Cyber 2.0

2022 Winner
THE NATIONAL
CYBER AWARDS®

2023
CYBERTECH
100

Cyber2OT

Cyber 2.0

The Team

2022 Winner THE NATIONAL CYBER AWARDS®

Hertzel Ozer

Founder & Chairman of the board

Chairman of the Board of few large companies such as **HOT** Telecommunication System

Sneer Rosenfeld

CEO

Well-experienced Manager

Erez Kaplan Haelion

Founder & CTO

Senior Advisor of **Microsoft**

Tanya Sarel

COO

HR Recruiter at Check Point Software Technologies

Guy Tessler

USA Business Development VP

Experience Managing Partner, GOT Group – Atlanta, GA

Sai Krishna

Manager - India

Founder of Global Cyber Security Forum

Cyber 2.0

Advisory Board

2022 Winner THE NATIONAL CYBER AWARDS®

Professor Lewi Stone, Ph.D. - Advisory Board

Advisory Board

Expert of mathematical modelling of chaotic systems

Col. (Ret.) Adi Bershadsky

Advisory Board

Former military attaché in Europe

Major Gen. (Res.) Professor Isaac Ben Israel

Advisory Board

The initiator of the National **Cyber Authority** at the **Prime Minister's Office** in Israel

Major Gen. (Res.) Yitzhak (Jerry) Gershon

Advisory Board

Chairman of the Israel Airports Authority

Professor Bryson R. Payne

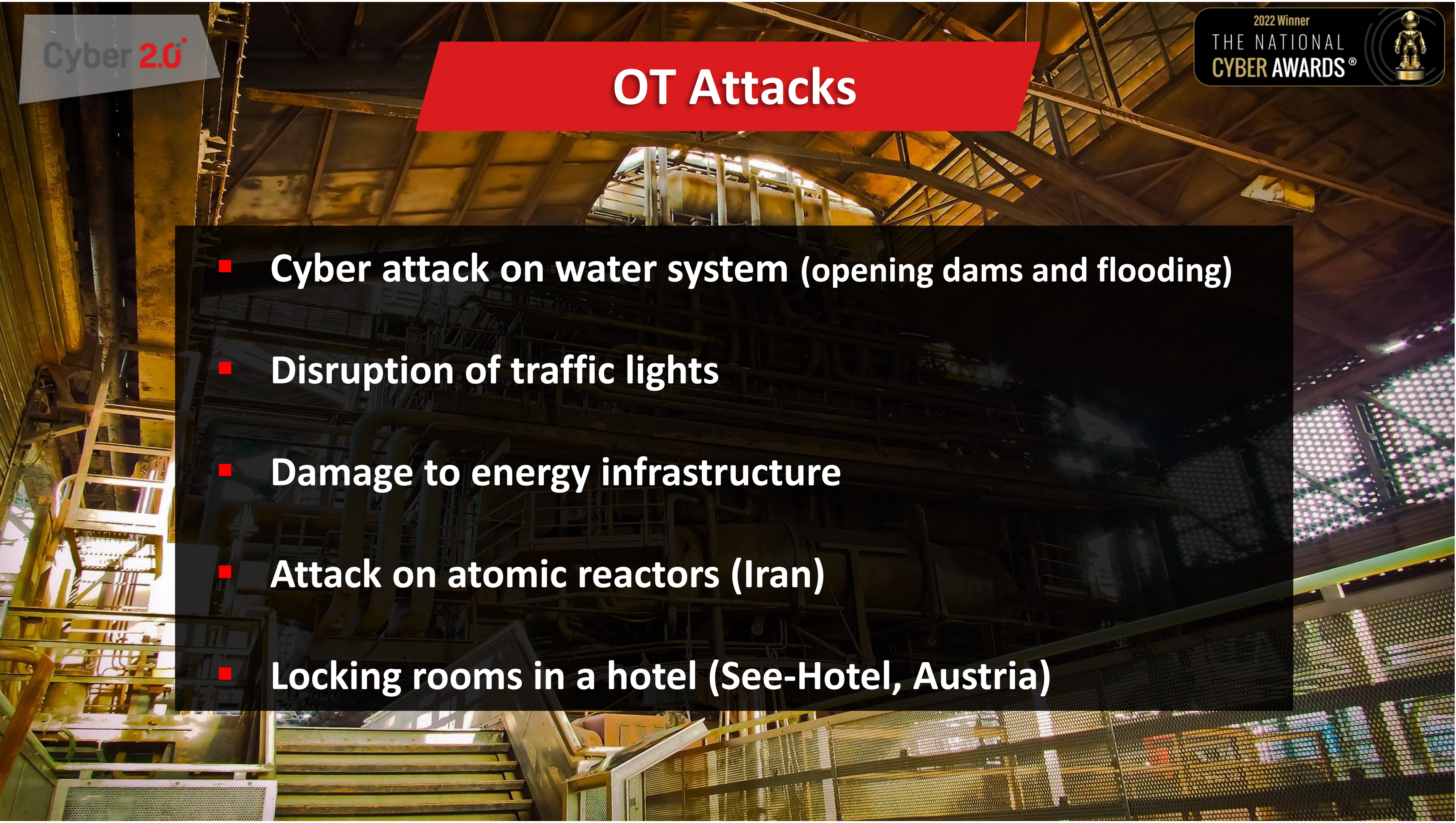
Advisory Board

Tenured Professor of Computer Science

What We Do

2022 Winner
THE NATIONAL CYBER AWARDS®

Cyber 2.0 for OT Environments prevents cyber-attacks from reaching the controllers
Effectively removing the hacker ability to attack the protected device and spreading through the network



Cyber 2.0

2022 Winner
THE NATIONAL
CYBER AWARDS®

OT Attacks

- Cyber attack on water system (opening dams and flooding)
- Disruption of traffic lights
- Damage to energy infrastructure
- Attack on atomic reactors (Iran)
- Locking rooms in a hotel (See-Hotel, Austria)

Cyber 2.0

2022 Winner
THE NATIONAL
CYBER AWARDS®

EDR is Not Enough

Detection → Prevention

First **try** to detect and recognize **every** malicious software

Then **try** to prevent its **spreading** within the organizational network

Why they don’t solve the problem

100% Detection is not possible

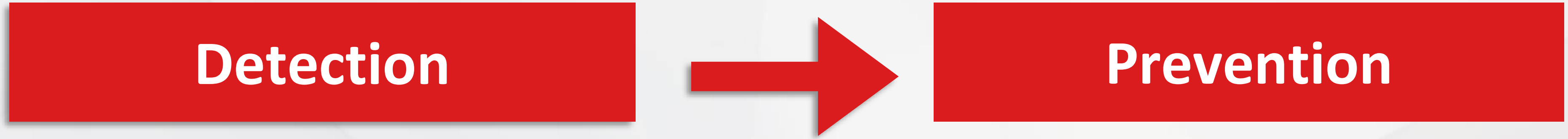
A new malicious software **every second**

100% Prevention is not possible

Hackers can **remove** the defense systems

2022 Winner
THE NATIONAL
CYBER AWARDS®

Cyber 2.0 – Beyond EDR



Detection

Prevention

Doesn’t miss any new cyber-attack

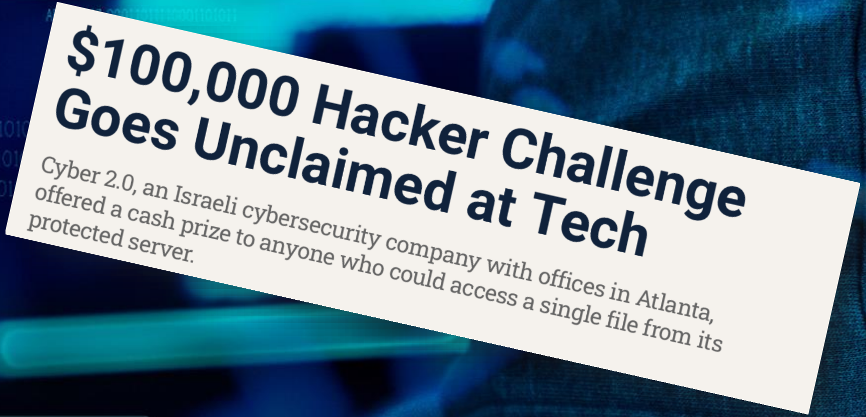
The system Continues protecting even if being removed

The technology: Zero Trust

The technology: Chaos Algorithm

2022 Winner
THE NATIONAL
CYBER AWARDS®

Challenging all Hackers

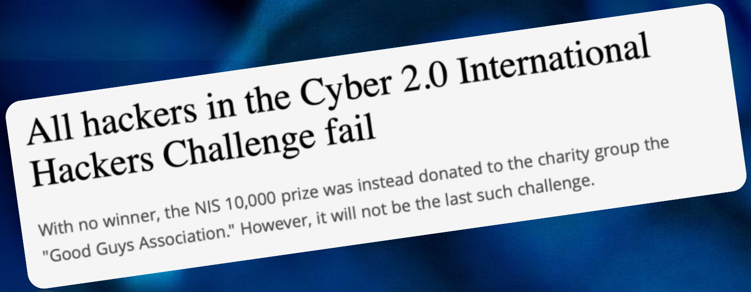


$100,000 Hacker Challenge Goes Unclaimed at Tech

Cyber 2.0, an Israeli cybersecurity company with offices in Atlanta, offered a cash prize to anyone who could access a single file from its protected server.

- 4 years
- 5,500 hackers
- $ 100,000 Reward

They all failed



All hackers in the Cyber 2.0 International Hackers Challenge fail

With no winner, the NIS 10,000 prize was instead donated to the charity group the "Good Guys Association." However, it will not be the last such challenge.

2022 Winner
THE NATIONAL
CYBER AWARDS®

WE COMBINES SEVERAL CAPABILITIES

EDR

NAC

SOC

FORENSIC CAPABILITY

ZERO TRUST

NETWORK OBSCURMENT

2022 Winner
THE NATIONAL
CYBER AWARDS®

Marking Approved Programs

The OT manager:
Marks **approved programs (1-5)**
that are allowed to access to network resources
In OT - Software that operates the controller)

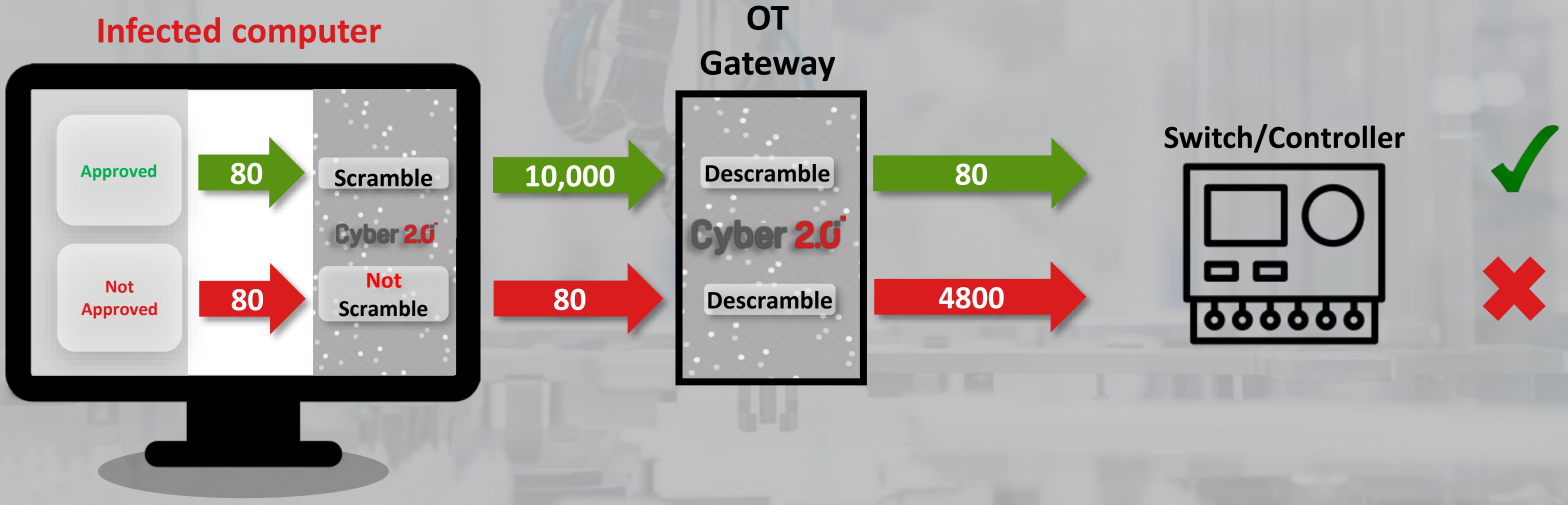
Not approved programs (all the rest):
Every software that was not marked as
an approved program
(including every new and unknown software)

Cyber 2.0

2022 Winner THE NATIONAL CYBER AWARDS®

Vortex Gateway for the OT/IOT World

PATENTED



Every Attack Against Cyber 2.0 Will fail

1. Direct attack on Protected Device

2. Attacking protected device from authorized computers

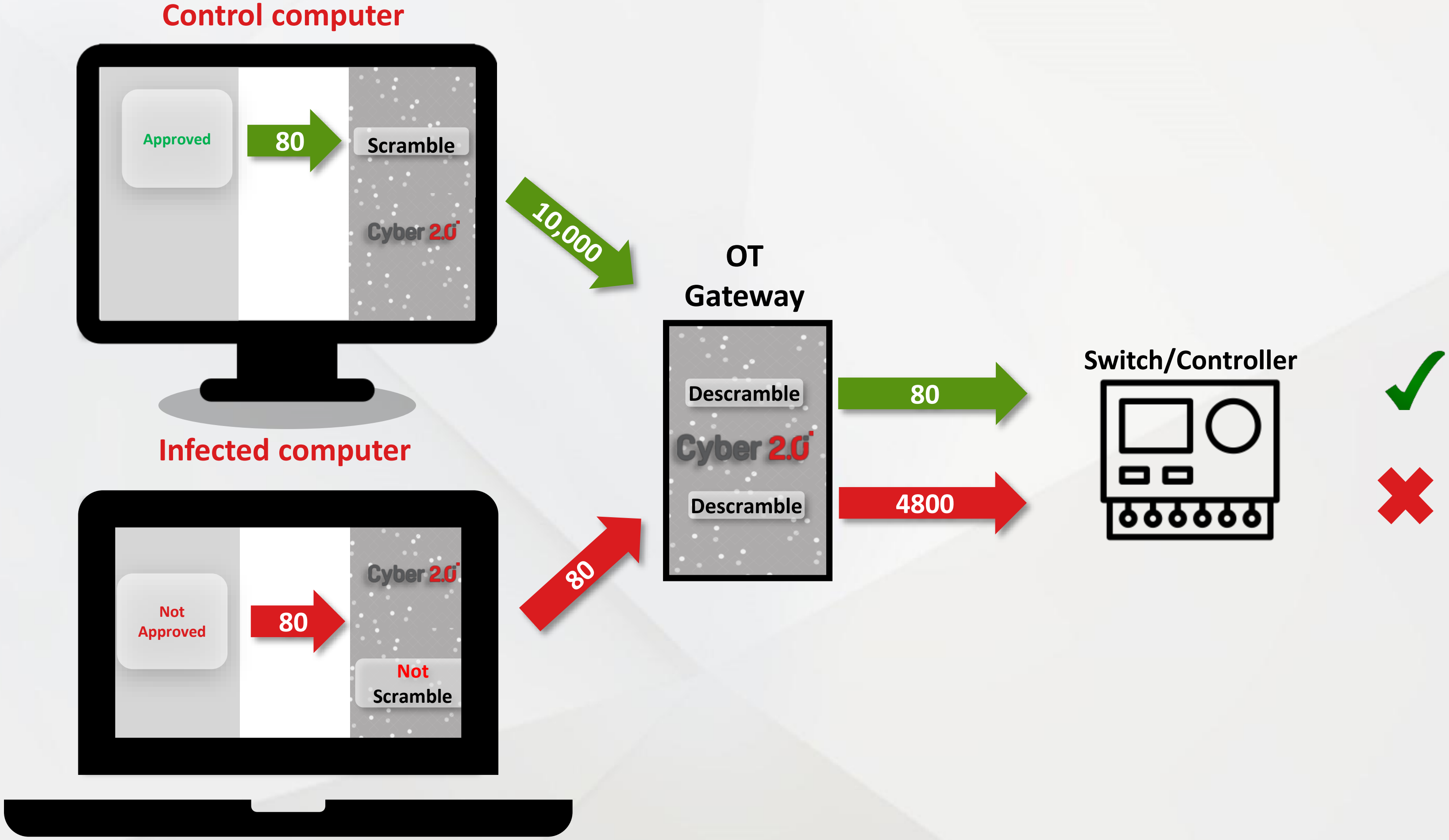
3. Adding malicious software to the trust list

4. Malicious software using other software to attack protected device

Cyber 2.0

1. Direct attack on Protected Device

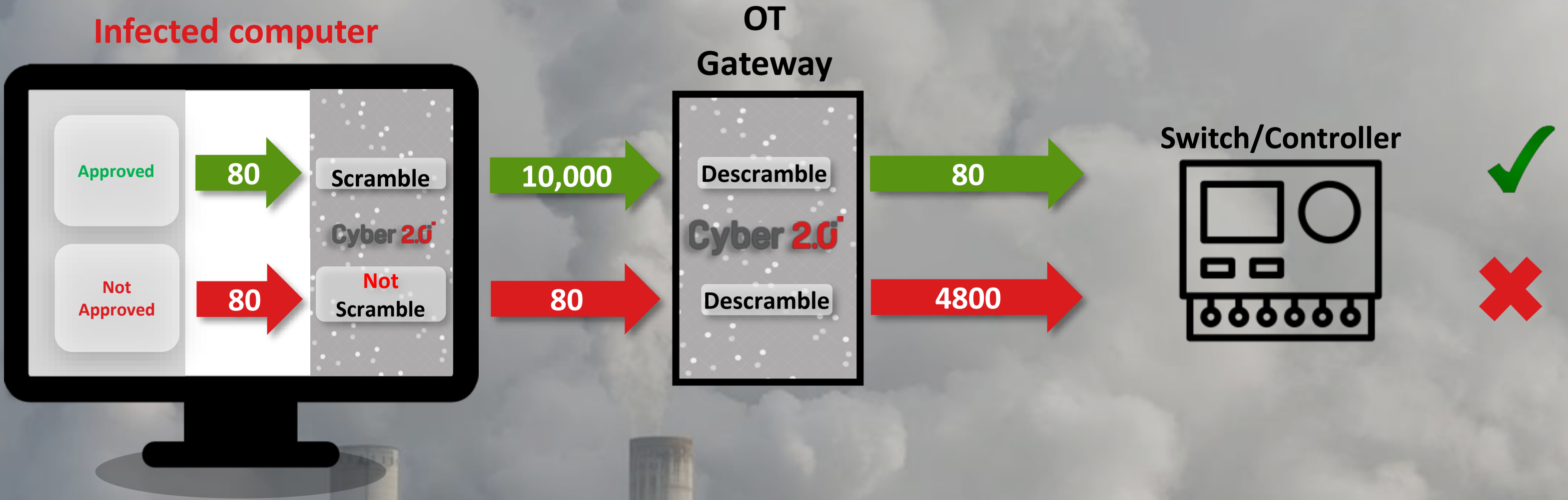
PATENTED



Cyber 2.0

2. Attacking protected device from authorized computers

PATENTED



Infected computer

Approved

80

Scramble

Cyber 2.0

Not Approved

80

Not Scramble

10,000

80

OT Gateway

Descramble

Cyber 2.0

Descramble

80

4800

Switch/Controller

✓

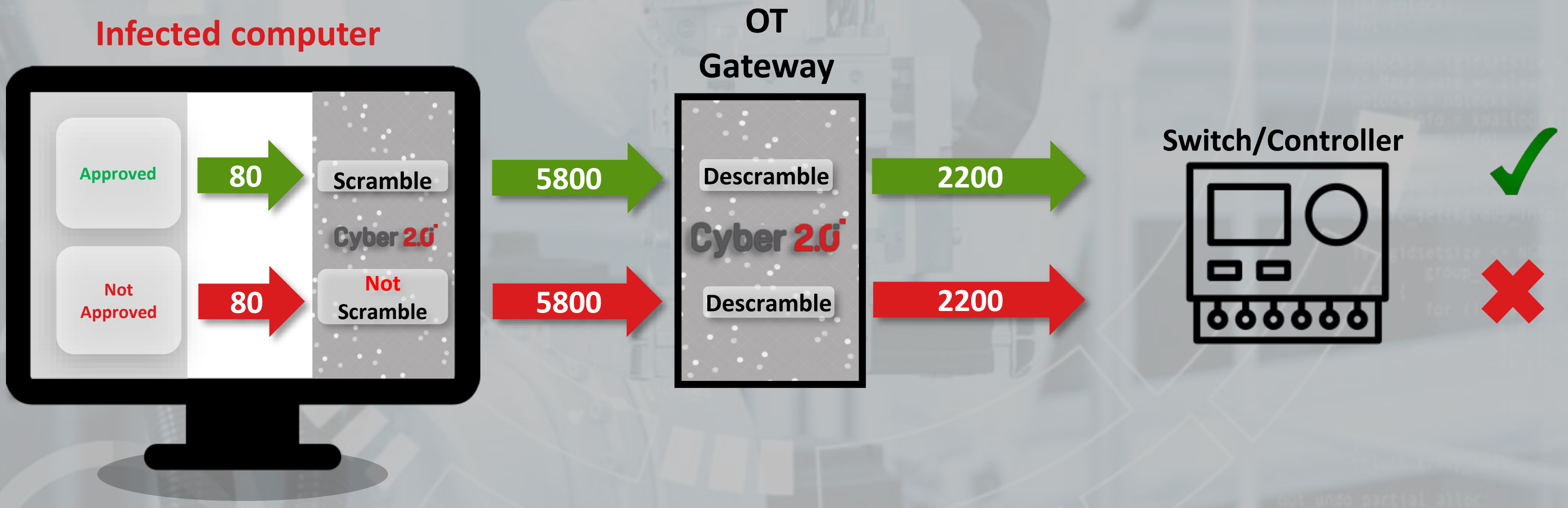
✗

Cyber 2.0

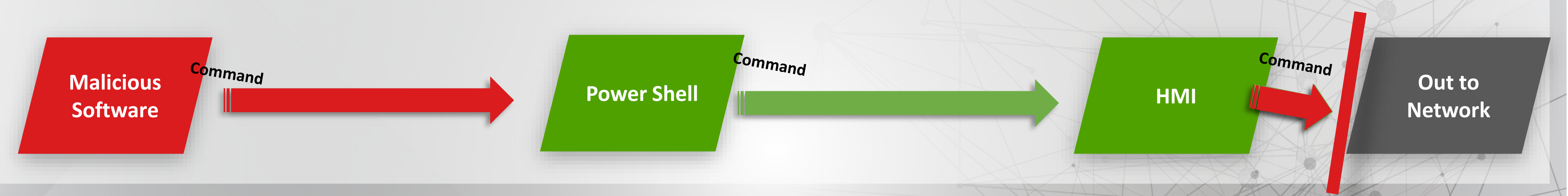
3. Adding Software to The List Will Fail

Changing the list breaks the chaos balance between computers, and the system will allocate incorrect port number

PATENTED



4. Malicious Software Using Other Software Will Fail


Malicious Software

Command

Power Shell

Command

HMI

Command

Out to Network

- Outlook sends legitimate emails according to legitimate commands
- If or when Outlook has been compromised by hackers, every cyber defense company will detect it
- But the hackers are sophisticated - they insert malware, using other legitimate software

Current cyber solutions

Malicious software activates a chain of legitimate software, that eventually gives a seemingly legitimate command. Cyber systems will not block Outlook from going out to the network

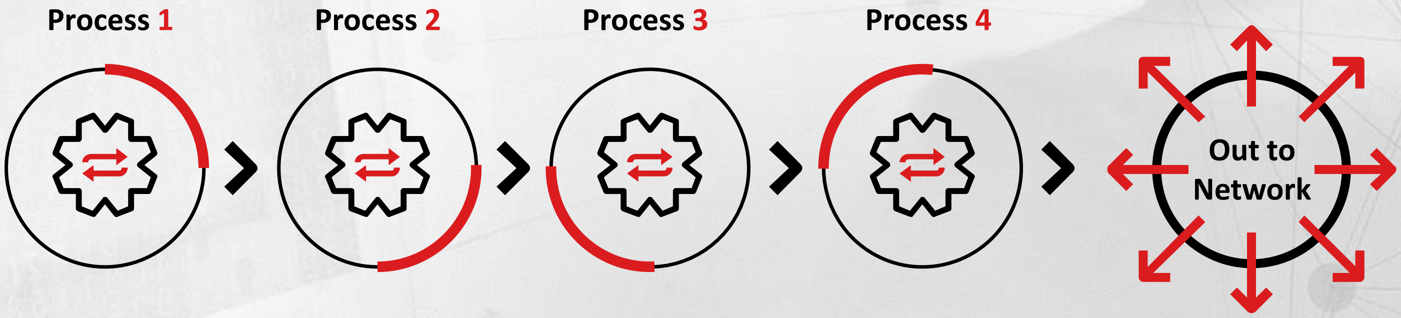
Cyber 2.0 - Reverse tracking

Our mechanism tracks the chain all the way back, using **Reverse Tracking Technology**, and blocks Outlook from going out to the network

Cyber 2.0

The Reverse Tracking

PATENTED PATENTED PATENTED



Every process and every library file that loads is recorded

The system takes their MD5 and SHA signature

Every access of a process to another process is recorded

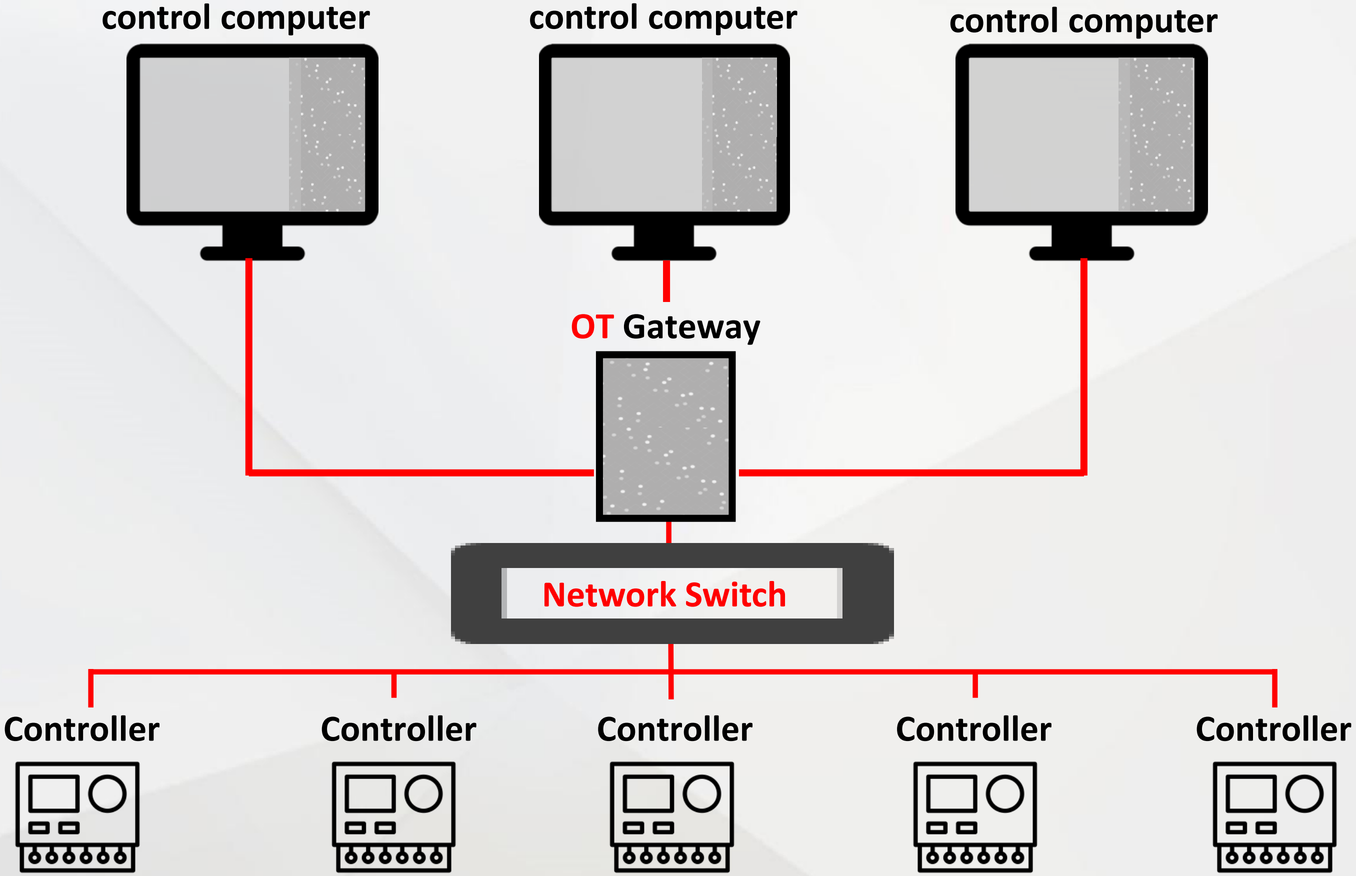
The Advantages of this Process

- We don’t read data
- Our solution complies with the Regulation and the GDPR (Privacy Protection Regulations)
- We do not create a load on the systems, nor do we slow down the network
- No software updates are required – allow cyber 2.0 to work in complete close environments

Cyber 2.0

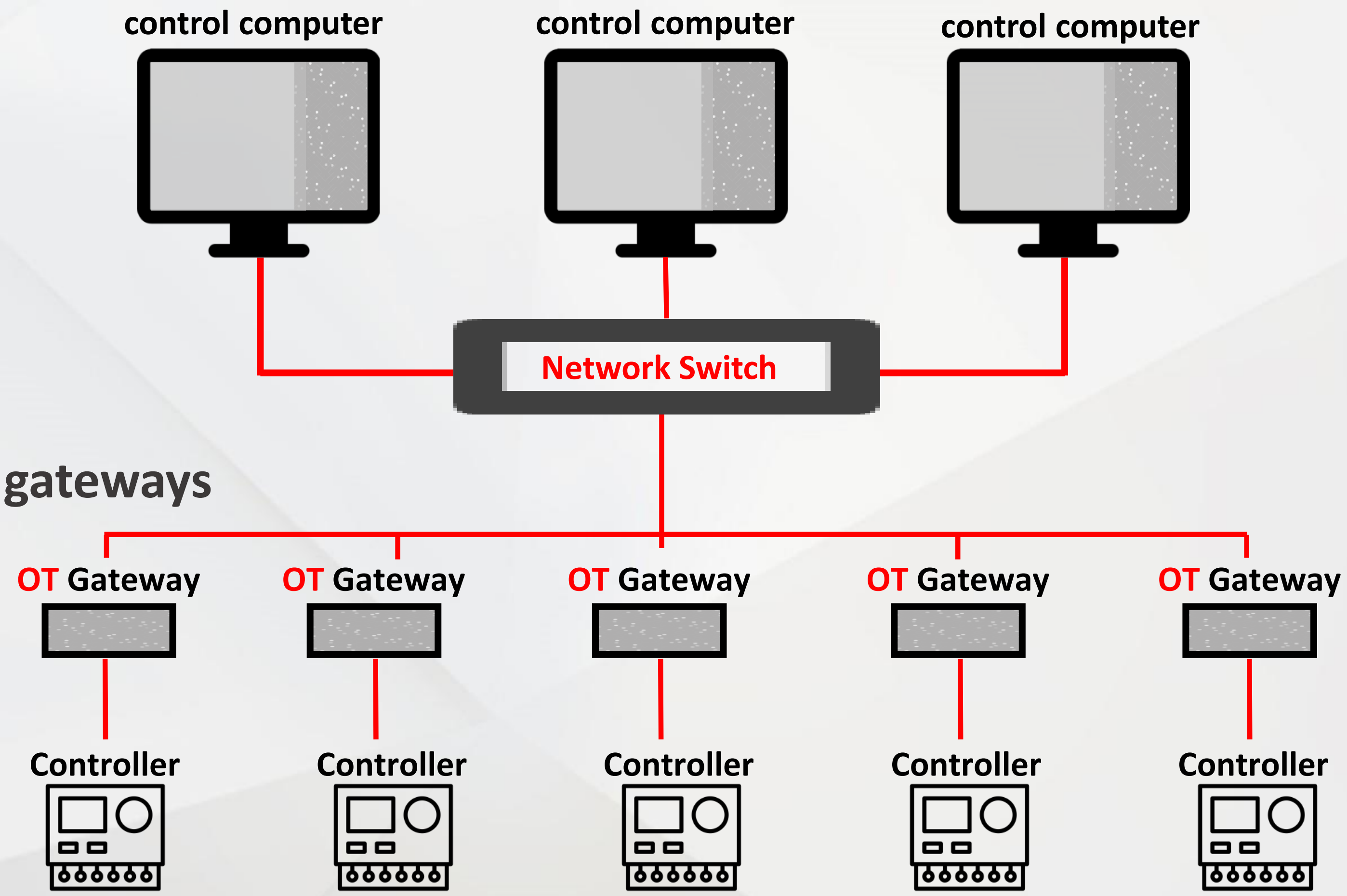
OT Full Protection in a Closed Environment

A single gateway



Cyber 2.0

OT Full Protection in a Widespread Environment



Multiple gateways