Сравнение решений аналитики безопасности

Ознакомьтесь с результатами сравнения Cisco Stealthwatch с другими решениями аналитики безопасности. Это решение легко масштабируется, обеспечивая контроль всей сети. Stealthwatch может обнаруживать сложные угрозы безопасности и реагировать на них в режиме реального времени, используя машинное обучение и моделирование объектов.

Stealthwatch

	Cisco Stealthwatch	Darktrace	Plixer
Обнаружение			
Анализ и обнаружение вредоносного ПО в зашифрованном трафике	✓ Используется платформа Encrypted Traffic Analytics (анализ зашифрованного трафика).	✗ Анализ и обнаружение вредоносного ПО в зашифрованном трафике	✗ Анализ и обнаружение вредоносного ПО в зашифрованном трафике
Обнаружение накопления данных	✓ События аккумулируются в индексе накопления данных, который измеряется либо по абсолютному предельному значению, либо по изученному поведению хоста или групп.	Ограничения. Может обнаружить аномалию, но не конкретное событие сбора данных.	✗
Обнаружение горизонтального перемещения	✓ Обеспечивает обнаружение интернет-червей и визуальное отслеживание вредоносного ПО во всей сети.	Ограничения. Может обнаружить аномалию, но (по опубликованным данным) не может выявлять горизонтальное перемещение.	✗
Ведение журнала событий сети	✓ Может регистрировать каждый сеанс связи в сети с помощью коллекторов Flow Collectors и датчиков Flow Sensor.	Ограничения. Использует только датчики, поэтому может упускать часть трафика.	✓ Поток трафика, хранящийся на устройстве
Обнаружение разведывательных атак	✓ Может обнаруживать быстрое и медленное сканирование с помощью уникального алгоритма, чрезвычайно чувствительного к событиям с очень малой скоростью сканирования.	Ограничения. Может обнаруживать разведывательные атаки, но, скорее всего, менее точно, чем уникальный алгоритм сканирования в Stealthwatch.	✓ С дополнительной аналитикой потоков (Flow Analytics)
Машинное обучение	✓ Использует многоуровневое машинное обучение для обеспечения высокой точности обнаружения.	✓	Ограничения. Предоставляет ограниченные возможности определения стандартных показателей, основанные на большом объеме трафика.

	Cisco Stealthwatch	Darktrace	Plixer
Обнаружение (продолжение)			
Обнаружение утечки	✓ Создает предупреждение о «подозрительной потере данных» для хостов, передающих наружу больше данных (включая зашифрованные), чем обычно.	**Ограничения** Использует только датчики, а не данные телеметрии от сетевого оборудования, и обнаружение ограничивается местоположениями, в которых размещены датчики.	✗
Обнаружение контроля и управления	✓ Может обнаруживать несколько событий безопасности с помощью аналитики и анализа угроз для обнаружения соседних серверов контроля и управления (C&C).	**Ограничения** Использует только датчики, а не данные телеметрии от сети, и обнаружение ограничивается местоположениями, в которых размещены датчики.	**Ограничения** Нет конкретных алгоритмов для обнаружения контроля и управления.
Обнаружение аномалий	✓ Использует развитую и апробированную систему обнаружения аномалий с более чем 150 алгоритмами.	**Ограничения** Использует только датчики, а не данные телеметрии от сетевого оборудования, и обнаружение ограничивается местоположениями, в которых размещены датчики.	**Ограничения** С дополнительной аналитикой потоков (Flow Analytics)
Обнаружение вредоносного ПО	✓ Может обнаруживать уязвимости «нулевого дня».	**Ограничения** Использует только датчики, а не данные телеметрии от сетевого оборудования, и обнаружение ограничивается местоположениями, в которых размещены датчики.	**Ограничения** С дополнительной аналитикой потоков (Flow Analytics)
Развертывание			
Масштабируемость	✓ Поддерживает масштабирование до 6 миллионов потоков в секунду, обработку подключений интерфейсов со скоростью от 100 Мбит/с до 10 Гбит/с, всплески объема трафика выше номинальных уровней и может собирать телеметрические данные от тысяч датчиков.	**Ограничения** Использует только датчики, а не телеметрические данные из сети.	**Ограничения** Необходимы значительная настройка и кастомизация для поддержки сводных отчетов и карт потоков в рамках нескольких коллекторов Plixer.
Хранение данных	✓ В среднем система может хранить данные о потоках за 30–45 дней (а часто намного больше) для проведения более глубокого расследования.	**Ограничения** Нет опубликованных данных для подтверждения возможностей хранения данных.	✓
Обнаружение уязвимости «нулевого дня»	✓ Может обнаруживать новое или уникальное вредоносное ПО, для которого еще не существует сигнатур, с помощью поведенческого метода с более чем 90 параметрами.	✓ Использует только датчики, а не данные телеметрии от сети, и обнаружение ограничивается местоположениями, в которых размещены датчики.	**Ограничения** Предоставляет ограниченные возможности определения стандартных показателей, основанные на большом объеме трафика.

	Cisco Stealthwatch	Darktrace	Plixer
Развертывание (продолжение)			
Сжатие данных	✓ По мере получения потоков средством сбора данных они включаются в двунаправленные потоки, находящиеся в оперативной памяти. Это уменьшает число ложных срабатываний и обеспечивает эффективное хранение данных и точную отчетность на уровне хоста.	**Неприменимо** Использует только датчики, а не телеметрические данные из сети.	**Ограничения** Часть информации отбрасывается.
Модель развертывания	**См. примечание.** Не требует развертывания датчиков или дорогостоящего программного зондирования. Телеметрические данные для анализа сетевого трафика можно легко получать от сетевых устройств.	**См. примечание.** Заказчикам необходимо приобрести датчики и выбрать соединения для мониторинга; нельзя просто включить телеметрические данные от сетевых устройств и получать данные обо всех сеансах связи; модель стоит дорого, и ее сложно масштабировать.	**См. примечание.** Может использовать большинство источников данных телеметрии на основе потоков.
Мониторинг оконечных устройств	✓ С помощью Cisco AnyConnect 4.2 и более поздней версии решение Endpoint Data License собирает телеметрические данные оконечных устройств с помощью протокола Cisco Network Visibility Flow (nvzFlow).	✗	✗ Не хватает ряда функций, таких как секретный пароль, предварительные настройки конфигурации для типов NAD и прокси-сервер TACACS+.
Мониторинг облачной среды	✓ Позволяет контролировать общедоступное облако с помощью решения Stealthwatch Cloud на базе SaaS.	**Ограничения** Использует датчики для мониторинга сети частного облака и Cloud Connector для конкретных приложений.	**Ограничения** Использует журналы Amazon AWS, которые аналогичны потокам и включают в себя действия разрешения и запрета.
Экспорт данных	**См. примечание.** Интегрируется с информационными системами обеспечения безопасности и предусматривает API-интерфейсы для пользовательских интеграций, а также поддерживает API-интерфейсы SOAP и REST.	**См. примечание.** Включает блок подключения Splunk, который принимает входные данные системного журнала JSON из устройства Darktrace и отображает инциденты безопасности в Splunk, а также связывает их с отчетами в Darktrace Threat Visualizer.	**См. примечание.** Поддерживает API-интерфейс REST и выходные данные журналов.
Уведомления о сигналах	**См. примечание.** Обеспечивает экспорт электронной почты или системного журнала в систему SIEM, Netcool, систему обработки заявок Remedy и т. д. с помощью уведомлений по электронной почте, SNMP и системного журнала.	**См. примечание.** Обеспечивает форматированный вывод данных системного журнала.	**См. примечание.** Обеспечивает регистрацию и оповещение для исходящего трафика.

	Cisco Stealthwatch	Darktrace	Plixer
Расследования			
Полномасштабные следственные рабочие процессы	✓ Позволяет расследовать долгосрочные события безопасности. Создает контекстные и пользовательские сигналы, связывает имя пользователя с IP-адресом, контролирует использование интерфейса, выполняет углубленную проверку пакетов и регистрирует каждое сетевое взаимодействие.	**Ограничения** Классифицирует обнаруженную угрозу и визуализирует ее в интерфейсе Threat Visualizer.	**Ограничения** Отсутствуют настраиваемые интерфейсы, быстрое выявление тенденций во времени, функции автоматического восстановления и средства анализа основных причин.
Эффективность для корпоративных заказчиков	✓ Упрощает сегментацию благодаря логическому моделированию группы узлов для организации пользователей по местоположению, IP-адресу, функции и т. д. и предоставляет настраиваемые сведения и форматы уведомлений с подтверждением.	**Ограничения** Использует только датчики, а не телеметрические данные из сети, поэтому сложно выполнить масштабирование до уровня предприятия.	**Ограничения** Необходимы значительная настройка и кастомизация для поддержки сводных отчетов и карт потоков в рамках нескольких коллекторов Plixer.
Гибкая система запросов и фильтрации	✓ Может отправлять запросы обо всех полученных полях. Доступен расширенный поиск по зашифрованному трафику (обмен ключами шифрования, алгоритм шифрования, длина ключа, версия TLS/SSL и т. д.).	**Неприменимо** В опубликованных материалах нет доступной для сравнения информации.	**Ограничения** Отсутствуют настраиваемые интерфейсы, быстрое выявление исторических тенденций, функции автоматического восстановления и средства анализа основных причин.
Панель управления киберугрозами	**См. примечание.** Обеспечивает соответствующую информацию для персонала службы обеспечения безопасности, например: какие индексы заполняются предупреждениями, какие предупреждения активны, с какими хостами связано большинство предупреждений и т. д. Также предоставляет возможность получения более подробной информации и связанных данных телеметрии.	**См. примечание.** В первую очередь средство обеспечения безопасности и рабочее пространство ориентированы на персонал службы обеспечения безопасности.	**См. примечание.** Панель управления мониторингом безопасности и сети
Визуализация и сопоставление	**См. примечание.** Создает автоматические карты, такие как пути распространения интернет-червей и настраиваемые карты взаимосвязей, позволяя визуализировать любой набор хостов и их взаимодействие с любым другим набором.	**См. примечание.** В значительной мере ориентирован на графику.	**См. примечание.** Простые схемы и графики
Расследование инцидентов	**См. примечание.** Пользовательский интерфейс ориентирован на рабочие процессы на основе личного профиля и направляет администраторов непосредственно к первопричинам и вспомогательной информации.	**См. примечание.** Включает средство Threat Visualizer, которое обеспечивает мониторинг и обработку угроз.	**См. примечание.** Предоставляются следственные рабочие процессы.

	Cisco Stealthwatch	Darktrace	Plixer
Контекст			
Контекстное многообразие данных	✓ Интегрируется с Cisco Identity Services Engine (ISE). Обеспечивает возможность поиска информации хоста, такой как идентификатор пользователя, MAC-адрес, тип устройства и информация о портах коммутатора; не требуется отдельный запрос для поиска связанного пользователя, поскольку может быть записан идентификатор пользователя.	**Ограничения** Интегрируется с Active Directory для обработки пользовательских данных.	**Ограничения** Обеспечивает датчики, ориентированные на различные данные, включая производительность приложений и подробную информацию о DNS.
Идентификационные данные	✓ Интегрируется с платформой Cisco ISE, многофункциональными устройствами обеспечения безопасности Cisco ASA (NSEL), серверами DHCP/RADIUS и серверами аутентификации Active Directory для сопоставления данных идентификации и телеметрии.	**Ограничения** Интегрируется с Active Directory для обработки пользовательских данных.	**Ограничения** Интегрируется с Active Directory.
Интеграция поставщиков средств маршрутизации и коммутации	✓ Основными источниками данных являются маршрутизаторы, коммутаторы, межсетевые экраны и контроллеры беспроводной связи. Может анализировать многие версии телеметрии и NetFlow от нескольких поставщиков, таких как IPFIX и sFlow, а также другие протоколы уровня 7.	✗ Использует только датчики, а не телеметрические данные из сети. Требуется SPAN или TAP для каждого из отслеживаемых каналов, ограничивается содержимым данного канала.	
Сбор данных об URL-адресах	**См. примечание.** Датчики потоков трафика (Flow Sensor) могут извлекать данные об URL-адресах, используемые коллекторами Flow Collectors и Management Center. Можно запрашивать данные об URL-адресах на основе операторов. Также интегрируется со средством Cisco Security Packet Analyzer, которое может загружать точные датаграммы, представляющие поток, в формате PCAP.	**См. примечание.** Работает полностью на основе датчиков и обеспечивает мониторинг данных в пакетах.	**См. примечание.** Может собирать данные об URL-адресах с помощью датчиков.

	Cisco Stealthwatch	Darktrace	Plixer
Контекст (продолжение)			
Формирование данных NetFlow для сред VMware	✓ Использует функцию экспорта NetFlow виртуального коммутатора или виртуальный датчик потоков.	**Неприменимо** Неприменимо, так как датчики используются для регистрации трафика.	✓ Может использовать данные телеметрии NetFlow от VMware.
Сбор данных о приложениях и потоках уровня 7	✓ Поддерживает состояние потока (активный, неактивный или текущий); создает NetFlow на основе мониторинга портов SPAN или TAP; интегрируется с прокси; обеспечивает идентификацию приложений от нескольких поставщиков, например Palo Alto Networks и L7 Defense; использует NBAR и NBAR2 с Flow Sensor.	✓ Использует датчики, которые анализируют эти данные непосредственно из необработанных пакетов.	**Ограничения** Может получать данные от межсетевого экрана, поток из SPAN с помощью датчика и идентификатор приложения от датчика или межсетевого экрана. Отсутствует поддержка NBAR и интеграция с прокси.
Полный перехват пакетов	✓ Интегрируется с Cisco Security Packet Analyzer, инструментом, установленным в SPAN или TAP, который поддерживает скользящий буфер датаграмм в сегменте и предоставляет возможность загрузки точных датаграмм, представленных телеметрией, в формате PCAP и даже файлов, содержащихся в PCAP. Может также запустить расшифровку пакета вместо загрузки другого приложения.	**Неизвестно** В опубликованных материалах нет доступной для сравнения информации.	✗ Отсутствует возможность полного перехвата пакетов.
Анализ зашифрованного трафика	✓ Использует Encrypted Traffic Analytics или расширенные телеметрические данные из сети Cisco для обнаружения вредоносного ПО и обеспечивает соблюдение нормативных требований шифрования. StealthWatch анализирует зашифрованный трафик, используя современные методы машинного обучения и глобальную аналитику угроз.	**Ограничения** Может обнаружить определенное аномальное поведение в зашифрованном трафике.	✗ Отсутствует возможность анализа зашифрованного трафика.
Оценка репутации в масштабе всего предприятия	✓ Создает оценку на основе индекса для каждого хоста, которая определяет необычную активность хоста.	**Неизвестно** Модель обнаружения аномалий может использовать механизм глобальной оценки.	✗ Нет концепции индексов безопасности; запускает только необработанные оповещения и сигналы тревоги.

	Cisco Stealthwatch	Darktrace	Plixer
Аналитика угроз			
Канал аналитики угроз	✓ Stealthwatch Threat Intelligence License и глобальная карта рисков, поддерживаемая Talos, представляют собой канал информации об угрозах из нескольких источников, обновляемый по крайней мере один раз в час. Его цель заключается в предоставлении набора данных с нулевым числом ложных срабатываний.	✓ Доступен канал информации об угрозах, который содержит список известных вредоносных веб-сайтов.	✗ Нет, хотя у Plixer есть ориентированное на DNS устройство для обнаружения проблем с DNS.
Обнаружение эксплойтов	✓ Позволяет обнаруживать внутренние угрозы, такие как кража данных и соединения контроля и управления, а также долгосрочные и медленные атаки. События безопасности отправляются в индексы для инициирования сигналов тревоги с помощью поведенческих алгоритмов и абсолютных предельных значений, которые могут быть заданы оператором.	✓ Заявлено обнаружение ряда эксплойтов, но масштаб неизвестен.	✗
Обмен аналитикой угроз	✓ Данные Stealthwatch Threat Intelligence используются в Cisco Talos, и наоборот. Cisco обменивается данными с сотнями партнеров, заказчиков и поставщиков в рамках программ Aegis, Crete и Aspis и является одним из членов-учредителей Cyber Threat Alliance.	✗	✗