Network Traffic Security Analytics

Обнаружение нарушений в режиме реального времени и полная видимость угроз

Bitdefender Network Traffic Security Analytics - это корпоративное решение безопасности, которое точно обнаруживает современные атаки в режиме реального времени и автоматизирует сортировку предупреждений для быстрого реагирования на инциденты. Оно позволяет организациям быстро обнаруживать сложные угрозы и бороться с ними, дополняя уже существующую архитектуру безопасности - сеть и конечные точки - специализированной защитой на базе сети.

Используя сетевой трафик в качестве источника надежной информации, NTSA немедленно обнаруживает нарушения при изменении поведения конечных точек после заражения. Обнаружение эффективно как против общих, так и против сложных постоянных угроз, известных или никогда ранее не встречавшихся. Уведомления об инцидентах автоматически сопоставляются и сортируются для повышения эффективности по обеспечению безопасности и улучшения расследования инцидентов и времени реагирования.

Обнаружение угроз в режиме реального времени для любого сетевого устройства

Обеспечивает полную видимость связанной с угрозами деятельности на всех конечных точках сети, независимо от типа или уже существующих решений безопасности (корпоративных или пользовательских устройств, сетевых элементов, BYOD, IoT).

Экономьте время с помощью автоматизированной сортировки инцидентов безопасности

Автоматизирует сортировку инцидентов безопасности путем автоматической корреляции событий и генерирует высокоточные оповещения для повышения эффективности поиска угроз аналитиков.

Охота на киберугрозы с подробной криминалистической экспертизой

Содержит подробные объяснения по каждому инциденту, связанному с безопасностью, с предлагаемым курсом действий для улучшения расследования и реагирования на инциденты.

Ведущие специалисты в области анализа киберугроз и искусственного интеллекта

NTSA использует превосходную аналитику киберугроз Bitdefender's Cyber Threat Intelligence, собранную с 500 миллионов конечных точек по всему миру, в сочетании с передовым машинным обучением и эвристикой для анализа метаданных сети в режиме реального времени и точного выявления активности угроз и подозрительного трафика. С автоматической аналитикой безопасности и фокусом на исходящем сетевом трафике, он снижает уровень шума и обеспечивает действенные предупреждения для обеспечения безопасности.

IntelliTriage - Автоматизирует сортировку предупреждений

IntelliTriage, новейший компонент NTSA, автоматизирует процесс сортировки инцидентов безопасности для улучшения времени расследования инцидентов и снижения организационных рисков благодаря высокоточным предупреждениям. В нем также содержатся рекомендации по исправлению положения, касающиеся шагов, которые следует предпринять в связи с инцидентом в области безопасности.

Обучение на основе сложных сценариев позволяет с высокой точностью обнаруживать современные атаки и формировать тысячи предупреждений о них для получения четкого представления о каждом инциденте. IntelliTriage предоставляет подробные объяснения для оценки тяжести инцидента. Рекомендуемые восстановительные меры также предоставляются для ускорения реагирования на инциденты.

Защита вещей (IoT) и BYOD в вашей среде

Корпоративная среда все чаще используется совместно с устройствами, управляемыми человеком, и искусственным интеллектом. В то время как традиционные конечные точки обычно находятся под пристальным вниманием и хорошо защищены, «интеллектуальные устройства» работают в «серой зоне» с ограниченной защитой или без нее. Все больше и больше устройств в сети становятся мишенью для атак и используются в качестве цели во время сложных атак.

Возможности обнаружения нарушений NTSA распространяются также и на интеллектуальные компоненты корпоративной сети. Сосредоточившись на сетевом поведении конечных точек, он может защитить устройства с ограниченными встроенными возможностями безопасности или без них и без агента безопасности конечных точек, работающего на них (как и большинство устройств IoT).

Поскольку сотрудники используют личные ноутбуки, мобильные телефоны и другие устройства в бизнес-среде, злоумышленники используют их для получения корпоративной информации. Обеспечение безопасности BYOD повышает производительность труда сотрудников и снижает риск раскрытия корпоративной информации. Технология NTSA помогает защитить организации от кражи информации путем постоянного мониторинга и отслеживания поведения всех пользователей и устройств в режиме реального времени и внедрения улучшенной системы сбора информации об угрозах. Он не содержит агентов, не проникает внутрь и не зависит от операционной системы.

Как это работает

Особенности

Обнаружение в режиме реального времени и ретроактивное обнаружение

Обнаруживает нарушения, пассивно проверяя исходящий сетевой трафик в режиме реального времени для всех вредоносных коммуникаций. Применяет новые данные информации об угрозах в записанных метаданных для обнаружения нарушений задним числом.

Облачная система сбора информации об угрозах, искуственный интеллект, машинное обучение и эвристика.

Сочетание «облачных» технологий Bitdefender и анализа сетевого трафика в режиме реального времени на основе AI/ML и эвристики позволяет достичь превосходных показателей обнаружения угроз при низком уровне ложных срабатываний.

Широкий охват, полная видимость

Охватывает все конечные точки в сети, независимо от типа или уже существующих решений по безопасности (корпоративные или управляемые пользователем устройства, сетевые элементы, BYOD, IoT). Обеспечивает полную видимость и понимание сетевой активности, связанной с угрозами, и аномалий в трафике конечных точек.

Автоматизированная перевозка, эффективная охота на угрозы

Автоматизирует анализ безопасности и снижает уровень шума для повышения эффективности поиска угроз аналитиков и генерирует действенные предупреждения для облегчения реагирования на инциденты.

Быстрое развертывание, немедленные результаты

Использование простой и гибкой архитектуры (физическое или виртуализированное развертывание) с компонентами plug-and-play для немедленного получения результатов.

Интеграция с GravityZone

Интеграция с GravityZone позволяет быстро и безупречно управлять системой.

Подробные системные требования см. на сайте https://www.bitdefender.com/business/enterprise-products/network-traffic-security-analytics.html