

# JET SECURITY CONFERENCE



## VIII ежегодная конференция Центра информационной безопасности

1-2 июня 2017 года

[WWW.JET.SU](http://WWW.JET.SU)

Radisson BLU



IMPERVA



POSITIVE TECHNOLOGIES

tufin

FORTINET



TRAPX  
SECURITY

ONE IDENTITY

RAPID7

iDeals  
VIRTUAL DATA ROOM



**JET** CONFERENCE

01/06/2017

# Проактивный контроль привилегированных пользователей

Александр Лопатин,  
менеджер по продвижению ЦИБ

## Привилегированные учетные записи – где они?



### Привилегированные уч. записи



## Последствия компрометации



Скомпрометированные уч. записи

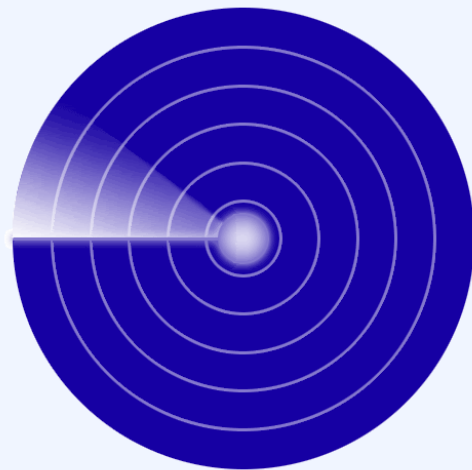




## Результаты 2016

**> 80%**

**крупных инцидентов безопасности связаны  
с компрометацией привилегированных учетных записей\***

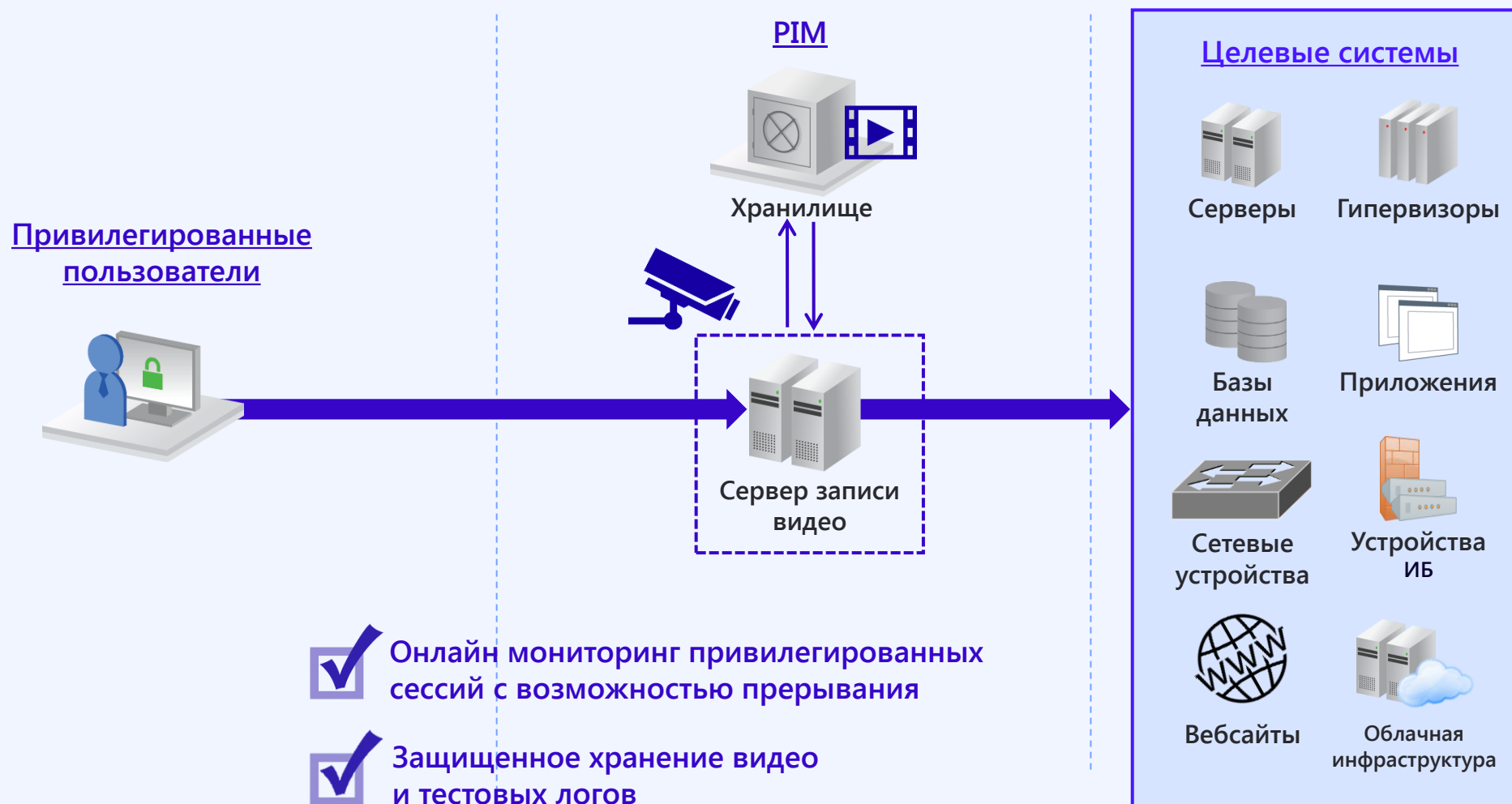


**Проникнув в сеть, нарушители остаются  
незамеченными месяцами**

- › Среднее время обнаружения  
проникновения для хорошо  
спланированных атак составляет 146 дней\*

\* по данным FireEye Madiant M-Trends 2017

## Классический ретроспективный подход



**JET**

CONFERENCE

Проактивный подход

Основная цель –  
сократить окно возможностей

## Управление паролями



### Поиск привилегированных учетных записей

- › Автоматическое обнаружение привилегированных уч. записей (в т. ч. App-to-App)
- › Передача управления учетной записью специализированному решению



### Централизованное защищенное хранилище паролей

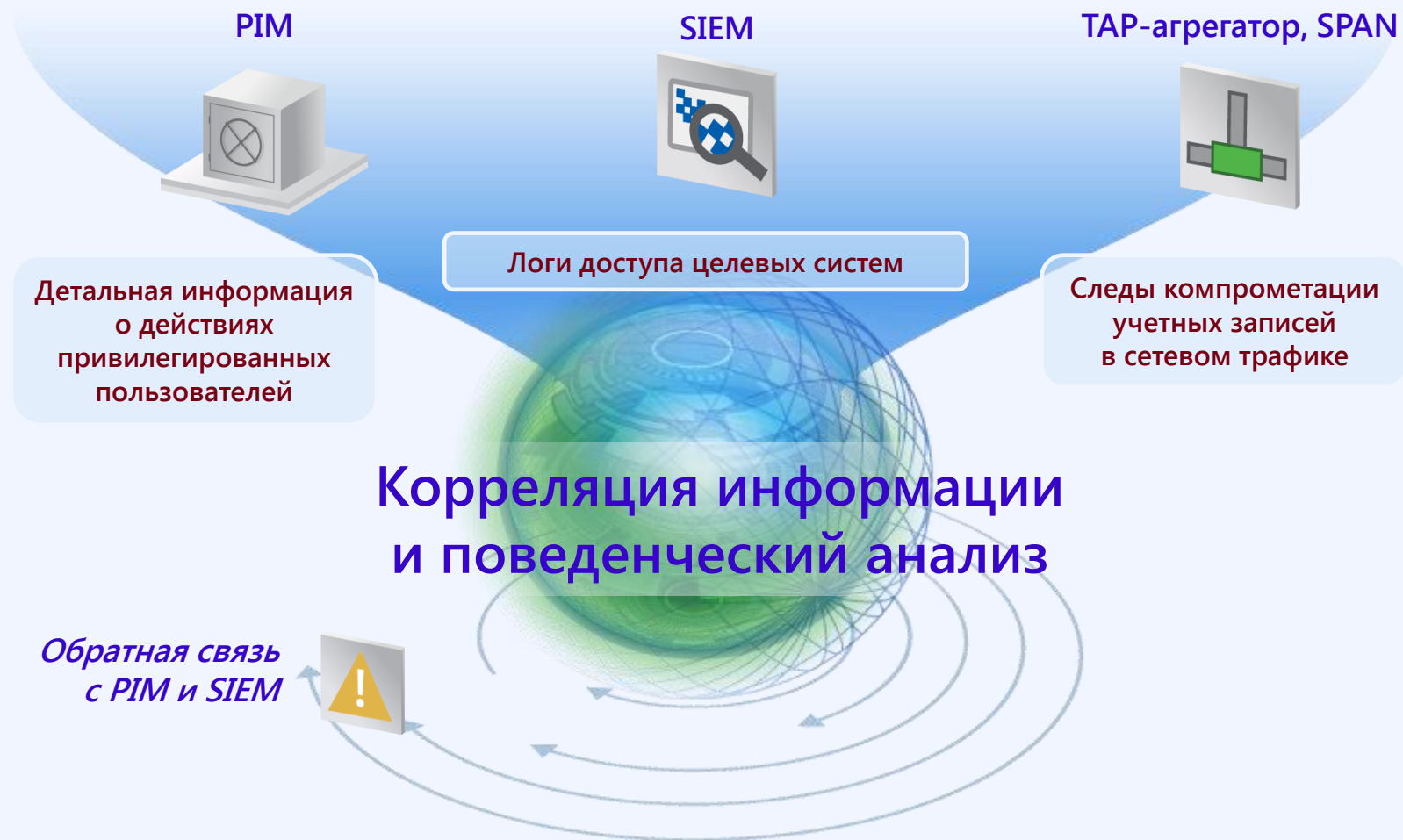
- › Хранение паролей во взломостойком хранилище
- › Реализация принципа «минимально необходимых привилегий» с помощью разграничения доступа к учетным записям



### Автоматическая ротация паролей привилегированных учетных записей

- › Ротация паролей на регулярной основе или после каждого использования в соответствии с политикой организации
- › Автоматическая смена и синхронизация паролей

## Real-time обнаружение



# JET

CONFERENCE

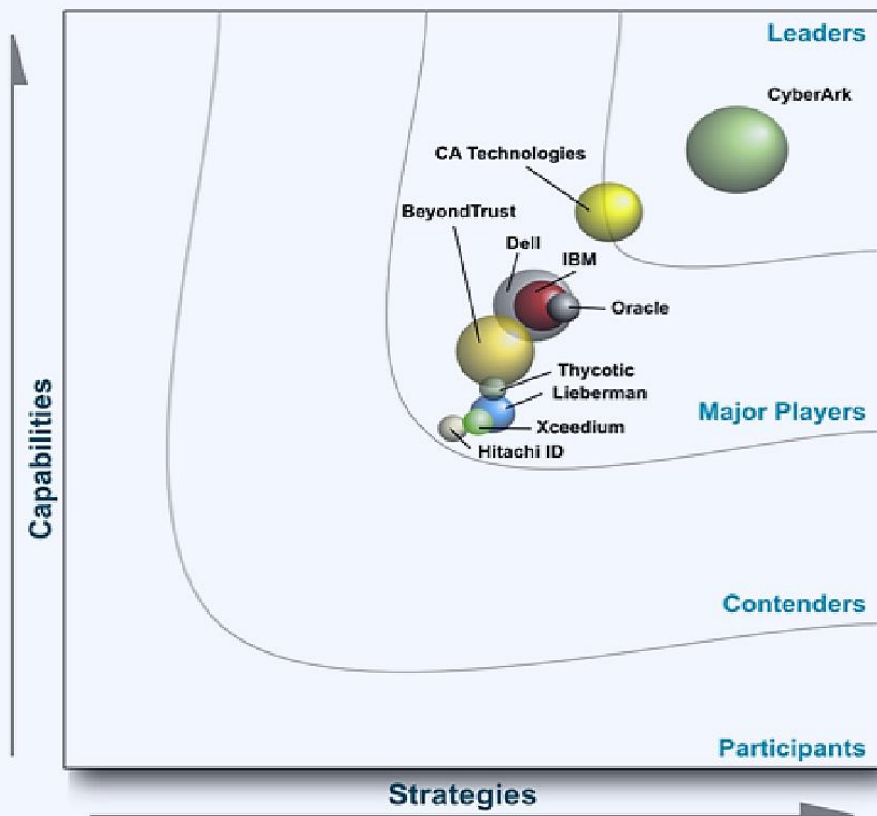
## Корреляция событий

- › Выявление признаков эскалации привилегий и кражи учетных записей
- › Обнаружение горизонтального продвижения (анализ нетипового поведения пользователей)
- › Детектирование нетипового запуска высококритичных команд и процессов, выявление инсайдерской активности
- › Выявление прямого использования привилегированных аккаунтов в обход PIM-решения



## Основные игроки рынка PIM

IDC MarketScape: Worldwide Privileged Access Management



Source: IDC

Инфосистемы Джет –  
единственный в России  
золотой партнер CyberArk





**JET** CONFERENCE

01/06/2017

**ИНФОСИСТЕМЫ ДЖЕТ**

Спасибо за внимание!