

Cyberbit SOC 3D

Оркестрация, Автоматизация и Реагирование в ИБ






Недостатки управления SOC

В условиях все более сложных сред реагирования на инциденты компании и MSSP ищут способы масштабирования своих возможностей, сокращения среднего времени реагирования, повышения качества обслуживания и оптимизации операционной деятельности. Испытывая сложности, охватывающие персонал, процессы и технологии, руководители SOC сталкиваются и с критическими препятствиями в управлении:

- Огромный объем срабатываний
- Многочисленные средства защиты
- Недостаток опытных профессионалов
- Возросшие нормативные требования
- Отсутствие совместимых процессов и методик
- Критичные во времени атаки
- Многовекторные (IT-OT-IoT) угрозы

Cyberbit SOC 3D один экран для полной автоматизации

В решении этих задач командам SOC помогает Cyberbit SOC 3D, представляющий собой платформу оркестровки, автоматизации и реагирования (SOAR), которая сокращает до 90% среднее время реагирования за счет оптимизации всего жизненного цикла инцидента. Развернув Cyberbit SOC 3D, Вы сможете:

-  Принимать срабатывания и логи с любых SIEM, SOC-систем и других источников событий
-  Ускорять реагирование на различные типы инцидентов с помощью как имеющихся: таких как фишинг, вирусы- вымогатели, DDoS и другие; так и настраиваемых пользователем плейбуков.
-  Автоматизировать повторяющиеся ручные операции, такие как сбор и обогащение данных, ускоряя процессы реагирования на инциденты с часов до минут или секунд
-  Автоматически приоритезировать инциденты, чтобы сосредоточиться на том, что действительно важно
-  Реагировать с использованием одной консоли, сокращая затраты времени вашей команды

Показатели реальных кейсов

Повышение KPI у внедривших SOC 3D компаний:

90%

Сокращение времени реагирования

50%

Сокращение количества эскалаций

3x

Увеличение числа обработанных за смену инцидентов

100%

Критических инцидентов решено



Рис. 1: Cyberbit SOC 3D – единая консоль «Инцидент – Реагирование»

Как это работает

Cyberbit SOC 3D ускоряет и оптимизирует реагирование на инциденты, используя многочисленные механизмы:

- 1** Автоматизирует сбор индикаторов компрометации со всей цифровой базы клиента
- 2** Автоматизирует расследование и сортировку инцидентов с использованием аналитики на основе больших данных
- 3** Автоматизирует процессы с помощью готовых или создаваемых пользователем плейбуков
- 4** Управляет восстановлением с единой консоли используя весь ваш арсенал средств обеспечения безопасности
- 5** Обеспечивает KPI, данные форензики и информационные панели с полным архивом инцидентов



Рисунок 2: Единая консоль Инцидент – Реагирование

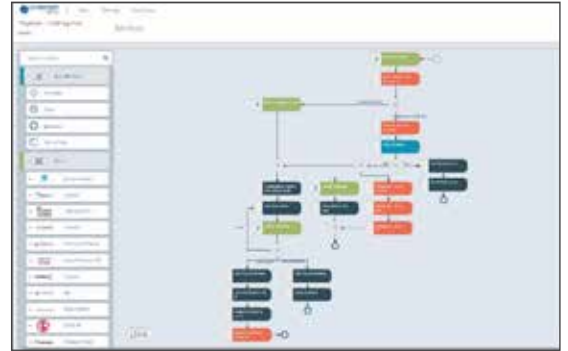


Рисунок 3: Легкий конструктор процессов

Чем отличается Cyberbit SOC 3D

- Богатый каталог плейбуков для 30 типов атак
- Интуитивно понятный конструктор процессов
- Не зависит от SIEM и поддерживает несколько SIEM одновременно
- Единая консоль Инцидент-Реагирование для всего жизненного цикла инцидента
- Возможности информационных панелей для расследований на базе (опциональной) платформы больших данных, обрабатывающей все «сырые» данные
- Неограниченная интеграция со средствами защиты и средствами работы с заявками

Интегрирована с ведущими решениями по ИБ



Готовы оценить SOC? Свяжитесь с нами для демонстрации: <https://www.cyberbit.com/>

О CYBERBIT™

Cyberbit предлагает платформу обнаружения и реагирования для защиты ИТ, ОТ и IoT сетей: поведенческий анализ, автоматизация и оркестровка обработки инцидентов и защита SCADA и лидирующий в мире кибер-полигон. Продукты Cyberbit разработаны и апробированы в самых жестких условиях.

С момента основания в 2015 продукты Cyberbit применяются и крупнейших компаниях, государственных и образовательных организациях и MSSP по всему миру. Cyberbit – подразделение Elbit Systems (NASDAQ: ESLT) имеет офисы в Израиле, Европе и Азии.

sales@cyberbit.com | www.cyberbit.com

US Office:
Cyberbit Inc.
9442 North Capital of Texas Highway, Suite
500, Austin, TX 78759 | Tel: +1.512.676.8731

Офис в Израиле:
Cyberbit Ltd.
22 Zarhin St. Ra'anana Israel 4310602
Tel: +972.9.779.9831

Singapore Office:
Cyberbit Singapore Pte. Ltd.
Temasek Avenue Centennial Tower
#21-23 Singapore 039190 | Tel: +65.6679.5771

PROPRIETARY INFORMATION

The information in is proprietary and includes trade secrets of Cyberbit Ltd. It shall not be utilized other than for the purpose for which it has been provided.

