

Информационная безопасность АСУ ТП критически важных объектов



Руслан Стефанов
27.02.2019

**МУЛЬТИСЕРВИСНАЯ ПЛАТФОРМА ОБЕСПЕЧЕНИЯ И
УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ КРУПНОГО ИЛИ
ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОГО ПРЕДПРИЯТИЯ**

Honeywell

Новости Honeywell

- ТАСС, 31 января. Американская компания Honeywell International открыла в особой экономической зоне (ОЭЗ) "Липецк" в Грязинском районе Липецкой области завод по производству систем автоматизации, пожарообнаружения, газовых детекторов.
- Объем инвестиций завода на площадке ОЭЗ «Липецк» составил 900 миллионов рублей. Источник: ГТРК «Липецк»



ГЛАВНАЯ

Липецкий «Honeywell» обеспечит россиян системами автоматизации и безопасности

31.01.2019 12:27

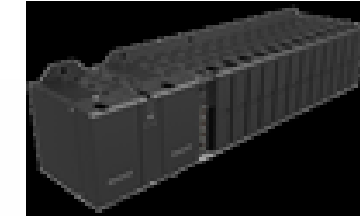


В эти минуты на территории ОЭЗ «Липецк» торжественно открывают завод компании «Honeywell». Известно, что ранее он уже был запущен, но лишь в техническом режиме.

Honeywell

Новости Honeywell Industrial Cybersecurity

- ControlEdge™ - первые и единственные в мире контроллеры, получившие сертификаты ISA Secure® Embedded Device Security Assurance (EDSA) Level 2
 - <http://www.isasecure.org/en-US/End-Users/ISAsecure-Certified-Devices>
- Safety Manager Control Processor с Quad Processor Pack QPP-0002 и Universal Safety Interface USI-0001 ISA Secure EDSA Level 1
- Новая версия Secure Media Exchange не просто обнаруживает вредоносное ПО, но и позволяет выявлять атаки следующего поколения, связанные с USB-носителями, сохраняя участие человека для подтверждения USB-устройств



Квалифицированное решение Carbon Black

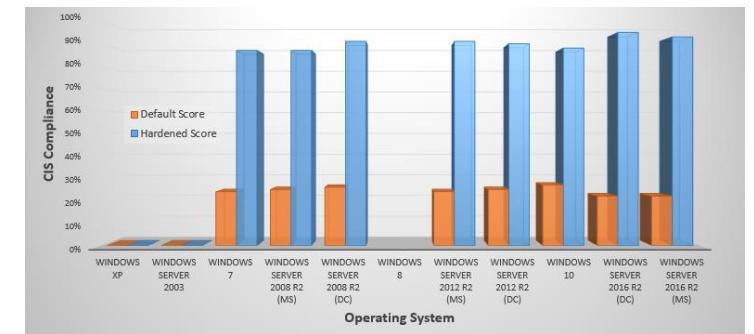
- 20.11.2018 объявлено о завершении квалификации CB AWL
- Белые списки приложений - Industrial Application Whitelisting
- Контроль сменных носителей - Portable Media/Device/USB Security
- Поставляется вместе с БД, содержащей белые списки процессов ПО Honeywell



Node Type	Version qualified with AWL- CB R200.1
Experion Server	R501, R432, R410, R400
Experion Flex Station	R501, R432, R410, R400
Experion Console Station	R501, R432, R410, R400
Experion Application Control Environment (ACE) and Simulation Control Environment (SCE)	R501, R432, R410, R400

Обновленные услуги

- Тесты на проникновение (CyberVantage Penetration Testing) позволяют выявить:
 - Выявить пробелы в защите
 - Выявить уязвимости, которые не выявляются сканерами
 - Определить способность защитников детектировать и реагировать на атаки
 - Обосновать инвестиции в кибербезопасность
- Укрепление защиты (PCN Hardening) включает:
 - Доменные групповые политики
 - Отключение не используемых сервисов (локально)
 - Определение прав пользователей (локально)
 - CIS Benchmarks



Center for Internet Security®

Honeywell

Окончание поддержки Windows 7 и Windows Server 2008

- Сняты с поддержки Windows XP (с 2014 года) и Windows Server 2003 (с 2015 года)
- В 2020 году ожидается окончание поддержки Windows 7 и Windows Server 2008
 - <https://support.microsoft.com/en-ca/help/13853/windows-lifecycle-fact-sheet>
- Это означает, что не будут выпускаться обновления безопасности для данных операционных систем

Решение: миграция АСУ ТП на новые версии

Новые «старые» угрозы - Shamoon 3



Saipem: cyber-attack on its servers identified

San Donato Milanese (MI), December 10, 2018 - Saipem informs that today a cyber-attack on its servers has promptly been identified.

We are collecting all the elements useful for assessing the impact on our infrastructures and the actions to be taken to restore normal activities.

We are also in the process of notifying the report of the incident to the competent Authorities.

Saipem is one of the world leaders in drilling services, as well as in the engineering, procurement, construction and installation of pipelines and complex projects, onshore and offshore, in the oil & gas market. The company has distinctive competences in operations in harsh environments, remote areas and deepwater. Saipem provides a full range of services with "EPC" and "EPCI" contracts (on a "turn-key" basis) and has distinctive capabilities and unique assets with a high technological content.

Website: www.saipem.com
Ph.: +39 0244244640

Lifecycle Solutions & Services


HPS Technical Support

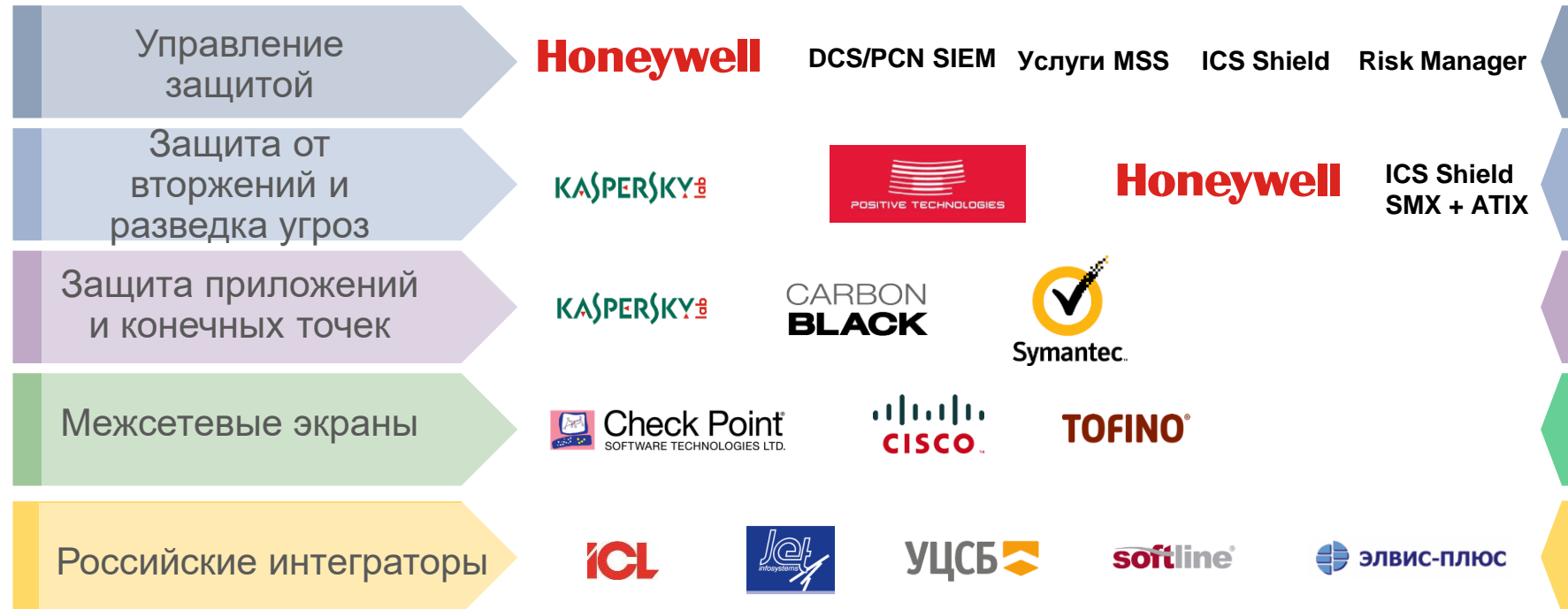
Knowledge Sharing Mail
Ref: KSM2019-001

Version: 001	Last Updated: Jan 03, 2019	Applicable Systems: Experion PKS	Releases: All	Author: HPS Technical Support
------------------------	--------------------------------------	--	-------------------------	---

SHAMOON Malware Vulnerability

Платформа и сервисы обеспечения и управления безопасностью (ICS Shield)

Портфель решений



Комплексная система безопасности

- Подход на базе эшелонированной защиты для нескольких площадок сразу
- Управление защитой разных производителей
- Удобство и доверие одному провайдеру



CyberVantage™ Услуги управления защитой

Мониторинг, Аналитика, Установка обновлений, Выявление угроз и пр.
(OT Security Operations Center)

Sentience и/или решение третьего производителя / поставщик OEM услуг и аналитики из облака

Центральный офис Заказчика / Security Operations Center (SOC)

Корпоративная киберзащита

ПО промышленной киберзащиты

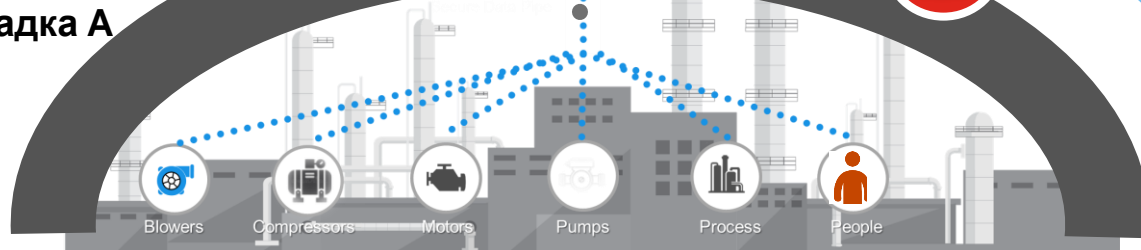
ICS Shield, Enterprise Risk Manager, Secure Media Exchange (SMX), Advanced Threat Intelligence Exchange (ATIX)

Встроенные меры защиты (белые списки, IDS, SIEM, антивирус и пр.)

ICS Shield Защищенный канал

Киберзащита площадки

Площадка А



Консультационные услуги по ИБ

Проектирование, Аудиты, Защита сетей и конечных точек, Обучение и тренинги, Реагирование и восстановление



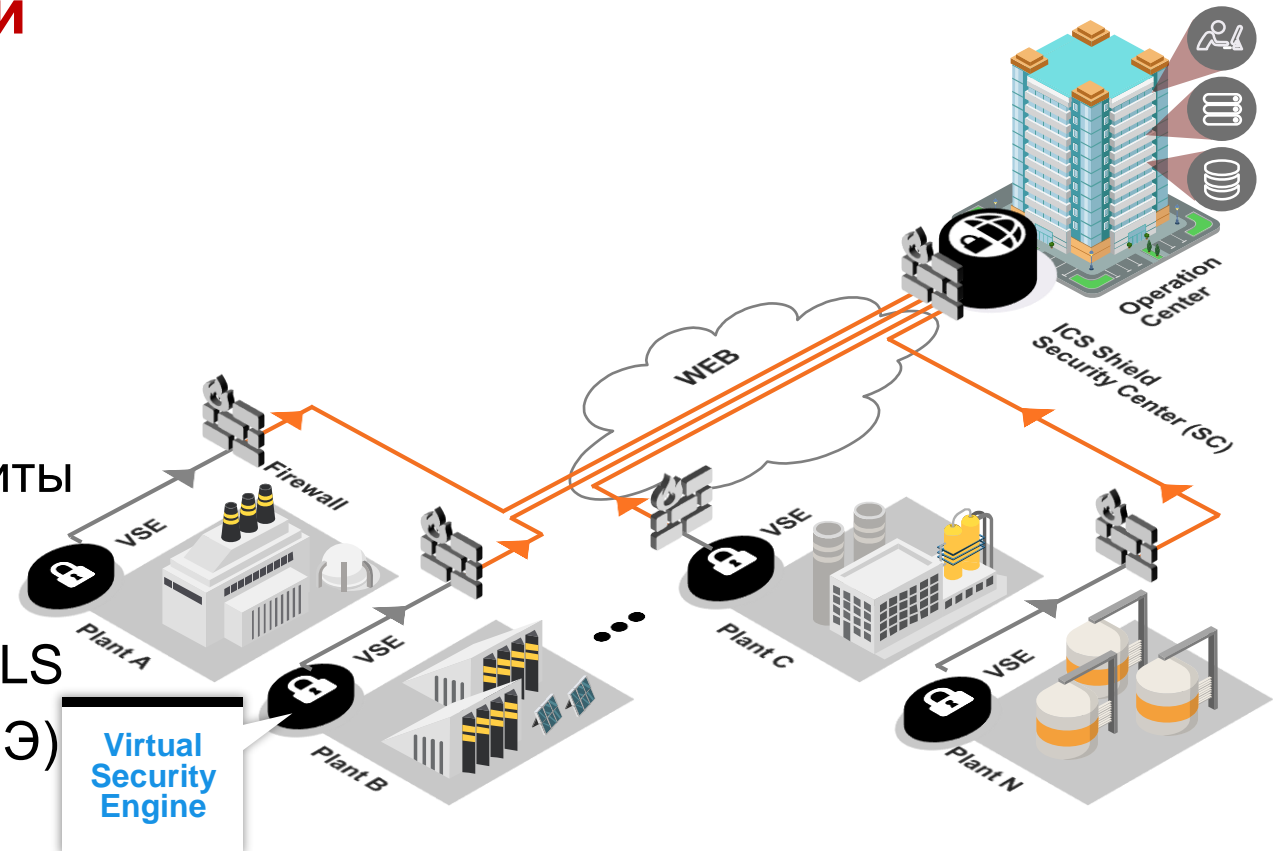
ICS Shield: Платформа управления операциями и защитой



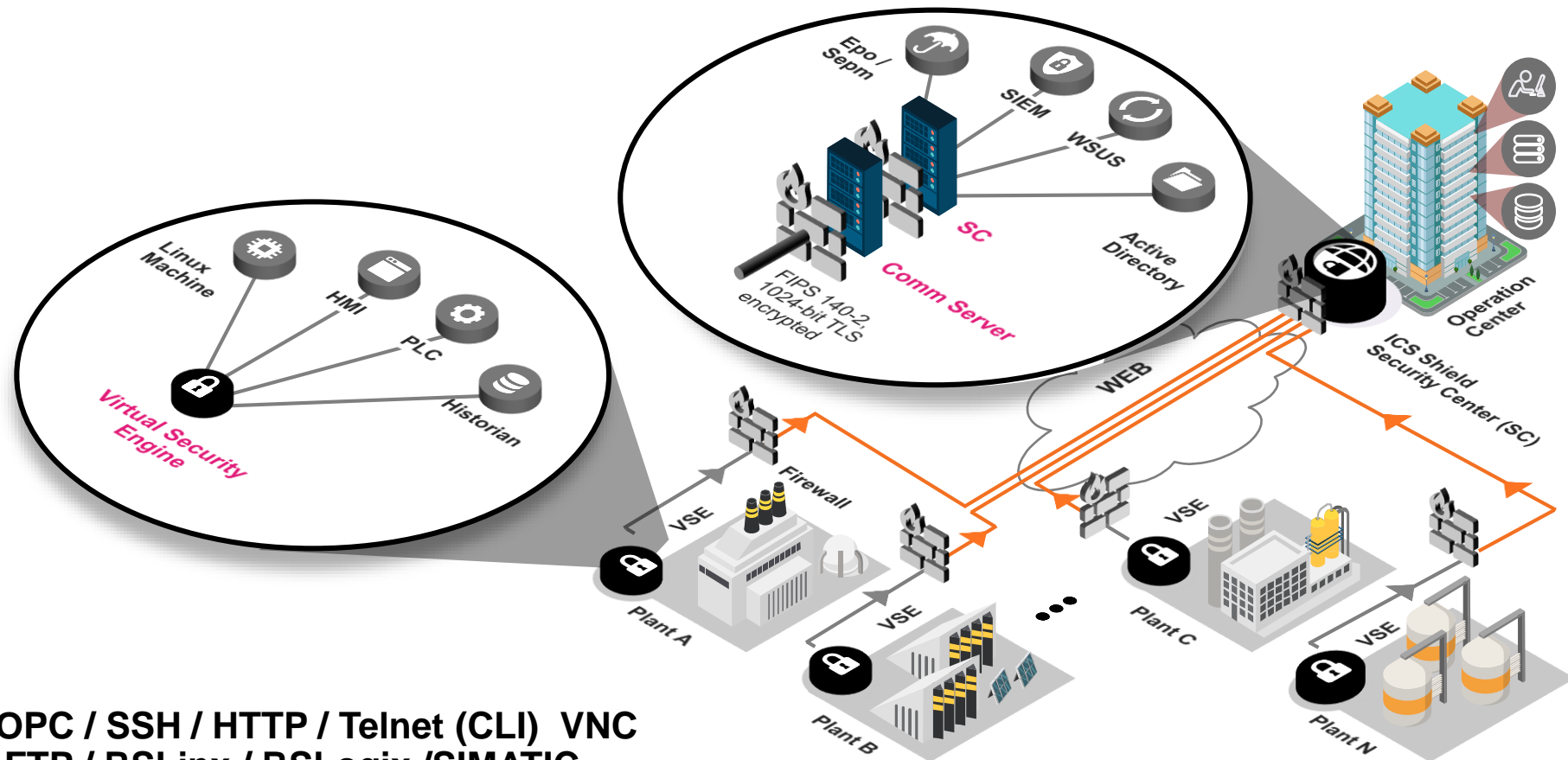
ICS Shield развертывание

Распределенная архитектура и защищенный канал между заводами и операционным центром

- Установка Центра защиты (SC) в операционном центре
- Установка виртуальных движков защиты (VSE) на каждом заводе
- Настройка исходящего защищенного канала по порт 443 с шифрованием TLS
- Одно правило межсетевого экрана (МЭ) для всех удаленных соединений



ICS Shield архитектура



WMI / SNMP / OPC / SSH / HTTP / Telnet (CLI) VNC
 / RDP / SFTP / FTP / RSLinx / RSLogix / SIMATIC
 любые частные TCP/UDP протоколы
Windows | Networking | Industrial

Услуги управления защитой (MSS)

Сервисы управления защитой

 Автоматизация обновлений ПО и антивирусов	 Мониторинг защищенности и производительности	 Отчеты о действиях и тенденциях	 Расширенный мониторинг и управление	 Защищенный удаленный доступ
<p>Протестированные и квалифицированные патчи для операционных систем и РСУ</p> <p>Протестированные и квалифицированные обновления и сигнатуры антивирусной защиты</p>	<p>Содержательный мониторинг здоровья системы и уровня защищенности</p> <p>Круглосуточное предупреждение об инцидентах в соответствии с заданными порогами</p> <p>Автоматизированная инвентаризация</p>	<p>Ежемесячные и квартальные комплаенс отчеты и отчеты о производительности</p> <p>Идентификация критичных вопросов и постоянных проблем</p>	<p>Межсетевые экраны, системы предотвращения вторжений и др.</p>	<p>Решение защищенного удаленного доступа</p> <p>Шифрование, двухфакторная аутентификация</p> <p>Полный аудит, отчетность и видео запись</p>

Услуги Managed Security Services: 24/7 мониторинг и экспертная поддержка



Экспертная поддержка для снижения простоев и рисков кибератак

Активно обслуживается 400+ площадок

Secure Media eXchange (SMX) + Advanced Threat Intelligence eXchange (ATIX)

Функции

- Безопасное использование сменных носителей USB при помощи управляемой износоустойчивой станции сканирования и локальных агентов (драйверов USB)
- Отслеживание и мониторинг содержимого носителей USB
- Нейтрализация угроз с эмуляцией HID-устройств (BadUSB, Rubber Ducky, Bash Bunny) и исполнением клавиатурных комбинаций и текстовых скриптов со скоростью до 100 слов в минуту
- Станция сканирования (шлюз SMX) не связана по сети с АСУ ТП, но подключена к серверу обновлений (АТІХ)
- Интегрируется с АСУ ТП через локальные агенты (драйверы USB) на АРМах и серверах
- Сканирование с использованием технологий обнаружения целенаправленных атак и угроз (хеши и репутация файлов, песочница АТІХ, фиды индикаторов компрометации крупнейших международных центров ИБ)
- Интеграция отчетности с Risk Manager



Сценарий использования



Заключение

Ресурсы

Сайт HICS

www.becybersecure.com



<https://www.ruscadasec.ru/>

Обновления безопасности

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

Honeywell

THE POWER OF CONNECTED

HOME EXPLORE SUPPORT TRAINING MY ACCOUNT

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

Security Updates

Home > Support

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 the become available to mitigate the Meltdown and Spectre vulnerabilities. Honeywell will continue to work with our hardware partners in order to identify and qua 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, tl 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.

Сообщить об уязвимости

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

Honeywell

CONTACT HONEYWELL | CORPORATE CITIZENSHIP | WORLDWIDE

PRODUCTS & SERVICES SOLUTIONS & TECHNOLOGIES ABOUT US INVESTORS NEWS

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.

Спасибо за внимание

www.becybersecure.com