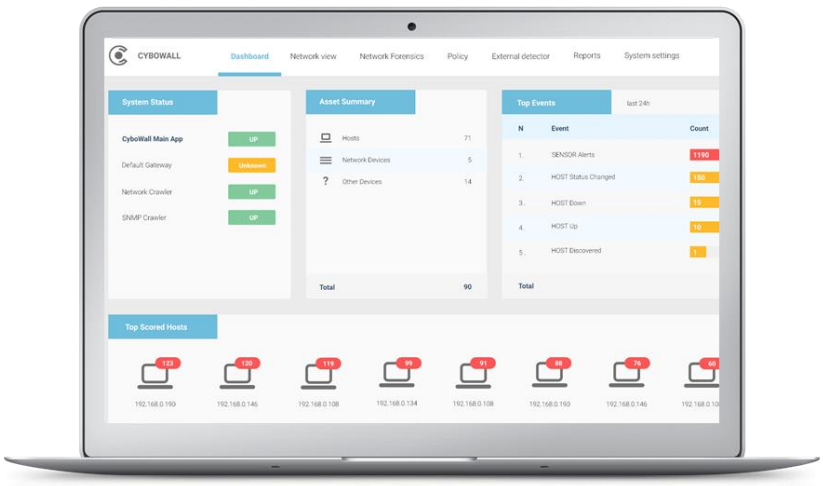
Cybowall™

СЕТЕВАЯ ВИДИМОСТЬ, УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ И ОБНАРУЖЕНИЕ НАРУШЕНИЙ



Интерфейс централизованного мониторинга Cybowall

ОБЗОР РЕШЕНИЯ

Cybowall - это неинтрузивное, безрисковое решение, которое обеспечивает полный и непрерывный мониторинг вашей сети по всем протоколам и распространяется на все конечные точки. Cybowall защищает вашу сеть в режиме реального времени; выявляя и реагируя на угрозы по мере их возникновения. **Уменьшите риски для своей организации, получив полную информацию о вашей сети.** Cybowall позволяет организациям:

- Быстро обнаруживать актуальные нарушения
- Определять и сокращать потенциальные уязвимости
- Готовить отчётность о соответствии (GDPR, PCI-DSS, ISO и т.д.)
- Записывать и анализировать все события и инциденты в сети для дальнейшего расследования

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Заблокировать атаку или вредоносное ПО: использование сети и конечных устройств для обнаружения постоянных целевых угроз
- Карта сетевых ресурсов: увеличивает видимость сети благодаря карте всех подключённых конечных точек, чтобы получить представление об окружении
- Выявление уязвимостей: будьте в курсе всех уязвимостей для определения приоритетов по их исправлению
- Обнаружение подозрительных активностей: ловушка для тех, кто уже нарушил внешний периметр
- Обнаружение нарушений: быстро обнаруживайте сетевые бреши, чтобы уменьшить разрушительные последствия
- Соответствие требованиям: придерживайтесь стандартов соответствия: GDPR, ISO, PCI-DSS, HIPAA и т.д.

Cybowall в едином решении сочетает в себе множество инструментов и возможностей для обеспечения информационной безопасности - обеспечивает безопасность для сетей всех размеров и в рамках единой защиты от постоянно развивающегося ландшафта угроз.

ОСОБЕННОСТИ РЕШЕНИЯ

Видимость сети

- **Отображение активов**: Динамическая карта активов для всех конечных точек, включая профили портов и их виды деятельности
- **WMI**: Использование WMI и непрерывного сканирования конечных точек для получения полной видимости сети
- **Возможности SIEM**: Управление журналом, управление событиями, корреляция событий и отчётности, чтобы помочь выявить нарушения правил и разрешить процедуры реагирования

Управление уязвимостями

- **Оценка уязвимости**: Мониторинг бизнес-активов и определение уязвимых систем внутри сети, включая оценку уровня риска, для определения приоритетов развёртывания патчей
- **Стандартные и слабые пароли**: Позволяет определить и изменить стандартные / слабые пароли для снижения рисков
- **Охотник за вредоносным ПО**: Идентифицируйте вредоносные файлы и где они находятся в сети

Обнаружение нарушений

- **Обнаружения вторжений**: Возможности обнаружения нарушений без сетевых помех
- **Сетевые ловушки**: Выявление нелегитимного трафика между оконечными точками и обнаружение угроз, выступая в качестве ловушки для активных атак
- **Сетевая экспертиза**: Обнаружение и анализ источника атак и инцидентов системы безопасности

ТЕХНИЧЕСКИЙ ОБЗОР

Решение Cybowall собирает и анализирует информацию как о конечных точках, так и сетевых событиях. Решение получает копию всего сетевого и внутреннего трафика через TAP / Port Mirroring, Cybowall функционирует как IDS на сетевом уровне. Cybowall также использует «Агентное сканирование», которое использует совместно с другими технологиями, возможности WMI для сбора подробных данных для исследования и корреляции с известными индикаторами компромисса (IOC). Благодаря централизованному обзору активности в сети, Cybowall получает данные, такие как CVE, хэш файла, DNS, URL, имена хостов, IP-адреса, домены, URL и пути к файлам. Используя технологию ловушек в сети и напрямую подключаясь к главному коммутатору сети через SNMP, Cybowall обеспечивает непрерывную видимость сети и эффективное обнаружение нарушений.