The final showdown: Business vs Research.

Who contributes to the ICS security community best?

Anton Shipulin vs Vladimir Dashchenko

kaspersky

Anton Shipulin

- Kaspersky Industrial Cybersecurity Business Development
- Head of program committee of the international KICS con in Sochi
- Coordinator for Russia at Industrial Cybersecurity Center (CCI)
- Co-founder of the ICS cybersecurity community RUSCADASEC
- Certified SCADA Security Architect (CSSA), CISSP, CEH
- Honored Beer ISAC coin holder #50
- Tweeting responsibly at @shipulin_anton

Vladimir Dashchenko

- Kaspersky ICS CERT Vulnerability Research
- Part of SAS (Security Analyst Summit) program committee
- Acknowledged by US ICS CERT, Siemens, Schneider Electric, Rockwell Automation, Mitsubishi and others
- Kaspersky Industrial CTF co-creator
- Beer ISAC coin holder
- @VDashchenko

Mission first

Building a safer world

We believe in a tomorrow where technology improves all of our lives. Which is why we secure it, so everyone, everywhere, can benefit from the endless opportunities it brings.

KASPERSKY IS A GLOBAL CYBERSECURITY COMPANY FOUNDED IN 1997. KASPERSKY'S DEEP THREAT INTELLIGENCE AND SECURITY EXPERTISE IS CONSTANTLY TRANSFORMING INTO INNOVATIVE SECURITY SOLUTIONS AND SERVICES TO PROTECT BUSINESSES, CRITICAL INFRASTRUCTURE, GOVERNMENTS AND CONSUMERS AROUND THE GLOBE. THE COMPANY'S COMPREHENSIVE SECURITY PORTFOLIO INCLUDES LEADING ENDPOINT PROTECTION AND A NUMBER OF SPECIALIZED SECURITY SOLUTIONS AND SERVICES TO FIGHT SOPHISTICATED AND EVOLVING DIGITAL THREATS. OVER 400 MILLION USERS ARE PROTECTED BY KASPERSKY TECHNOLOGIES AND WE HELP 270,000 CORPORATE CLIENTS PROTECT WHAT MATTERS MOST TO THEM.

ics.kaspersky.com | @KasperskyICS

kaspersky

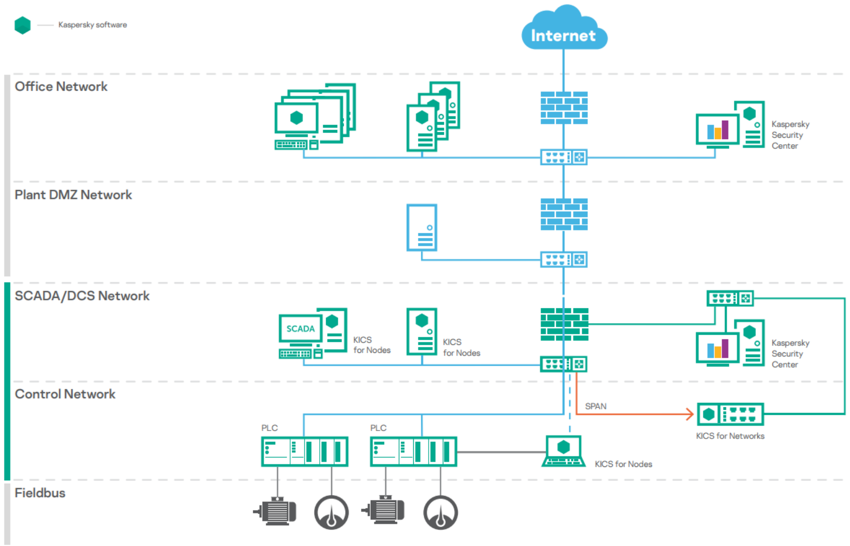
Collaboration Program for Industrial Laboratories and Research Communities

Technologies to laboratories at

- CERT/CSIRTS
- Universities
- Cyber Ranges/Testbeds
- MSSP/ SOC
- Industrial companies

For education and research purposes

- Attack Analysis
- Defense Mechanism Tests/Analysis
- Impact Analysis
- Vulnerability Analysis
- Education and Training
- Threat Analysis
- Performance/QoS Analysis
- Creation of Policies and(or) Standards

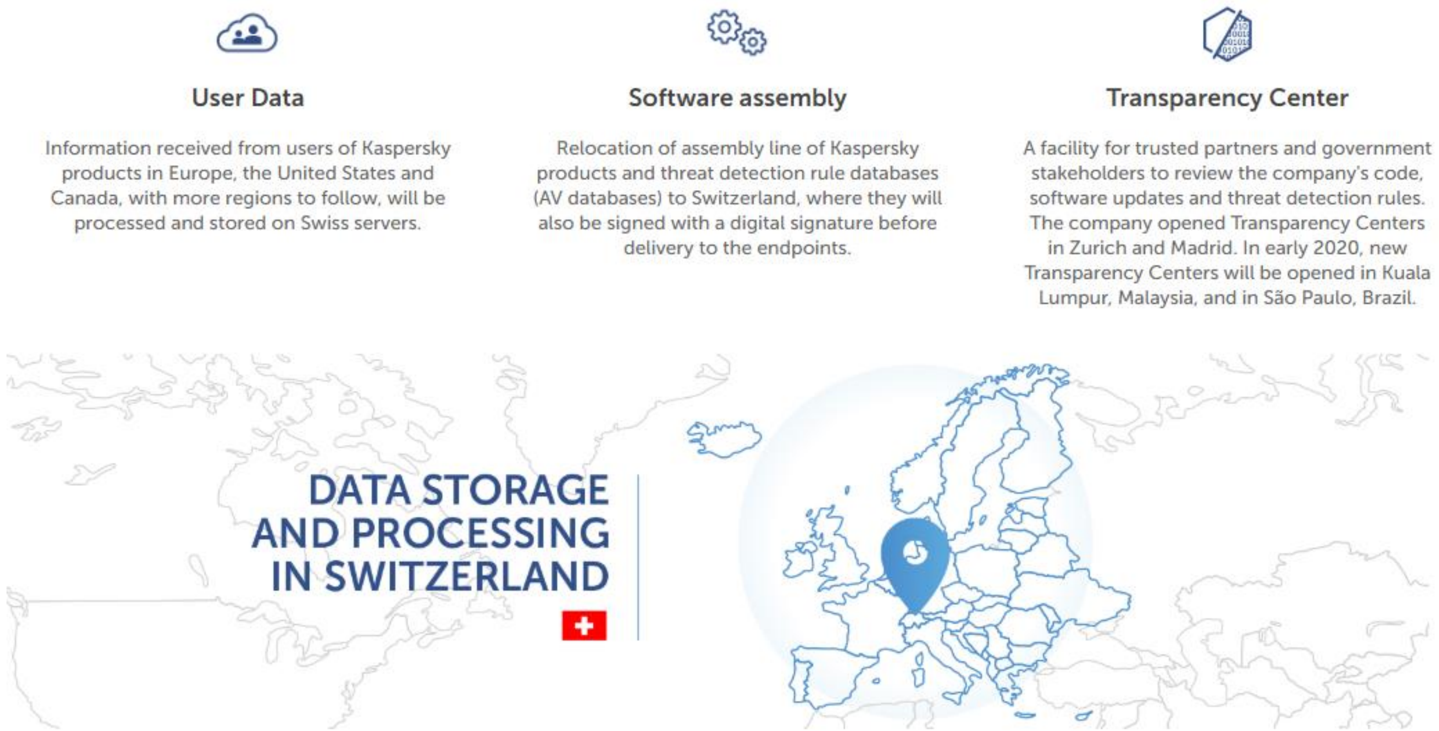


Kaspersky Industrial Cybersecurity Conference in Sochi / KICS con 2020, September 2-4

Industrial Cybersecurity 2018:
Opportunities and challenges in Digital Transformation
Sochi, September 19-21
KASPERSKY
Kaspersky Industrial Cybersecurity
Industrial Cybersecurity: Safeguarding Progress
Saint Petersburg, Russia
September -29

https://ics.kaspersky.com/conference/

Kaspersky Global Transparency Initiative



User Data

Information received from users of Kaspersky products in Europe, the United States and Canada, with more regions to follow, will be processed and stored on Swiss servers.

Software assembly

Relocation of assembly line of Kaspersky products and threat detection rule databases (AV databases) to Switzerland, where they will also be signed with a digital signature before delivery to the endpoints.

Transparency Center

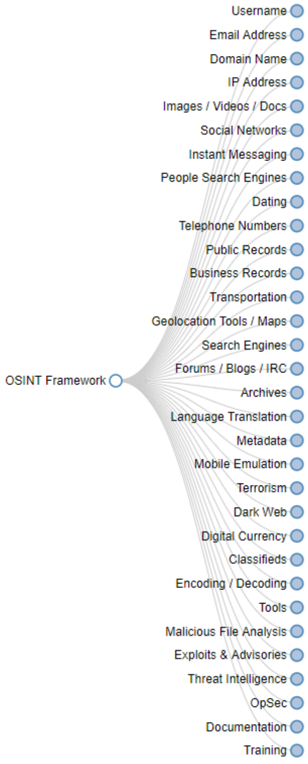
A facility for trusted partners and government stakeholders to review the company's code, software updates and threat detection rules. The company opened Transparency Centers in Zurich and Madrid. In early 2020, new Transparency Centers will be opened in Kuala Lumpur, Malaysia, and in São Paulo, Brazil.

DATA STORAGE AND PROCESSING IN SWITZERLAND

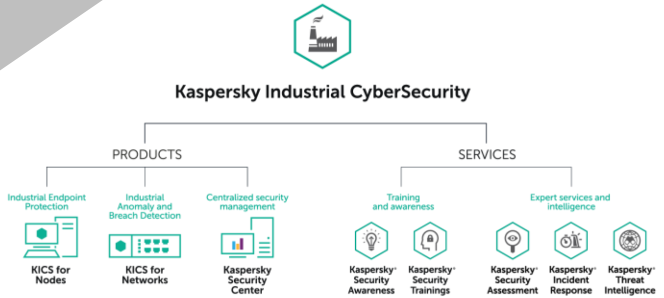
TransparencyCenter@kaspersky.com

https://www.kaspersky.com/transparency-center

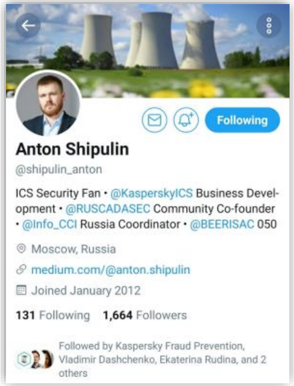
OSINT For The Good Of The Business And The Community



https://osintframework.com/


Kaspersky Industrial CyberSecurity
PRODUCTS
Industrial Endpoint Protection
KICS for Nodes
Industrial Anomaly and Breach Detection
KICS for Networks
Centralized security management
Kaspersky Security Center
SERVICES
Training and awareness
Kaspersky Security Awareness
Kaspersky Security Trainings
Expert services and intelligence
Kaspersky Security Assessment
Kaspersky Incident Response
Kaspersky Threat Intelligence

https://ics.kaspersky.com/



Following

Anton Shipulin

@shipulin_anton

ICS Security Fan • @KasperskyICS Business Development • @RUSCADASEC Community Co-founder • @Info_CCI Russia Coordinator • @BEERISAC 050

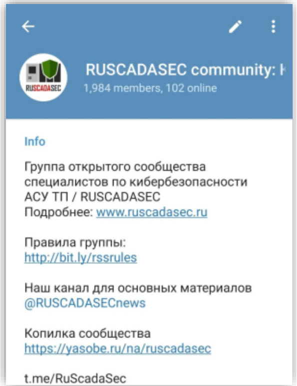
Moscow, Russia

medium.com/@anton.shipulin

Joined January 2012

131 Following **1,664** Followers

Followed by Kaspersky Fraud Prevention, Vladimir Dashchenko, Ekaterina Rudina, and 2 others



RUSCADASEC community: I

1,984 members, 102 online

Info

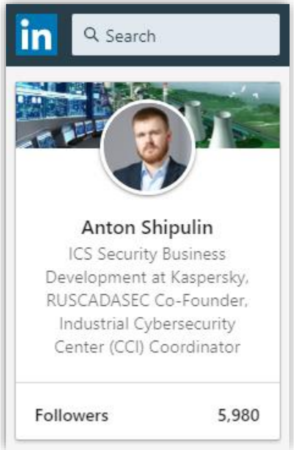
Группа открытого сообщества
специалистов по кибербезопасности
АСУ ТП / RUSCADASEC
Подробнее: www.ruscadasec.ru

Правила группы:
http://bit.ly/rssrules

Наш канал для основных материалов
@RUSCADASECnews

Копилка сообщества
https://yasobe.ru/na/ruscadasec

t.me/RuScadaSec

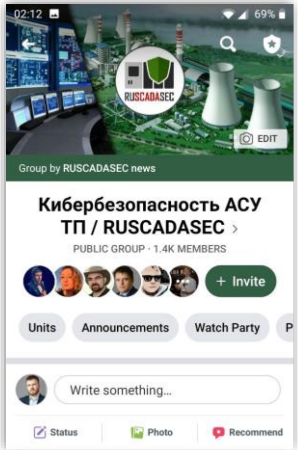


Search

Anton Shipulin

ICS Security Business Development at Kaspersky, RUSCADASEC Co-Founder, Industrial Cybersecurity Center (CCI) Coordinator

Followers 5,980



02:12 69%

EDIT

Group by RUSCADASEC news

Кибербезопасность АСУ ТП / RUSCADASEC ›

PUBLIC GROUP · 1.4K MEMBERS

+ Invite

Units | Announcements | Watch Party | P

Write something...

Status | Photo | Recommend

Russian Industrial Cybersecurity Community / RUSCADASEC

- An independent non-profit initiative on developing the open Russian-speaking international community of industrial cyber security

- Goals:
  - Awareness & knowledge sharing,
  - Professional networking,
  - Market development.

- Best ideas from other initiatives: SCADASEC, S4, CS3, CCI, SANS ICS Community, Beer ISAC, ICS Village etc.

2K members

Join our Facebook group

Join our Telegram group

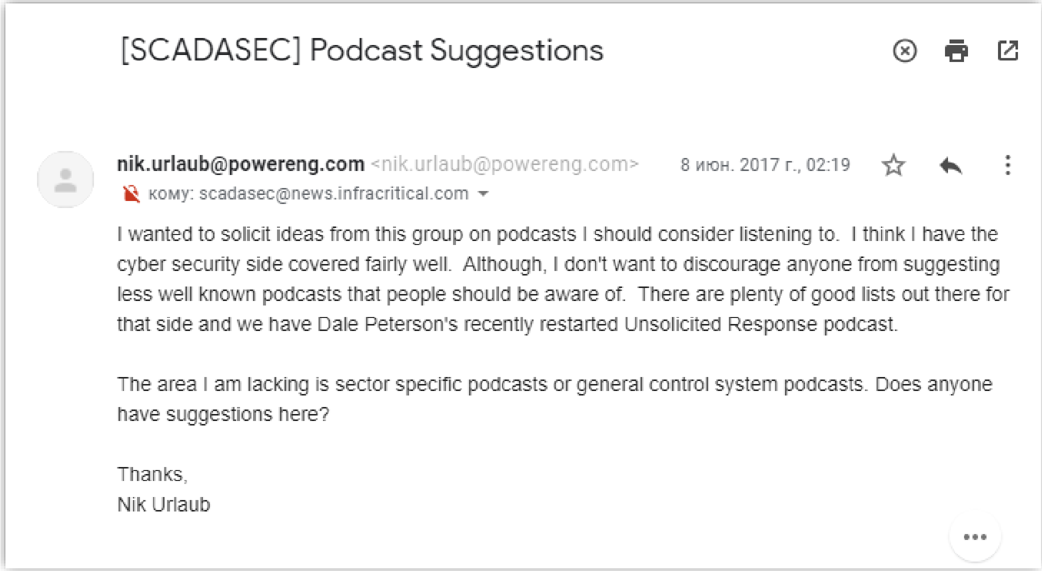
RUSCADASEC Con2020

April, Moscow

RUSCADASEC KEEP CALM AND PROTECT ICS

ruscadasec.ru
con.ruscadasec.ru
info@ruscadasec.com

@BEERISAC: CPS/ICS Security Podcast Playlist



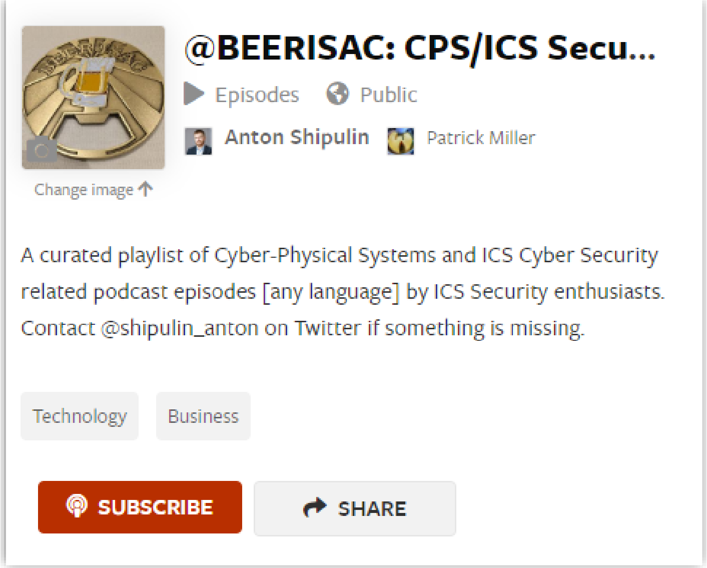
[SCADASEC] Podcast Suggestions

nik.urlaub@powereng.com <nik.urlaub@powereng.com> 8 июн. 2017 г., 02:19
кому: scadasec@news.infracritical.com

I wanted to solicit ideas from this group on podcasts I should consider listening to. I think I have the cyber security side covered fairly well. Although, I don't want to discourage anyone from suggesting less well known podcasts that people should be aware of. There are plenty of good lists out there for that side and we have Dale Peterson's recently restarted Unsolicited Response podcast.

The area I am lacking is sector specific podcasts or general control system podcasts. Does anyone have suggestions here?

Thanks,
Nik Urlaub



@BEERISAC: CPS/ICS Secu...

A curated playlist of Cyber-Physical Systems and ICS Cyber Security related podcast episodes [any language] by ICS Security enthusiasts. Contact @shipulin_anton on Twitter if something is missing.

...

LISTEN NOTES

bit.ly/beerisac

Educate, share your knowledge!

Commercial things	**Free of charge**
ICS Cybersecurity Awareness Training IoT/IIoT Vulnerability research and exploitation (with reference) ICS Digital Forensics Advanced fuzzing for Windows and Linux ICS Pentest	webinars/bright talks University courses CTFs

Knowledge sharing

Practical University Courses:

- ICS Security
- Vulnerability research
- Fuzzing
- IoT/IIoT Security
- Malware analysis
- Threat hunting for ICS
- And many many more

Capture The Flag for students:

- ICS and non-ICS tasks
- Online and offline
- Attack and defense/task based/research
- and destroy
- Infrastructure for online CTFs
- Provide write-ups for each task; explanation

what is a vulnerability behind it

- So much fun!

Educate, share your knowledge!

CTF

Gamification of practical security task solving

Task-based CTF: Solving different task categories (web security, binary exploitation, cryptography, reverse engineering, forensics etc..). Individual or team-based. We have environment and infrastructure.
Audience: Students, SOCs, Product security teams, security researchers, developers, forensics and investigation experts

Attack-and-Defense CTF: Usually played by teams. You have to protect your infrastructure, keep it stable and running and attack other teams.
Audience: SOCs, CERTs, security researchers, govs, students

Research-and-Destroy CTF: Played by teams or individually. You need to research infrastructure (IT+Industrial), find pre-made or 0day vulnerabilities, break from one network to another and influence technological process. Usually cyber-physical effect is shown.
Audience: SOCs, CERTs, Product Security Teams, security researchers, govs

IoT Vulnerability research

3-4 days

Target Audience

Product Security Teams, Researchers, Architects, Product owners

5 Main Topics

1. Typical IoT Architectures
2. How to extract firmware
3. Firmware reverse engineering
4. Cloud Vulnerabilities
5. Vulnerability research and exploiting vulnerabilities

Key Take outs / Skills

- IoT firmware extraction
- Vulnerability identification
- Vulnerability Exploitation

Trainings

Advanced fuzzing for Windows

3-4 days

Target Audience

Product Security Teams, Researchers, Architects, Product owners

5 Main Topics

1. Fuzzing types
2. Various tools
3. Fuzzer customization
4. How improve bug identification results
5. Searching for real 0day

Key Take outs / Skills

- Fuzzing for Windows
- Customize your fuzzer for better results
- Unusual fuzzing techniques

ICS Incident Response

3-4 days

Target Audience

ICS personnel, security experts, IR teams

5 Main Topics

1. Common Forensics (x86)
2. Network Forensics
3. Memory Forensics
4. Forensics for ICS devices (e.g. PLC) and software (e.g. SCADA)
5. Enterprise Forensics (tools and methods for big networks)

Key Take outs / Skills

- Conduct successful forensics for ICS
- Apply specific tools and methods to ICS software and hardware
- Reconstruct incident timeline

Plug’n’Play Security: Enhance your solution

ICS Malware data feed:

- Once in 5 min you get IoCs
- Based on ICS dataset only
- Specific industries

Launch: March 2020

0day/1day detection exploitation:

- We all know that it takes sooooo much time to fix a bug
- ICS exploitation in the wild is rare - maybe we just don’t see all the things. No statistics, no IR etc..
- We research a lot – you can use all the knowledge that we have
- Advanced advisories for each found bug & SNORT rules to detect

Plug'n'Play Security: Expand your knowledge

ICS TI and APT reports:

- A custom chapter at Threat Intelligence Portal
- ICS and suppliers focused reports
- All the threat actors – financial gangs, espionage campaigns etc..

Launch: March 2020

VulnDB project:

- There's a huge inconsistence of current security advisories

Contribution to the global ICS/IIoT Security standardization

industrial internet CONSORTIUM

ISO

ITU International Telecommunication Union

IEC

IEEE

enisa European Network and Information Security Agency

GLOBAL PLATFORM
The Standard for Managing Applications on Secure Chip Technology

OPC FOUNDATION

industrial internet CONSORTIUM

www.iiconsortium.org

Key Safety Challenges for the IIoT

An Industrial Internet Consortium Technical White Paper

IIC:WHT:IN6:V1.0:PB:20171201

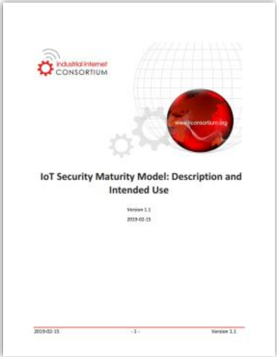
2017-12-01 Version 1.0

industrial internet CONSORTIUM

www.iiconsortium.org

Industrial Internet of Things
Volume G4: Security Framework

IIC:PUB:G4:V1.0:PB:20160926



industrial internet CONSORTIUM

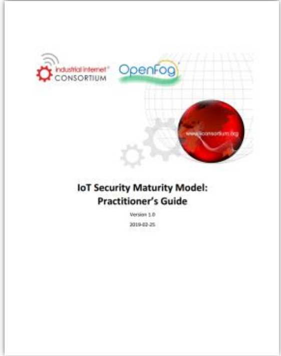
www.iiconsortium.org

IoT Security Maturity Model: Description and Intended Use

Version 1.1

2019-02-15

2019-02-15 - 1 - Version 1.1



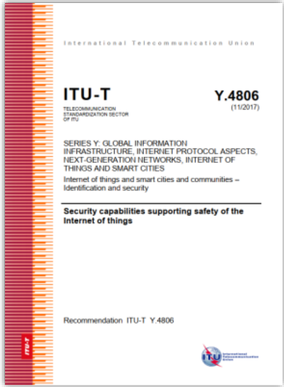
industrial internet CONSORTIUM OpenFog

www.iiconsortium.org

IoT Security Maturity Model:
Practitioner's Guide

Version 1.0

2019-02-25



International Telecommunication Union

ITU-T
TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4806
(11/2017)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Identification and security

Security capabilities supporting safety of the Internet of things

Recommendation ITU-T Y.4806

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

GOOD PRACTICES FOR SECURITY OF IOT

Secure Software Development Lifecycle

NOVEMBER 2019

enisa

Baseline Security Recommendations for IoT

in the context of Critical Information Infrastructures

NOVEMBER 2017

www.enisa.europa.eu European Union Agency For Network And Information Security

enisa

Good Practices for Security of Internet of Things

in the context of Smart Manufacturing

NOVEMBER 2018

www.enisa.europa.eu European Union Agency For Network and Information Security

In conclusion

> “ Do goodness and throw it into the water; it will appear in front of you.

Armenian proverb

Thank you!

Anton Shipulin

39A/3 Leningradskoe Shosse, Moscow
T: +7 (495) 797 8700
Anton.Shipulin@kaspersky.com
@shipulin_anton

ics.kaspersky.com

Vladimir Dashchenko

39A/3 Leningradskoe Shosse, Moscow
T: +7 (495) 797 8700
Vladimir.Dashchenko@kaspersky.com
@Vdashchenko

Ics-cert.kaspersky.com

kaspersky