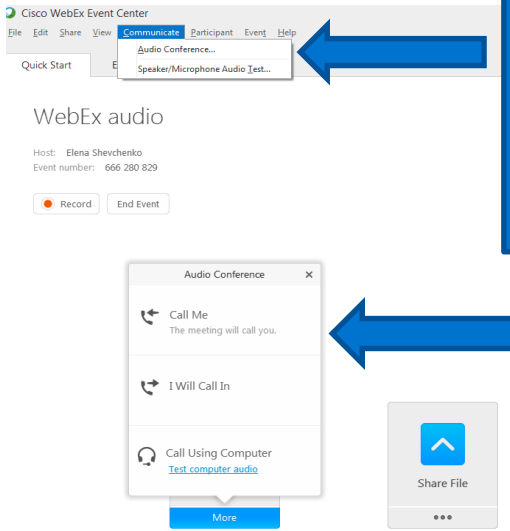
«Вебинар: «Информационная безопасность на производстве и ее реализация средствами PI System»

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

OSIsoft.

План

- **Кибератаки** → **типы**

↓ ↘ **статистика**

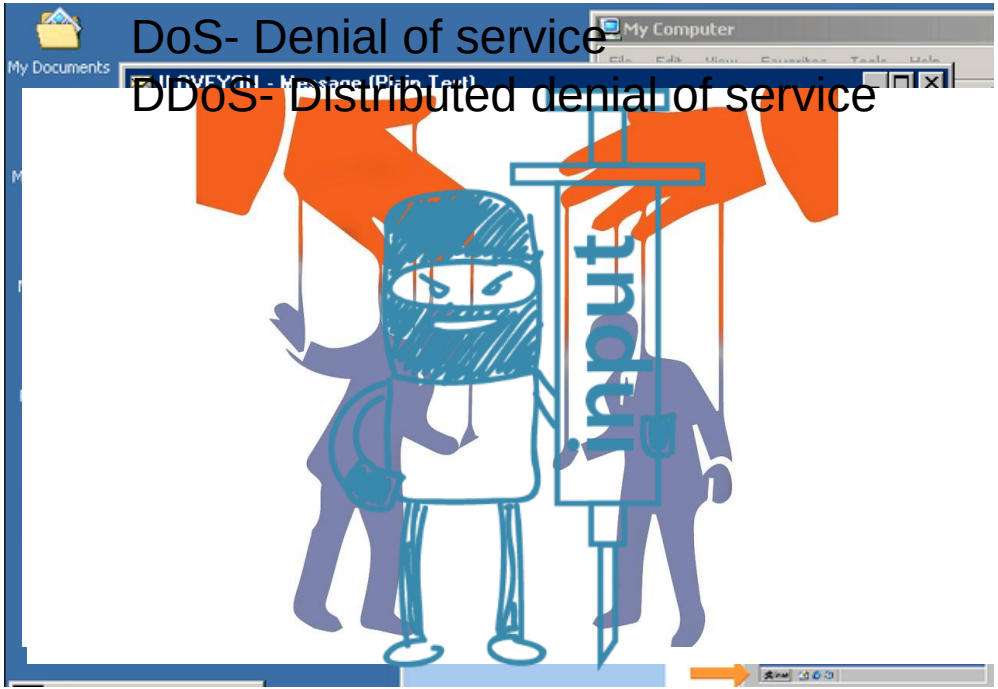
Известные кибератаки

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

Кибератаки в терминах и цифрах

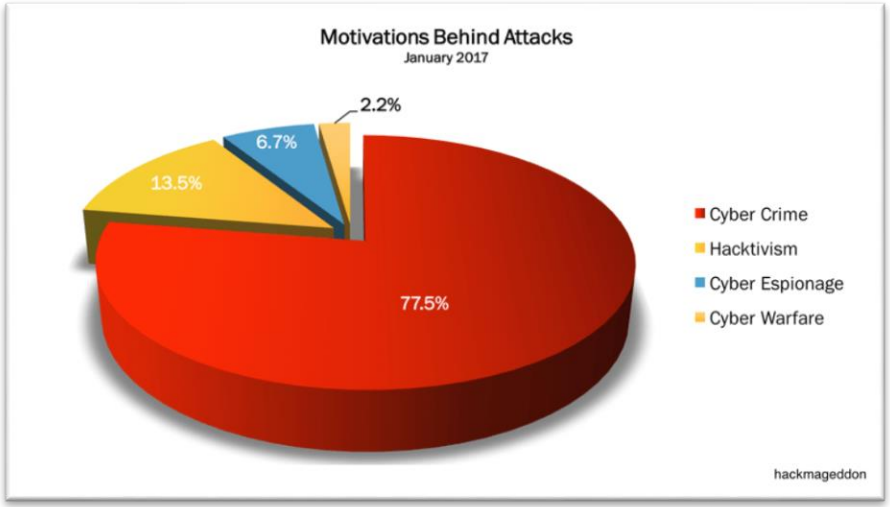
Кибератаки

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

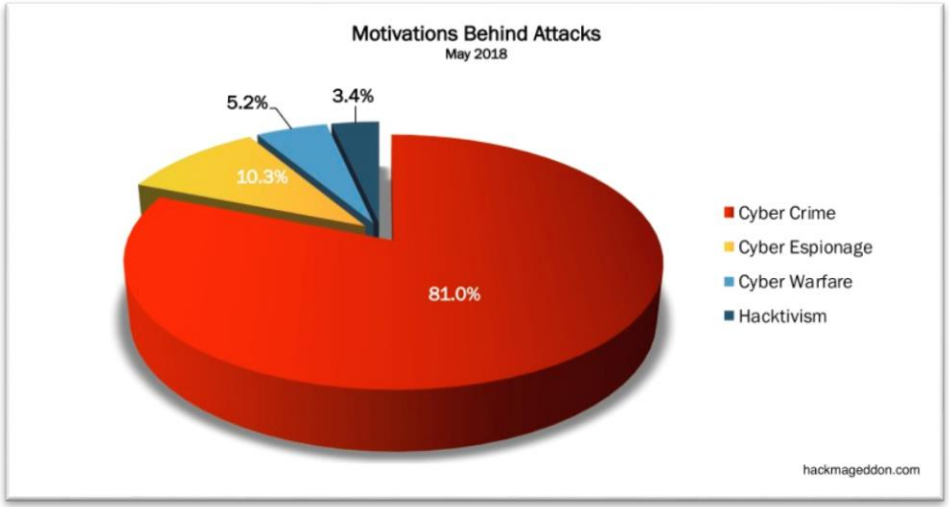


Статистика хакерских атак (Мотивация)

Январь 2017 Статистика кибератак



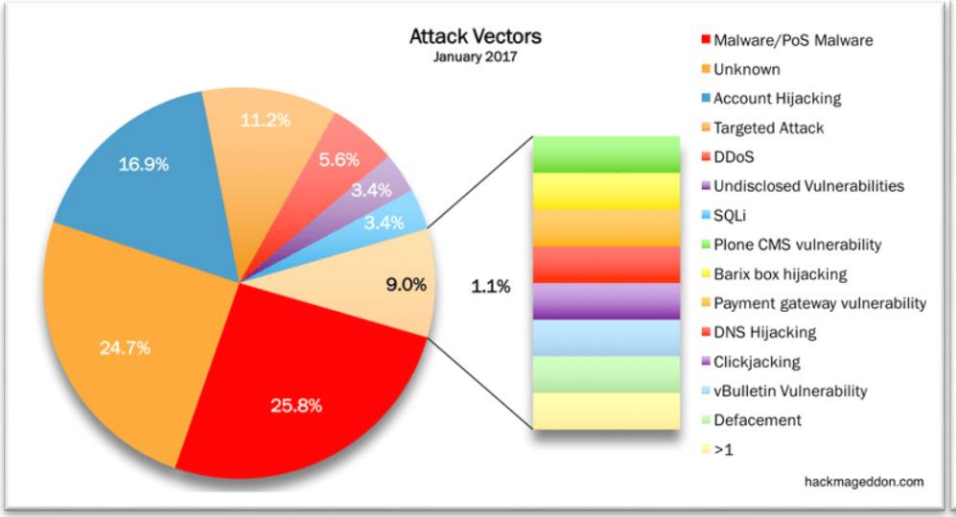
Май 2018 Статистика кибератак



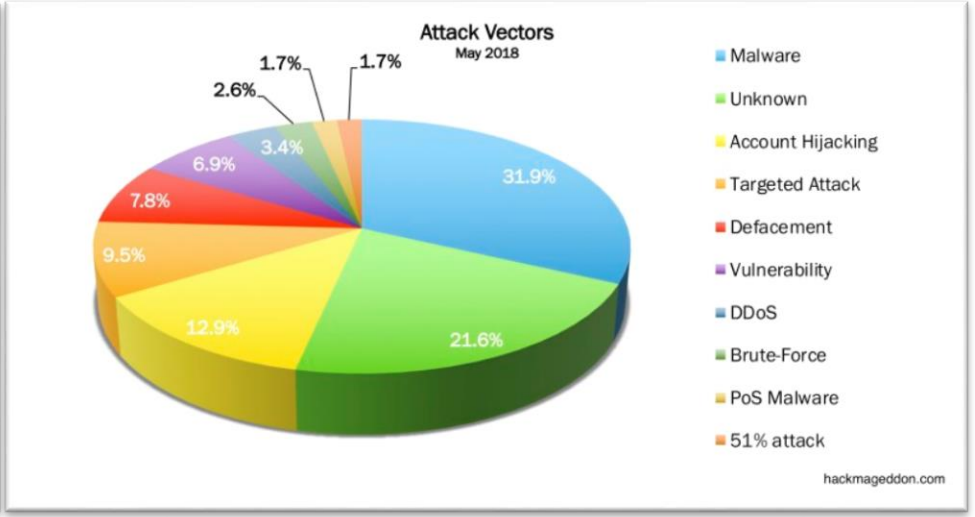
https://www.hackmageddon.com/2017/03/02/january-2017-cyber-attacks-statistics/

Статистика хакерских атак (Векторы атак)

Январь 2017 Статистика кибератак



Май 2018 Статистика кибератак

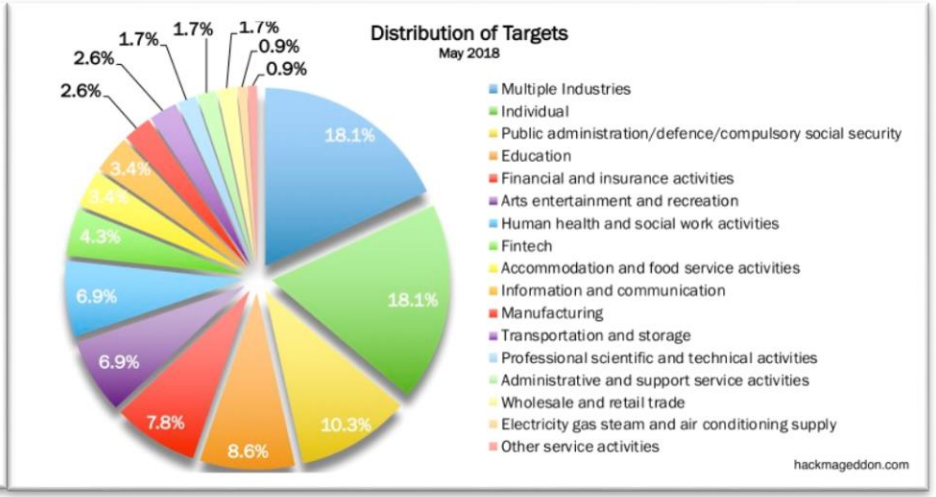


https://www.hackmageddon.com/2017/03/02/january-2017-cyber-attacks-statistics/

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, эксплойт EternalBlue	Уязвимость «нулевого дня»	Взлом, как стандартная транзакция

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

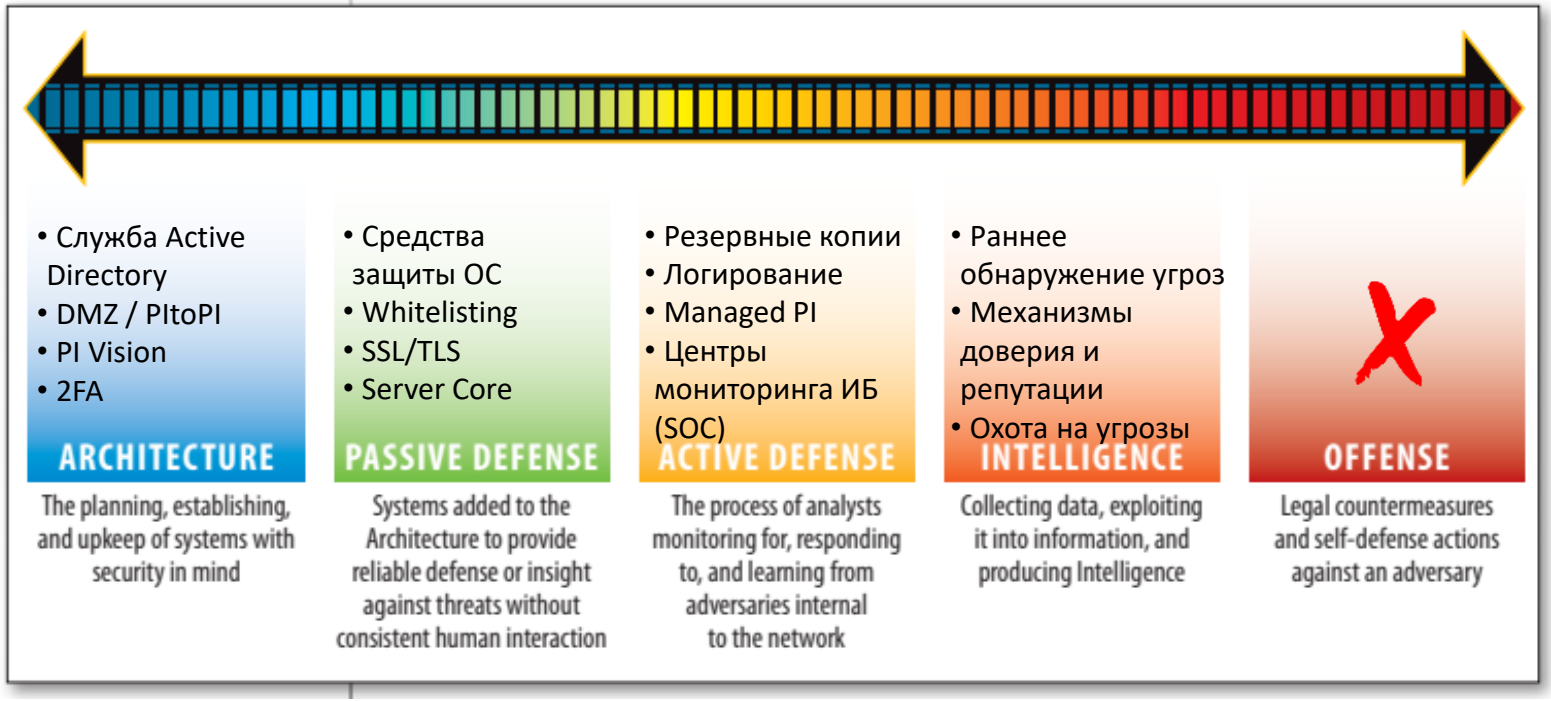
Ginter, Andrew (2016*) SCADA Security: What's broken and how to fix it*. Calgary: Abterra

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)

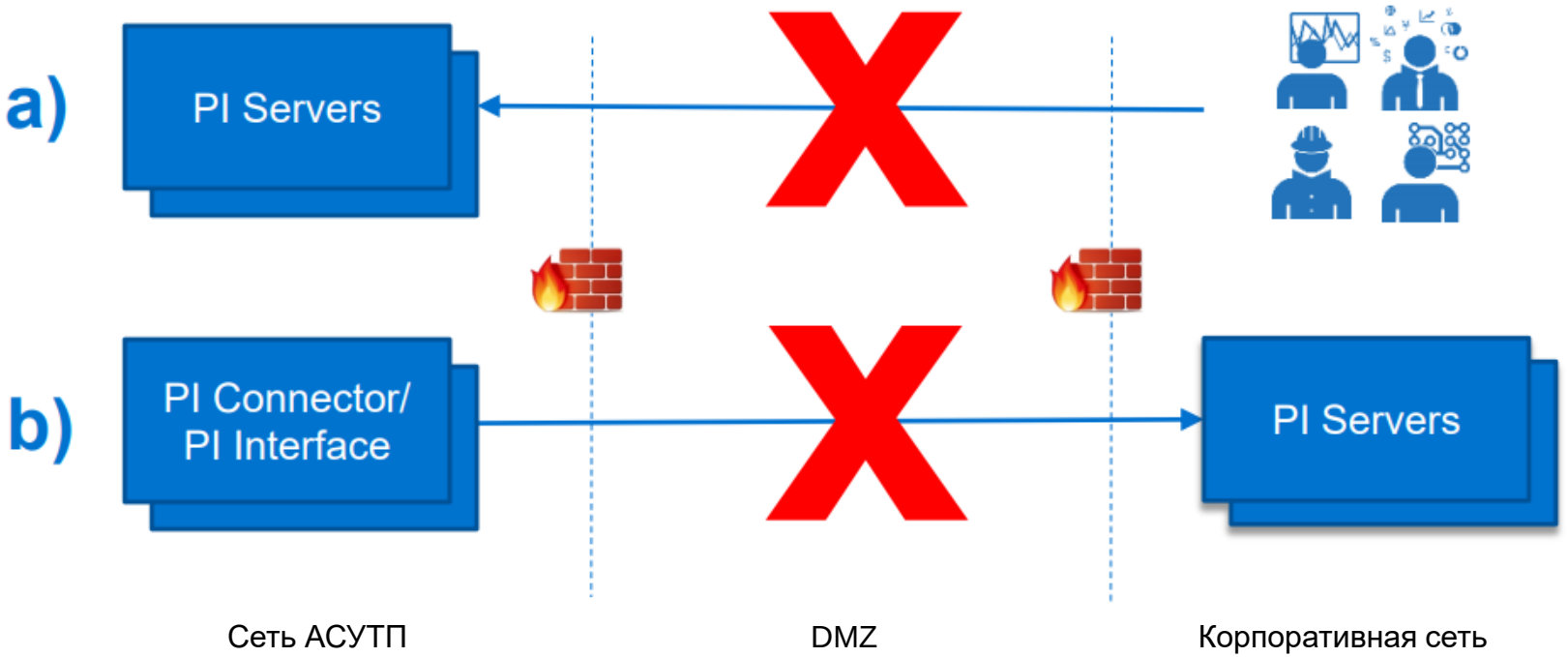
Комсомольская правда: Информационная безопасность предприятия: ключевые угрозы и средства защиты

SANS “Sliding Scale of Security” Архитектурная защита должна быть высокоприоритетной

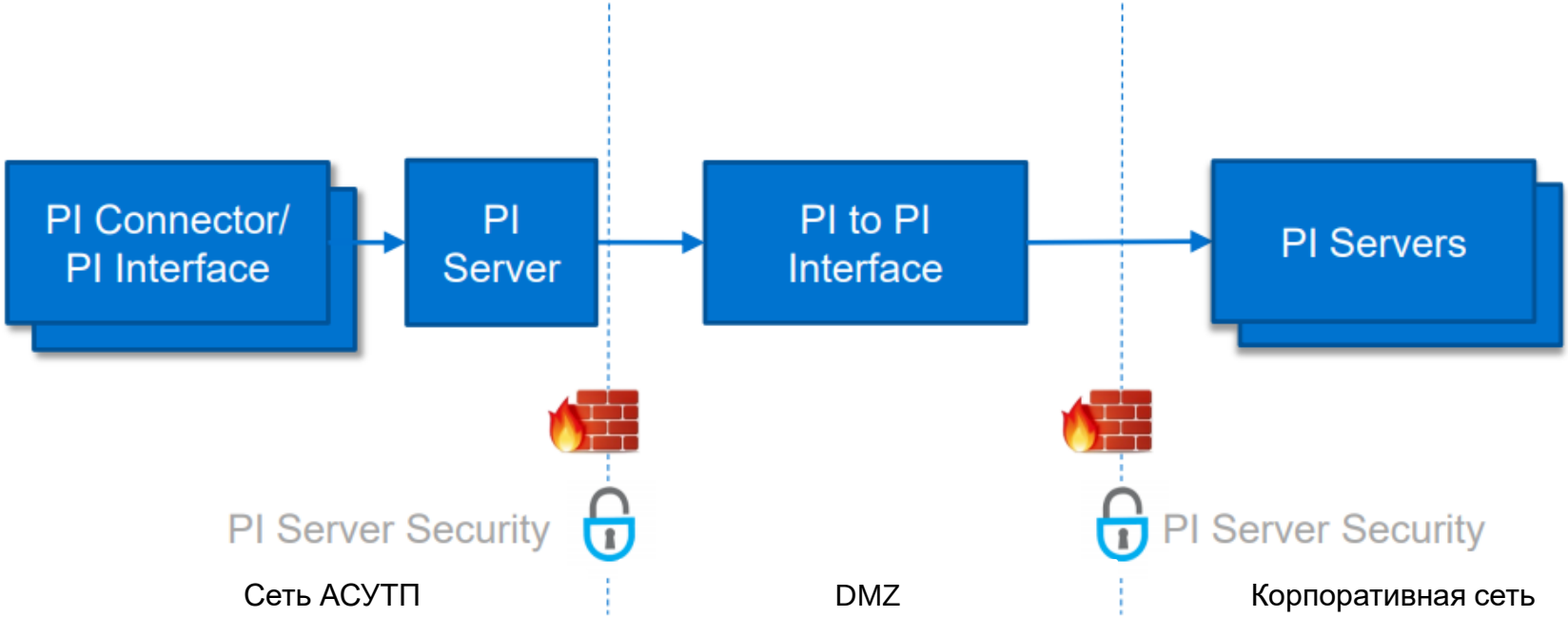


Архитектурные решения PI System

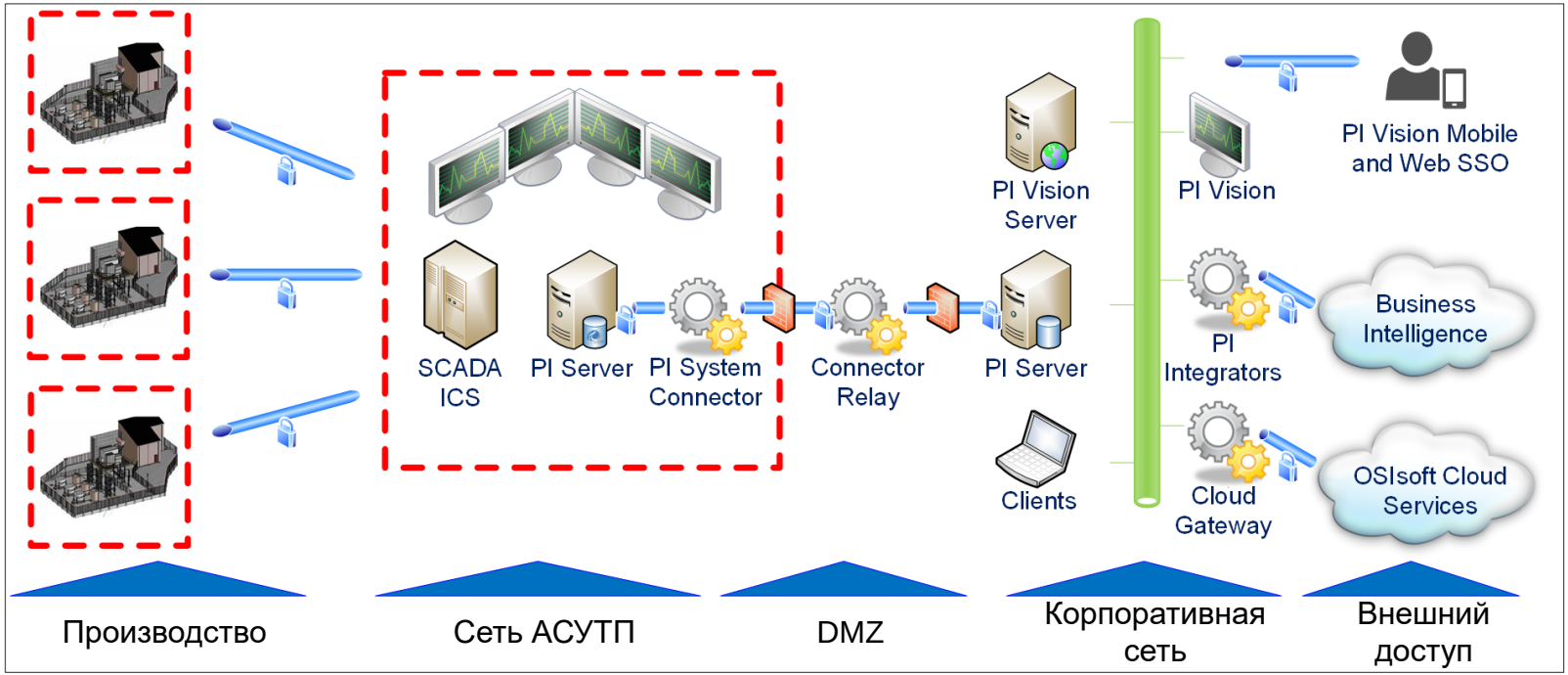
Нерекомендуемая топология



Стандартное решение



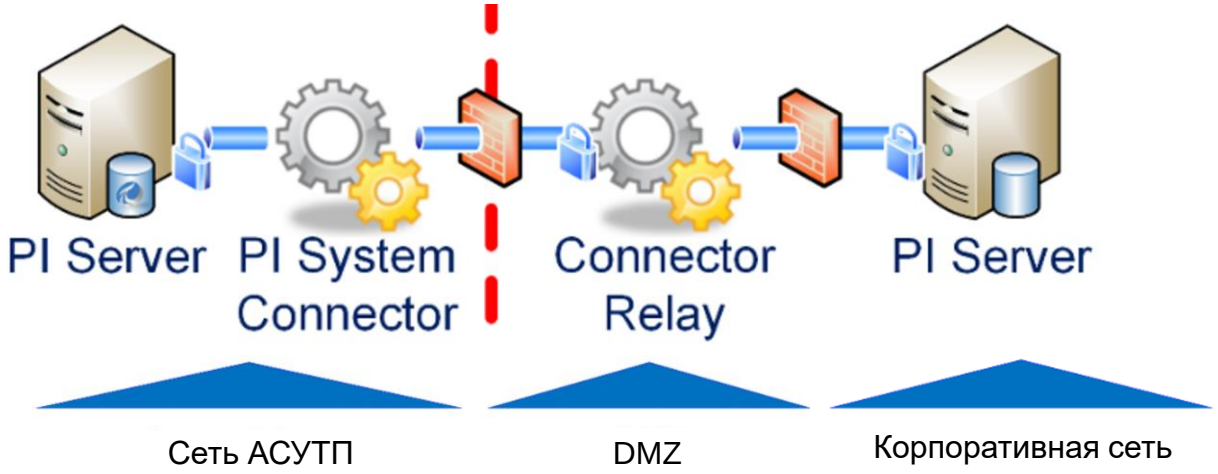
Архитектура безопасности PI System



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 однонаправленный поток данных из сети АСУТП в корпоративную сеть



Ограничение рисков критических систем с PI System

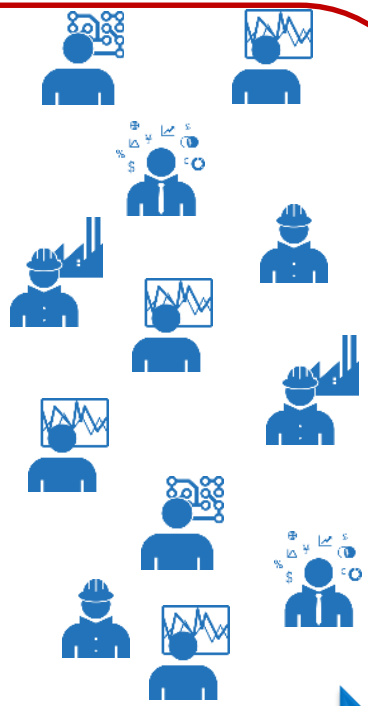
Передача & Распределение SCADA

Распределительная система управления

ПЛК

Система экологической безопасности

Другие критические операционные системы



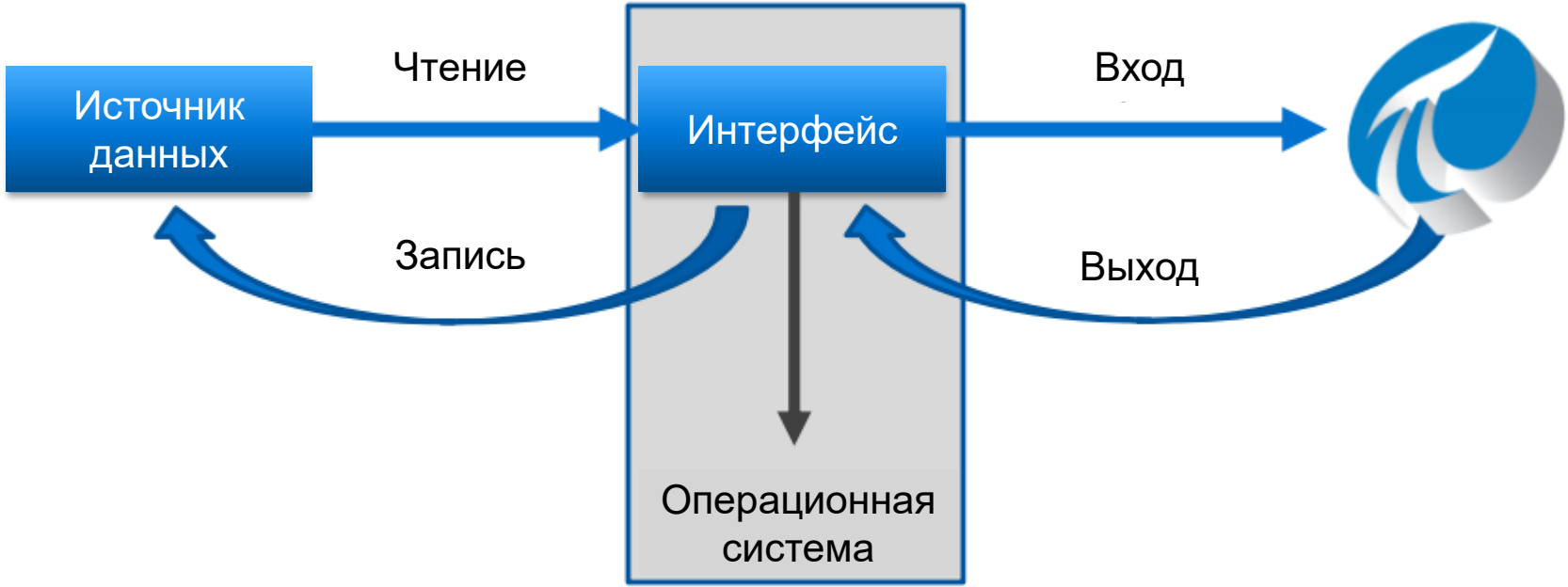
OSIsoft.

Infrastructure

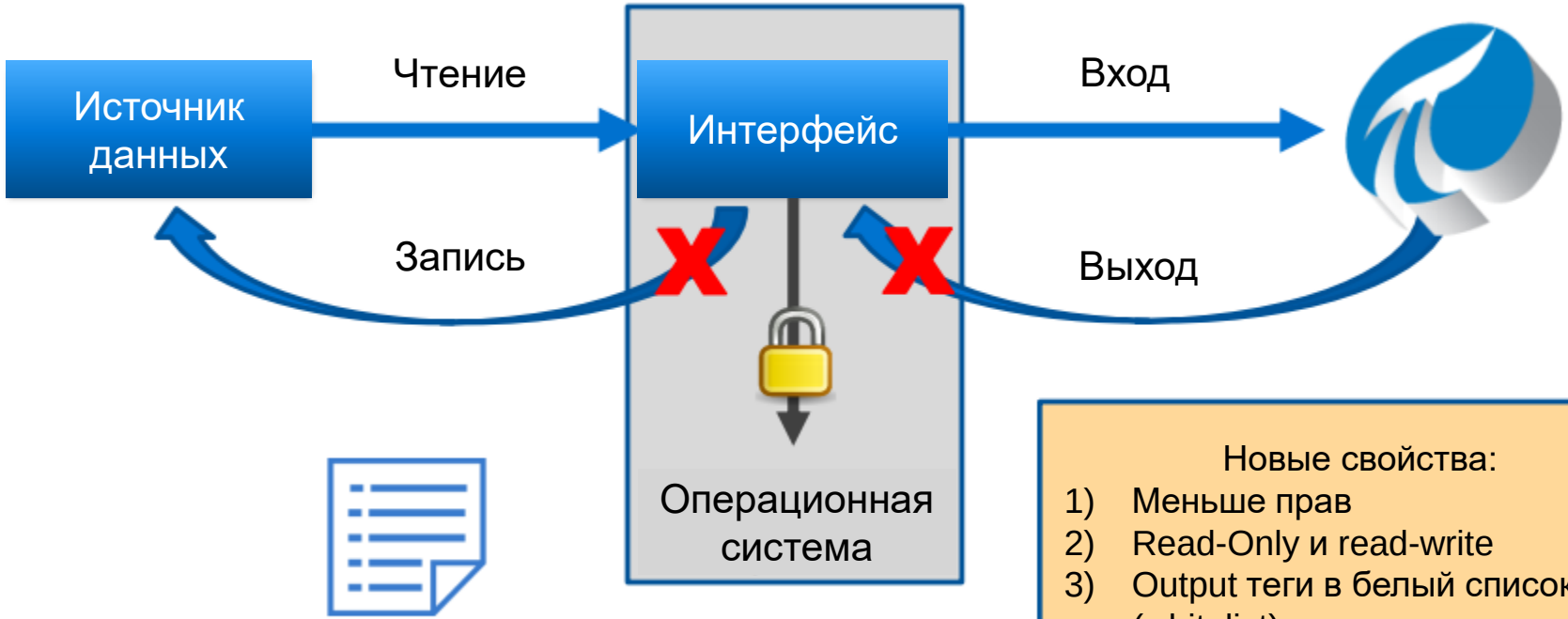
Периметр безопасности

Снижение рисков на критических системах

Read-Write Интерфейсы



Read-Only Интерфейсы



Белый список “Whitelist”

Новые свойства:
1) Меньше прав
2) Read-Only и read-write
3) Output теги в белый список (whitelist)

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

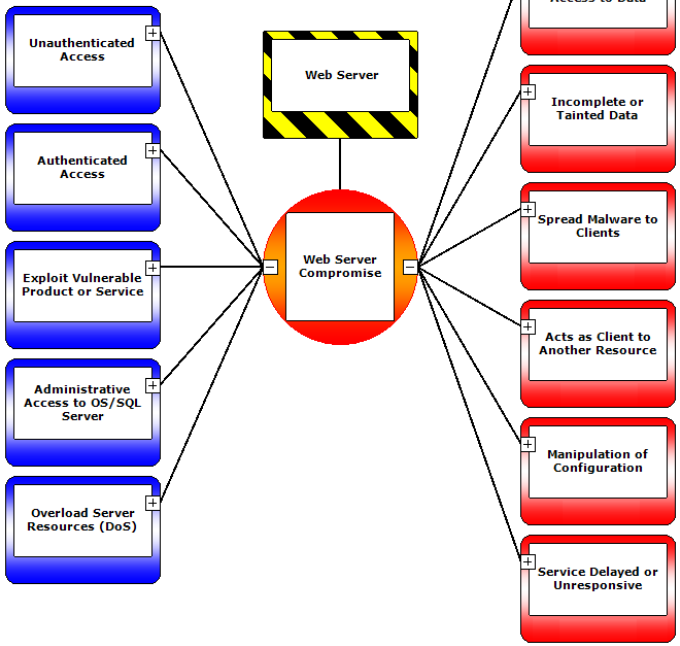
Пример: минимум полномочий для ограничения доступа, предоставляемого злоумышленнику, в случае компрометации компонента

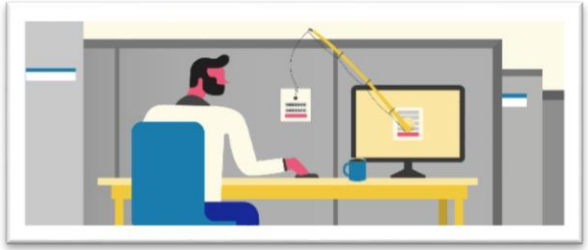
3) Обнаружить аномалии и отреагировать

Определение угроз и последствий

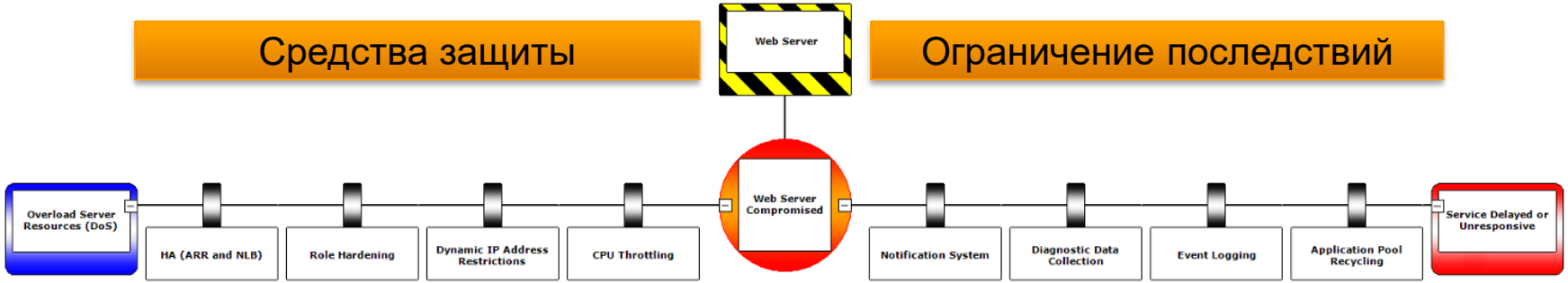
Угрозы

Последствия

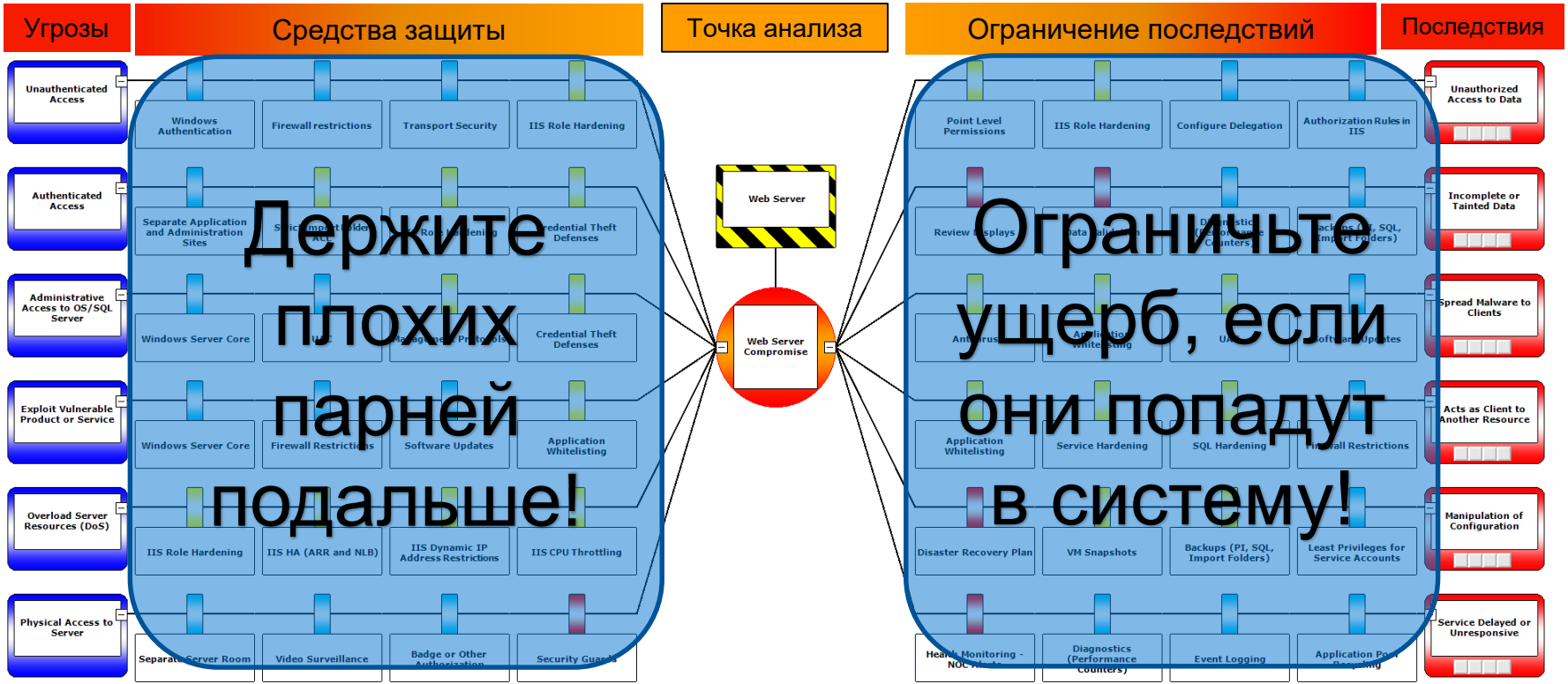




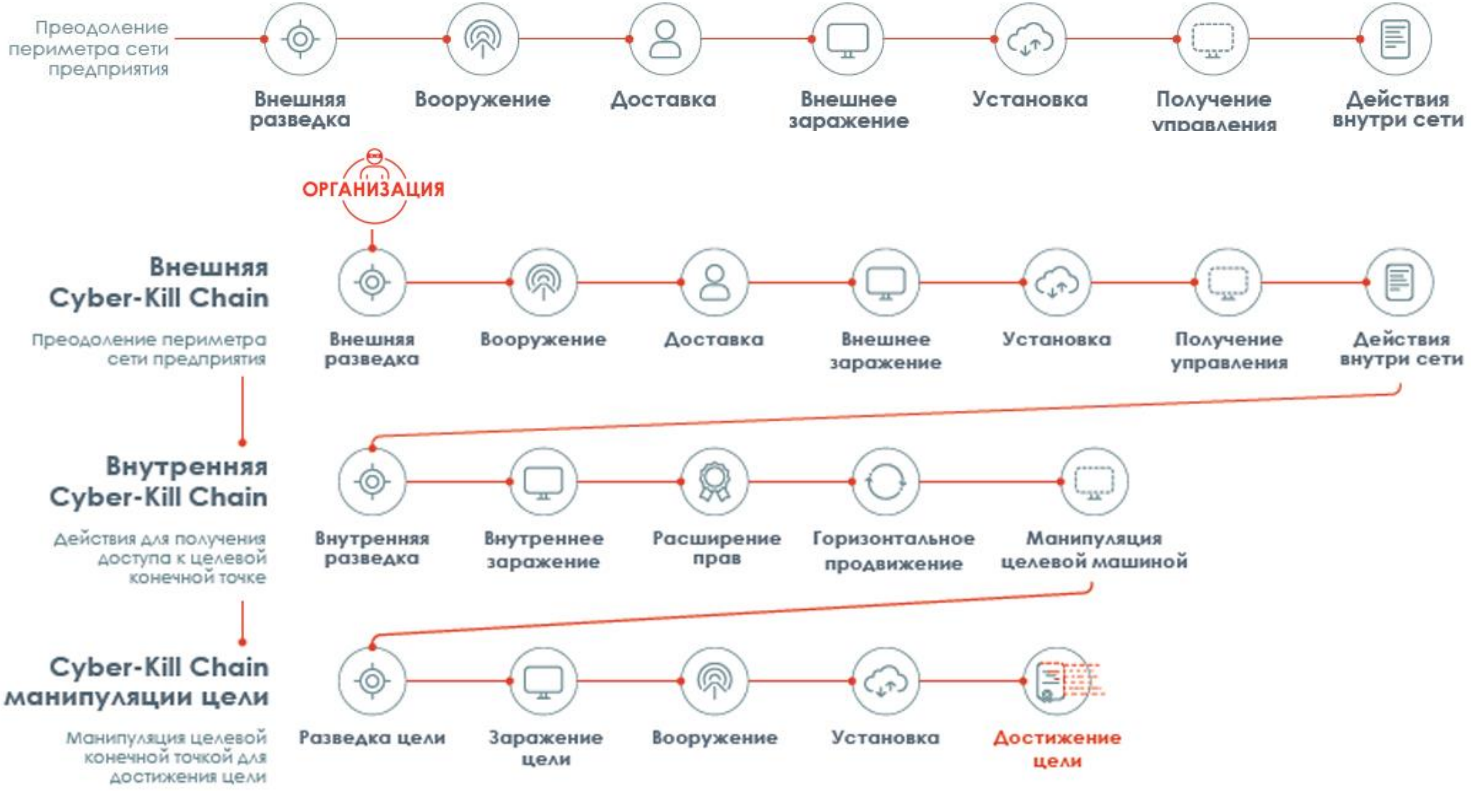
Выстраивание барьеров



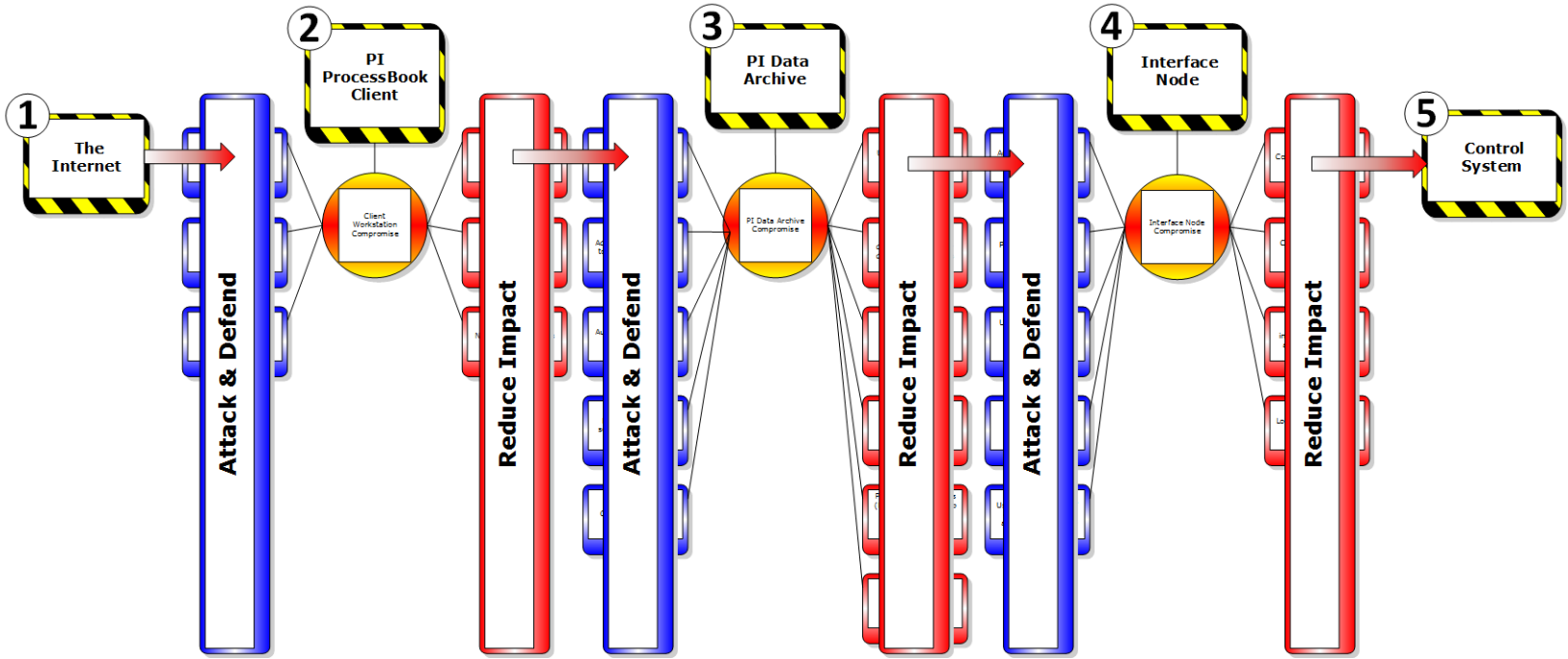
Переход к модели Bow-Tie



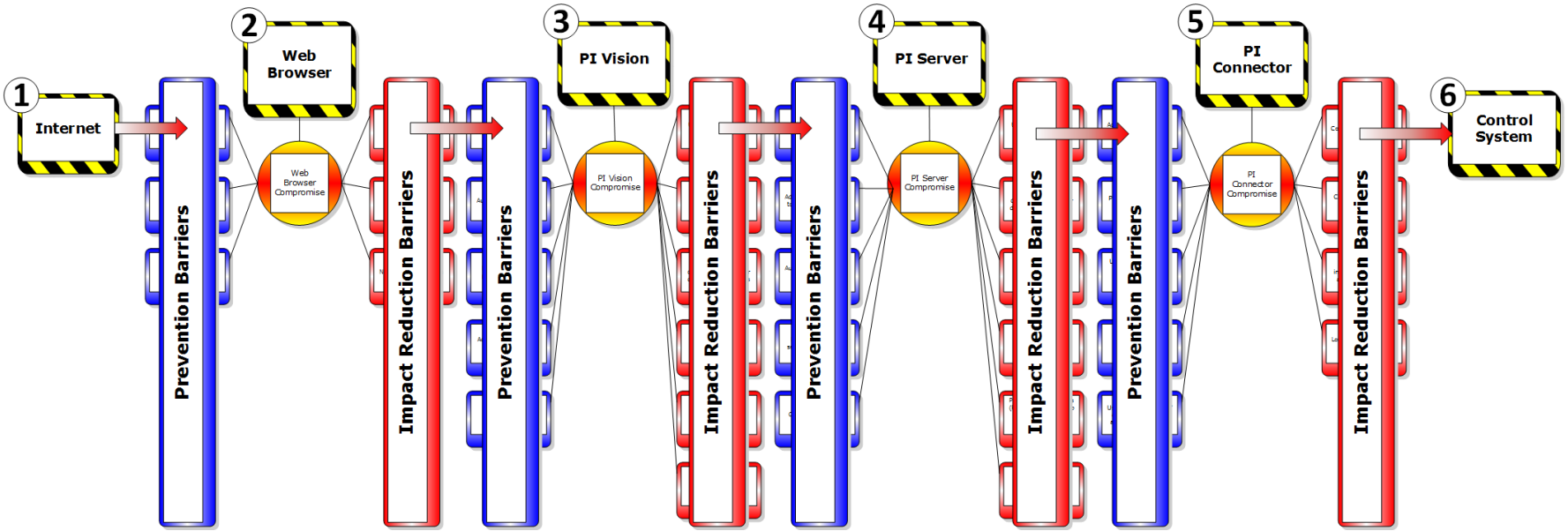
Модель и этапы



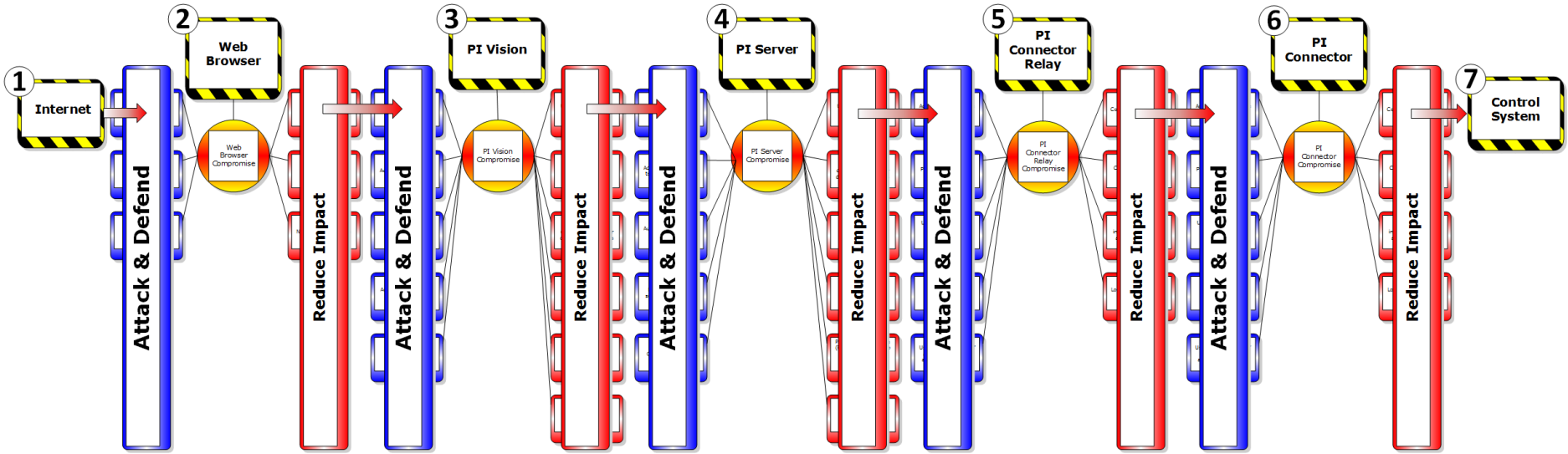
Классическая PI System Kill Chain



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 whitelistening (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:

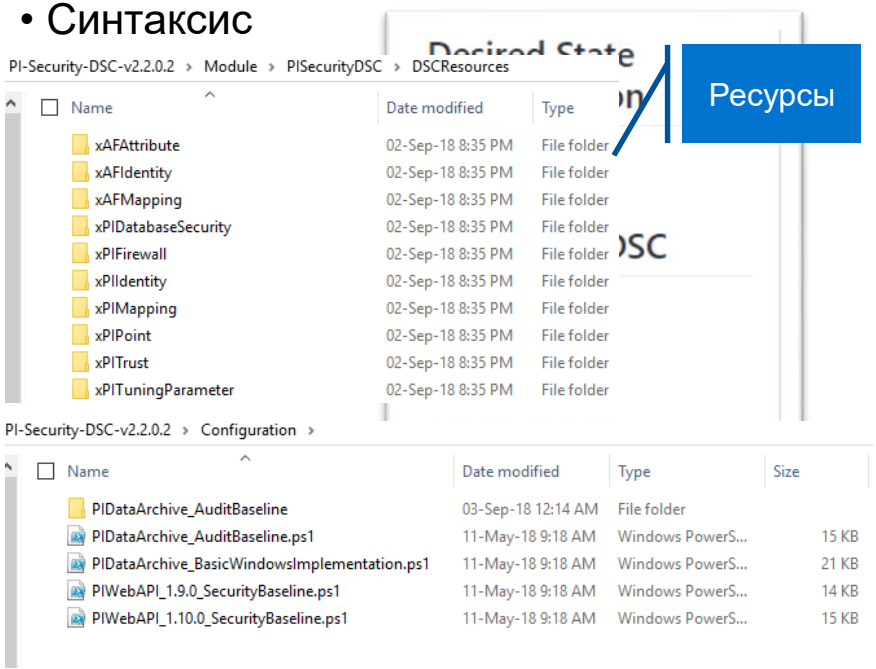
- PSv3+
- Run as Admin (AF&Vision)
- Osisoft.Powershell
- WinRM enabled (if remote)

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
1	ID	ServerName	AuditItemName	AuditItemValue	AuditItemFunction	MessageL	Group1	Group2
2	AU10002	PICLIENT01	Operating System Installation Type	Fail	Get-PISysAudit_CheckOSInstallationType	The follov	Machine	Operating System
3	AU10006	PICLIENT01	Hello World	Fail	Get-PISysAudit_HelloWorld	Chuck Nor	Machine	Policy
4	AU10007	PICLIENT01	Disallowed Scheduled Tasks	Fail	Get-PISysAudit_ScheduledTasks	List of dis	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	Recomme	Machine	Policy
8	AU10001	PICLIENT01	Domain Membership Check	Pass	Get-PISysAudit_CheckDomainMemberShip	Machine i	Machine	Domain
9								
10								
11								
12								

PI Security DSC Recourses

- Getting Started Guide в Wiki
- Синтаксис



Ресурсы

Конфигурации

PIConfiguration AF DataBase

- AFAttribute

PI AF Security

- AF Identity
- AF Mapping

PI Data Archive

- PIDataBaseSecurity
- PIFirewall
- PIPoint
- PITrust
- PITuningParameter

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

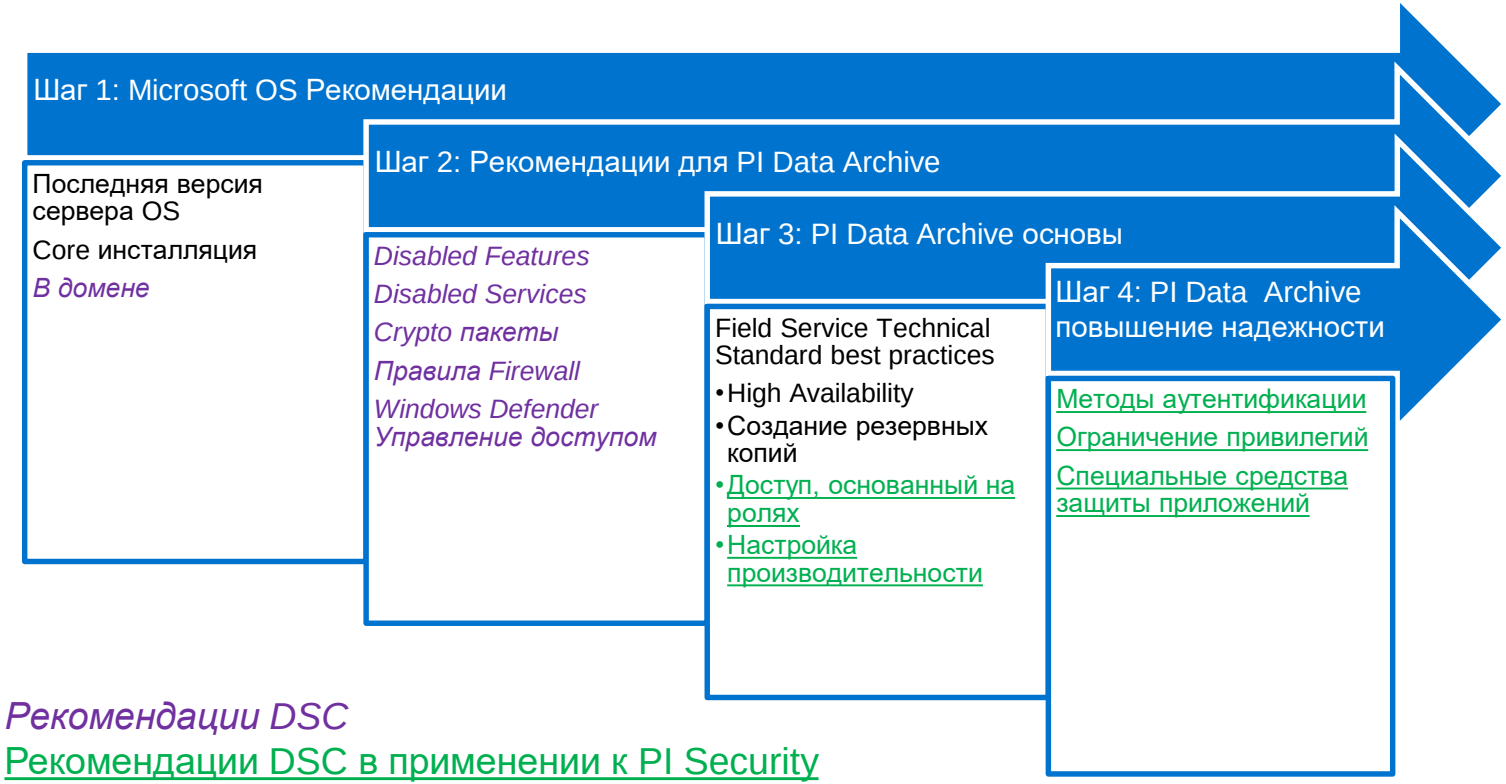
- Как начать работу с DSC?
- Проверка желаемых настроек конфигурации для PI Data Archive (tuning parameter, PI Identities)
- Проверка желаемых настроек конфигурации PI AF Security (AF Mapping)
- Как применить изменения?

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)



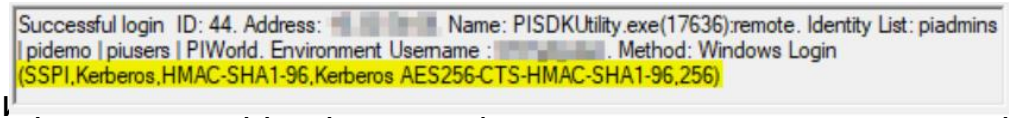
Рекомендации DSC

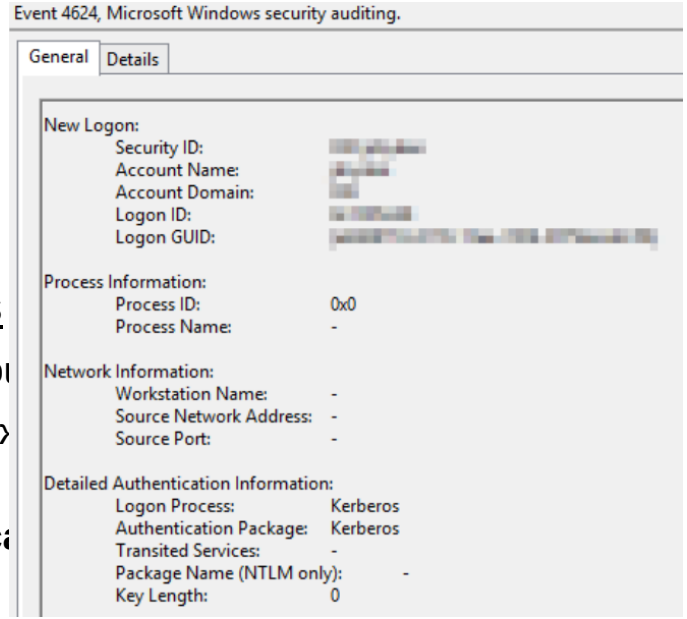
Рекомендации DSC в применении к PI Security

WIS TRUST

Преимущества:

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





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

https://piworld.osisoft.com/emea2018

По вопросам участия обращайтесь по электронной почте:

efateeva@osisoft.com

+7 495 139 59 99

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.**


謝謝
KEA LEBOHA
TAPADH LEIBH
고맙습니다
DZIĘKUJĘ CI
БАЯРЛАЛАА
MISAOTRA ANAO
NGIYABONGA
GRÀCIES
SALAMAT
OBRIGADO
شكرا
TEŞEKKÜR EDERIM
DANKIE
TERIMA KASIH
DANKON
TANK
TAPADH LEAT
KÖSZÖNÖM
СПАСИБО
MULȚUMESC
OSIsoft
PAKMET CIЗГЕ
FAAFETAI
GO RAIBH MAITH AGAT
ESKERRIK ASKO
HVALA
HVALA
ХВАЛА ВАМ
БЛАГОДАРЯ
GRACIAS
THANKYOU
TEŞEKKÜR EDERIM
ТИ БЛАГОДАРАМ
MAHADSANID
DANK JE
ΕΥΧΑΡΙΣΤΩ
GRATIAS TIBI
GRAZIE
TAK
DANKE
AČIŪ
SALAMAT
MAHALO IĀ ʻOE
TAKK SKAL DU HA
ДЯКУЙ
DI OU MÈSI
RAHMAT
MERCI
GRAZZI
ÞAKKA ÞÉR
ありがとうございました
ĎAKUJEM
HATUR NUHUN
PAXMAT САГА
SIPAS JI WERE
TERIMA KASIH
MATUR NUWUN
CẢM ƠN BẠN
UA TSAUG RAU KOJ
FALEMINDERIT
WAZVIITA
ТИ БЛАГОДАРАМ
СИПОС