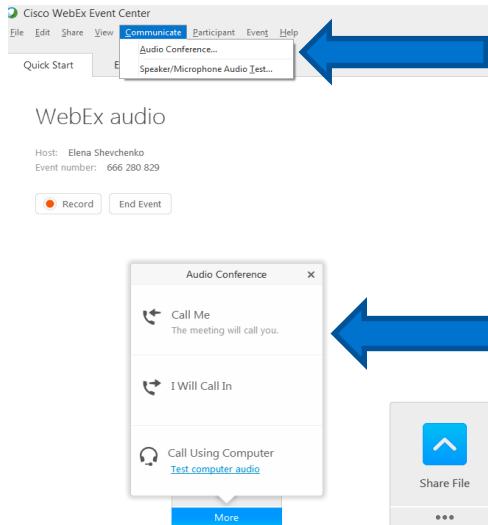


«Вебинар: «Информационная безопасность на производстве и ее реализация средствами PI System»

Настройте звук. Как это сделать?



Нажмите на «Communicate» на панели инструментов. Здесь Вы сможете подключиться к звуку (Audio Conference), а также проверить настройки (Speaker/Microphone Audio Test)

Попробуйте воспользоваться функцией «Call Using Computer». Если соединение не устанавливается, то воспользуйтесь функцией «Call me». Для этого введите прямой номер телефона (без добавочного), на который Вам можно перезвонить.

Информационная безопасность на производстве и ее реализация средствами PI System

Жамиля Алимбекова

11/09/2018

План

- Кибератаки → типы



Известные кибератаки

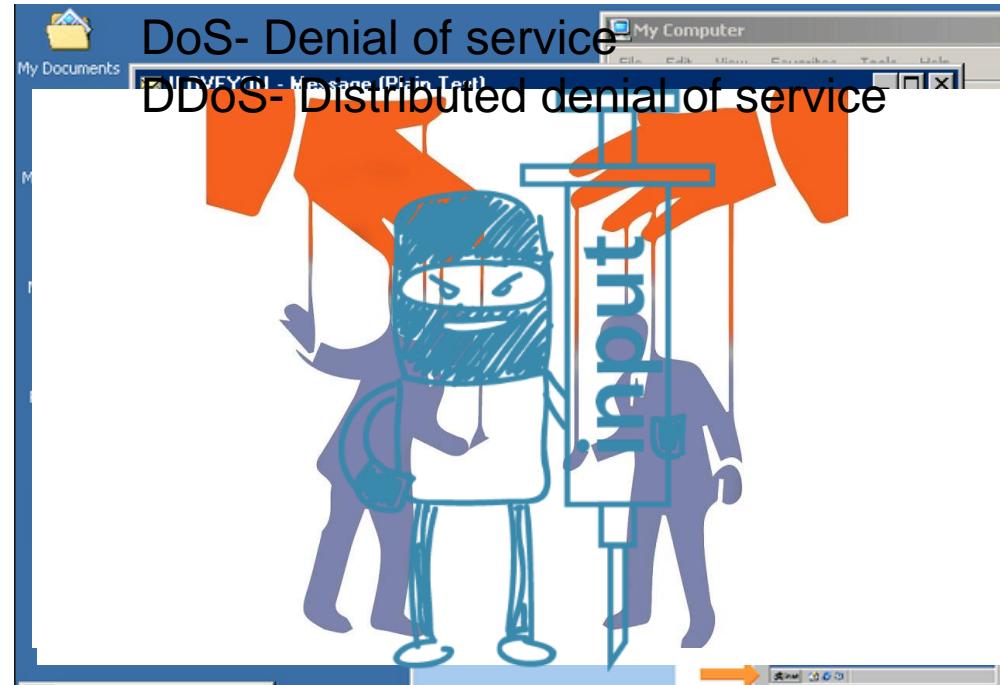
- Общие методы защиты
- Архитектурные решения PI System
- Моделирование угроз
- Средства защиты PowerShell



Кибератаки в терминах и цифрах

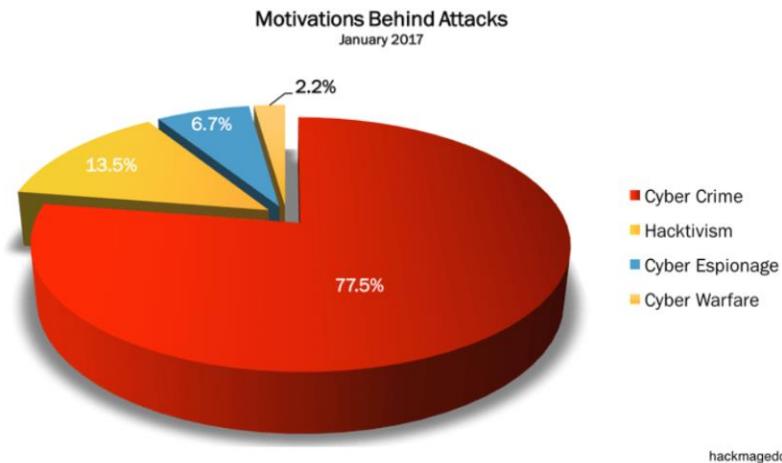
Кибератаки

- Mailbombing (SMTP), Phishing
- DoS/DDoS атаки
- Вирусы, троянские программы, черви, сифферы, руткиты
- Социальная инженерия
- Инъекция кода

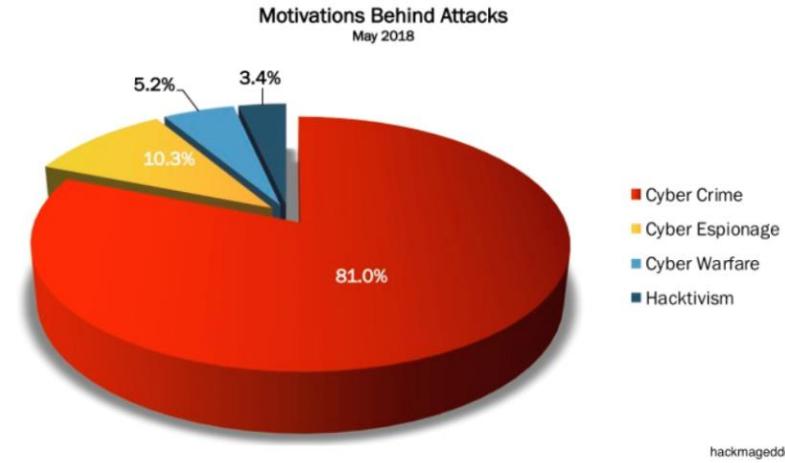


Статистика хакерских атак (Мотивация)

Январь 2017 Статистика кибератак



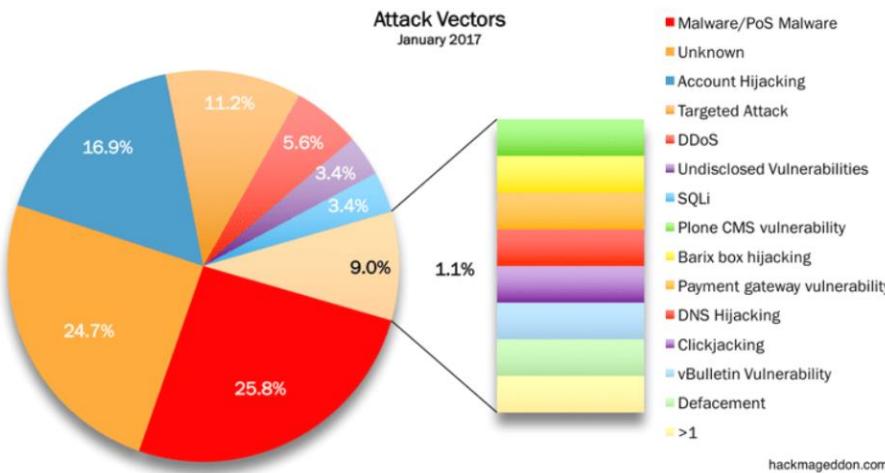
Май 2018 Статистика кибератак



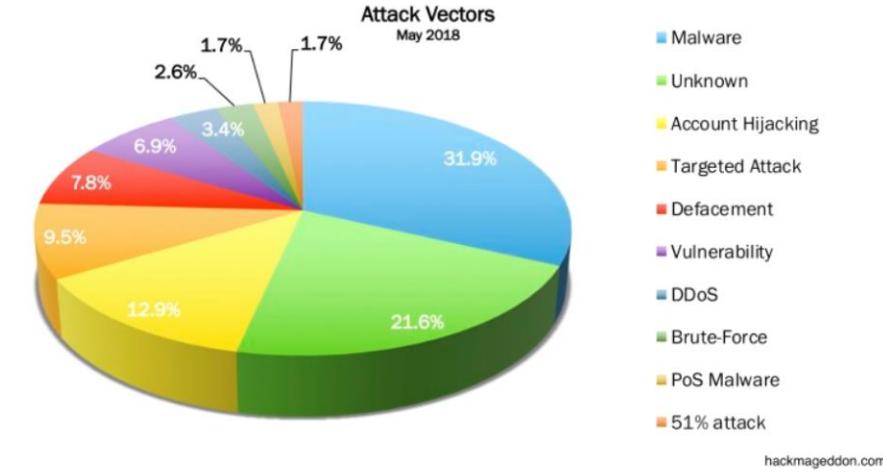
<https://www.hackmageddon.com/2017/03/02/january-2017-cyber-attacks-statistics/>

Статистика хакерских атак (Векторы атак)

Январь 2017 Статистика кибератак



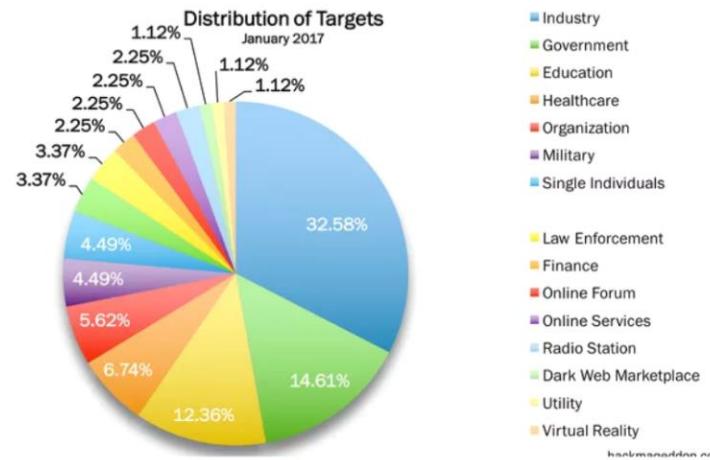
Май 2018 Статистика кибератак



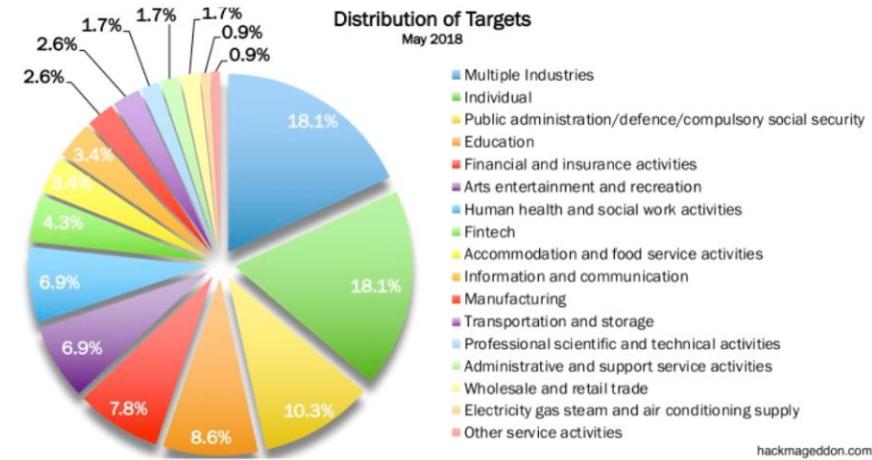
<https://www.hackmageddon.com/2017/03/02/january-2017-cyber-attacks-statistics/>

Статистика хакерских атак (Цели)

Январь 2017 Статистика кибератак



Май 2018 Статистика кибератак



<https://www.hackmageddon.com/2017/03/02/january-2017-cyber-attacks-statistics/>

Известные кибератаки

	WannaCry	Win32/Stuxnet	БД Sony Playstation
Ущерб	> \$ 1млрд	-	~ \$10 млн
Страны, понесшие потери	150 стран	Иран	Россия, Украина, Германия, Турция
Уязвимость	ОС Windows, протокол SMB	ПЛК Simatic-S7 и Simatic WinCC	Сервер веб приложений
Принцип работы	бэкдор DoublePulsar, экспloit EternalBlue	Уязвимость «нулевого дня»	Взлом, как стандартная транзакция

Oops, your important files are encrypted.

If you see this text, your files have been encrypted. Recover your files, but don't waste time on decryption service.

We guarantee that you can recover your files. All you need to do is submit the payment.

Please follow the instructions.

Wana DecryptOr 2.0

English

Oops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
CMT: From Monday to Friday...

Send \$300 worth of bitcoin to this address:

 **bitcoins**
ACCEPTED HERE

12t9YDPgwueZ9NyMgw619p7AA8isjr6SMw

[About bitcoin](#)
[How to buy bitcoins?](#)

[Contact Us](#)

Общие методы защиты информации

Три закона безопасности SCADA

1. Ничто не безопасно
2. Любое программное обеспечение можно взломать
3. Любая часть информации может быть атакой

Ginter, Andrew (2016) *SCADA Security: What's broken and how to fix it.* Calgary: Abterra

Методы защиты информации

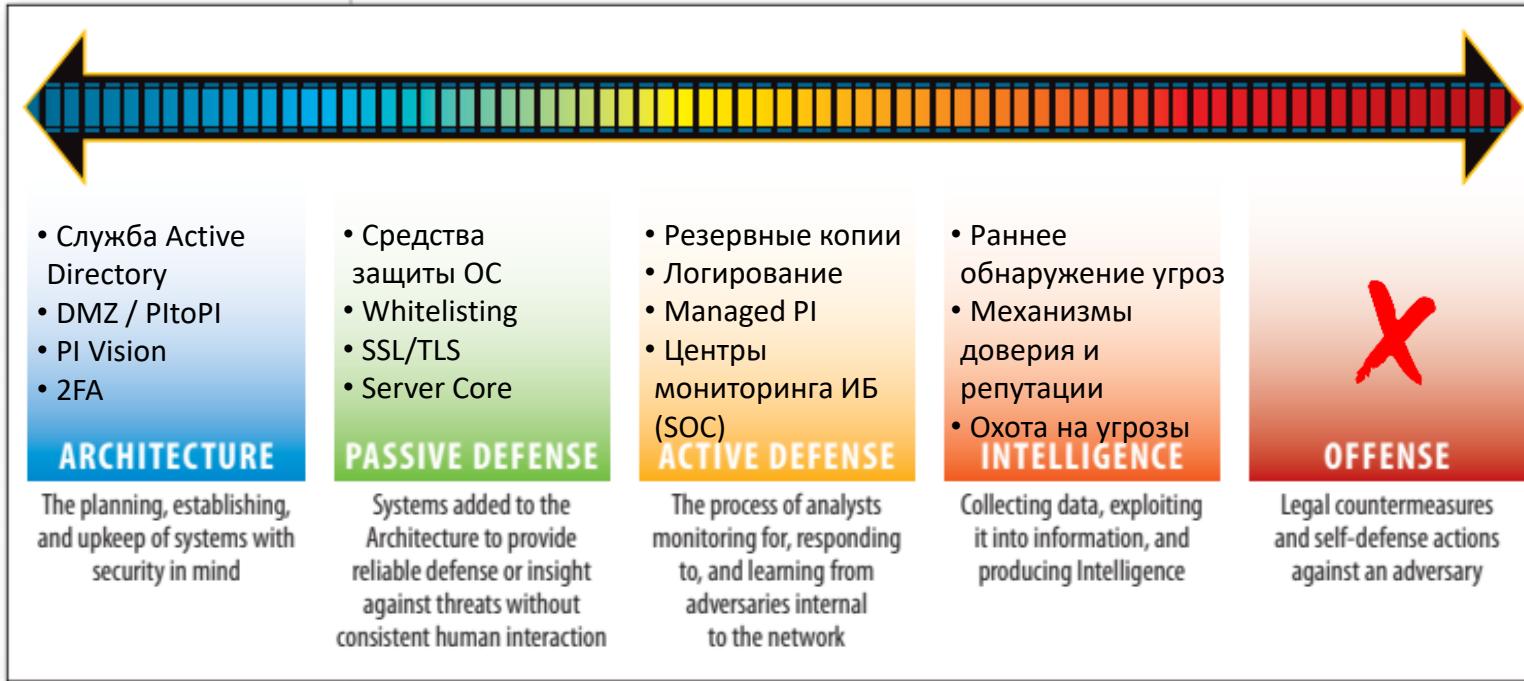
- Физические средства
- Базовые средства защиты электронной информации
- Анти-DDoS
- Резервное копирование данных
- План аварийного восстановления данных
- Шифрование данных при передаче информации в электронном формате (end-to-end protection)



[Комсомольская правда: Информационная безопасность предприятий: ключевые угрозы и средства защиты](#)

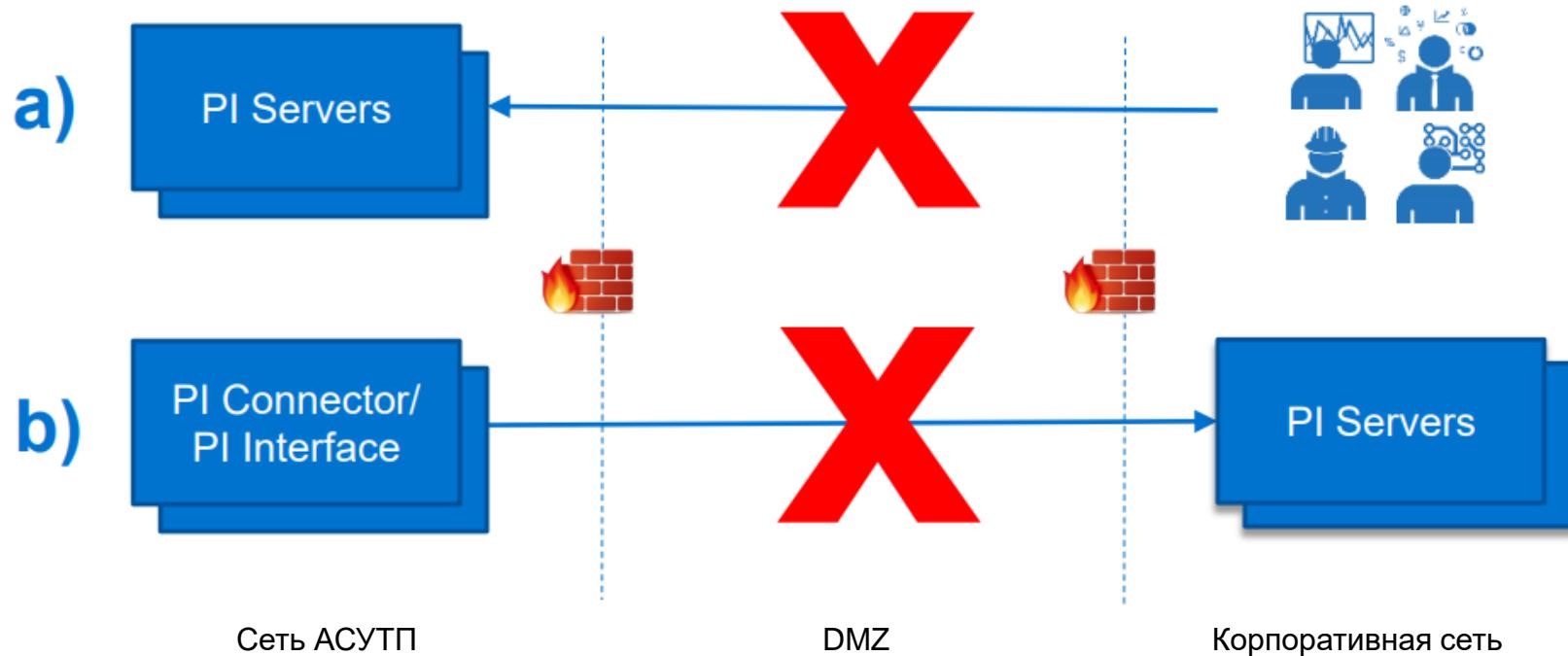
SANS “Sliding Scale of Security”

Архитектурная защита должна быть высокоприоритетной

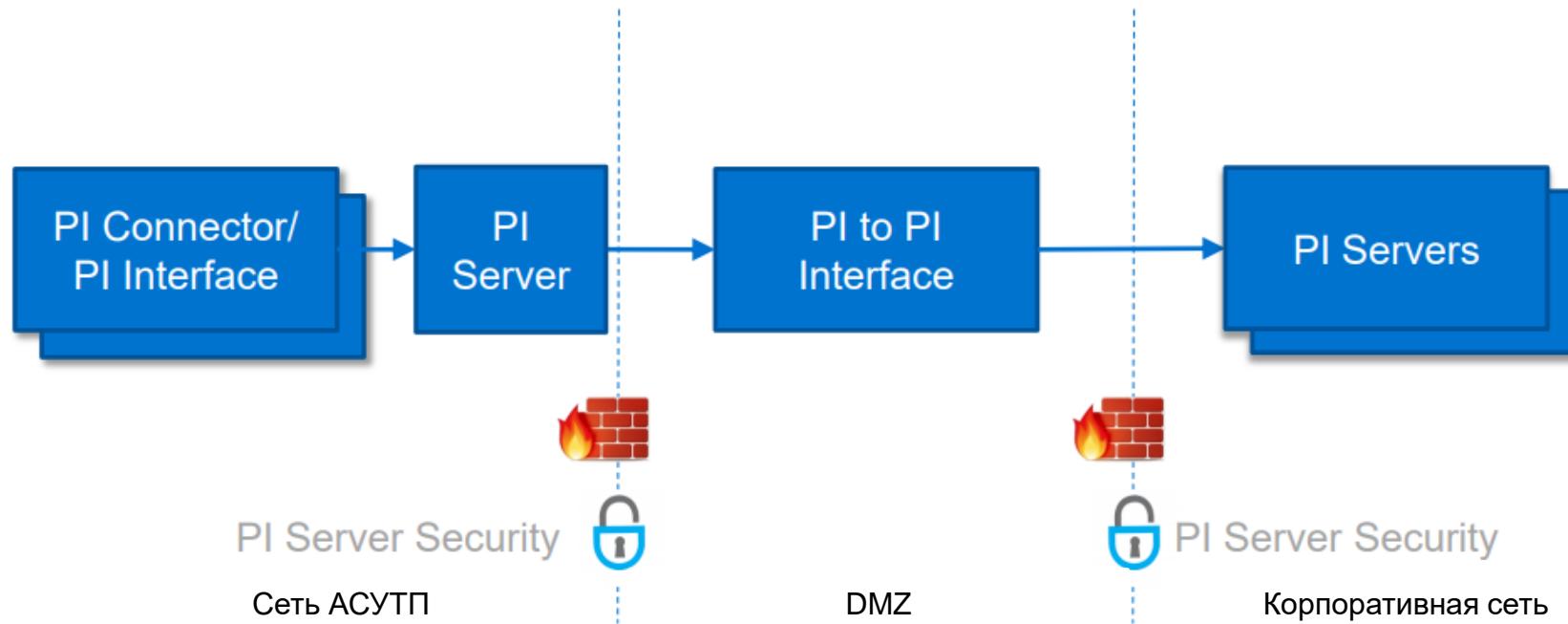


Архитектурные решения PI System

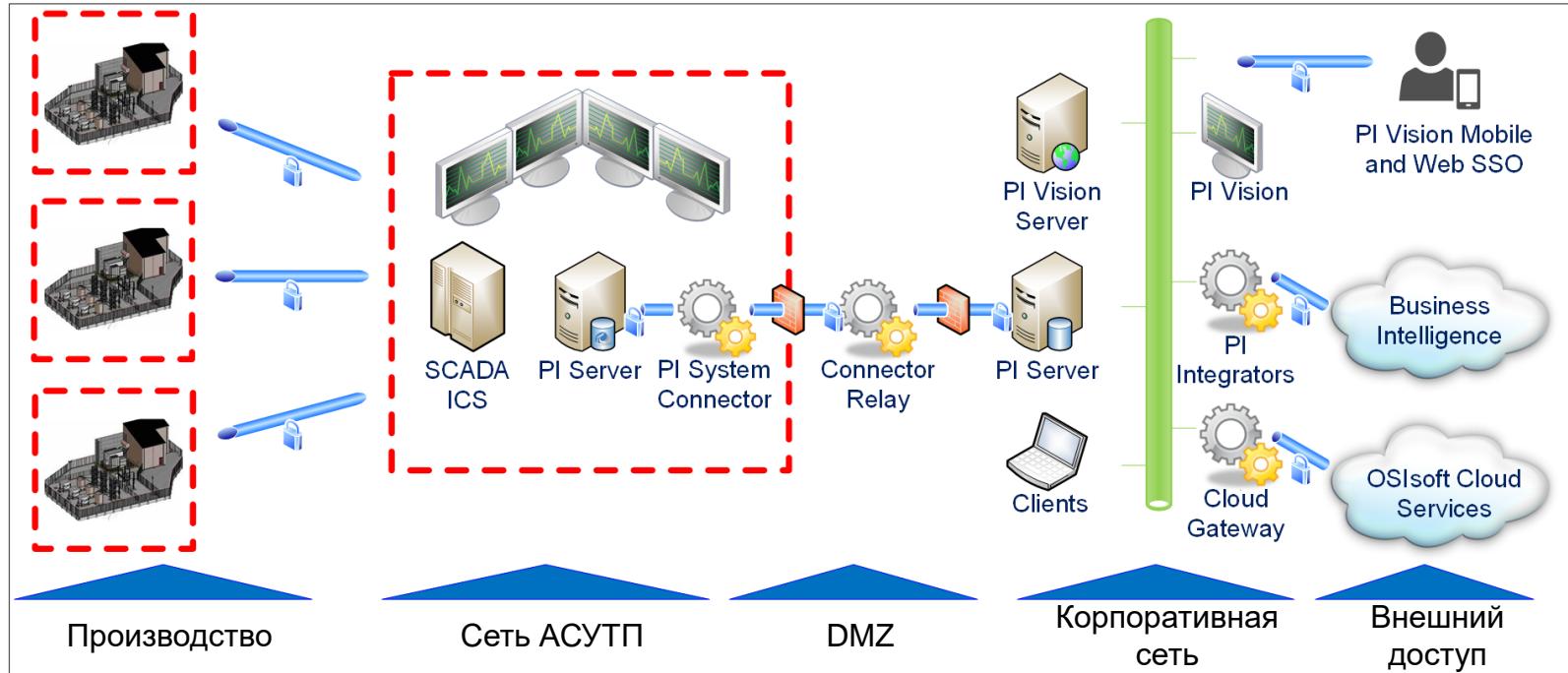
Нерекомендуемая топология



Стандартное решение



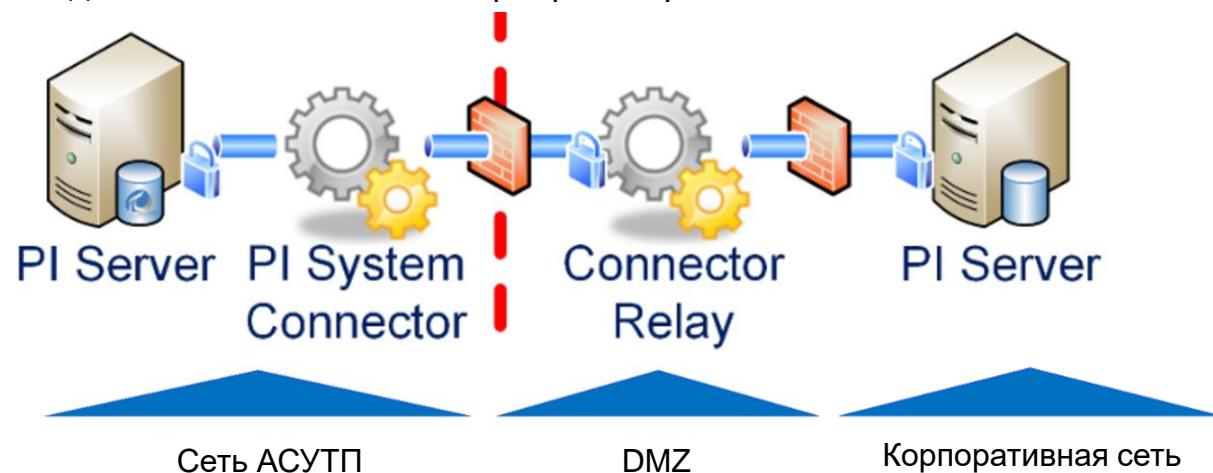
Архитектура безопасности PI System



Что здесь особенного?

PI System Connector:

- Изначально ориентирован на архитектуру в DMZ
- Вносит дополнительный отдельный уровень безопасности с помощью аутентификации при пересечении границ DMZ
- Передает односторонний поток данных из сети АСУТП в корпоративную сеть



Ограничение рисков критических систем с PI System

Передача &
Распределение
SCADA



Распределительная
система управления



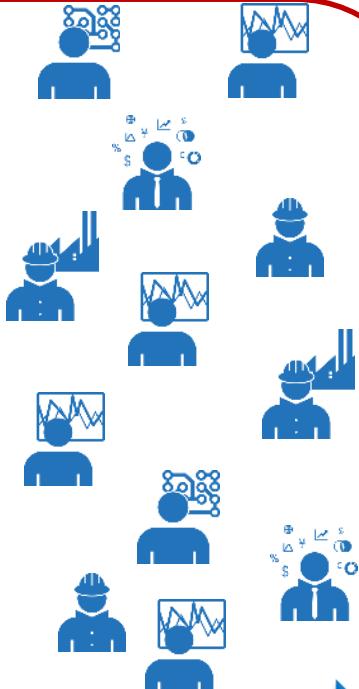
ПЛК



Система
экологической
безопасности



Другие критические
операционные системы

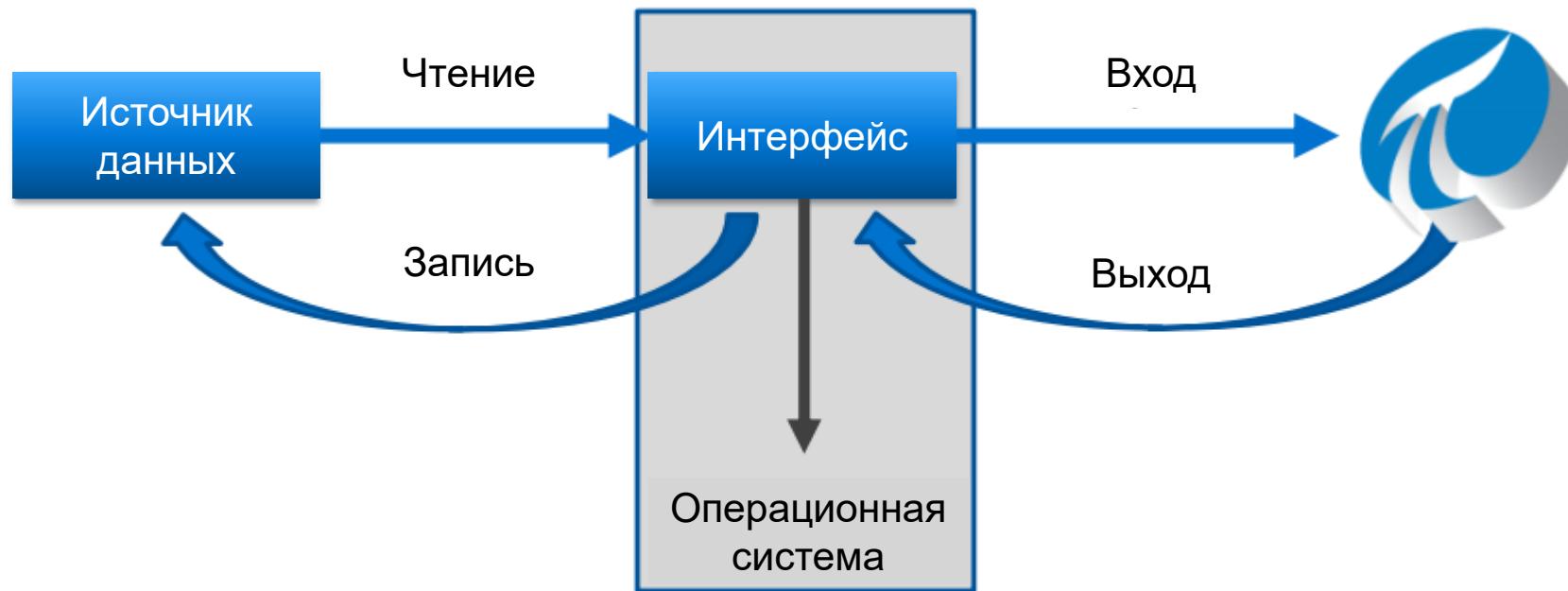


Периметр безопасности

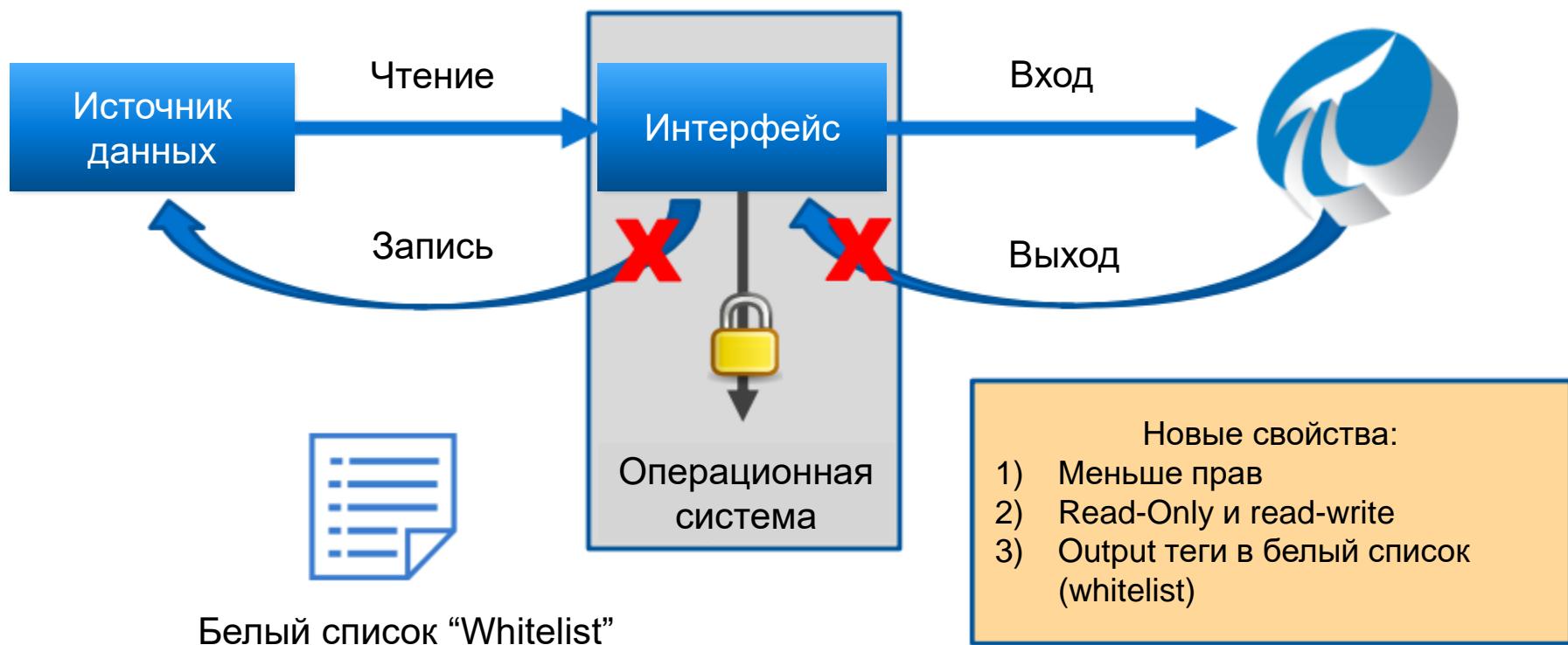
Снижение рисков на критических системах



Read-Write Интерфейсы



Read-Only Интерфейсы



Интерфейсы с повышенной защитой

Интерфейсы с усиленной защитой	Read-Only интерфейсы
PI Interface for ESCA HABConnect Alarms and Events	PI Interface for Foxboro I/A 70 Series
PI Interface for Cisco Phone	PI Interface for Metso maxDNA
PI Interface for ESCA HABConnect	PI Interface for Citect
PI to PI Interface	PI Interface for SNMP Trap
PI Interface for CA ISO ADS Web Service	PI Interface for Modbus Ethernet PLC
PI Interface for IEEE C37.118	PI Interface for OPC HDA
PI Interface for Performance Monitor	PI Interface for GE FANUC Cimplicity HMI
PI Interface for Siemens Spectrum Power TG	PI Interface for ACPLT/KS
PI Interface for Relational Database (RDBMS via ODBC)	PI Interface for OPC DA
PI Interface for Universal File and Stream Loading (UFL)	

Моделирование угроз

Три правила безопасности

1) Держать плохих парней подальше

Пример: усиленная аутентификация

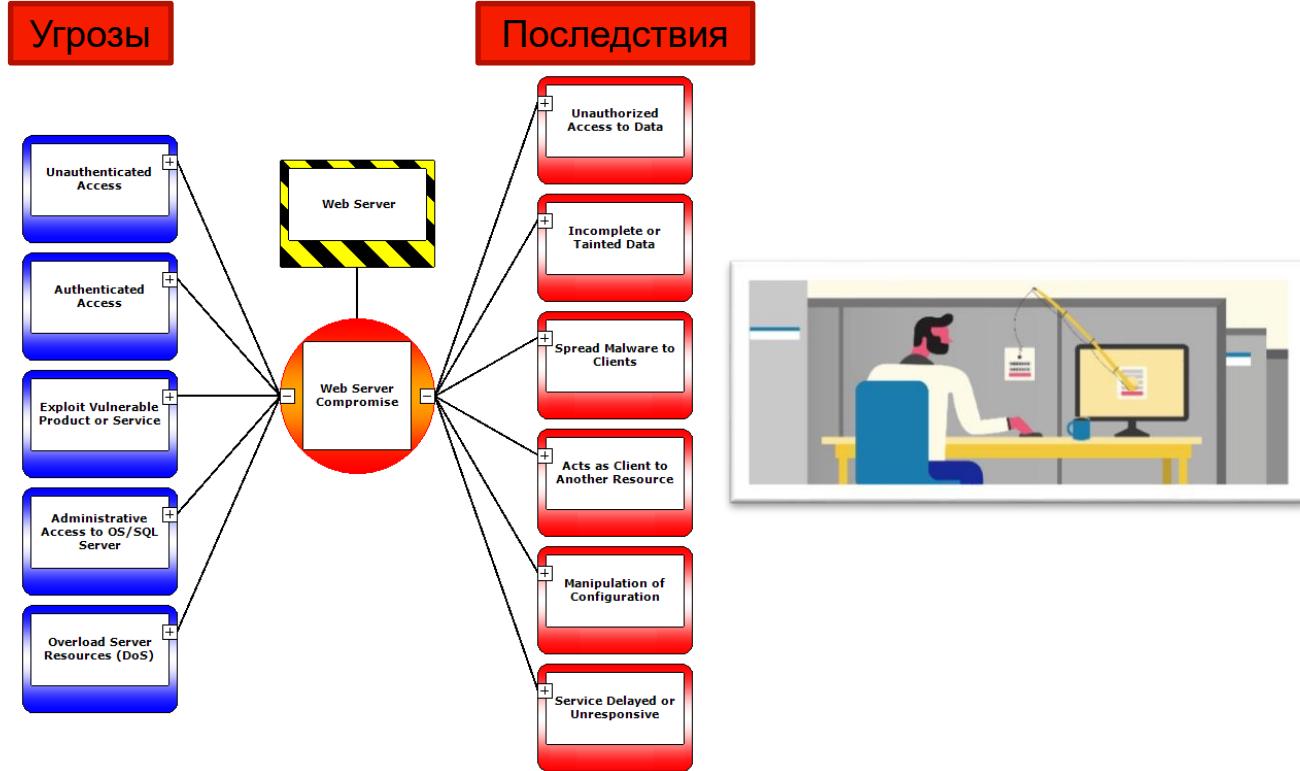
2) Ограничить ущерб, если они попадут в систему

Пример: минимум полномочий для ограничения доступа, предоставляемого злоумышленнику, в случае компрометации компонента

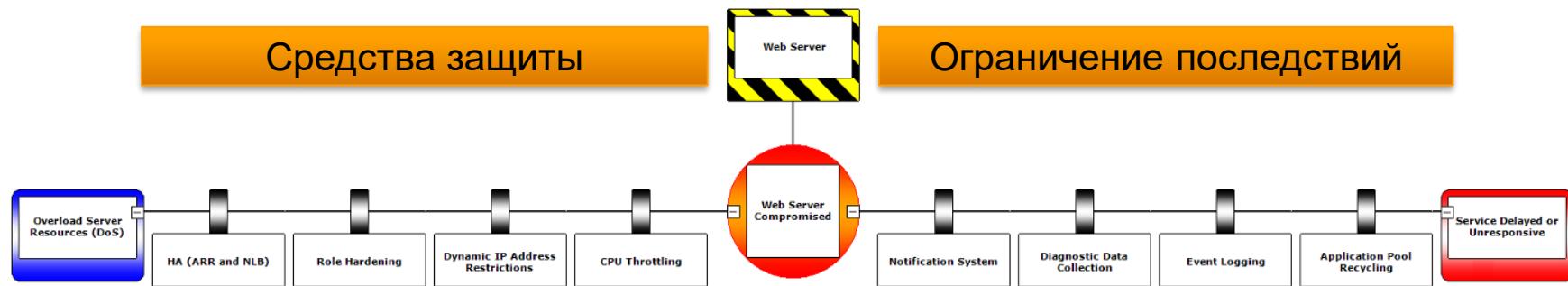


3) Обнаружить аномалии и отреагировать

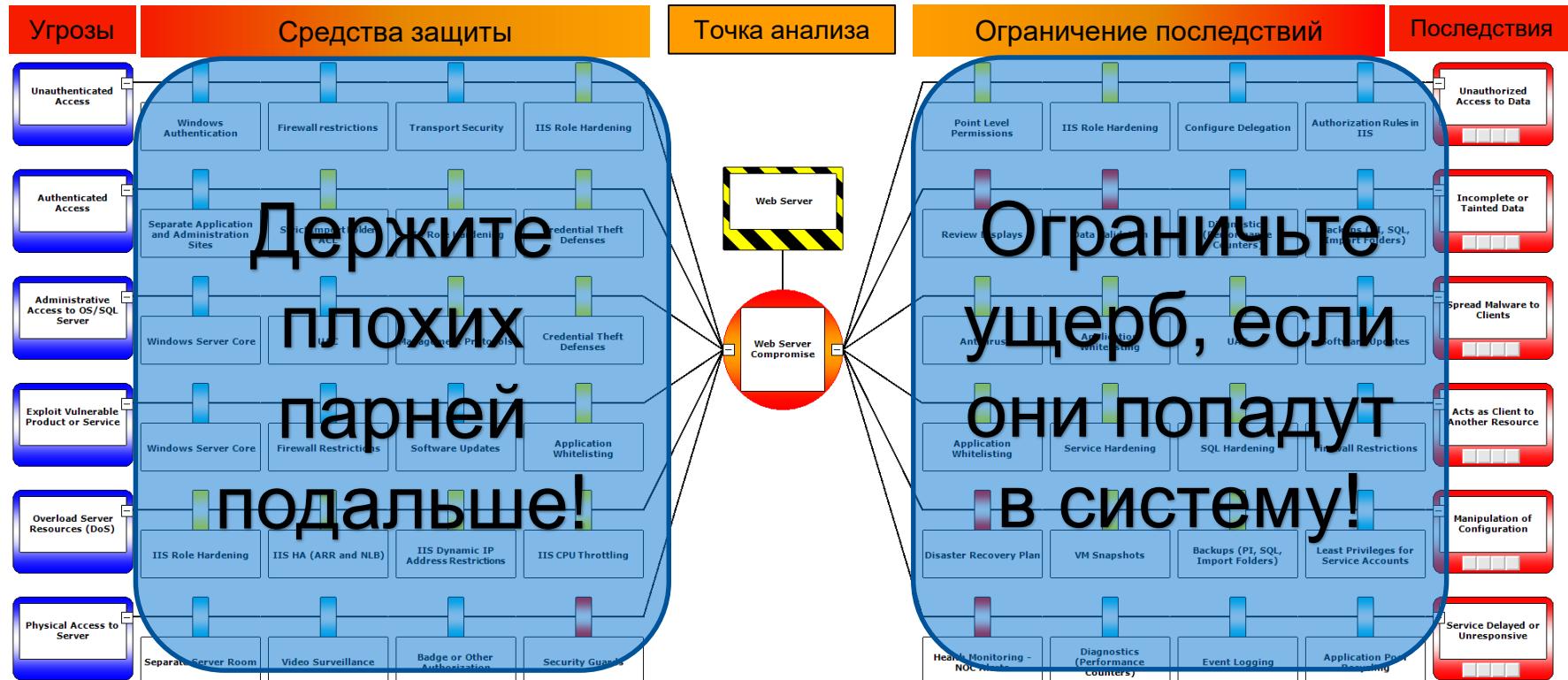
Определение угроз и последствий



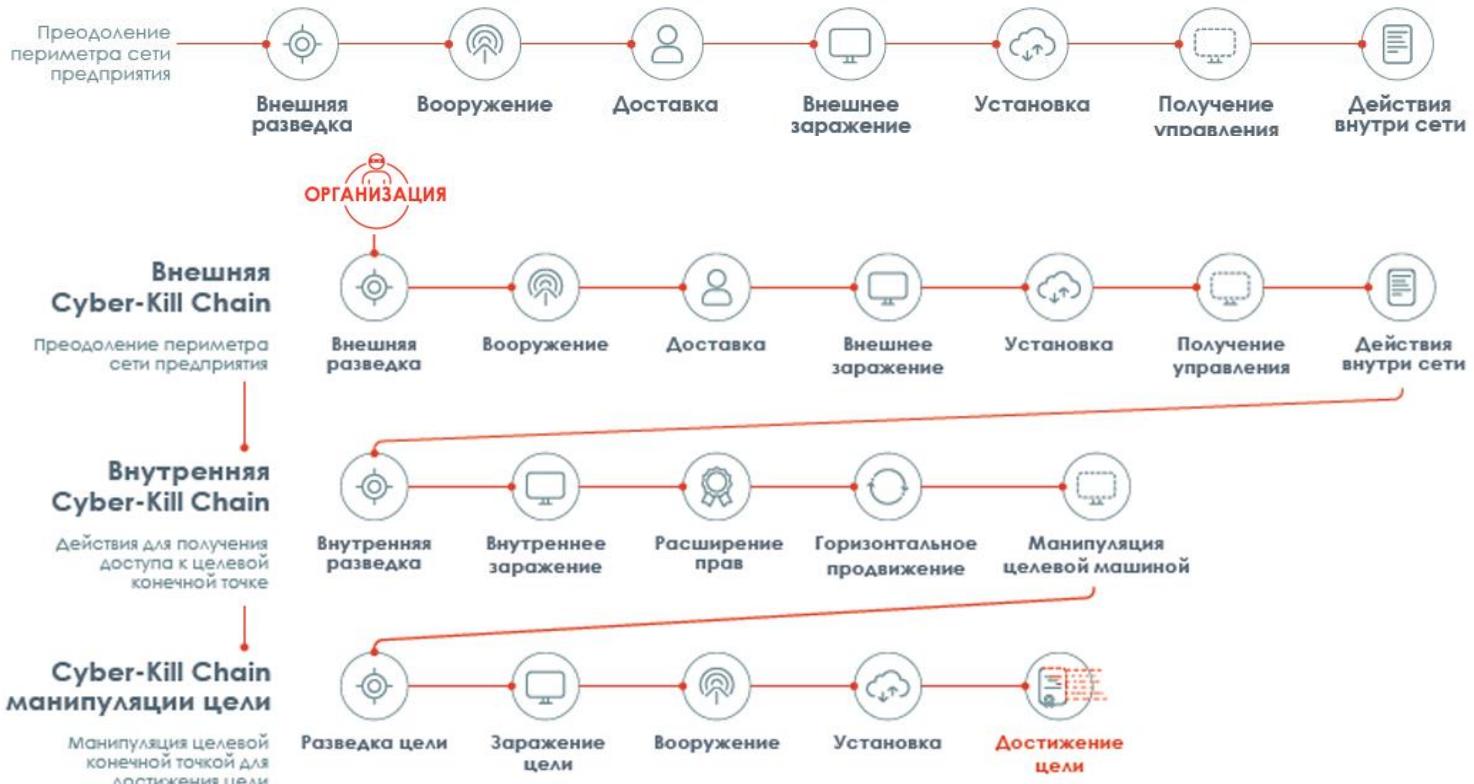
Выстраивание барьеров



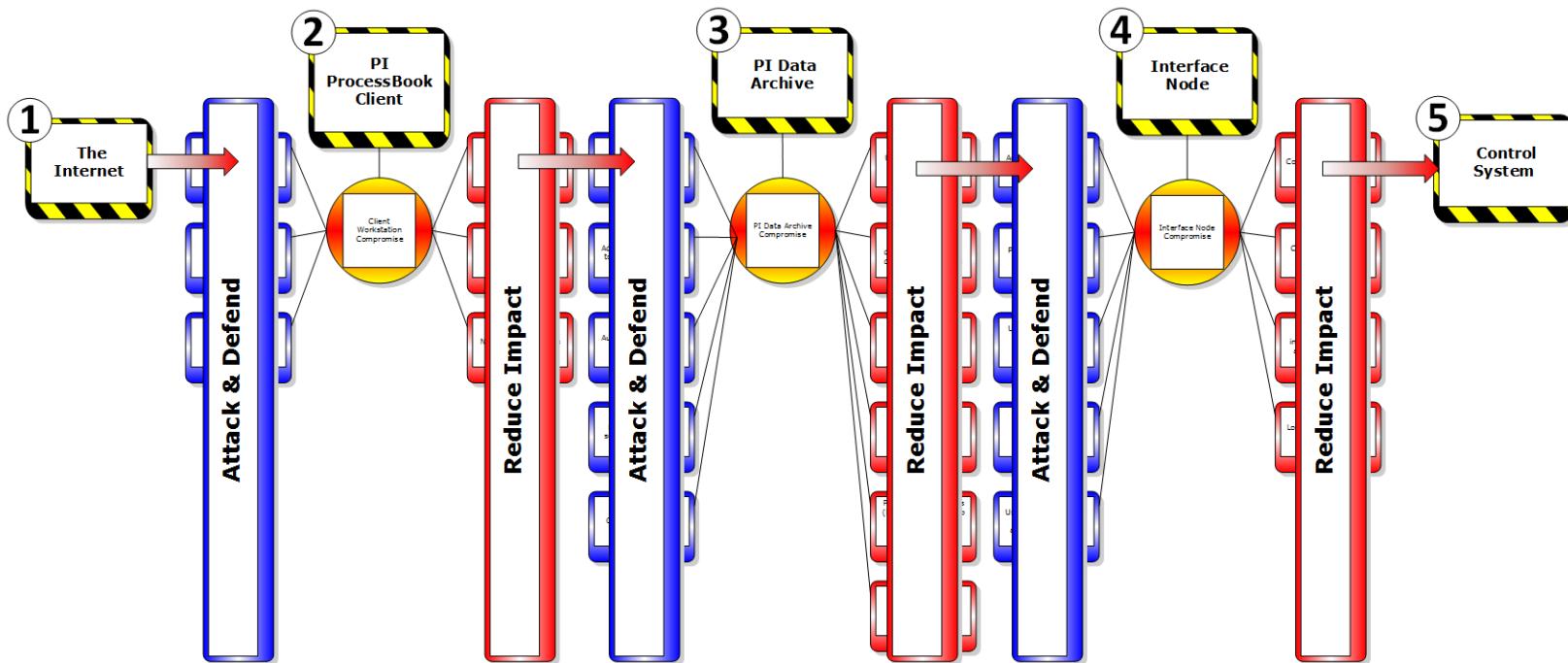
Переход к модели Bow-Tie



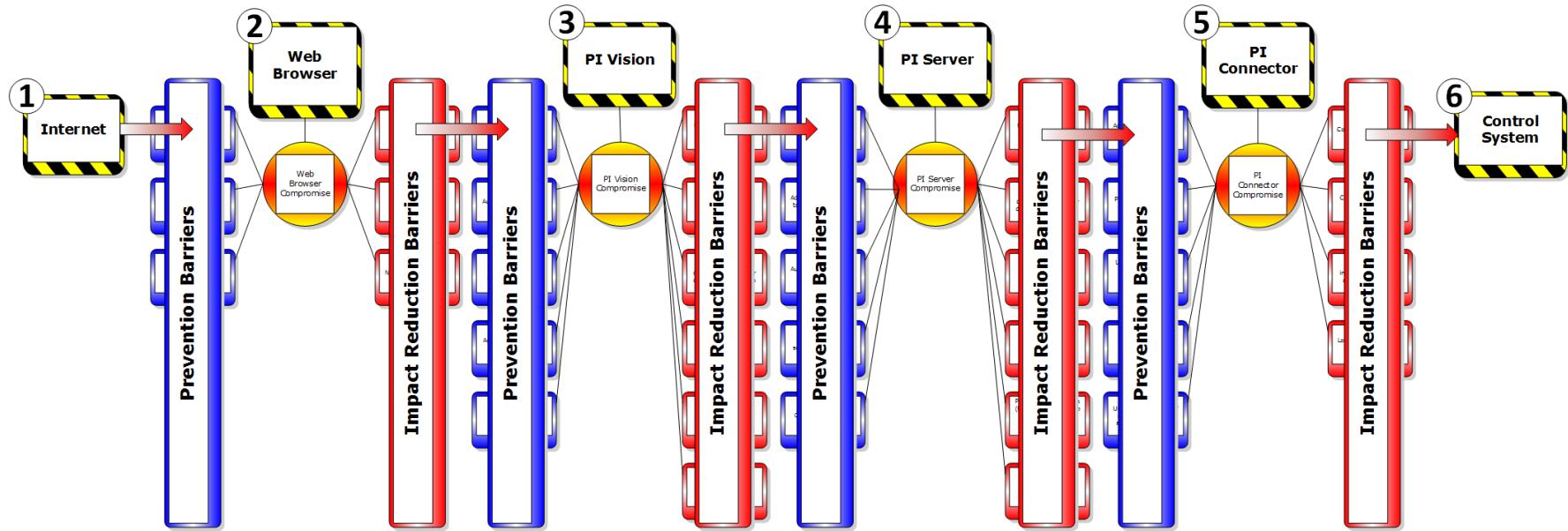
Модель и этапы



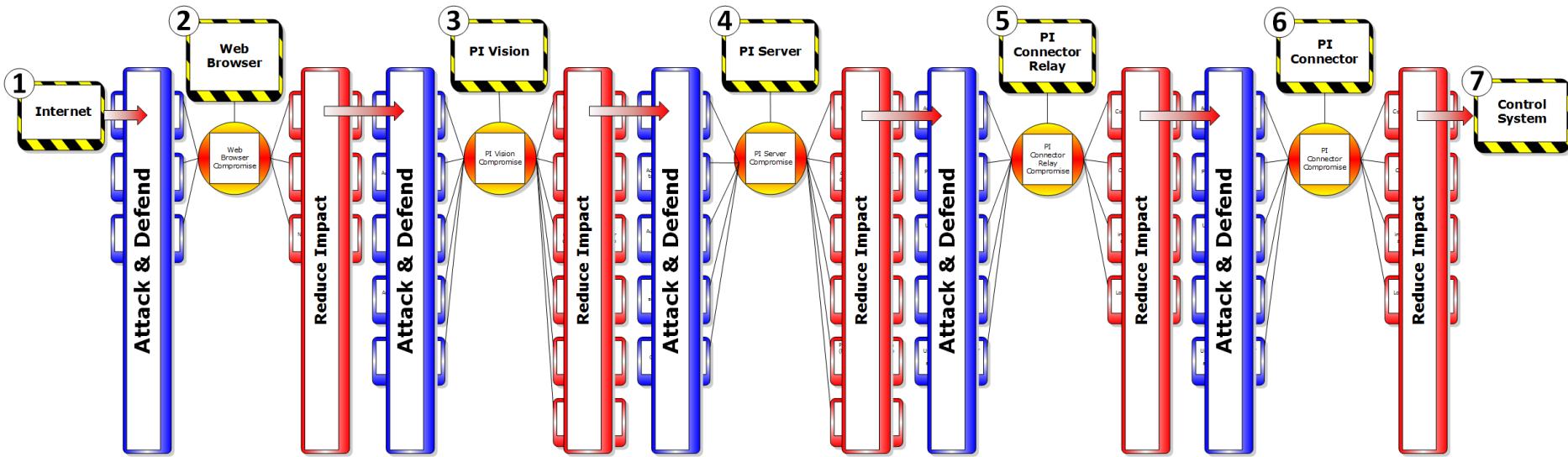
Классическая PI System Kill Chain



Kill Chain c PI Vision



Kill Chain c PI Connector Relay



PowerShell, как средство защиты

Топ 10 причин, почему хакеры любят PowerShell



- Установлен по умолчанию
- Удаленный доступ с использованием шифрования по умолчанию
- Постоянно растущее сообщество
- Системные администраторы охотно используют и доверяют



- Запуск/загрузка полезных данных из памяти
- Слабый трейсинг
- Легко сбить с толку
- Антивирусное ПО с трудом справляется с вредоносными программами, основанными на скриптах



- Антивирусное ПО часто игнорирует скрипты при повышении защиты своих систем
- Обходят инструменты whitelisting (зависит от конфигурации)

Symantec, [Increased use of PowerShell in attacks](#)

Почему системные администраторы любят PowerShell

“Обновления в WMF 5.0 (или WMF 4.0 с KB3000850) делают PowerShell худшим инструментом для хакера при **включении регистрации блоков сценариев и общесистемной транскрипции**. Хакеры будут оставлять отпечатки пальцев повсюду в отличие от популярных утилит CMD.”

~ Ashley McGlone, [Who's afraid of PowerShell security](#)

Engine	Event Logging	Transcription	Dynamic Evaluation Logging	Encrypted Logging	Application Whitelisting	Antimalware Integration	Local Sandboxing	Remote Sandboxing	Untrusted Input Tracking
Bash	No**	No*	No	No	Yes	No	No*	Yes	No
CMD / BAT	No	No	No	No	Yes	No	No	No	No
Jscript	No	No	No	No	Yes	Yes	No	No	No
LUA	No	No	No	No	No	No	No*	Yes	Yes
Perl	No	No	No	No	No	No	No*	Yes	Yes
PHP	No	No	No	No	No	No	No*	Yes	Yes
PowerShell	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No**
Python	No	No	No	No	No	No	No	No	No**
Ruby	No	No	No	No	No	No	No**	No**	Yes
sh	No**	No*	No	No	No	No	No*	Yes	No
T-SQL	Yes	Yes	Yes	No	No	No	No**	No**	No
VBScript	No	No	No	No	Yes	Yes	No	No	No
zsh	No**	No*	No	No	No	No	No*	Yes	No

* Feature exists, but cannot enforce by policy
** Experiments exist

PowerShell Team Blog: [A Comparison of Shell and Scripting Language Security \(4/10/2017 post\)](#)

Применение PowerShell для PI System

Системное администрирование

Инструменты PowerShell для PI System

Аудит безопасности

PI Security Audit tools

Конфигурация в виде кода

PI Security DSC ресурсы

<https://github.com/osisoft/PI-Security-DSC>

<https://github.com/osisoft/PI-Security-Audit-Tools>

PI Security Audit Tools

Проверяет:

- Machine (General)
- PI Data Archive
- PI AF Server
- MS SQL Server
- PI Vision
- PI Web API

Требования:

- PSv3+
- Run as Admin (AF&Vision)
- Osisoft.Powershell
- WinRM enabled (if remote)



ID	Server	Validation	Result	Severity	Message	Category	Area
AU10002	PICLIENT01	Operating System Installation Type	Fail	Severe	The following installation type is used: Server	Machine	Operating System
AU10003	PICLIENT01	Firewall Enabled	Fail	Moderate	Firewall not enabled.	Machine	Policy
AU10004	PICLIENT01	AppLocker Enabled	Fail	Moderate	AppLocker is not configured to enforce.	Machine	Policy
AU10005	PICLIENT01	UAC Enabled	Fail	Low	Recommended UAC feature ValidateAdminCodeSignatures disabled.	Machine	Policy
AU10001	PICLIENT01	Domain Membership Check	Pass	N/A	Machine is a member of an AD Domain.	Machine	Domain

A	B	C	D	E	F	G	H
ID	ServerName	AuditItemName	AuditItemValue	AuditItemFunction	Message1	Group1	Group2
1	AU10002	PICLIENT01	Operating System Installation Type	Fail	Get-PISysAudit_CheckOSInstallationType	The follow Machine	Operating System
2	AU10006	PICLIENT01	Hello World	Fail	Get-PISysAudit_HelloWorld	Chuck Not Machine	Policy
4	AU10007	PICLIENT01	Disallow Scheduled Tasks	Fail	Get-PISysAudit_DisallowedScheduledTasks	List of disallow Machine	Policy
5	AU10003	PICLIENT01	Firewall Enabled	Fail	Get-PISysAudit_CheckFirewallEnabled	Firewall n Machine	Policy
6	AU10004	PICLIENT01	AppLocker Enabled	Fail	Get-PISysAudit_CheckAppLockerEnabled	AppLocke Machine	Policy
7	AU10005	PICLIENT01	UAC Enabled	Fail	Get-PISysAudit_CheckUACEnabled	Recommence Machine	Policy
8	AU10001	PICLIENT01	Domain Membership Check	Pass	Get-PISysAudit_CheckDomainMembership	Machine Machine	Domain
9							
10							
11							
12							

PI Security DSC Recourses

- Getting Started Guide в [Wiki](#)
- Синтаксис

The screenshot shows two parts of the module structure:

DSCResources:

Name	Date modified	Type
xAFAttribute	02-Sep-18 8:35 PM	File folder
xAFIdentity	02-Sep-18 8:35 PM	File folder
xAFMapping	02-Sep-18 8:35 PM	File folder
xPIDatabaseSecurity	02-Sep-18 8:35 PM	File folder
xPIFirewall	02-Sep-18 8:35 PM	File folder
xPILidentity	02-Sep-18 8:35 PM	File folder
xPIMapping	02-Sep-18 8:35 PM	File folder
xPIPoint	02-Sep-18 8:35 PM	File folder
xPITrust	02-Sep-18 8:35 PM	File folder
xPTuningParameter	02-Sep-18 8:35 PM	File folder

Configuration:

Name	Date modified	Type	Size
PIDataArchive_AuditBaseline	03-Sep-18 12:14 AM	File folder	
PIDataArchive_AuditBaseline.ps1	11-May-18 9:18 AM	Windows PowerShell	15 KB
PIDataArchive_BasicWindowsImplementation.ps1	11-May-18 9:18 AM	Windows PowerShell	21 KB
PIWebAPI_1.9.0_SecurityBaseline.ps1	11-May-18 9:18 AM	Windows PowerShell	14 KB
PIWebAPI_1.10.0_SecurityBaseline.ps1	11-May-18 9:18 AM	Windows PowerShell	15 KB

PIConfiguration AF DataBase

- AFAttribute

PI AF Security

- AF Identity
- AF Mapping

PI Data Archive

- PIDataBaseSecurity
- PIFirewall
- Конфигурации
- PIPoint
- PITrust
- PTuningParameter

Demo 1: PI Security Audit Tools

- Как начать работу с PSAT?
- Как создать обычный и расширенный аудит отчет?
- Как создать отчет по настройке Kerberos?
- Какую еще информацию можно собрать о PI Data Archive?

Demo 2: PI Security DSC Resources

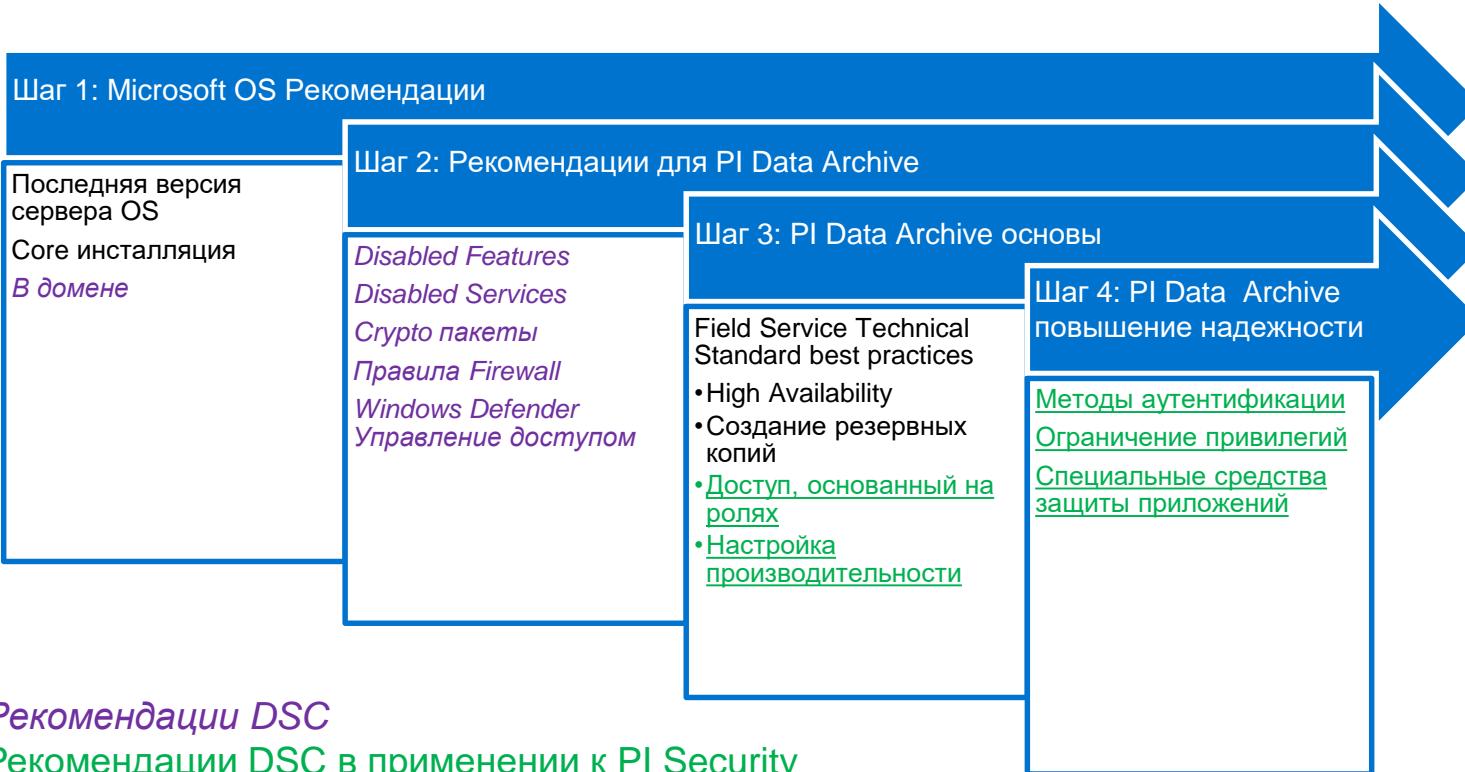
- Как начать работу с DSC?
- Проверка желаемых настроек конфигурации для PI Data Archive (tuning parameter, PI Identities)
- Проверка желаемых настроек конфигурации PI AF Security (AF Mapping)
- Как применить изменения?

Demo 3: Data Archive connection history

- Как получить отчет о всех подключениях к PI Data Archive?
- Как получить отчет о всех подключениях, которые были установлены в прошлом?
- Как посмотреть их статус?

```
pidiag --connectionhistory -r -s *-1d -e * -f connectionhistory.csv
```

Повышение надежности с Desired State Configuration (DSC)



Преимущества:

- Security event logs
- PI Message Logs (ID: 7082)
- PI Data Archive connection history

Successful login ID: 44. Address: [REDACTED] Name: PISDKUtility.exe(17636):remote. Identity List: piadmins
[REDACTED] pidemo [REDACTED] piusers [REDACTED] PIWorld. Environment Username : [REDACTED]. Method: Windows Login
(SSPI,Kerberos,HMAC-SHA1-96,Kerberos AES256-CTS-HMAC-SHA1-96,256)

Миф №1: Для работы PI Trust необходимы открытые порты в Workgroup.

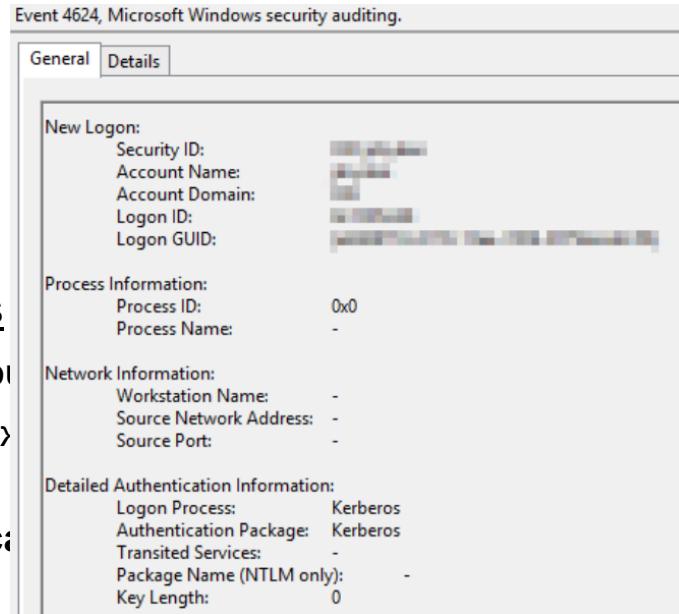
Правда: Приложения могут использовать PI Mappings как межсетевой протокол для взаимодействия с PI Data Archive в Workgroup.

[**KB01457 - Using Windows Credential Manager with PI applications**](#)

Миф №2: PI Mappings необходимо больше открытых портов чем PI Trust

Правда: Никаких дополнительных портов открывать не нужно.

[**2820OSI8 - Which firewall ports should be opened for a PI Data Archive?**](#)



Ресурсы

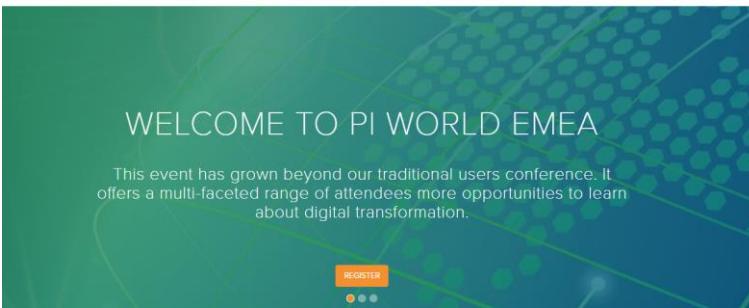
<https://github.com/osisoft/PI-Security-Audit-Tools/wiki/0.-Run-an-audit-%28USERS%29>

<https://github.com/osisoft/PI-Security-DSC/wiki/Getting-Started>

<https://pisquare.osisoft.com/videos/2020-pi-developers-club-webinar-series-introducing-the-pi-security-audit-tools>

<https://www.osisoft.com/Presentations>

<https://www.youtube.com/playlist?list=PLMcG1Hs2JbcvDuN8FhBrfMPDF5Gya5bYt>



WELCOME TO PI WORLD EMEA

This event has grown beyond our traditional users conference. It offers a multi-faceted range of attendees more opportunities to learn about digital transformation.

REGISTER

TOP REASONS TO ATTEND

FEATURED TOPICS:
EDGE STRATEGY
CLOUD SERVICES8 INDUSTRY SPECIFIC
TRACKS15 PRODUCT
PRESENTATIONS41 BOOTHES @ PARTNER
& PRODUCT EXPO18 HANDS-ON
TRAINING LABSNIGHTLY NETWORKING
EVENTS

<https://piworld.osisoft.com/emea2018>

По вопросам участия обращайтесь по
электронной почте:

efateeva@osisoft.com

+7 495 139 59 99

SCHEDULE OF EVENTS

PRE-CONFERENCE EVENTS	DAY 1	DAY 2	DAY 3
MONDAY, SEPT. 24 <ul style="list-style-type: none">• Academic Symposium• Partner Meeting & Reception• Enterprise Summit• Innovation Hackathon• Diversity & Inclusion Forum• First Time Attendee Presentation & Networking Reception• Welcome Reception	TUESDAY, SEPT. 25 <ul style="list-style-type: none">• General Session & Keynotes• Networking Lunch• Partner & Product Expo• Customer Presentations• Executive Forum• Discussion Forums (pre-registration required)• Expo Reception• Industry Dinners (invite only)	WEDNESDAY, SEPT. 26 <ul style="list-style-type: none">• Industry-specific Customer Presentations (nine tracks)• Networking Lunch• Partner & Product Expo• User Group Meetings• La Fiesta de OSIsoft Offsite Dinner Networking Event	THURSDAY, SEPT. 27 <ul style="list-style-type: none">• General Session• Product Track• Developer Track• Marketplace Partner Showcase• Partner & Product Expo• Training labs (pre-registration required)• Closing Fiesta del Sol - Puro Beach - Hilton

[VIEW AGENDA](#)

Осенняя серия тренингов по PI System в Москве

8 - 11 октября 2018 года - [PI SYSTEM ARCHITECTURE, PLANNING AND IMPLEMENTATION](#)

15 - 18 октября 2018 года - [PI SYSTEM ADMINISTRATION FOR IT PROFESSIONALS](#)

22 - 25 октября 2018 года - [BUILDING PI SYSTEM ASSETS AND ANALYTICS WITH PI AF](#)

29 - 31 октября 2018 года - [ANALYZING PI SYSTEM DATA](#)

19 - 22 ноября 2018 года - [PI SYSTEM ADMINISTRATION FOR IT PROFESSIONALS](#)

Заявки на участие, а также все интересующие Вас вопросы отправляйте по
адресу **RUSSIA@OSISOFT.COM** или звоните по телефону **+7 495 139 59
99.**

Адрес места проведения обучения: г.Москва, БЦ Аквамарин III, Озерковская
набережная, дом **24**, строение **3**, офис **203**.

 **osisoft** **THANKYOU**

DZIĘKUJĘ CI
NGIYABONGA
TEŞEKKÜR EDERIM
DANKIE
СПАСИБО
PAKMET CІЗГЕ
GO RAIBH MAITH AGAT
БЛАГОДАРЯ **GRACIAS**
ТИ БЛАГОДАРАМ
TAK DANKE MAHADSANID
RAHMAT **MERCI**
HATUR NUHUN
CẨM ƠN BẠN
WAZVIITA

謝謝 KEA LEBOHA
ТАPADH LEIBH 고맙습니다
БАЯРЛАЛАА MISAOTRA ANAO
OBRIGADO شکرا
DANKON TANK TAPADH LEAT

MULȚUMESC
FAAFETAI
ESKERRIK ASKO
HVALA ХВАЛА ВАМ
TEŞEKKÜR EDERIM
ДЗЯКУЙ **GRAZIE**
DI OU MÈSI
ĐAKUJEM
MATUR NUWUN

EYXAPISTΩ GRATIAS TIBI
AČIU SALAMAT MAHALO IĀ 'OE TAKK SKALDU HA
GRAZZI PAKKA PÉR SIPAS JI WERE TERIMA KASIH
PAXMAT CATA FALEMINDERIT
ありがとうございました
UA TSAUG RAU KOJ
ТИ БЛАГОДАРАМ
СИПОС