

EDR доверяет подписанным драйверам

И именно это использует **BYOVD**

@lionsoulbatyshchikov

ЧТО ТАКОЕ BYOVD?

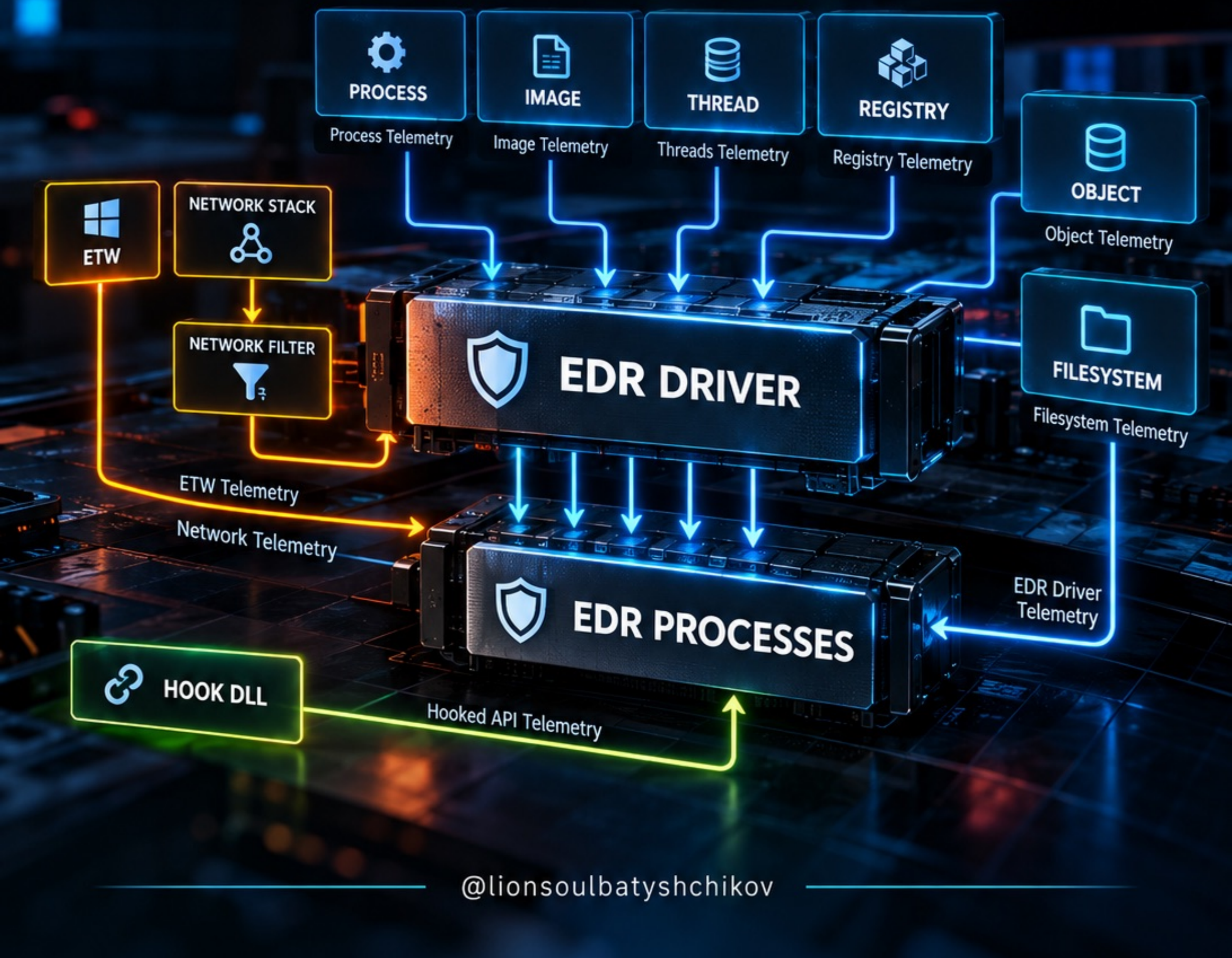
BYOVD (Bring Your Own Vulnerable Driver) — это метод, при котором атакующий загружает на систему **легитимный**, но **уязвимый драйвер**, и использует его уязвимости для выполнения действий на уровне **kernel**.



@lionsoulbatyshchikov

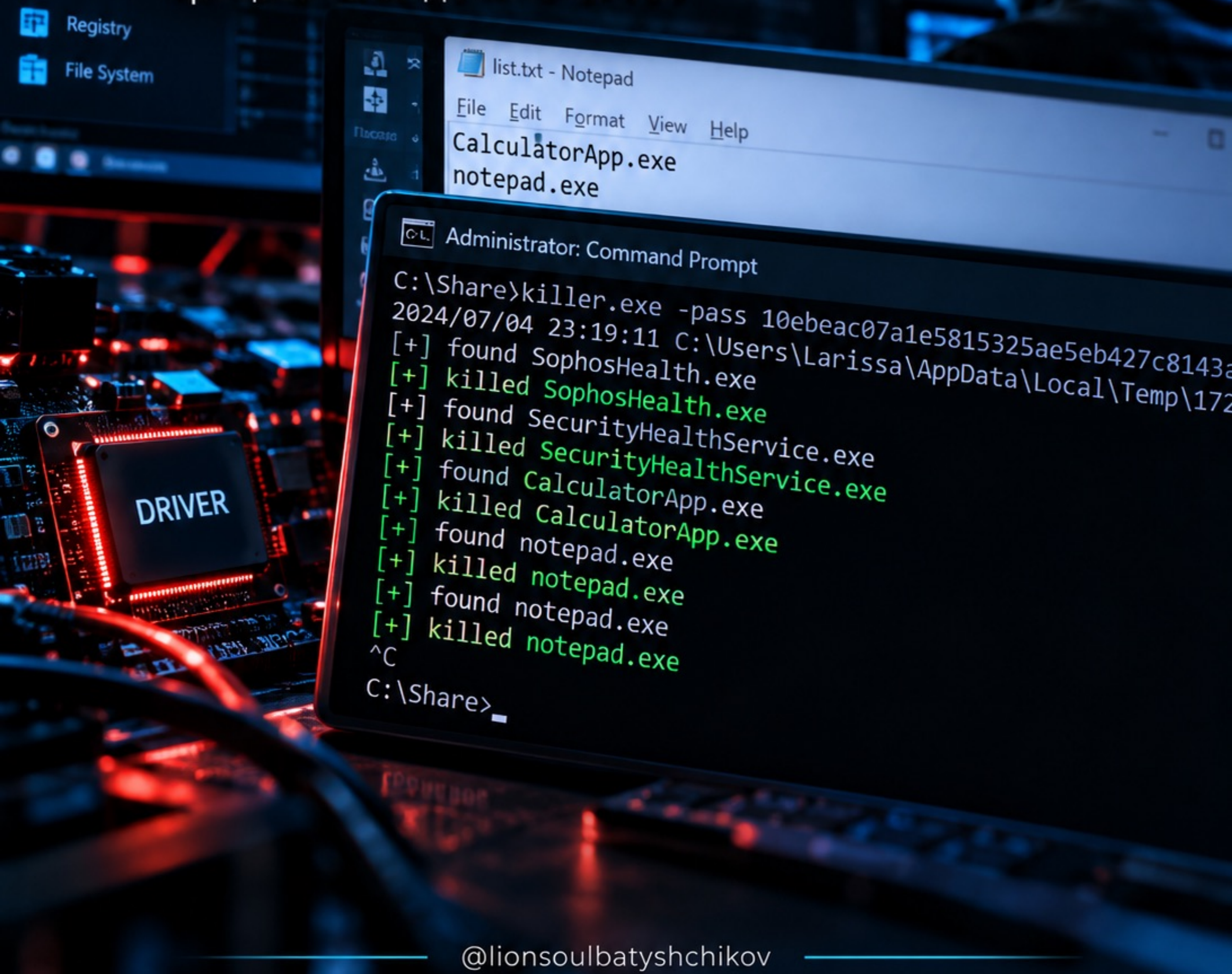
ЗАЧЕМ НУЖЕН KERNEL

EDR работает в **user mode**, но использует драйвер в **kernel**, чтобы получать данные **на низком уровне**.
Так он может видеть и контролировать действия процессов, файлов, реестра, сети и других объектов.
Именно драйвер позволяет перехватывать, приостанавливать или блокировать активность до того, как она будет выполнена.



ДРАЙВЕР КАК КЛЮЧ

Драйверы работают в **kernel**.
Один драйвер, подписанный **Microsoft**,
но с уязвимостью записи в память,
может стать ключом: атакующий загружает его
и получает привилегии, которые обычный
процесс никогда не имел бы.



@lionsoulbatyshchikov

ПОЧЕМУ ЕГО ТАК ЧАСТО ИСПОЛЬЗУЮТ?

Драйвер **легитимный** и **подписанный**, поэтому он имеет доступ к множеству привилегированных функций. Многие группы **ransomware** используют такие драйверы, потому что это **дешево**, **надежно** и **сложно обнаружить**, а также блокировать без предварительной подготовки.



@lionsoulbatyshchikov

КАК ОБНАРУЖИТЬ

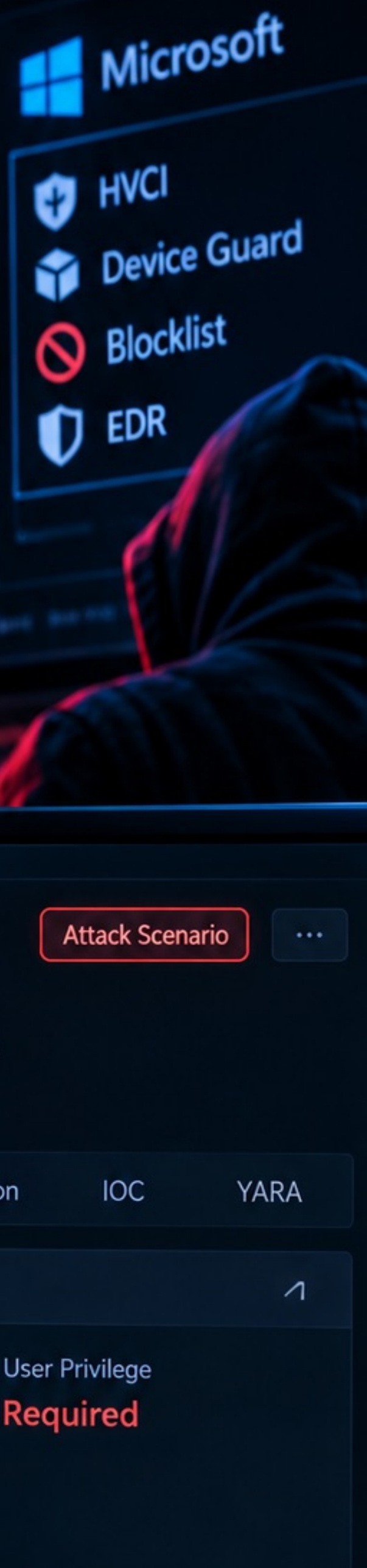
Отслеживайте загрузку известных уязвимых **driver** и сервисов, которые создаются только, чтобы загрузить **driver** и получить нестандартный доступ к **kernel** ещё до того, как **EDR** успеет среагировать.



@lionsoulbatyshchikov

КАК ЗАЩИТИТЬСЯ

Включите блокировку уязвимых driver’ов от **Microsoft** (**HVCI** и **driver blocklist**), ограничьте установку driver’ов только от доверенных издателей и настройте правила в EDR для обнаружения и блокировки подозрительной загрузки.







@lionsoulbatyshchikov

ГЛАВНОЕ ПОМНИТЬ

Подписанный драйвер — не всегда **безопасный драйвер.**
Доверие к цифровой подписи — это **слабое место.**
Проверяйте и блокируйте известные уязвимые driver’ы до того, как они окажутся в системе.



@lionsoulbatyshchikov