



POSITIVE
TECHNOLOGIES

MaxPatrol SIEM + MaxPatrol VM

Что дает синергия двух продуктов

ptsecurity.com



Анастасия Зуева
Менеджер по маркетингу
MaxPatrol VM



Сергей Сухоруков
Технический менеджер
отдела развития продуктов



Что в основе?

ptsecurity.com

MaxPatrol 10

MaxPatrol 10 объединяет продукты Positive Technologies, обеспечивает полную прозрачность сети и мониторинга безопасности.

Все продукты в составе MaxPatrol 10:

- работают на основе единых актуальных знаний об IT-инфраструктуре
- учитывают изменения в IT-инфраструктуре
- могут взаимообогащать друг друга информацией об активах сети



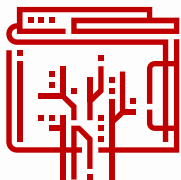
MaxPatrol 10

SECURITY ASSET MANAGEMENT

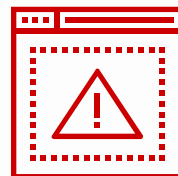
- Сбор полной информации об инфраструктуре
- Автоматическое определение активов, непрерывная актуализация данных, учет изменений

ОСНОВА

Управляем активами. Зачем?



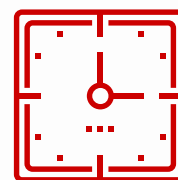
Переходим от IP-адресов к IT-активам, учитываем изменения в инфраструктуре



Приоритизируем активы с учетом их уровня значимости



Автоматизируем работу с активами: задаем статические и динамические группы



Регулярно актуализируем данные об инфраструктуре и храним историю изменений

MaxPatrol 10

MAXPATROL SIEM

ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ ИБ В РЕАЛЬНОМ ВРЕМЕНИ

- Сбор и анализ событий
- Выявление актуальных атак
- Расследование сложных инцидентов

MAXPATROL VM

ПОСТРОЕНИЕ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ, РЕЗУЛЬТАТЫ КОТОРОГО ВИДНЫ

- Обнаружение и приоритизация уязвимостей
- Настройка политик сканирования и устранения уязвимостей
- Контроль защищенности

SECURITY ASSET MANAGEMENT

- Сбор полной информации об инфраструктуре
- Автоматическое определение активов, непрерывная актуализация данных, учет изменений

ВОЗМОЖНОСТИ

ОСНОВА

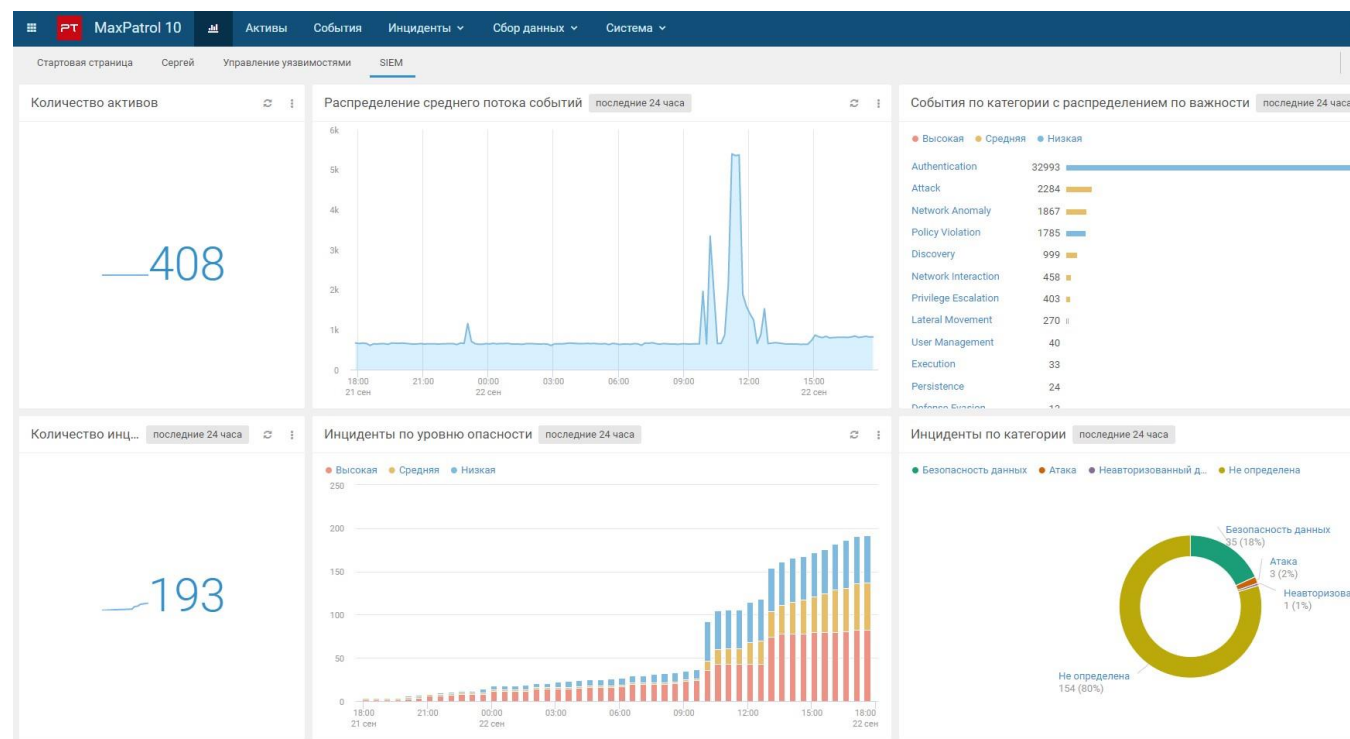
MaxPatrol SIEM



MaxPatrol SIEM — система выявления инцидентов с уникальным подходом к обеспечению прозрачности IT-инфраструктуры и глубокой экспертизой в обнаружении угроз.

Система точно детектирует инциденты за счет:

- регулярного получения экспертных знаний о способах детектирования актуальных видов атак
- полной видимости инфраструктуры
- адаптации к изменениям в ней.

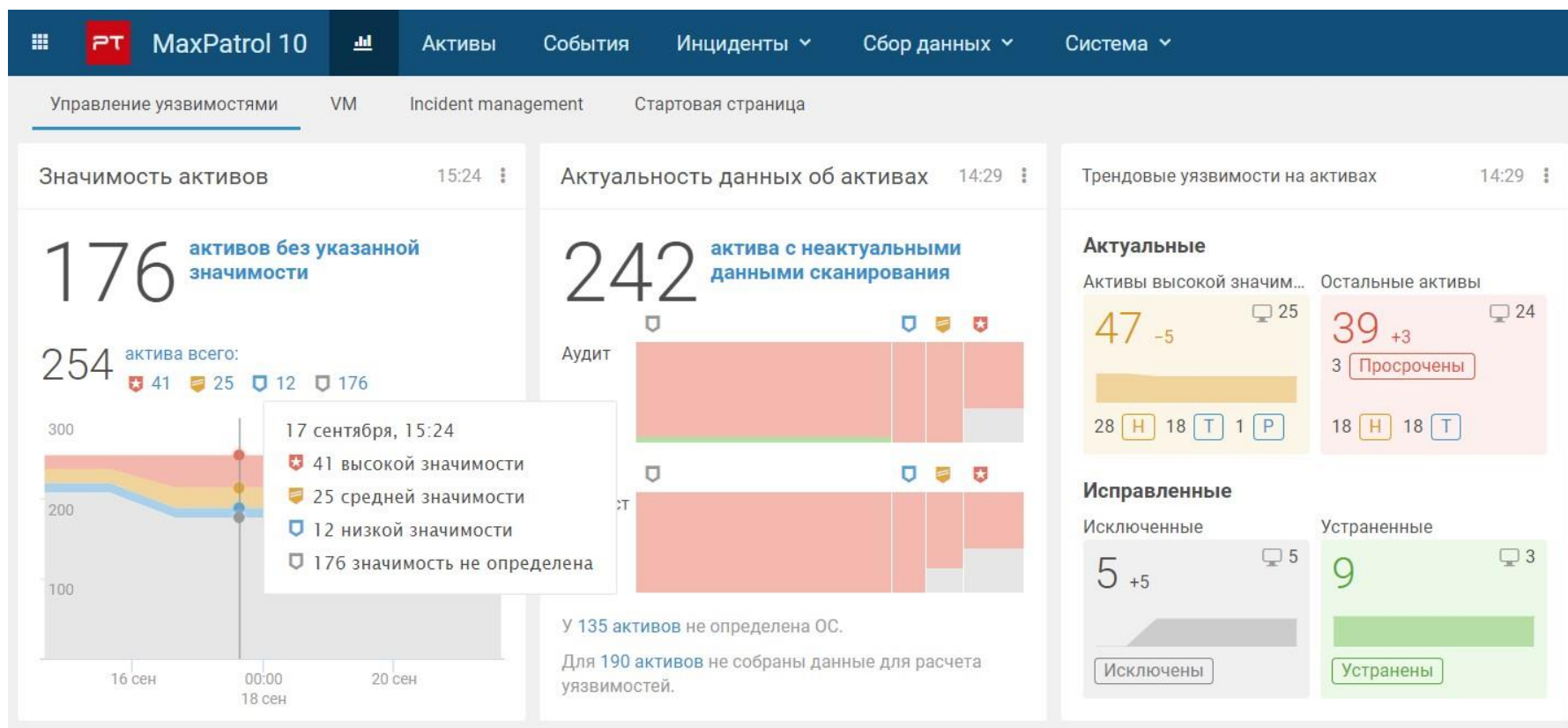


В тройке лидеров российского рынка SIEM согласно исследованию компании IDC

MAXPATROL VM



Система нового поколения для управления уязвимостями



Решение, которое поможет построить **полноценный процесс** управления уязвимостями и сделать реализацию конкретных рисков компании слишком **дорогой и сложной** для злоумышленника.

MaxPatrol 10

Сочетание двух сделает уровень безопасности еще выше: события можно коррелировать с уязвимостями и оперативно на них реагировать.

PT

В ПАКЕТАХ ЭКСПЕРТИЗЫ:

- Правила выявления атак
- Рекомендации по реагированию
- Обновления параметров сбора и обработки событий ИБ

В БАЗЕ ЗНАНИЙ:

- Правила расчета уязвимостей
- Трендовые уязвимости
- Рекомендации по устранению выявленных уязвимостей

ЭКСПЕРТИЗА РТ

MAXPATROL SIEM

ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ ИБ В РЕАЛЬНОМ ВРЕМЕНИ

- Сбор и анализ событий
- Выявление актуальных атак
- Расследование сложных инцидентов

MAXPATROL VM

ПОСТРОЕНИЕ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ, РЕЗУЛЬТАТЫ КОТОРОГО ВИДНЫ

- Обнаружение и приоритизация уязвимостей
- Настройка политик сканирования и устранения уязвимостей
- Контроль защищенности

ВОЗМОЖНОСТИ

SECURITY ASSET MANAGEMENT

- Сбор полной информации об инфраструктуре
- Автоматическое определение активов, непрерывная актуализация данных, учет изменений

ОСНОВА

Платформа MaxPatrol

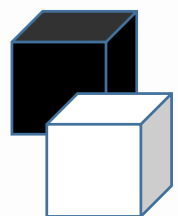


Positive
Technologies
Expertise

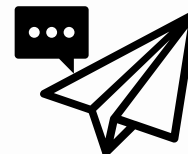


■ Asset Management

Синергия рождается из активов



СКАНИРОВАНИЕ

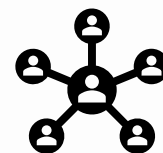


СОБЫТИЕ

АКТИВ

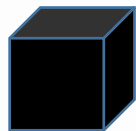


API / СИСТЕМЫ IT /
РУЧНОЙ ВВОД

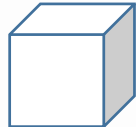


СЕТЕВОЙ
ТРАФИК

Как узнать все об активах



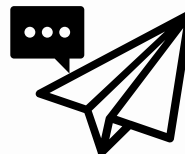
- Host Discovery
- * Discovery
- * Pentest



- Windows Updates Discovery
- * Audit



- AD
- SCCM
- VmWare vCenter



- DHCP servers
- DNS servers
- Checkpoint, Cisco
- Kaspersky Security Center
- и другие



- PT NAD

Поиграем в игру: «MaxPatrol 10, покажи мне ...»

PT

Кейс №1:



... живые активы, которые могут участвовать в инцидентах и **потребуют дополнительного времени** на сбор данных

Запрос: **Хосты созданные и регулярно обновляемые из событий с известной ОС**

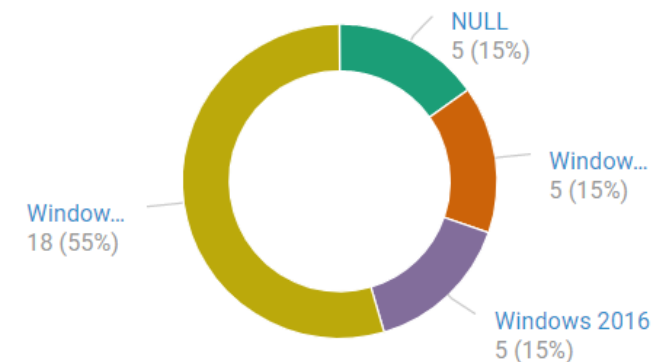
```
select(@Host, Host.OsName, Host.@CreationTime, Host.@UpdateTime, host.@PentestTime, Host.@AuditTime) | filter(host.@PentestTime = null and Host.@AuditTime = null) | filter(Host.@UpdateTime >= Now() - 1day) | group(Host.OsName, COUNT(*))
```

▶ **Выполнить** Ctrl+Enter

Операционная система Host.OsName	COUNT(*)	Узел @Host	Операционная система Host.OsName	Дата и время создания... Host.@CreationTime	Дата и время последне... Host.@UpdateTime	Дата и время последне... host.@PentestTime	Дата и время последне... Host.@AuditTime
null	5	rdg1.external.pl...	Windows 2016	20 июля, 12:35	Вчера, в 23:23	null	null
Windows 10	5	rdg2.external.pl...	Windows 2016	20 июля, 12:36	Вчера, в 23:23	null	null
Windows 2016	5	wsus.external.p...	Windows 2016	20 июля, 12:35	Вчера, в 23:23	null	null
Windows 7	18	mim.bf.plat.form	Windows 2016	20 июля, 12:50	Сегодня, в 3:13	null	null
		10.125.3.2	null	27 июля, 14:49	Вчера, в 10:04	null	null
		eboldyrev.plat...	Windows 7	20 июля, 05:55	Сегодня, в 0:26	null	null

Хосты созданные и регулярно обновляемые из событий с известной ОС 03:31

● NULL ● Windows 10 ● Windows 2016
● Windows 7



Поиграем в игру: «MaxPatrol 10, покажи мне ...»

PT

Кейс №2:



... живые уязвимые активы которые не помогут мне приоритизировать инциденты в соответствии с их значимостью

+ Добавить актив ▾ 📄 Выпустить отчет 📊 Создать табличный список

Запрос: **Хосты без заданной значимости с проведенным аудитом (есть ОС и уязвимости) ***

```
filter(Host.@Importance = 'ND') | select(@Host, host.OsName, Host.@Vulners, host.@Vulners.CVEs, Host.@UpdateTime, host.@AuditTime, host.@PentestTime, host.@DeviceType) | filter(host.OsName) | group(host.@DeviceType, COUNT(*))
```

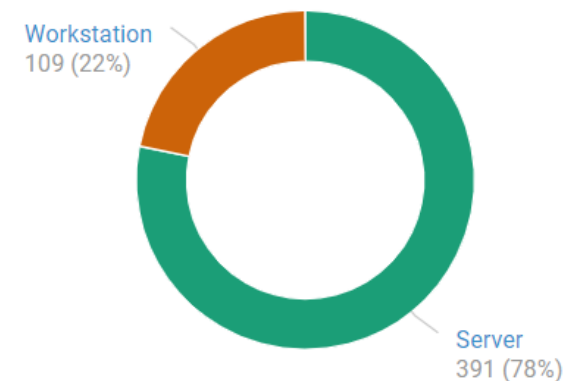
▶ Выполнить Ctrl+Enter

Тип устройства host.@DeviceType	COUNT(*)	Узел @Host	Операционная с... host.OsName	Уязвимость Host.@Vulners	CVE-идентификато... host.@Vulners.CVEs	Дата и время посл... Host.@UpdateTime	Дата и время посл... host.@AuditTime	Дата и время посл... host.@PentestTime	Тип устройства host.@DeviceType
Server	391	10.125.253.100	Ubuntu	Бюллетень г	CVE-2021-26691	16 сентября, 05:02	null	26 июля, 13:52	Server
Workstation	109	10.125.253.100	Ubuntu	Проблема с	CVE-2020-1927	16 сентября, 05:02	null	26 июля, 13:52	Server
		10.125.253.100	Ubuntu	Бюллетень г	CVE-2021-30641	16 сентября, 05:02	null	26 июля, 13:52	Server
		10.125.253.100	Ubuntu	Использова	CVE-2020-1934	16 сентября, 05:02	null	26 июля, 13:52	Server
		10.125.253.100	Ubuntu	Бюллетень г	CVE-2019-17567	16 сентября, 05:02	null	26 июля, 13:52	Server
		10.158.3.30	Debian	Утечка инфо	CVE-2020-15666	14 сентября, 20:22	null	26 июля, 14:06	Workstation
		10.158.3.30	Debian	Обход огран	CVE-2020-26953	14 сентября, 20:22	null	26 июля, 14:06	Workstation
		10.158.3.30	Debian	Проблема с	CVE-2020-26976	14 сентября, 20:22	null	26 июля, 14:06	Workstation
		10.158.3.30	Debian	Обход огран	CVE-2020-15648	14 сентября, 20:22	null	26 июля, 14:06	Workstation
		10.158.3.30	Debian	Поврежден	CVE-2020-15673	14 сентября, 20:22	null	26 июля, 14:06	Workstation

Хосты без заданной значимости с проведенным аудитом (есть ОС и...

04:09

● Server ● Workstation



Поиграем в игру: «MaxPatrol 10, помоги мне ...»

PT

Кейс №3:



... создание инцидентов с проверкой наличия уязвимостей на хосте и приоритизацией с учетом значимости актива

8,8

Обход механизма защиты | [CVE-2016-6662](#)

Изменить статус

Отметить как важную

Изменить метки

Обнаружена 23 сентября, 12:51

Основная информация

Опасность

Высокий уровень

Эксплойт

Нет

Удаленная эксплуатация

Да

Статус

Новая

Устранение

Нет политики

Актив

db-test-2.plat.form (10.1.1.3)

»

23.09.2021 12:54:03

Узел ssukhorukov-nb обнаружил эксплуатацию уязвимости EternalBlue на узле ip: 10.1.1.3 mac: 00:50:56:B6:2B:49

Роли во взаимодействии

Объект

object

alert

object.name

CVE-2016-6662

object.id

7365b4c6-562e-45f3-9e8b-c3fa1b28882a

object.property

TIAS recommendations

object.value

Провести аудит используемого ПО, наличие пос

object.type

Сетевой

object.state

Не обработан

Поиграем в игру: «MaxPatrol 10, помоги мне ...»

PT

Кейс №3:



... создание инцидентов с проверкой наличия уязвимостей на хосте и приоритизацией с учетом значимости актива

Vulnerabilities_on_hosts (данные об активах) [Открыть в Knowledge Base](#)

Последняя запись: Сегодня, в 7:56
Создан: Сегодня, в 7:51
Группы (со вложенными): Все активы
Запрос: select(@Host as host, host.@Vulnerabilities.CVEs as cve, Host.@Vulnerabilities as VulnerabilitiesName, host.@Importance as importance)

Записи (21375) Правила корреляции (1)

Экспорт

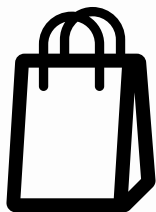
_last_changed	host	cve	vulnerabilitiesname	importance
23.09.2021 07:56:05	scom.rf.plat.form (10.125.135.33)	CVE-2021-24091	Удаленное выполнение кода	Н
23.09.2021 07:56:05	DC01.plat.form (10.125.120.3)	CVE-2019-1064	Повышение привилегий	Н
23.09.2021 07:56:05	DC01.plat.form (10.125.120.3)	CVE-2020-1038	Отказ в обслуживании	Н
23.09.2021 07:56:05	DC01.plat.form (10.125.120.3)	CVE-2021-24103	Повышение привилегий	Н
23.09.2021 07:56:05	plat-DC01-2.plat.form (10.125.120.4)	CVE-2020-1336	Повышение привилегий	Н
23.09.2021 07:56:05	ZGoncharova.plat.form (10.125.123.4)	CVE-2020-0961	Удаленное выполнение кода	Н

Правило корреляции Exploit_On_Vulner_Host

```
1 query VulnerHost($host, $cve) from Vulnerabilities_on_hosts {  
2   host == $host  
3   and cve == $cve  
4 }  
5  
6 event ExploitOnVulnerHost:  
7   key:  
8     dst.ip  
9   filter {  
10    (  
11      event_src.category == "IDS/IPS" or  
12      event_src.category == "Firewall" or  
13      event_src.category == "Network Security"  
14    )  
15  }
```

Пакет экспертизы работающий с уязвимостями на активах

>> **Усиление синергии**



- Новые правила корреляции
- Переосмысление и рефакторинг наработанного контента
- Расширение экспертизы в других продуктах Positive Technologies



POSITIVE
TECHNOLOGIES

Портал техподдержки:
support.ptsecurity.com

Отдел продаж:
sales@ptsecurity.com

Telegram-канал о новостях продуктов Positive Technologies:
t.me/ptproductupdate

Задать вопрос о функционале MaxPatrol 10:
t.me/MPSIEMChat