Managed Detection and Response

Как наиболее эффективный способ организации мониторинга и реагирования на угрозы ИБ

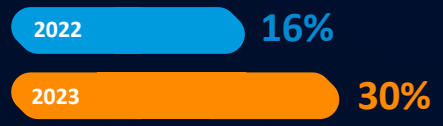
UZTELECOM

uztelecom.uz

Рост количества и сложности атак

На фоне 5.500 киберпреступлений*, совершенных в Республике Узбекистан в 2023 году, в 1 квартале 2024 предпринято **более 3 миллионов попыток кибератак.** В скором времени следует ожидать роста количества атак шифровальщиков и кибершпионажа в коммерческих, промышленных и государственных организациях, что спровоцирует спрос на сервисы, обеспечивающие их реальную безопасность.

Эксплуатация действующих учетных данных



Эксплуатация уязвимостей в общедоступных приложениях

Фишинг

*https://kun.uz/en/news/2023/12/21/5500-cybercrimes-committed-in-uzbekistan-in-2023
**IBM X-Force Threat Intelligence Index 2024

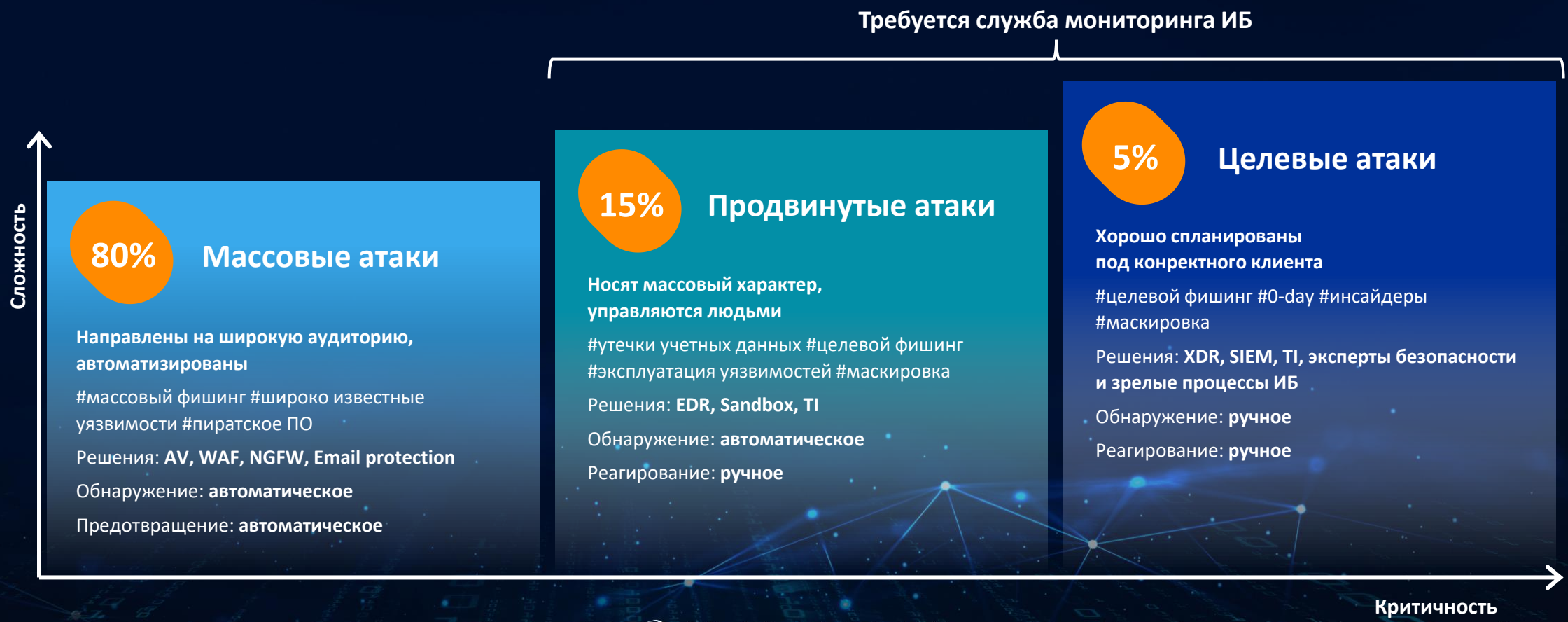
UZTELECOM

uztelecom.uz

Разные типы кибератак требуют разных подходов к защите

Превентивные средства защиты (такие, как антивирусы, межсетевые экраны, системы предотвращения вторжений) помогают в борьбе с типовыми угрозами. Однако, сегодня организовать «продвинутую» атаку группам злоумышленников становиться все проще и дешевле.

Обнаружить и предотвратить такие инциденты можно только с использованием полу-автоматических систем под управлением экспертов ИБ.



UZTELECOM

uztelecom.uz

Архитектура противодействия целевым атакам

Для того, чтобы в современных условиях компания могла своевременно выявлять угрозы в своей сети, а также оперативно и четко реагировать на них – ей необходимо реализовать целый комплекс мер.

Но, к сожалению, практика показывает, что далеко не каждая организация имеет возможность содержать собственную группу мониторинга и реагирования на кибер-угрозы.

ПРОЦЕССЫ

Работа центра мониторинга – это непрерывные рутинные процессы разбора массы событий и четкая последовательность действий в случае обнаружения угрозы.

Для того, чтобы их реализовать, требуются специфические знания и опыт.

ТЕХНОЛОГИИ

Актуальный стек технологий для мониторинга и реагирования включает:

- **SIEM и XDR** для обнаружения угроз
- **Threat Intelligence** для актуализации баз индикаторов компрометации
- **IRP и SOAR** платформы для автоматизации анализа и работы над инцидентами

Не каждая организация может совершить такие инвестиции в собственную службу мониторинга ИБ.

ЛЮДИ

Для эффективной отделы собственной службы мониторинга требуется собрать и развивать обширную команду дорогостоящих экспертов:

- **Не менее 6ти аналитиков** для работы в режиме 24/7
- **Инженеров ИБ** для поддержки средств мониторинга
- **Экспертов ИБ** для актуализации набора правил обнаружения угроз

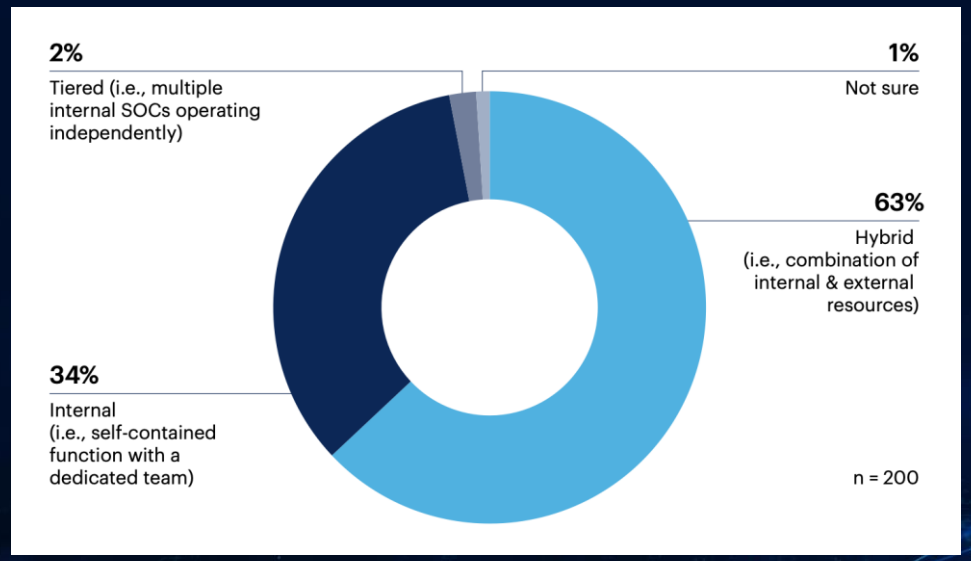
В условиях глобального дефицита кадров это также зачастую непосильная задача.

Мировой опыт: приоритет сервисной модели ИБ

В результате, глобальным трендом становится применение гибридной модели обеспечения информационной безопасности, при которой функции непрерывного мониторинга угроз отдаются на аутсорс специализированным организациям – SOC провайдерам или MSSP.

Такие компании, обеспечивая безопасность большого количества клиентов, позволяют последним получить доступ к высокому уровню экспертизы, а также лучшим технологиям обнаружения угроз без необходимости совершать капитальные вложения, а также рисков и сложностей, связанных с задачами построения собственных SOC команд.

1. **63% респондентов Gartner Peer Community** используют гибридную модель SOC, комбинируя собственные и внешние ресурсы



- Modern Security Operations Center (SOC) Strategies, Gartner Peer Communtiy

2. *К 2025 году, 33% организаций с собственной службой ИБ предпримут попытки построить внутренний SOC и потерпят неудачу ввиду недостатка бюджета, экспертизы и кадров.*

- SOC Model Guide, 2023, Gartner

3. *К 2025 году, 90% SOC крупнейших компаний G2000 будут применять гибридную модель SOC, отдавая на аутсорс не менее 50% своей операционной нагрузки.*

- Gartner

MANAGED DETECTION AND RESPONSE – Сервис UZTELECOM

UZTELECOM и **HWG Sababa** предлагают совместную реализацию сервиса кибербезопасности для корпоративных клиентов, который позволит обеспечить актуальный уровень зрелости процессов мониторинга и реагирования на киберугрозы с максимальной эффективностью инвестиций

UZTELECOM MANAGED XDR 24/7

Для широкого круга корпоративных клиентов

Мониторинг угроз | Реагирование на угрозы | Расследование инцидентов | Внедрение и поддержка EDR / XDR

Мониторинг ключевых элементов инфраструктуры: ПК, серверов и сети

HWG Sababa

Партнер сервиса: HWG Sababa (Италия)

- Глобальный SOC провайдер. На рынке с 2011 года
- Реализовано более 150 проектов SOC
- Полная локализация SOC в Республике Узбекистан

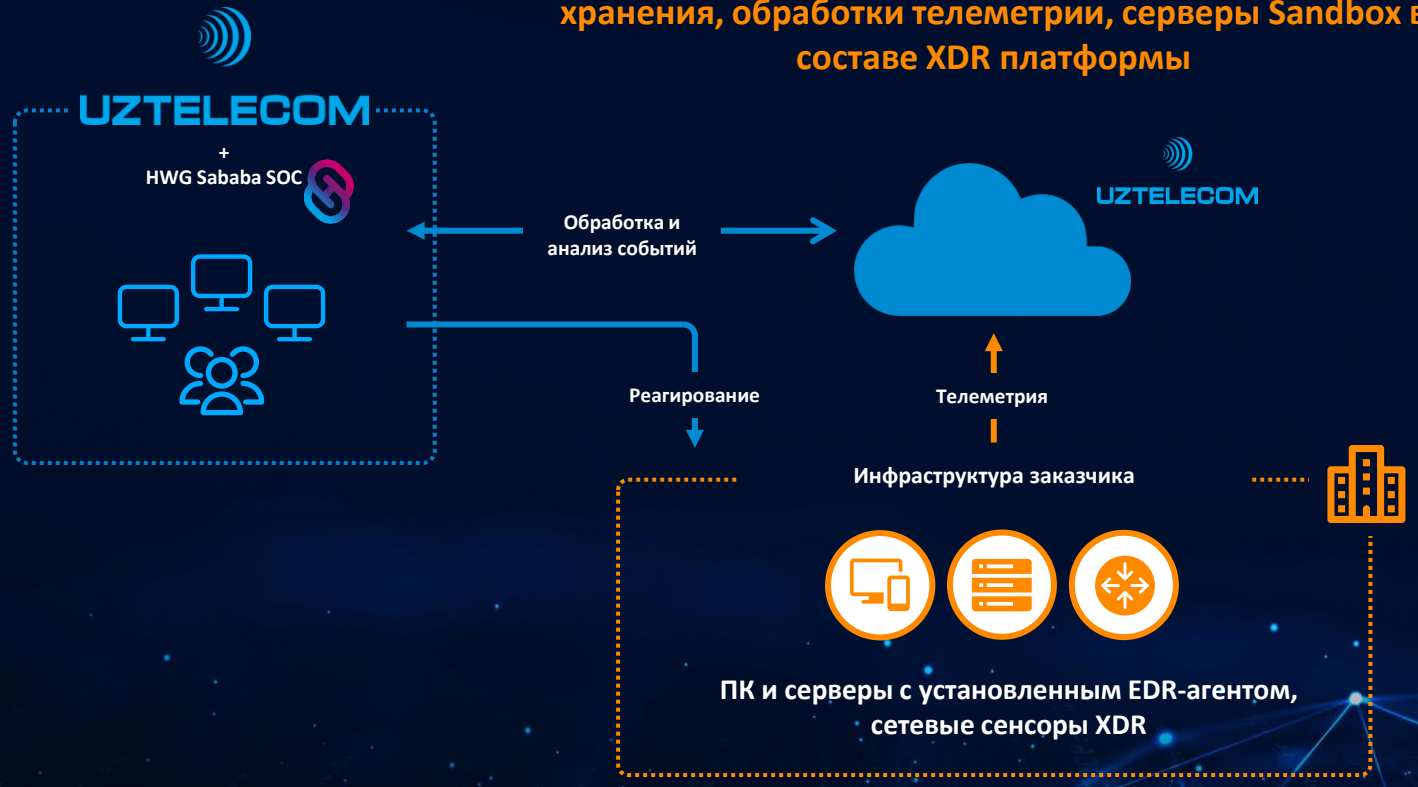
UZTELECOM

uztelecom.uz

Описание сервиса

MXDR (Managed Extended Detection and Response) **– это самый эффективный сервис по мониторингу и реагированию на угрозы ИБ,** который сочетает в себе высокий уровень обнаружения угроз и возможность их гранулярного анализа аналитиками сервиса с простотой и оперативностью развертывания. Сервис не предъявляет высоких требований к зрелости Заказчика – достаточно установить агенты и сенсоры в своей сети.

Сервис оказывается на базе облачной инфраструктуры хранения, обработки телеметрии, серверы Sandbox в составе XDR платформы



Сервис оказывается на базе XDR платформы GROUP-IB

СОСТАВ УСЛУГИ

UZTELECOM
Managed Detection and Response

- 24/7 мониторинг событий XDR
- Обработка и анализ событий безопасности
- Уведомление заказчика об инцидентах
- Формирование инструкций по реагированию
- Реагирование силами ИТ и ИБ Заказчика
- Отчетность

Преимущества сервиса

Облачный сервис

Сервис развернут в облаке Узбекистана, от заказчика требуется только установить агенты и сенсоры в своей инфраструктуре. Все остальные задачи берут на себя Uztelecom и HWG Sababa

Продвинутая защита

Заказчик находится под постоянной защитой, в том числе от продвинутых и целевых угроз. С заказчиком ведется полноценная коммуникация по выявленным угрозам.

Экспертиза «из коробки»

В качестве технологической платформы используется XDR-решение с встроенными детектирующими логиками, а для расследования и выявления неизвестных угроз — телеметрию непрерывно изучают аналитики HWG Sababa

Сокращение расходов

За счет того, что управление сервисом берет на себя Uztelecom и HWG Sababa, заказчик может тратить освободившиеся внутренние ИТ-ресурсы на более приоритетные задачи

Быстрый старт

В отличие от более сложного Managed SOC, MXDR сервис лицензируется по количеству рабочих станций и серверов, а его запуск в пилотном режиме можно осуществить за 1 неделю.

Экономическая эффективность сервиса

Сравнение TCO: Сервис MDR PRO vs Собственный SOC (Средняя инфраструктура на 500 рабочих станций)

Альтернативой нашего сервиса для заказчика является создание собственной службы мониторинга ИБ и внедрения нужного стека технологий. Рассмотрим оценку совокупных затрат Заказчика, необходимых для того, чтобы обеспечить аналогичный уровень защиты.

Категория затрат	Сумма в год	Комметарии
Продукт (EDR)	$50,000	Лицензии EDR ($100/endpoint/год)
Команда SOC	От $60,000 до $180,000	От 2х чел (1 junior + 1 senior) при мониторинге 8/5 до 7ми чел (6 junior + 1 senior) при мониторинге 24/7
Threat Intelligence	$10,000	Базовый TI feed от внешнего провайдера
Инфраструктура	$5,000	Амортизация on-prem серверов, хранилища, лицензий ОС и БД (на 3 года)
Инструменты и автоматизация	От $10,000 до $200,000	Open-source или коммерческие SIEM/SOAR и IRP
Обучение персонала	От $5,000 до $20,000	Обучение и сертификация от 2 до 7 сотрудников
ИТОГО	От $140,000 до **$465,000 (24/7)**	

Итого собственный SOC: От $140,300 (при мониторинге 8/5) до **$465,000 (24/7) в год.**

Готовность к эксплуатации: от 12 мес

Сервис MDR PRO 24/7: $ 120 000 в год

Готовность к эксплуатации: 1 мес

СПАСИБО

Контакты: Дамир Зарипов
Менеджер продаж UZTELECOM
+998 95 008 01 75