ЛУЧШИЕ ТЕХНОЛОГИИ ЗАЩИТЫ ПРОТИВ ВЕДУЩИХ БЕЛЫХ ХАКЕРОВ — КТО КОГО?

МЕТАПРОДУКТЫ НА STANDOFF

STANDOFF — ЭТО КИБЕРБИТВА, В КОТОРОЙ ИБ-СПЕЦИАЛИСТЫ ПРОТИВОСТОЯТ АТАКАМ БЕЛЫХ ХАКЕРОВ, ЗАЩИЩАЯ КОМПАНИИ ИЗ РАЗНЫХ ОТРАСЛЕЙ ЭКОНОМИКИ НА ПРИМЕРЕ ВИРТУАЛЬНЫХ ГОСУДАРСТВ

В ходе битвы **КРАСНЫЕ КОМАНДЫ** — белые хакеры — атакуют системы виртуальных государств. Например, пытаются украсть данные клиентов банка, взломать светофорную систему или остановить работу нефтеперерабатывающего завода. Задача **СИНИХ КОМАНД** — ИБ-специалистов — выявлять, расследовать атаки и реагировать на них.

STANDOFF 13 В ЦИФРАХ

8 отраслей	**179** целей для хакеров	**36** часов кибербитвы
11 команд защитников	**25** команд атакующих	

STANDOFF — ЭТО ТАКЖЕ ПРОВЕРКА НА ДЕЛЕ НАШИХ ПРОДУКТОВ

За защиту инфраструктуры виртуальных государств отвечают MaxPatrol SIEM, PT Network Attack Discovery, MaxPatrol EDR, PT Application Firewall, PT Sandbox.

А с недавних пор к ним добавились метапродукты: MaxPatrol O2, MaxPatrol Carbon.

MAXPATROL O2

Это первый метапродукт Positive Technologies. Обнаруживает злоумышленника, собирает контекст атаки, прогнозирует возможный сценарий её развития с учетом недопустимых для компании событий и останавливает атаку до нанесения непоправимого ущерба.

MAXPATROL CARBON

Это второй метапродукт Positive Technologies. Анализирует возможные сценарии атак на компанию, формирует рекомендации по повышению защищенности IT-инфраструктуры с учетом недопустимых для компании событий и контролирует их выполнение. Это не позволяет злоумышленнику добраться до критически важных активов или существенно усложняет его путь.

MAXPATROL O2

STANDOFF

STANDOFF 13 ПЛЕЙ-ОФФ

Май 2024 г.

MAXPATROL O2 ПРОТИВОСТОЯЛ 4 ЛУЧШИМ КОМАНДАМ АТАКУЮЩИХ 6 ЧАСОВ В ПЛЕЙ-ОФФ STANDOFF 13

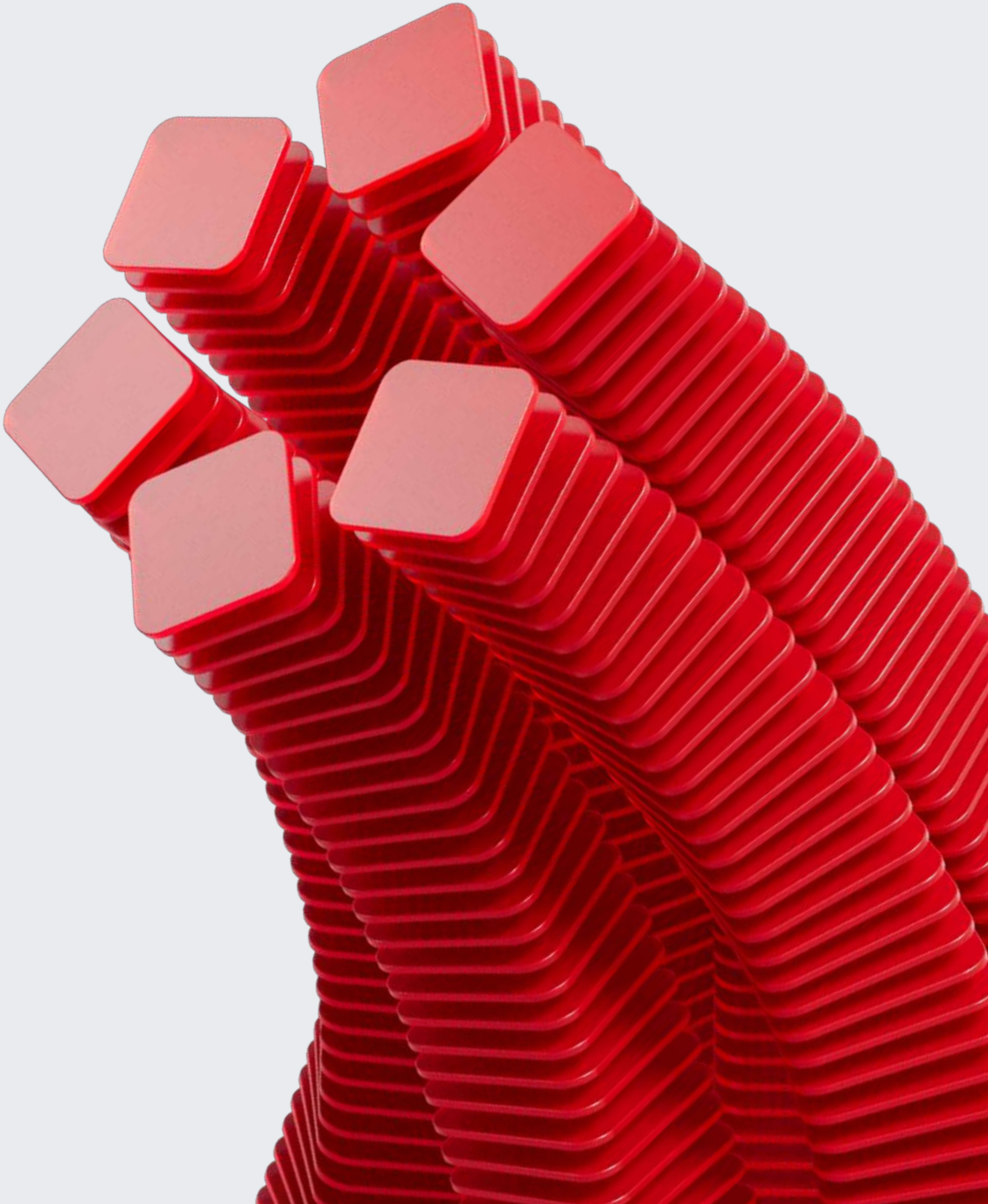
В этом году кибербитва состояла из двух этапов: основной этап соревнований и плей-офф.

По итогам основного этапа четыре лучшие команды атакующих вышли в плей-офф. Плей-офф — это заключительный этап кибербитвы, который длился 6 часов. В ходе него командам предложили выполнить специальное задание — реализовать одно из двух недопустимых событий в копии реальной инфраструктуры Positive Technologies.

За кражу денежных средств со счета компании или вмешательство в процесс разработки, сборки и доставки ПО победитель получил бы **7,5 миллионов рублей**.

Белые хакеры могли пользоваться любыми инструментами без ограничений. **Главный челлендж — ускользнуть от MaxPatrol O2**, который работал в режиме реагирования. Им управлял **один аналитик**. Специалист верифицировал выявленные цепочки событий и вовремя подтверждал предложенный MaxPatrol O2 сценарий реагирования, чтобы отобрать у хакеров захваченные ресурсы и остановить атаку.

MaxPatrol O2 мог завершать вредоносные процессы, удалять файлы с полезной нагрузкой, блокировать учетные записи в домене и внешние соединения на межсетевом экране, разрывать VPN-соединения и многое другое.



РЕЗУЛЬТАТ

Лучшие белые хакеры не смогли обойти MaxPatrol O2 и реализовать недопустимые события

Разбор самых интересных цепочек с противостояния хакеров и MaxPatrol O2

ЦИФРЫ

STANDOFF

ЗА 6 ЧАСОВ ПЛЕЙ-ОФФ КИБЕРБИТВЫ:

событий в инфраструктуре	срабатываний правил корреляции в MaxPatrol SIEM	цепочки действий атакующих в MaxPatrol O2	из них в статусе «Требует внимания»
98+ миллионов →	**220+ тысяч** →	**1764** →	**148**

MaxPatrol O2 снизил нагрузку на аналитика в 1500 раз

До начала кибербитвы эксперты Positive Technologies настроили расширенный сбор событий с систем в копии инфраструктуры компании. Это увеличивает шансы на обнаружение злоумышленников, хоть и повышает число срабатываний, регистрируемых в средствах защиты.

Точно так же мы рекомендуем поступать нашим клиентам, которые хотят быть уверены в том, что успеют заметить хакера в инфраструктуре.

В рамках основного этапа кибербитвы была зафиксирована следующая статистика:

Кто защищает	Численность команды (чел.)	Время расследования (мин.)
Синие команды	Средняя — 15 Минимальная — 10 Максимальная — 25	Среднее — 354 Минимальное — 37 Максимальное — 840
MaxPatrol O2	1	2,5

Численность команды защиты меньше в 15 раз

Время расследования и реагирования меньше в 15 раз

В рамках основного этапа кибербитвы 2 синие команды участвовали в режиме реагирования. Процент предотвращенных и расследованных ими атак на Standoff 13

Кто защищает	Предотвращенные атаки	Расследованные атаки
Команда защитников № 1 выбрала стратегию предотвращения атак, в связи с чем не успевала их расследовать	54% (110 из 204)	1% (2 из 204)
Команда защитников № 2 выбрала стратегию расследования атак, но им не хватало времени на полноценное реагирование	7% (5 из 68)	31% (21 из 68)
MaxPatrol O2	**100%** (148 из 148)	**100%** (148 из 148)

1 аналитик расследовал и предотвратил все атаки с помощью MaxPatrol O2

Команды атакующих смотрят, как MaxPatrol O2 собрал их действия в цепочки. Хотите тоже посмотреть?

КАК MAXPATROL O2 ВИДЕЛ ДЕЙСТВИЯ АТАКУЮЩИХ

STANDOFF

5 МИНУТ С НАЧАЛА КИБЕРБИТВЫ

Получая множество вердиктов от других продуктов Positive Technologies, MaxPatrol O2 принимает решение о том, какие срабатывания связаны между собой, и строит цепочку атаки (см. рис. 1).

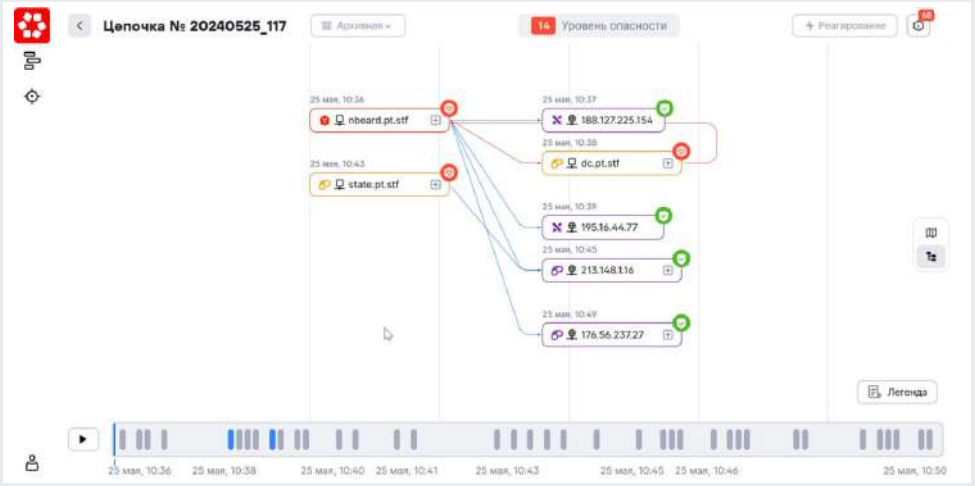


Рисунок 1. Верхнеуровневое представление действий атакующих в одной из цепочек событий

Так, атакующие пытались захватить контроллер домена, но были «выбиты» из инфраструктуры. Реагирование осуществлялось сразу, как только цепочки переходили в статус **«Требует внимания»**.

В цепочке представлены:

- Узлы, по которым белые хакеры перемещались в инфраструктуре
- Внешние адреса, с которыми они устанавливали соединения с захваченных узлов

Разбор самых интересных цепочек с противостояния хакеров и MaxPatrol O2

2 ЧАСА С НАЧАЛА КИБЕРБИТВЫ

Аналитик перестал реагировать сразу в момент получения оповещения, предоставив хакерам возможность развить атаку. В рамках кибербитвы среднее время перехода цепочек в статус «Требует внимания» — 20 минут.

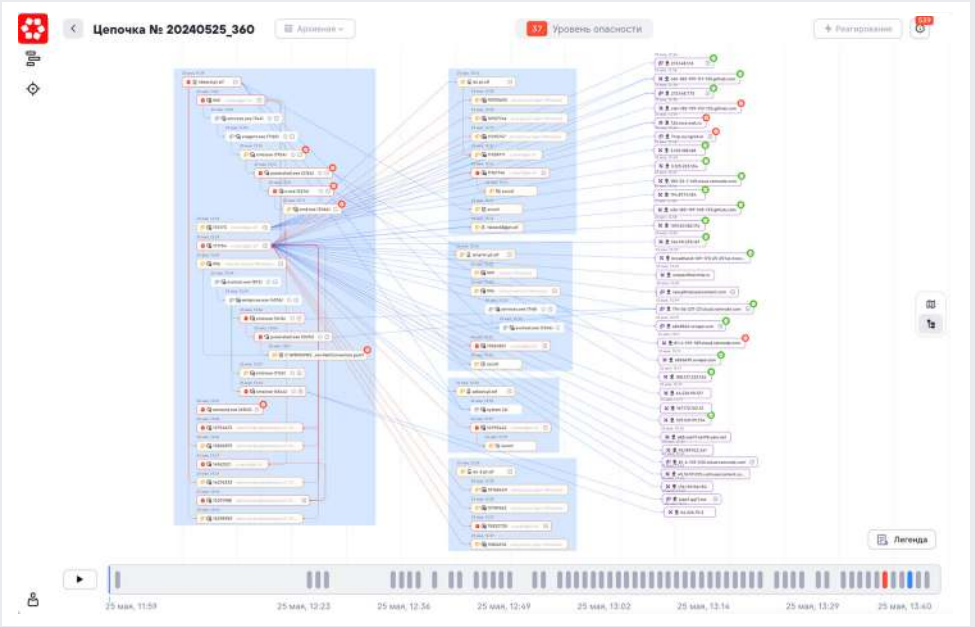


Рисунок 2. Пример цепочки с развитием атаки хакеров

ЧТО БЫЛО ДАЛЬШЕ

Команды белых хакеров **не смогли реализовать ни одного недопустимого события** за 6 часов противостояния с MaxPatrol O2. Мы отключили реагирование в метапродукте и начали серию пенальти со специальными заданиями, в которых и определился победитель.

В этот раз 7,5 миллионов рублей не нашли своего обладателя, но мы обязательно дадим командам шанс в будущем ;)

MAXPATROL CARBON

STANDOFF

STANDOFF 13

Май 2024 г.

КЕЙС ИЗ ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

100+
активов

150+
учетных записей

MAXPATROL CARBON ВЫЯВИЛ:

Векторов атак

200+
тысяч

Шагов в векторах

1–27

Самый быстрый вектор атаки

11
минут

Сформированных рекомендаций, чтобы нивелировать все векторы атак

217 → **4**

Из них — для устранения векторов атак, реализуемых за один шаг

РЕЗУЛЬТАТ

MaxPatrol O2 в ходе кибербитвы выявил цепочки атак, которые заранее рассчитал MaxPatrol Carbon