



Кто такой false positive, и как перестать его бояться

Антон Исаев

Эксперт отдела мониторинга событий ИБ

Станислав Черкасов

Менеджер по продвижению продуктов

План вебинара. Часть 1



1. Что такое false positive и почему он есть.
2. Теория борьбы с ложными срабатываниями.
3. Нововведение MaxPatrol SIEM 6.0 – отбраковка «фолзов» из интерфейса.
4. Видео-сценарий 1.1: добавление исключения в интерфейсе MP SIEM 6.0.
5. Видео-сценарий 1.2: работа с табличными списками в MP SIEM 6.0.
6. Ответы на вопросы, разъяснение технической части.

План вебинара. Часть 2



1. Описания пакетов экспертизы – ваш союзник для борьбы с FP.
2. Переход к практической части: как вносить исключения самому.
3. Сценарий 2.1: работа в конструкторе правил корреляции.
4. Сценарий 2.2: работа в коде правила корреляции.
5. Бонус!

«Фолзы» – бич SIEM-систем



- Любая SIEM-система «из коробки» будет генерировать ложные срабатывания.
- Откладывание в долгий ящик работы с ложными срабатываниями ведет к быстрой деградации проекта.
- Если соотношение ложных срабатываний к актуальным инцидентам выше 75% – SIEM-систему можно считать небоеспособной.

Какими бывают ложные срабатывания



- Три всадника апокалипсиса:
 - «Исторически сложилось»
 - «Так и задумано»
 - «А, это нормально»
- Неверные пороговые значения и условия выборки
- Применение правил корреляции в неправильных местах
- Некорректные поставщики событий и/или их настройка
- Неизбежные ложные срабатывания (0,5%...)

Проблемы и подводные камни

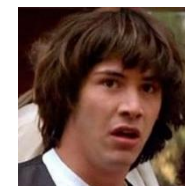


- Взаимодействие со службой IT
- Затянутость в получении информации по инцидентам
- Недостаточная настройка аудита событий на источниках
- Ошибки нормализации событий
- Незнание критичных бизнес-процессов и основных рабочих процессов
- Отсутствие организованности активов
- ...

Проблемы и подводные камни



- Взаимодействие со службой IT
- Затянутость в получении информации по инцидентам
- Недостаточная настройка аудита событий на источниках
- Ошибки нормализации событий
- Незнание критичных бизнес-процессов и основных рабочих процессов
- Отсутствие организованности активов
- ...Ошибки в создании собственных правил корреляции



Как бороться. Общее



- Понимание происходящего в инфраструктуре
- Наиболее полное покрытие инфраструктуры по источникам событий
- Наиболее полный аудит событий на источниках
- Плотное взаимодействие с IT-службой
- Разбор ситуаций «по месту»

Как бороться в MaxPatrol SIEM.

Часть 1. Структурно



- Приоритизация, разграничение действий правил корреляции применительно к разным группам активов
- Только нужные наборы правил корреляции
- Специфическая для конкретной инфраструктуры фильтрация отдельных правил

Как бороться в MaxPatrol SIEM.

Часть 2. Технически

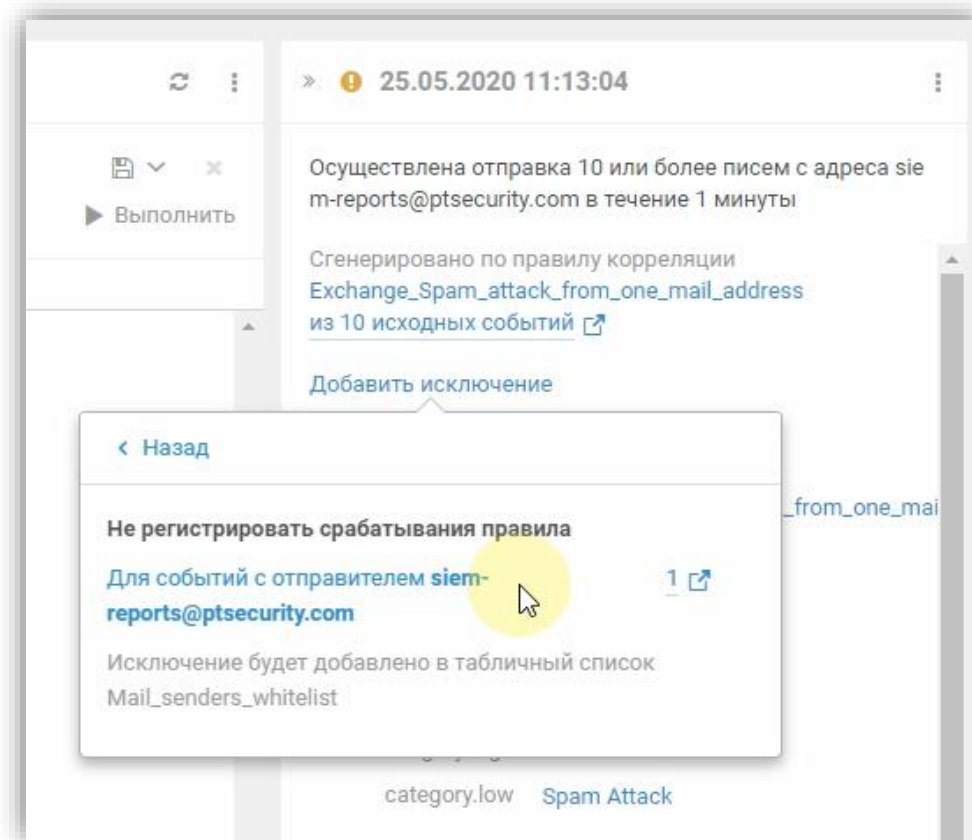


- «Вайтлистинг» и его последствия
- Наполнение табличных списков информацией об инфраструктуре
- Наиболее возможная полная информация об активах и их взаимодействии
- Доработка условий в правилах корреляции

Работа с ложными срабатываниями в MP SIEM 6.0



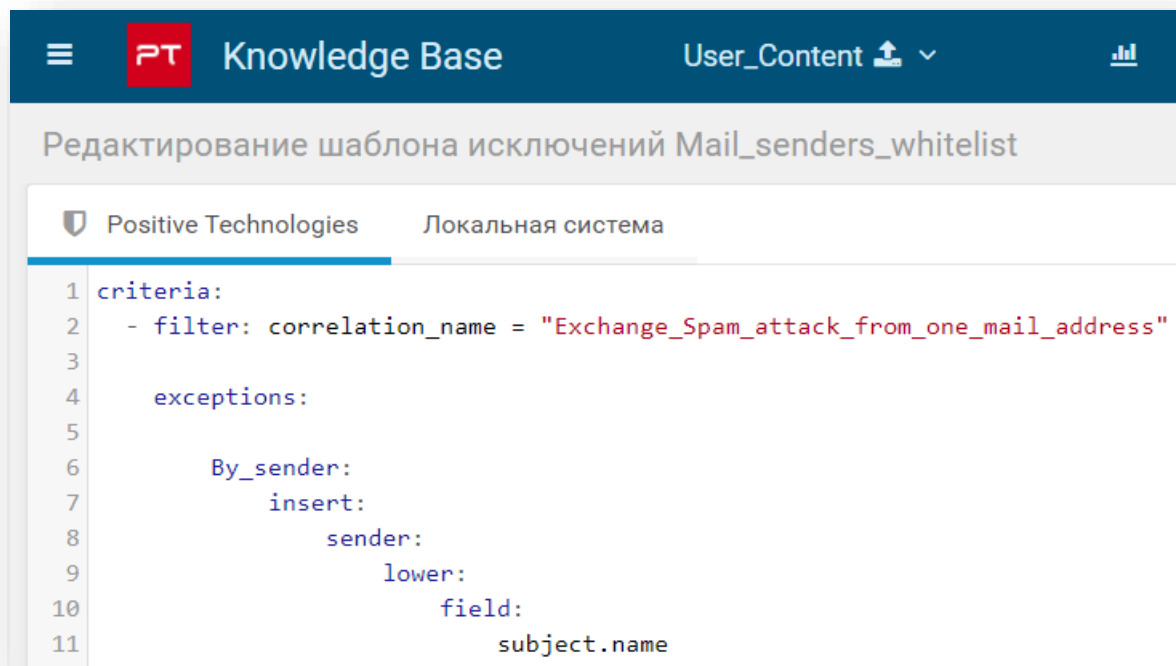
- Система сама подсказывает вам доступные варианты исключений
- Анализ «масштаба бедствия» по срабатываниям правил
- Удобное добавление/удаление исключений в пару кликов



Работа с ложными срабатываниями в MP SIEM 6.0

PT

- «Магия» описана в новых шаблонах исключений



The screenshot shows the 'Knowledge Base' interface with the title 'Редактирование шаблона исключений Mail_senders_whitelist'. It features two tabs: 'Positive Technologies' (selected) and 'Локальная система'. The main area displays a JSON configuration for an exception rule. The configuration includes a filter for 'Exchange_Spam_attack_from_one_mail_address' and a nested 'exceptions' section with a 'By_sender' condition. The 'By_sender' condition is further defined with 'insert', 'sender', 'lower', and 'field' properties, where the field is 'subject.name'.

```
1 criteria:
2   - filter: correlation_name = "Exchange_Spam_attack_from_one_mail_address"
3
4   exceptions:
5
6     By_sender:
7       insert:
8         sender:
9           lower:
10            field:
11              subject.name
```

Тексты исключений

Название (русский)	Не регистрировать срабатывания правила
Название (английский)	Do not register rule triggerings
Приоритет	Высокий
Условие 1	
Ключ	By_sender
Значение (русский)	Для событий с отправителем {subject.name}
Значение (английский)	For events with the sender {subject.name}

[Добавить условие](#)

[Добавить тексты исключений](#)

Работа с ложными срабатываниями в MP SIEM 6.0



- Создавайте свои шаблоны исключений в соответствии с developer guide (раздел 7)

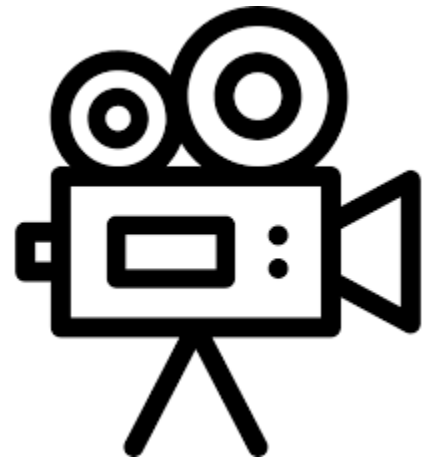
7. Создание шаблона исключений для заполнения табличного списка

После создания шаблона исключений и добавления его в Knowledge Base вы сможете по ссылкам из сводок о корреляционных событиях, зарегистрированных в PT MaxPatrol SIEM, автоматически добавлять исключения в табличный список типа "белый список" или удалять исключения из табличного списка типа "черный список".

Для создания шаблона исключений используется разметка YAML. Шаблон состоит из секции `criteria`, которая должна содержать хотя бы одну секцию `filter` для условия применения шаблона и одну секцию `exceptions` для описания исключений.

Сценарий 1.1

РТ

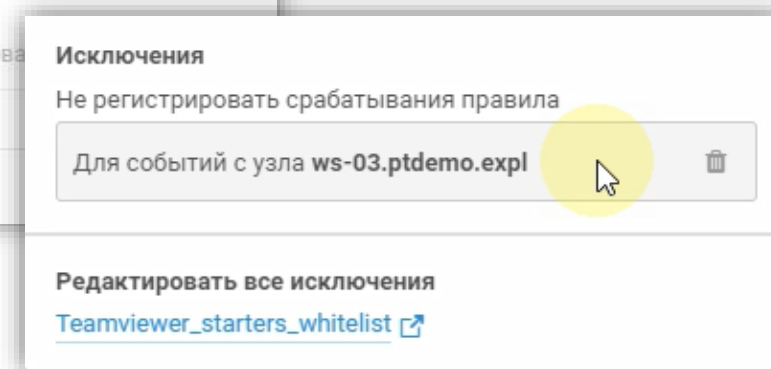
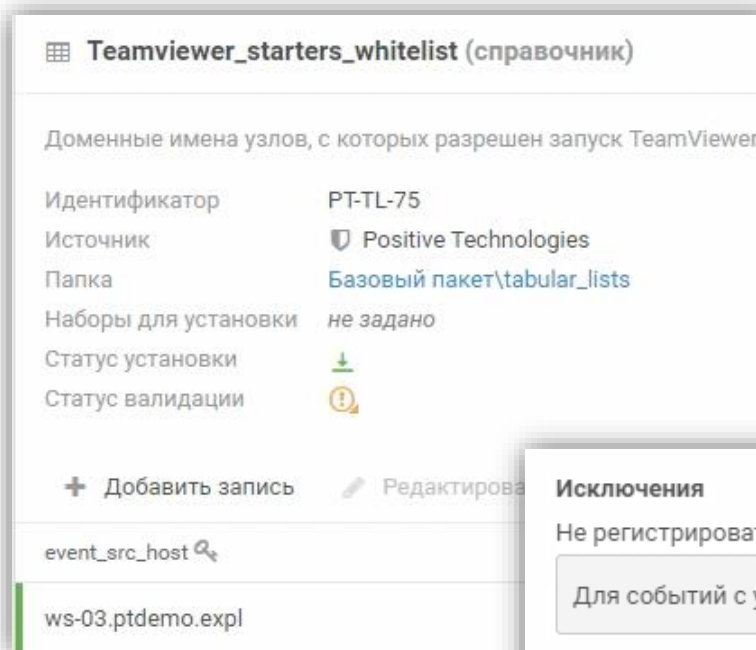


Video Demo

Работа с ложными срабатываниями в MP SIEM 6.0

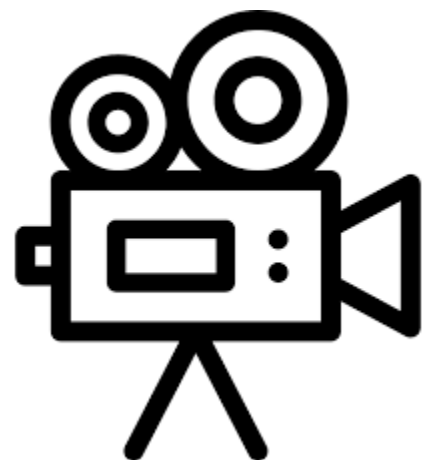
PT

- А что будет с моими текущими исключениями в табличных списках?
- Могу ли я вносить исключения через табличные списки, как раньше?



Сценарий 1.2

РТ



Video Demo

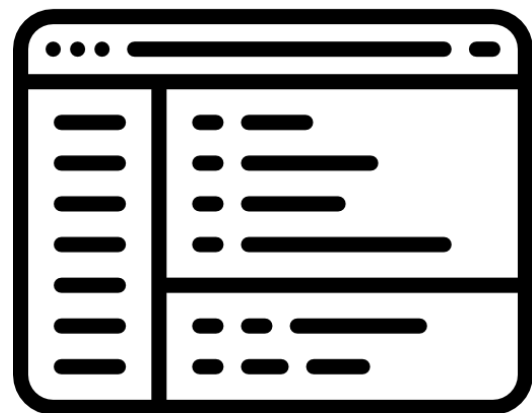
Часть 2. Практическая



- Что важно знать перед началом работ
- Описания экспертных паков
- Заведение исключений до включения, дофилльтрация после

Обзор пакетов экспертизы в MP SIEM 6.0

РТ



Live Demo

Практическая часть

Сценарий 2.1

РТ

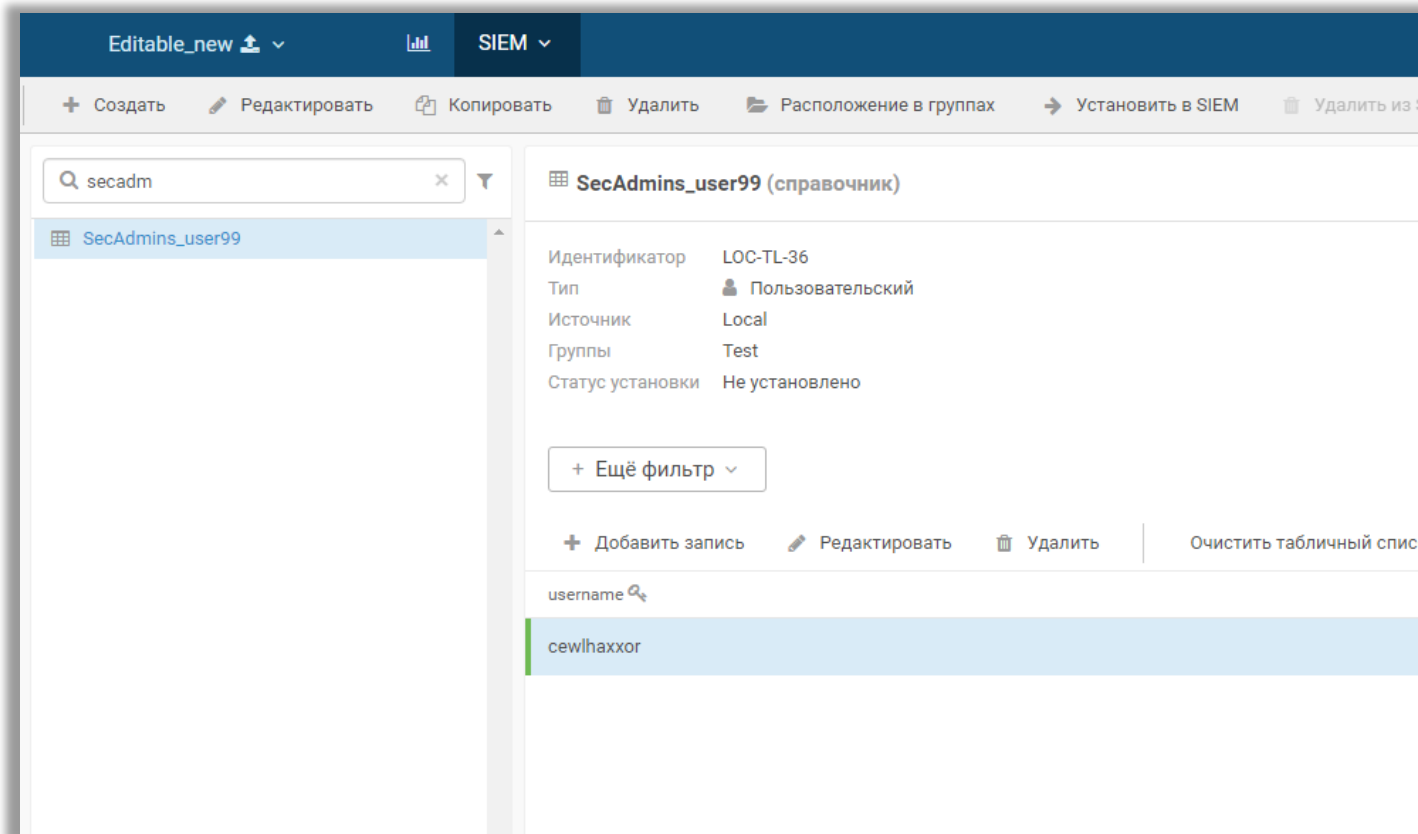
Сценарий номер 2.1:
работа в конструкторе
правил корреляции



2.1 Заводим пререквизиты



- Переходим в РТКВ
- Создаем табличный список SecAdmins_WBNR, добавляем колонку username (string)
- Сохраняем и добавляем в колонку произвольного пользователя
- Находим табличный список Critical_hosts, отмечаем его в памяти



2.1 Простейшее правило корреляции

- Начинаем создание правила
- Задаем имя и прочие параметры
- Блок А – вход в ОС Windows
- Блок Б – очистка журнала событий
- Проверяем условия срабатывания
- Выбираем, что складывать в инцидент
- Правило будет «фолзить»... Почему?

Условие корреляции

A → B

10 минут ▾

Должны произойти все события последовательно ▾

Событие A LoginSuccessful_Windows

Должно произойти ▾ 1 ▴ раз

Макрос

Успешный вход в систему (ОС Windows) ▾

успе

Все макросы

- Успешное повышение уровня...
- Успешный вход в систему
- Успешный вход в систему (ОС...
- Успешный вход в систему (ОС...

Успешный вход в ОС Windows от имени пользовательской учетной записи

Метки
Windows, Вход в систему, Пользователи и доступ

Аргументы макроса

Код макроса

```
filter LoginSuccessful_Windows() {  
  filter::NotFromCorrelator()  
  and event_src.vendor == "microsoft"  
  and event_src.title == "windows"  
  and msgid == "4624"  
  and  
  filter::UserAccount_Windows(subject.name,  
    subject.id)  
  and src.host != null  
}
```

Выбрать

2.1 Фильтрация: учетные записи

- Работа в основной вкладке конструктора
- Добавляем запрос в ранее созданный табличный список (SecAdmins_WBNR)
- Задаем сопоставление (!=) поля subject.name с соответствующей колонкой из списка

Условие корреляции

A → B

10 минут ▾

Должны произойти все события последовательно ▾

Событие A LoginSuccessful_Windows

Должно произойти ▾ 1 ▴ ▾ раз

Макрос

Успешный вход в систему (OC Windows) ▾

И

Запрос в табличный список

SecAdmins_user99 ▾

Есть запись, для которой выполняется хотя бы одно из условий ▾

Колонка табличного списка

username ▾ != ▾ subject.name ⚙ ▾

Колонка табличного списка ▾

И

Добавить условие для события ▾

ИЛИ

Добавить блок условий для события ▾

2.1 Фильтрация: узлы

- Работа в основной вкладке конструктора
- Добавляем запрос в отмеченный ранее табличный список Critical_hosts
- Задаем сопоставление (==) поля event_src.ip с соответствующей колонкой из списка

Условие корреляции

A → B

10 минут ▾

Должны произойти все события последовательно ▾

Событие A LoginSuccessful_Windows

Должно произойти ▾ 1 ▴ ▾ раз

Макрос

Успешный вход в систему (OC Windows) ▾

И

Запрос в табличный список

SecAdmins_user99 ▾

Есть запись, для которой выполняется хотя бы одно из условий ▾

Колонка табличного списка

username ▾ != ▾ subject.name ⚙ ▾

Колонка табличного списка ▾

И

Добавить условие для события ▾

ИЛИ

Добавить блок условий для события ▾

2.1 Фильтрация: условия (время и т.д.)

- Работа в основной вкладке конструктора
- Переходим к блоку условий
- В событии A уже отфильтровываются только события на критичных узлах, поэтому смело ставим длительность срабатывания – 1 час

Условие корреляции

A → B

60 минут ▾

Должны произойти все события последовательно ▾

Событие A LoginSuccessful_Windows

Должно произойти ▾ 1 ▴ раз

Макрос

Успешный вход в систему (OC Windows) ▾

2.1 Фильтрация: магия IF

PT

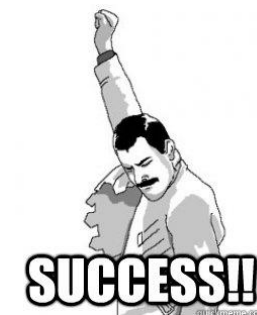
- А что, если нам все равно нужно фиксировать подобные события, даже если они произошли не на критичных узлах?
- Следующий сценарий нам поможет!



2.1 Ура! Конец сценария!

PT

- Валидация
- Ответы на вопросы



Практическая часть. Сценарий 2.2

РТ

Сценарий номер 2.2:

Работа в коде правил
корреляции



2.2 Введение.

Из чего состоит правило в коде

РТ

- Как перестать бояться XP
- Всего три с половиной блока – вот так просто
- Старые и новые фильтры в блоках
- Переменные и поля таксономии
- Warning: фарш нельзя повернуть назад!

2.2 Варианты фильтрации: табличные списки в коде

- Старый и новый способ вызова запроса в табличные списки – оба работают
- Правило Critical_host_threat_detection как образец старого способа запроса в табличный список
- В созданном нами ранее правиле – новый способ запроса в табличный список, его и будем использовать

```
ost_threat_detection

1 query CriticalHost($ip, $fqdn) from Critical_hosts {
2   (
3     ip == $ip or
4     fqdn == $fqdn
5   )
6 }
7
8 event Malware_detected_src:
9   key:
```

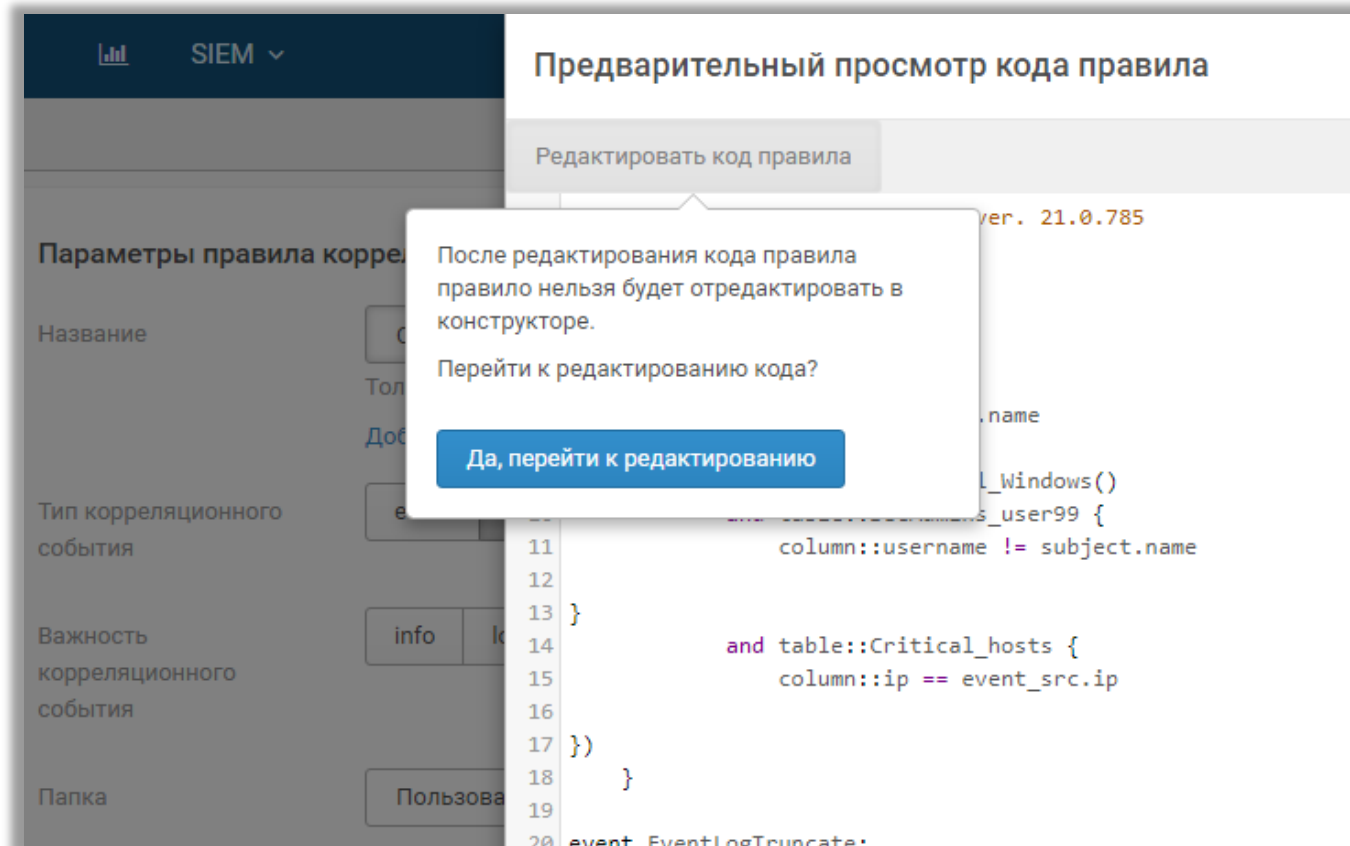
```
23   and correlation_name == null
24   and exec_query("CriticalHost", [src.ip, src.fqdn])
25 }
```

```
12
13 }
14   and table::Critical_hosts {
15     column::ip == event_src.ip
16 }
```


2.2 Заводим пререквизиты



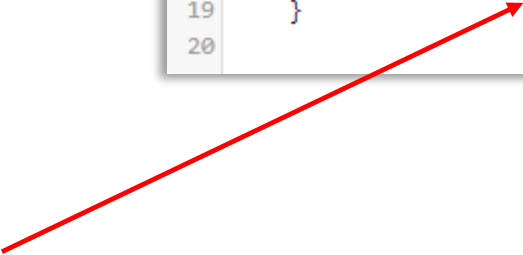
- Вспоминаем табличный список Critical_hosts
- Создаем копию нашего правила
- Через предварительный просмотр отправляемся в редактор кода



2.2 Фильтруем по учетной записи

- Отмечаем конструкцию filter в блоке event
- Используем операнд “and”
- Указываем нужно поле subject.name и декларируем его неравенство пользователю alloweduser (не забываем про кавычки!)

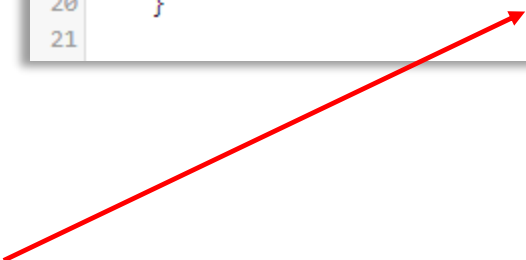
```
5 event LoginSuccessful_Windows:
6   key:
7     event_src.host, subject.name
8   filter {
9     (filter::LoginSuccessful_Windows()
10      and table::SecAdmins_user99 {
11        column::username != subject.name
12      })
13   }
14   and table::Critical_hosts {
15     column::ip == event_src.ip
16   }
17 })
18   and subject.name != "alloweduser"
19 }
20
```



2.2 Фильтруем по узлам

- Возвращаемся в конструкцию filter в блоке event
- Снова используем операнд “and”
- Указываем нужное поле event_src.ip и декларируем его неравенство какому-нибудь адресу, например 192.168.1.1

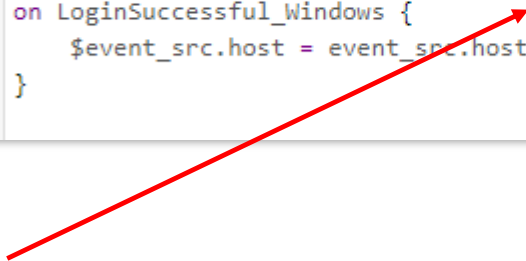
```
5 event LoginSuccessful_Windows:
6   key:
7     event_src.host, subject.name
8   filter {
9     (filter::LoginSuccessful_Windows()
10      and table::SecAdmins_user99 {
11        column::username != subject.name
12      })
13   }
14   and table::Critical_hosts {
15     column::ip == event_src.ip
16   }
17 })
18   and subject.name != "alloweduser"
19   and event_src.ip != "192.168.1.1"
20 }
21
```



2.2 Фильтруем по времени/условию

- Переходим к блоку rule
- Обратим внимание на формат воспроизведения
- Поменяем значение времени срабатывания на 100 минут

```
29
30 rule CleanEvenLog_user99_encode:(LoginSuccessful_Windows
31     -> EventLogTruncate) within 100m
32 on LoginSuccessful_Windows {
33     $event_src.host = event_src.host
34 }
35
```



2.2 Немного магии. Условие IF

- Возвратимся к идее регистрировать события, но не инциденты
- Скопируем запрос к табличному списку из блока event в блок rule (первое событие) и облачим его в if-endif
- Таким образом, явно указываем, что если узел присутствует в табличном списке, то это однозначно инцидент

```
29
30 rule CleanEvenLog_user99_encode:(LoginSuccessful_Windows
31     -> EventLogTruncate) within 100m
32 on LoginSuccessful_Windows {
33     $event_src.host = event_src.host
34 }
35
```

```
29
30 rule CleanEvenLog_user99_encode:(LoginSuccessful_Windows
31     -> EventLogTruncate) within 100m
32 on LoginSuccessful_Windows {
33     $event_src.host = event_src.host
34     if table::SecAdmins_User99 {column::username != subject.name}
35     then $correlation_type = "incident"
36     endif
37 }
38
```



2.2 Немного магии. Условие IF

- Перейдем к блоку emit
- Облачим переменную correlation_type в if-endif
- Укажем, что если переменная correlation_type не была назначена ранее (null), то считать корреляционное событие просто событием
- (Сопоставление обозначается двойным "==", назначение одинарным "=")

```
47
48 emit {
49     $correlation_name = "CleanEvenLog_user99_encode"
50     $correlation_type = "incident"
51
```

```
47
48 emit {
49     $correlation_name = "CleanEvenLog_user99_encode"
50     if $correlation_type == null
51     then $correlation_type = "event"
52     endif
53
```

2.2 Мы сделали это!

PT

- Валидация
- Ответы на вопросы



Что дальше:



Обзор пакета экспертизы для удаленки:

ptsecurity.com/ru-ru/research/webinar/310842/

Заказать пилот:

ptsecurity.com/ru-ru/solutions/secure-remote-work/

Пройти обучение:

edu@ptsecurity.com

Купить:

sales@ptsecurity.com



Антон Исаев

Специалист по системам мониторинга безопасности



Станислав Черкасов

Менеджер по продвижению продуктов

Бонус:

Вносим IP-адреса / FQDN контроллеров домена:

- **AD_Domain_Controllers**
- **Directory_Replication_Agent**

Вносим IP-адреса DNS серверов:

- **Trusted_DNS_servers**

Вносим логины учетных записей / IP-адреса / FQDN узлов, для которых допустим Bruteforce:

- **Bruteforce_entities_whitelist**

Вносим логины привилегированных учетных записей, IP-адреса и FQDN узлов, с которых выполняется администрирование:

- **AD_Security_Administrators**



Примечание: Буквы в табличные списки нужно вводить только в нижнем регистре.

Кроме того, если данные в колонках могут принимать любые значения, необходимо ввести звездочку (*) в колонки с типом данных String и ноль в колонки с типом данных Number.

Бонус:

☰

РТ

MaxPatrol SIEM

Активы ▾

События

Инциденты ▾

Сбор данных ▾

Система ▾

События

за последние 12 месяцев 📅

🔍 Все события ✕

»

Визуализация

+ Создать инцидент

🔗 Связать с инцидентом

📄 Выпустить отчет

🗺 Показать на топологии

🔄

⋮

Все события

correlation_name != null ✕

correlation_name ✕

Σ

Выполнить

📄 ▾

✕

«	Кол.	correlation_name		time ▾	event_src.host	text
2911530	many_tcp_connections	!	29.05.2019 12:40:38	Нет данных	С узла 1	наблюдается большое количество запросов на установку TCP-соединения за короткий
1262437	subrule_stat_current_average	!	29.05.2019 12:40:37	Нет данных	С узла 1	наблюдается большое количество запросов на установку TCP-соединения за короткий
1252964	is_windows_login_from_one_host_using_different_accounts	!	29.05.2019 12:40:37	Нет данных	С узла 1	l.32 наблюдается большое количество запросов на установку TCP-соединения за коро
968410	mac_notification_detect	!	29.05.2019 12:40:36	Нет данных	С узла 1	l.30 наблюдается большое количество запросов на установку TCP-соединения за коро
814393	windows_login_from_one_host_using_different_accounts	!	29.05.2019 12:40:36	Нет данных	С узла 1	наблюдается большое количество запросов на установку TCP-соединения за короткий
244178	windows_bruteforce_from_src_to_diff_dst_remote	!	29.05.2019 12:40:35	Нет данных	С узла 1	l.46 наблюдается большое количество запросов на установку TCP-соединения за коро
93908	is_many_tcp_connections	!	29.05.2019 12:40:33	Нет данных	С узла 1	l.46 наблюдается большое количество запросов на установку TCP-соединения за коро
33923	the_same_account_login_from_different_hosts	!	29.05.2019 12:40:32	Нет данных	С узла 1	наблюдается большое количество запросов на установку TCP-соединения за короткий
25281	bruteforce_attempt_atomic	!	29.05.2019 12:40:31	Нет данных	С узла 1	l.32 наблюдается большое количество запросов на установку TCP-соединения за коро
24133	resource_overload	!	29.05.2019 12:40:30	Нет данных	С узла 1	l.30 наблюдается большое количество запросов на установку TCP-соединения за коро
18755	infected_object_detect_and_not_clean_on_event_src_host	!	29.05.2019 12:40:30	Нет данных	С узла 1	наблюдается большое количество запросов на установку TCP-соединения за короткий

Группы и фильтры

Бонус:

MaxPatrol SIEM

Активы ▾ События Инциденты ▾ Сбор данных ▾ Система ▾

События за последние 12 месяцев 📅 🔍 Все события ✕

Визуализация + Создать инцидент 🔗 Связать с инцидентом 📄 Выпустить отчет 🗺 Показать на топологии ↻ ⋮

Все события

correlation_name = windows_malicious_service_registration ✕ object.name ✕ Σ Выполнить 📄 ▾ ✕

Кол.	object.name	time ▾	event_src.host	text
15	kav_inst_agent\$c69dbb26301b4a0282a6173cfb75c698_1	04.04.2019 15:50:35	1...	Сервис "KAV_Inst_Agent\$c69dbb26301b4a0282a6173cfb75c698_1", находящийся
10	kl deployment wrappera1	25.03.2019 15:20:06	N...	Сервис "KAV_Inst_Agent\$c69dbb26301b4a0282a6173cfb75c698_1", находящийся
8	kl deployment wrapper11	12.03.2019 14:55:46	N...	Сервис "KAV_Inst_Agent\$c69dbb26301b4a0282a6173cfb75c698_1", находящийся
8	kl deployment wrapper32	12.03.2019 14:55:46	1...	Сервис "KAV_Inst_Agent\$c69dbb26301b4a0282a6173cfb75c698_1", находящийся
8	kl deployment wrapper65	12.03.2019 14:55:00	s...	Сервис "KAV_Inst_Agent\$c69dbb26301b4a0282a6173cfb75c698_1", находящийся
8	kl deployment wrapper91	12.03.2019 14:55:00	s...	Сервис "KAV_Inst_Agent\$c69dbb26301b4a0282a6173cfb75c698_1", находящийся
8	kl deployment wrapperd2	12.03.2019 14:54:59	s...	Сервис "KAV_Inst_Agent\$c69dbb26301b4a0282a6173cfb75c698_1", находящийся

Викторина:

Windows_Hacktool_detect

Запуск программного обеспечения, обычно используемого взломщиками.

```
in_list(["hydra.exe", "mimikatz.exe", "ora-auth-alter-session.exe", "ora-brutesid.exe", "ora-getsid.exe",  
        "ora-pwdbrute.exe", "ora-userenum.exe", "ora-ver.exe", "nbtscan.exe", "fgdump.exe", "pwdump.exe",  
        "cain.exe", "nmap.exe", "hash_suite_64.exe", "hash_suite_32.exe", "psfile.exe", "psexec.exe",  
        "psgetsid.exe", "psinfo.exe", "pskill.exe", "pslist.exe", "psloggedon.exe", "psloglist.exe",  
        "pspasswd.exe", "psping.exe", "psservice.exe", "psshutdown.exe", "pssuspend.exe",  
        "smsniff.exe", "wireshark.exe", "putty.exe", "saminside.exe", "nc.exe", "nc64.exe", "hping.exe",  
        "sncan.exe", "ettercap.exe", "netbios_enumerator.exe", "shareenum.exe", "accessenum.exe",  
        "superscan4.1.exe", "cachedump64.exe", "netenum.exe", "unicornscan.exe", "medusa.exe"], lower(object.name))
```


Викторина:

Windows_Hacktool_detect

Запуск программного обеспечения, обычно используемого взломщиками.

```
in_list(["hydra.exe", "mimikatz.exe", "ora-auth-alter-session.exe", "ora-brutesid.exe", "ora-getsid.exe",  
        "ora-pwdbrute.exe", "ora-userenum.exe", "ora-ver.exe", "nbtscan.exe", "fgdump.exe", "pwdump.exe",  
        "cain.exe", "nmap.exe", "hash_suite_64.exe", "hash_suite_32.exe", "psfile.exe", "psexec.exe",  
        "psgetsid.exe", "psinfo.exe", "pskill.exe", "pslist.exe", "psloggedon.exe", "psloglist.exe",  
        "pspasswd.exe", "psping.exe", "psservice.exe", "psshutdown.exe", "pssuspend.exe",  
        "smsniff.exe", "wireshark.exe", "putty.exe", "saminside.exe", "nc.exe", "nc64.exe", "hping.exe",  
        "sncan.exe", "ettercap.exe", "netbios_enumerator.exe", "shareenum.exe", "accessenum.exe",  
        "superscan4.1.exe", "cachedump64.exe", "netenum.exe", "unicornscan.exe", "medusa.exe"], lower(object.name))
```

Hacktool_whitelist (справочник)

A whitelist of hosts that are allowed to run hacktools

```
and not exec_query("Check_event_src_host_Hacktool_whitelist", [lower(event_src.host), lower(subject.id)])
```

Викторина:

Exchange_Spam_attack_from_one_mail_address

Множественная рассылка писем (10 и более) с одного фиксированного почтового адреса в течение одной минуты.

Exchange_Spam_attack_on_one_mail_address

Множественные входящие письма (10 и более) на фиксированный почтовый ящик в течение одной минуты.

Викторина:

Exchange_Spam_attack_from_one_mail_address

Множественная рассылка писем (10 и более) с одного фиксированного почтового адреса в течение одной минуты.

Exchange_Spam_attack_on_one_mail_address

Множественные входящие письма (10 и более) на фиксированный почтовый ящик в течение одной минуты.

 Mail_senders_whitelist (справочник)

A whitelist of mail senders

 Mail_recipients_whitelist (справочник)

A whitelist of mail recipients

```
and not exec_query("Check_receiver-Mail_recipients_whitelist", [lower(subject.name)])
```

```
and not exec_query("Check_sender-Mail_senders_whitelist", [lower(subject.name)])
```


Викторина:

Many_tcp_connections

Частые запросы на установку TCP-соединения от узла.

Викторина:

Many_tcp_connections

Частые запросы на установку TCP-соединения от узла.

 **Many_tcp_connections_whitelist** (справочник)

A whitelist of hosts that are allowed to establish many TCP connections

```
and not exec_query("Check_hostname_Many_tcp_connections_whitelist", [lower(event_src.host)])
```

src.host

Викторина:

Work_at_night

Работа пользователя в ночное время во внутренней сети компании. Вход пользователя, затем выполнение им любых действий в период с 21:00 до 7:00

Викторина:

Work_at_night

Работа пользователя в ночное время во внутренней сети компании. Вход пользователя, затем выполнение им любых действий в период с 21:00 до 7:00

 Night_work_users_whitelist (справочник)

A whitelist of users who are allowed to work night shifts

```
and not exec_query("Check_username_domain_src_ip_Night_work_users_whitelist", [lower(subject.domain),  
lower(subject.name), src.ip])
```

Викторина:

TeamViewer_service_detect

На узле было обнаружено использование TeamViewer.

TeamViewer_connection_detect

Возможно, зафиксировано подключение TeamViewer (любое подключение на порт 5938 или HTTP(S)-подключение к одному из известных серверов TeamViewer).

Викторина:

TeamViewer_service_detect

На узле было обнаружено использование TeamViewer.

TeamViewer_connection_detect

Возможно, зафиксировано подключение TeamViewer (любое подключение на порт 5938 или HTTP(S)-подключение к одному из известных серверов TeamViewer.

 **Teamviewer_starters_whitelist** (справочник)

A whitelist of hosts that are allowed to run TeamViewer

```
and not exec_query("Check_hostname_Teamviewer_starters_whitelist", [lower(event_src.host)])
```


Викторина:

Windows_login_from_one_host_using_different_accounts *

Вход с 1 источника на 1 узел под 2 различными учетными записями за 8 часов

Викторина:

Windows_login_from_one_host_using_different_accounts *

Вход с 1 источника на 1 узел под 2 различными учетными записями за 8 часов

Добавляем в исключения терминальные сервера Заказчика,
на которых по определению работает куча пользователей, которые постоянно куда-то ходят:

```
and not in_list(["x.x.x.x", "x.x.x.x"], src.host)
and find_substr(lower(src.host), "srv-rds-") == null
```

А также...

Викторина:

Windows_login_from_one_host_using_different_accounts *

Вход с 1 источника на 1 узел под 2 различными учетными записями за 8 часов

Добавляем в исключения терминальные сервера Заказчика, на которых по определению работает куча пользователей, которые постоянно куда-то ходят:

```
and not in_list(["x.x.x.x", "x.x.x.x"], src.host)
and find_substr(lower(src.host), "srv-rds-") == null
```

А также...

- Добавляем в исключения почтовые сервера Заказчика
- Добавляем в исключения файловые сервера Заказчика

Викторина:

Windows_bruteforce_from_src_to_diff_dst_remote *

Обнаружение признаков вредоносного ПО: 10 попыток удаленного входа в систему с одного узла на несколько узлов в течение 5 минут

Викторина:

Windows_bruteforce_from_src_to_diff_dst_remote *

Обнаружение признаков вредоносного ПО: 10 попыток удаленного входа в систему с одного узла на несколько узлов в течение 5 минут

- Добавляем в исключения адреса агентов SIEM, с которых будут происходить сканирования:

```
and not in_list(["mpsiemagent"], lower(src.host))
```

- Добавляем в исключения УЗ, с которой SIEM запускает задачи:

```
and not in_list(["siem"], lower(subject.name))
```

- Добавляем в исключения терминальные сервера, на которых по определению работает куча пользователей, которые постоянно куда-то ходят:

```
and not in_list(["x.x.x.x", "x.x.x.x"], src.host)  
and find_substr(lower(src.host), "srv-rds-") == null
```