

Industrial Cybersecurity: Opportunities and challenges in Digital Transformation



Ruslan Stefanov
20.09.2018

KICS*HICS=TESTED & SECURED

Collaboration with Kaspersky Lab in Russia and Customs Union

Honeywell

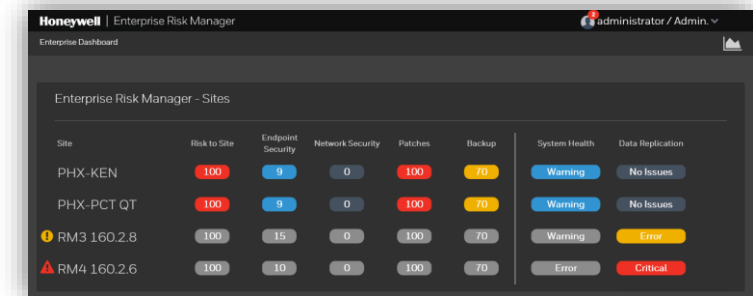
THE POWER OF **CONNECTED**

Honeywell ICS (HICS) 2018 News

- ControlEdge™ - the first in the world, certified for ISASecure® Embedded Device Security Assurance (EDSA) Level 2
 - ControlEdge™ Remote Terminal Unit (UOC)
 - ControlEdge™ Remote Terminal Unit (RTU)
 - ControlEdge™ Remote Terminal Unit (PLC)

<http://www.isasecure.org/en-US/End-Users/ISASecure-Certified-Devices>

- Cyber security solutions portfolio renewal
 - New version Risk Manager R170
 - New version ICS Shield
 - Cyber Vantage Managed Security Services (MSS)



Honeywell in Russia and Customs Union

Presence in Russia

- 1974 – office in Moscow was opened
- All business lines and functions (engineers, sales, marketing, logistics, service, etc.)
- Local production in Moscow, Arzamas and Lipetsk.
- Honeywell Process Automation Systems and UOP technologies are deployed at major Russian refineries.
- Honeywell equipment is deployed at Olympic in Sochi, CPC, IKEA, MEGA, Hermitage, Bolshoi Theater.
- Honeywell Air & Space products are installed on aircrafts (SSJ100, MC21) and helicopters produced in Russia.



More than
1000
employees



25 offices in Russia, Belarus,
Kazakhstan, Uzbekistan,
Armenia

Cyber Security approach in Russian Federation

- FSTEC licenses
- Knowledge of legislation and requirements
- Collaboration with strong local security vendors and integrators
- Solutions portfolio based on leading local security products



Solutions portfolio



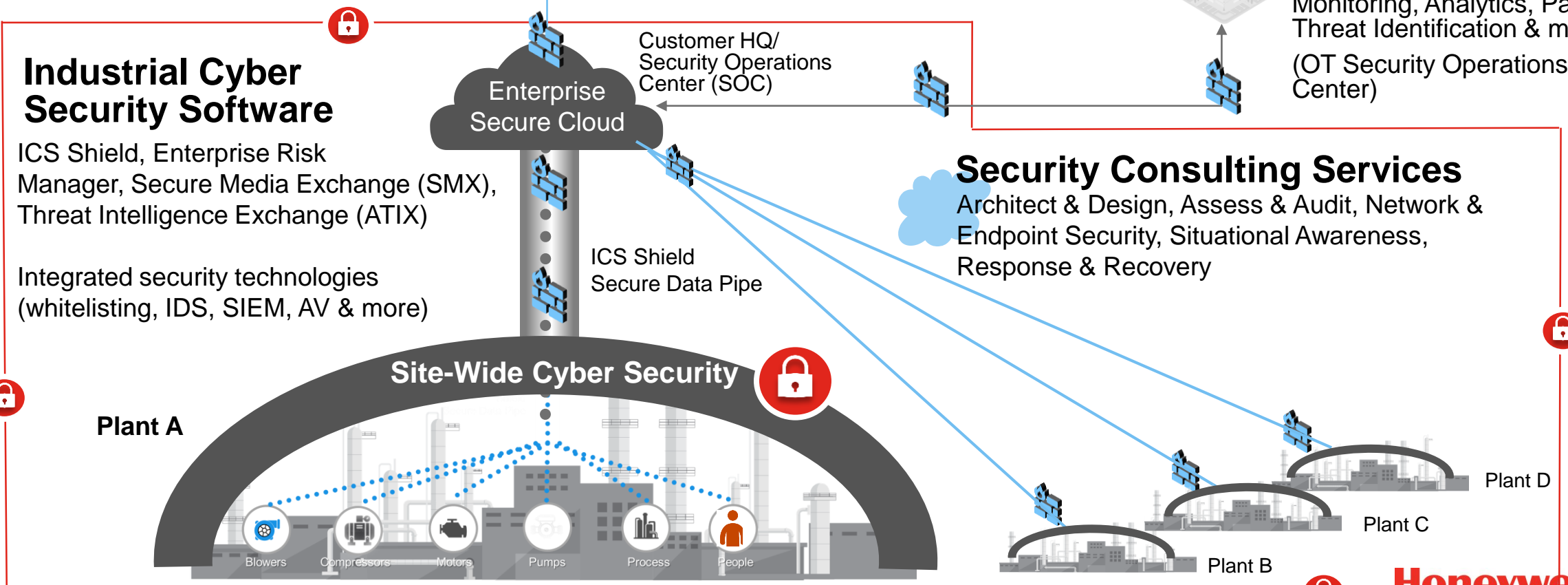
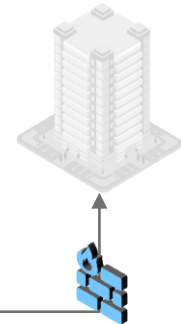
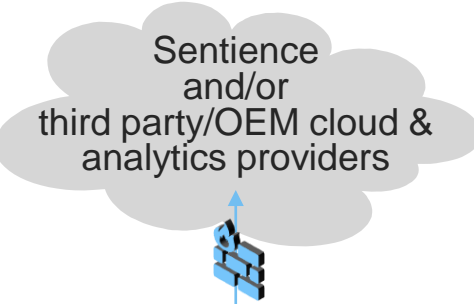
Honeywell's Industrial Cyber Security Solutions

- Multi-site, defense-in-depth approach
- Multi-vendor security management
- Single provider convenience & trust



CyberVantage™ Managed Security Services

Monitoring, Analytics, Patching, Threat Identification & more
(OT Security Operations Center)



Industrial Cyber Security Software

ICS Shield, Enterprise Risk Manager, Secure Media Exchange (SMX), Threat Intelligence Exchange (ATIX)

Integrated security technologies (whitelisting, IDS, SIEM, AV & more)

Security Consulting Services

Architect & Design, Assess & Audit, Network & Endpoint Security, Situational Awareness, Response & Recovery

Site-Wide Cyber Security

Plant A



Plant D

Plant C

Plant B



Benefits and specifics of collaborative approach



- Individual protection of DCS based on ESID – Experion System ID
- Unified solution for overall DCS computers protection
- Maintenance cost optimization for the site/plant security system
- Tested cyber security solution
- Tested updates and trusted distribution infrastructure

What is done in 2018

FAT in Lipetsk



FAT in Sofia (Bulgaria)



Compatibility Tests at refinery



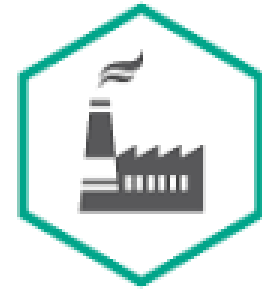
First direct shipment (oil&gas)



What is proposed

- KICS for Nodes annual maintenance:
 - For each Experion PKS identified by ESID
 - After compatibility approval for ESID

- KICS for Nodes annual maintenance includes:
 - Correct KICS for Nodes configuration profile
 - Tested updates
 - Updates and profiles distribution



**Kaspersky®
Industrial
CyberSecurity**

Compatibility test/check

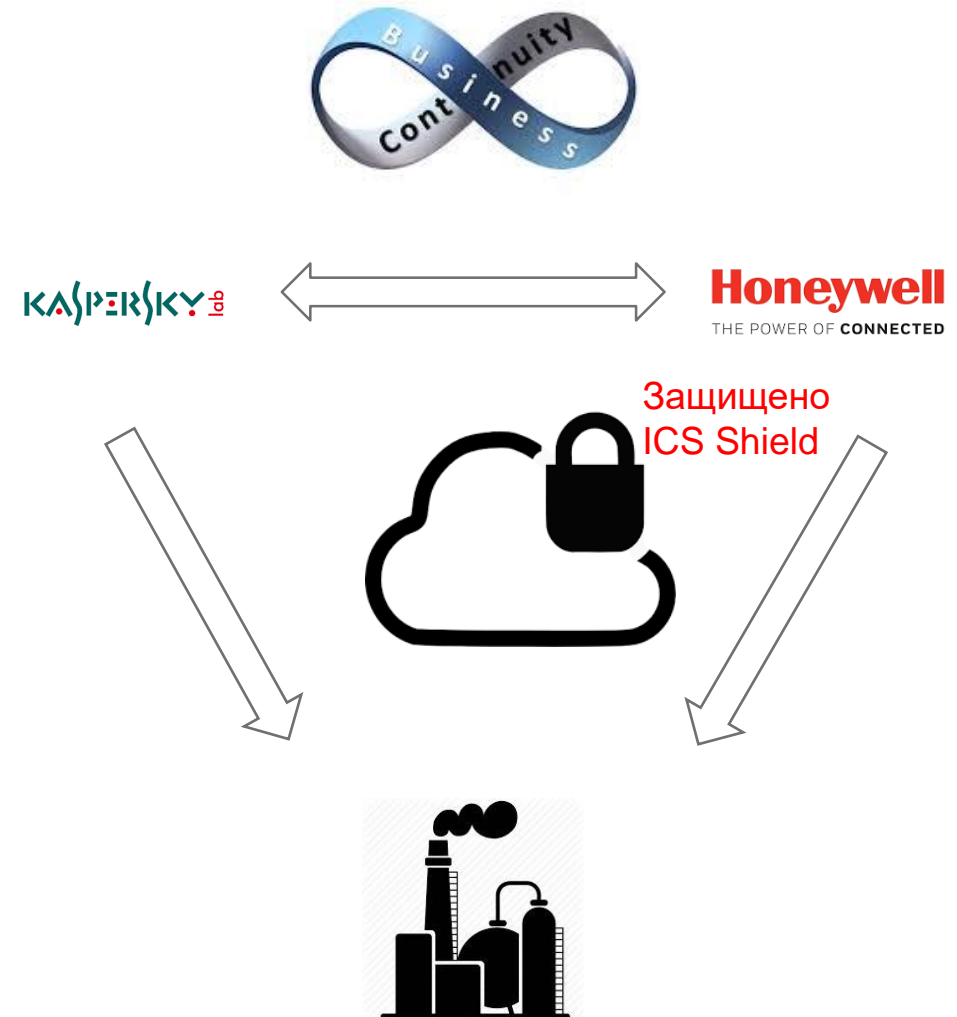
- Why?
 - About 20 Experion PKS versions
 - New versions are issued both for Experion PKS and KICS for Nodes
 - DCS productivity, continuity and security
 - Compliance with security requirements
 - Correct KICS for Nodes configuration profile
 - DCS executables “white” lists
 - Compatibility approval
- When and Where?
 - Factory acceptance tests (FAT)
 - Site acceptance tests (SAT)
 - Maintenance time-off on Customer’s site
 - Non-critical Experion PKS components at Customer’s site



**Kaspersky®
Industrial
CyberSecurity**

Updates testing and distribution

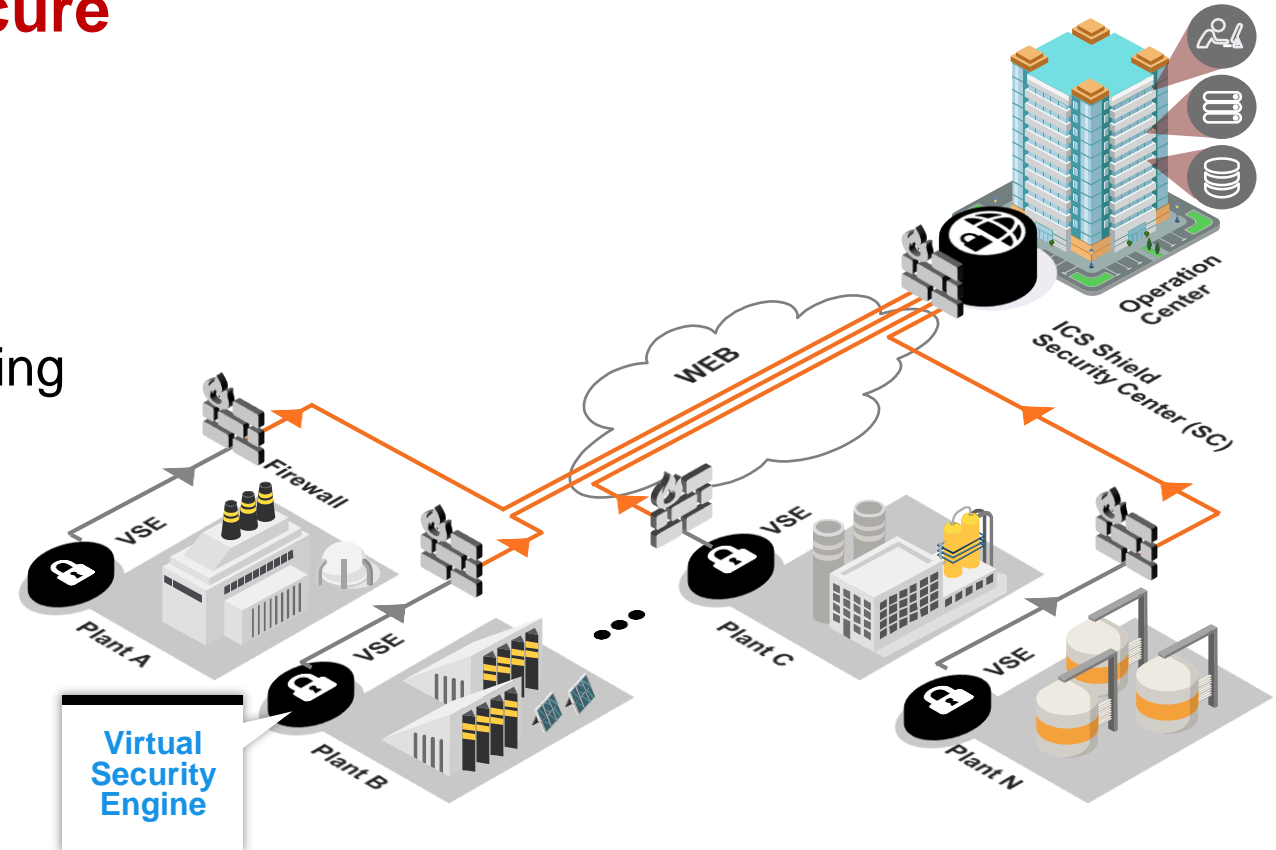
- Why?
 - Operational assurance
 - Reduce downtime risk
- When and Where?
 - As new updates are published
 - Virtual Lab Datacenter-based tests
- How to distribute?
 - Manually
 - Automatically via ICS Shield infrastructure



ICS Shield Infrastructure

Distributed architecture and secure tunnel from plants to center

- Install SC at the data center
- Install VSEs at each plant
- Establish a secure tunnel, outbound, using port 443, TLS encrypted
- One FW rule to manage all remote connections



Links and resources

HICS

www.becybersecure.com

Honeywell SMX named "The Best Product of the Year 2017"

Secure Media Exchange was named "The Best Product of the Year 2017" in "Industrial Safety" category, by Control Engineering China. Visit hwi.co.uk/SMX to know more about SMX.

Control Engineering China 2017

Download eBook | Explore Our Cyber Security Lab | Watch Videos | Read Case Studies | Know Our Technology Partners

Honeywell Launches First Industrial Cyber Security Center Of Excellence In The Middle East

The state-of-the-art facility will strengthen industrial cyber security preparedness in the Middle East by providing a safe environment to test process control network vulnerabilities and training customers through real-time attack simulations.

EXPERIENCE WORLD-CLASS CYBER SECURITY

Read the press release

Download eBook | Explore Our Cyber Security Lab | Watch Videos | Read Case Studies | Know Our Technology Partners

Security updates

<https://www.honeywellprocess.com/en-US/support/Pages/security-updates.aspx>

Honeywell THE POWER OF CONNECTED

Purchase Online | News & Events | Resources | About Us | Contact Us

Search Explore & Training

HOME | EXPLORE | SUPPORT | TRAINING | MY ACCOUNT

Webinars | Products A-Z | Product Families A-Z | HCP | PAS | BMA-PBM

Security Updates

[Home](#) > [Support](#)

Print Page
Add to My Book
SHARE

Meltdown and Spectre Vulnerabilities

Honeywell is aware of the recently published Meltdown and Spectre vulnerabilities. These vulnerabilities take advantage of optimization methods for CPU instruction execution and could cause information disclosure. There are no known exploits at this point in time. Honeywell is actively qualifying patches as they become available to mitigate the Meltdown and Spectre vulnerabilities. Honeywell will continue to work with our hardware partners in order to identify and qualify security patches to impacted hardware as these patches become available.

Honeywell has qualified the following updates for Windows:

Operating System Version	Update KB
Windows 7 SP1 and Windows Server 2008 R2 SP1	KB4056894
Windows 8.1 and Windows Server 2012 R2	KB4056895
Windows Server 2012	KB4056896
Windows 10 Version 1607 and Windows Server 2016	KB4056890

For customers who use Honeywell's Managed Industrial Cyber Security Services, these updates will be available on 16 January 2018. For other customers, all updates will be included in the January Microsoft Security Updates at www.honeywellprocess.com.

Note that mitigations for these vulnerabilities may decrease PC platform performance; the magnitude of the decrease depends on the specific platforms in use. All Honeywell products, including Honeywell applications that run on standalone platforms, care should be taken to ensure that this decrease in platform performance does not significantly affect critical operations.

For more information on these vulnerabilities, please see <https://www.us-cert.gov/ncas/current-activity/2018/01/03/Meltdown-and-Spectre-Side-Channel-Vulnerabilities> and <https://www.us-cert.gov/ncas/alerts/TA18-004A>.

It is recommended that you follow the best practices described on this page under "Honeywell Recommends Steps to Mitigate Threats Posed by Malware," including installing the latest qualified Windows patches.

Vulnerability report

<https://honeywell.com/pages/vulnerabilityreporting.aspx>

Honeywell CONTACT HONEYWELL | CORPORATE CITIZENSHIP | WORLDWIDE

PRODUCTS & SERVICES | SOLUTIONS & TECHNOLOGIES | ABOUT US | INVESTORS | NEWS

SEARCH

Honeywell International

Vulnerability Reporting

Text Size: + -

Report a Security Vulnerability

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services. If you are a security researcher and believe you have found a security vulnerability, please send an e-mail to us at security@honeywell.com with as much of the below information as possible. This information will help us to better understand the nature and scope of the possible issue.

- Type of issue (buffer overflow, SQL injection, cross-site scripting, etc.)
- Product and version that contains the bug
- Service packs, security updates, or other updates for the product you have installed
- Any special configuration required to reproduce the issue
- Step-by-step instructions to reproduce the issue
- Proof-of-concept or exploit code
- Impact of the issue, including how an attacker could exploit the issue

To encrypt your message to our PGP key, please download it from [here](#).

You should receive a response within 24 hours. If for some reason you do not, please follow up with us to ensure we received your original message.

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited in a cyber attack to reduce the operational or security assurances provided by the software.

Thank you

www.becybersecure.com