.0 system monitors all incoming and outgoing traffic from all components. The information is saved in the form of FLOW, as individual packets - which enables efficient and quick reading of the information.

The received information includes

The software released to the network

Who is responsible for that FLOW

The used ports in FLOW (Source and Destination)

The source and destination of the FLOW - IP4 and IP6.

Who is the reporting computer

IS it a UDP, TCP or BROADCAST

The location of the software inside the computer (PATH)

The programs involved in porting the software to the network

The information analysis capabilities

The information of the system is saved in an elastic database that enables maximum flexibility when accessing the information required to investigate the findings.

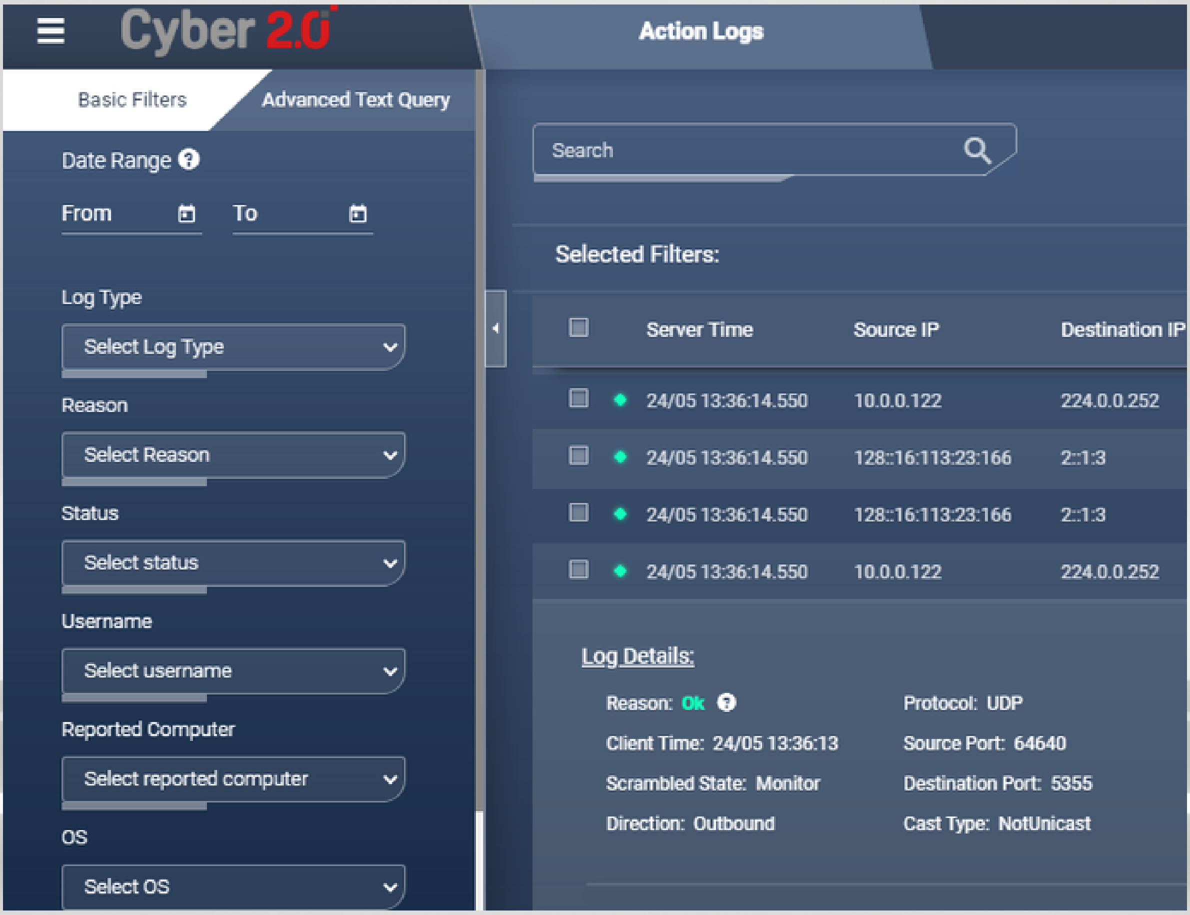
The flexibility of the information can reach the following levels:

- Per date
- Per user
- Per hours
- Per software

The system enables two types of searches

Advanced search according to complex search sentences

Search according to predetermined parameters



□		Server Time	Source IP	Destination IP
□	●	24/05 13:36:14.550	10.0.0.122	224.0.0.252
□	●	24/05 13:36:14.550	128::16:113:23:166	2::1:3
□	●	24/05 13:36:14.550	128::16:113:23:166	2::1:3
□	●	24/05 13:36:14.550	10.0.0.122	224.0.0.252

Log Details:

Reason: Ok
Client Time: 24/05 13:36:13
Scrambled State: Monitor
Direction: Outbound

Protocol: UDP
Source Port: 64640
Destination Port: 5355
Cast Type: NotUnicast

Analysis and learning of the behavior and active programs

The system learns the network behavior of the various components in the network, where each action that is taken creates repetition and a fixed behavior that is maintained

When a software component performs an action it has not done

an alert is generated

When a user performs an action that he has not been done before

an alert is generated

Any action is measured in the system according to the following parameters

Active software

Ports
source and destination

IP
source and destination

The software active in the same process

A user who activated the software or the service

The direction of movement of the FLOW

Analysis of active software and processes, to identify new processes

When monitored software changes because of one of the following changes

The hash (#) of the attribute has changed

A virus penetrates it

Version update

Mail notification of the change will immediately be sent, even if the software itself did not address the network or create a FLOW.

Implementing a Cyber 2.0 based system

System Requirements

Agents of the system are installed on Windows-based systems.
Gateway devices are installed in front of controllers and on systems on which an agent cannot or must not be installed.
A central server that monitors, analyzes, and collects the information from the monitored systems.

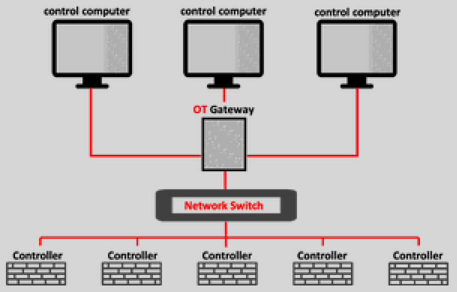
Communication requirements

The communication between the agents and the Gateway systems (vortexes) is done through ports 80 and 8080, while the information itself is protected through our chaos mechanism.
The communication is initiated by the agents, when the server acts as a passive party, and only after a successful connection, it transmits the necessary information to the agent.
Make sure that there is a communication line connected from all monitored locations, and that it is open on the appropriate ports for linking to the management server.
It is recommended to use the existing APN network.

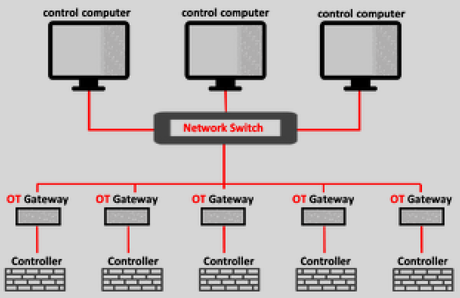
Deployment points of the Gateway (vortex) systems

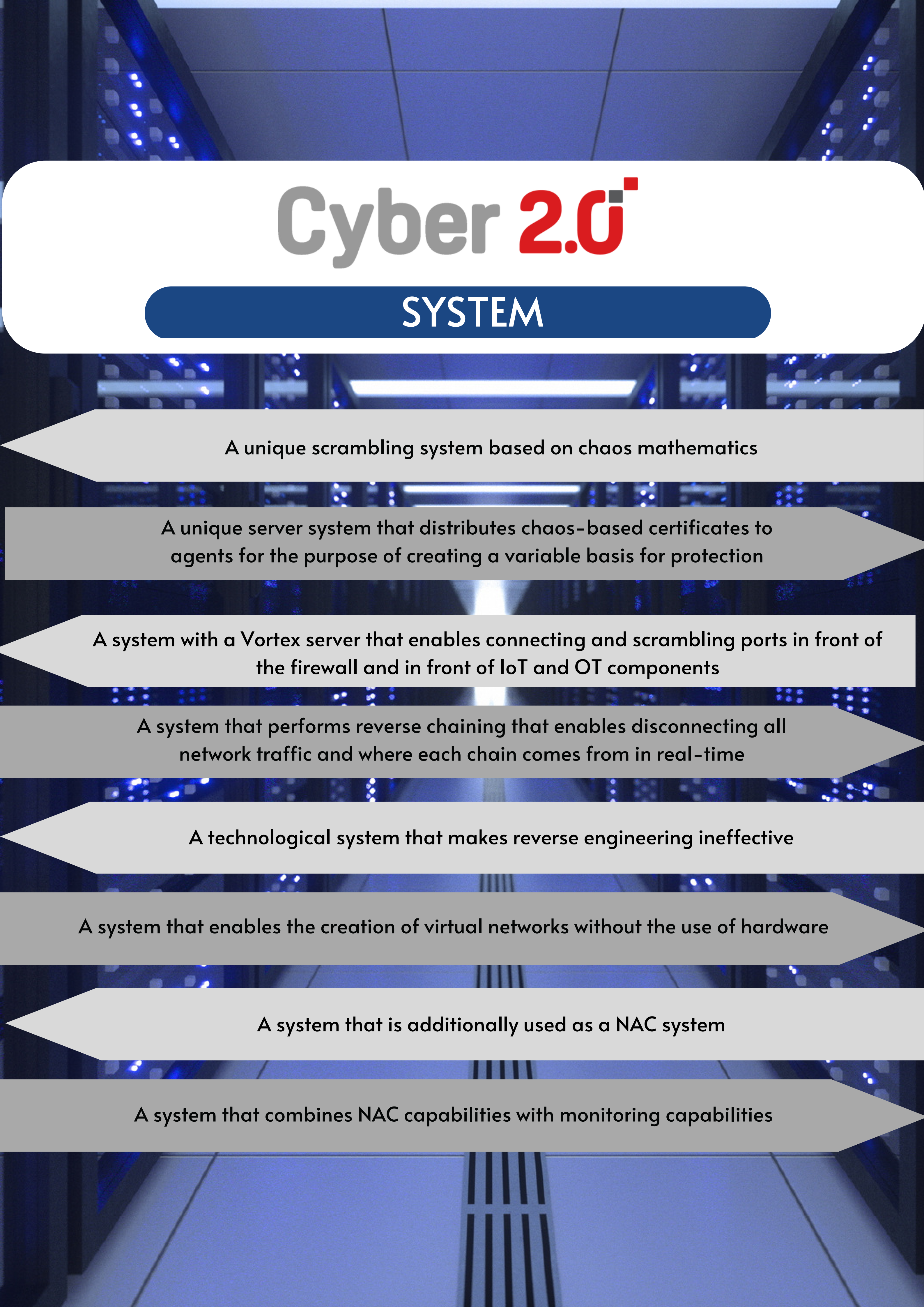
The Gateway system can be deployed in several ways, depending on the deployment of the equipment in the field
One Gateway can be deployed against a number of systems.
Gateway can be deployed in front of any system.
The types can be combined.

A single gateway



Multiple gateways





Cyber 2.0

SYSTEM

A unique scrambling system based on chaos mathematics

A unique server system that distributes chaos-based certificates to agents for the purpose of creating a variable basis for protection

A system with a Vortex server that enables connecting and scrambling ports in front of the firewall and in front of IoT and OT components

A system that performs reverse chaining that enables disconnecting all network traffic and where each chain comes from in real-time

A technological system that makes reverse engineering ineffective

A system that enables the creation of virtual networks without the use of hardware

A system that is additionally used as a NAC system

A system that combines NAC capabilities with monitoring capabilities