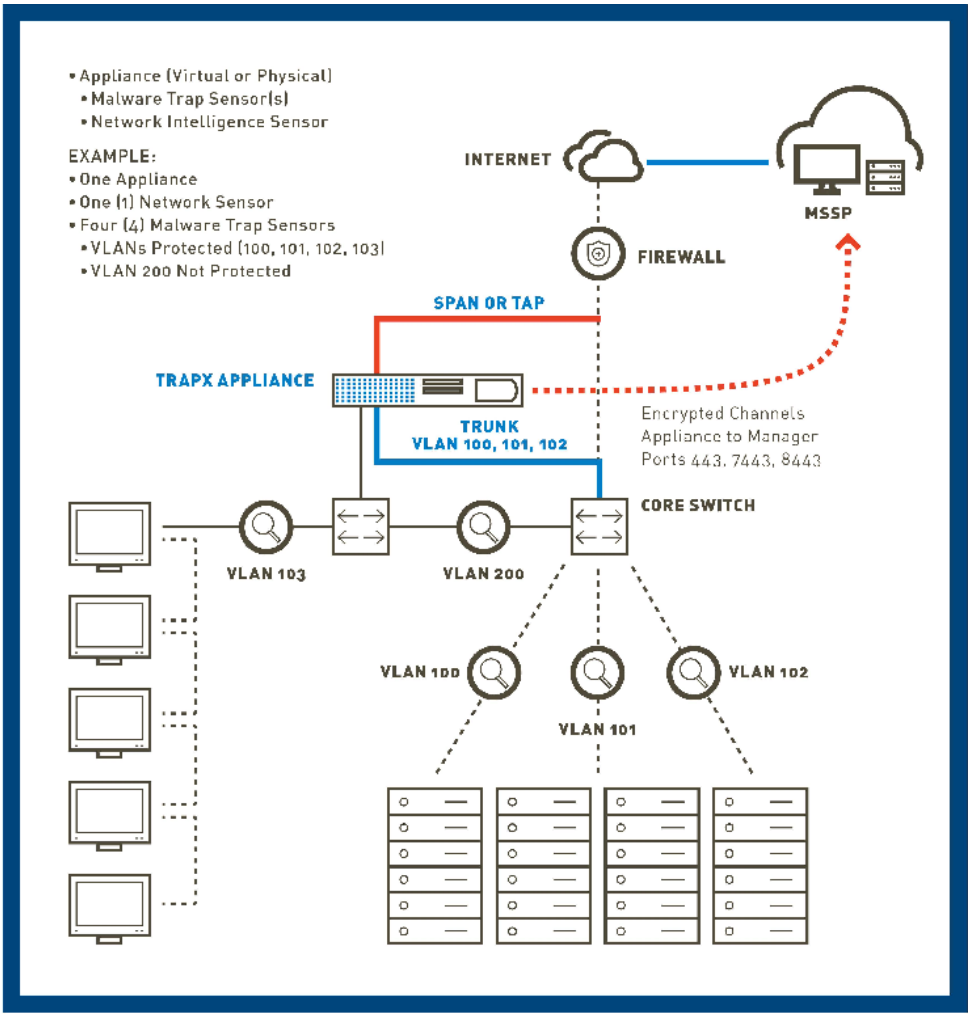
DECEPTIONGRID™ (Сеть обнаружения атак) - Обзор решения

Эффективная архитектура

DeceptionGrid автоматически разворачивает сигнальную сеть ловушек, которые абсолютно идентичны Вашим настоящим IT-ресурсам. Как только вредоносное ПО или атакующий проникает в Вашу корпоративную сеть, они скрыто распространяются и ищут наиболее важные объекты. Всего один контакт вредоносного ПО с DeceptionGrid включает режим тревоги. Система автоматического поиска в реальном времени изолирует вредоносное ПО и предоставляет полный отчет прямо в центр обеспечения безопасности.



Основные компоненты DeceptionGrid

Виртуальные ловушки

Сеть ловушек DeceptionGrid в корпоративной сети может насчитывать сотни и тысячи устройств, которые будут непрерывно отслеживать всю подозрительную активность. Топология сети определяется автоматически и используется для создания скрытой сети эмулированных систем: серверов, сетевого оборудования, баз данных, приложений. Они объединены с реальными

Основные преимущества

- Защита от вредоносного ПО нового поколения. Наша инновационная система киберзащиты, основанная на технологии «ложных систем» (honey pots), находит продвинутое вредоносное ПО и уязвимости «нулевого дня», которые не могут выявить другие защитные системы
- Сокращение или избежание финансовых потерь. Продвинутые технологии поиска вредоносного ПО уменьшают риск финансовых потерь из-за выведения из строя компьютерной техники, кражи данных или вмешательства в бизнес-процессы.
- Высокая скорость реакции. Усовершенствованный процесс анализа в режиме реального времени дает возможность центру обеспечения безопасности действовать быстро и нейтрализовать все атаки в сети.
- Соответствие стандартам. Функционал TrapX Deception Grid помогает обеспечить соответствие стандартам безопасности данных PCI, HIPAA, нормам законов об хранении данных и других законодательных актов во всем мире.
- Более низкая стоимость реализации. Технологии «ложных систем» всегда были эффективными, но очень дорогими и не применимыми в крупных масштабах. С появлением DeceptionGrid использование этой технологии в больших масштабах стало экономически эффективным.

компьютерными устройствами. Ловушки могут содержать ложные данные, которые вынуждают атакующего тратить время на их анализ и замедляют его продвижение по сети.

Анализ кода

Инструменты автоматизации в реальном времени изолирует обнаруженное вредоносное ПО и размещают его в «песочнице». DeceptionGrid проводит статический и динамический анализ и подает полный отчет в центр обеспечения безопасности

Управление событиями и аналитика угроз

Информация, полученная в результате автоматизированного анализа, направляется в систему управления и после присвоения уникального ID хранится в объединенной базе данных управления событиями. На основе этих данных система создает профили, сигнатуры для распознавания и предотвращения атак в будущем.

Усовершенствованный механизм выявления бот-сетей

Ботнет-детектор DeceptionGrid анализирует исходящий трафик с реальных ИТ-активов и выявляет узлы, которые общаются с командными центрами.

Гибкие варианты развертывания системы

DeceptionGrid разработан специально для быстрого развертывания. Средства автоматизации позволяют выполнить полное развертывание за несколько часов. Решение готово к развертыванию, в том числе, и как сервис провайдера управляемых услуг безопасности (MSSP). Решение может быть внедрено как полностью в инфраструктуре Клиента, так и с использованием облачных технологий.

О TrapX

TrapX Security – лидер в сфере киберзащиты на основе технологии «ложных» систем. Наши продукты быстро определяют, анализируют и нейтрализуют новейшие APT-атаки и атаки нулевого дня в режиме реального времени. DeceptionGrid обеспечивает автоматизированный, тщательный анализ вредоносного ПО и подозрительной активности, невидимых для других средств киберзащиты. Мы следуем проактивной концепции безопасности, в корне меняя экономический аспект киберзащиты. Для хакеров атаки становятся дороже. Услугами TrapX Security уже пользуются 2000 коммерческих и правительственных структур в сферах защиты, здравоохранения, финансов, жнергетики, потребительских товаров и многих других ключевых отраслей по всему миру.

- Совместимость с уже существующими инструментами. Технология DeceptionGrid может интегрироваться с существующими средствами ИБ и повышать глубину защиты.

Особенности решения

- Обнаружение в режиме реального времени вредоносных программ и скрытых атак в любом месте сети предприятия.
- Отсутствие проблемы информационной перегрузки. Решение TrapX обеспечивает практически нулевой уровень ложных срабатываний.
- Полный анализ вредоносных программ, в том числе и эксплоитов «нулевого дня» выполняется автоматически. Центр безопасности быстро получает всю информацию для оперативного адекватных принятия мер.

- Автоматическое развертывание DeceptionGrid позволяет легко обеспечить защиту в масштабе всего предприятия, что ранее было невозможно при использовании традиционных Honey Pots
- Защита всех VLAN от вредоносных программ / 0-dayz в случае обнаружения даже единичного случая в сети. Наш центр аналитики угроз использует собственную глобальную статистику и решения ряда сторонних источников.