



EVGENY GONCHAROV

Kaspersky Lab

- Head of Kaspersky Lab ICS CERT
- More than 14 years of experience in IT security
- In 2014 led KL team that protected the Sochi 2014 Olympic Games' critical infrastructure
- Since 2014, has been driving ICS cybersecurity research and development

[linkedin.com/in/evgeny-goncharov-a4446634/](https://www.linkedin.com/in/evgeny-goncharov-a4446634/)





KASPERSKY

5 Myths of Industrial Cyber Security

Evgeny Goncharov

Head of Kaspersky Lab ICS CERT

Myth #1

”Our ICS are not connected to Internet”

...e.g. they are not accessible from Internet

...and therefore are not exposed to threats coming from Internet

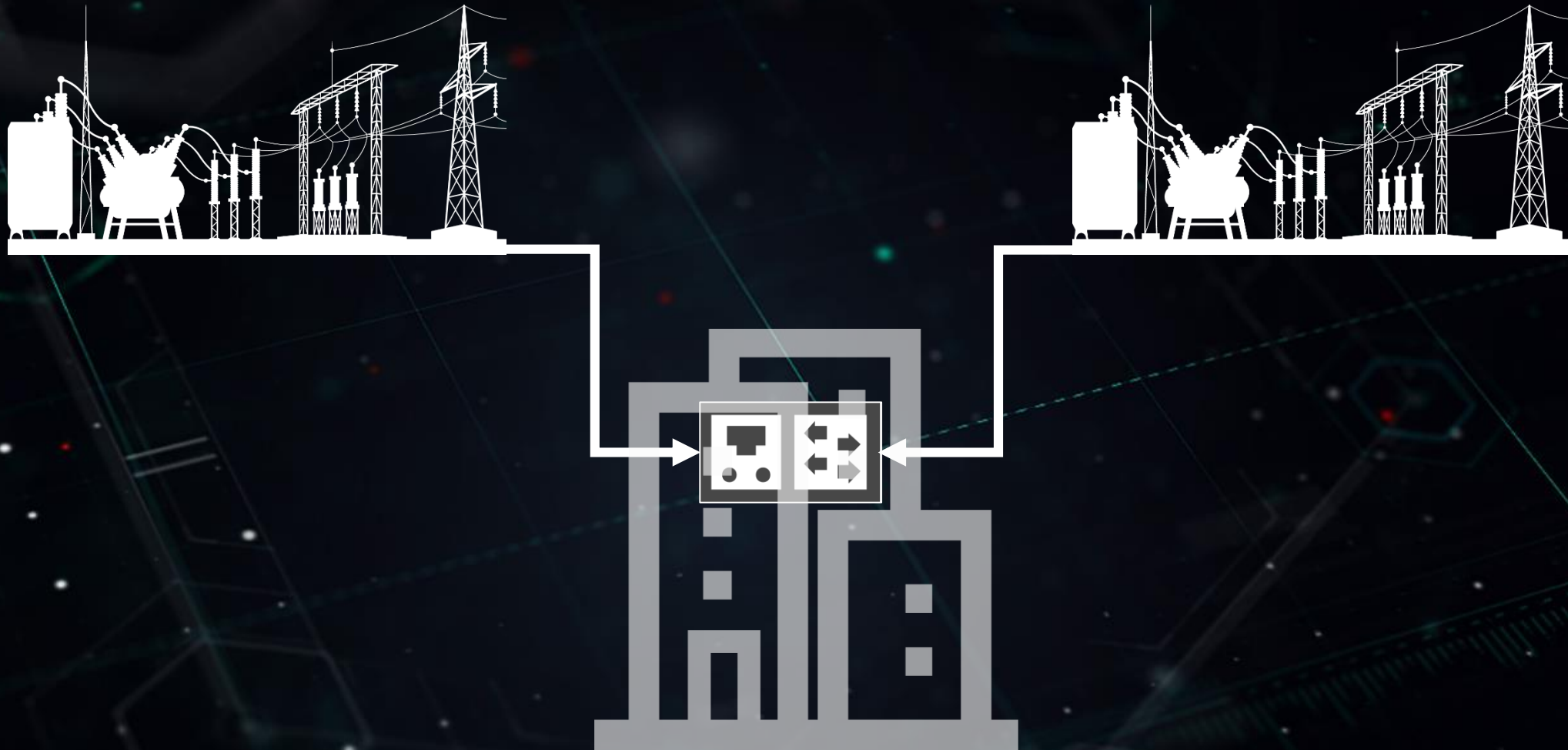
Myth #1: ICS are not connected to Internet

Scenario #1: multiple connected plants



Myth #1: ICS are not connected to Internet

Scenario #2: connected substations



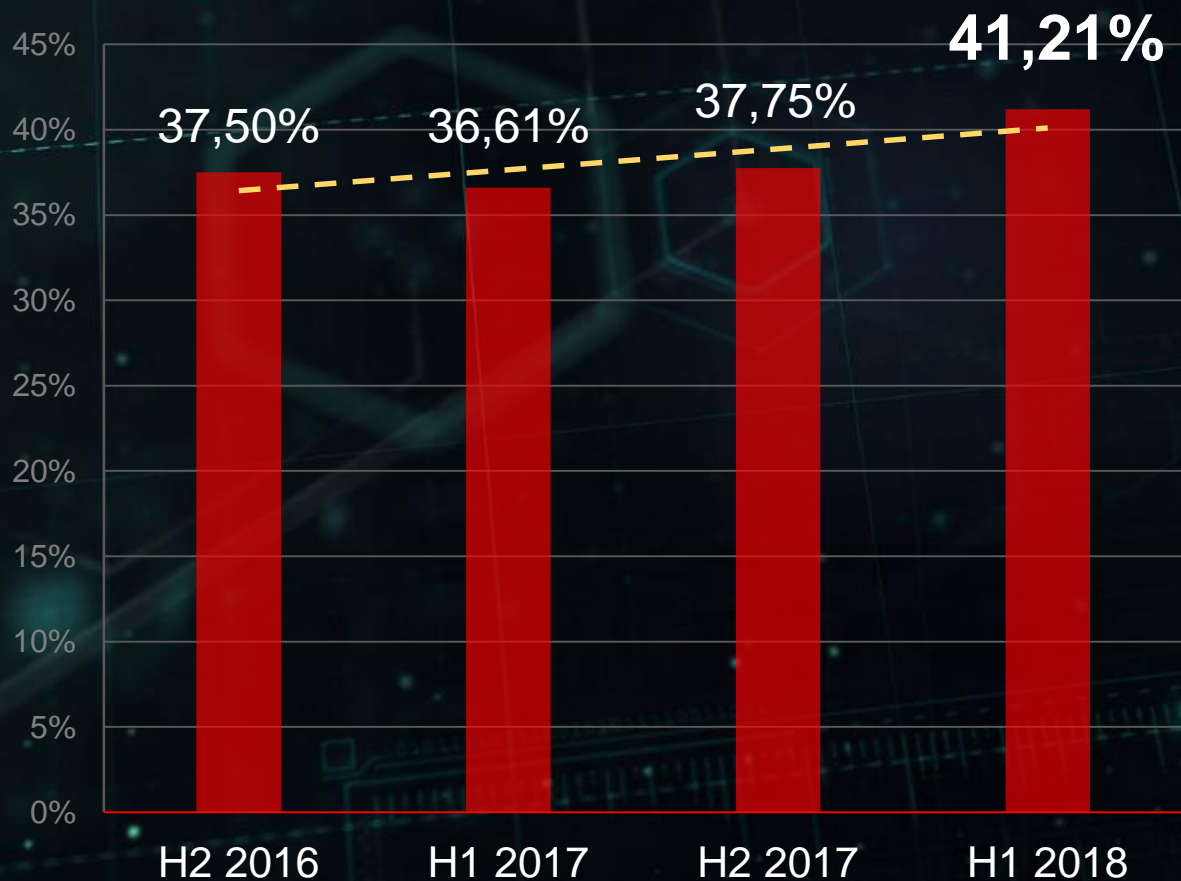
Myth #1: ICS are not connected to Internet

Scenario #3: bank in ICS network



Myth #1: ICS are not connected to Internet

% of ICS Computers Attacked by Malware – According to KSN Statistics



19.400 Malware modifications

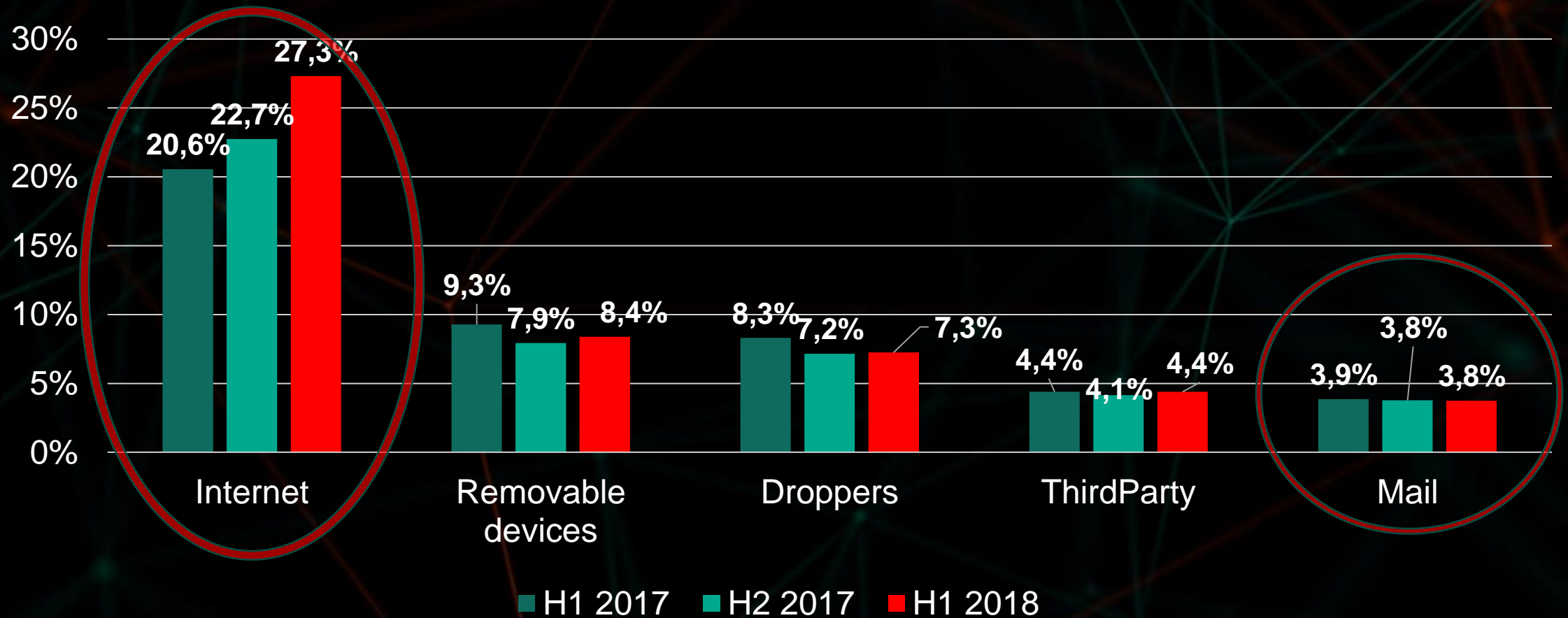
▲ UP 1500 compared to H2, 2017

2.800 Malware families

▲ UP 400 compared to H2, 2017

Myth #1: ICS are not connected to Internet

% of ICS computers attacked by malware via selected attack vector - according to KSN statistics



Myth #2

”It makes no practical sense to attack us”

...there are NO simple WAYS for the criminals to monetize an attack

...we are either not attacked or attacked by a highly capable adversary

...so there is no need to spent too much resources to defend

Myth #2: no practical sense to attack

Wide-spread attack campaigns targeting hundreds of industrial enterprises

Criminal attack campaigns

Nigerian phishing: **500+** Industrial organizations attacked world-wide

.RU campaign: **400+** Industrial organizations attacked in Russia

Politically motivated (?) attack campaigns

Energetic Bear / Crouching Yeti attacks in 2017-2018

It's getting harder to find differences

Myth #3

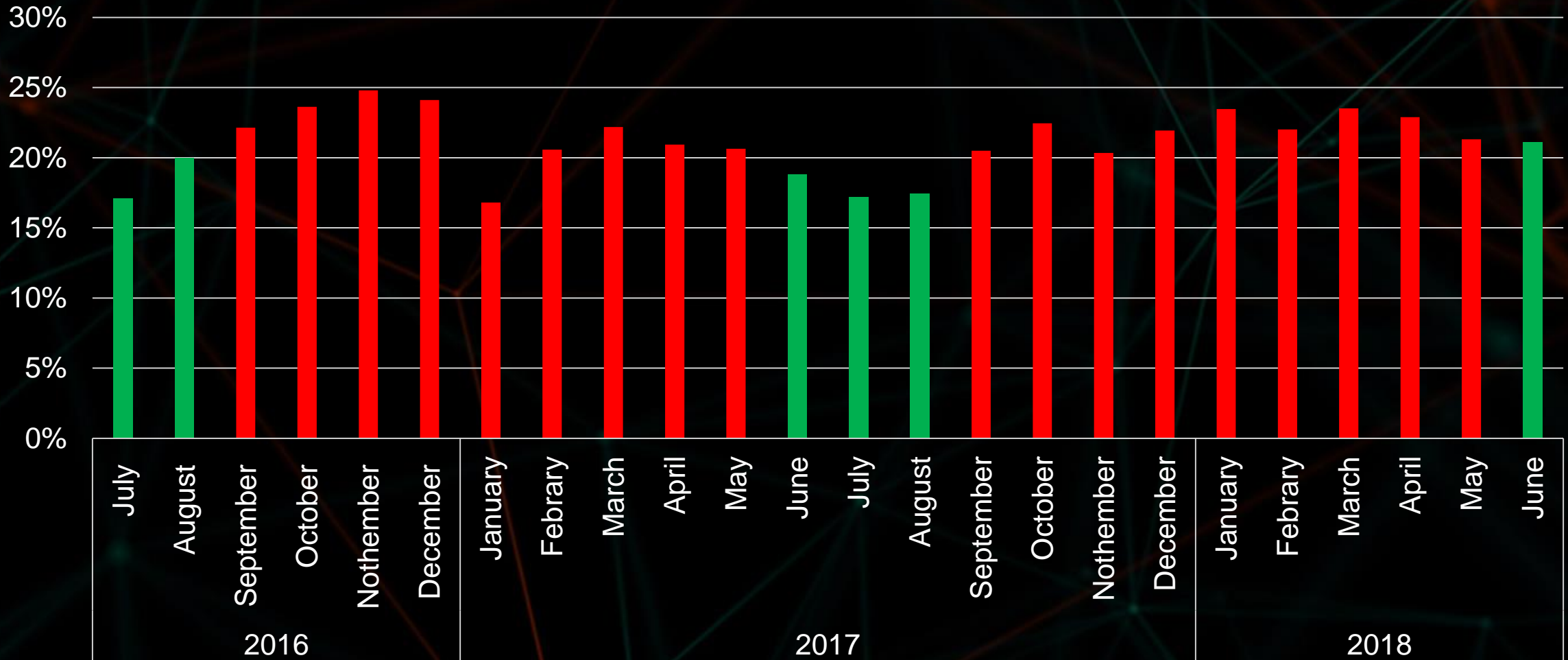
”It’s sufficient just to train the staff”

...to protect from random and criminal attacks we **just** need to train the staff

...**no** additional security measures and tools are needed

Myth #3: just train the staff

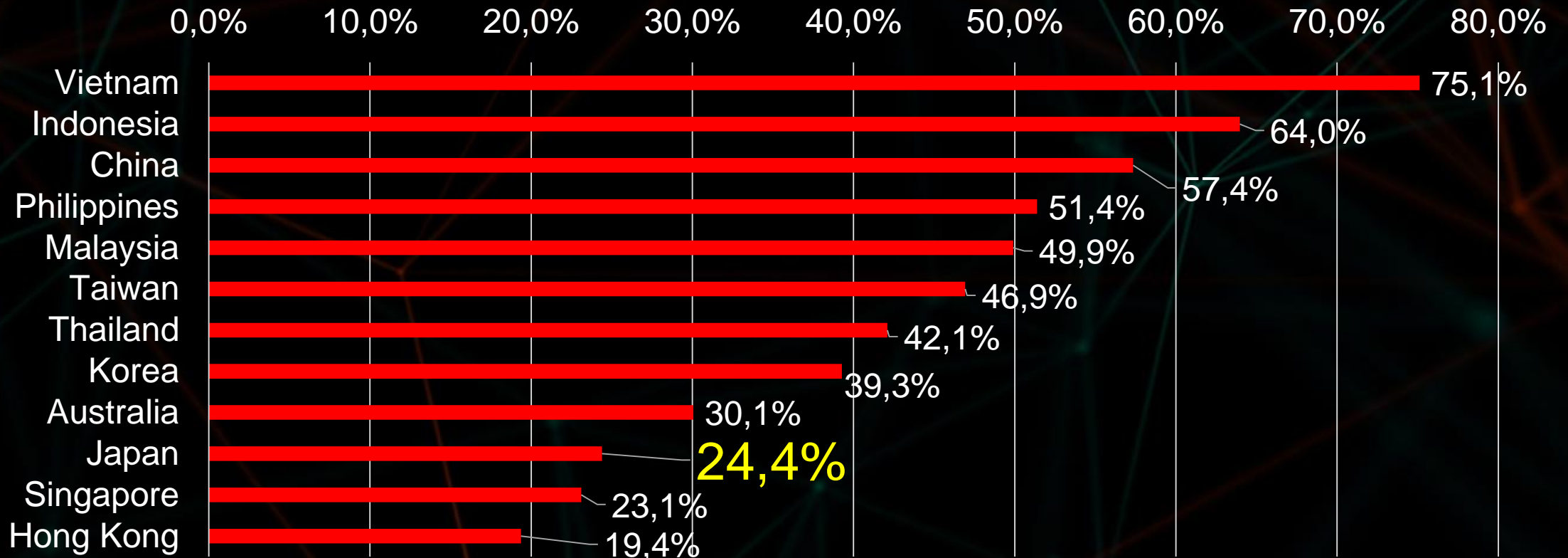
% of ICS computers attacked by malware - according to KSN statistics



¹²<https://ics-cert.kaspersky.com/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/>

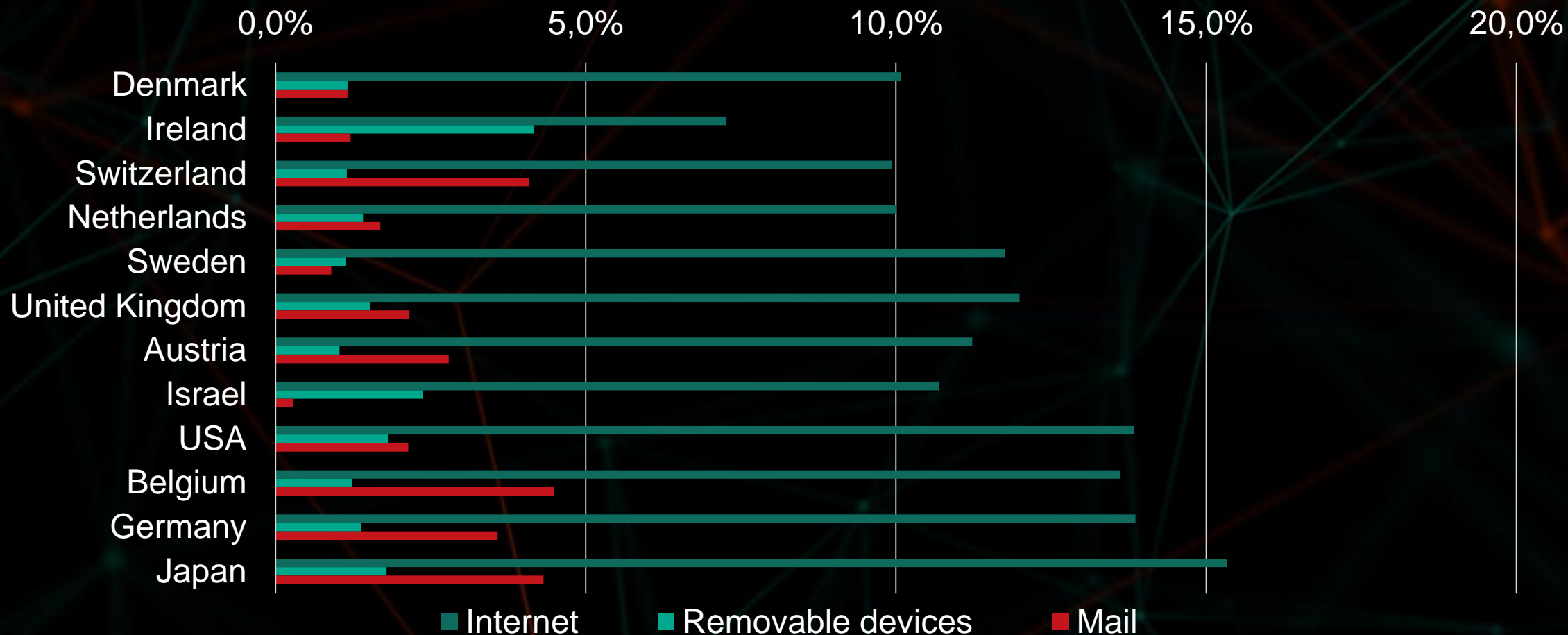
Myth #3: just train the staff

% of ICS computers attacked by malware in APAC, H1 2018 - according to KSN statistics



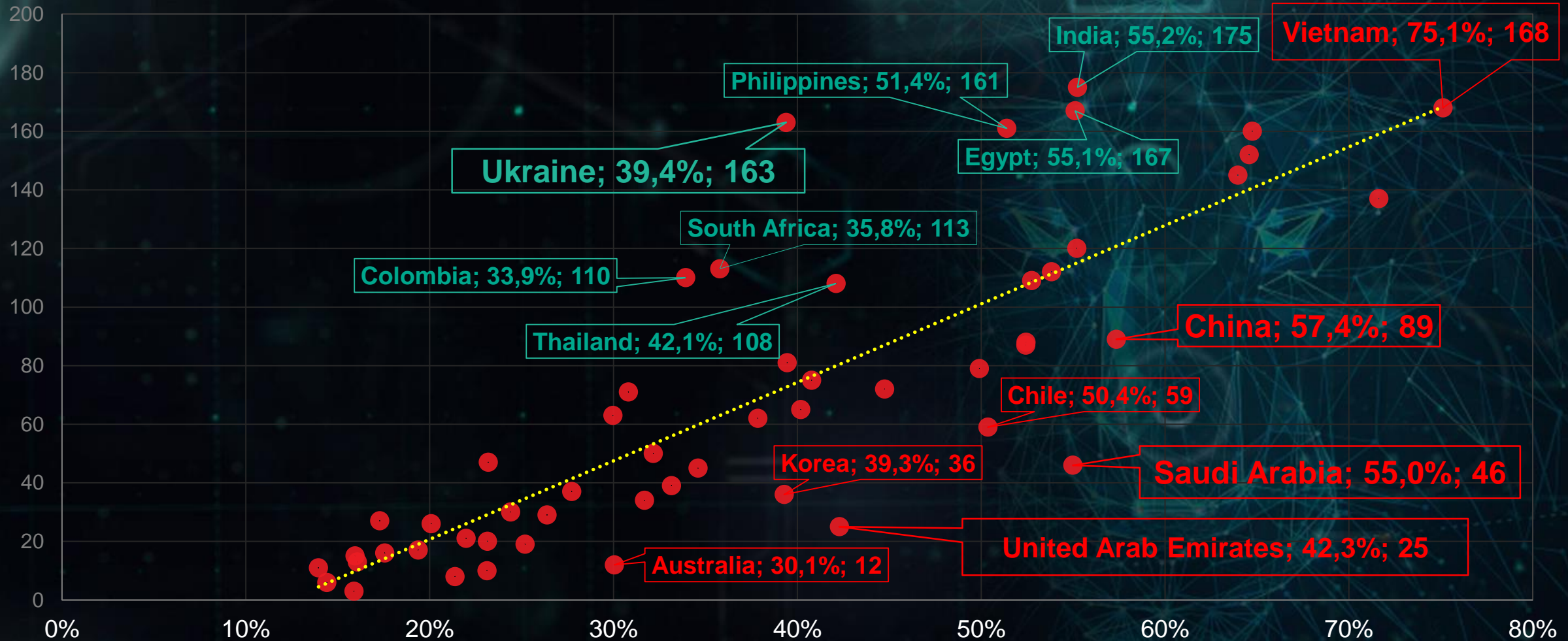
Myth #3: just train the staff

% of ICS computers attacked by malware in APAC, H1 2018 - according to KSN statistics



Myth #3: just train the staff

% of ICS Computers Attacked by Malware – According to KSN Statistics vs GDP Rank



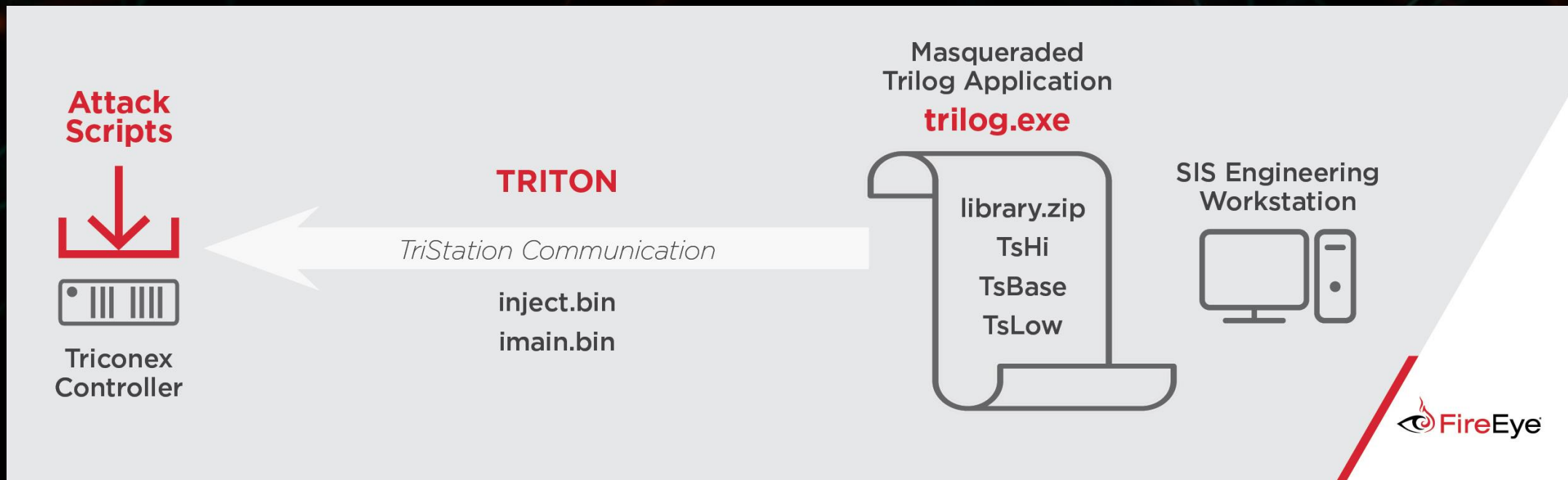
Myth #4

”Safety > Security”

- ...safety measures are sufficient to protect from cyber attacks
- ...we might need to upgrade them to mitigate cyber risks
- ...no additional security measures and tools are needed

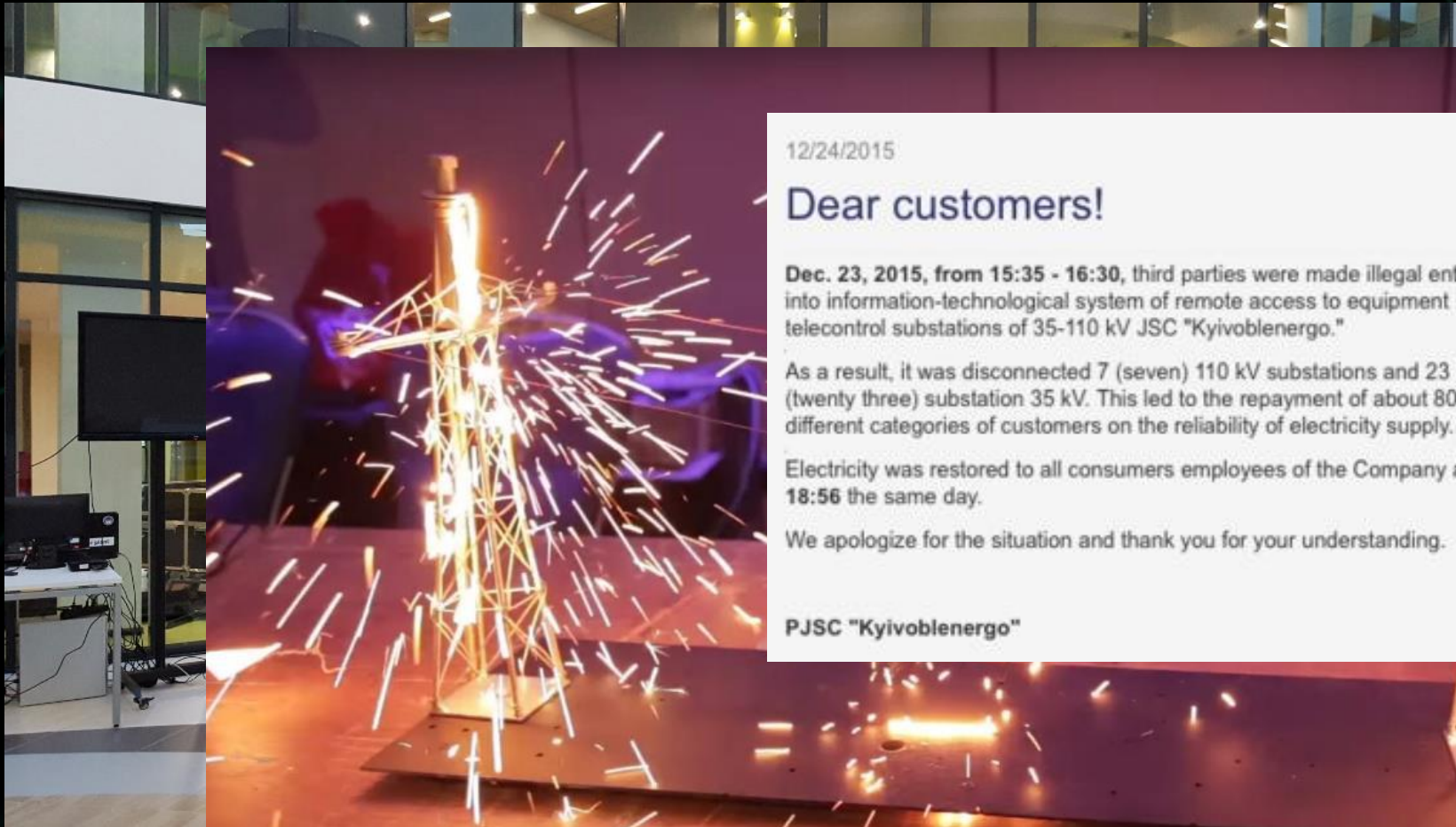
Myth #4: safety > security

TRITON case study



Myth #4: safety > security

Power & Energy sector cases



12/24/2015

Dear customers!


Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"



Myth #5

”New ICS products are secure by design”

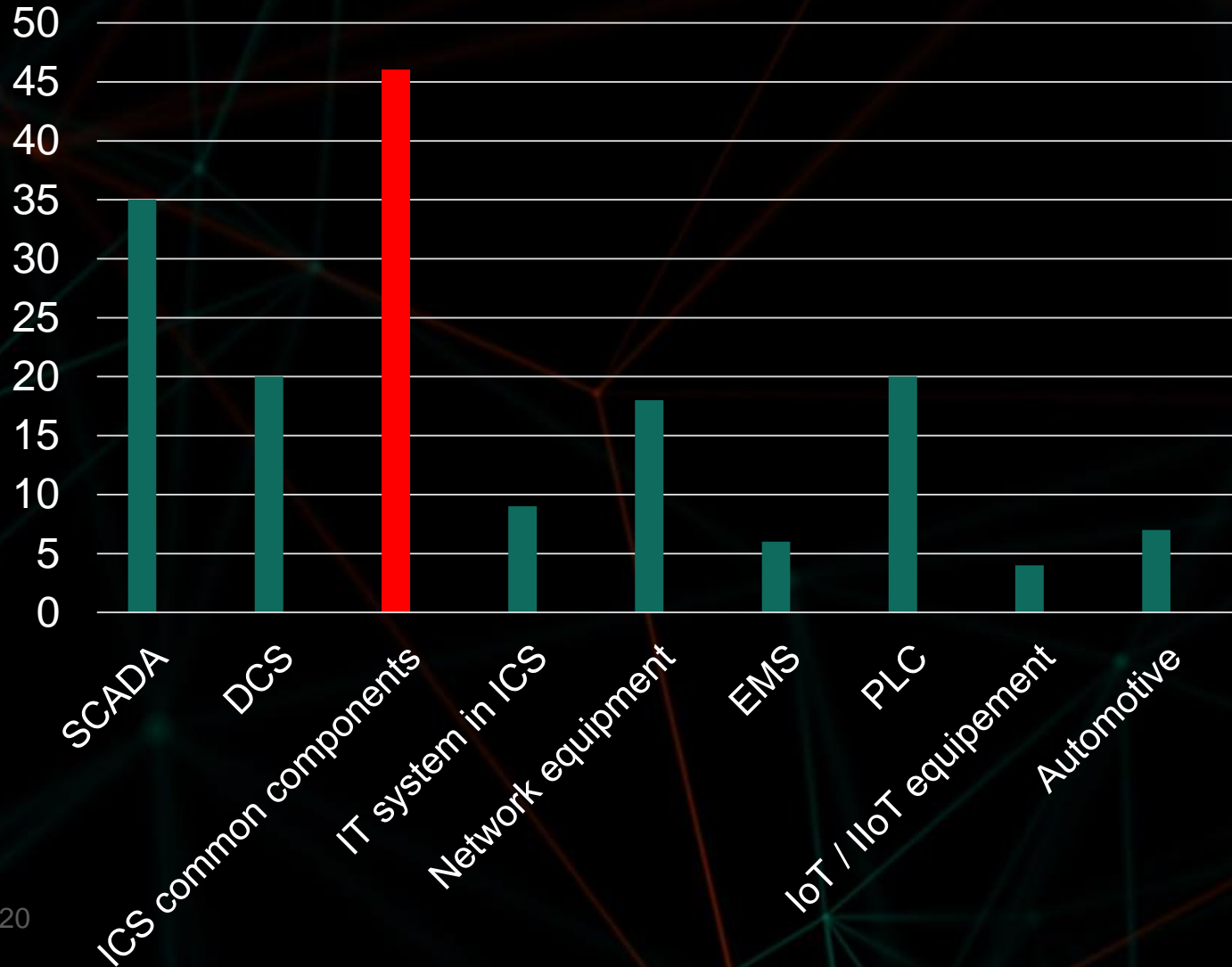
...since Stuxnet ICS vendors started to pay more attention to security

...their new products' architecture & implementation is getting more secure by design

...no additional security measures and tools are needed

Myth #5: new ICS products are secure by design

0-day vulnerabilities in ICS products found and reported by KL ICS CERT



Myth #5: new ICS products are secure by design

Vulnerable common technologies – OPC-UA case study

GE is First to Implement and Release New OPC-UA Standard with Launch of Global Discovery Server

Browses for Registered Server

GE GDS

On behalf of UA Application:

- Registers OPC Client or Server
- Obtains signed certificate
- Downloads trust lists

The diagram shows a process flow where a client browses for a registered server (GE GDS). The GDS then acts on behalf of the UA application to register the client, obtain a signed certificate, and download trust lists.

OPC FOUNDATION
The Industrial Interoperability Standard™

LET OUR OPC UA COMPLIANT ALGORITHMS DO THE WORK FOR YOU

About Membership Products Certification Markets & Collaboration Resources

Security

Security

Security Bulletins

The OPC Foundation publishes security bulletins that affect software that it maintains or distributes. In many cases these bulletins will affect code that OPC vendors incorporate into their products. As a result, vendors will have to patch their products to address the vulnerabilities identified.

On May 10th, 2017 Kaspersky Labs released a report identifying 17 zero day vulnerabilities in OPC Foundation code.

The OPC Foundation's formal response can be found [here](#).

Kaspersky Labs released a report identifying 17 zero day vulnerabilities



GE is First to Implement and Release New OPC-UA Standard with Launch of Global Discovery Server

Secure-by-design methodologies and richer context for data provide a foundation for cloud-based

Secure-by-design methodologies

UP to 468 products could possibly be affected:
<https://opcfoundation.org/products>

Kaspersky Lab ICS CERT

ics-cert.kaspersky.com

KASPERSKY 