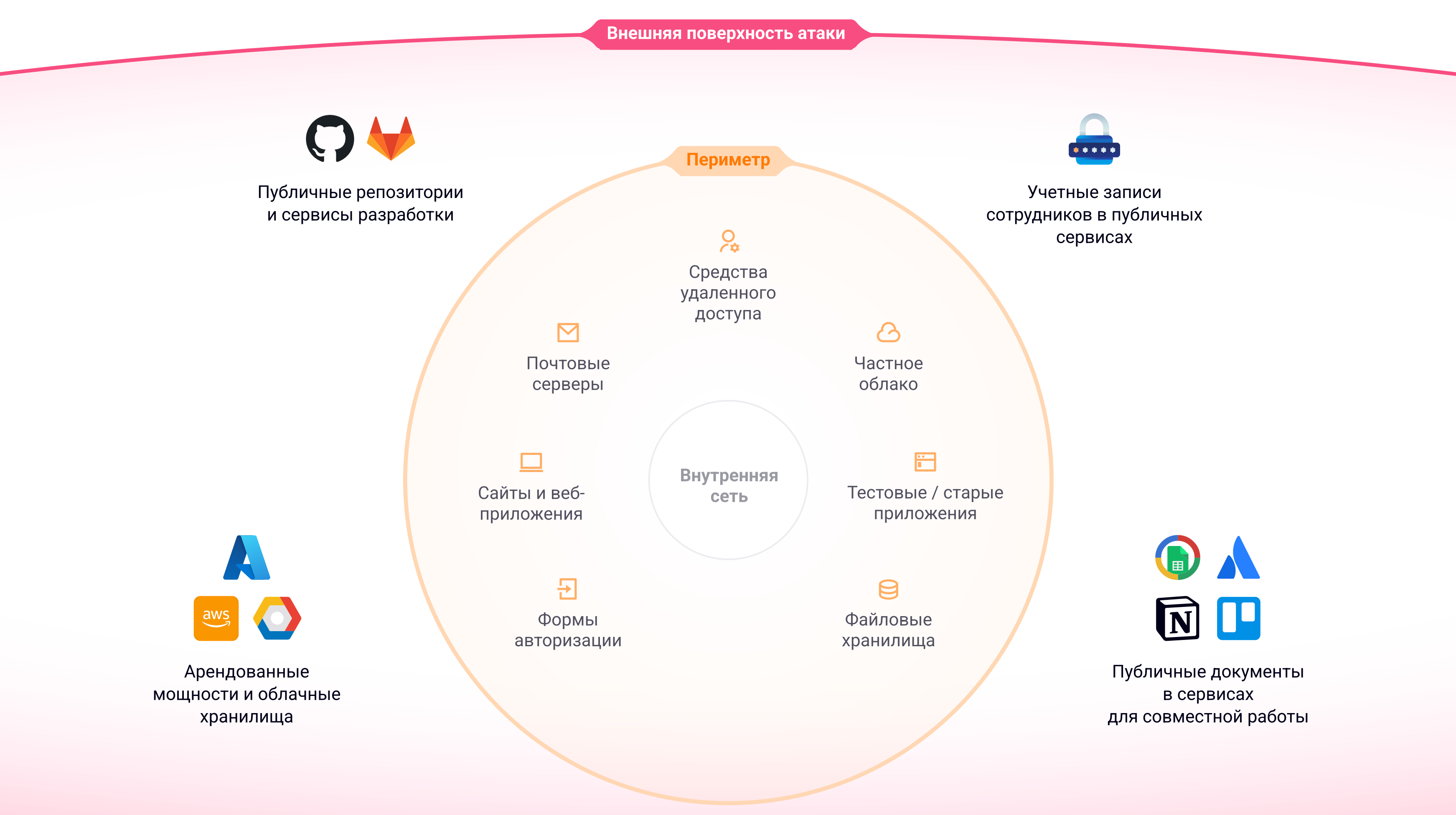
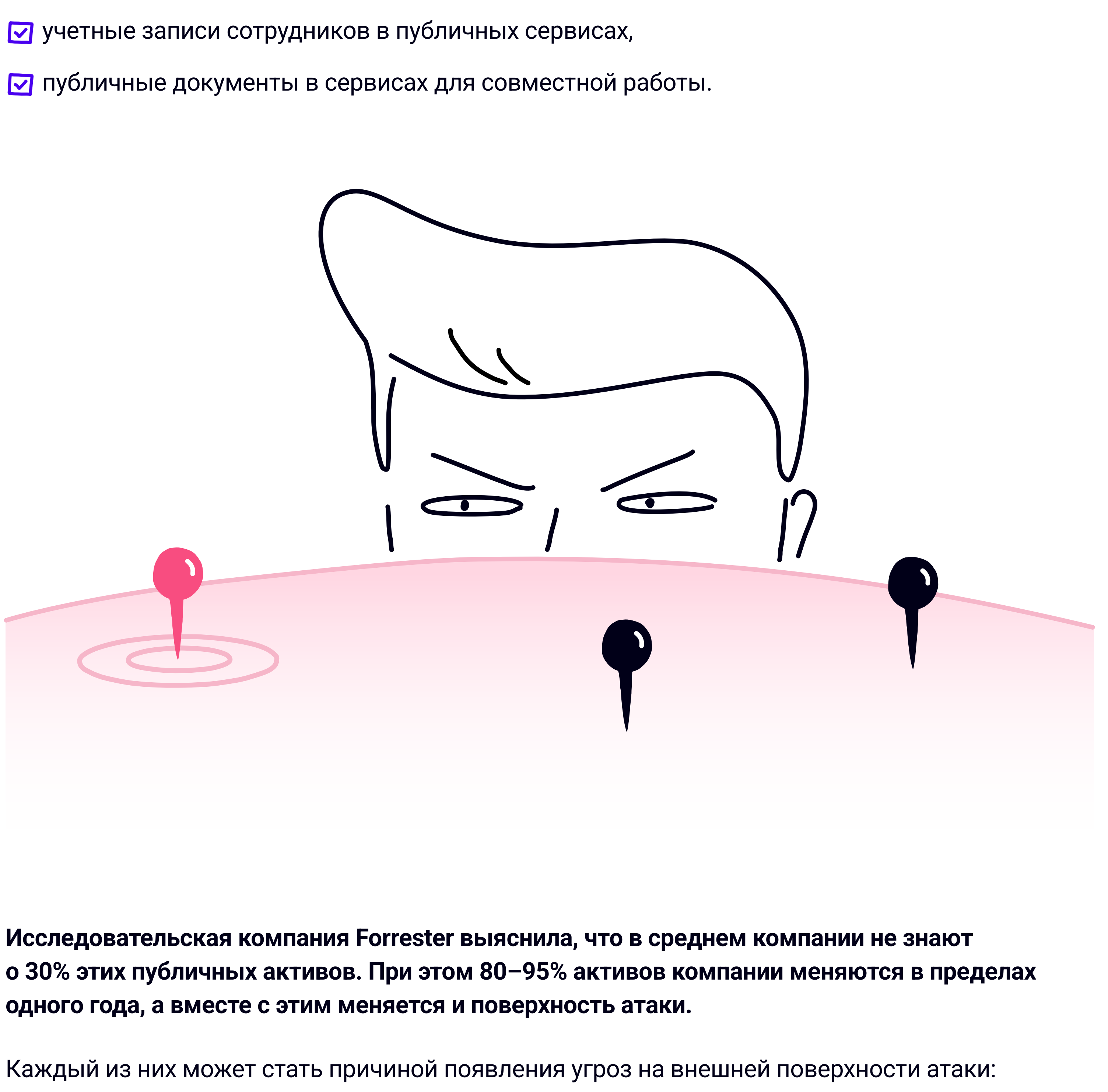
Карта самых популярных угроз на внешней поверхности атаки: почему возникают и как предотвратить

Объясняем, почему действия людей — главная причина возникновения угроз на внешней поверхности атаки, и рассказываем, что с этим делать команде безопасности



Обычно, когда говорят об управлении внешней поверхностью атаки, имеют в виду периметр компании. На самом деле внешняя поверхность атаки не равна периметру компании, потому что включает в себя больше цифровых активов:

- ☑ публичные репозитории и сервисы разработки,
- ☑ арендованные мощности и облачные хранилища,
- ☑ учетные записи сотрудников в публичных сервисах,
- ☑ публичные документы в сервисах для совместной работы.



Исследовательская компания Forrester выяснила, что в среднем компании не знают о 30% этих публичных активов. При этом 80–95% активов компании меняются в пределах одного года, а вместе с этим меняется и поверхность атаки.

Каждый из них может стать причиной появления угроз на внешней поверхности атаки: в первую очередь именно такие активы используют злоумышленники, чтобы проникнуть в инфраструктуру компании и получить доступ к системам и данным клиентов.

Для решения этой проблемы компании концентрируются только на улучшении обнаружения публичных активов — совершенствуют сканирующую инфраструктуру, которая помогает собирать больше данных в большем количестве сред.

Чтобы эффективно управлять внешней поверхностью атаки, нужно не только проводить анализ защищенности технических активов, но и работать с причиной возникновения на ней угроз.

> Главная причина возникновения угроз на внешней поверхности атаки — небезопасные действия сотрудников или подрядчиков: DevOps-инженеров, разработчиков, HR-менеджеров и других людей.

Мы разобрали самые популярные техники эксплуатации уязвимостей по классификации MITRE ATT&CK и на примерах и показали, какое действие сотрудника стоит за каждым инцидентом.

Причина появления угрозы	**Действия злоумышленника**	**Последствия для компании**	**Что делать**
Сотрудник открыл публичный доступ к доске с задачами в Trello. В одной из задач был документ с данными коллег: именами и адресами электронной почты	T1598 · Фишинг с целью сбора сведений Злоумышленник нашел документ и провел фишинговую атаку на сотрудников, чтобы получить пароли от корпоративных учетных записей	T1485 · Уничтожение данных Он украл и уничтожил корпоративные данные, к которым у сотрудников был доступ	Регулярно обучать и тренировать сотрудников безопасно работать с внешними сервисами — закрывать публичные доски, не оставлять персональные данные коллег в задачах и комментариях. Тренировать навыки сотрудников с помощью имитированных фишинговых атак
Сотрудник использовал рабочую почту и такой же пароль, как в корпоративной системе для регистрации в сервисе бронирования отелей. Разработчики сервиса хранили пароли в открытом виде и не знали про опасность SQL-фильтров в ORM, что привело к уязвимости	T1565 · Манипуляция с данными Злоумышленник нашел уязвимость и украл все данные пользователей, включая логины и пароли в открытом виде	T1078.003 · Учетные записи домена Он использовал рабочую почту и пароль сотрудника для входа в корпоративные системы и получения доступа к данным клиентов компании	Регулярно обучать и тренировать сотрудников безопасно работать с внешними сервисами — выбирать уникальные логины, придумывать сложные и разные пароли. А разработчиков — не хранить пароли в открытом виде и писать безопасный код. В том числе, уметь использовать подготовленные выражения, безопасно и эффективно использовать ORM
Девопс настроил репозиторий и забыл сделать его приватным. Разработчик не знал, как работать с секретами и сделал коммит с токенами в открытом виде	T1593.003 · Репозитории кода Злоумышленник обнаружил публичный репозиторий с секретами в процессе разведки	T1552 · Незащищенные учетные данные Он получил доступ к API-ключам, паролям учетных записей, токенам аутентификации и другим данным	Регулярно обучать и тренировать разработчиков и девопсов правильно работать с секретами: создавать, ротировать, инвалидировать. Если используется on-prem система контроля версий и она должна быть доступна удаленно, необходимо обеспечить к ней доступ только через защищенные каналы VPN с двухфакторной аутентификацией. Система должна быть настроена таким образом, чтобы все репозитории были приватными по умолчанию
Разработчик реализовал API логистической компании, в аутентификации которого была уязвимость бизнес-логики. Системы контроля и статические анализаторы не увидели проблем с точки зрения безопасности	T1190 · Недостатки в публичном приложении Злоумышленник изучил принципы работы API, нашел и проэксплуатировал уязвимость	T1489 · Остановка службы Данные клиентов — ФИО, адреса, номера телефонов — скомпрометированы, есть риск полной остановки сервиса и бизнес-процессов, связанных с доставкой товаров и грузов	Регулярно обучать и тренировать разработчиков писать безопасный код. Привлекать AppSec-специалиста на этапе проектирования, чтобы не допускать появления уязвимостей
IT-специалист забыл разделегировать домен, у которого истек срок регистрации. По этому домену отдел маркетинга размещал промо-сайт для проведения рекламной кампании	T1583 · Захват домена Злоумышленник обнаружил хостинг промо-сайта, оплатил его и опубликовал на этом хостинге фишинговую страницу, которая имитирует вход в корпоративный портал	T1598 · Фишинг с целью сбора сведений Он отправил письма сотрудникам со ссылкой на фишинговую страницу, на которой они вводили свои корпоративные логины и пароли. Злоумышленник продал эти данные другой хакерской группировке, которая использовала их в целевой атаке на компанию	Описать и внедрить процесс управления активами — в том числе созданными доменами, промо-сайтами и хостингом. Использовать EASM для мониторинга внешней поверхности атаки. Вовремя продлять или разделегировать все созданные домены, промо-сайты и хостинг. Наладить коммуникацию и слаженную работу между IT-специалистами, отделами маркетинга и безопасности
IT-специалист использовал логин admin и слабый пароль (Да, тот, о котором вы подумали) на внешнем тестовом стенде для команды разработки	T1110 · Метод перебора Злоумышленник обнаружил публичный сервис в процессе разведки и легко подобрал пароль	T1564.002 · Скрытие артефактов Он получил доступ к сервису и обнаружил, что в базе данных хранятся реальные данные действующих клиентов компании	Описать и внедрить процесс управления тестовыми данными в ходе разработки: персональные данные клиентов не должны использоваться на тестовых стендах. Не публиковать тестовые среды на периметре, а держать их внутри за VPN. Обучить команды инфраструктуры, разработки и тестирования безопасно готовить наборы тестовых данных для таких публикаций. Описать и внедрить процесс управления паролями, который будет выполняться даже на тестовых средах
IT-специалист опубликовал внешний сервис для ведения документации, в котором можно зарегистрироваться самостоятельно	T1078.003 · Облачные учетные записи Злоумышленник обнаружил публичный сервис в процессе разведки и получил доступ	T1565 · Манипуляция с данными Он получил доступ к конфиденциальным документам и данным компании, которые могут быть скомпрометированы или использованы против нее	Описать и внедрить процесс управления доступами, в том числе к внешним сервисам с возможностью самостоятельной регистрации. Описать и внедрить процесс работы с информацией, который определит, какие документы могут быть доступны всем внешним пользователям, а какие — только сотрудникам компании и по отдельному согласованию. Проверить, что IT-команда понимает требования и внедрила эти процессы на всех корпоративных сервисах

Как эффективно управлять внешней поверхностью атаки и защитить компанию от угроз, связанных с человеческим фактором

Чтобы защитить компанию, важно выстроить процесс, который позволит своевременно выявлять публичные активы компании, которые содержат угрозы на внешней поверхности атаки, а также видеть связь между возникновением этих угроз и небезопасными действиями сотрудников. А чтобы избежать повторения этих действий — формировать у людей навыки безопасной работы.

Если ваша компания среднего или крупного размера, имеет множество активов и задействует подрядчиков, скорее всего, вы не имеете полного представления о составе внешней поверхности атаки. В таком случае для эффективного управления и мониторинга активов можно использовать автоматизированные SaaS-решения.

> Благодаря этому команды безопасности могут увидеть и устранить саму причину появления угроз на внешней поверхности атаки — через целевое обучение сотрудников, тренировку навыков безопасной работы и доставку актуальных требований до продуктовых команд.

Start X
+7 499 677 19 07
startx.team