



Обзор пакета экспертизы для безопасной удалёнки

Антон Исаев

Эксперт отдела мониторинга событий ИБ

Станислав Черкасов

Менеджер по продвижению продуктов

Наталья Казанькова

Менеджер по продуктовому маркетингу

ptsecurity.com

План вебинара



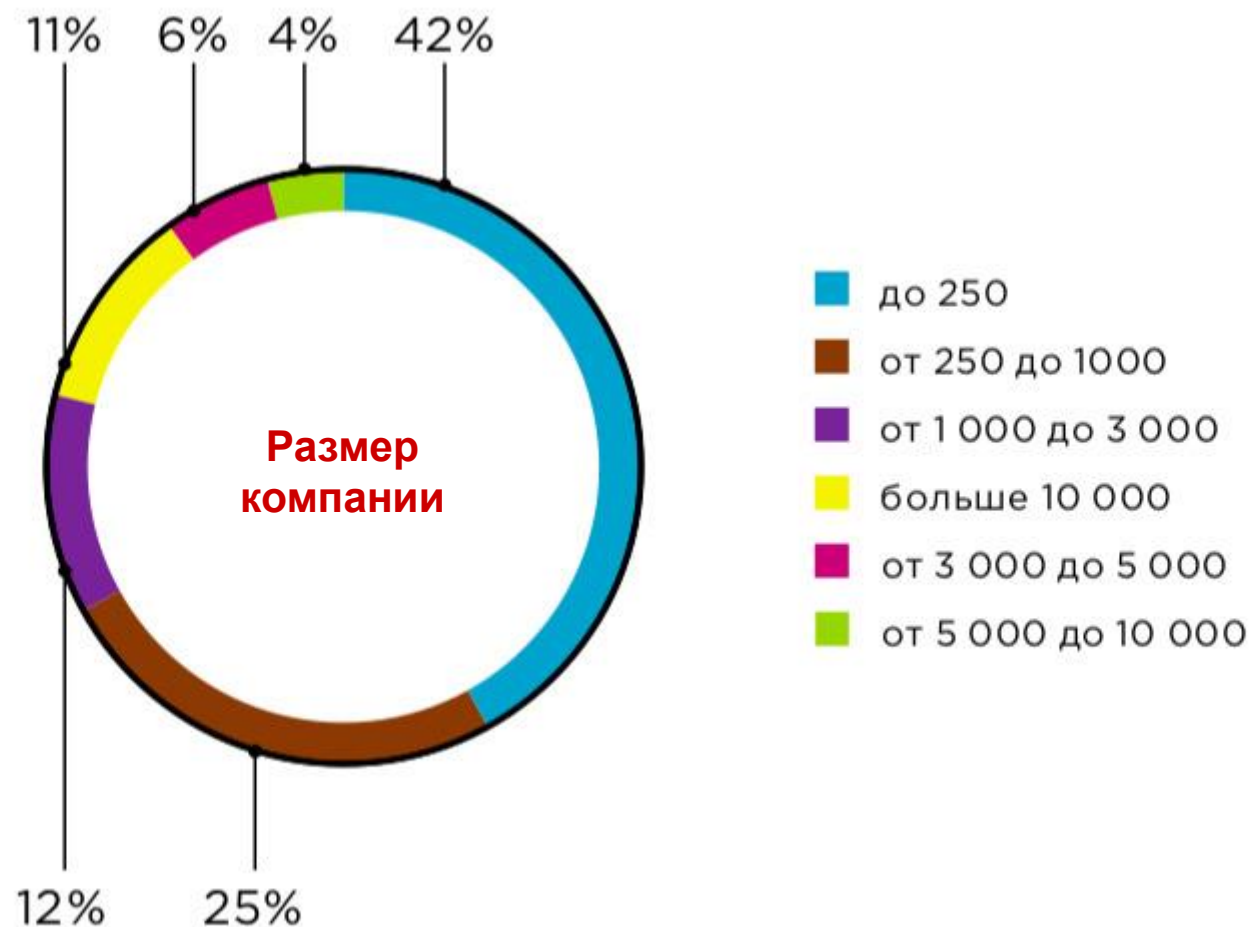
1. Результаты опроса, как устроена удаленка в компаниях
2. Пакеты экспертизы MaxPatrol SIEM и работа с ними
3. Примеры работы пакета для удаленной работы
4. Разбор примеров инцидентов
5. Обзор правил, входящих в пакет экспертизы для удаленки



Что показал опрос специалистов по ИБ и IT

Респонденты

776
участников



Кто был готов к удаленке



Удаленный режим работы был организован еще до карантина в:

63% IT-компаний

54% телеком компаний

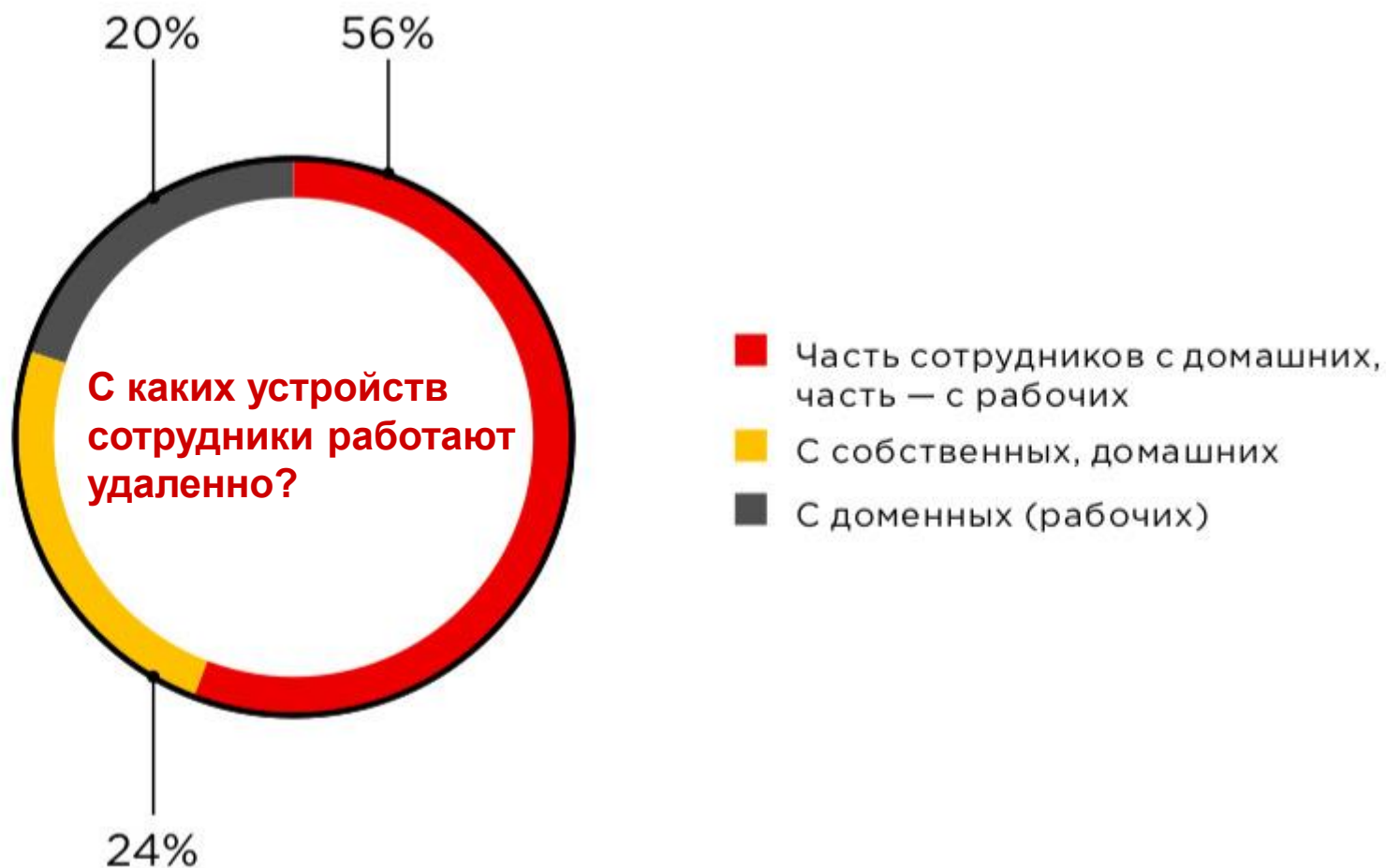
46% банков

32% промышленных компаний

26% ТЭК

24% госструктур

Работа с домашних устройств



Самые защищенные отрасли

Доля компаний, в которых сотрудники работают с корпоративных устройств

26% в IT-отрасли

23% в финансах

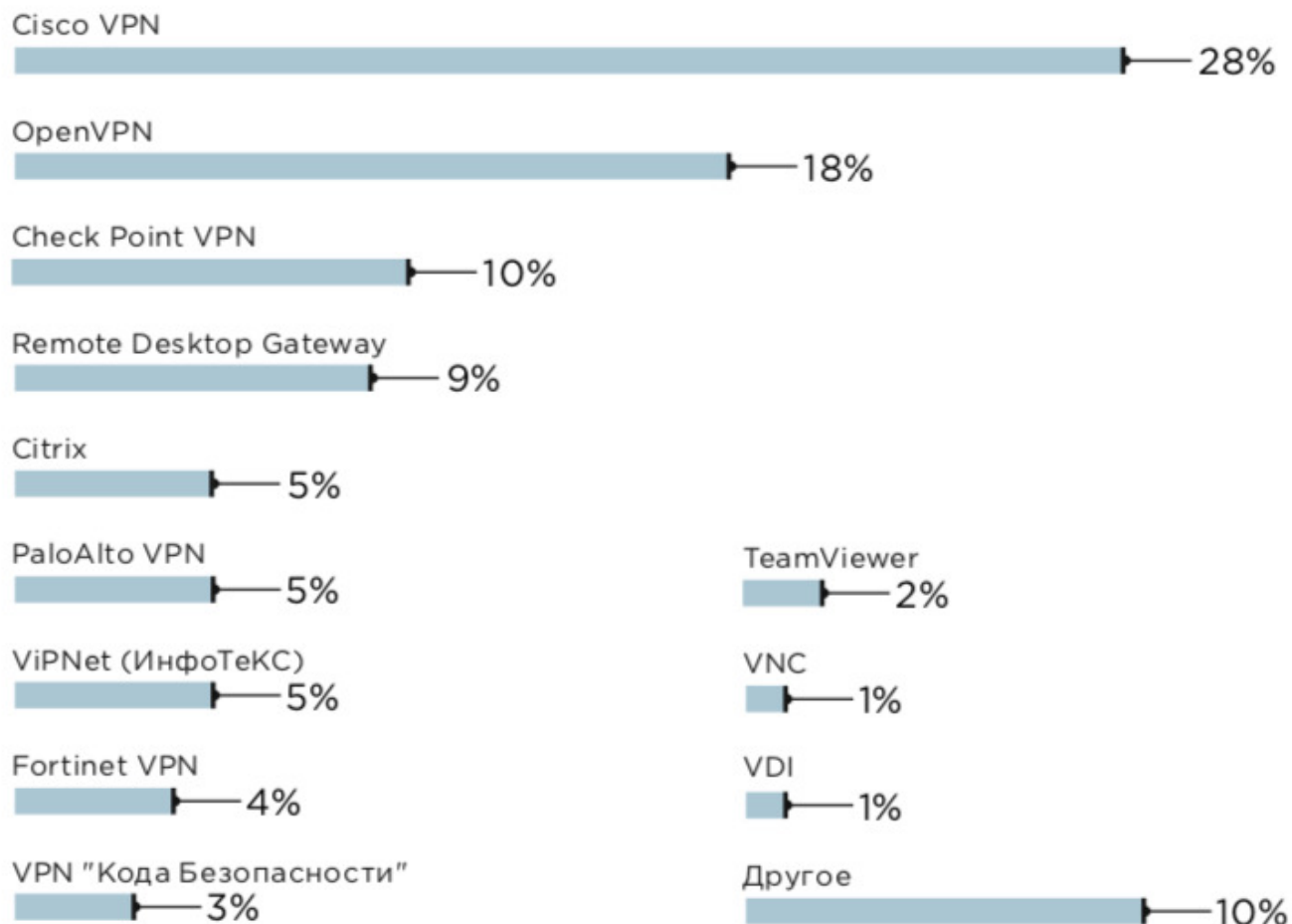
Антирейтинг:

11% в промышленности

Топ ПО в крупных компаниях



Какими способами организована удаленная работа в вашей компании?

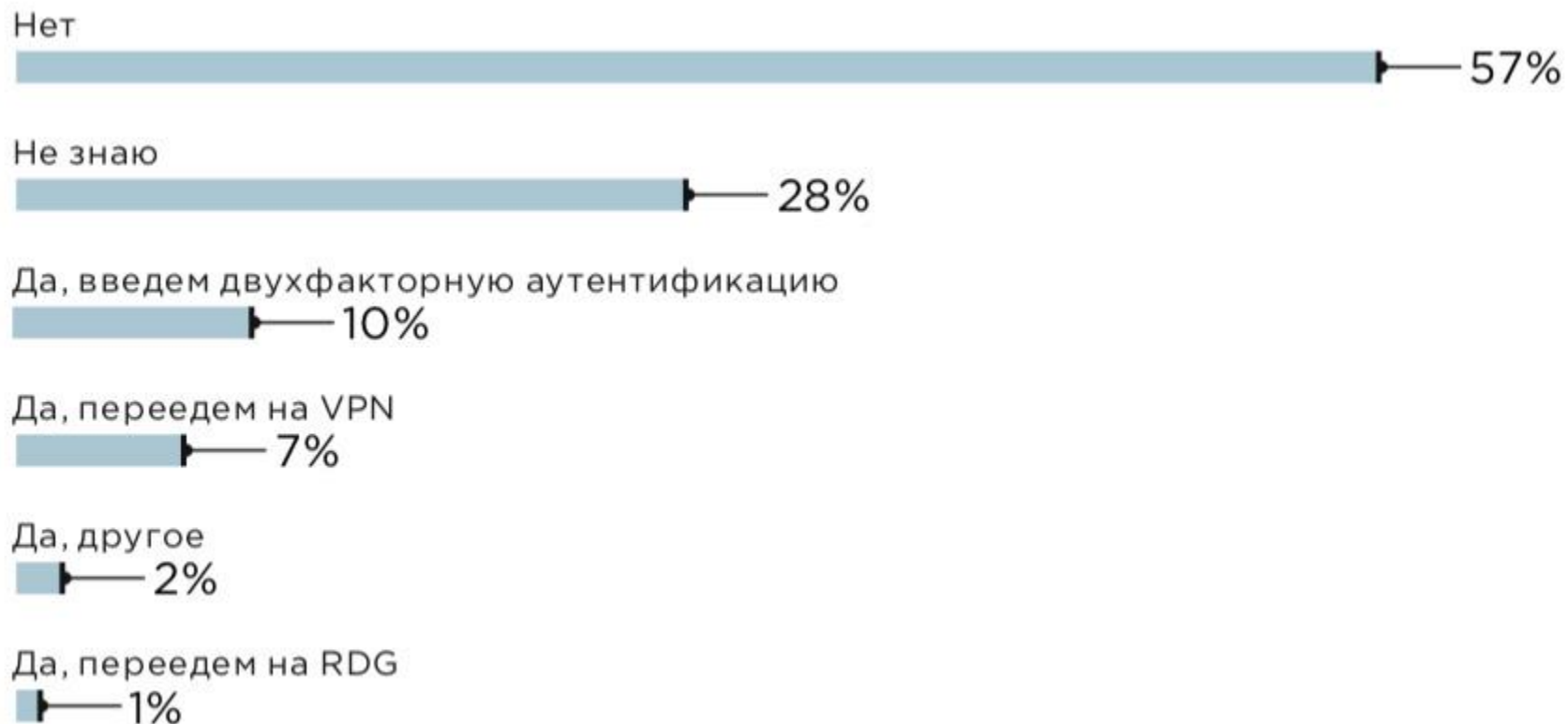


OpenVPN, Check Point и RDG содержат критически опасные уязвимости. Подробности в отчете: ptsecurity.com/ru-ru/research/analytics/remote-work-in-russia-and-the-cis-2020/

MaxPatrol SIEM выявляет аномалии в сети с использованием OpenVPN, RDG, межсетевых экранов Cisco ASA, Check Point и Palo Alto

Что изменится

Планируете что-то менять в организации удаленки в ближайшие месяцы?



РТ и актуальные тренды ИБ



- Следим за происходящим
- Проводим исследования
- Выпускаем внеочередные пакеты экспертизы

РТ КВ и пакеты экспертизы



Как это работает:

1. Новые пакеты подтягиваются из облака
2. Вы выбираете, что актуально для вас
3. Формируете свой набор данных
4. Работаете с выбранными пакетами

The screenshot displays the PT Knowledge Base interface. On the left, a sidebar shows a tree view of folders including 'ATT&СК: «Выполнен...', 'ATT&СК: «Закрепле...', 'ATT&СК: «Перемещ...', 'ATT&СК: «Разведка', 'Active Directory. Под...', 'Linux. Подозритель...', 'Microsoft SQL Server', and 'Oracle Database'. The 'Oracle Database' folder is expanded, showing sub-folders like 'correlation_rules', 'enrichment_rules', and 'tabular_lists'. Below this, there are 'Наборы для установки' (Installation sets) including 'Все объекты', 'Вне наборов', 'Production', and 'SIEM+NAD demo'. The main area shows a table of expert packages for 'Oracle Database'. The table has columns for '№', 'С...', 'Идентификатор', 'Системное название', 'Описание', 'Источник', and 'Папка'. The table lists 16 packages, each with a status icon (green checkmark or red X) and a link to the package details.

№	С...	Идентификатор	Системное название	Описание	Источник	Папка
1		PT-TL-107	Oracle_tables_with_hashes	Названия таблиц Oracle Database, для которых отслеживае...	↓	Oracle Database/tabular_lists
2		PT-TL-106	Oracle_audit_tables	Названия таблиц Oracle Database, для которых отслеживаю...	↓	Oracle Database/tabular_lists
3	✓	PT-CR-12	Oracle_privilege_decoding	Расшифровка кодов привилегий из СУБД Oracle	↓	Oracle Database/enrichment_rules
4	✓	PT-CR-285	Oracle_Select_table_with_hash	Чтение записей из таблиц, содержащих хеши паролей	↓	Oracle Database/correlation_rules
5	✓	PT-CR-284	Oracle_listener_version_check	Выполнение команды VERSION в Oracle Listener	↓	Oracle Database/correlation_rules
6	✓	PT-CR-283	Oracle_listener_instance_guessing	Потенциальная попытка подобрать экземпляр СУБД Oracle	↓	Oracle Database/correlation_rules
7	✓	PT-CR-282	Oracle_audit_truncate	Очистка таблицы аудита	↓	Oracle Database/correlation_rules
8	✓	PT-CR-281	Oracle_audit_entry_update	Изменение записей в таблице аудита	↓	Oracle Database/correlation_rules
9	✓	PT-CR-280	Oracle_audit_entry_insert	Вставка записей в таблицу аудита	↓	Oracle Database/correlation_rules
10	✓	PT-CR-279	Oracle_audit_entry_delete	Удаление записей из таблицы аудита	↓	Oracle Database/correlation_rules
11	✓	PT-CR-278	Oracle_audit_drop	Удаление таблицы аудита	↓	Oracle Database/correlation_rules
12	✓	PT-CR-277	Oracle_audit_disable_via_noaudit	Журнал аудита в СУБД Oracle отключен из-за выполнения ко...	↓	Oracle Database/correlation_rules
13	✓	PT-CR-276	Oracle_audit_disable_via_drop_policy	Журнал аудита в СУБД Oracle отключен из-за удаленной поли...	↓	Oracle Database/correlation_rules
14	✓	PT-CR-275	Oracle_audit_disable_via_disable_policy	Журнал аудита в СУБД Oracle отключен из-за отключения по...	↓	Oracle Database/correlation_rules
15	✓	PT-CR-274	Oracle_audit_disable_for_sysdba	Журнал аудита отключен для пользователей с привилегией S...	↓	Oracle Database/correlation_rules
16	✓	PT-CR-273	Oracle_audit_disable	Журнал аудита отключен в СУБД Oracle	↓	Oracle Database/correlation_rules

Пример работы

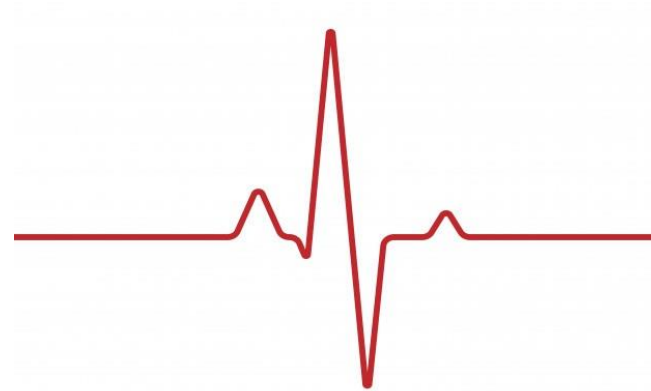


- Работаем с пакетом экспертизы
- Изучаем описание
- Понимаем содержимое
- Настраиваем источники
- Заполняем табличные списки
- Расследуем инциденты

РТ КВ и пакеты экспертизы

РТ

Live Demo

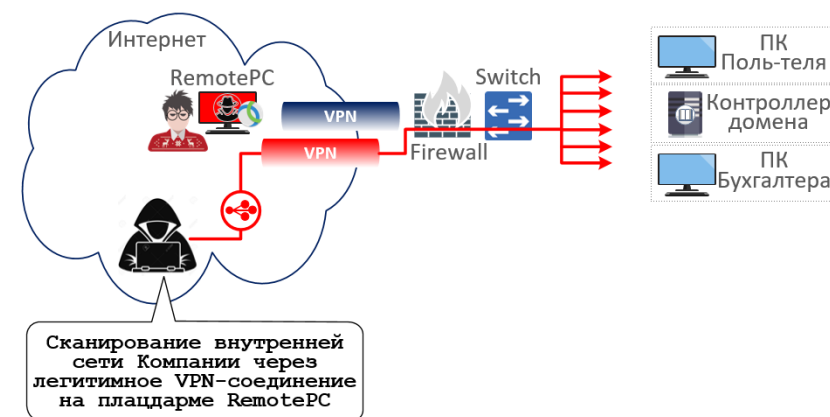


Разбор полетов



Что происходит:

1. Домашний компьютер сотрудника скомпрометирован
2. Злоумышленник использует его тоннель с целью проникновения в инфраструктуру
3. MaxPatrol SIEM позволяет выявить факт несанкционированного доступа



Работа с инцидентами

РТ

Live Demo

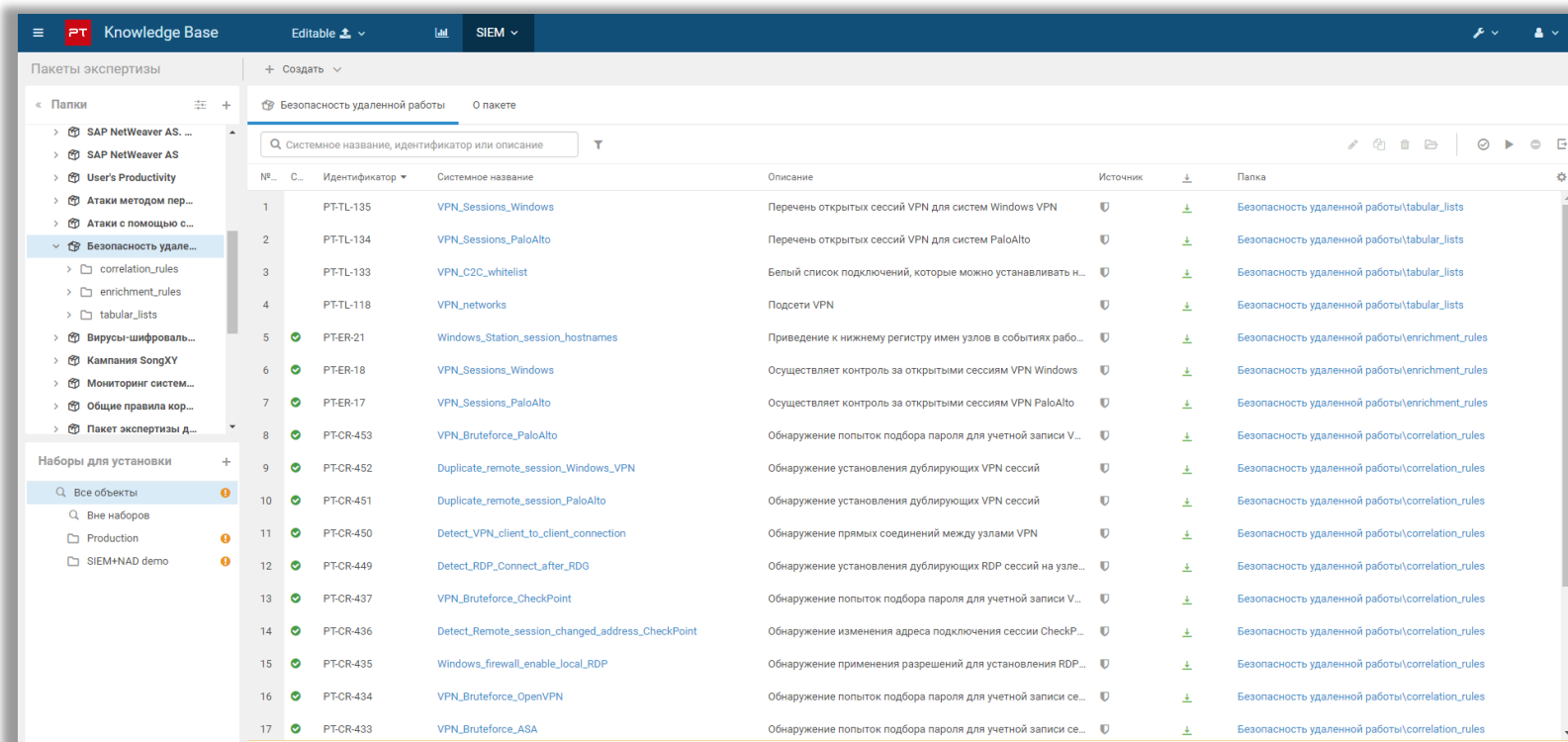


Состав пакета экспертизы под удаленную работу

PT

Из чего состоит:

1. Правила корреляции для большинства популярных ситуаций
2. Табличные списки для сбора и предоставления данных
3. Правила обогащения для более ясной картины событий



The screenshot displays the PT Knowledge Base interface, specifically the 'Пакеты экспертизы' (Expertise Packages) section. The left sidebar shows a tree view of packages, with 'Безопасность удаленной работы' (Remote Work Security) selected. The main area shows a table of rules for this package.

№	C..	Идентификатор	Системное название	Описание	Источник	Панка
1		PT-TL-135	VPN_Sessions_Windows	Перечень открытых сессий VPN для систем Windows VPN	У	Безопасность удаленной работы\tabular_lists
2		PT-TL-134	VPN_Sessions_PaloAlto	Перечень открытых сессий VPN для систем PaloAlto	У	Безопасность удаленной работы\tabular_lists
3		PT-TL-133	VPN_C2C_whitelist	Белый список подключений, которые можно устанавливать н...	У	Безопасность удаленной работы\tabular_lists
4		PT-TL-118	VPN_networks	Подсети VPN	У	Безопасность удаленной работы\tabular_lists
5	✓	PT-ER-21	Windows_Station_session_hostnames	Приведение к нижнему регистру имен узлов в событиях рабо...	У	Безопасность удаленной работы\enrichment_rules
6	✓	PT-ER-18	VPN_Sessions_Windows	Осуществляет контроль за открытыми сессиям VPN Windows	У	Безопасность удаленной работы\enrichment_rules
7	✓	PT-ER-17	VPN_Sessions_PaloAlto	Осуществляет контроль за открытыми сессиям VPN PaloAlto	У	Безопасность удаленной работы\enrichment_rules
8	✓	PT-CR-453	VPN_Bruteforce_PaloAlto	Обнаружение попыток подбора пароля для учетной записи V...	У	Безопасность удаленной работы\correlation_rules
9	✓	PT-CR-452	Duplicate_remote_session_Windows_VPN	Обнаружение установления дублирующих VPN сессий	У	Безопасность удаленной работы\correlation_rules
10	✓	PT-CR-451	Duplicate_remote_session_PaloAlto	Обнаружение установления дублирующих VPN сессий	У	Безопасность удаленной работы\correlation_rules
11	✓	PT-CR-450	Detect_VPN_client_to_client_connection	Обнаружение прямых соединений между узлами VPN	У	Безопасность удаленной работы\correlation_rules
12	✓	PT-CR-449	Detect_RDP_Connect_after_RDP	Обнаружение установления дублирующих RDP сессий на узле...	У	Безопасность удаленной работы\correlation_rules
13	✓	PT-CR-437	VPN_Bruteforce_CheckPoint	Обнаружение попыток подбора пароля для учетной записи V...	У	Безопасность удаленной работы\correlation_rules
14	✓	PT-CR-436	Detect_Remote_session_changed_address_CheckPoint	Обнаружение изменения адреса подключения сессии CheckP...	У	Безопасность удаленной работы\correlation_rules
15	✓	PT-CR-435	Windows_firewall_enable_local_RDP	Обнаружение применения разрешений для установления RDP...	У	Безопасность удаленной работы\correlation_rules
16	✓	PT-CR-434	VPN_Bruteforce_OpenVPN	Обнаружение попыток подбора пароля для учетной записи се...	У	Безопасность удаленной работы\correlation_rules
17	✓	PT-CR-433	VPN_Bruteforce_ASA	Обнаружение попыток подбора пароля для учетной записи се...	У	Безопасность удаленной работы\correlation_rules

Подытожим



- Мир меняется, удаленная работа – лишь один из прецедентов
- Мы здесь, чтобы вместе реагировать на актуальные события
- Успех возможен только при совместной работе

Демо новой версии MaxPatrol SIEM



18 июня —
запуск 6-й версии MaxPatrol SIEM

Детали: t.me/MPSIEMChat

Что дальше:



Посмотреть вебинар про детект сетевых аномалий:
ptsecurity.com/ru-ru/research/webinar/310423/

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