Артем Мелехин
Заместитель директора по развитию бизнеса
инфраструктурных проектов, Positive Technologies

Можно ли посчитать киберустойчивость?

О спикере

Более 20 лет опыта работы в сфере информационной безопасности.

Начал карьеру в дочернем предприятии ФСТЭК, затем работал в крупнейших вендорах: Positive Technologies, «Лаборатории Касперского»,развивал MSSP в «МегаФоне». Вернулся в Positive Technologies.

Сейчас продвигаю в массы подход к определению путей и времени атаки хакера методом анализа ИТ-инфраструктуры.

Задачи бизнеса, ИТ и ИБ

Задача бизнеса

- Приносить прибыль владельцам (акционерам)
- Увеличивать капитализацию компании
- Оказывать услуги населению (государственные компании)

Задача ИТ и ИБ

- Поддерживать стабильную работу бизнес-сервисов
- Внедрять новые сервисы и подходы
- Обеспечивать работу ИТ-инфраструктуры компании
- Защищать ИТ-инфраструктуру от внешних и внутренних воздействий злоумышленников

Что может случиться

Недопустимое событие?!

Логистика

- Взлом систем управления логистикой и отслеживания отправлений
- Махинации с денежными переводами и кража денежных средств
- Отправка поддельных квитанций
- Взлом клиентов через уязвимости в цифровых продуктах и сервисах
- Уничтожение всех операционных и резервных данных
- Остановка работы ПВЗ (пунктов выдачи заказов)

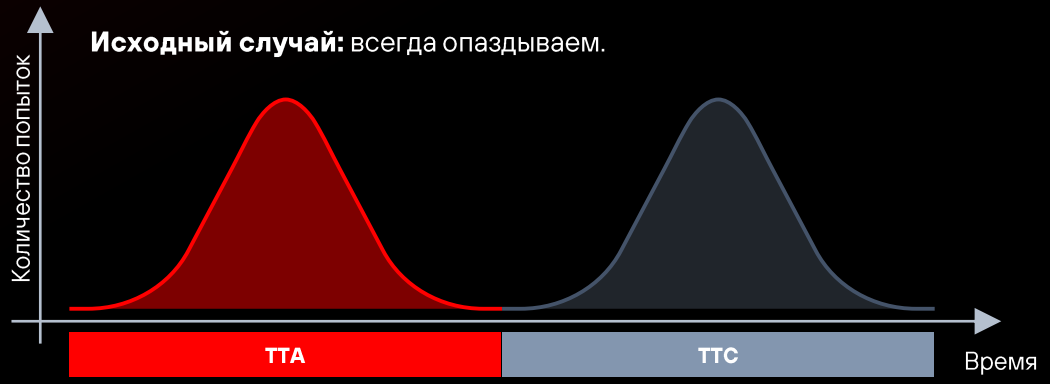
Ритейл

- Остановка автоперевозок из-за сбоя в логистической системе
- Потеря денег из-за кражи баллов лояльности со счетов клиентов
- Остановка деятельности магазинов из-за сбоя в работе касс
- Остановка деятельности магазинов из-за сбоя в работе системы отслеживания маркировки
- Остановка деятельности РЦ (распределительного центра) из-за сбоя в работе ИТ-систем

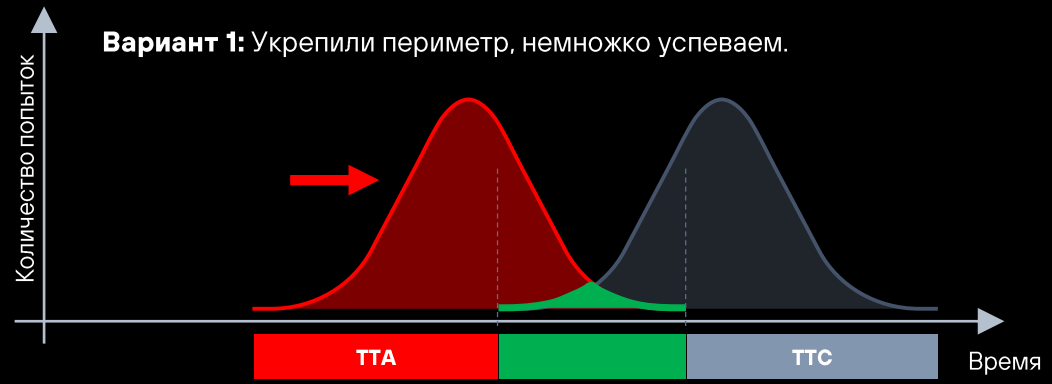
E-commerce

- Вывод денежных средств со счетов компании – общее для всех недопустимое событие
- Остановка деятельности из-за сбоев в работе торговой площадки (онлайн-маркетплейса)
- Остановка деятельности распределительных центров (складов)
- Нарушение управленческих процессов из-за сбоев в работе корпоративной инфраструктуры
- Утрата или искажение информации в базах данных

Подход ХардкорИТ



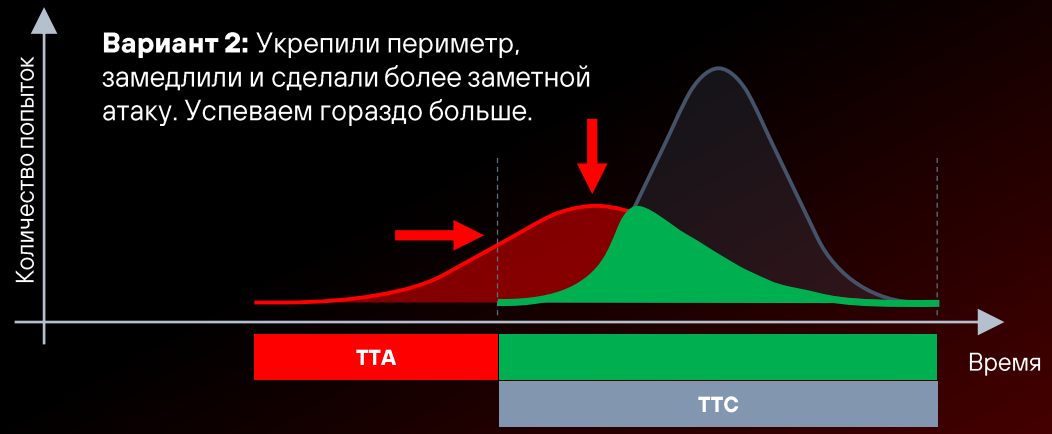
Атакующий всегда достигает своей цели, реагирование происходит слишком поздно.



Замедлили атаку на периметре (атакующему надо долго вести разведку и предпринимать неоднократные попытки проникновения).

Задача — достичь и поддерживать состояние ИТ-инфраструктуры, при котором реализация недопустимого события максимально затруднена преимущественно за счет средств, находящихся в арсенале ИТ (харденинг), а заметность атаки повышается настолько, что реагирование может быть проведено до начала реализации недопустимого события.

Область применения — разные сценарии реализации недопустимого события в ИТ-инфраструктуре.

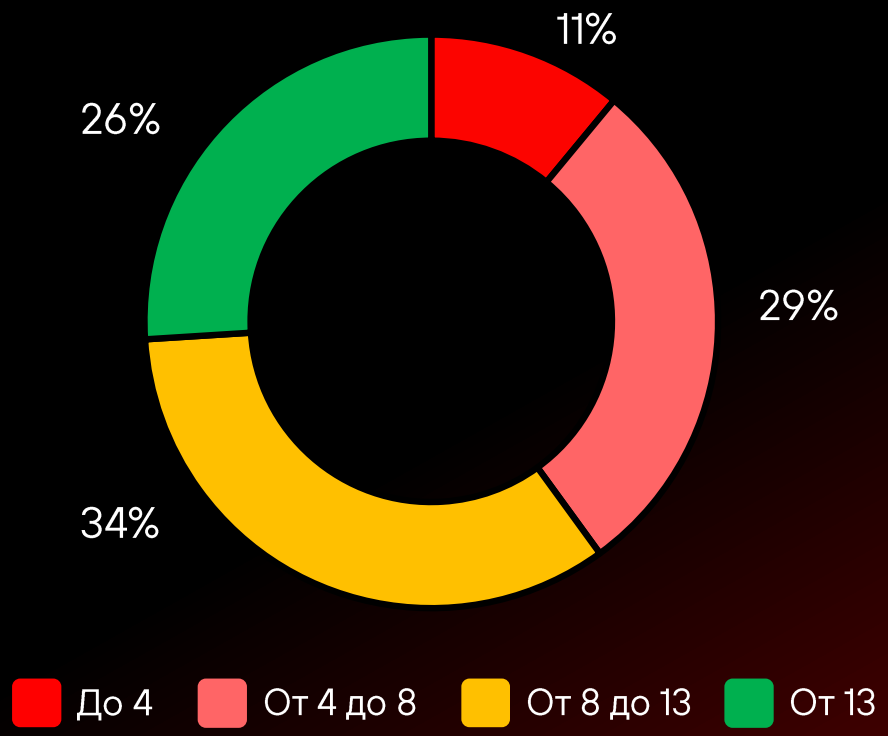


Удлинили и замедлили атаку. Распределение попыток атаки не только сдвинулось вправо, но и «сплющилось»

Предпосылки для перехода к ХардкорИТ

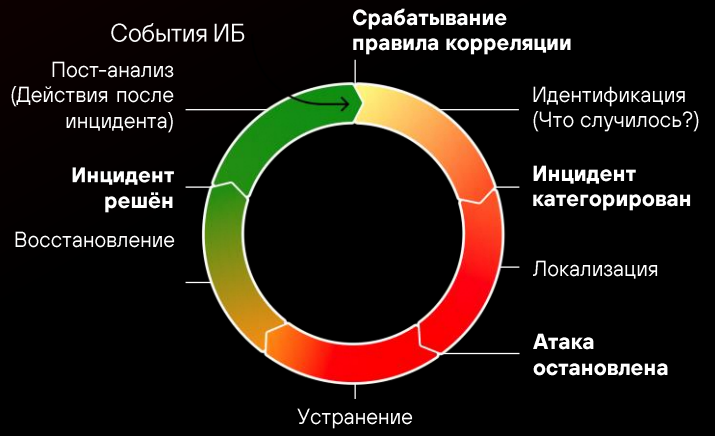
- Слабая парольная политика
- Недостатки конфигураций приложений
- Уязвимости в коде приложений
- Отсутствие актуальных обновлений

Минимальное число шагов для получения максимальных привилегий в домене



https://www.ptsecurity.com/ru-ru/research/analytics/results-of-pentests-2023/#id8

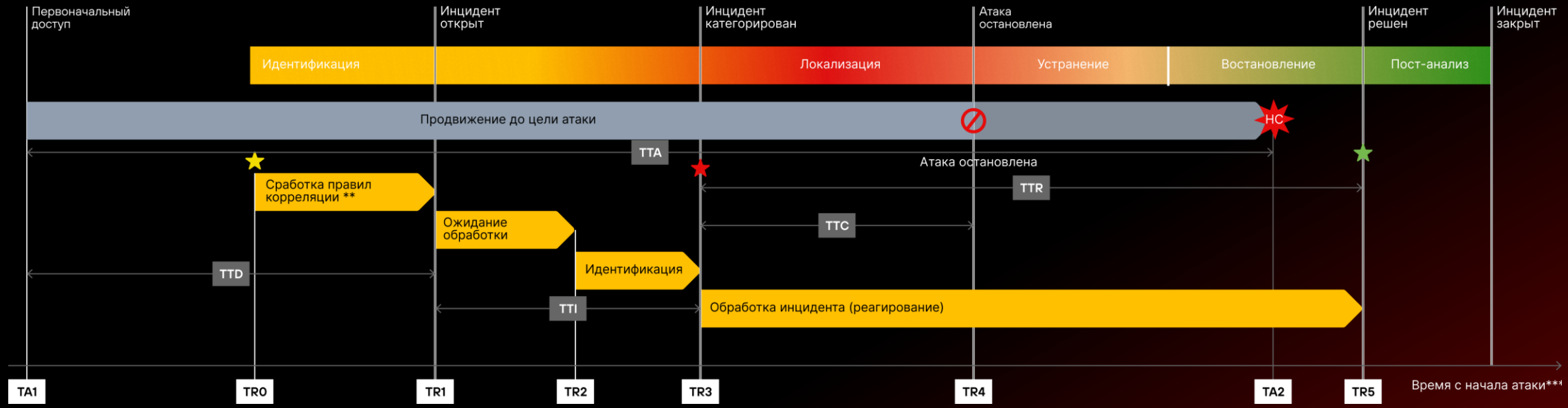
Метрики киберустойчивости



Жизненный цикл инцидента в соответствии с определением реагирования на ИИБ из NIST 800-61 Rev 2*:

- Подготовка
- Идентификация инцидента
- Локализация угрозы
- Устранение угрозы
- Восстановление (снижение последствий реализации угрозы)
- Действия после инцидента

Метрика	Формула вычисления****	Определение
TTD	**TR1-TA1**	Время обнаружения – время от момента первоначального доступа агента угрозы в сеть организации до окончания обнаружения атаки.
TTI	**TR3-TR1**	Время идентификации – время от момента первоначального доступа агента угрозы в сеть организации до определения шагов по реагированию.
TTA	**TA2-TA1**	Время атаки – время от первоначального доступа до момента реализации Недопустимого события.
TTC	**TR4-TR3**	Время локализации – время от категоризации инцидента (т.е. когда становится ясно, что делать) до окончания локализации (блокирования и изоляции агента угрозы).
TTR	**TR5-TR3**	Время реагирования – время от начала локализации до перевода инцидента в статус «Решён».



Примечания:

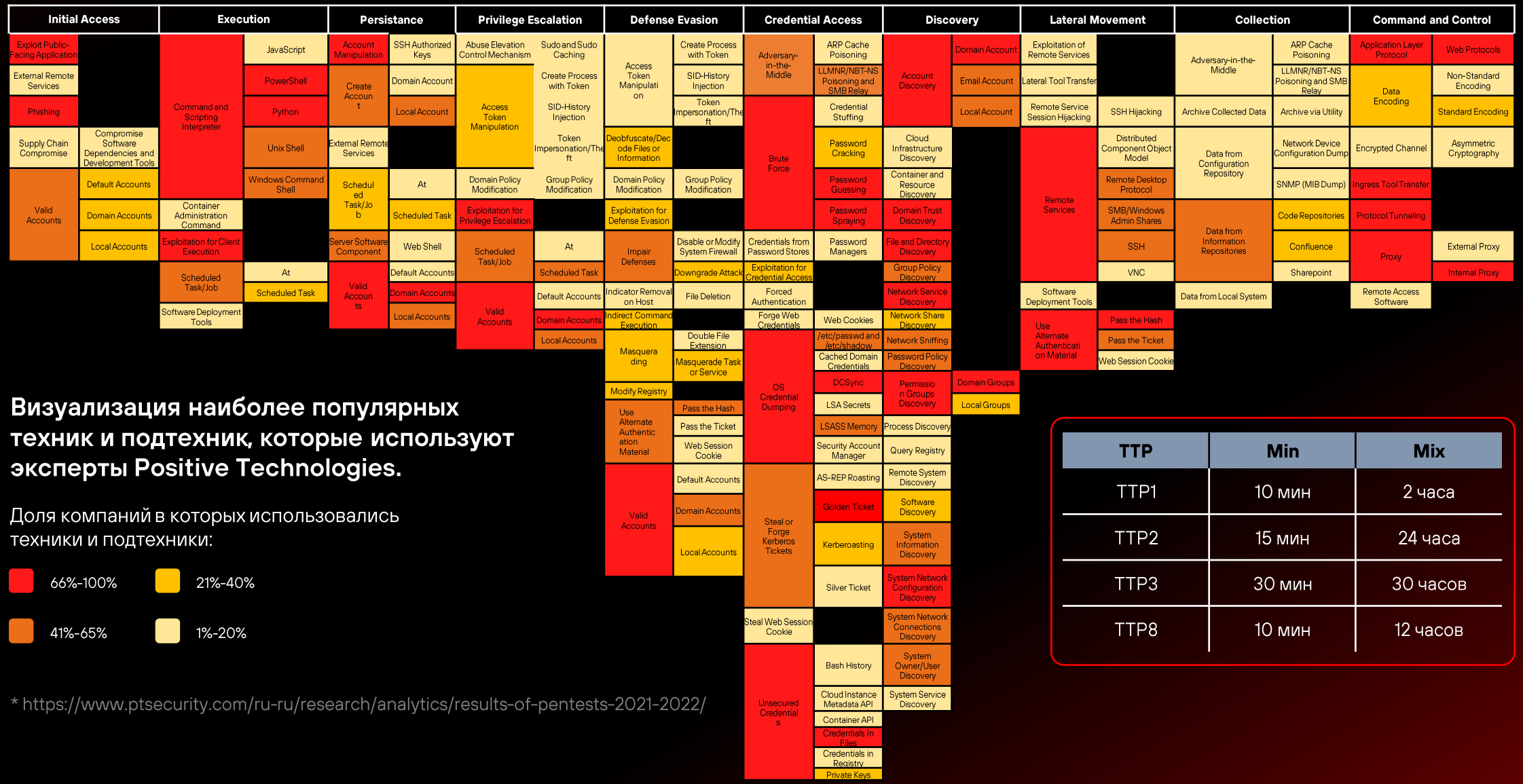
* NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide. nist.gov

** В SIEM или иного другого правила в СЗИ, предназначенного для обнаружения атаки.

*** Длина отрезков на временной шкале не соответствует реальной длительности этапов реагирования на ИИБ и приведена только для иллюстрации общей последовательности этапов и их относительного расположения.

**** Относительно вех на графике

Тепловая карта MITRE ATT&CK



Визуализация наиболее популярных техник и подтехник, которые используют эксперты Positive Technologies.

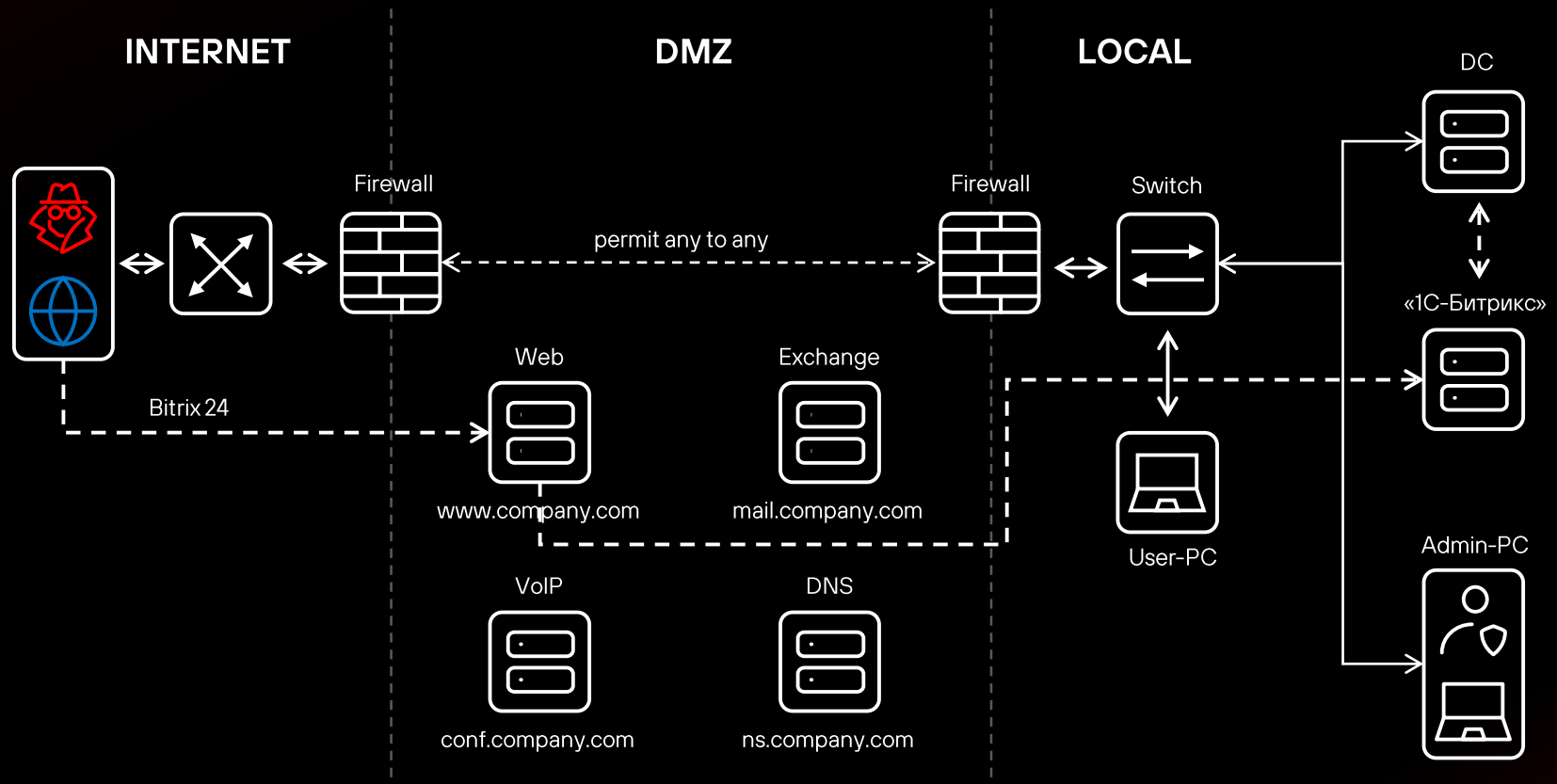
Доля компаний в которых использовались техники и подтехники:

- 66%-100%
- 41%-65%
- 21%-40%
- 1%-20%

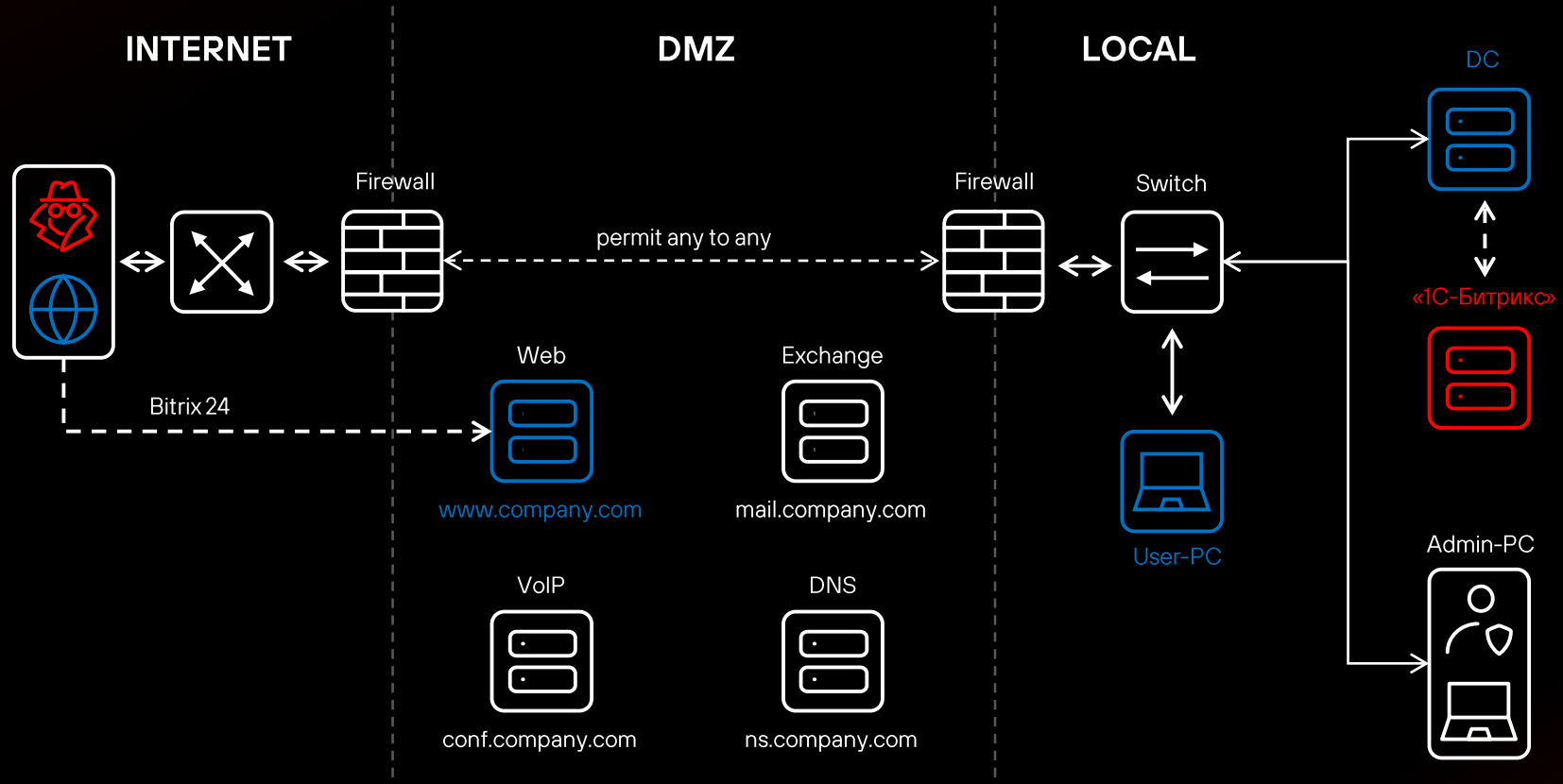
* https://www.ptsecurity.com/ru-ru/research/analytics/results-of-pentests-2021-2022/

TTP	Min	Mix
TTP1	10 мин	2 часа
TTP2	15 мин	24 часа
TTP3	30 мин	30 часов
TTP8	10 мин	12 часов

Пример ИТ-инфраструктуры



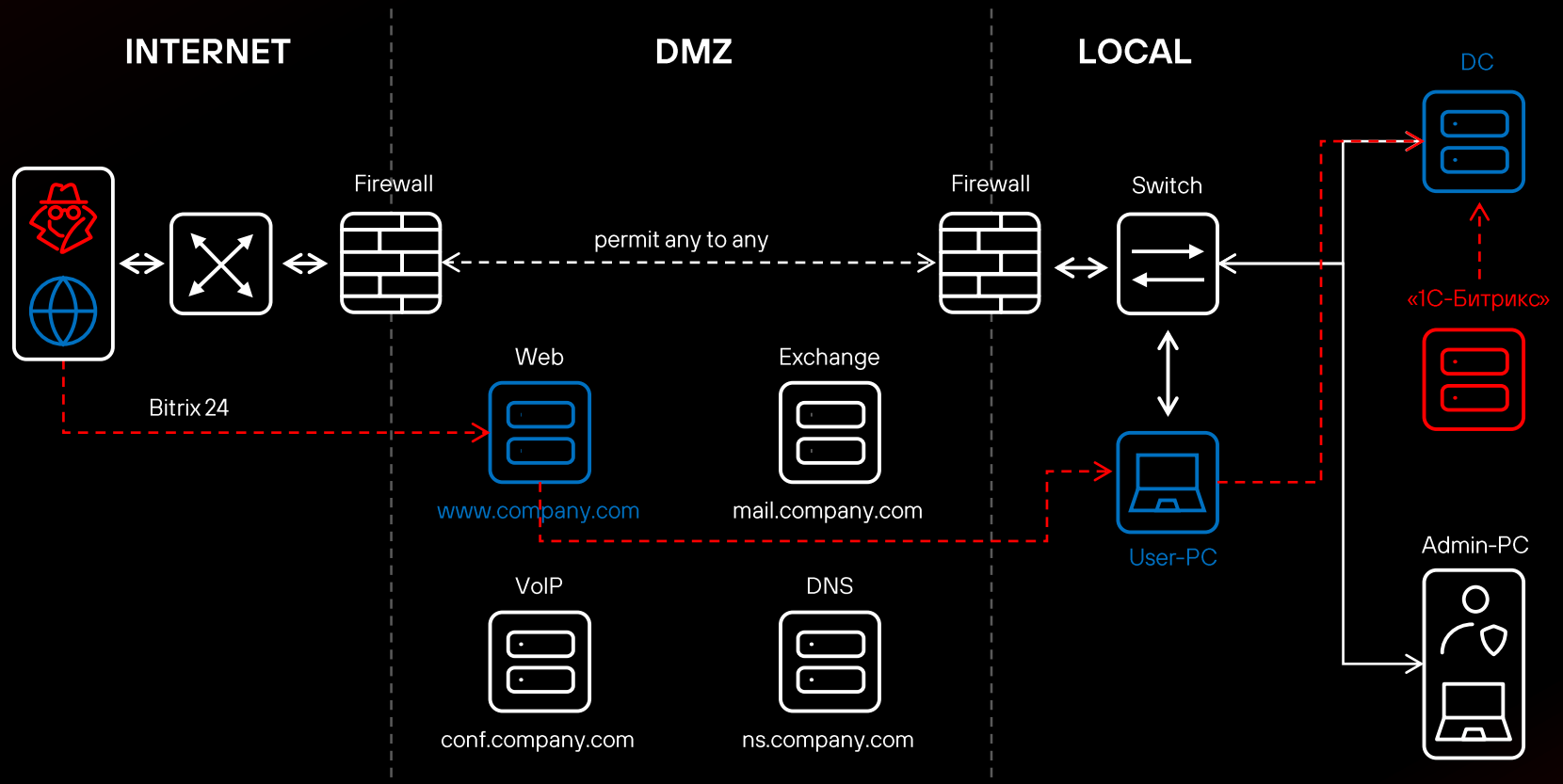
Определение ЦС и КС



Целевая ИС — один или несколько объектов в ИТ-инфраструктуре, воздействие на которые может привести к реализации НС. Как правило, эти объекты являются конечной целью злоумышленника при реализации НС.

Ключевая ИС — объект в ИТ-инфраструктуре, несанкционированный доступ к которому или воздействие на который необходимы нарушителю, чтобы развить атаку на целевую систему, или система, взлом которой существенно упростит сценарий атаки.

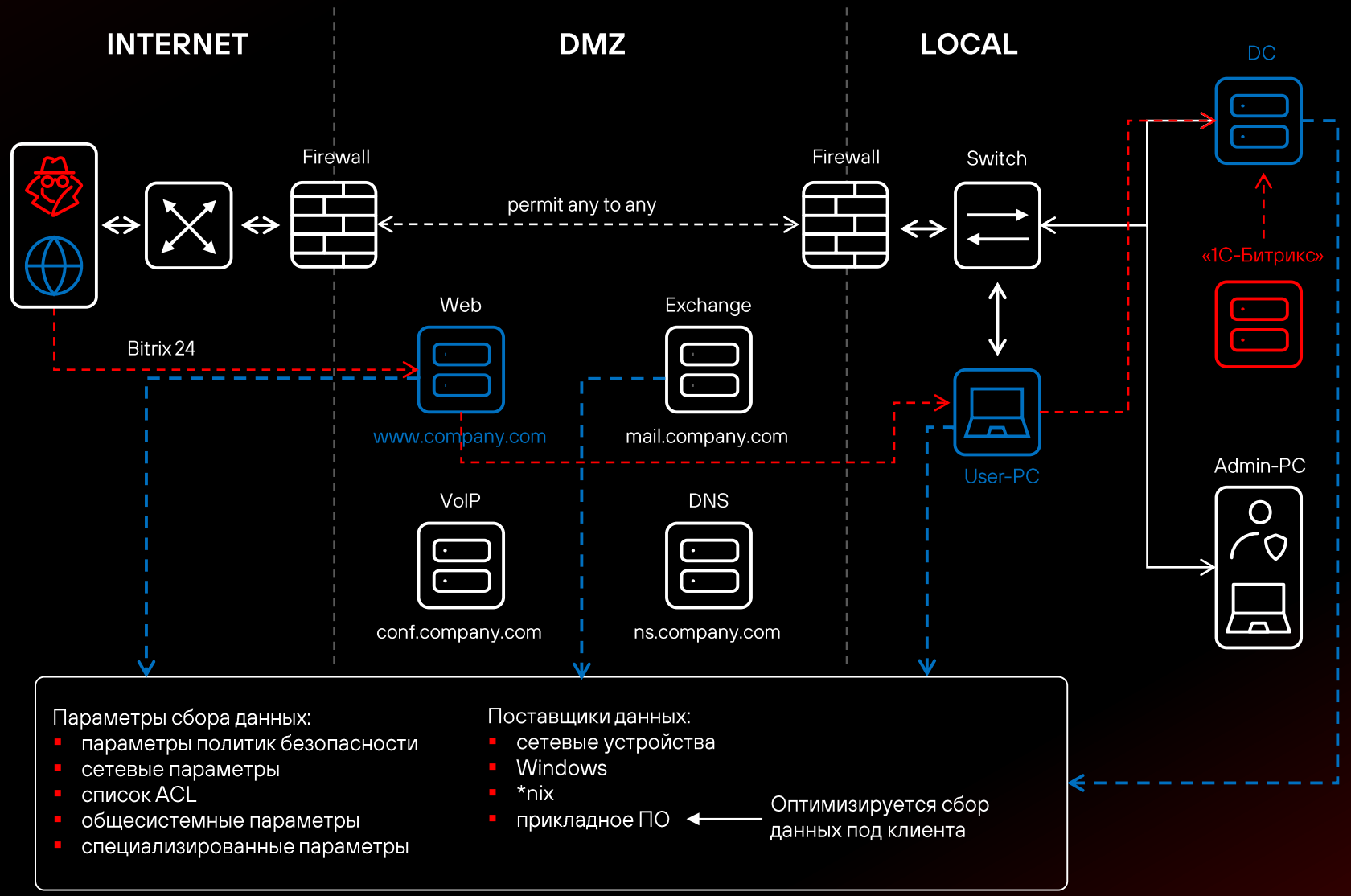
Построение маршрута атаки



Целевая ИС — один или несколько объектов в ИТ-инфраструктуре, воздействие на которые может привести к реализации НС. Как правило, эти объекты являются конечной целью злоумышленника при реализации НС.

Ключевая ИС — объект в ИТ-инфраструктуре, несанкционированный доступ к которому или воздействие на который необходимы нарушителю, чтобы развить атаку на целевую систему, или система, взлом которой существенно упростит сценарий атаки.

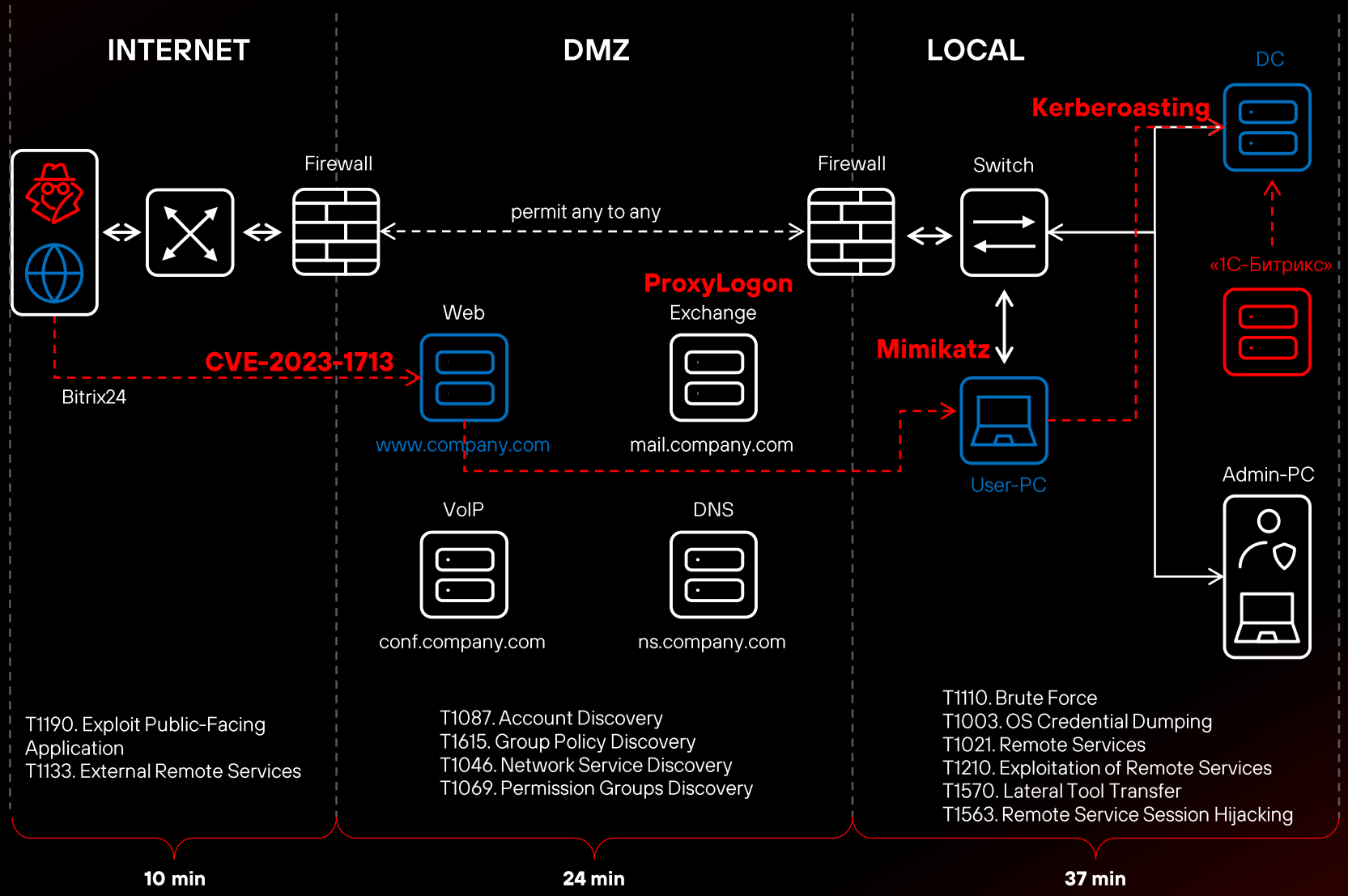
Построение маршрута атаки



Целевая ИС — один или несколько объектов в ИТ-инфраструктуре, воздействие на которые может привести к реализации НС. Как правило, эти объекты являются конечной целью злоумышленника при реализации НС.

Ключевая ИС — объект в ИТ-инфраструктуре, несанкционированный доступ к которому или воздействие на который необходимы нарушителю, чтобы развить атаку на целевую систему, или система, взлом которой существенно упростит сценарий атаки.

Построение маршрута атаки



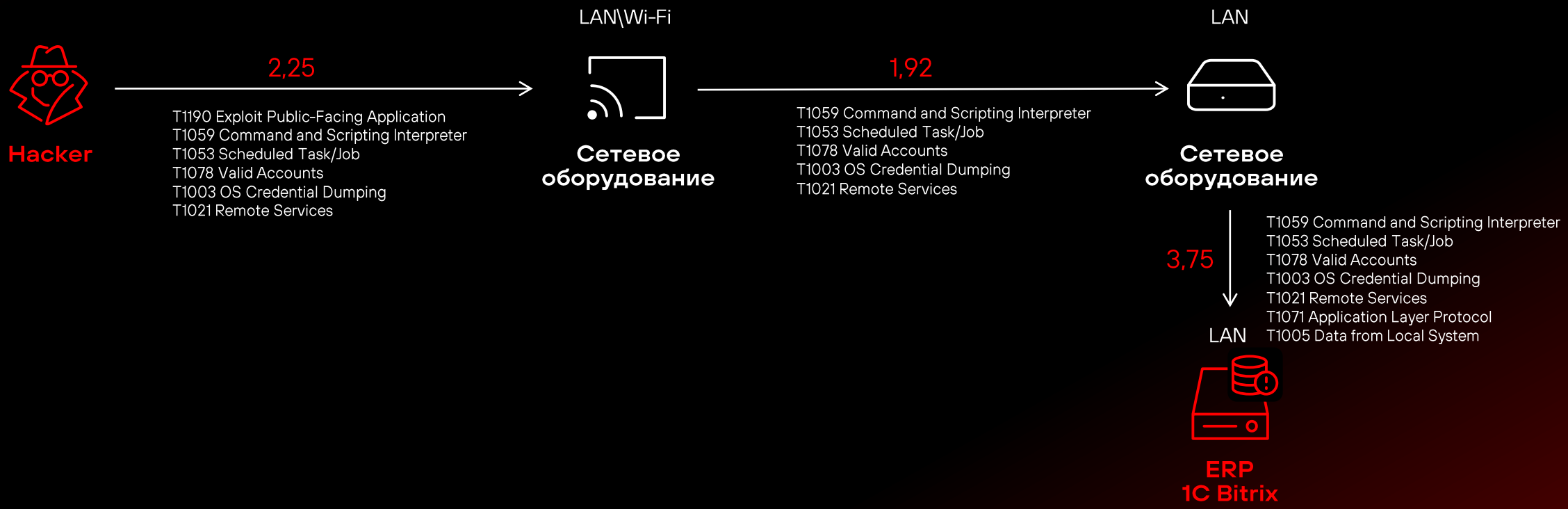
Целевая ИС — один или несколько объектов в ИТ-инфраструктуре, воздействие на которые может привести к реализации НС. Как правило, эти объекты являются конечной целью злоумышленника при реализации НС.

Ключевая ИС — объект в ИТ-инфраструктуре, несанкционированный доступ к которому или воздействие на который необходимы нарушителю, чтобы развить атаку на целевую систему, или система, взлом которой существенно упростит сценарий атаки.

Посчитали: до

Недопустимое событие: несанкционированный доступ к бизнес-системе ERP

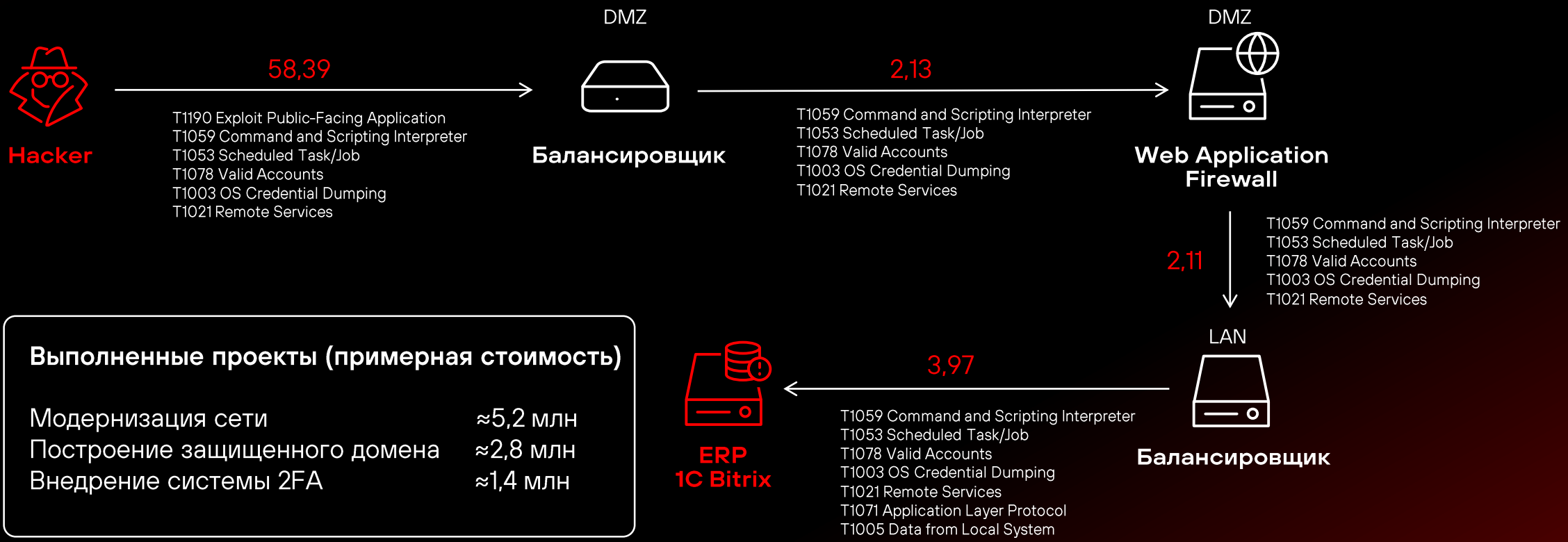
Время атаки: 7,92 часа



Посчитали: после

Недопустимое событие: несанкционированный доступ к бизнес-системе ERP

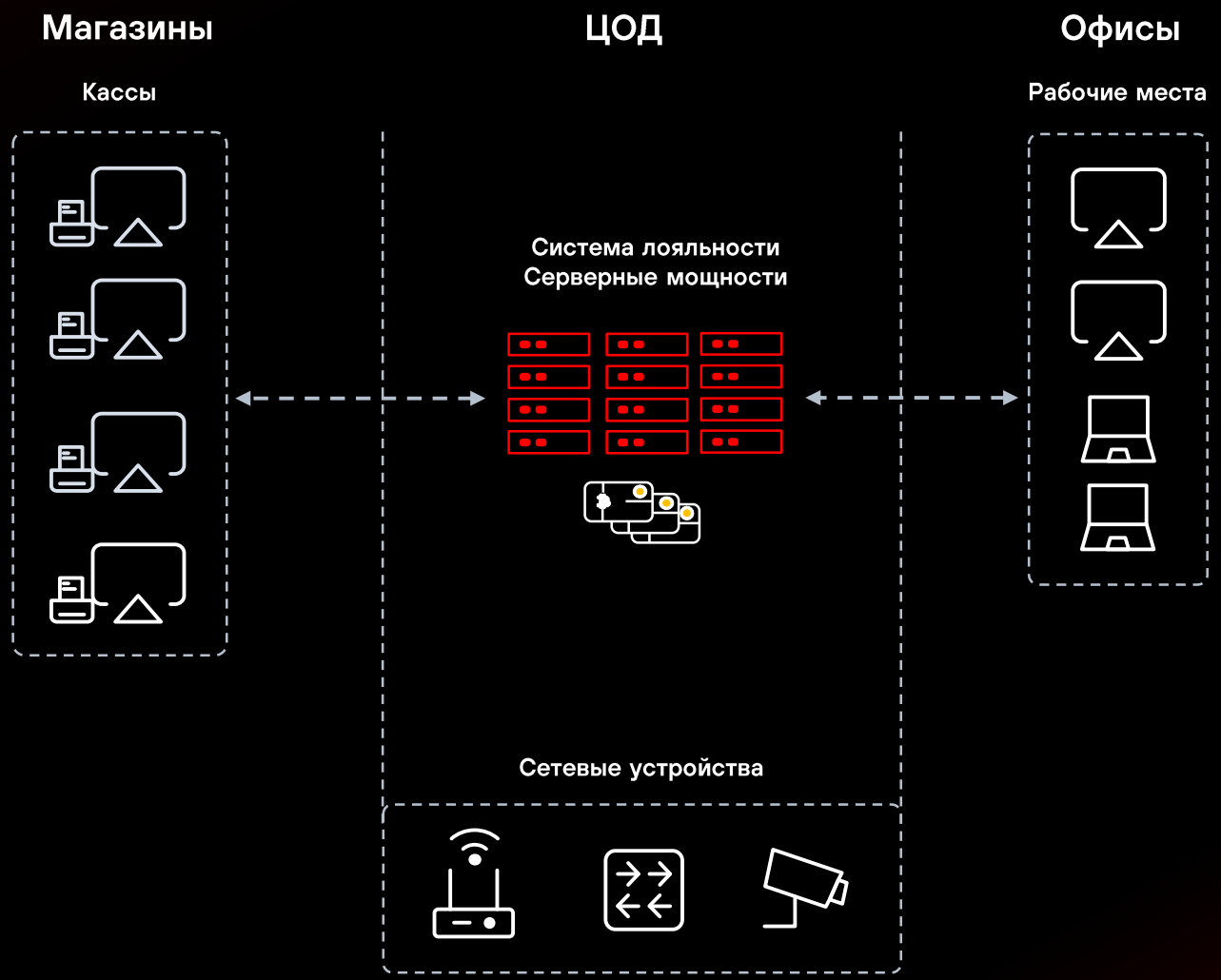
Время атаки: 66,6 часа



Выполненные проекты (примерная стоимость)

Модернизация сети	≈5,2 млн
Построение защищенного домена	≈2,8 млн
Внедрение системы 2FA	≈1,4 млн

А на самом деле...



Исходные данные

- 24 000 магазинов
- 3 работающие одновременно кассы

Особенности и ограничения

- Использование Windows
- Обязательный ответ от системы лояльности — иначе простой кассы

Потенциальные убытки

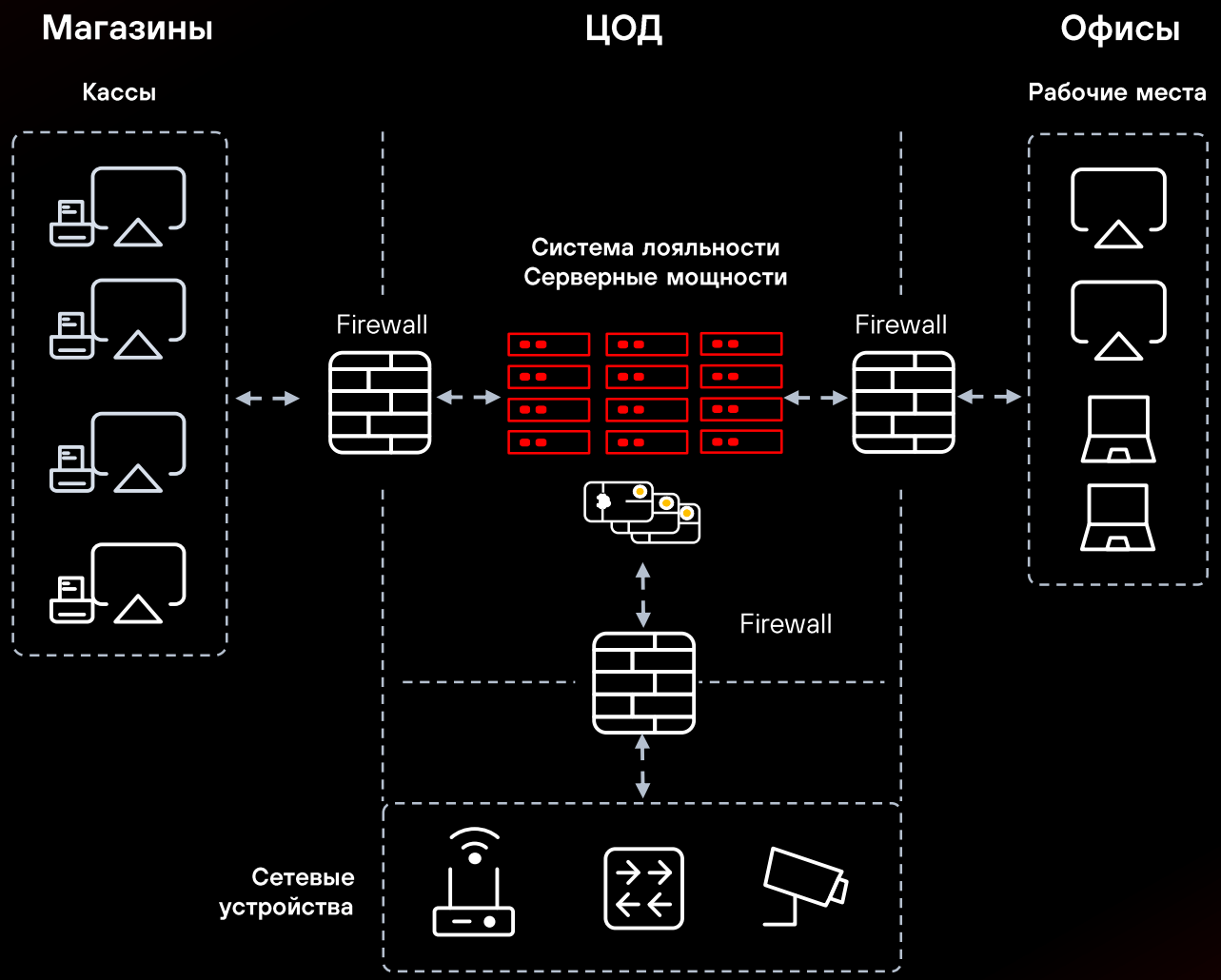
- Простой касс в течение часа оценивается в ≈500 000 в одном магазине*

Атаки

- Фрод из внутренней сети (вход через Wi-Fi)
- Продажа УЗ перед увольнением
- Атаки системы лояльности и всей инфраструктуры
- Дампы базы данных с перебором карт
- Маскировка под кассу и подмена файлов JSON
- Уязвимости в Windows, включая непредвиденные ситуации

* Размер убытка взят из кейса крупной компании в области ритейла

С этим было покончено!



Сетевая инфраструктура

- Сегментация сети
- Фильтрация JSON и проверка содержимого
- Ограничение протоколов
- Фильтрация SRC --- DST
- Тестовая среда для обкатки обновлений Windows

Система лояльности

- Система контроля запросов к базе данных
- Проверка подлинности запросов и устройств
- Контроль запросов к базе данных

Серверная инфраструктура

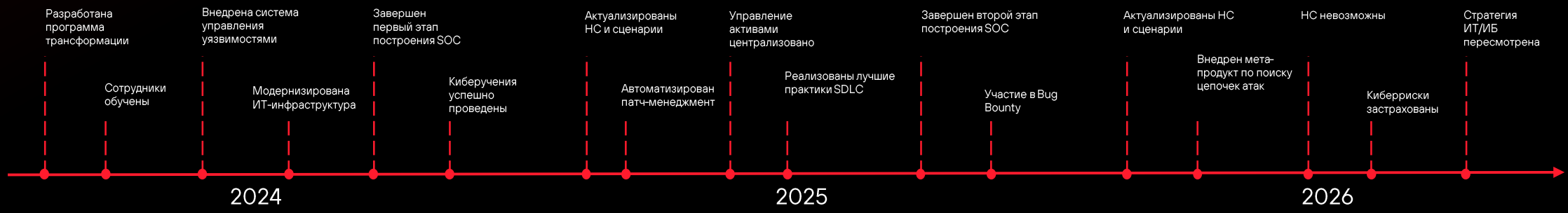
- Тестовая среда для обкатки обновлений Windows
- Постепенный переход с Windows

Общая

- Сегментация сети
- Фильтрация файлов JSON и проверка содержимого
- Ограничение протоколов
- Фильтрация SRC — DST
- Проверка подлинности запросов и устройств
- Контроль запросов к базе данных
- Тестовая среда для обкатки обновлений Windows
- Постепенный переход с Windows на другие ОС
- Усиление контроля за физической безопасностью

* Размер убытка взят из кейса крупной компании в области ритейла

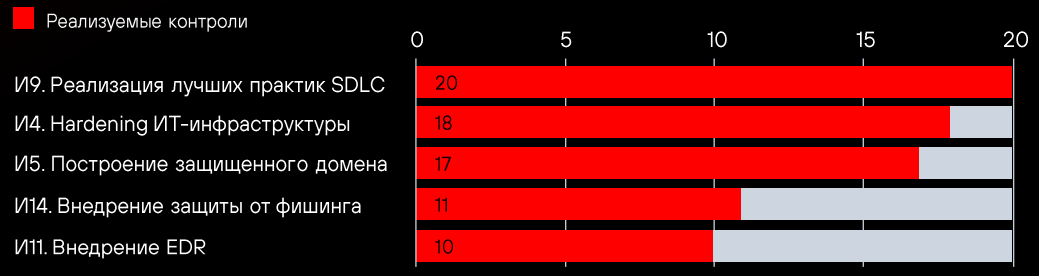
Путь к киберустойчивости ИТ-инфраструктуры



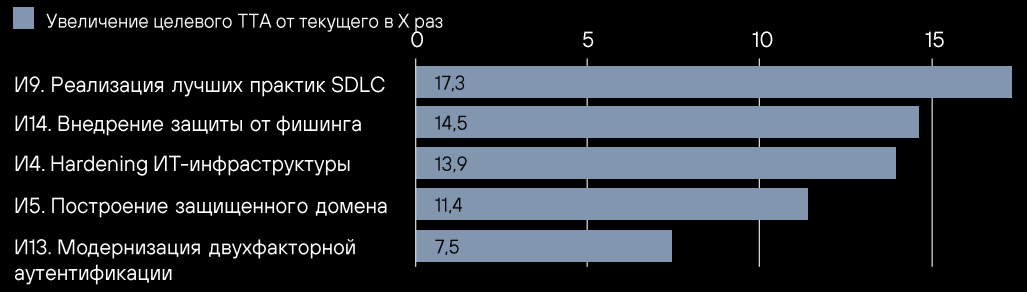
	Инициативы / Проекты	Влияние на TTA	Влияние на TTC	Стоимость	Сроки	Сложность	Приоритет
И1	Обучение сотрудников киберграмотности	низкое	низкое	xxx	xx	2	1
И2	Модернизация сети	высокое	среднее	xxx	xx	1	1
И3	Модернизация программной ИТ-инфраструктуры	среднее	низкое	xxx	xx	2	2
И4	Hardening ИТ-инфраструктуры	высокое	низкое	xxx	xx	4	1
И5	Построение защищенного домена	высокое	низкое	xxx	xx	3	2
И6	Автоматизация патч-менеджмента	низкое	низкое	xxx	xx	3	2
И7	Внедрение системы управления уязвимостями	низкое	низкое	xxx	xx	3	1
И8	Централизация управления активами	среднее	низкое	xxx	xx	3	1
И9	Реализация лучших практик SDLC	высокое	низкое	xxx	xx	1	2
И10	Внедрение решений класса NTA, WAF	низкое	низкое	xxx	xx	3	1
И11	Внедрение EDR	среднее	среднее	xxx	xx	2	1
И12	Построение SOC	среднее	высокое	xxx	xx	4	2
И13	Модернизация двухфакторной аутентификации	высокое	низкое	xxx	xx	4	2
И14	Внедрение защиты от фишинга	высокое	низкое	xxx	xx	2	2
И15	Проведение киберучений	среднее	высокое	xxx	xx	3	3

Есть что показать бизнесу

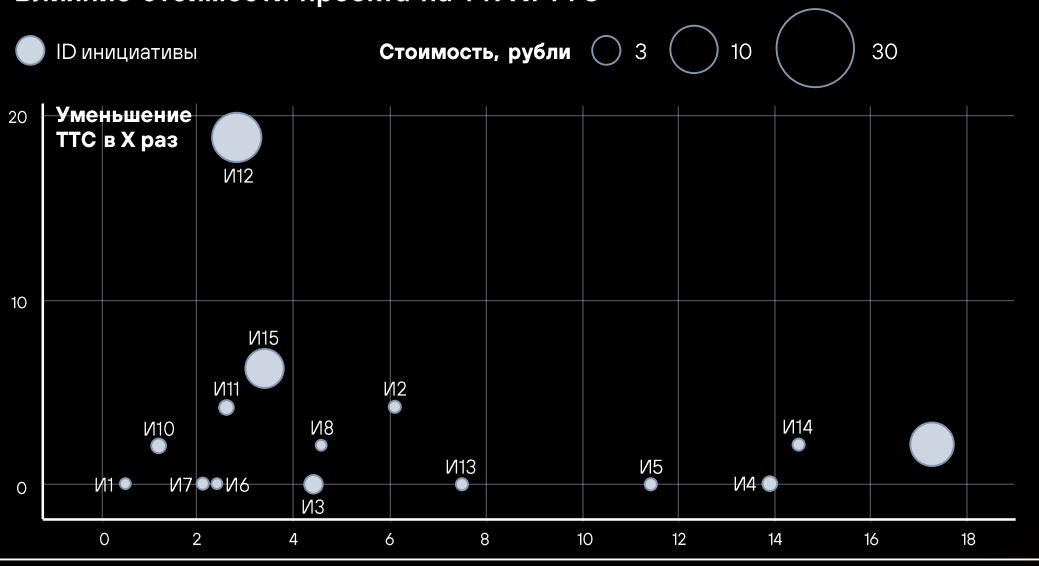
Влияние реализуемых проектов на контроли ИБ



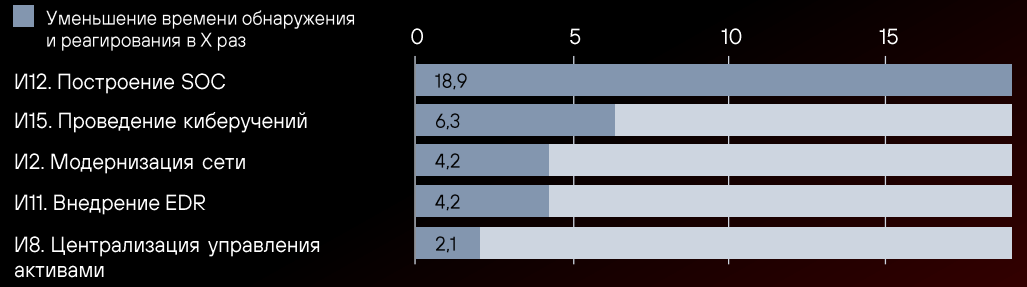
Влияние реализуемых проектов на TTA



Влияние стоимости проекта на TTA и TTC



Влияние реализуемых проектов на TTC

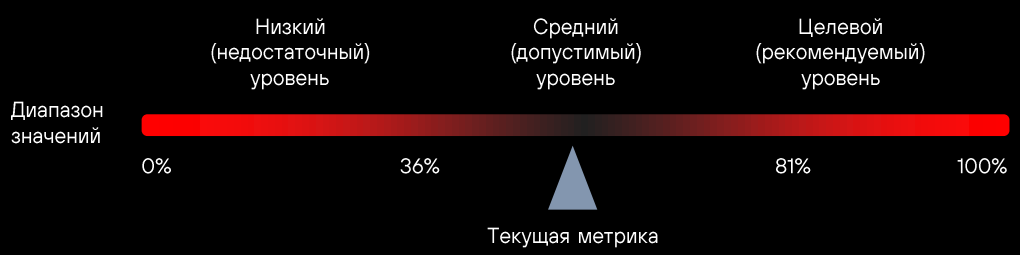


Общая оценка киберустойчивости

Метрики, полученные по результатам анализа и расчетов, отражают текущий уровень киберустойчивости.

Совокупный уровень киберустойчивости*

38%



Текущий показатель киберустойчивости находится в нижней половине среднего (допустимого) уровня.

* Данные вымышленные.

Сводная оценка киберустойчивости

Общая оценка киберустойчивости

APT-багбаунти — объективная и всесторонняя оценка реального состояния уровня защищенности компании от киберугроз.

APT-багбаунти проходят на платформе Standoff 365

Это концептуально новый подход: независимые исследователи проводят проверку в реальных условиях 24/7.

Специалисты Positive Technologies помогут запустить и будут сопровождать процесс APT-багбаунти, а индивидуально подобранные лучшие багхантеры продемонстрируют объективную картину защищенности компании.

Брошюра
ХардкорИТ

РезБез

Харденинг
Microsoft Exchange

AMelekhin@ptsecurity.com

ptsecurity.com

Спасибо!