Cyber 2.0

CYBER 2.0 – TOTAL DEFENSE AGAINST THE SPREAD OF CYBER ATTACKS

Cyber 2.0 (founded in 2015) is the only system in the world that provides total defense against the spread of cyber attacks within organizational networks. (Viruses, ransomware, trojan, information leakage, browser hijacking, and every new attack)

The first computer may be penetrated, but Cyber 2.0 will isolate the attack and block its spreading.
The infected computer will also be blocked from sending information outside the organization, even if it was infected before the installation of Cyber 2.0

We are aware of the immediate responses: "There is no total defense", and "it's too good to be true".

Therefore, we decided to We announced The biggest hackers challenge: We invited all hackers to hack our system, for a reward of NIS 100,000. We didn’t ask them to find our weakness; We simply said: "No one is going to hack the system. Do you want to try? Go ahead".
All of them failed.

Next step: February 14th, 2019 in Atlanta, for a reward of $ 100,000.
And we will continue to do it all over the world, and to increase the reward each time.

We have many clients in process of implementation, who said at the start "It's too good to be true" and are now very satisfied with our technology.

All attacks (of hacking companies and hackers) against Cyber 2.0 failed.

Cyber 2.0 Registered 9 Patents (the most important were already approved in the USA).

We are supported by the Israel Innovation Authority (3 consecutive years)

We believe that Cyber 2.0 will make most other cyber-security systems irrelevant.

OUR UNIQUE SOLUTION: THE CHAOS MODEL, AND PREVENTION WITH NO DETECTION:

The Company has developed a **disruptive cyber-security technology,** that allows blocking all kinds of attacks.

The cyber world (defensive and offensive) is based on biological models, making them vulnerable to penetration by systems using similar models (virus vs. anti-virus). Cyber 2.0 system is based on a **mathematical chaos model**, that cannot be breached.

The classic process is "**Detection>Prevention**": first you have to detect and to recognize every new malicious software, then try to prevent (or to alert).

It is known that there is no 100% detection! (because of the emergence of new malicious software every second). It is also known that there is no 100% prevention! (because once the system is penetrated, the organization is no longer protected).

Cyber 2.0 does not fail the Detection Test, because it skips over it, effectively blocking every malware without first identifying it.
Cyber 2.0 does not fail the Prevention Test, because by using the **chaos** model, it blocks 100% of what is required to be blocked, since it is designed in a way that even if it is bypassed or deactivated, it still protects the organization.

Unlike other systems: We don’t study the organization’s routine, we don’t use attack database, we don’t look for anomalies, we don’t legitimize previous malicious programs, we don’t rely on the infected computer, we don’t have false positives or delayed response to real threats. Our system does nnot required any updates.

All the ordinary methods of attacking cyber companies, including bypassing, deactivating, adding malicious software to the legitimate software list- will fail**.**

Unique solution for the OT world

Although the attacks in the OT field have a greater significance than in the IT field, today there is no real defense against attacks in the OT field.
There is a fear of updates /changes in the controllers, and Regulating obliges mainly to identify / detect.

Cyber 2.0 is the only system that provides total prevention for the OT. There is no need to install over the controller, and It is easy to operate: just define the 1-2 software that are allowed to use the network resources. The system works in unconnected networks, and it does not slow dawn the network, and does not required any updates

SENIOR MANAGEMENT

Hertzel Ozer, Founder & CEO:

Highly experienced leader in telecommunications, retail, manufacturing, food and consumer goods industries:

- **CEO** & **Chairman of the Board** of **HOT Telecommunication Systems Group**
- **CEO** of the food division of **NESTLE ISRAEL group**
- **CEO** of **NESHER** – Israel Cement Enterprises

- **CEO** of **SHEKEM-food** – retail chain stores
- **VP** Marketing & Sales & Customer Care & Business Development of **BEZEQ-** Israel's Leading Telecommunications Company
- **Founder and Owner** of **All Jobs** – the leading online recruitment website in Israel
- **Chairman of the Board of Governors** of the **College of Management**, Israel
- **M.B.A** in Business Administration, **Hebrew University of Jerusalem**
- **B.A** in Economics and Statistics, **Hebrew University of Jerusalem**

Erez Kaplan Haelion – Founder & CTO:

Highly experienced in leading large-scale computer projects:

- **Advisor** of **Microsoft**
- **Designed, integrated and led projects** for complex Monitoring and Control Systems in the **Israeli Defense Forces**, **Orange Telecommunications**, **Ben-Gurion University**, and others
- **Designed, integrated and led** BI and SharePoint projects at The **College of Management, Afeka College, JDC** and others
- Served as founder & **CTO** in several startup companies
- **Initiated** several classified projects with the **Israeli Security Forces**

Holds a degree in **Engineering** from Amal B Vocational School

Sneer Rozenfeld– VP sales
Highly experienced in sales

- VP sales of Mobisec - System integrator
- Regional Sales Manager of Partner – Cellular Operator

Idan Ivgi - Professional Service Manager

- Infrastructure Manager or Arkia Airlines
- Head of System of Hertz Rent a Car

Link to company's presentation:

cyber20.com/Resources/Cyber20pre.ppsx