CYBERARK

Средства анализа уязвимостей привилегированных учетных записей и мониторинга действий привилегированных пользователей

21 октября 2014

CYBERARK

PAS 9.0!

Новые возможности

- **AD Bridge**
- Без агентов
- AD управляет пользователями UNIX/Linux
- Нет необходимости управлять УЗ UNIX
- Унификация ОРМ

- **EPV**
- Мастер описания процессов обнаружения новых аккаунтов
- Инструмент принятия решения на защиту
- «Тестовый» режим

- **AIM Central Credential Provider**
- Без агентов (серверных провайдеров)
- Поддержка аутентификации:
  - Доменный пользователь
  - Адрес машины
  - Цифровой сертификат

- **А также… (!)**

CYBERARK

Детализированный аудит сессий Windows

Функциональная конкуренция?...

Конкурент	Запись сессий	Изоляция и управление	Гетерогенное окружение	Без агентов	Доверенный аудит	Масштаби-руемость	Поддержка любых платформ
№1	+	-	-	-	-	-	-
№2	+	-	+-	+	-	+	-
№3	+-	+	+	+	+	-	-
CyberArk	+	+	+	+	+	+	+

«Администратор легко останавливает агент, а затем снова его включает».

«Мы не можем быть уверены, что записывается все, как требует регулятор».

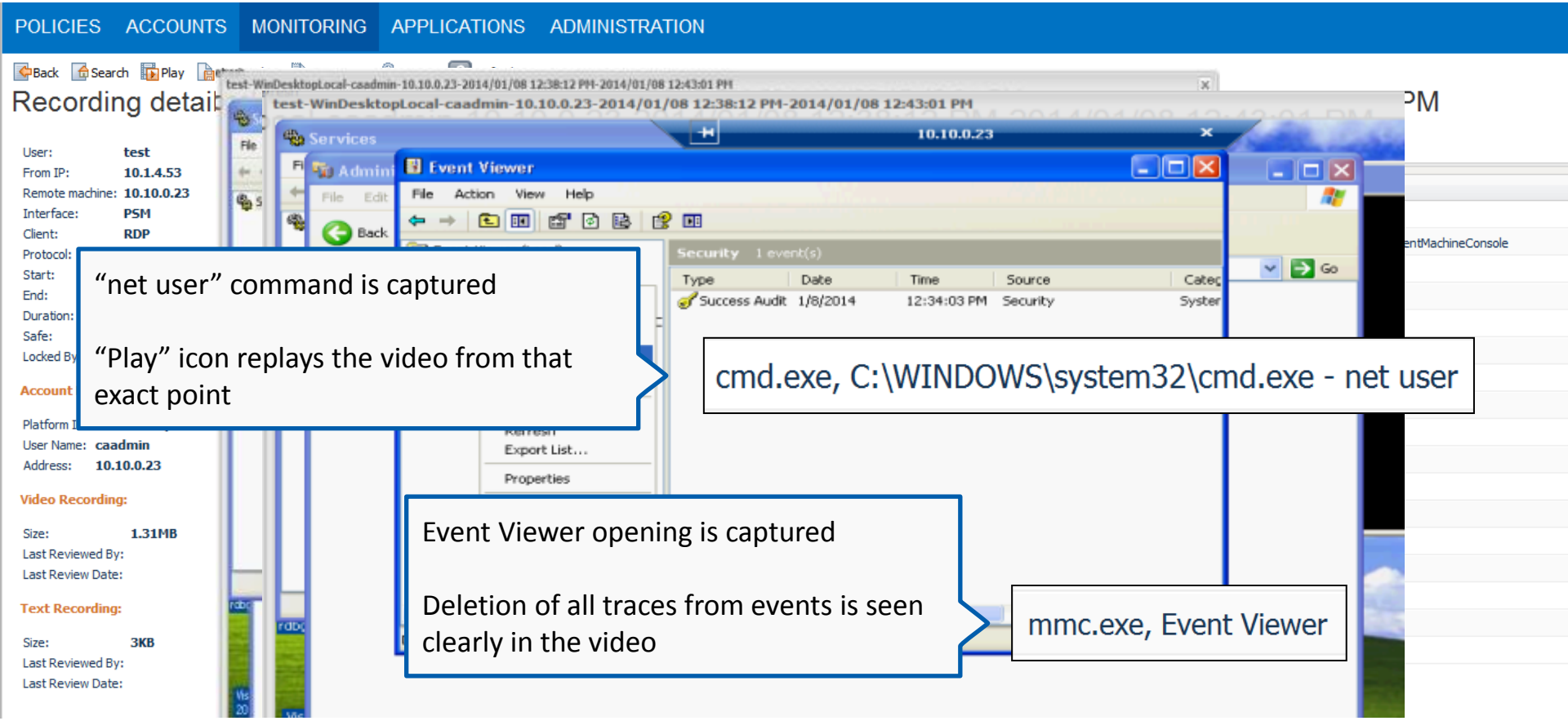
«Агент на сервере или на клиенте – легко компрометируется».

«Не защищенный репозиторий аудита – записи можно удалить».

«Репозиторий аудита DBA вообще не контролируется».

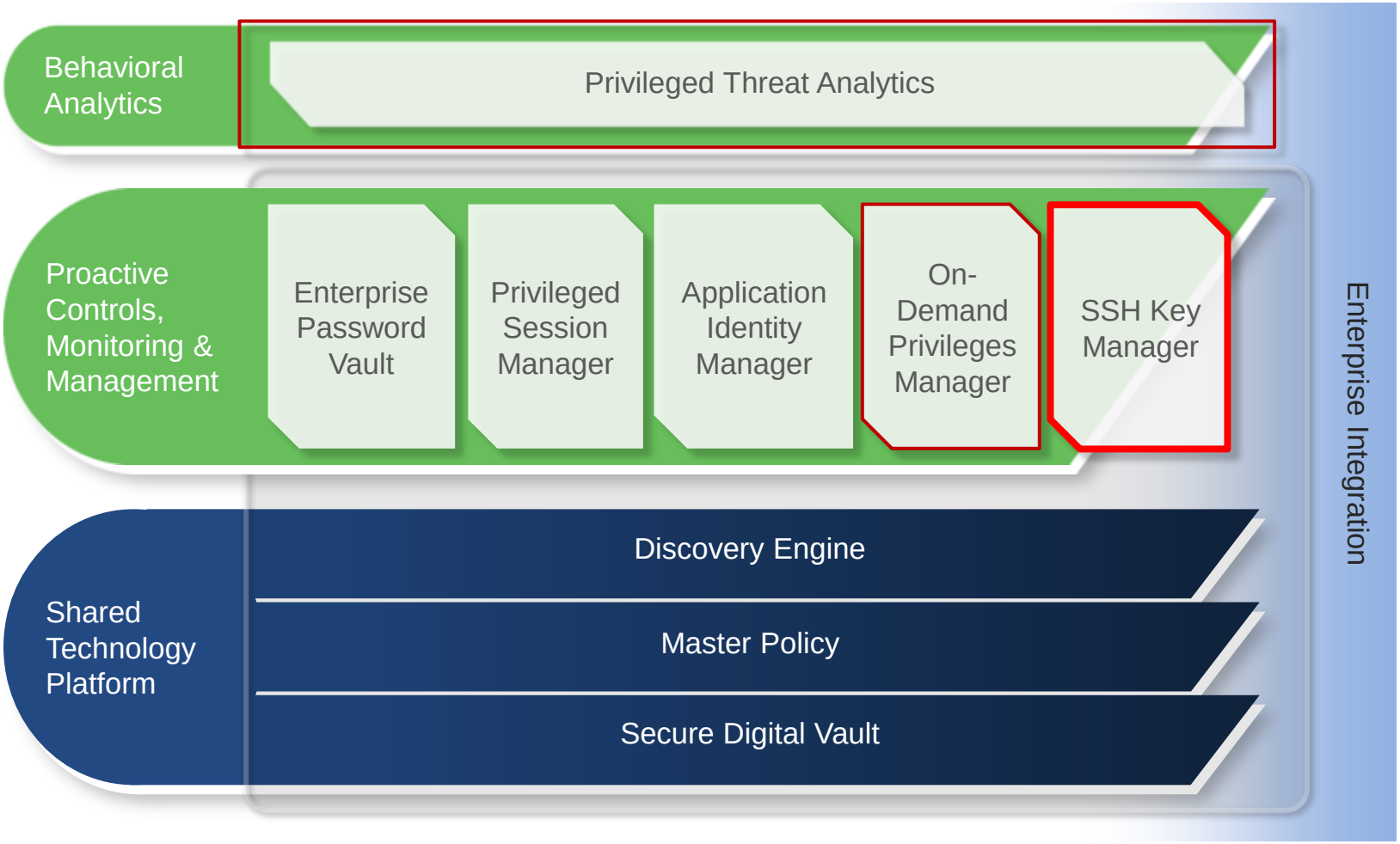
CYBERARK

Индексация, метка времени, поиск >> результат



- **Просмотр локализованного фрагмента, без агента**
  - Захват событий сессий RDP в Windows, включая текст (команды)
  - Легкий поиск и просмотр
- **Обнаружение угроз**
  - Интеграция с SIEM для создания правил реагирования

Решение CyberArk PAS



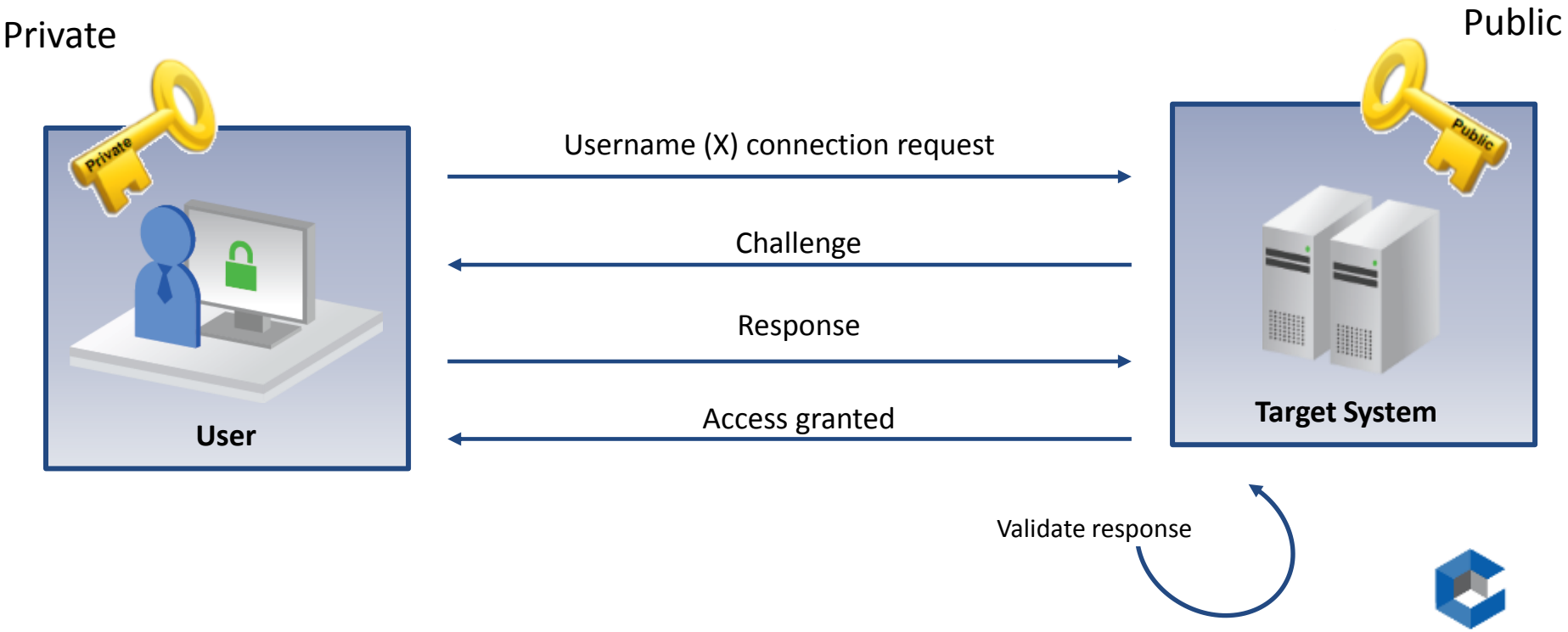
CYBERARK

SSH Key Manager

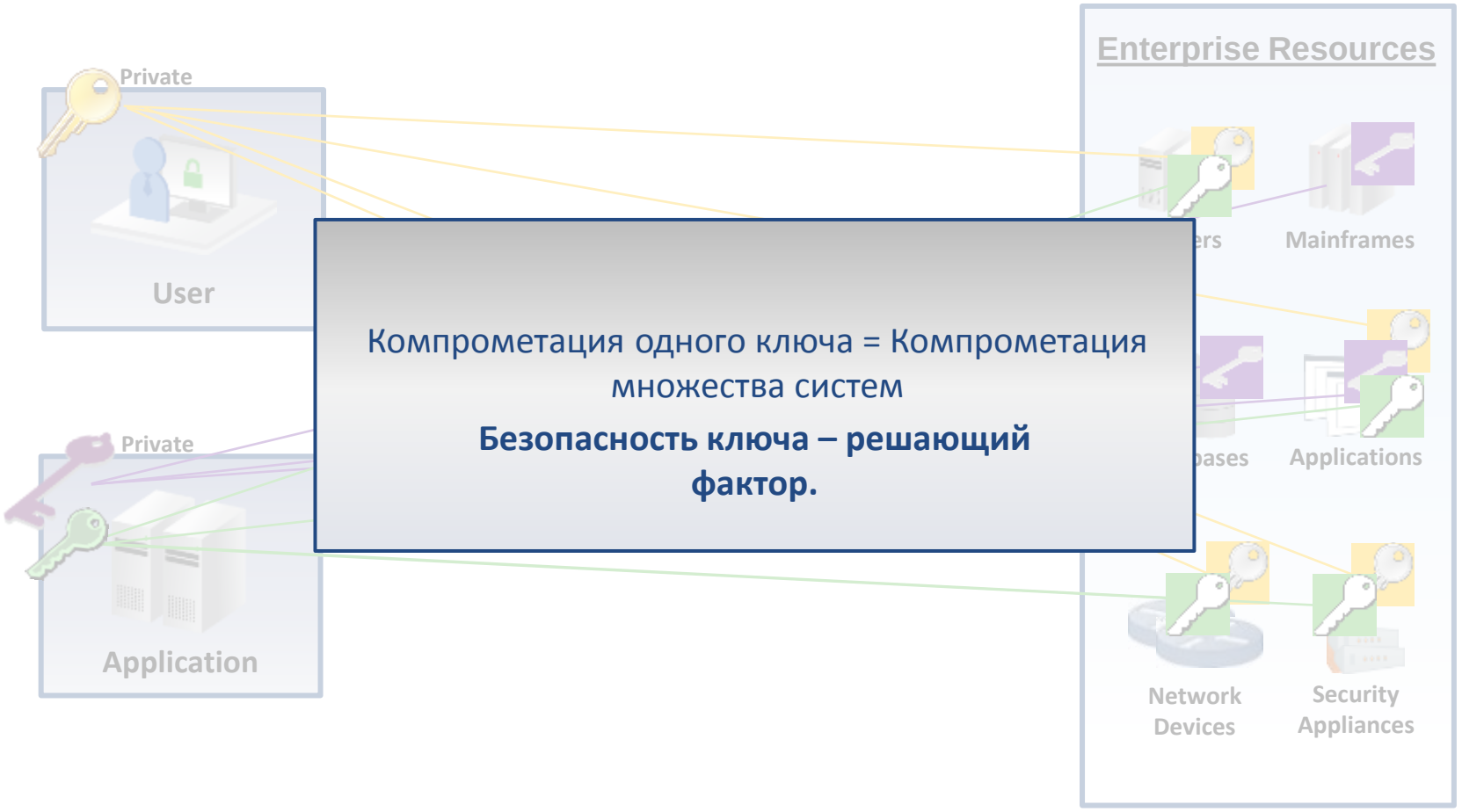
Аутентификация SSH

SSH – сетевой защищенный протокол, использует инфраструктуру открытых ключей (SSH keys):

- Шифрование сессии
- Применяется в Unix/Linux
- Альтернатива паролям
- Аутентификация машин и приложений



Ключи повсюду…



CYBERARK

Проблемы управления SSH ключами

ПРОБЛЕМЫ

Непрозрачность

Какие есть ключи и кто имеет к ним доступ?

Отсутствие контроля

Их легко создавать, но сложно отслеживать

Сложность управления

Процедура смены ключей затратная и сложная

ПОСЛЕДСТВИЯ

Риски несоответствия

Аудиторы проверять

Риски безопасности

Статичные, неуправляемые ключи приводят к успешным атакам

CYBERARK

Как CyberArk помогает решить проблемы?

ФУНКЦИИ

Обнаружение

Поиск ключей и систематизация информации о них

Управление ключами

Защита и смена ключей

Управление и наблюдение

Enforce granular access controls and monitor every SSH session

ВЫГОДЫ

Соответствие

Защита, мониторинг ключей, доступа к ним, и отчетность

Снижение рисков безопасности

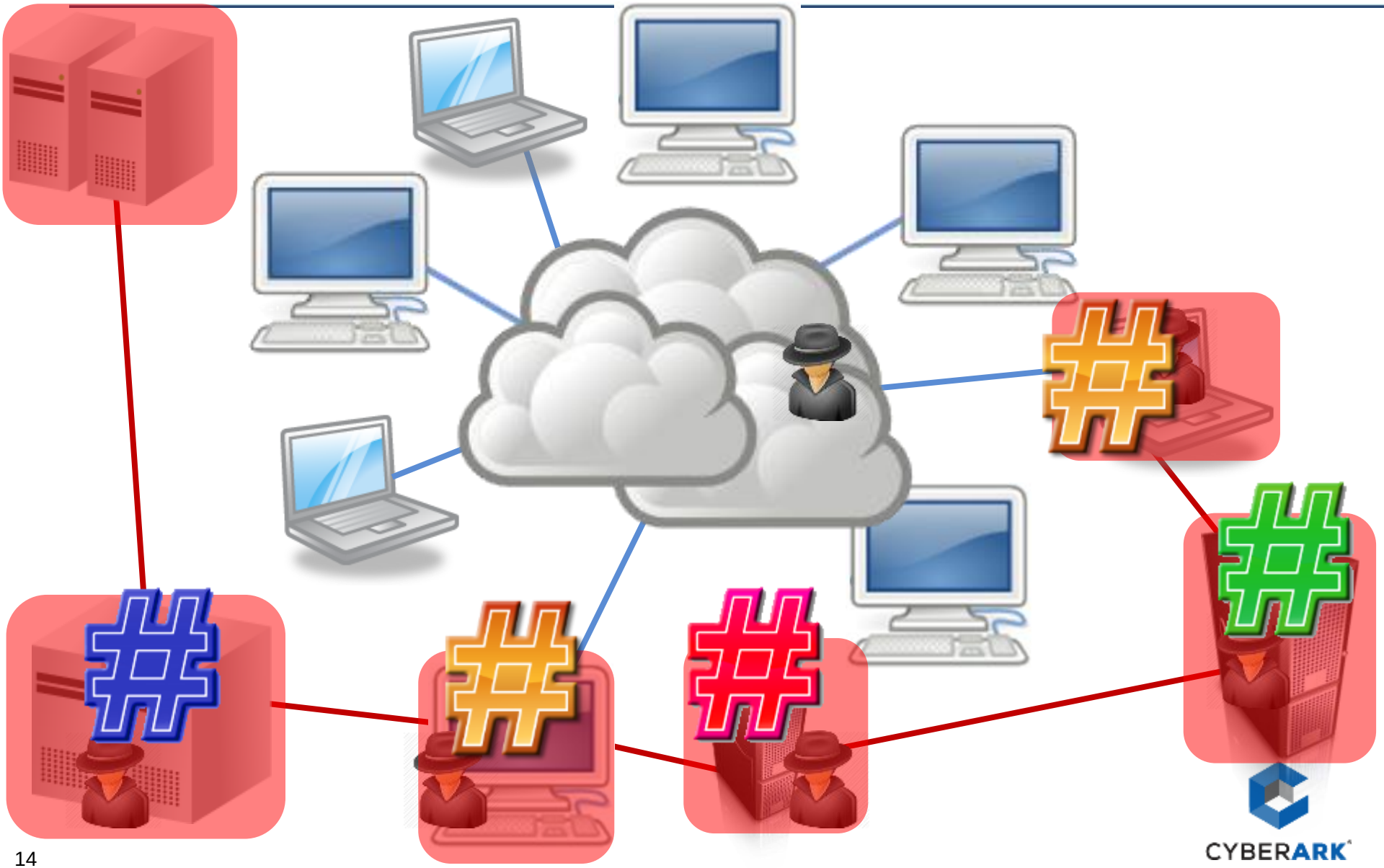
Устранение бэкдоров, повышение защищенности и определением подозрительной активности

CYBERARK

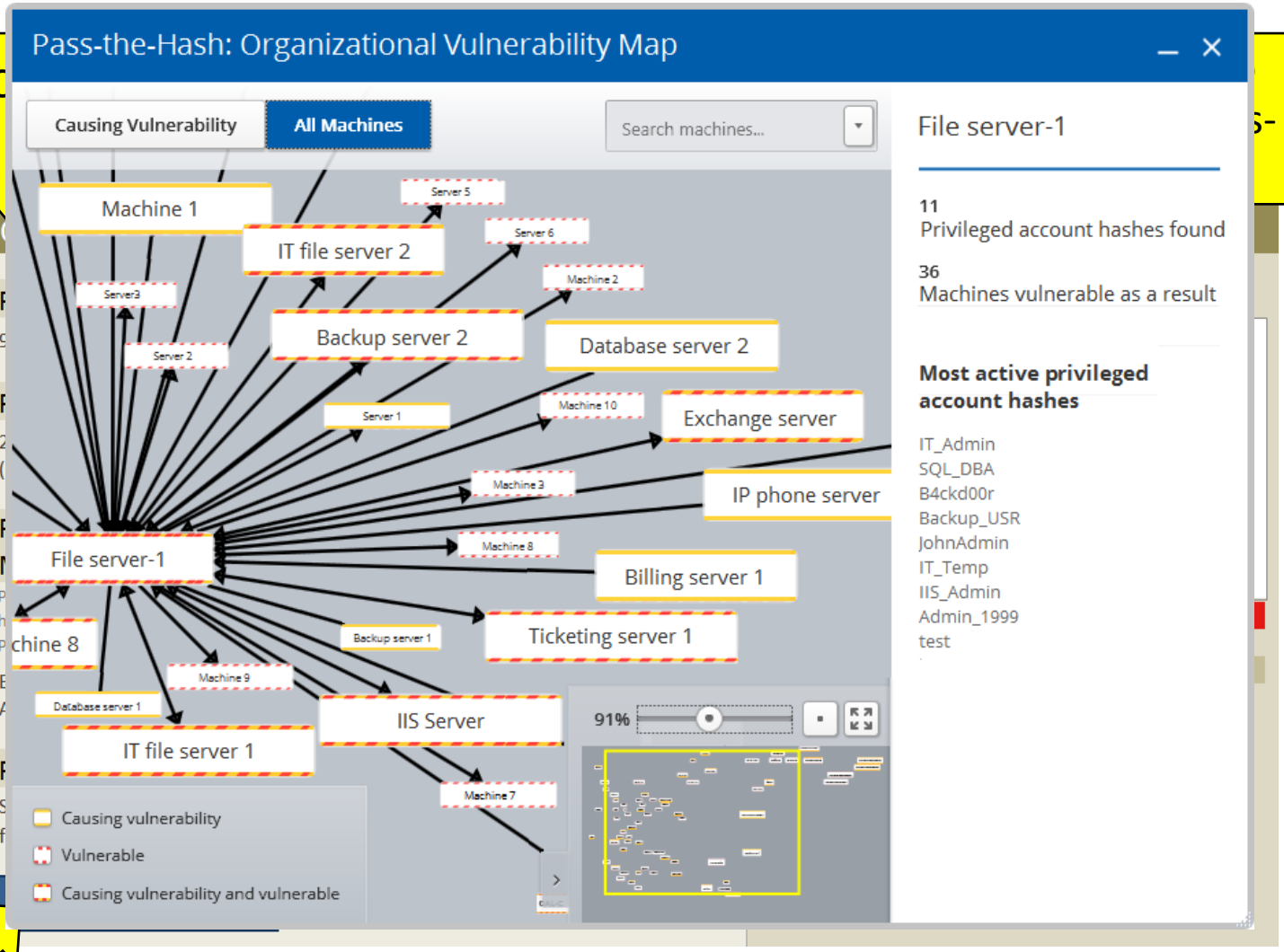
CYBERARK

Discover and Audit (DNA)

Как работает Pass-the-Hash?



DNA v5.0 – уязвимы ли Вы?



- Как может выполняться атака на мою компанию?
- Какие серверы и УЗ необходимо защитить в первую очередь?

CYBERARK

Как CyberArk может снизить риск PtH?

Применить PAS для:

Управление учетными данными

Хэши не представляют угрозы при:

OTP

Разделение об

доменных

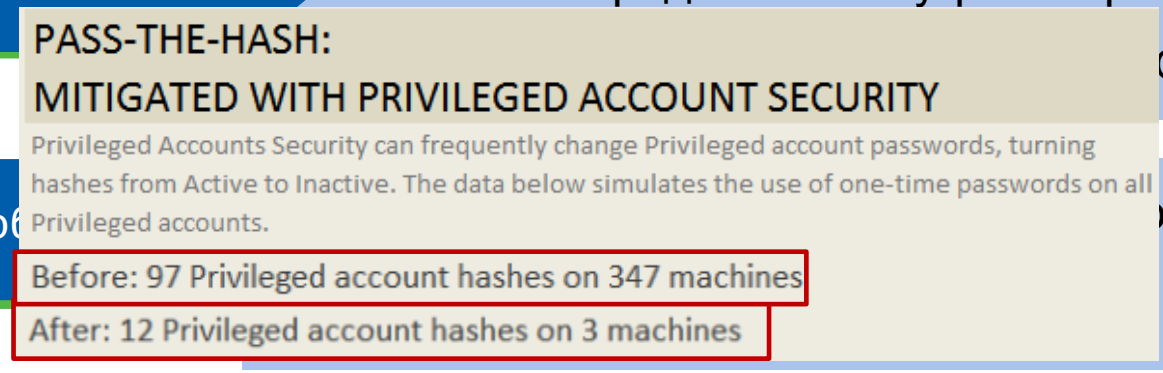
Минимальные привилегии

Применяйте стратегию минимальных привилегий (OPM)

Привилегированный SSO

PSM исключает кражу учетных данных (P-SSO)

(но не кражу хэшей!!!) – это делает EPV



CYBERARK

Как DNA v5 работает с SSH ключами?

- Обнаруживает, включая «зависшие», ключи, извлекает необходимые данные о них и сообщает статус каждого ключа.
- Коррелирует и устанавливает связей между ключами, УЗ и машинами.
- Генерирует отчет о текущем статусе ключей.
- Предоставляет карту зависимостей между ключами, УЗ и машинами.
- Формирует детальный отчет по данным карты зависимостей.

On-demand Privileges Manager (OPM)

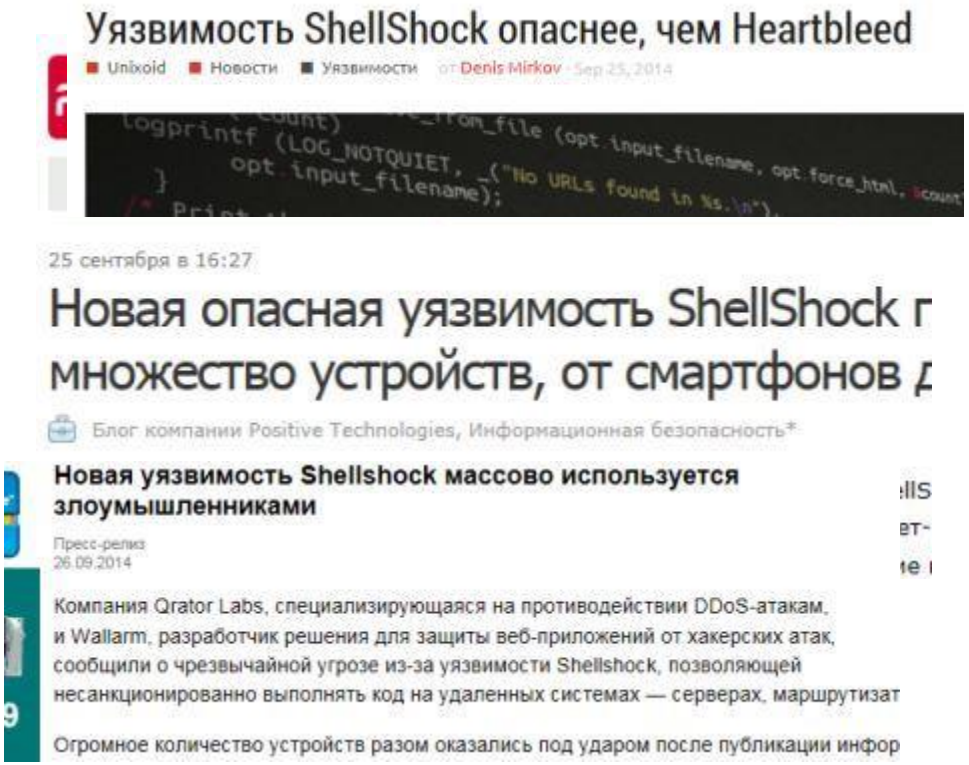
Штатные средства контроля доступа ОС

«Экономить $1,264 с Windows ПК в год, удалив права admin…»

Gartner

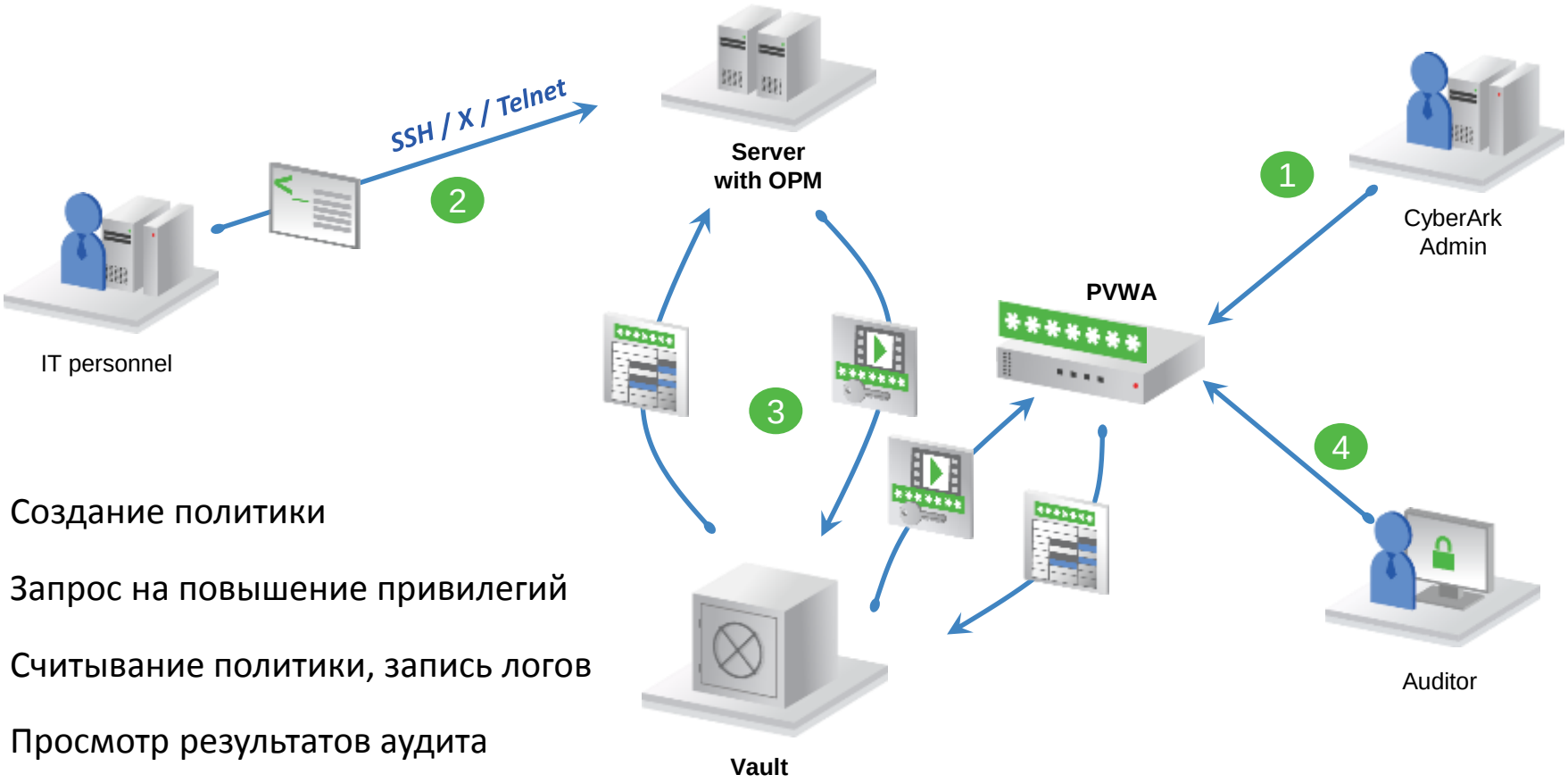
«Закрыть 92% всех уязвимостей Windows, удалив права admin…»

Microsoft



CYBERARK

Как работает OPM?



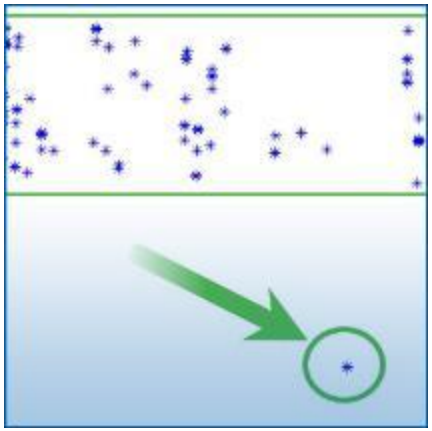
1. Создание политики
2. Запрос на повышение привилегий
3. Считывание политики, запись логов
4. Просмотр результатов аудита

CYBERARK

Privileged Threat Analytics (PTA)

Что такое PTA?

- Патентованный алгоритм изучает **поведение** привилегированных пользователей.
- Самообучение корректирует **профиль** по изменению поведения.
- Активность сравнивается с профилем поведения для выявления **аномалий**.
- Баллы угрозы присваиваются каждой аномалии, инциденту или группе событий для выявления наиболее рисковых **событий**.
- Целевые предупреждения включают детальную информацию о событиях и позволяют непосредственно реагировать на атаки через **панель управления**.
- Панель управления и уведомления по электронной почте оперативно позволяют предпринять **ответные действия**.
- Двухсторонняя **интеграция с SIEM**.



CYBERARK

Как работает PTA?

АКТИВНОСТЬ НАД УЗ

Привилегированный пользователь

Защищаемые системы

ORACLE

CyberArk Vault

SIEM

ArcSight CERTIFIED CEF COMPLIANT

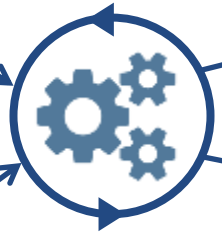
splunk>

RSA

McAfee COMPATIBLE

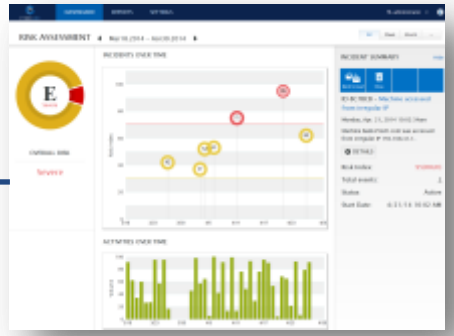
IBM

Анализ поведения



Ок

ALERT: Предупреждение SIEM & CyberArk



Анализ поведения: Статистическая модель на основе комбинации алгоритма анализа, данных Digital Vault и целевых систем и интеграции с SIEM.

CYBERARK

CYBERARK | DASHBOARD | REPORTS | SETTINGS | Hi, administrator

RISK ASSESSMENT

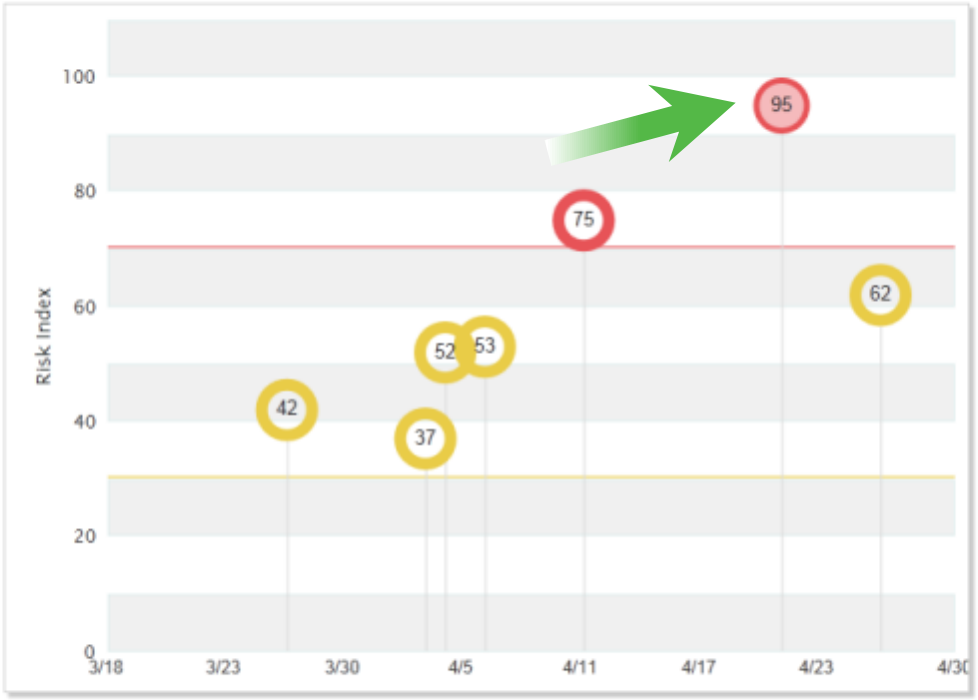
◀ Mar18.2014 – Apr30.2014 ▶

All | Week | Month | ...

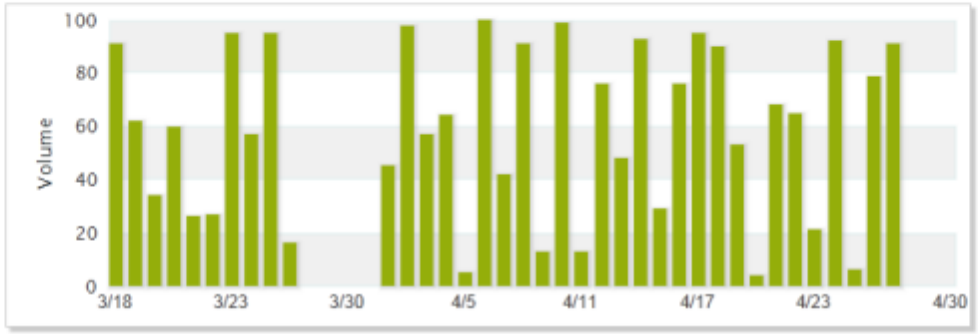
OVERALL RISK

Severe

INCIDENTS OVER TIME



ACTIVITIES OVER TIME



INCIDENT SUMMARY

Hide

Mark Unread | Close

ID 8C7BCB – Machine accessed from irregular IP

Monday, Apr. 21, 2014 10:02:34am

Machine Bank.Prod1.com was accessed from irregular IP 192.168.41.1.

DETAILS

Risk Index:	95(HIGH)
Total events:	1
Status:	Active
Start Date:	4/21/14 10:02 AM

Спасибо за внимание!