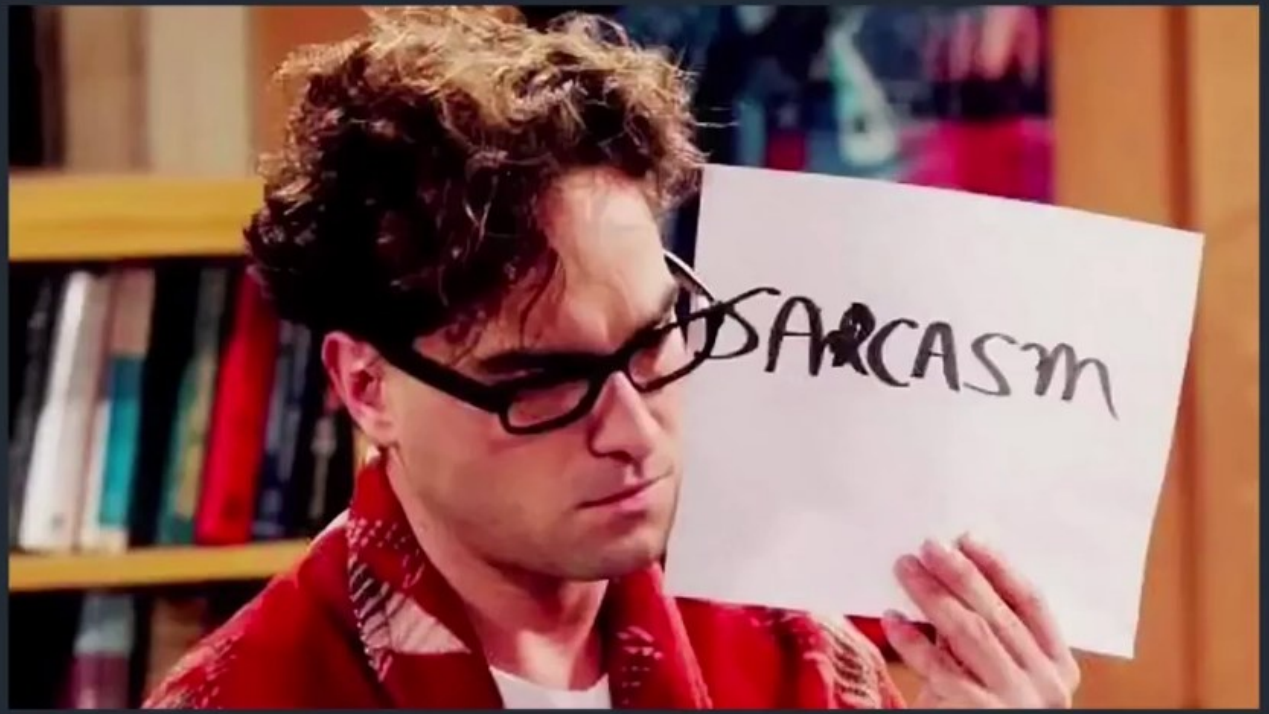
ЦЕННОСТЬ ИНСТРУМЕНТОВ ИБ: ЧЕГО БЫ У НАС НЕ БЫЛО, ЕСЛИ Б У НАС ВСЕ БЫЛО

Словосочетания "кибер-зрелость" придуманное ИБ-маркетологами, чаще всего, звучит как: "У вас нет 5 млн. рублей за наш ВЕЛИКИЙ продукт? Ну так вы еще не доросли! Идите отседова, не мешайте торговать!"

😁 8 🔥 7 💯 5

756 23:41

Leave a Comment


SARCASM

МИФЫ О РАЗУМНОСТИ И ЗРЕЛОСТИ

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

Антивирус ищет, блокирует и удаляет вредоносное ПО.

Антивирус — это базовый уровень защиты конечных точек: пользователи, офисные машины, серверы. Самый первый шаг в стратегии кибербезопасности.

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

НЮАНСЫ:

- Ложные срабатывания (False Positives)
- Ложное чувство безопасности
- Ограниченность обнаружения
- Недостаточная интеграция с другими ИБ-средствами
- BYOD
- Сложности в расследовании инцидентов

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

ЧТО НАС ЖДЕТ БЕЗ АНТИВИРУСА:

- Простые угрозы не будут блокироваться сразу
- Рост нагрузки на другие системы ИБ
- Повышенный риск заражения «снизу»
- Утрата базового уровня соответствия требованиям
- Финансовые и репутационные последствия

Это фундамент, база. Если у вас в компании используется хотя бы **одно цифровое устройство** — вам необходим **антивирус**.

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

DATA LOSS PREVENTION/PROTECTION

Базовая задача DLP — предотвратить утечку данных (персональных, финансовых, конфиденциальных) путем контроля каналов.

КОГДА ПРИМЕНЯЕТСЯ:

- При необходимости соблюдений требований GDPR, HIPAA, ISO 27001, ФЗ-152 и пр.
- При высоком риске утечки инсайдерской или коммерческой информации.

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

ОСНОВНЫЕ СЛОЖНОСТИ РАБОТЫ С DLP В КОРПОРАТИВНОЙ ИБ:

- Высокие требования к настройке и классификации данных
- Ложные срабатывания и «шум»
- Негативная реакция пользователей
- Технические ограничения
- Интеграция с бизнес-процессами
- Эволюция каналов утечек — нужна постоянная донастройка
- Баланс (разумность!!!!111!11!) во всем

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

ЧТО НАС ЖДЕТ БЕЗ DLP:

- Рост риска утечек данных
- Отсутствие контроля над каналами передачи
- Финансовые и репутационные потери
- Нарушение законодательства и штрафы
- Отсутствие расследований инцидентов!
- Возможность инсайдерских атак
- Сложность соблюдения требований партнеров

DLP — **хороша** и **важна**!

DLP, поставленная **«на сдачу»**, — **плохо**, жрет деньги, генерирует проблемы.

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

Endpoint Detection and Response (EDR) — мониторит ПК и серверы, но делает это чуть более интересно, чем антивирус: фиксирует поведение процессов, сетевые соединения, запуск скриптов и пр.

Extended Detection and Response (XDR) — это более масштабный EDR. В качестве источников данных использует сеть, почту, облака и т.д., обеспечивает корреляцию событий между системами, предоставляет единую панель управления и расследования.

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

НЮАНСЫ EDR/XDR В КОРПОРАТИВНОЙ ИБ:

- Шум и перегрузка алертами
- Сложность внедрения и настройки
- Высокие требования к компетенции сотрудников
- Интеграция с другими системами
- Баланс между безопасностью и удобством пользователей
- Дорого масштабировать (а придется!!!)

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

ЧТО НАС ЖДЕТ БЕЗ EDR/XDR:

- Плохая видимость конечных устройств
- Позднее обнаружение инцидентов
- Сложности расследования (DFIR)
- Неэффективность SOC
- Рост ущерба от атак
- Несоответствие современным стандартам безопасности

EDR и XDR — **это мощные инструменты для защиты** корпоративной инфраструктуры, которые обеспечивают высокий уровень безопасности. Однако перед внедрением важно тщательно оценить все преимущества и недостатки, а также **готовность компании к** таким **изменениям.**

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

SECURITY INFORMATION & EVENT MANAGEMENT

SIEM собирает логи и хранит события, применяет правила корреляции.

ВАЖНО:

Не реагирует автоматически (в отличие от SOAR), не защищает сама по себе — она обнаруживает и информирует, может получать данные от EDR, AV, сетевых устройств, DLP и других систем.

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

ТЕРНИИ НА ПУТИ К SIEM:

- «Мусор» на входе
- Нужно писать детальные правила под инфраструктуру
- Нужно четко понимать, что у нас есть ресурсы для ручного или автоматического реагирования на зов SIEM, иначе смысла нет

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

ЧТО НАС ЖДЕТ БЕЗ SIEM:

- Нет единой картины событий безопасности
- Плохая видимость атак в реальном времени
- SOC становится «слепым»
- Сложность расследований (DFIR)
- Несоответствие требованиям и стандартам

В масштабе без SIEM компания фактически теряет **центральный мозг мониторинга**. Все остальные системы работают, но **каждая сама по себе**, и у бизнеса нет полной картины безопасности.

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

SECURITY ORCHESTRATION, AUTOMATION & RESPONSE

SOAR — это автоматический разгребатель проблем.
Эта система не собирает данные сама, но автоматизирует реакцию.

ЧТО НАС ЖДЕТ? ХОТИМ SOAR!

- Сложность настройки и интеграции
- Разработка плейбуков
- Опасность автоматических действий
- Сопротивление со стороны других команд

  Реальность: SOAR должна вмешиваться в процессы других команд (системных админов, ИТ, службы поддержки)
- SOAR ≠ искусственный интеллект. SOAR сама ничего не решит. Она не «думает»

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

ЧТО НАС ЖДЕТ БЕЗ SOAR:

- Медленное реагирование на инциденты
- Перегрузка SOC и выгорание аналитиков
- Рост числа ошибок
- Неравномерный уровень защиты
- Трудности при масштабировании
- Финансовые последствия

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

SECURITY OPERATION CENTER

SOC — центр мониторинга информационной безопасности. Организационная единица, которая получает отовсюду сигналы, разгребает их и реагирует соответствующим образом.

ВЕЛИКИЙ И УЖАСНЫЙ!!!

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

ЧТО НАС ЖДЕТ БЕЗ SOC:

- Стоимость
- Дефицит годных кадров
- Поток инцидентов и alert fatigue
- Сложность интеграции разных систем
- Реакция на инциденты — ручная и медленная
- Сложность работы 24/7
- Отсутствие бизнес-поддержки
- Эволюция атак

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOC

DFIR

ЧТО НАС ЖДЕТ БЕЗ SOC:

- Отсутствие круглосуточного мониторинга
- Замедленное реагирование
- Нет централизованной картины угроз
- Рост числа невыявленных инцидентов
- Хаос в реагировании
- Финансовые и репутационные потери
- Отсутствие экспертизы по расследованиям
- Трудности с соответствием требованиям

SOC — это не «опция», а **необходимый элемент** зрелой киберзащиты **на определенном масштабе**.

Успешный SOC = баланс технологий (SIEM, SOAR, EDR/XDR, DLP), процессов и людей.

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOC

SOAR

DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

DFIR = расследование + реагирование на инциденты.

Работа с DFIR — это как расследовать аварию на ядерной подводной лодке, но спустя неделю, по обломкам, без доступа к бортовому журналу, с руководством, которое хочет «закрыть тему к обеду».

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOAR

DFIR

ВСЁ ТОЖЕ НЕ ПРОСТО:

- Отсутствие должной фиксации информации
- Время критично
- Необходим огромный опыт
- Мириады сложных инструментов (вендорские + опенсорс + кулибинские)
- Высокие требования к сбору и хранению данных

АНТИВИРУС

DLP

EDR/XDR

SIEM

SOAR

SOAR

DFIR

МОЖЕТ, НЕ НАДО? НАДО!

- Неясна причина инцидентов
- Нет уверенности, что атака устранена
- Отсутствие цифровых доказательств
- Невозможно отследить действия злоумышленника
- Сложности с регуляторами и правоохранительными органами
- Увеличение бизнес-рисков

ЧИТШИТ-НАПОМИНАЛКА:

ТЕХНОЛОГИЯ / СИСТЕМА	АНАЛОГ В РЕАЛЬНОМ МИРЕ	ПОЯСНЕНИЕ
Антивирус (AV)	Охранник на входе с металлодетектором	Проверяет всех входящих на наличие оружия. Реагирует на известные угрозы (сигнатуры)
EDR	Камеры в каждом кабинете + аналитик, следящий за поведением	Наблюдает за тем, что происходит внутри, фиксирует странные действия, дает тревогу
XDR	Охранная система, объединяющая камеры, датчики движения, электронные замки и пр.	Централизованная видимость — связывает поведение на входе, в кабинетах, на парковке
SIEM	Центр управления с журналами и архивом событий	Хранит и анализирует данные со всех систем: кто зашел, что открыл, куда пошел
SOAR	Система автоответа и реагирования: тревога → блокировка двери → вызов охраны	При обнаружении угрозы запускает заранее запрограммированные действия
DLP	Рентген на выходе, который проверяет, не выносят ли секретные документы	Контролирует, чтобы никто не уносил конфиденциальные данные
SOC	Комната охраны с круглосуточным дежурством	Команда наблюдает за всеми сигналами, реагирует на тревоги, координирует действия
DFIR	Следственная группа после инцидента: анализ отпечатков, журналов, допрос охраны	Расследует, что произошло, как вор проник, что украл и как это предотвратить в будущем

ВМЕСТО ВЫВОДА:

- Не ведитесь на голую рекламу
- Оценивайте, советуйтесь, коммуницируйте, считайте все в цифрах (не хотите думать — идите к пентестерам)
- При отсутствии адекватного подхода любой инструмент (даже антивирус) — это просто дорогая, жрущая деньги и нервы игрушка

СПАСИБО

КОНТАКТЫ:

+7 (495) 909-92-78

clients@mko-systems.ru

mko-security.ru