NGIDS NeuroFortress

Аппаратно-программный комплекс обнаружения и предотвращения угроз безопасности сетевой инфраструктуры, включая беспроводные среды интернета вещей и умных устройств IoT

ФОНД СОДЕЙСТВИЯ ИННОВАЦИЯМ

ПРОГРАММА «СТАРТ»

ФГАНУ НИИ «СПЕЦВУЗАВТОМАТИКА»

ФГУП "РНИИРС"
Федеральный научно-производственный центр

РГЭУ (РИНХ) Ростовский государственный экономический университет

ЮФУ Южный федеральный университет Ростов-на-Дону-Таганрог

РСТ РОСТОВСКИЙ ЦСМ

ТЕХНОСКВЕР

aura

ПИХТИН АВТО

BITCORD БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ

Что это

NGIDS NeuroFortress – это аппаратно-программный комплекс обнаружения и предотвращения угроз безопасности сетевой инфраструктуры, включая беспроводные среды интернета вещей и умных устройств.

Технология обнаружения и предотвращения киберугроз – сердце комплекса – набор кибер-детекторов с искусственным интеллектом - защищена патентом и авторскими правами.

NeuroFortress охраняет сети IoT

NF IoT - это интегрированная программа услуг и технологий, разработанная, чтобы помочь вашей организации на протяжении всего пути управления угрозами. Наше решение NF IoT помогает реализовать структуру NIST для доменов OT, IoT и IoMT, чтобы обеспечить прозрачность неуправляемых и подключенных устройств.

Наше решение предлагает:

Обнаружение угроз с использованием запатентованного искусственного интеллекта, машинного обучения и автоматизации с помощью платформы NF IoT, обеспечивающей непрерывный мониторинг и обнаружение атак или подозрительной активности.

Мы используем технологию, которая обнаруживает потенциальные угрозы в вашей среде - управляемые и неуправляемые устройства как в вашей сети, так и за ее пределами, а также в вашем воздушном пространстве. NF IoT объединяет возможности атакующих служб безопасности, управляемых служб безопасности, искусственного интеллекта, реагирования на инциденты и непрерывного совершенствования. NF IoT предлагает интегрированное управление жизненным циклом угроз и инцидентов.

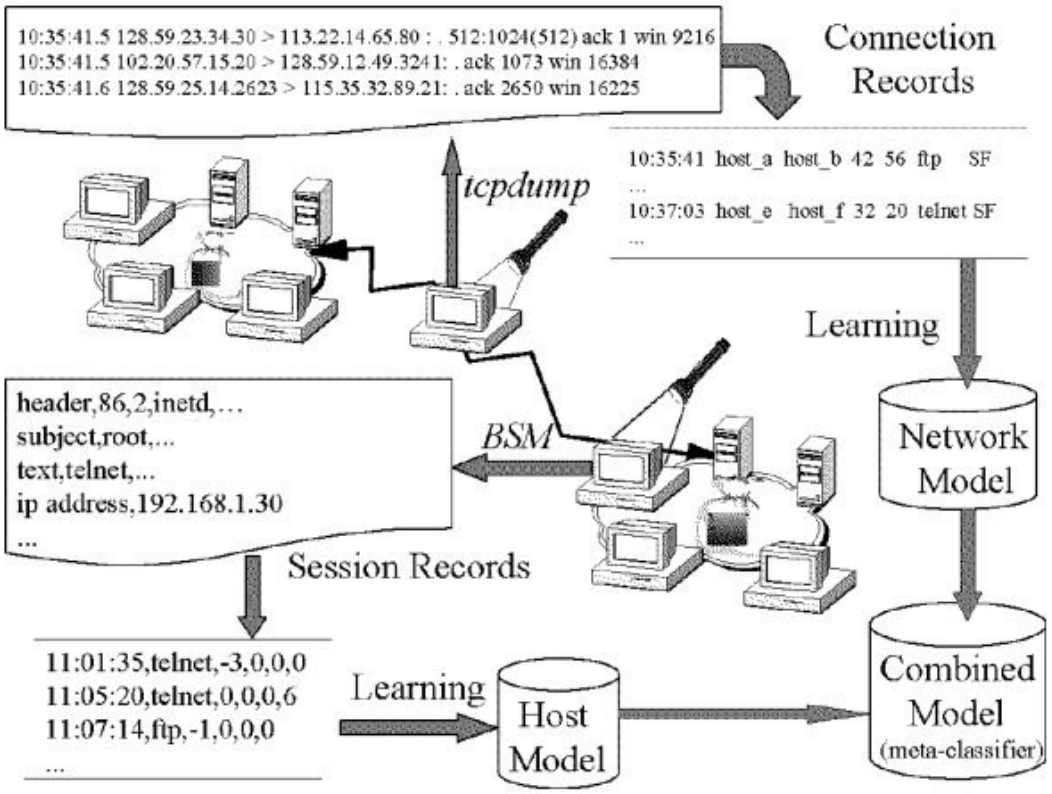
Обнаружение, расследование и реагирование на расширенные атаки на основе ИИ - Расширенная аналитика сокращает количество бессмысленных предупреждений и обнаруживает угрозы, которые пропускают ваши текущие инструменты.

Для кого

Частные лица и Компании, владеющие важными данными: объектами авторского права, персональных данных, стратегических сведений, интеллектуальной собственностью, выполняющие требования Регуляторов; организации, использующие беспроводные среды; малый и средний бизнес, ИТ-компании, госкомпании, энергетика, СМИ, банки, платежные системы, частные пользователи…

Как работает

Архитектура NGIDS NeuroFortres



Клиент - сервер:

- агент устанавливается в точку в зависимости от модели угроз и топологии сети

- связь агента и сервера (нейросети) по закрытому протоколу и API

- инсталляция производится администратором сети или сервером в автоматическом режиме.

NGIDS NeuroFortress анализирует только параметры траффика ваших сред, не нарушая конфиденциальность информации, он применяет нашу специально разработанную нейронную сеть нового поколения, чтобы предупредить вас о подозрительной активности, требующей внимания и оперативных действий.

Алгоритмы работы:

- Агент производит сбор данных по сетевой активности, программного обеспечения и аппаратных средств
- Подготавливает данные для передачи и классификации на сервер
- Нейронная сеть классифицирует переданные данные и проводит идентификацию угроз вторжения
- Сервер выводит уведомления об угрозе и передаёт сообщения администратору сети или модулю автоматического реагирования.

Масштабируемость решения:

- Система масштабируется путем расширения обучающей модели, сетевого охвата, интегрируется посредством стандартных сетевых протоколов
- Алгоритм может быть расширен за счет увеличения количества используемых ИНС и применения других типов ИНС в зависимости от поставленной задачи
- Возможна интеграция как на сетевом уровне, так и на уровне модели угроз гетерогенных и моносетей.

Суть научной новизны продукта:

- Применение нейронной сети, использование потенциала «самообучения» и выход за пределы экспертной системы, а также повышение точности определения сетевых аномалий новых видов, особенно в отношении сред интернета вещей и умных устройств, что отличает наш продукт от классических систем безопасности, требующих постоянного обновления базы и проводящими анализ по заранее заданному шаблону
- Уникальный метод сокращения объема ключевой информации для классификации угроз, что позволяет существенно сократить трафик в сети, а также уменьшить вероятность перехвата ценной информации, эта реализация отличается от известных систем, передающих на детектор полные информационные блоки
- Радиоконтроль беспроводных сетей, сетей умных устройств, анализ сетевых сервисов, это отличает продукт от существующих решений в части среды обеспечения кибербезопасности
- Уникальные алгоритмы машинного обучения - применение слоев Кохонена, что позволяет увеличить сходимость решений, это отличает создаваемый продукт от других нейросетевых детекторов киберугроз высокой точностью и скоростью.

Наша система в максимуме «из коробки» включает в себя:

- Платформу сбора, анализа и корреляции событий
- Локальную систему обнаружения и предотвращения вторжений (включая анализ исполняемых кодов и подключаемых устройств, анализ протоколов 7 уровня OSI)
- Программный модуль первичной обработки информации
- Программный модуль взаимодействия с API
- Сетевую систему обнаружения и предотвращения вторжений с модулями интеграции в межсетевые экраны и сервисные службы
- Беспроводную систему обнаружения вторжений - включая умные устройства (Интернет-вещей) и активность в сетях BT, BLE, ZigBee, Lora и т.д.
- Мониторинг узлов сети;
- Анализ сетевых аномалий + включая беспроводные радио аномалии и аномалии сетей умных устройств (Интернет-вещей)
- Программный модуль мониторинга, сигнализации и контроля
- Сканер уязвимостей – отдельным продуктом и как дополнение к настройке системы из коробки
- Система обмена и переноса обученных моделей машинного обучения (нейросеть)
- Множество специализированных плагинов для парсинга и корреляции логов со всевозможных внешних устройств и служб, открытый API для разработки внешний модулей и плагинов
- Платформа биллинга стоимости предоставляемых услуг в локальном и облачном решении.

Результаты тестирования NGIDS NeuroFortress

Преимущества, чем превосходит других

На рынке кибербезопасности представлено множество различных продуктов, но стоит обратить внимание на следующие недостатки:

- Стандартные средства обеспечения кибербезопасности не фиксируют атаки с неизвестной или нестабильной сигнатурой структурой (неизвестные атаки)
- Отсутствие интегральных систем безопасности, включающих беспроводные сети и среды умных устройств IoT (интернет-вещей)
- Существующие реализации эвристических механизмов обнаружения имеют большое количество ложных срабатываний
- Недостаточная скорость работы механизмов обнаружения атак, задержки большого трафика
- Идентификационные базы сигнатурных методов требуют обязательного обновления.

Все эти недостатки делают стандартные и популярные средства безопасности не только бесполезными, но и опасными, так как у пользователя возникает ложное представление о его защищенности.

Конкурентными преимуществами являются:

- Как идентификация вторжений, так и предотвращение
- Параллельный анализ трафика различных информационных сред
- Высокая скорость реакции
- Возможность для нейронной сети полностью использовать потенциал «самообучения» и выходить за пределы базы знаний экспертной системы
- Отсутствие потребности регулярного обновления базы знаний
- Контроль беспроводных сетей и сред умных устройств (интернет-вещей)
- Планируется поддержка сертифицированных в РФ сред для интеграции (например, в рамках «ГосСОПКА»).

Защитите свой бизнес сейчас и ничего не теряйте в будущем!

Запишитесь на бесплатную опытную эксплуатацию https://cvatec.com

Как подключить

3 шага и все готово!

1. Оставить заявку
2. С Вами свяжутся наши специалисты
3. Подключить необходимую конфигурацию