FortiEDR Managed Detection and Response

Сервис Managed Detection and Response (далее MDR) оказывается на базе облачного решения FortiEDR.

В рамках сервиса команда Fortinet выполняет мониторинг и анализ угроз 24/7, а именно:

1. Обзор и анализ всех событий безопасности, отображаемых в консоли управления FortiEDR:
    a. Статический и динамический анализ ВПО
    b. Анализ процессов в оперативной памяти
    c. При необходимости артефакты атаки могут быть собраны с конечных узлов для последующего анализа (например, записи Windows Event log, файлы, журналы приложений, данные браузера и др.)
2. Управление событиями безопасности:
    a. Валидация и классификация событий
    b. Расследование и отчет об обнаруженном ранее неизвестном ВПО или потенциально опасных приложениях. При обнаружении вредоносной активности или потенциально нежелательной программы заказчику направляется письмо с описанием угрозы и рекомендациями по реагированию и дальнейшим шагам при устранении угрозы. Для событий, классифицированных как вредоносные (malicious) данное письмо будет выслано в течение 60 минут. По требованию заказчик может запросить звонок для уточнения данных об угрозе, а также рекомендаций по устранению угрозы, включая помощь в конфигурации плэйбуков FortiEDR.
    c. Звонки раз в квартал в квартал с обзором событий, сводкой по оказанному сервису. Данное ревью может включать в себя следующие пункты:
        i. Обзор покрытия устройств агентами FortiEDR
        ii. Обзор работоспособности решения (health status)
        iii. Обзор обнаруженных угроз
        iv. Тренды по управлению угрозами

Подробное описание сервиса доступно по следующей ссылке:
https://fortinet.egnyte.com/dl/dBqqF7q6FG