ENDPOINT DETECTION AND RESPONSE

БОЛЬШЕ,
ЧЕМ
АНТИВИРУС

ЧТО ОТСЛЕЖИВАЕТ EDR?

EDR непрерывно анализирует активность конечных устройств и выявляет подозрительное поведение **в реальном времени.**

Запущенные процессы

Какие приложения и процессы выполняются в системе.

Изменения файлов

Создание, удаление и модификация файлов.

Изменения в реестре

Подозрительные правки Windows Registry и механизмы persistence.

Сетевые соединения

Необычные подключения, внешние адреса и подозрительный трафик.

Действия пользователей

Входы, права доступа и нестандартное поведение.

Системные события

Логи, ошибки и другие признаки потенциальной атаки.

02 / 02

ENDPOINT DETECTION AND RESPONSE

БОЛЬШЕ, ЧЕМ АНТИВИРУС

КАК РАБОТАЕТ EDR?

От сбора данных до реагирования — всё происходит автоматически и **в реальном времени.**



1 СБОР ДАННЫХ

EDR-агенты постоянно собирают информацию с конечных устройств (процессы, файлы, реестр, сеть, действия пользователей).

2 АНАЛИЗ

Собранные данные анализируются на предмет аномалий, подозрительного поведения и известных угроз (с помощью правил, ML и threat intelligence).

3 ОБНАРУЖЕНИЕ

Выявляется подозрительная активность, которая связывается в единый инцидент и приоритезируется по уровню риска.

4 РЕАГИРОВАНИЕ

EDR автоматически блокирует, изолирует или нейтрализует угрозы (например, завершает процесс, отключает устройство от сети и т.д.).

5 ОТЧЁТНОСТЬ

Формируются детальные алерты и инсайты, которые помогают команде быстрее расследовать инциденты и улучшать защиту.

БЫСТРОЕ ОБНАРУЖЕНИЕ. МЕНЬШЕ РИСКОВ. **БОЛЬШЕ КОНТРОЛЯ.**

ТВОИ УСТРОЙСТВА.
НАША БЕЗОПАСНОСТЬ.

БОЛЬШЕ ПОЛЕЗНОГО В
@lionsoulbatyshchikov

ENDPOINT DETECTION AND RESPONSE

БОЛЬШЕ, ЧЕМ АНТИВИРУС

EDR СМОТРИТ НА ПОВЕДЕНИЕ, А НЕ ТОЛЬКО НА ФАЙЛЫ.

Вместо обычного сканирования файлов EDR анализирует, что реально происходит на endpoint — **в реальном времени.**

ЧТО ОТСЛЕЖИВАЕТ EDR?

Подозрительные действия

Необычные команды, scripts и выполнение процессов.

Повышение привилегий

Попытки получить расширенные права в системе.

Defense Evasion

Попытки отключить или обойти средства защиты.

Lateral Movement

Подозрительные подключения и перемещение между системами.

Доступ и эксфильтрация данных

Аномальный доступ к чувствительным данным или их массовая передача.

ПОВЕДЕНИЕ ПОКАЗЫВАЕТ РЕАЛЬНЫЕ НАМЕРЕНИЯ.

БОЛЬШЕ ПОЛЕЗНОГО В **@lionsoulbatyshchikov**

02 / 03
ENDPOINT DETECTION AND RESPONSE

БОЛЬШЕ, ЧЕМ АНТИВИРУС

КАК EDR ВИДИТ АТАКУ?

EDR связывает события, анализирует контекст и выявляет подозрительное поведение **в реальном времени.**



ПРИМЕР ДЕТЕКТА

2026-09-06 14:37:21

ОБНАРУЖЕНО ПОДОЗРИТЕЛЬНОЕ ПОВЕДЕНИЕ

Process:	powershell.exe
Action:	Encoded Command Execution
Target:	System32\cmd.exe
User:	Admin
Severity:	High

MALICIOUS BEHAVIOR

ENCODED COMMAND

ATT&CK T1059.001

ENDPOINT PROTECTED

Windows PowerShell

```
PS C:\Users\admin> powershell.exe
-enc JABjAG0AZAAgAD0AIABBDAGUAwAt
AE0AYbBKAGUAYwBbACAAUwByAHMAdABle
AG0ALgBEAGikAY0BbngBvAHMAdABAGMAcw
AuAPAAcgBvAGMAZ0Be3AHMAUwB0AGEAcg
B0AEKAbgBmAG0AOwAgAC.ALgAu
```

EDR ALERT

Process	powershell.exe
Action	Encoded Command
Target	System32\cmd.exe
User	Admin
Severity	High

ЗАБЛОКИРОВАНО

ВЕРДИКТ EDR

ВРЕДОНОСНАЯ АКТИВВОСТЬ ЗАБЛОКИРОВАНА

Угроза изолирована. Дальнейшее выполнение предотвращено.

БЫСТРОЕ ОБНАРУЖЕНИЕ.
МЕНЬШЕ РИСКОВ.

БОЛЬШЕ ПОЛЕЗНОГО В
@lionsoulbatyshchikov

03 / 03
ENDPOINT DETECTION AND RESPONSE

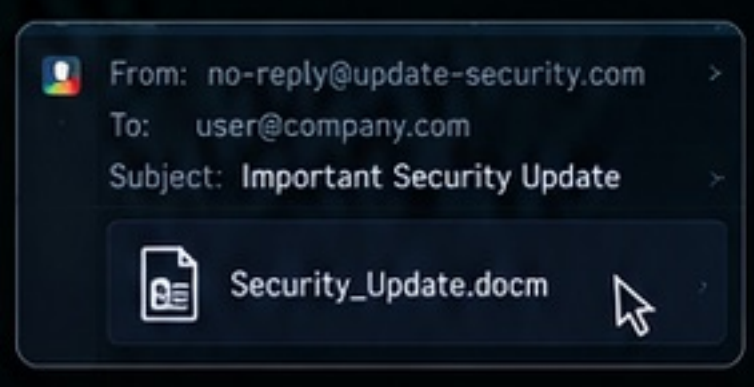
БОЛЬШЕ, ЧЕМ АНТИВИРУС

EDR ВИДИТ ВСЮ ЦЕПОЧКУ.

От первого доступа до конечного воздействия — EDR связывает события в единую картину и выявляет атаку **на ранних этапах.**

1 INITIAL ACCESS

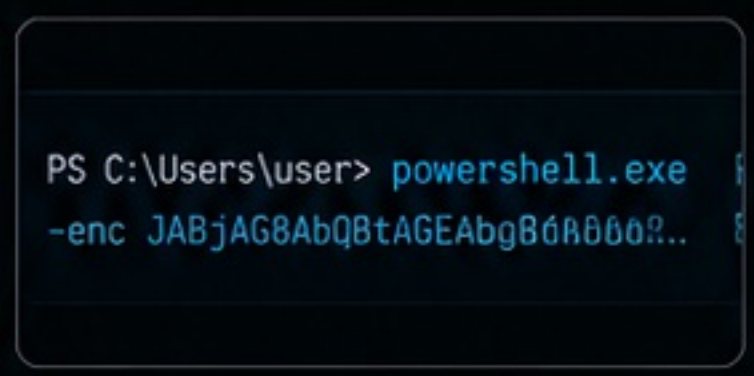
Фишинговое письмо доставлено пользователю.



Пользователь открывает вложение.

2 EXECUTION

Запущен вредоносный скрипт (например, PowerShell).



Выполняется закодированная команда.

3 PERSISTENCE

Создаётся механизм автозапуска (изменение в реестре).



Вредоносный скрипт закрепляется в системе.

4 PAYLOAD

Загружается и запускается основной вредоносный модуль.



Скачивается и запускается malware.

5 IMPACT

Подозрительная активность выявлена и заблокирована.



EDR обнаруживает атаку и блокирует дальнейшие действия.

ОТДЕЛЬНОЕ СОБЫТИЕ МОЖЕТ ВЫГЛЯДЕТЬ НОРМАЛЬНО.
ЦЕПОЧКА СОБЫТИЙ — УЖЕ ПОКАЗЫВАЕТ АТАКУ.

- БОЛЬШЕ КОНТЕКСТА
- БЫСТРЕЕ ОБНАРУЖЕНИЕ
- МЕНЬШЕ РИСКОВ
- ВЫШЕ УРОВЕНЬ ЗАЩИТЫ

ПОВЕДЕНИЕ СЕГОДНЯ — БЕЗОПАСНОСТЬ ЗАВТРА.

БОЛЬШЕ ПОЛЕЗНОГО В @lionsoulbatyshchikov