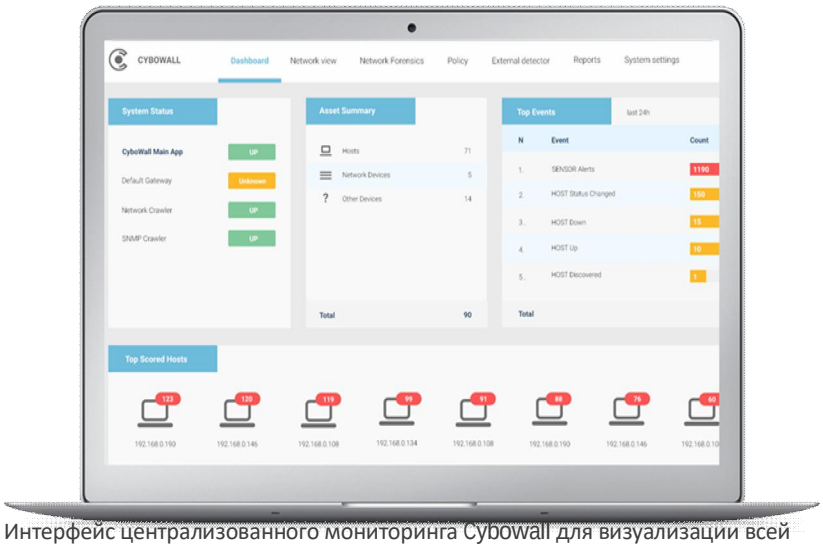
Cybowall™

ОБНАРУЖЕНИЕ УГРОЗ, ВИЗУАЛИЗАЦИЯ СЕТИ И УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ



Интерфейс централизованного мониторинга Cybowall для визуализации всей сети и составления отчетов

ОБЗОР РЕШЕНИЯ

Cybowall — это не требующее установки агента неинтрузивное решение, которое обеспечивает постоянный мониторинг всей вашей сети по всем используемым протоколам и всем периферийным устройствам. Решение Cybowall защищает сеть в режиме реального времени, обнаруживает угрозы и оперативно реагирует на них. Сократите риски в своей организации за счет визуализации всей сети. Решение Cybowall предоставляет организациям следующие возможности:

- Быстрое обнаружение активных угроз
- Идентификация и минимизация потенциальных уязвимостей
- Управление и отчеты о соответствии нормативным требованиям (GDPR, PCI-DSS, ISO и т. п.)
- Запись и анализ информации обо всех событиях и инцидентах внутри сети для дальнейшего исследования

Решение Cybowall объединяет в себе множество инструментальных средств кибербезопасности, комплексно защищая сети любого размера в условиях постоянно усложняющихся угроз.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- **Предотвращение атак вредоносного ПО и несанкционированного вмешательства в работу периферийных устройств**: обнаружение современных постоянно активных угроз в сети и на периферийных устройствах
- **Отображение сетевых ресурсов**: улучшенная визуализация среды с отображением всех периферийных устройств, подключенных к вашей сети
- **Идентификация уязвимостей**: актуальная информация об уязвимостях для определения приоритетов развертывания патчей
- **Обнаружение «горизонтального движения**: «ловушки» для злоумышленников, сумевших преодолеть защитный периметр организации
- **Обнаружение активных угроз**: оперативное выявление сетевых угроз с целью снижения их вредного воздействия
- **Соблюдение нормативных требований**: обеспечение соответствия нормативным стандартам GDPR, ISO, PCI-DSS, HIPAA и т. п.

ФУНКЦИИ РЕШЕНИЯ

Обнаружение угроз

- Обнаружение вторжений: Функции обнаружения угроз без помех для работы сети
- Сетевые «ловушки»: информация о «горизонтальном движении» между периферийными устройствами и обнаружение угроз — «приманка» для активных сетевых атак
- Сетевая криминалистическая экспертиза Изучение инцидентов и анализ источников атак на систему безопасности

Визуализация сети

- Отображение ресурсов: динамическое отображение ресурсов всех периферийных устройств, включая профили портов и выполняемые операции
- Функции WMI: использование функций WMI и постоянное сканирование периферийных устройств для полной визуализации сети
- Технология SIEM: управление журналами, управление событиями, корреляция событий и составление отчетов, помогающих идентифицировать нарушение политики и активировать процедуры отклика

Управление уязвимостями

- Оценка уязвимостей: мониторинг бизнес-ресурсов и идентификация уязвимых систем внутри сети, в том числе определение уровня риска и приоритетов развертывания патчей
- Пароли по умолчанию: выявление и замена паролей, установленных по умолчанию, для снижения уровня риска
- Поиск вредоносного ПО: выявление файлов с вредоносным ПО и их местоположения в сети

ТЕХНИЧЕСКОЕ ОПИСАНИЕ

Решение Cybowall собирает и анализирует информацию о периферийных устройствах и сетевых событиях. Благодаря датчику, не подключенному к сети напрямую, но проверяющему копию всего сетевого и внутреннего трафика через сетевой отвод/дублирование трафика, решение Cybowall на уровне сети выполняет функцию системы обнаружения вторжений. Кроме того, решение Cybowall производит сканирование без установки агента с использованием функций WMI и других технологий. С их помощью решение собирает детальные криминалистические данные и сопоставляет их с известными индикаторами компрометации (IOC). Благодаря централизованной агрегации действий по всей сети решение Cybowall получает индикаторы компрометации. В их числе общий перечень уязвимостей и рисков, хеш-суммы файлов, имена DNS, URL-адреса, названия хост-систем, IP-адреса, домены, универсальные идентификаторы ресурсов и пути доступа к файлам. С помощью технологии сетевых «ловушек», подключаемых непосредственно к основному сетевому коммутатору по протоколу SNMP, решение Cybowall обеспечивает непрерывную визуализацию сети и эффективно выявляет угрозы.