

КАК ОРГАНИЗОВАТЬ РАБОТУ С ИСКЛЮЧЕНИЯМИ/FALSE POSITIVE ДЛЯ КОРОБОЧНОГО КОНТЕНТА В MRSIEM И НЕ СОЙТИ С УМА

Горбачев Валерий

Руководитель направления внедрения средств защиты информации

АО «ДиалогНаука»

Summary по текущей версии(6.2)

- Распределённый поиск событий между площадками (без репликации между хранилищами)
- Распределение этапов сбора и обработки событий между несколькими системами (на разных площадках)
- Улучшены возможности траблшутинга с помощью модуля мониторинга обработки активов



Summary по текущей версии(6.2)



- Сверхнагруженная конфигурация до 60к EPS (если поток более 45к EPS, понадобится 2 MP SIEM Server)
- Изменение параметров табличного списка в Knowledge Base теперь не приводит к его очистке
- Условная запись в табличный список (условие в insert_into)
- Во время установки объектов из Knowledge Base в MaxPatrol SIEM теперь доступен просмотр событий и табличных списков

Краткий обзор коробочного контента

Пакеты экспертизы + Создать

Папки +

Системное название, идентификатор или описание

№	Статус	Идентификатор	Системное название	Описание	Источник	Папка
1	✓	PT-TL-195	Network_devices_trusted_hosts	Исключения из правил пакеты экспертизы "Сетевые устройства...	U	Сетевые устройства. Индикаторы компрометации\tabular_lists
2	✓	PT-TL-182	Solaris_ppids	Родительские PID для обогащений	U	Oracle Solaris. Подозрительная сетевая активность\tabular_lists
3	✓	PT-TL-181	Solaris_whitelist	Исключения из пака "Solaris"	U	Oracle Solaris. Подозрительная сетевая активность\tabular_lists
4	✓	PT-TL-180	Sensitive_registry_keys_modifiers_whitelisting	Названия процессов, которым разрешено изменять важные раз...	U	Windows. Подозрительные действия пользователей\tabular_lists
5	✓	PT-TL-179	SAP_JAVA_Significant_users	Черный список учетных записей систем SAP JAVA	U	SAP NetWeaver AS Java. Подозрительная активность пользовате...
6	✓	PT-TL-178	SAP_JAVA_default_users	Учетные записи по умолчанию систем SAP JAVA	U	SAP NetWeaver AS Java. Подозрительная активность пользовате...
7	✓	PT-TL-177	SAP_JAVA_admin_users	Привилегированные учетные записи систем SAP JAVA	U	SAP NetWeaver AS Java. Подозрительная активность пользовате...
8	✓	PT-TL-176	SAP_JAVA_admin_groups	Привилегированные группы систем SAP JAVA	U	SAP NetWeaver AS Java. Подозрительная активность пользовате...
9	✓	PT-TL-175	Auditd_network_activity_whitelist_regex	Исключения для пакета экспертизы "Linux_suspicious_network_a...	U	Linux. Подозрительная сетевая активность\tabular_lists
10	✓	PT-TL-163	Auditd_autowhitelist_known_hosts	Известные узлы Linux и временной интервал для автоматическо...	U	Базовый пакет\tabular_lists
11	✓	PT-TL-162	Auditd_autowhitelist_exceptions	Исключения, добавленные автоматически для пакетов эксперти...	U	Базовый пакет\tabular_lists
12	✓	PT-TL-161	vSphere_VM_files_assets	Файлы виртуальных машин	U	VMware vSphere. Подозрительная активность пользователей\tab...

Краткий обзор коробочного контента

Пакеты экспертизы + Создать ▾

< Папки +

Все объекты

- Базовый пакет
- Active Directory
- Active Directory. Подозрительная активность...
- АТТ&СК: «Выполнение» и «Предотвращение...
- АТТ&СК: «Закрепление»
- АТТ&СК: «Перемещение внутри периметра»
- АТТ&СК: «Повышение привилегий» и «Управ...
- АТТ&СК: «Получение учетных данных»
- АТТ&СК: «Разведка»
- АТТ&СК: «Сбор данных» и «Воздействие»
- Linux. Подозрительная сетевая активность
- Linux. Подозрительные действия пользоват...
- Linux. Подозрительные изменения системн...
- Microsoft SQL Server
- MongoDB
- Oracle Database
- Oracle MySQL
- Oracle Solaris. Подозрительная сетевая акти...
- PostgreSQL
- PT Application Firewall
- SAP NetWeaver AS ABAP
- SAP NetWeaver AS ABAP. Подозрительная ак...
- SAP NetWeaver AS Java. Подозрительная акт...
- VMware vSphere. Подозрительная активност...
- Windows. Подозрительные действия пользо...
- Атаки методом перебора
- Атаки с помощью специализированного ПО

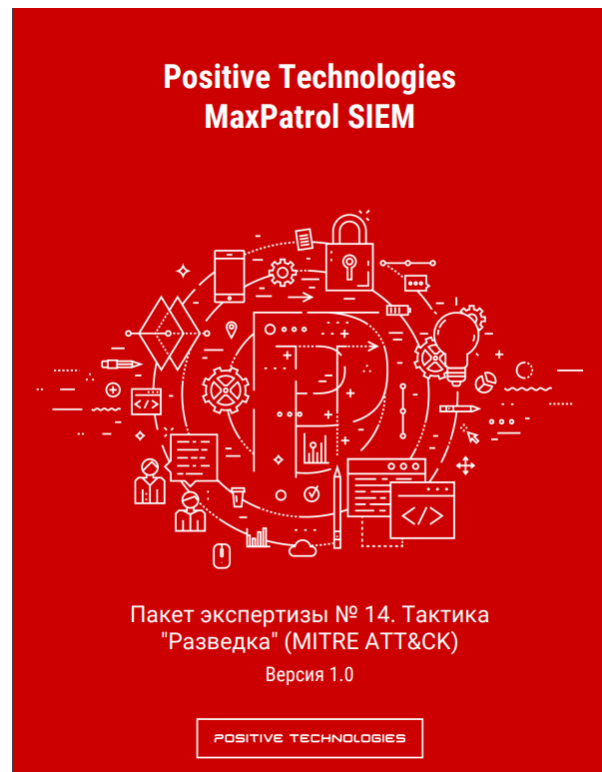
Атаки с помощью специализированного ПО 0 пакета

Системное название, идентификатор или описание

№...	С...	Идентификатор ▾	Системное название
1	✔	PT-CR-403	Silver_Shell_Subrule_1
2	✔	PT-CR-402	Koadic_WMIC_Win7_Subrule_2
3	✔	PT-CR-401	Koadic_WMIC_Win7_Subrule_1
4	✔	PT-CR-400	Koadic_WMIC_V2_Subrule_2
5	✔	PT-CR-399	Koadic_WMIC_V2_Subrule_1
6	✔	PT-CR-398	Koadic_rundll32_Win7_Subrule_3
7	✔	PT-CR-397	Koadic_rundll32_Win7_Subrule_2
8	✔	PT-CR-396	Koadic_rundll32_Win7_Subrule_1
9	✔	PT-CR-395	Koadic_Rundll32_V2_Win7_Subrule_1
10	✔	PT-CR-394	Koadic_Rundll32_V2_Subrule_2
11	✔	PT-CR-393	Koadic_Rundll32_V2_Subrule_1
12	✔	PT-CR-392	Koadic_REGSVR32_Win7_Subrule_3
13	✔	PT-CR-391	Koadic_REGSVR32_Win7_Subrule_2
14	✔	PT-CR-390	Koadic_REGSVR32_Win7_Subrule_1
15	✔	PT-CR-389	Koadic_REGSVR32_V2_Win7_Subrule_1
16	✔	PT-CR-388	Koadic_REGSVR32_V2_Subrule_2
17	✔	PT-CR-387	Koadic_REGSVR32_V2_Subrule_1
18	✔	PT-CR-386	Koadic_MSHTA_Win7_Subrule_3

- Всего 7020 объектов в РТКВ
- Большинство Заказчиков сразу устанавливают весь контент из коробки
- Поддерживаемые источники приведены в Приложении Б refguide
- Частично поддерживаемые источники приведены в Приложении В refguide

- Для отдельных категорий ПО и вендоров (MSSQL, Linux, Windows, SAP, Oracle)
- Для отдельных тактик MITRE (Разведка, Сбор данных, Выполнение)
- Для отдельных видов атак (перебором, с помощью специального ПО)
- Для каких-то актуальных задач (обеспечение безопасной удалённой работы)



Реагирование на инцидент

Если обнаруженная активность не является для учетной записи ожидаемой и легитимной, рекомендуется принять меры к блокировке учетной записи и (или) изоляции узла, с которого производилась атака.

При выявлении ложного срабатывания необходимо настроить механизм обработки ложных срабатываний. Для этого данные связанного с инцидентом события ИБ необходимо внести в табличный список `MITRE_ATTACK_whitelist`. Вы можете сделать это автоматически по ссылке из сводки о событии ИБ в интерфейсе MaxPatrol SIEM или вручную.

Примечание. Буквы во все колонки табличного списка, кроме колонки `rule`, 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`.

В колонках табличного списка нужно указать:

- `rule` – имя правила корреляции, по которому зарегистрировано событие (указано в поле события `correlation_name`).
- `host` – имя узла, на котором зарегистрировано событие (указано в поле `event_src.host`).
- `user_id` – имя учетной записи, с которой связана подозрительная активность (указан в поле `subject.name`).
- `specific_value` – запрос, выполненный в СУБД (указан в поле `object.value`).
- `user_name` – не используется.
- `user_domain` – не используется.

- Результат работы команды экспертов РТ
- Есть руководства по настройке источников
- Есть инструкции по обработке false positive

- Встроенное категорирование инцидентов в пакетах экспертизы, базирующихся на MITRE

The screenshot displays a security tool interface. On the left, a tree view shows a list of correlation rules under the 'correlation_rules' folder. The rule 'Detect_Abusing_CredSSP' is selected and highlighted in blue. A red box highlights the rule name in the list. On the right, the configuration for the 'Detect_Abusing_CredSSP' rule is shown. The configuration includes several fields for event data and a red box highlighting the category settings at the bottom.

```
Правило корреляции Detect_Abusing_CredSSP
41   $object.state = object.state
42   $object.property = object.property
43   $object.value = object.value
44
45   $datafield1 = datafield1 # ID сессии
46   $datafield2 = datafield2 # Идентификатор процесса-субъекта
47   $datafield3 = datafield3 # Путь к исполняемому файлу процесса-субъекта
48   $datafield4 = datafield4 # Имя процесса-субъекта
49   $datafield7 = datafield7 # GUID процесса-субъекта
50
51   $reason = string(regex(lower(object.name),
52   "allowdefaultcredentials|concatenatedefaults_allowdefault|allowdefcredentialswhenntlmonly|concatenatedefaults_allowdefntlmonly", 0))
53
54   $event_src.ip = event_src.ip
55   $event_src.hostname = event_src.hostname
56   $event_src.fqdn = event_src.fqdn
57   $event_src.host = event_src.host
58   $event_src.asset = event_src.asset
59   $event_src.vendor = event_src.vendor
60   $event_src.title = event_src.title
61   $event_src.subsys = event_src.subsys
62 }
63 emit (
64   $correlation_type = "incident"
65
66   if $subject.name != null then
67     $subject = "account"
68   endif
69
70   $action = "modify"
71   $object = "configuration"
72   $status = "success"
73
74   $object.type = "CredSSP configuration in registry"
75
76   $importance = "high"
77
78   $category_generic = "Attack"
79   $category_high = "Credential Access"
80   $category_low = "Credential Dumping"
81
```


Установка/удаление правил

Правила корреляции

Включить Отключить

Список правил корреляции

Все статусы x

Статус	Идентификатор	Название	Категория	Тип	Срабатываний за сутки ...
🔴	PT-CR-488	Detect_system_API_calls_from_suspicious_dir	Attack / Execution / Native API	🔴	697
🔴	PT-CR-296	Detect_run_reverse_shell_by_something	Attack / Command And Control / Reverse-shell	🔴	696
🔴	PT-CR-446	Detect_log_modify	Attack / Persistence / File System Permissions Weakness	🔴	108
🔴	PT-CR-478	Detect_etc_read_utlile	Attack / Discovery / System Information Discovery	🔴	88
🔴	PT-CR-181	Bruteforce_attempt_atomic	Attacks & Recon / Attack / Bruteforce	🔴	53
🔴	PT-CR-489	Subrule_Detect_PrivEscalation_via_GTFOBINS	//	🔴	34

Некоторые правила корреляции были приостановлены, поскольку срабатывали слишком часто.

13:55

[Перейти к правилам корреляции](#)

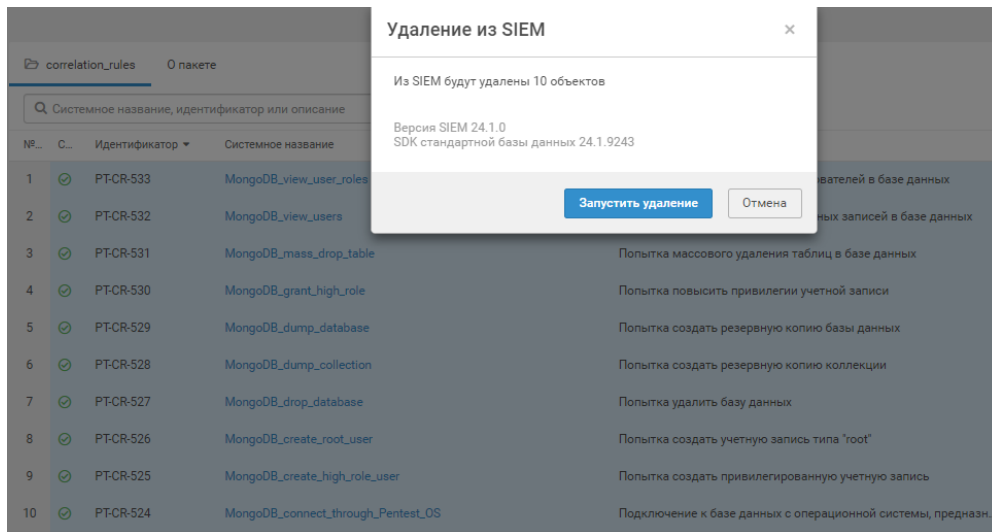
ATT&CK: «Закрепление» 0 пакете

Системное название, идентификатор или описание

№...	С...	Идентификатор	Системное название	Описание	Источник	↓
1	🟢	PT-CR-568	Detect_Possible_IIS_Native_Module_Installation	Обнаружение попыток установить модуль расширения IIS с помо...	🔴	↓
2	🟢	PT-CR-521	Detect_Debugger_in_Image_File_Execution_Options	Обнаружение попыток встроить стороннее ПО в цепочку запуска ...	🔴	↓
3	🟢	PT-CR-459	Detect_Possible_Malicious_StickyKey_used	Попытка обойти вход в систему, используя особенности ОС Wind...	🔴	↓
4	🟢	PT-CR-370	Detect_WMI_Substitutions_modification	Обнаружение подмены объектов WMI	🔴	↓

Установка/удаление правил

- Не бегите за «количеством» правил и пакетов
- Определите применимость правил и пакетов экспертизы для вашей инфраструктуры и источников
- Лучший подход:
 1. Формирование списка источников
 2. Определение применимых правил и пакетов
 3. Поэтапное включение правил



Корректировка параметров правил корреляции

correlation_rules 0 пакете

Правило корреляции Windows_Disabling_DeviceLock_before_using_USB_storage_devices

```
1 # Microsoft Windows
2
3 event USB_storage_connection:
4   key:
5     event_src.host
6   filter {
7     id == "PT_Microsoft_Windows_wmi_Usb_device_is_connected" and
8     object.name == "USB Mass Storage Device"
9   }
10
11 event Off_DeviceLock:
12   key:
13     event_src.host
14   filter {
15     object.name == "DeviceLock Service" and
16     ((id == "PT_Microsoft_Windows_eventlog_7034_Service_terminated_unexpected_multiple_times") or
17     (id == "PT_Microsoft_Windows_eventlog_7040_Start_type_was_changed" and object.property == "start type" and object.value
18     == "disabled"))
19   }
20 rule Windows_Disabling_DeviceLock_before_using_USB_storage_devices: (Off_DeviceLock -> USB_storage_connection) within 30m
21
22 on USB_storage_connection {
23   $object.id = object.id
24   $object.name = object.name
```

USB-устройство подключено к узлу после отключения службы DeviceLock

Системное название	Windows_Disabling_DeviceLock_before_using_USB_storage_c
Идентификатор	PT-CR-40
Тип	Стандартный
Источник	Positive Technologies
Папка	Общие правила корреляции\correlation_rules
Статус валидации	✓
Статус установки	↓

Правила локализации

Критерии	correlation_name = "Windows_Disabling_DeviceLock_bef ore_using_USB_storage_devices"
Значение (русский)	USB-устройство (object.name) было подключено к узлу (event_src.host) после отключения службы DeviceLock
Значение (английский)	USB device (object.name) was connected to the host (event_src.host) when the DeviceLock service was disabled

- Изменение параметров счётчика, таймера
- Изменение логики корреляции
- Обязательная переустановка правила в MPSIEM!!!

Работа с табличными списками

```
correlation_rules  0 пакете

Правило корреляции External_mail_service_usage

1 query Check_if_service_whitelisted_src($ip) from Trusted_network_services_whitelist {
2   service_type == "MAIL"
3   and (
4     src_ip == $ip
5     or in_subnet($ip, src_subnet)
6   )
7 }
8
9 query Check_if_service_whitelisted_dst($ip) from Trusted_network_services_whitelist {
10  service_type == "MAIL"
11  and (
12    dst_ip == $ip
13    or in_subnet($ip, dst_subnet)
14  )
15 }
16
```

Trusted_network_services_whitelist

№...	С...	Идентификатор ▾	Системное название	Описание	Исто...	↓ ...	Папка
1	✔	PT-TL-140	Trusted_network_services_whitelist	Исключения из правил доступа к сетевым сервисам	🛡	↓	Сетевые устройства. Подозрительная сетевая активность\tabular_lists

- Определение, какой ТС используется в правиле
- Какие параметры проверяются?
- Какие фильтры при проверке? (service_type=MAIL)

Работа с табличными списками

Trusted_network_services_whitelist (справочник)

Исключения из правил доступа к сетевым сервисам

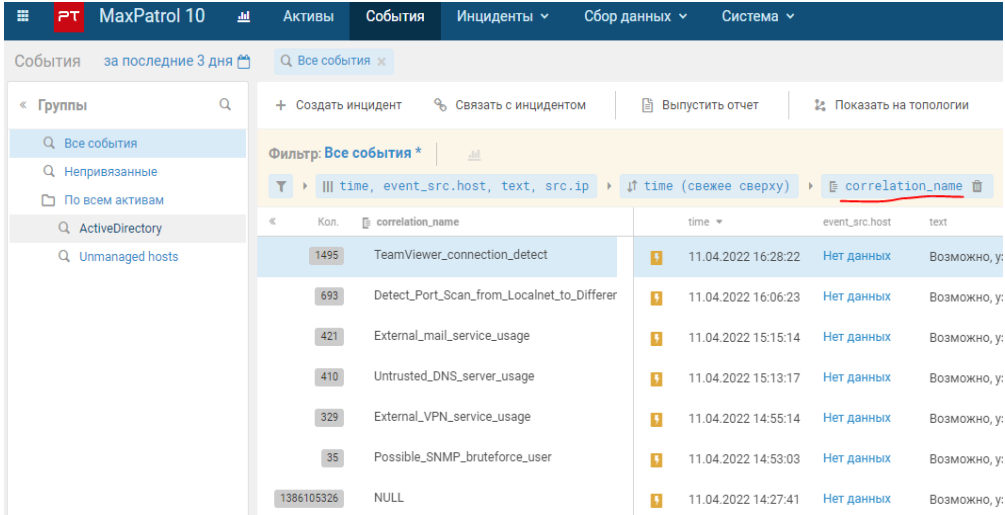
Идентификатор: PT-TL-140
Источник: Positive Technologies
Папка: Сетевые устройства. Подозрительная сетевая активность/tabular_lists
Наборы для установки: не задано
Статус установки:
Статус валидации:

[+](#) Добавить запись [✎](#) Редактировать [🗑](#) Удалить [▶](#) Активировать [▶](#) Деактивировать [📄](#) Импорт [📄](#) Экспорт

service_type	src_subnet	src_ip	dst_subnet	dst_ip	Источник
MAIL					
MAIL					
VPN	null	null	null		
DNS			172.16.0.0/12		
DNS			192.168.0.0/16		
DNS			10.0.0.0/8		
VPN			172.16.0.0/12		
VPN			192.168.0.0/16		
VPN			10.0.0.0/8		
MAIL			172.16.0.0/12		
MAIL			192.168.0.0/16		
MAIL			10.0.0.0/8		

- Встроенные внутренние подсети
- (null, *, пустое поле) = любое значение
- Для некоторых правил корреляции возможно добавление исключения в MPSIEM прямо из интерфейса просмотра события

Группировки полей



События за последние 3 дня

Фильтр: Все события *

time, event_src.host, text, src.ip

time (свежее сверху)

correlation_name

Кол.	correlation_name	time	event_src.host	text
1495	TeamViewer_connection_detect	11.04.2022 16:28:22	Нет данных	Возможно, у;
693	Detect_Port_Scan_from_Localnet_to_Differer	11.04.2022 16:06:23	Нет данных	Возможно, у;
421	External_mail_service_usage	11.04.2022 15:15:14	Нет данных	Возможно, у;
410	Untrusted_DNS_server_usage	11.04.2022 15:13:17	Нет данных	Возможно, у;
329	External_VPN_service_usage	11.04.2022 14:55:14	Нет данных	Возможно, у;
35	Possible_SNMP_bruteforce_user	11.04.2022 14:53:03	Нет данных	Возможно, у;
1386105326	NULL	11.04.2022 14:27:41	Нет данных	Возможно, у;

- Фильтрация событий и группировка по полям позволяет максимально эффективно выявить наиболее активные фолзющие хосты и учетные записи
- Наглядно видны подсети, на которые нужно обратить внимание

Группировки полей

Фильтр: Все события * |

correlation_name = "TeamViewer_connec... | time, event_src.host, text, src.ip | time (свежее сверху) | src.ip

< Кол. src.ip

472	10.144.	
472	10.144.	
464	10.144.	
10		
10		
4		
3		
—		

Группировки полей

Фильтр: Все события * |

correlation_name = "Untrusted_DNS_ser..." | time, event_src.host, text, src.ip | time (свежее сверху)

dst.ip, src.ip |

< Кол. dst.ip, src.ip

358	dst.ip	8.8.8.8
	src.ip	
13	dst.ip	8.8.8.8
	src.ip	
11	dst.ip	8.8.8.8
	src.ip	
8	dst.ip	8.8.8.8
	src.ip	
8	dst.ip	8.8.8.8
	src.ip	
5	dst.ip	8.8.4.4
	src.ip	
5	dst.ip	8.8.8.8
	src.ip	
2	dst.ip	8.8.8.8
	src.ip	

- Инвентаризация и выявление сущностей (узел, подсеть, учётка), которые могут себя вести не так как все остальные (гостевой wi-fi, техническая УЗ, файловая шара)
- Не пытайтесь объять необъятное – работайте с пакетами и правилами по очереди
- Читайте документацию
- Тесное взаимодействие с ИТ
- Ответьте на вопрос:
«Как мы хотим использовать SIEM?»

Количество инцидентов последние 24 часа

17:38 ⋮

—0

Спасибо за внимание