cezurity

Решение Cezurity для обнаружения целенаправленных атак (APT, Advanced Persistent Threats) и сложного вредоносного программного обеспечения

В отличие от антивирусов и других традиционных средств защиты корпоративных сетей от атак и вредоносных программ, решение Cezurity основано на технологии *динамического обнаружения*. Технология динамического обнаружения включает поиск и анализ аномалий, возникающих в изменениях систем во времени. Динамическое обнаружение позволяет выявить атаки и вредоносные программы, которые отличает:

- **Конкретная цель атаки**

  Атакующего интересует заранее определенная информационная система компании или государственной организации. С помощью атаки решаются конкретные задачи, связанные с кибершпионажем или получением выгоды от компрометации информационных систем и данных.

- **Первостепенная задача — обойти защиту**

  Атакуемый объект всегда защищен. Для успеха атаки защиту нужно уметь обходить или отключать. Злоумышленники используют уникальные, еще не известные ИБ-индустрии вредоносные программы, уязвимости и способы атаки (0day).

- **Адаптивность и протяженность во времени**

  Атакующая сторона постоянно адаптирует методы атаки к используемым средствам безопасности. Неудачная атака не может остановить злоумышленников — они придумают более изощренный метод и повторят попытку.

- **Скрытость атаки**

  Злоумышленники часто ставят цель закрепиться в атакуемых системах и как можно дольше оставаться незамеченными. Так можно, например, постоянно похищать конфиденциальную информацию. Для этого они используют инструменты для сокрытия присутствия в информационных системах.

Как работает решение Cezurity

Каждый из компьютеров IT-инфраструктуры периодически сканируется с целью сбора и классификации широкого спектра характеристик. Результат каждого сканирования — срез системы (slice). Срез состоит из объектов, их характеристик и взаимосвязей между ними.

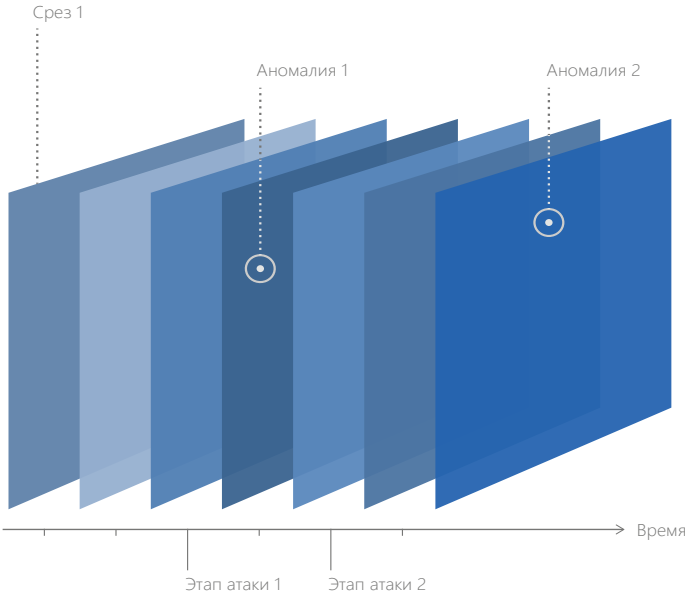
Срезы системы подвергаются нескольким видам анализа.

1. Статический анализ

Классификация всех объектов, входящих в срез системы (slice). Используются такие методы, как классификаторы («decision tree»), «белые списки» (whitelisting), анти-руткит технологии, механизм выявления похожих объектов («задача k-ближайших соседей»). С помощью статического анализа выявляются объекты, обладающие нетипичными для легитимного ПО характеристиками.

2. Динамический анализ

Выявление изменений во времени в срезах каждой системы и поиск в этих изменениях аномалий. Используются ассоциативные правила и кластерный анализ в рамках Big Data-подхода, реализованного в Cezurity Cloud.



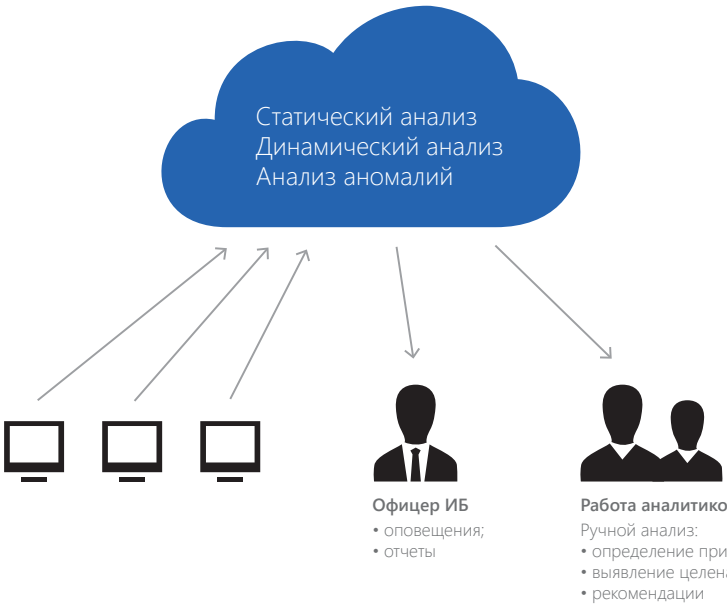
3. Анализ аномалий

Определение причин появления аномалий в изменениях. Используется разработанная Cezurity экспертная система и ряд метаклассификаторов, оперирующих результатами работы других видов анализа (статического и динамического). В некоторых случаях к анализу привлекается аналитик. Если причиной появления аномалии была атака, она будет обнаружена.

Преимущества решения Cezurity

Комплексная система обнаружения

Все типы атак могут быть обнаружены с помощью единого решения.



Решение опирается на такой набор признаков, который достаточен для обнаружения практически любых атак, в том числе и тех, где используются неизвестные методы атаки, уязвимости и уникальные вредоносные программы (0day). Если IT-инфраструктура атакована, на некотором этапе это приведет к аномальному изменению хотя бы одной системы, и атака будет обнаружена.

Другие решения зачастую фрагментарны — они могут быть эффективны в случае одной попытки атаки, но бесполезны при атаке другого типа. Например, могут отследить аномальный трафик, но не в состоянии сопоставить его с появлением новых файлов в критических областях системы.

Скорость обнаружения

Атака будет обнаружена сразу после того, как в одной из защищаемых систем зафиксировано критическое изменение.

Достаточная для защиты информация сразу при обнаружении атаки

Подход позволяет не только обнаружить атаку, но и без дополнительных инструментов определить пути защиты. Это возможно благодаря тому, что в основе решения лежит анализ всех критически важных изменений систем, которые протоколируются и доступны для анализа.

Просто внедрить и начать использовать

Решение не зависит от инфраструктуры и топологии защищаемой информационной системы, так как опирается на мониторинг изменений конечных точек. Это позволит быстро внедрить и начать использовать решение Cezurity даже в том случае, если IT-инфраструктура организации сложна и включает много различных систем. Использование решения не требует специальной экспертизы от персонала, обслуживающего IT-систему.

Низкая нагрузка на системные ресурсы

Наиболее ресурсоемкие процессы анализа происходят в облаке или в приватном облаке (private cloud). Это позволяет снизить нагрузку на конечные точки системы.

Совместимость с другими решениями

Решение может использоваться вместе с любыми другими средствами обеспечения информационной безопасности.

Высокая стабильность работы

За счет того, что клиентское программное обеспечение не нуждается в обновлениях, а его работа ограничивается сбором информации, снижается риск «падения» систем.

Дополнение DLP-решений: позволит обнаружить использование технических средств, примененных для похищения корпоративной информации

Использование решения закрывает важную уязвимость DLP-систем. Хотя DLP-системы и предназначены для защиты от утечек информации, они, как правило, не включают средств обнаружения специализированных вредоносных программ, которые могут использоваться для похищения данных и обхода DLP-защиты. Решение позволит обнаружить используемые для похищения инструменты и, соответственно, предотвратить утечку данных.

Cezurity — российская компания, разрабатывающая технологии и решения для защиты от широкого круга вредоносных программ и хакерских атак. Основана в 2006 году (до 2011 года называлась «Онлайн Решения»), с момента своего появления фокусируется на разработке технологий защиты нового поколения, реализация которых стала возможна благодаря широкому применению облачных технологий и методов интеллектуального анализа больших массивов данных (Big Data). Среди ключевых технологий Cezurity — анализ событий, мониторинг изменений систем, создание защищенных сред исполнения программного обеспечения.

Россия, Санкт-Петербург
ул. Матроса Железняка, 57

+7 812 640 4143
www.cezurity.com