



От разовых проверок к постоянной защите

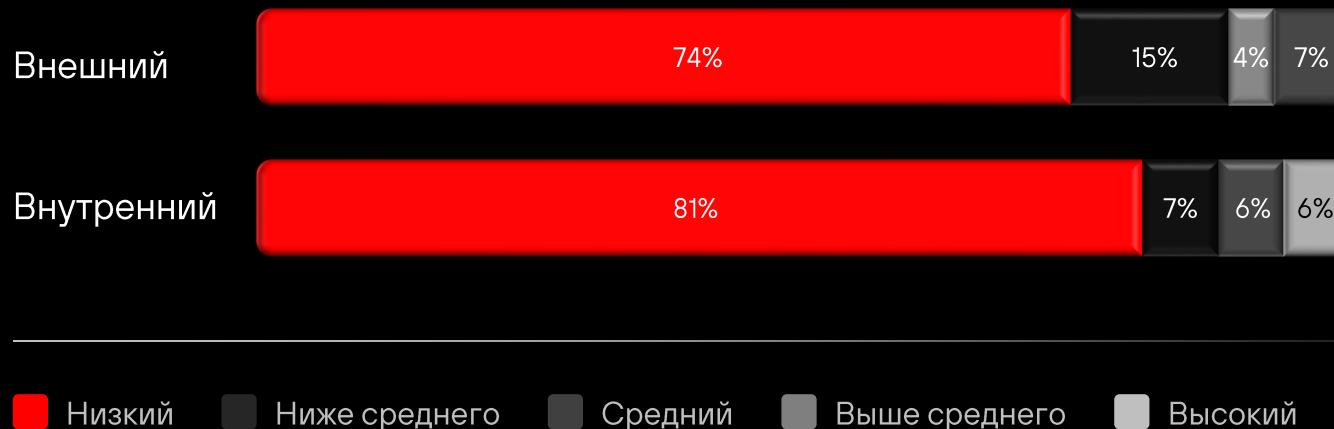
Как автопентест меняет подход
к безопасности инфраструктуры

Родион Тульский
Менеджер по развитию бизнеса

Тестирование на проникновение —

один из самых объективных способов оценки защищенности

Уровень защищенности информационных систем по результатам пентестов



9 отраслей

в выборке исследования

74–81% систем

имеют низкий уровень защищенности
вне зависимости от отрасли

Чем заканчиваются пентесты



В ходе проведения работ исследователями было верифицировано 90% недопустимых событий, обозначенных клиентами дополнительно

Среди таких событий были, например:

- привилегированный доступ к целевым системам,
- утечка кодовой базы или ее безвозвратная потеря,
- хищение определенной информации или ее компрометация,
- вывод денежных средств или получение финансовой выгоды путем, не заложенным в логику приложения.

10%

не реализовано

90%

реализовано



Оценивать защищенность инфраструктуры все сложнее

Инфраструктура
постоянно меняется

**в 79%
компаний**

изменения в ИТ-среде
происходят чаще, чем раз в квартал

Количество СЗИ
растет

**только 20%
компаний**

используют
меньше десяти СЗИ

Ландшафт киберугроз
становится более изощренным

на 35%

может вырасти количество
успешных кибератак на российские
компании в 2026 году

Что такое PT Dephaze



Автопентест для оценки уровня защищенности
внутренней инфраструктуры



Атакуем контролируемо

Даем возможность управлять согласованием и интенсивностью атак, исключениями области тестирования и прозрачно показываем все атакующие действия

ВНЕДРЕНИЕ ЗА ОДИН ЧАС



Помогаем оценить и исправить

Говорим, какие атаки должны обнаруживать ваши средства защиты, где были небезопасные пароли, как пропатчить системы и изменить небезопасные конфигурации. Для удобства оформляем это в отчет

FALSE POSITIVE = 0



Регулярно пополняем набор атак

Используем в продукте двадцатилетнюю экспертизу и опыт Positive Technologies в тестировании на проникновение, расследованиях и разведке техник атакующих

ПЕРВЫЕ РЕЗУЛЬТАТЫ ЗА ОДИН ЧАС

Ключевые сценарии применения PT Dephaze



Регулярная оценка защищенности

После обновления ПО, изменений в сети или внедрения систем PT Dephaze запускается, чтобы проверить, не появились ли новые уязвимости или ошибки конфигураций



Проверка эффективности СЗИ

После изменения или обновления средств защиты (NGFW, EDR, XDR, NAC и других систем) PT Dephaze запускается, чтобы проверить, способны ли они обнаружить и предотвратить реальные атаки



Обучение и тестирование SOC

PT Dephaze используется для тренировки аналитиков SOC и проверки готовности команды к реальным инцидентам

Как использовать PT Dephaze



Триггеры запуска

- Плановое тестирование
- Изменения в ИТ-инфраструктуре
- Обновление продукта

Повторное тестирование
с PT Dephaze
и подтверждение
устранения недостатков



Тестирование
с PT Dephaze

Рекомендации
по устранению
выявленных
недостатков

PT Dephaze в действии



У части ключевых пользователей (из отделов ИТ и ИБ) настройки антивируса были недостаточными, в результате чего PT Dephaze получил доступ к важным учетным данным на узлах



Простая парольная политика позволила получить доступ к почте ключевых сотрудников



Отсутствуют важные события из SIEM-системы, свидетельствующие о компрометации



Полностью скомпрометирован домен, а значит, есть возможность полностью зашифровать все устройства



PT Dephaze vs SIEM-система



1

Экспертиза PT Dephaze:

- Повышение привилегий учетной записи через уязвимость в службе сертификатов Active Directory (ESC1)
- Получение информации об учетных записях Active Directory через LDAP-запросы к контроллеру домена
- Эксфильтрация учетных данных из LAPS

2

Правила корреляции в SIEM-системе:

- Cert_Request_And_Approved_With_Alt_SAN
- Cert_Allowed_Alt_SAN
- LDAP_Discovery
- LAPS_Enumeration

3

На что обратить внимание:

- Есть ли активы не покрытые SIEM-системой (shadow IT)?
- Журналы не идут с узла, который был пробит за счет PT Dephaze
- Журналы с узла идут, но не все (отключено расширенное журналирование)
- Корреляционные правила отключены (отключили временно и забыли включить)
- Некорректный белый список может стать причиной отсутствия необходимых корреляций

PT Dephaze vs NTA-система



1

Экспертиза PT Dephaze:

- Проверка возможности выполнения RCE через xp_cmdshell в БД MSSQL
- Извлечение учетных данных пользователей из контроллера домена
- Проверка на наличие уязвимости Zerologon

2

Правила обнаружения в NTA-системе:

- ATTACK [PTsecurity] MSSQL xp_cmdshell_*
- ATTACK AD [PTsecurity] Malicious DCSync_*
- ATTACK AD [PTsecurity] Zerologon Probe_*

3

На что обратить внимание:

- Корректно ли заведен сетевой трафик?
- Видна ли полностью активность PT Dephaze?
- Правильность заполненных групп узлов для корректной работы правил обнаружения атак

PT Dephaze vs EDR-система



1

Экспертиза PT Dephaze:

- Повышение привилегий на узле с ОС Windows (CVE-2025-33073)
- Проверка доступа в БД MSSQL для полученных локальных учетных данных
- Выполнение атаки типа «человек посередине» NTLM Relay на протокол SMB

2

Правила обнаружения в EDR-системе:

- CVE_2025_33073_SMB_Client_Elevation
- MSSQL_Password_Brute
- Ntlm_relay_auth

3

На что обратить внимание:

- Все ли активные узлы покрыты EDR- и EPP-системами?
- Правильно выставлены настройки политики EDR-системы?
- На необходимость наличия реагирования (в случае атаки на инфраструктуру)

В результате



Приоритизация
инвестиций
в средства защиты



Устранение популярных
и простых векторов
компрометации

- Изменение сегментации инфраструктуры
- Пересмотр парольной политики
- Изменение параметров СЗИ и политик безопасности



Готовая к атаке команда
SOC



Приходите на стенд,
продемонстрируем
работу, обсудим пилот!

Задай
вопрос
спикеру





Спасибо!



Попробовать PT Derhaze



Канал PT Derhaze
в Telegram