DECEPTIONGRID™ (Сеть обнаружения атак) – Энергетика

Защита от нового поколения вредоносных программ.

Кибератаки постоянно совершенствуются. Наши передовые линии защиты взламываются. Существующие инструменты обеспечения безопасности из-за недостаточной гибкости не могут устранить эти угрозы. Существующий периметр безопасности оказался уязвим перед современными продвинутыми атаками (APT) и уязвимостями «нулевого дня». Применение технологии DeceptionGrid (Сигнальная сеть на базе ловушек) в системе кибербезопасности позволяет устранить эти новые угрозы. DeceptionGrid представляет собой новый подход в деле обеспечения ИТ-безопасности, своеобразное «минное поле» для хакеров. Он основан на передовых технологиях, способных моментально выявлять и ликвидировать новые угрозы.

Применение Deception-технологии для обнаружения новых вредоносных программ

DeceptionGrid автоматически разворачивает поверх Вашей сети специальную сигнальную сеть замаскированных ловушек для вредоносных программ и хакеров. Ловушки полностью имитируют реальные ИТ-активы (ПК, серверы, сетевое оборудование, SCADA-системы). После того, как вредоносная программа или злоумышленник проникли в периметр Вашего предприятия, они применяет тактику скрытого изучения и распространения с целью обнаружения приоритетных целей. Как только вредоносная программа начинает взаимодействовать с DeceptionGrid, система подает сигнал предупреждения. После этого можно автоматически в реальном времени изолировать вредоносное ПО, провести его всесторонний анализ и принять меры противодействия.

Таким образом, мы можем прерывать алгоритм атаки на этапе изучения и скрытого распространения. После обнаружения атаки автоматически проводится динамический и статический анализ инструментария, который используют атакующие. Это позволяет команде SOC практически немедленно получить полное представление о характере атаки. Вы можете быстро выбрать и применить эффективные меры для восстановления системы и удаления вредоносной программы. На данный момент никакие другие ИБ-системы не могут обеспечить таких широких возможностей, комплексного масштабного подхода и высокого уровня автоматизации.

Защита ядра энергетических систем

Применение DeceptionGrid снижает расходы на устранение влияния ИБ- инцидентов на энергетический сектор путем быстрого выявления и прерывания последовательности атаки. Мы предлагаем новый, активный подход к обеспечению безопасности, который в корне меняет экономическую составляющую кибервойны и перекладывает основные затраты на атакующую сторону.

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 невидимы для других защитных систем
- 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 быстро 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 т.п..
- Более низкая стоимость реализации. Технологии «ложных систем» всегда были эффективными, но очень дорогими и не применимыми в крупных сетях. С появлением DeceptionGrid использование этой технологии в больших масштабах стало экономически эффективным.
- Совместимость с уже существующими инструментами.

Гибкие варианты развертывания системы

DeceptionGrid разработан для максимально быстрого развертывания даже в самых крупных инфраструктурах. Инструменты автоматизации позволяют развернуть решение полностью всего за несколько часов. Также доступен вариант развертывания как сервис провайдера управляемых услуг безопасности (MSSP).

Прерывание алгоритма атаки

Вредоносные инструменты, используемые взломщиками, постоянно меняются, каждый день появляются новые уязвимости, которые могут быть использованы. Однако общая логика атаки остается неизменной. Любую направленную атаку можно представить в виде устойчивого и повторяющегося алгоритма, который получил название Kill Chain. Технологические разрывы, недостаточная степень интеграции существующих систем ИБ не позволяют организациям обнаруживать, анализировать и прерывать атаки на ранних стадиях Kill Chain. Однако, с появлением TrapX DeceptionGrid ™ мир ИТ-безопасности изменился…

О TrapX

TrapX Security – лидер в сфере киберзащиты на основе технологии «ложных» ИТ-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 подозрительных активностей, 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.

Технология DeceptionGrid может интегрироваться с существующими средствами ИБ и увеличивать 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 принятия адекватных 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.