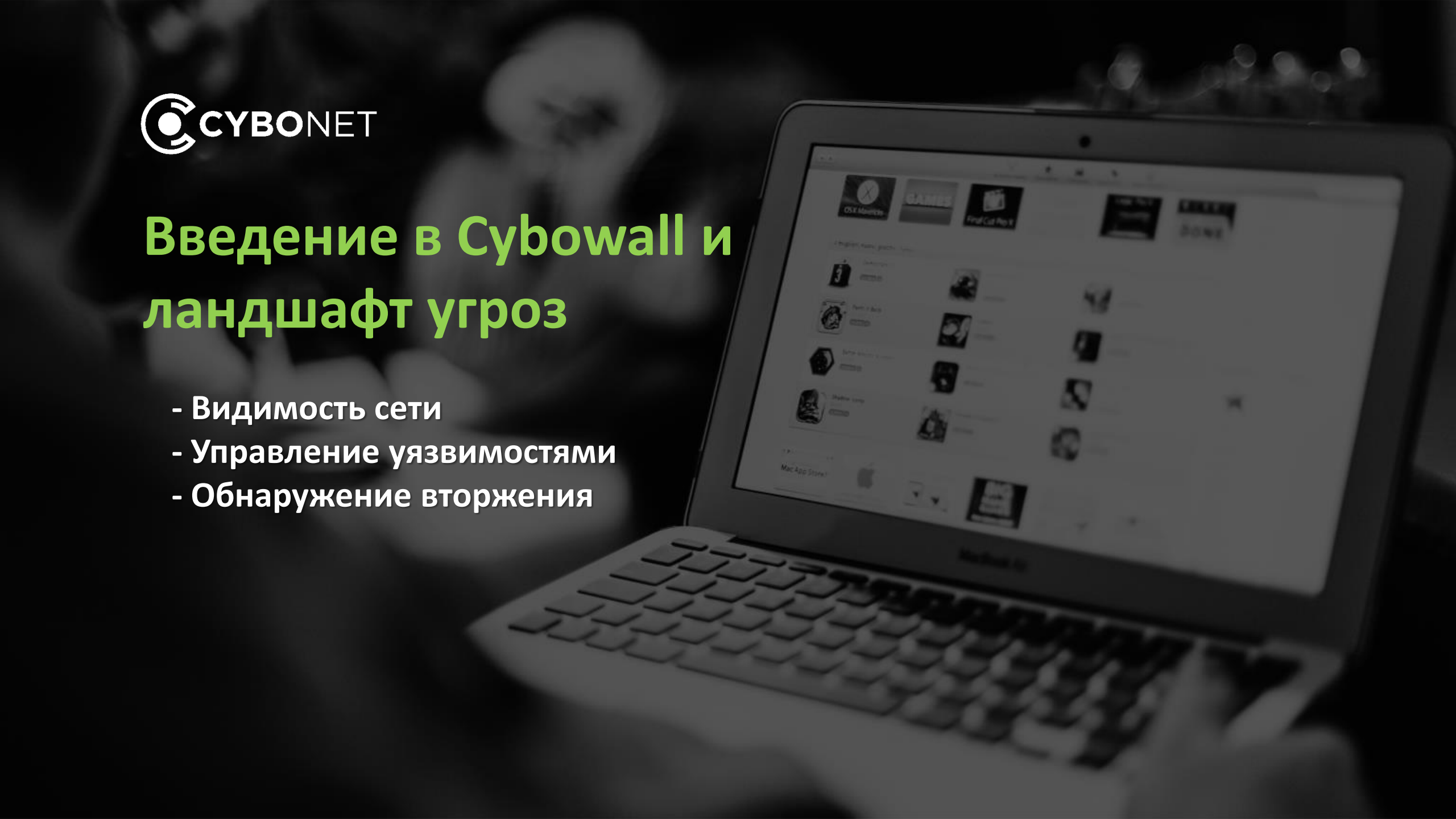
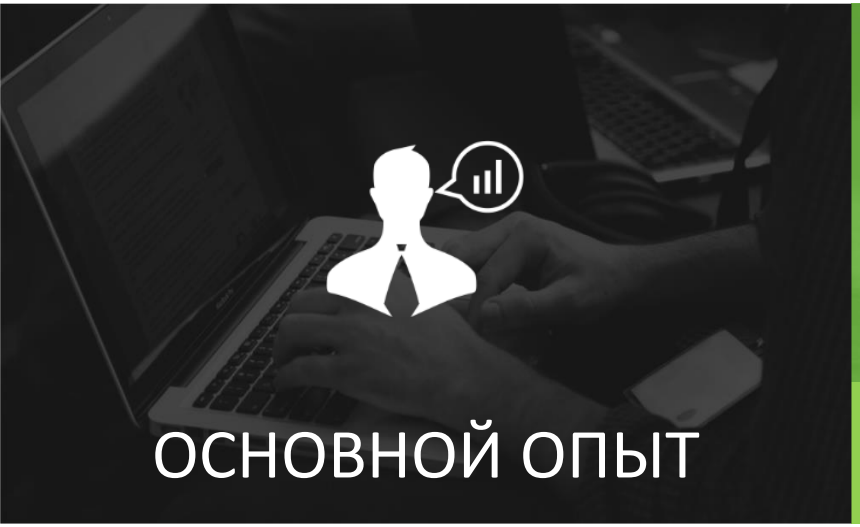
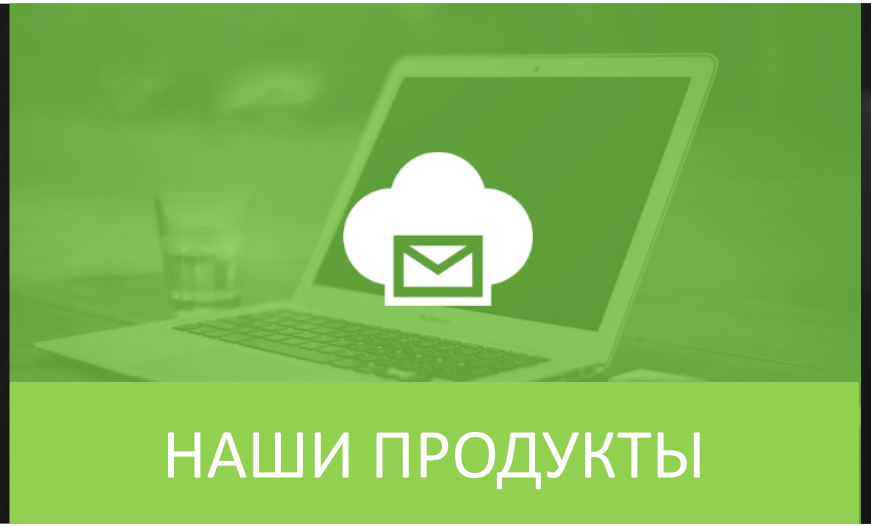

CYBONET
Введение в Cybowall и ландшафт угроз
- Видимость сети
- Управление уязвимостями
- Обнаружение вторжения

Немного о CYBONET



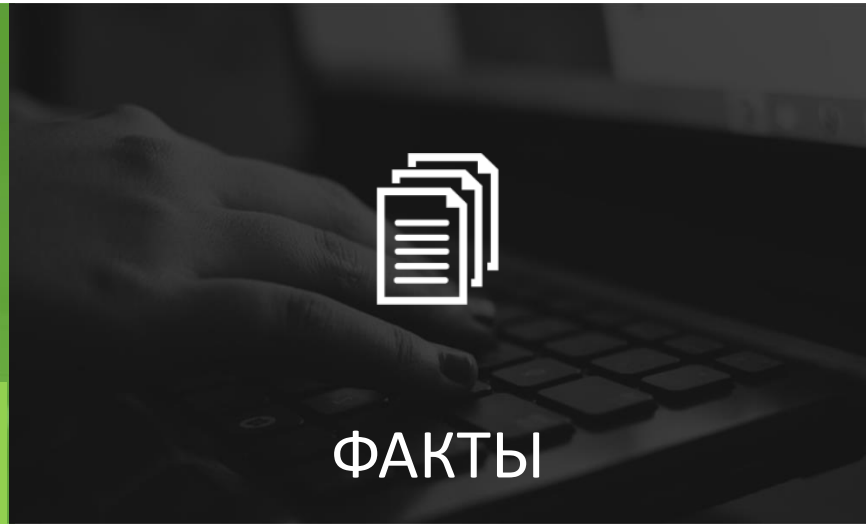
ОСНОВНОЙ ОПЫТ

- Ведущая компания, обслуживающая множество рынков
- Развертывание и управление крупномасштабными корпоративными облачными платформами
- Управляемые услуги, корпоративные программы, SaaS
- Установка Telco по всему миру
- Инноватор и лидер в области борьбы с ботнетом



НАШИ ПРОДУКТЫ

- Сайбовол:
  - Видимость сети, Управление уязвимостями, Обнаружение вторжения
- Пайнэп – Безопасность Эл. почты:
  - Продвинутый обмен сообщений
- Сайбоклауд:
  - Облачное решение Пайнэпа
- Исходящий спам-гвард (OSG):
  - Защита от вноса IP в черный список для телекоммуникаций



ФАКТЫ

- Штаб, техподдержка, разработка и исследования находятся в Израиле
- В частной собственности
- Глобальная компания с партнерами в Северной Америке, Европе, СНГ и Дальнем Востоке
- Наши продукты установлены в более 60 странах

ГЛАВНЫЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ МСБ

РЕСУРСЫ И ЭКСПЕРТИЗА

МСБ сталкиваются с теми же угрозами, с меньшим количеством ресурсов и нехваткой экспертизы

ВОССТАНОВЛЕНИЕ ОТ КИБЕР-АТАК

33% МСБ компаниям заняло 3 дня, чтобы оправиться от атаки, а 60% МСБ потеряли свой бизнес в течение 6-ти месяцев после атаки

ЦЕНА УТЕЧКИ ДАННЫХ

Восстановление от утечки данных МСБ стоит в области 36,000 до 50,000 долларов

ГЛОБАЛЬНАЯ ЦЕЛЬ АТТАКИ

43% глобальных атак целились на МСБ с менее чем 250 сотрудников (на 9% больше, чем в предыдущем году)

ЦЕЛЕВОЙ ФИШИНГ

Зафиксирован рост на 55% по сравнению с предыдущим годом в количестве фишинговых кампаний, ориентированных на все бизнесы

ПЛАН РЕАГИРОВАНИЯ НА КИБЕРАТАКИ

8 из 10 МСБ не имеют базового ответного плана на кибер-атаку

CYBONET

CYBOWALL СОВ СПОСОБНОСТИ

- Сетевой датчик TAP / Port Mirroring берет копию всего входящего и исходящего трафика для полной видимости
- Аномальные / подозрительные действия пользователя или службы идентифицируются анализированием захваченного сетевого трафика
- Использует СОВ механизм мониторинга Suricata с открытым исходным кодом
- Использует фингерпринтинг конечных точек и файлов для обнаружения, классификации и мониторинга подключенных устройств и данных, включая нетрадиционные конечные точки
- Нулевое вмешательство в деятельность организации
- Не выявляет мониторинг трафика потенциально вредоносным источникам

COB ПОЧЕМУ ЭТОГО НЕДОСТАТОЧНО?

- COB всего лишь прислушивается к трафику, пассивно мониторит и уведомляет
- Несмотря на то, что трафик контролируется, и результаты могут быть сообщены администратору, COB не может автоматически предпринимать действия, чтобы предотвратить обнаруженный эксплойт системы
- Как только сеть взломана, уязвимости могут быть использованы очень быстро; сам по себе, COB не может обеспечить адекватный ответ
- COB может быть подвержен «ошибочным результатом»; требует эффективной настройки и интерпретации

CYBOWALL СПОСОБНОСТИ СЕТЕВЫХ ЛОВУШЕК

- Позволяет понять поперечное перемещение между конечными точками, способен обнаруживать угрозы, возникающие внутри сети
- Распределенная ложная сеть замедляет и останавливает автоматические атаки, такие как черви или авторутеры, которые рандомальным образом сканируют сеть для выявления уязвимых систем
- Поражает человеческие атаки, уводя атакующего; побуждая их тратить свое время, не причиняя ни вреда, ни потерь
- Обнаруживает злоумышленников, которые нарушили защиту периметра сети, чтобы организация могла анализировать, смягчить и доложить об этих нарушениях

СЕТЕВЫЕ ЛОВУШКИ ПОЧЕМУ ИХ НЕДОСТАТОЧНО?

- Не заменяет механизмы безопасности; Сетевые ловушки всего навсего улучшают общую архитектуру безопасности
- Узкое поле зрения; сетевые ловушки видят только активность, направленную против них
- Злоумышленник, который идентифицирует сетевую ловушку, может избежать этого и проникнуть в организацию

CYBOWALL ОЦЕНКА УЯЗВИМОСТИ И ЕЁ СПОСОБНОСТИ

- Интегрированное решение, включающее сопоставление объектов, обнаружение вторжений, SIEM и оценка уязвимостей, все на единой панели.
- Круглосуточно сканирует сетевые системы и устройства для обнаружения и выявления уязвимостей по мере их возникновения.
- Коллекционирует данные и их детали, сравнивая с современной базой данных угроз, включая известные индикаторы разоблачения (IOC)
- Уведомляет об уязвимостях к примеру, не обновленные программы, неподтвержденные установки программ, ошибки конфигурации, отсутствие безопасности конечных приборов и слабые пароли.

ОЦЕНКА УЯЗВИМОСТИ ПОЧЕМУ ЕЁ НЕДОСТАТОЧНО?

- Если её изолировать, оценка уязвимости не обеспечит всю нужную информацию чтобы эффективно приоритизировать ответные шаги.
- Точно расчитанные проверки являются ключем удостоверения в том что "ошибочный негатив" и "ошибочный позитив" не повредят анализу.
- Результаты оценки зависят от качества данных, используемых для перекрестных ссылок
- Важные задачи, такие как установка патчей, требуют своевременной реализации

CYBOWALL SIEM СПОСОБНОСТИ

- Объединяет вывод из многовекторного решения; Сетевой датчик, сетевые ловушки, безагентное сканирование конечной точки
- Корреляция и анализ событий по разным источникам в сети
- Панель; интуитивный интерфейс для оптимизации мониторинга и обнаружения нарушений
- Включает: корреляция событий, оповещения, реагирование на инциденты и отчетность

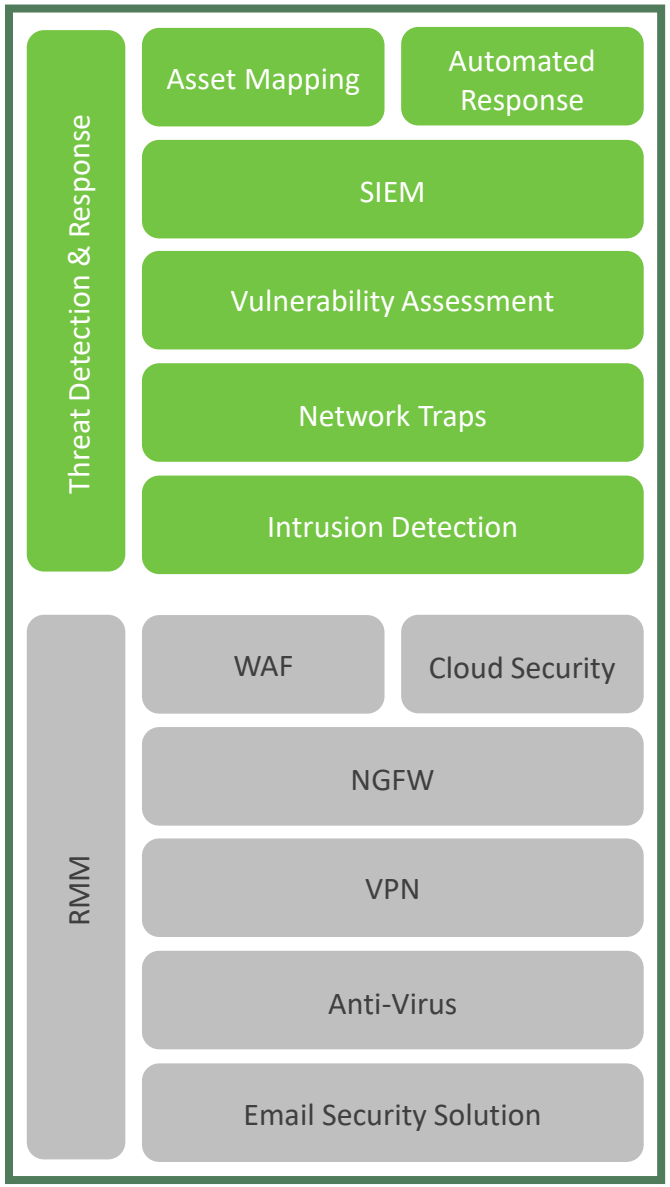
SIEM ПОЧЕМУ ЕГО НЕДОСТАТОЧНО?

- Сложный в настройке и управлении, включая сбор данных, нормализацию, корреляцию
- SIEM занимает много времени для развертывания.
- Данные отчета часто не поддаются действию, их трудно понять и они содержат слишком много «шума»
- Аналитические возможности могут быть ограниченными для текущего ландшафта угроз; недостаточно гибкий и быстро реагирующий чтобы противодействовать продвинутым постоянным угрозам
- SIEM требует значительных инвестиций; стоимость решения, стоимость найма и обучения специалистов по безопасности / консультантов для анализа и эксплуатации данных

CYBONET

CYBOWALL НАША ЦЕЛЬ

CYBONET МАРКЕТНАЯ ВОЗМОЖНОСТЬ ДЛЯ ОДНОГО МСБ РЕШЕНИЯ



Типичный слой защиты Энтерпрайз

- Очень дорого
- Требует надзора специалиста по аналитике /CISO / SOC

Типичный слой защиты МСБ

- Доступно для МСБ
- Легкий в управлении в рамках МСБ бюджета

CYBOWALL ОСОБЕННОСТИ РЕШЕНИЯ

Видимость девайсов

Постоянно обновляемый список всех конечных точек, включая профили портов и действия

Обнаружение вторжения

Полная видимость входящего и исходящего сетевого трафика без возникновения помех

SIEM

Управление журналом, управление событиями, корреляция событий и отчетность, чтобы помочь выявить нарушения правил и разрешить ответные процедуры

Сетевые ловушки

Включить понимание бокового перемещения между конечными точками и выявить угрозы, возникающие в сети, выступая в качестве ловушки для активных атак

Оценка уязвимости

Мониторинг бизнес-активов и определение уязвимых систем внутри сети, включая уровень риска, для определения приоритетов развертывания патчей

Охотник на Малвар

Идентифицируйте вредоносные файлы и где они находятся в сети

CYBONET

CYBOWALL ЛУЧШАЯ ПРАКТИКА

Cybowall обеспечивает отличный сервис, основанный на двух основных факторах:

- Конфигурация port mirroring на глав. свитче
- Подключение к станциям с помощью WMI /WinRM

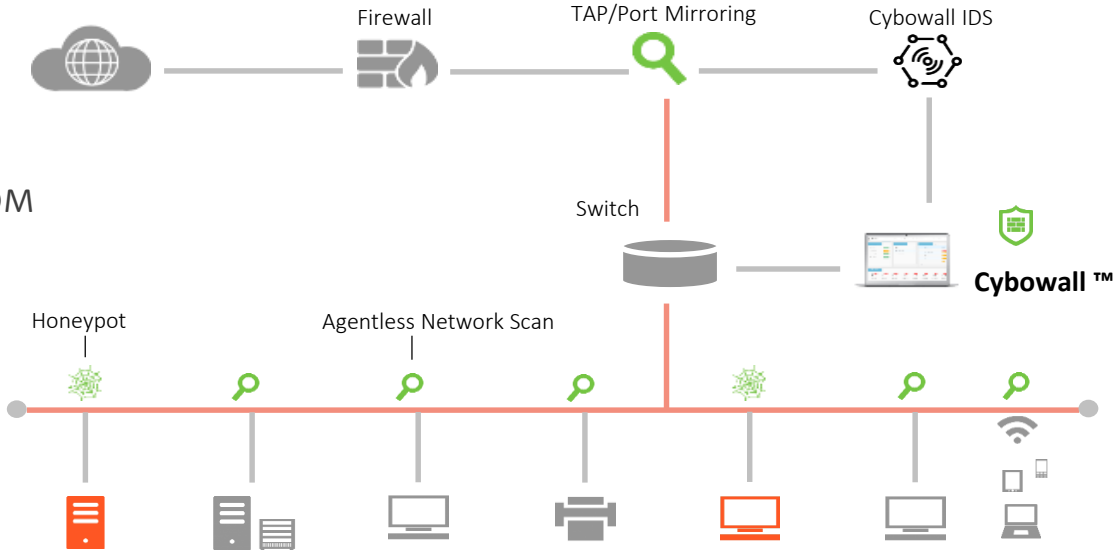
Port Mirroring

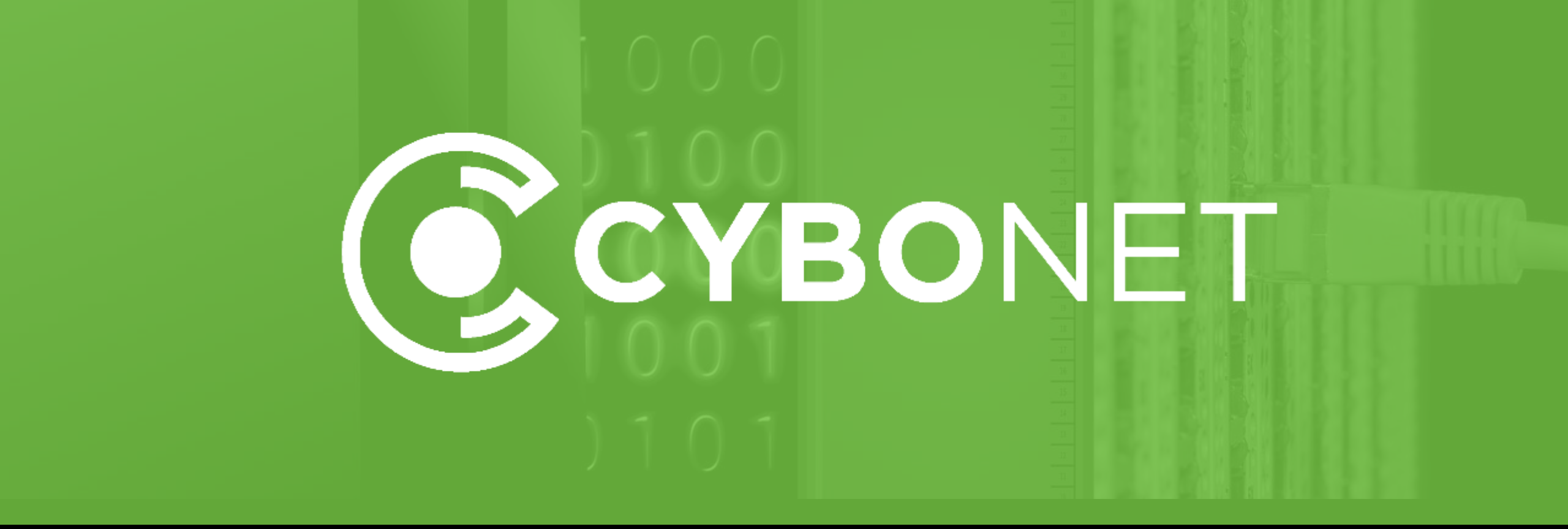
Обеспечивает анализ трафика с помощью IDS - без которого невозможно просматривать связь между данным устройством и его C & C (злоумышленником)
https://wiki.wireshark.org/SwitchReference

WMI/WinRM

Предоставляет анализ конечных точек, который можно разделить между защитой / риском и уязвимостями:

- Защита / риск = WIN апдейт / антивирус / фаервол/ разрешения
- Уязвимости = ОС / программы





CYBONET

R&D Center

Matam, Building 23,

P.O.B. 15102

Haifa 3190501 Israel

info@cybonet.com

www.cybonet.com