Станислав Черкасов
Ведущий специалист отдела продвижения и развития продуктов
scherkasov@ptsecurity.com

MaxPatrol SIEM: постоянно обновляемая экспертиза и противодействие новым угрозам

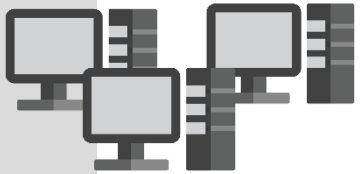
POSITIVE TECHNOLOGIES

ptsecurity.ru

О чем поговорим

POSITIVE TECHNOLOGIES

1

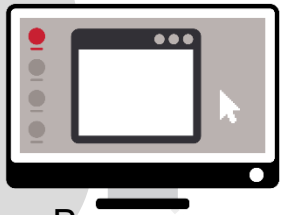


Всё те же проблемы ИБ
в 2018 году

2

Особенности
MaxPatrol SIEM

3



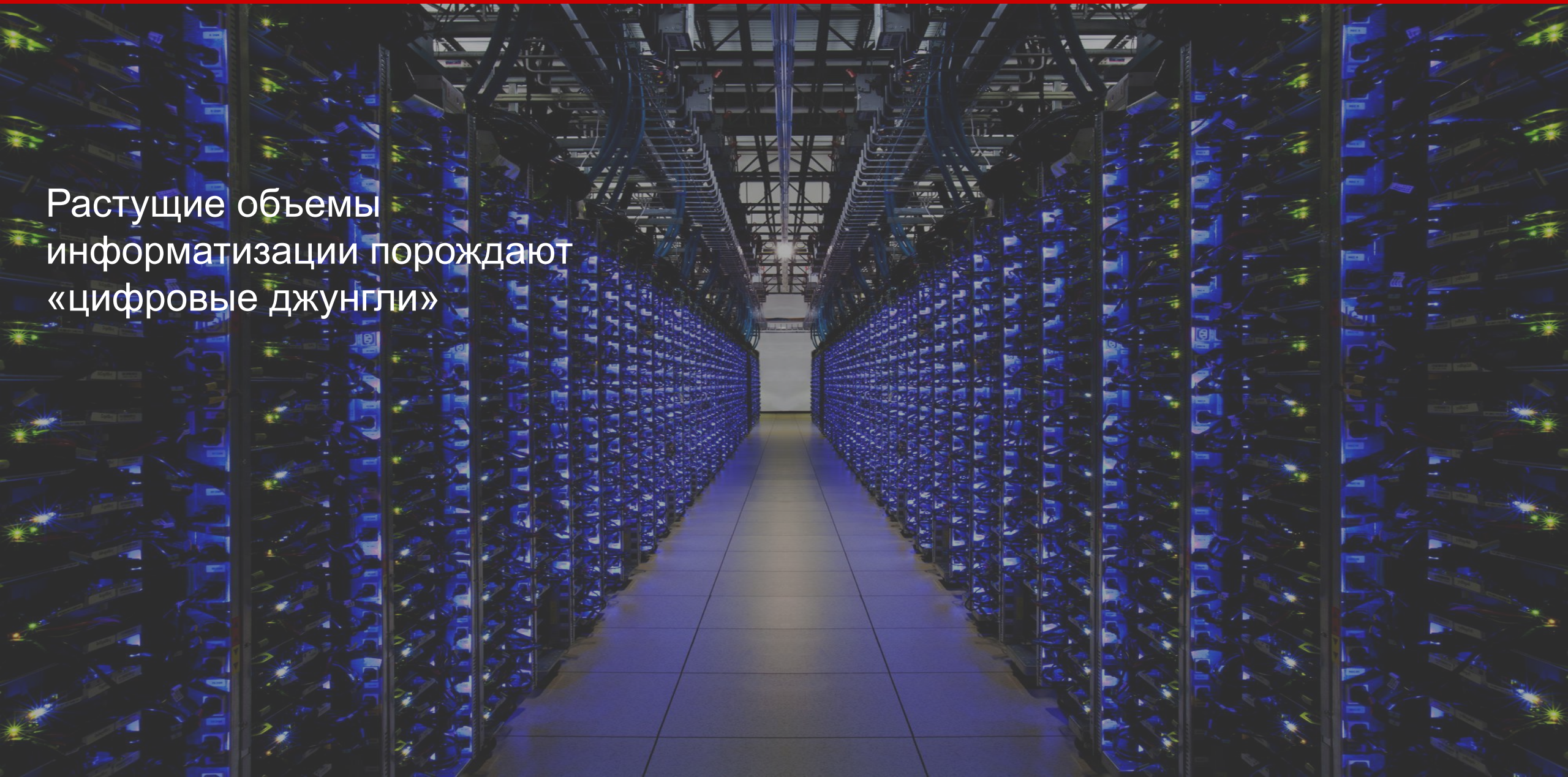
Взгляд на
компрометацию с обоих
сторон баррикад

4

Что еще нового

2018: новый год, старые проблемы

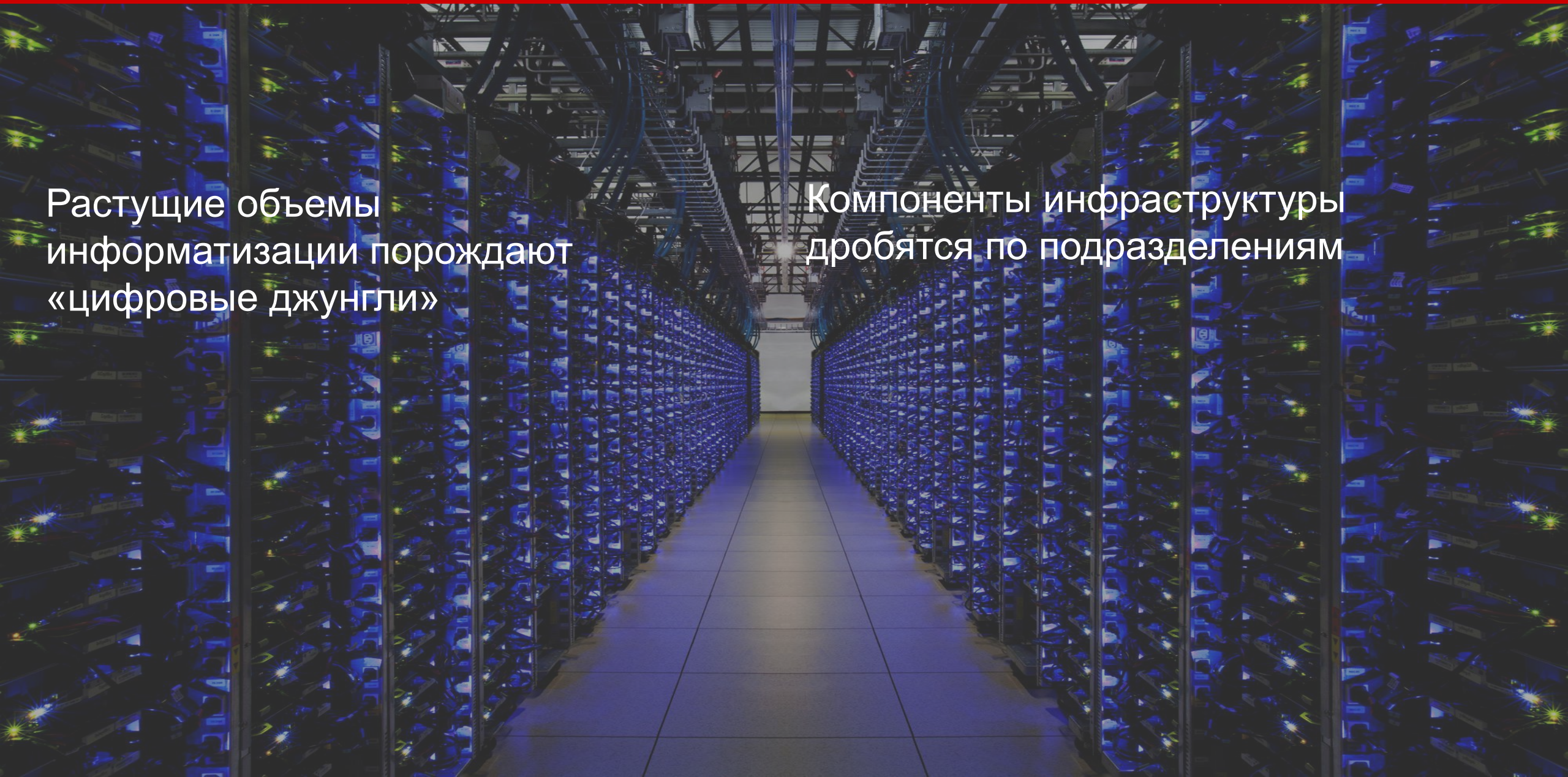
POSITIVE TECHNOLOGIES



Растущие объемы информатизации порождают «цифровые джунгли»

2018: новый год, старые проблемы

POSITIVE TECHNOLOGIES

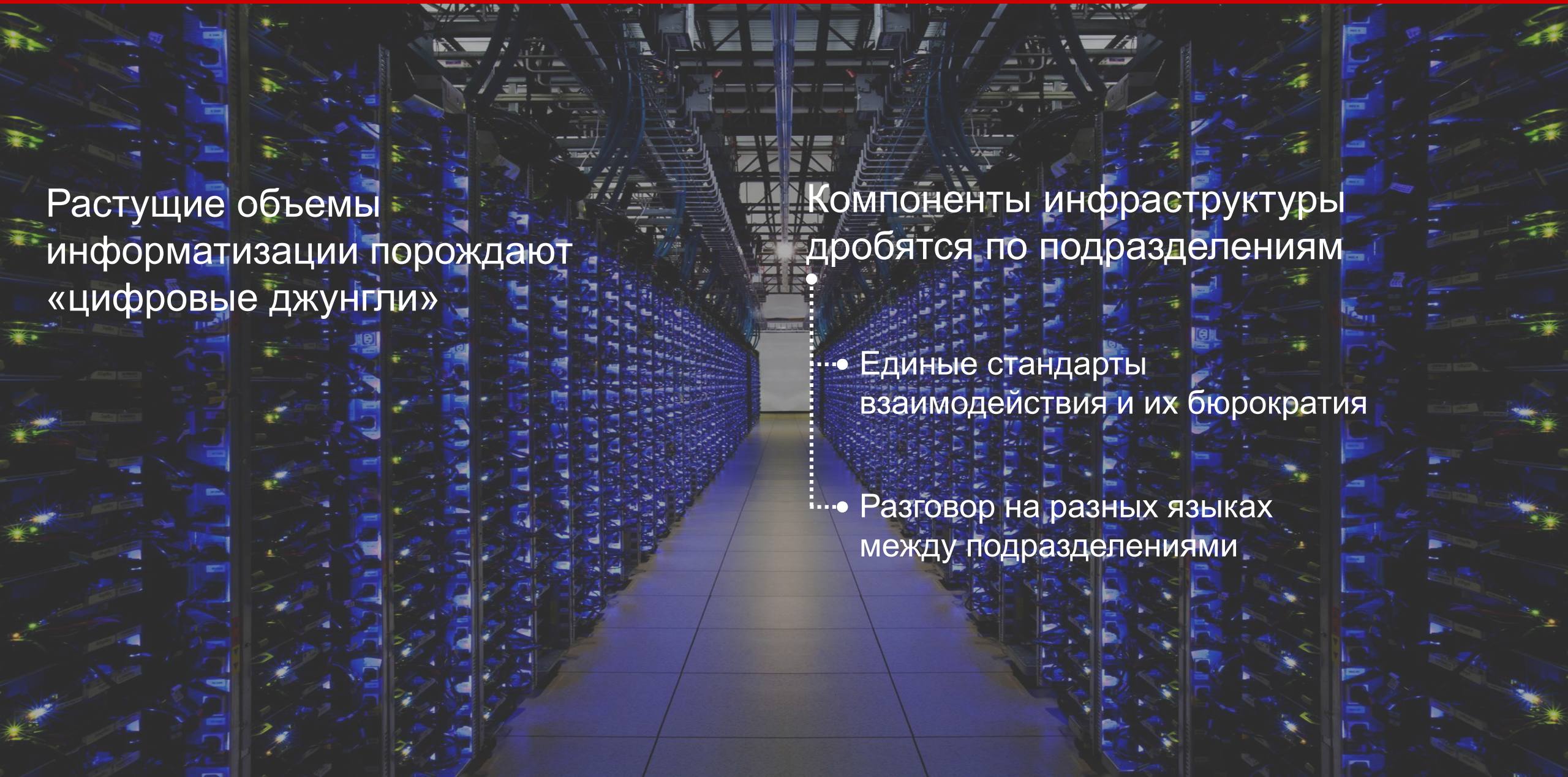


Растущие объемы информатизации порождают «цифровые джунгли»

Компоненты инфраструктуры дробятся по подразделениям

2018: Новый год, старые проблемы

POSITIVE TECHNOLOGIES



Растущие объемы информатизации порождают «цифровые джунгли»

Компоненты инфраструктуры дробятся по подразделениям

- Единые стандарты взаимодействия и их бюрократия
- Разговор на разных языках между подразделениями

Тенденции сохраняются

POSITIVE TECHNOLOGIES

3 года
среднее время присутствия злоумышленника в инфраструктуре

Источник: Кибербезопасность (2017–2018): цифры, факты, прогнозы, Positive Technologies

Тенденции сохраняются

POSITIVE TECHNOLOGIES

3 года
среднее время присутствия злоумышленника в инфраструктуре

Классические SIEM-системы:

– требуют увеличения штата высококвалифицированных сотрудников

– остаются статичными

– генерируют большое количество ложных срабатываний, рассеивая внимание

Источник: Кибербезопасность (2017–2018): цифры, факты, прогнозы, Positive Technologies

Особенности MaxPatrol SIEM

POSITIVE TECHNOLOGIES

Никаких коллекторов, коннекторов, сборщиков. Только источники, только хардкор

Особенности MaxPatrol SIEM

POSITIVE TECHNOLOGIES

Никаких коллекторов, коннекторов, сборщиков. Только источники, только хардкор

Активоцентрическая модель – работаем с событиями актива, а не с событиями с источника

Особенности MaxPatrol SIEM

POSITIVE TECHNOLOGIES

Никаких коллекторов, коннекторов, сборщиков. Только источники, только хардкор

Активоцентрическая модель – работаем с событиями актива, а не с событиями с источника

NAD Sensor: теперь не только разбор трафика, но и сигнатурный анализ вместе с хранением последних суток

Особенности MaxPatrol SIEM

POSITIVE TECHNOLOGIES

Никаких коллекторов, коннекторов, сборщиков. Только источники, только хардкор

Активоцентрическая модель – работаем с событиями актива, а не с событиями с источника

NAD Sensor: теперь не только разбор трафика, но и сигнатурный анализ вместе с хранением последних суток

Централизованный источник знаний: PT Knowledge Base

MaxPatrol SIEM: курс на автоматизацию

POSITIVE TECHNOLOGIES

Продолжаем развивать тему
гибкости в изучении ландшафта

MaxPatrol SIEM: курс на автоматизацию

POSITIVE TECHNOLOGIES

Продолжаем развивать тему гибкости в изучении ландшафта

Positive Technologies Knowledge Base (PT KB):

- Наборы правил от Экспертного центра безопасности (PT ESC)
- Централизованное распространение контента
- Автоматизированная настройка источников

MaxPatrol SIEM: курс на автоматизацию

POSITIVE TECHNOLOGIES

Продолжаем развивать тему гибкости в изучении ландшафта

Positive Technologies Knowledge Base (PT KB):

- Наборы правил от Экспертного центра безопасности (PT ESC)
- Централизованное распространение контента
- Автоматизированная настройка источников

API: возможность работы в связке со сторонним ПО

MaxPatrol SIEM: курс на автоматизацию

POSITIVE TECHNOLOGIES

Продолжаем развивать тему гибкости в изучении ландшафта

Positive Technologies Knowledge Base (PT KB):

- Наборы правил от Экспертного центра безопасности (PT ESC)
- Централизованное распространение контента
- Автоматизированная настройка источников

API: возможность работы в связке со сторонним ПО

Стремление к идеалу: не ментор, а помощник

Герой дня без галстука: PT Knowledge Base

POSITIVE TECHNOLOGIES

Реструктуризация и перенос всей подкапотной информации в единую точку

Регулярные обновления: не реже 1 раза в 2 месяца

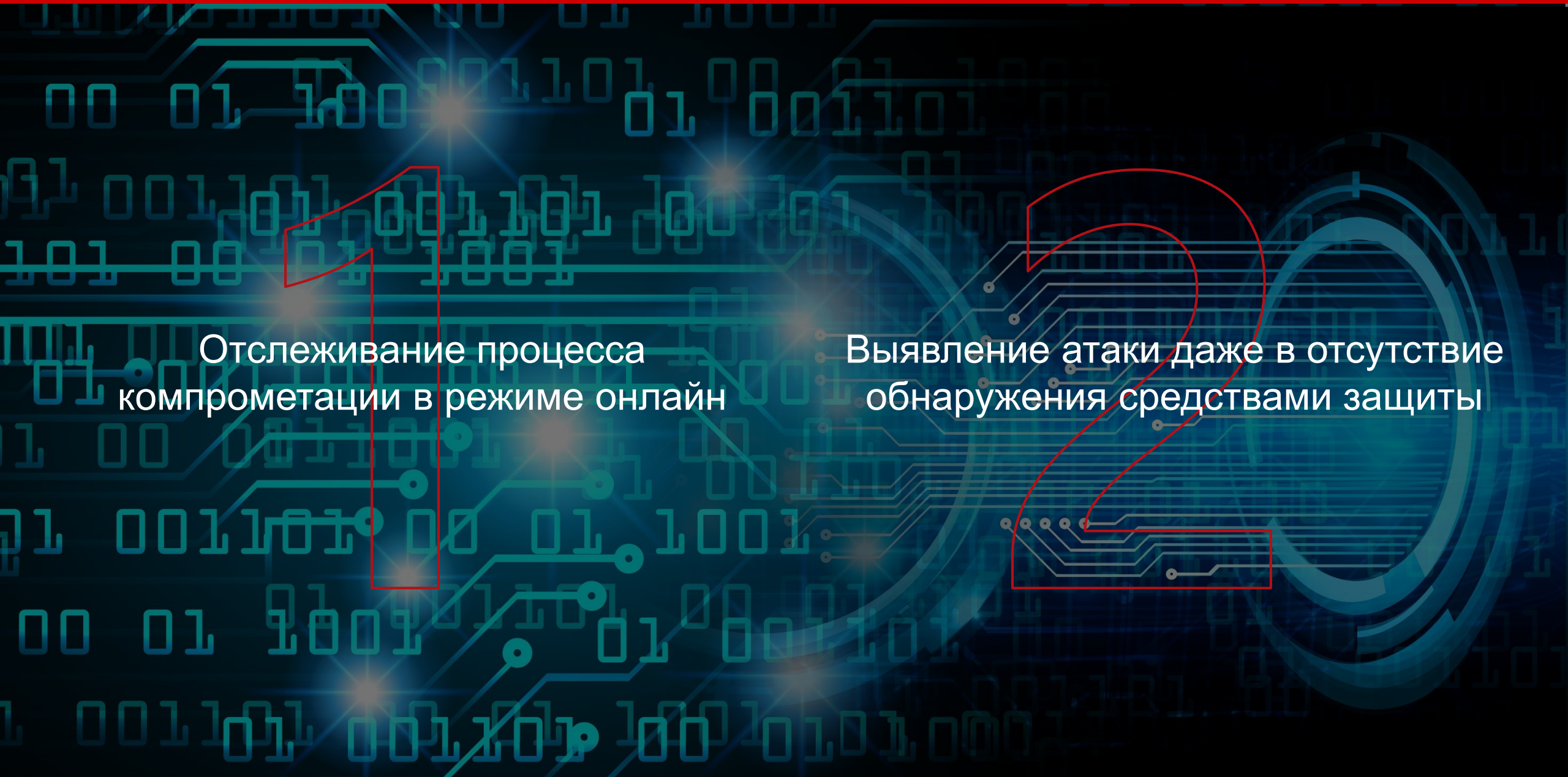
Пакеты экспертизы

Табличные списки из коробки для борьбы с ложными срабатываниями

Автоматизация настройки аудита на источнике

PT Knowledge Base IRL: от громких слов к делу

POSITIVE TECHNOLOGIES



1

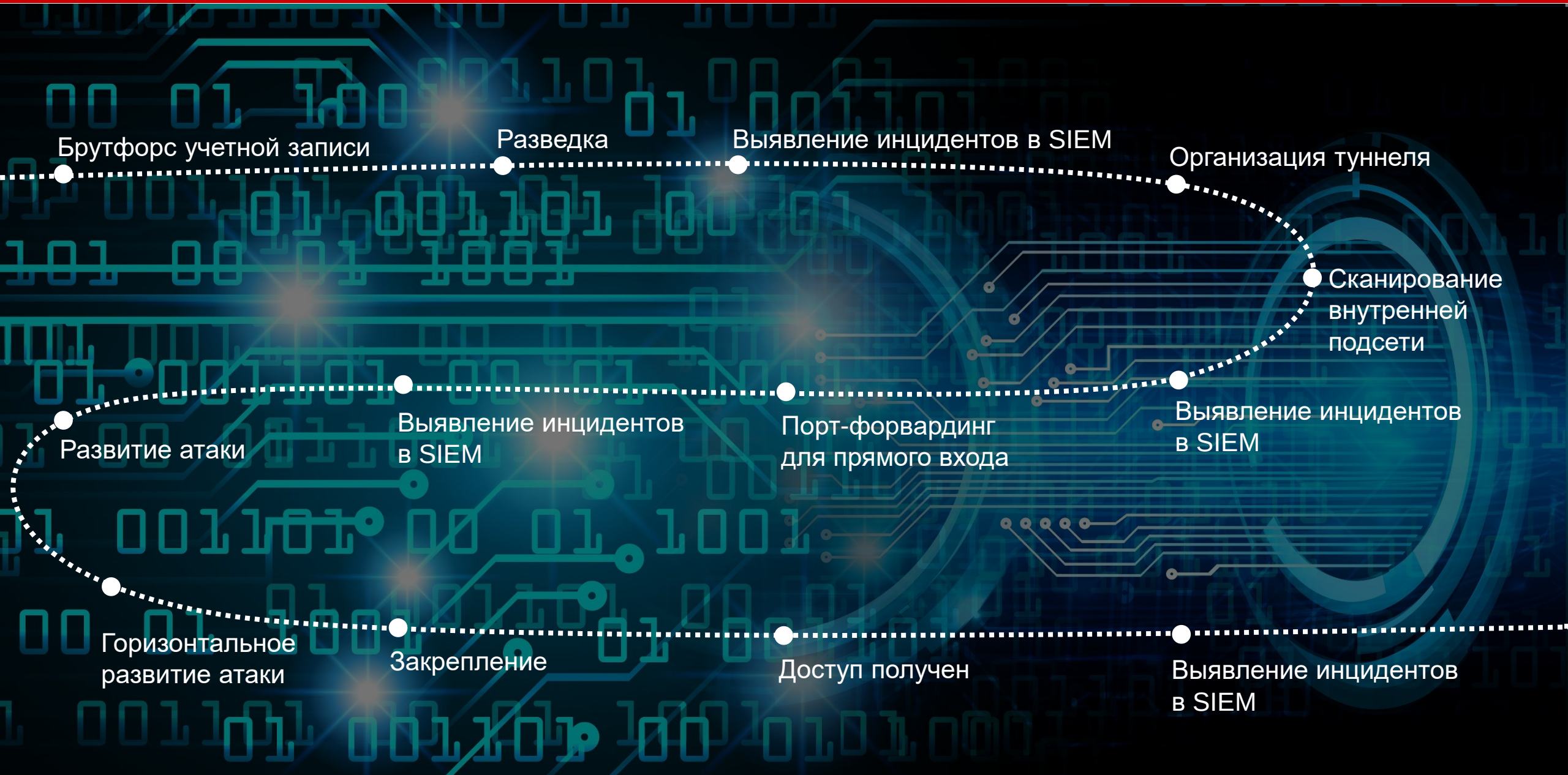
Отслеживание процесса компрометации в режиме онлайн

2

Выявление атаки даже в отсутствие обнаружения средствами защиты

Kill Chain - цепочка атаки

POSITIVE TECHNOLOGIES



MaxPatrol SIEM: новые кандидаты в ключевые фичи

POSITIVE TECHNOLOGIES

Мониторинг источников. Не «просто мониторинг»:

1

Обнаружение и своевременное реагирование на **недоступность источника**

MaxPatrol SIEM: новые кандидаты в ключевые фичи

POSITIVE TECHNOLOGIES

Мониторинг источников. Не «просто мониторинг»:

1

Обнаружение и своевременное реагирование на **недоступность источника**

2

Возможность **отслеживать аномалии** в распределении потока событий с источников

MaxPatrol SIEM: новые кандидаты в ключевые фичи

POSITIVE TECHNOLOGIES

Мониторинг источников. Не «просто мониторинг»:

1

Обнаружение и своевременное реагирование на **недоступность источника**

2

Возможность **отслеживать аномалии** в распределении потока событий с источников

3

Гибкая система **настройки мониторинга** в зависимости от типичной активности
ночью меньше событий, чем днем и т.д.

Мониторинг источников

MaxPatrol SIEM: новые кандидаты в ключевые фичи

POSITIVE TECHNOLOGIES

Расширенный фильтр по активам (грид активов)

1

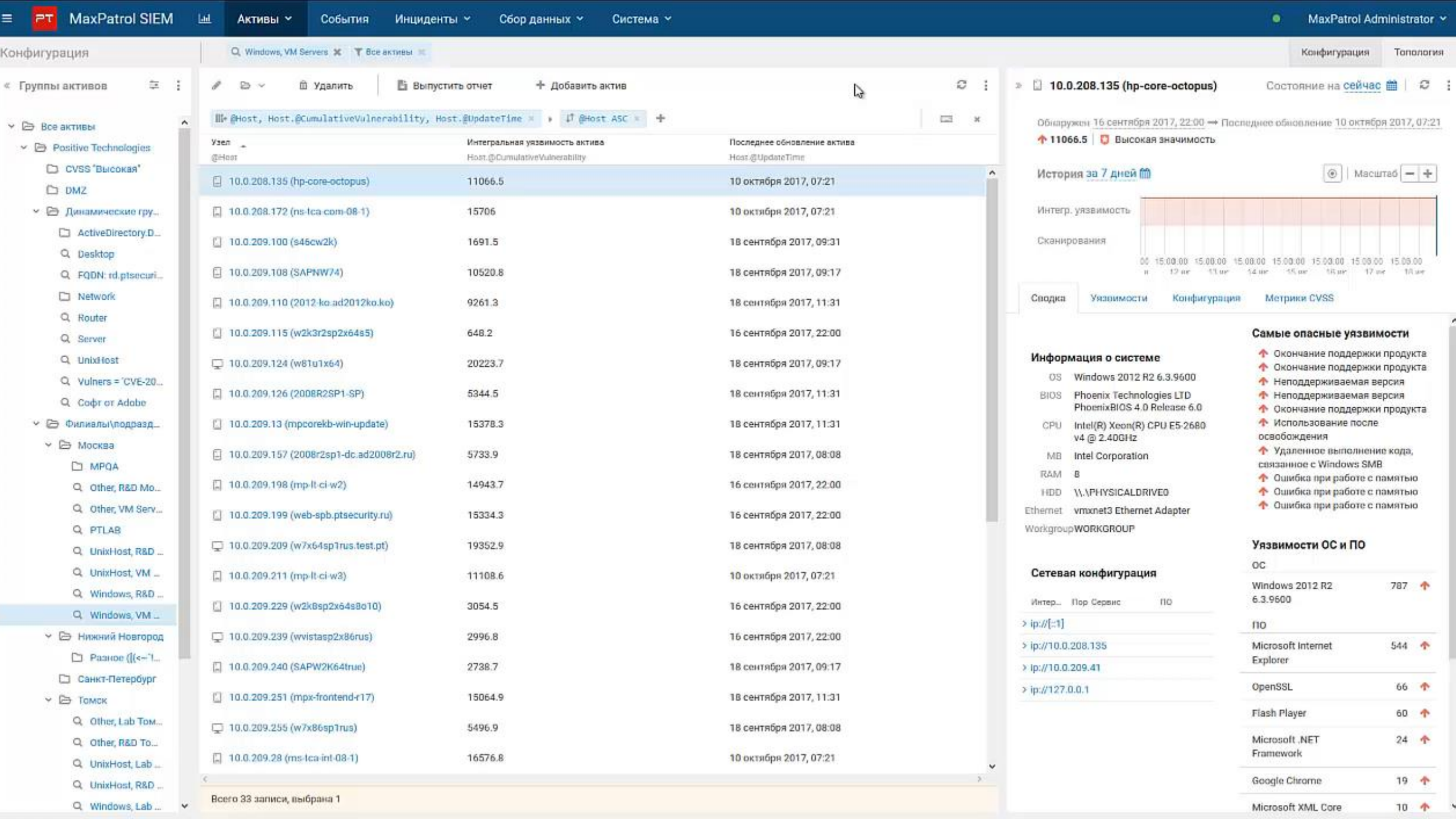
Выявление учетных записей на активах

2

Выявление нежелательных процессов

3

Оперативное устранение уязвимостей


MaxPatrol SIEM
Активы
События
Инциденты
Сбор данных
Система
MaxPatrol Administrator
Конфигурация
Windows, VM Servers
Все активы
Конфигурация
Топология
Группы активов
Все активы
Positive Technologies
CVSS "Высокая"
DMZ
Динамические гру...
ActiveDirectory.D...
Desktop
FQDN: rd.ptsecuri...
Network
Router
Server
Unixhost
Vulners = 'CVE-20...
Софт от Adobe
Филиалы\подразд...
Москва
MPQA
Other, R&D Mo...
Other, VM Serv...
PTLAB
UnixHost, R&D ...
UnixHost, VM ...
Windows, R&D ...
Windows, VM ...
Нижний Новгород
Разное ([(<-"!...
Санкт-Петербург
Томск
Other, Lab Том...
Other, R&D To...
UnixHost, Lab ...
UnixHost, R&D ...
Windows, Lab ...
Удалить
Выпустить отчет
Добавить актив
@Host, Host.@CumulativeVulnerability, Host.@UpdateTime
@Host ASC
Узел
@Host
Интегральная уязвимость актива
Host.@CumulativeVulnerability
Последнее обновление актива
Host.@UpdateTime
10.0.208.135 (hp-core-octopus) 11066.5 10 октября 2017, 07:21
10.0.208.172 (ns-lca-com-08-1) 15706 10 октября 2017, 07:21
10.0.209.100 (s45cw2k) 1691.5 18 сентября 2017, 09:31
10.0.209.108 (SAPNW74) 10520.8 18 сентября 2017, 09:17
10.0.209.110 (2012-ko.ad2012ko.ko) 9261.3 18 сентября 2017, 11:31
10.0.209.115 (w2k3r2sp2x64s5) 648.2 16 сентября 2017, 22:00
10.0.209.124 (w81u1x64) 20223.7 18 сентября 2017, 09:17
10.0.209.126 (2008R2SP1-SP) 5344.5 18 сентября 2017, 11:31
10.0.209.13 (mpcorekb-win-update) 15378.3 18 сентября 2017, 11:31
10.0.209.157 (2008r2sp1-dc.ad2008r2.ru) 5733.9 18 сентября 2017, 08:08
10.0.209.198 (mp-lt-ci-w2) 14943.7 16 сентября 2017, 22:00
10.0.209.199 (web-spb.ptsecurity.ru) 15334.3 16 сентября 2017, 22:00
10.0.209.209 (w7x64sp1rus.test.pt) 19352.9 18 сентября 2017, 08:08
10.0.209.211 (mp-lt-ci-w3) 11108.6 10 октября 2017, 07:21
10.0.209.229 (w2k8sp2x64s8o10) 3054.5 16 сентября 2017, 22:00
10.0.209.239 (wvistasp2x86rus) 2996.8 16 сентября 2017, 22:00
10.0.209.240 (SAPW2K64true) 2738.7 18 сентября 2017, 09:17
10.0.209.251 (mpx-frontend-r17) 15064.9 18 сентября 2017, 11:31
10.0.209.255 (w7x86sp1rus) 5496.9 18 сентября 2017, 08:08
10.0.209.28 (ms-lca-int-08-1) 16576.8 10 октября 2017, 07:21
Всего 33 записи, выбрана 1
10.0.208.135 (hp-core-octopus)
Состояние на сейчас
Обнаружен 16 сентября 2017, 22:00 → Последнее обновление 10 октября 2017, 07:21
11066.5
Высокая значимость
История за 7 дней
Масштаб
Интегр. уязвимость
Сканирования
Сводка
Уязвимости
Конфигурация
Метрики CVSS
Информация о системе
OS Windows 2012 R2 6.3.9600
BIOS Phoenix Technologies LTD PhoenixBIOS 4.0 Release 6.0
CPU Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz
MB Intel Corporation
RAM 8
HDD \\.\PHYSICALDRIVE0
Ethernet vmxnet3 Ethernet Adapter
Workgroup WORKGROUP
Сетевая конфигурация
Интер... Пор Сервис ПО
ip://[::1]
ip://10.0.208.135
ip://10.0.209.41
ip://127.0.0.1
Самые опасные уязвимости
Окончание поддержки продукта
Окончание поддержки продукта
Неподдерживаемая версия
Неподдерживаемая версия
Окончание поддержки продукта
Использование после освобождения
Удаленное выполнение кода, связанное с Windows SMB
Ошибка при работе с памятью
Ошибка при работе с памятью
Ошибка при работе с памятью
Уязвимости ОС и ПО
ОС
Windows 2012 R2 6.3.9600 787
ПО
Microsoft Internet Explorer 544
OpenSSL 66
Flash Player 60
Microsoft .NET Framework 24
Google Chrome 19
Microsoft XML Core 10

И на десерт

POSITIVE TECHNOLOGIES

- Стабильность под высокими нагрузками

Flow Control

Динамические табличные списки

Виджеты из группировок событий

Уведомления об изменении состава динамических групп

Инсталлятор 2.0

до
35
тысяч
EPS

И на десерт

POSITIVE TECHNOLOGIES

Стабильность под высокими нагрузками

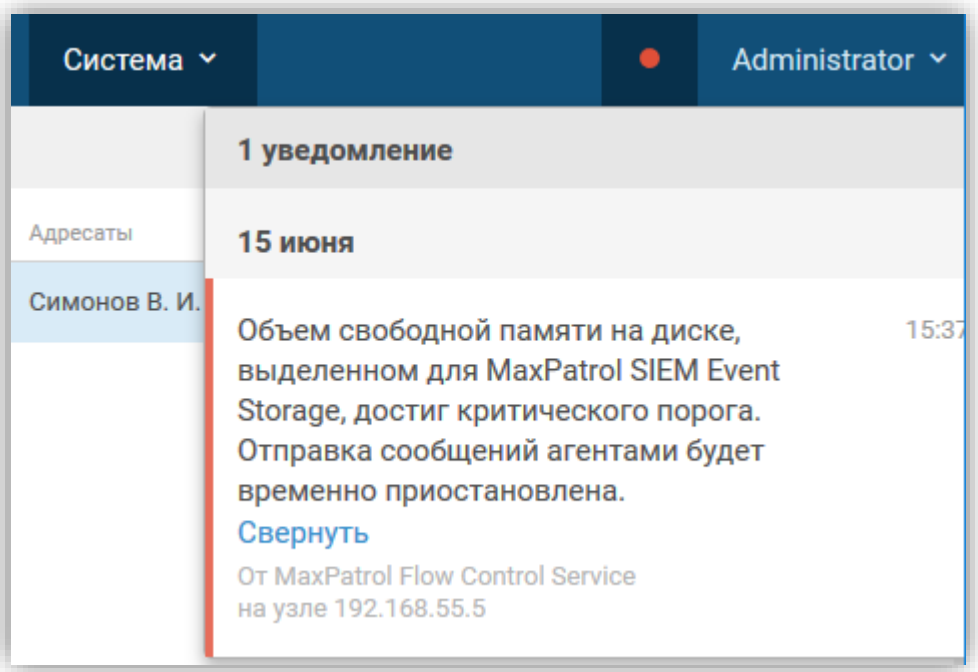
Flow Control

Динамические табличные списки

Виджеты из группировок событий

Уведомления об изменении состава динамических групп

Инсталлятор 2.0



И на десерт

POSITIVE TECHNOLOGIES

Стабильность под высокими нагрузками

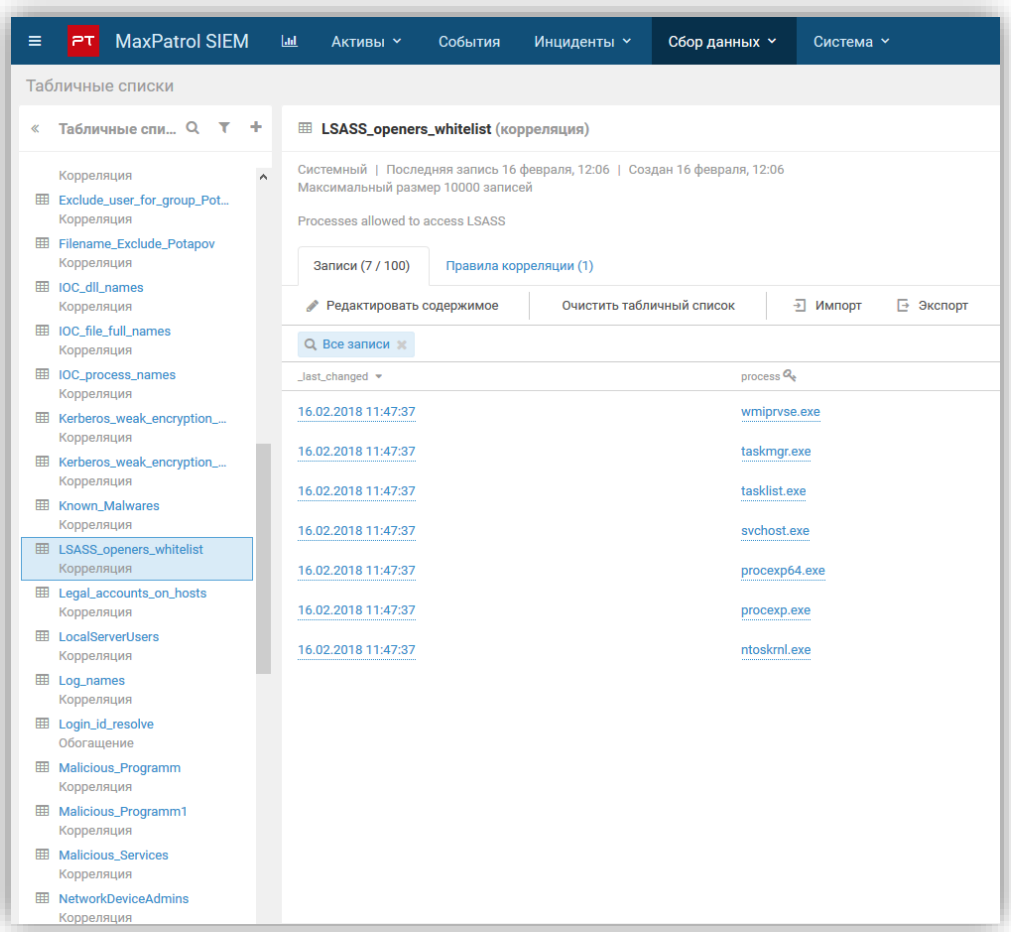
Flow Control

- Динамические табличные списки

Виджеты из группировок событий

Уведомления об изменении состава динамических групп

Инсталлятор 2.0



И на десерт

POSITIVE TECHNOLOGIES

Стабильность под высокими нагрузками

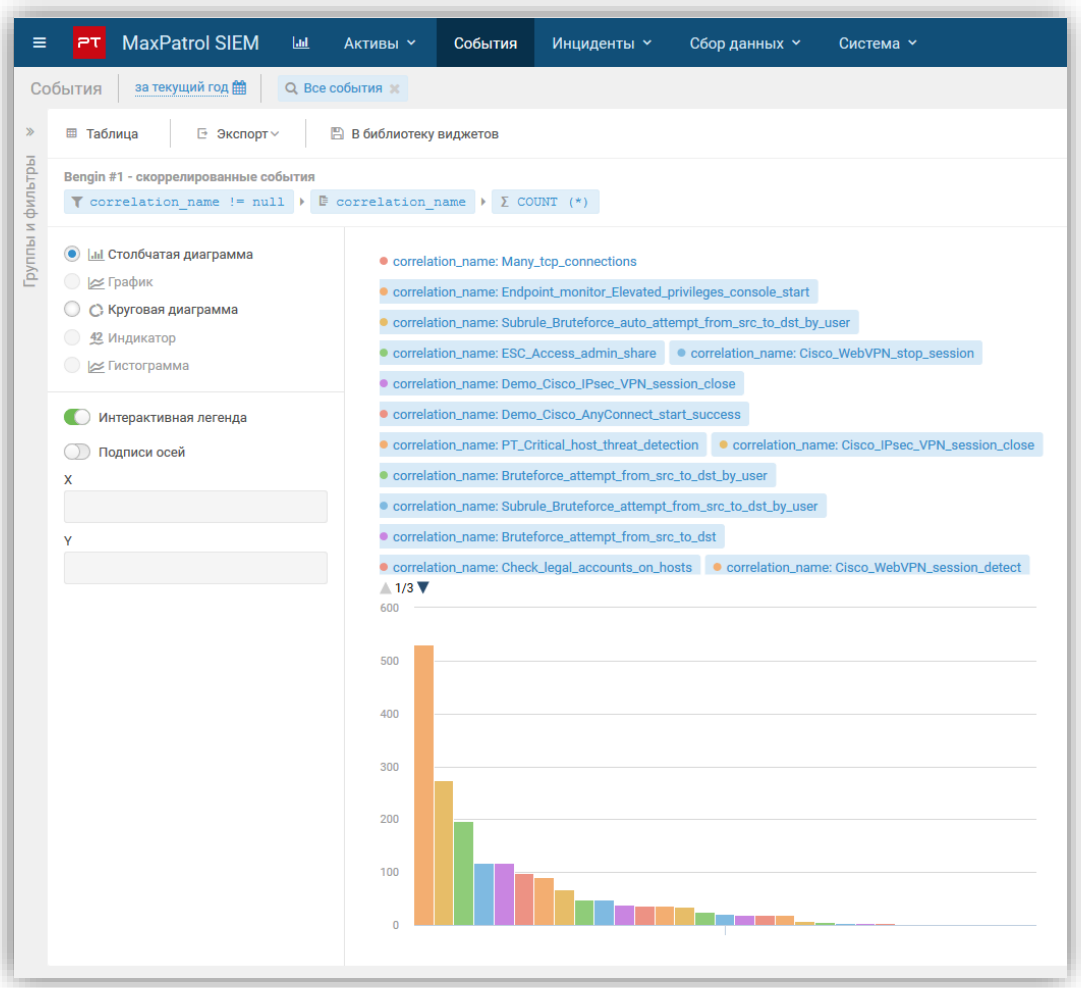
Flow Control

Динамические табличные списки

Виджеты из группировок событий

Уведомления об изменении состава динамических групп

Инсталлятор 2.0



И на десерт

POSITIVE TECHNOLOGIES

Стабильность под высокими нагрузками

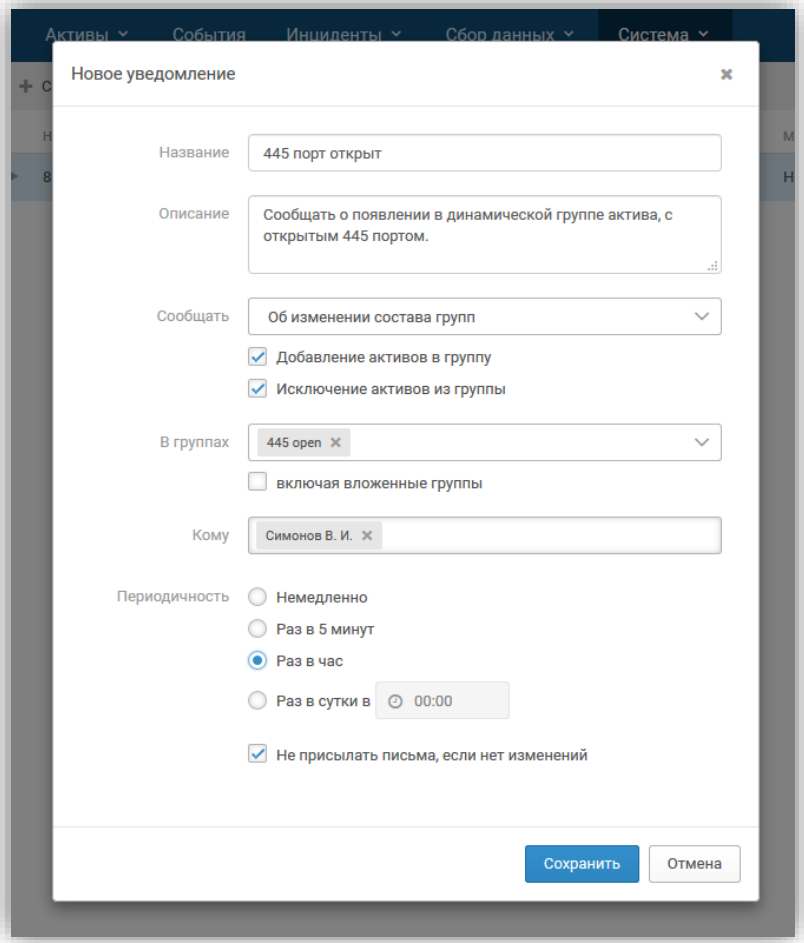
Flow Control

Динамические табличные списки

Виджеты из группировок событий

- Уведомления об изменении состава динамических групп

Инсталлятор 2.0



И на десерт

POSITIVE TECHNOLOGIES

Стабильность под высокими нагрузками

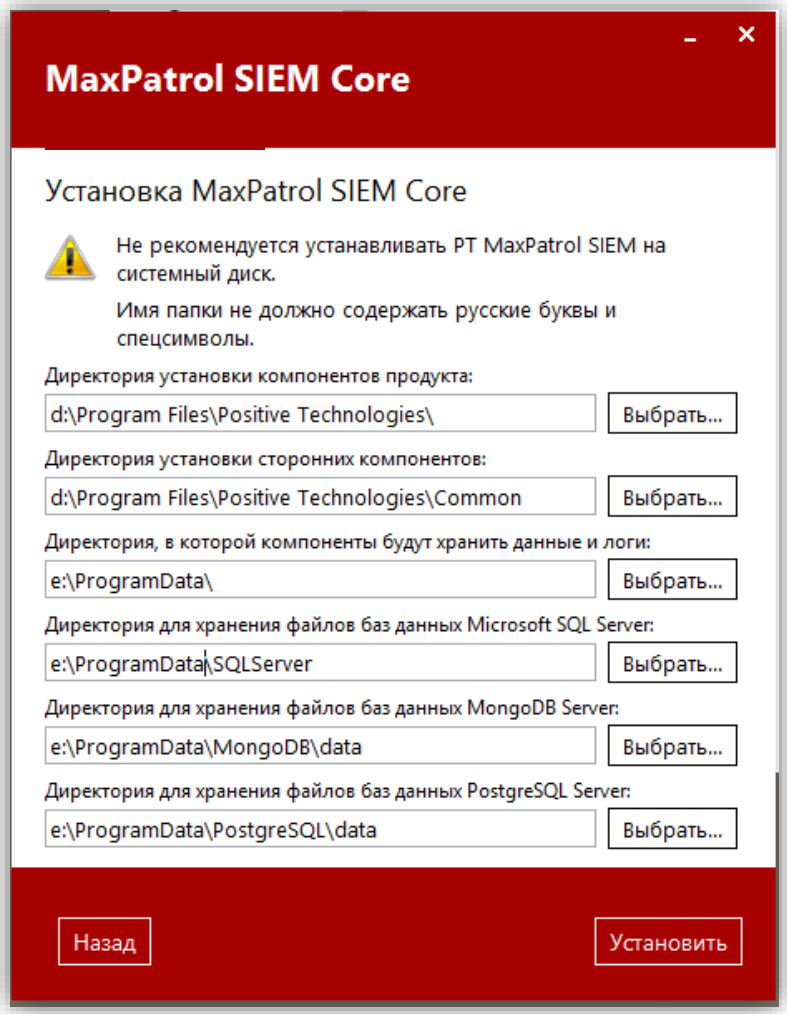
Flow Control

Динамические табличные списки

Виджеты из группировок событий

Уведомления об изменении состава динамических групп

Инсталлятор 2.0




Спасибо!
POSITIVE TECHNOLOGIES
ptsecurity.ru