cezurity

Технология динамического обнаружения целенаправленных атак

White Paper

Проблема

Взгляд Cezurity

Есть ли проблема? Различие между массовыми и целенаправленными (таргетированными) атаками

Сообщения о целенаправленных атаках, направленных на компании и правительственные организации, регулярно обсуждаются IT-сообществом начиная с 2006 года. После нескольких громких инцидентов, в результате которых были скомпрометированы информационные системы предприятий и государств, в индустрии защиты от киберугроз для обозначения целенаправленных атак стали использовать отдельный термин — **APT (Advanced Persistent Threat).**

Можно провести различие между «массовыми» атаками («commodity» threats) и целенаправленными. Цели «массовых» атак — очень широкий круг пользователей. При этом жертвами становятся лишь наименее защищенные из них, которых все равно оказывается довольно много по той причине, что атакуется большое число целей. Если атакующие планируют обойти защиту, то, как правило, их интересуют лишь наиболее распространенные решения — этого достаточно, чтобы атака оказалась успешной. То есть, принцип здесь можно сформулировать как «миля вширь, дюйм вглубь». При этом надежность защиты может оказаться достаточной, если у других атакуемых она просто ниже. Например, на улице, где все двери открыты, от воров спасет даже самый простой замок.

Массовые	**Целенаправленные**
Множество целей	Конкретная цель
Жертвы — «слабое звено»	Обойти защиту
«Молниеносная война»	Протяженные во времени
Заметные	Скрытые

Целенаправленные атаки строятся по другому принципу. Здесь атакующего интересует конкретная информационная система компании или государственной организации. С помощью атаки решаются задачи, связанные с кибершпионажем или получением той или иной выгоды от компрометации информационных систем и данных. При этом атакуемый объект всегда защищен разнообразными решениями обеспечения безопасности. Для успеха атаки все эти решения нужно уметь обходить или отключать. То есть, в отличие от «массовых» атак, принцип здесь противоположен: «дюйм вширь, миля вглубь».

Целенаправленные атаки обычно хорошо спланированы, включают несколько этапов — от внедрения в информационную систему до уничтожения следов присутствия, и, как правило, растянуты во времени — от начала атаки до получения результатов могут пройти месяцы или годы. Иногда злоумышленники ставят цель закрепиться в атакуемых системах и как можно дольше оставаться незамеченными — это дает возможность, например, постоянно похищать конфиденциальную информацию.

Зачастую для осуществления целенаправленных атак злоумышленники совершают точечные нападения на одного или нескольких пользователей. Задействуются самые разные методы сбора данных и внедрения в информационные системы. Это может быть социальная инженерия, эксплуатация известных и неизвестных (0day) уязвимостей, вредоносные программы и инструменты сокрытия их присутствия в системах. В таких атаках могут участвовать инсайдеры — помощники злоумышленников, работающие в атакуемых организациях.

Некоторые примеры целенаправленных атак

Число осуществляемых в каждый момент времени атак неизвестно. Безусловно, корпоративный шпионаж был всегда. Но сегодня специалисты в области компьютерной безопасности часто говорят о том, что мы вошли в новую эру киберпреступности — об этом свидетельствует характер обнаруженных в последнее время атак.

Stuxnet

Червь Stuxnet был обнаружен 17 июня 2010 года. Он поражал компьютеры под управлением ОС Microsoft Windows и был обнаружен на компьютерах обычных пользователей и в промышленных системах, которые управляли производственными процессами. Для внедрения в систему вирусом использовалось несколько уязвимостей операционной системы Windows — это были как известные уязвимости, так и неизвестные (0day). Вредоносной программе удалось несколько лет оставаться не замеченной ни одной антивирусной лабораторией, а мировой общественности она стала известна во многом случайно.

Duqu

В сентябре 2011 года была описана другая вредоносная программа — Duqu, эксплуатирующая неизвестную на тот момент (0day) уязвимость ОС Windows и, возможно, имеющая общее происхождение со Stuxnet. Антивирусными экспертами однозначно установлено, что атакованы были заранее выбранные цели. При этом срок существования вредоносной программы, которая использовалась для атаки, остается неизвестным. Отдельные модули существовали уже в мае 2011 года. На протяжении всего времени атакующие производили сбор информации в зараженных информационных системах. Компания Symantec нашла подтверждения того, что было атаковано минимум 6 компаний в 8 государствах.

Операция Аврора

Сообщение об атаке было опубликовано 12 января 2010 года в блоге компании Google, информационная система которой оказалась скомпрометирована. Данная атака продолжалась с середины декабря 2009 года и закончилась 4 января 2010 года. В результате злоумышленники получили доступ к информационным сетям нескольких известных американских компаний, таких как Google, Adobe, Symantec. По разным сообщениям в ходе данной атаки могло пострадать от 20 до 35 компаний. Предположительно, атака была осуществлена из Китая. Для внедрения в информационные системы использовалась неизвестная (0day) уязвимость в Internet Explorer.

Атака на Nortel

Сообщение о том, что хакеры около 10 лет похищали информацию у компании Nortel, было опубликовано в феврале 2012 года в The Wall Street Journal со ссылкой на слова бывшего сотрудника. По его словам, злоумышленники регулярно осуществляли доступ к информационным системам Nortel начиная с 2000 года. В 2004 году взлом был замечен

и предприняты меры для решения инцидента. Но признаки присутствия хакеров в сетях компании обнаруживались и позже — вплоть до 2009 года. Предположительно, в результате атаки регулярно похищалась конфиденциальная информация, среди которой были технические документы, отчеты об исследованиях и разработках, маркетинговые планы, переписка сотрудников.

Атака на компанию RSA

В марте 2011 года компания RSA (впоследствии RSA The Security Division of EMC) объявила, что стала жертвой целенаправленной атаки, а украденная из ее внутренней сети информация может быть использована для взлома систем, защищенных SecurID — разработанной RSA технологией двухфакторной аутентификации между пользователем и сетевым устройством. В июне 2011 года RSA пришлось подтвердить, что как минимум один ее клиент — компания Lockheed Martin, являющаяся крупнейшим предприятием военно-промышленного комплекса США, подверглась атаке, которая стала возможна по причине компрометации технологии SecureID. В атаке на RSA использовалась уязвимость Adobe Flash. Эксплуатирующая уязвимость троянская программа содержалась в направленных злоумышленниками сотрудникам RSA фишинговых письмах.

Операция Lurid

Lurid — это серия целенаправленных атак, о которой в сентябре 2011 года сообщила компания Trend Micro. В результате атаки было скомпрометировано около 1500 компьютеров, принадлежащих дипломатическим миссиям, министерствам, государственным космическим агентствам, исследовательским институтам и другим организациям в 61 стране. Атакующие с помощью вредоносных программ собирали с компьютеров жертв информацию. Исследование Trend Micro показало, что нападавшие хотели украсть конкретные документы.

Почему трудно найти решение?

Большинство методов, используемых для защиты от «массовых» атак («commodity» threats) и ставших уже традиционными в индустрии информационной безопасности, в случае с целенаправленными атаками оказываются практически бесполезными. Так, почти во всех получивших в последнее время известность целенаправленных атаках (Stuxnet, Duqu, и т. д.) использовались вредоносные программы, которые для антивирусной индустрии оставались неизвестными на протяжении нескольких лет. Что, безусловно, стало одной из главных причин успешности этих атак.

Существует ряд мер, которые могут усложнить задачу для атакующей стороны.

Это может быть, например:
- следование политикам безопасности;
- своевременное обновление программного обеспечения;
- использование антивирусного решения;
- системы обнаружения вторжений;
- SIEM-решения;
- оценка критичности всех систем и разграничение инфраструктуры.

При этом никакая из подобных мер в отдельности, ни их комплекс, не в состоянии обеспечить абсолютно надежную защиту. Трудности связаны с таким фундаментальным свойством целенаправленных атак, как готовность атакующей стороны адаптировать методы атаки к используемым средствам безопасности. Идеология большинства решений для защиты не учитывает то обстоятельство, что неудачная атака не в состоянии остановить злоумышленников — скорее всего, они придумают более изощренный метод и повторят попытку.

Можно отметить и такую особенность целенаправленных атак, как уникальность используемых злоумышленниками инструментов и методов, которые долгое время остаются для индустрии информационной безопасности неизвестными (0day).

Таким образом, предлагаемые сегодня ИБ-индустрией решения позволяют лишь усложнить задачу для злоумышленников, но не превратить ее в нерешаемую.

Динамическое обнаружение атак

Предлагаемая компанией Cezurity технология обнаружения целенаправленных атак основана на *мониторинге* и *оценке изменений* во времени состояния каждой из систем, составляющих IT-инфраструктуру.

Действия злоумышленников на каком-то этапе атаки неизбежно приведут к изменению атакуемых систем. Но так как заведомо не известны ни метод атаки, ни эксплуатируемая уязвимость, а инструментом атакующих может быть уникальная вредоносная программа (0day), отсутствующая в сигнатурных базах антивирусов, анализ атакованной системы не всегда позволяет обнаружить атаку. Атака может быть выявлена, если проанализировать все произошедшие изменения системы. Если система атакована, в изменениях появятся *аномалии*.

Например, если для закрепления в системе атакующие модифицируют какой-либо из критических файлов неизвестным способом (0day), то это приведет к появлению аномалии в изменении, которая может быть обнаружена в результате сравнения двух состояний: до изменения и после. То есть, аномалии выявляются при сравнении между собой состояний системы в разные моменты времени — в процессе *мониторинга изменений*.

Другими словами, безопасность можно обеспечить, если защита, как и атака, представляет собой постоянный, протяженный во времени процесс. Центральное место в процессе обеспечения защиты занимает анализ изменений состояний систем, выявление в них аномалий, их классификация и выявление признаков атаки. Динамическое обнаружение позволяет адаптировать защиту в соответствии с шагами злоумышленников. Такой подход можно сравнить с шахматной партией: когда у защищающейся стороны есть инструмент, позволяющий обнаруживать замысел противника после каждого хода на основе его предыдущих действий.

Выявление аномалий в изменениях представляет собой новое поколение средств детектирования — *динамическое обнаружение атак*. В отличие от статического обнаружения, когда разные состояния системы анализируются отдельно, динамическое обнаружение опирается на такой набор признаков атаки, который позволит выявить опасность без заведомого знания о том, что именно она собой представляет. То есть, технология динамического обнаружения не требует точного знания о том, как именно проводится атака.

В отличие от широко используемого большинством разработчиков статического обнаружения — когда разные состояния системы анализируются отдельно — динамическое обнаружение опирается на анализ изменений признаков, возникших в системе за определенный интервал времени.

Таким образом, используемый подход, по сравнению с другими решениями, значительно снижает риск компрометации информационной системы в результате целенаправленных атак.

Описание решения Cezurity. Принципы работы

Решение Cezurity предназначено для проведения аудита информационных систем предприятия с целью выявления активных целенаправленных атак или их следов, в том числе заражений сложными вредоносными программами (вредоносные программы обычно являются инструментом атакующих). Результатом аудита является отчет, включающий список найденных признаков атак и рекомендации по их устранению.

На каждом из компьютеров, составляющих IT-инфраструктуру, периодически выполняются сканирования критических областей системы, цель которых — сбор и классификация широкого спектра их характеристик. Результатом такого сканирования является срез системы (slice). Срез системы состоит из объектов, их характеристик и взаимосвязей между ними.

Срезы системы передаются в облачную экспертную систему Cezurity Sensa, где подвергаются анализу. При анализе учитываются контексты трех типов: контекст среза, контекст времени и контекст окружения.

1. Контекст среза — анализируются отдельные срезы системы

Задача данного анализа — классифицировать все объекты, входящие в срез системы (slice). Используется ряд методов, в том числе индуктивно обученные классификаторы («decision tree»), «белые списки» (whitelisting), анти-руткит технологии, механизм выявления похожих объектов («задача k-ближайших соседей»). Помимо статических характеристик объектов на данном этапе используются статистические данные об объектах, их взаимосвязях и положении в системе. Используются такие данные, как:

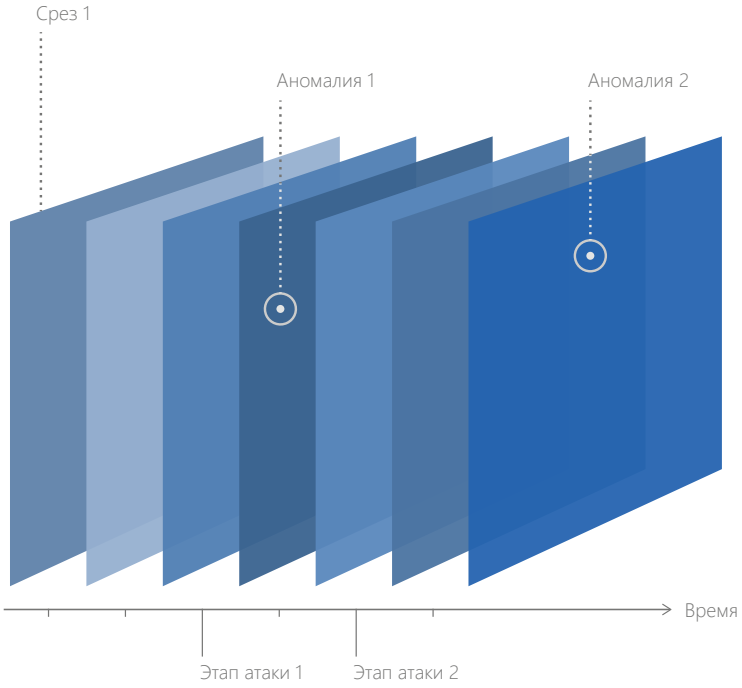
- ареал распространения;
- частота упоминаний объекта;
- частотные характеристики параметров упоминаний объектов и их связей;
- гистограммы «внешних» характеристик.

В данном виде анализа могут быть обнаружены такие виды аномалий, как, например, нетипичные или противоречивые наборы характеристик одной системы. В Cezurity Sensa постоянно поступает, подвергается классификации с использованием механизмов ML (Machine Learning) и хранится информация об объектах и их характеристиках, которые встречаются на компьютерах.

Пример 1: компьютер оборудован сетевой картой NVIDIA — в этом случае в срезе будет представлен целый набор файлов, относящихся к вендору NVIDIA. Появление не всего набора, а лишь одного файла драйвера при отсутствии прочих, делает такой файл подозрительным.

Пример 2: несовпадение в одних и тех же наборах характеристик объекта, полученных разными способами — этот механизм выявляет наличие rootkit-компонентов, которые являются признаком аномалии.

2. Контекст времени — анализируются изменения срезов системы



Срезы системы, полученные в разные моменты времени, сравниваются между собой, а произошедшие изменения подвергаются анализу. Причем ни исходное состояние, ни конечное могут не играть никакой роли — рассматривается именно появление новых объектов и изменение их характеристик. Отслеживаются и анализируются любые изменения — это важно, так как изменения характеристик могут не иметь признаков аномалий. Например, они могут быть вызваны обновлением программ, изменением конфигураций, иногда появление новых легитимных объектов модифицирует характеристики уже существующих.

Для определения того, какие срезы сравнивать между собой, используется алгоритм, учитывающий динамику во времени, возникновение критических событий в системе, внешние изменения. Алгоритм может «отматывать» состояния системы в прошлое с целью понять и классифицировать изменения в «будущем».

Пример 1: выявлено изменение файла с целью получения механизма автозапуска вредоносного кода — такое изменение достаточно просто отличить от штатного обновления, так как экспертная система обладает знанием об исходных характеристиках объекта.

Пример 2: характеристики объекта неоднократно менялись, но каждая из модификаций не приводит исходный объект к его текущему состоянию. Для поиска таких аномалий Cezurity Sensa формирует некий вектор изменения объекта, который анализируется. Так может быть обнаружена попытка сокрытия следов атаки путем коррекции измененных веток реестра, атрибутов файлов или перемещения объектов в исходные локации.

3. Контекст окружения — сравниваются срезы систем, составляющих IT-инфраструктуру компании

Оценивается взаимосвязь между изменениями срезов, полученных со всех компьютеров, составляющих единую IT-инфраструктуру. Для достижения цели злоумышленники могут предпринять целый ряд шагов, которые сами по себе не вызывают подозрения. Компьютеры, не являющиеся конечной целью, становятся «трамплином» для каждого следующего этапа атаки. Оценка событий, произошедших на отдельных компьютерах, может измениться после анализа их взаимосвязи.

Пример: на нескольких компьютерах одной организации обнаружены изменения объектов, каждое из которых в отдельности подозрения не вызывает. Сопоставление таких изменений может привести к тому, что потребуется дополнительный анализ, либо из последовательности событий «сложится» вектор атаки, и, соответственно, это приведет к сигналу тревоги.

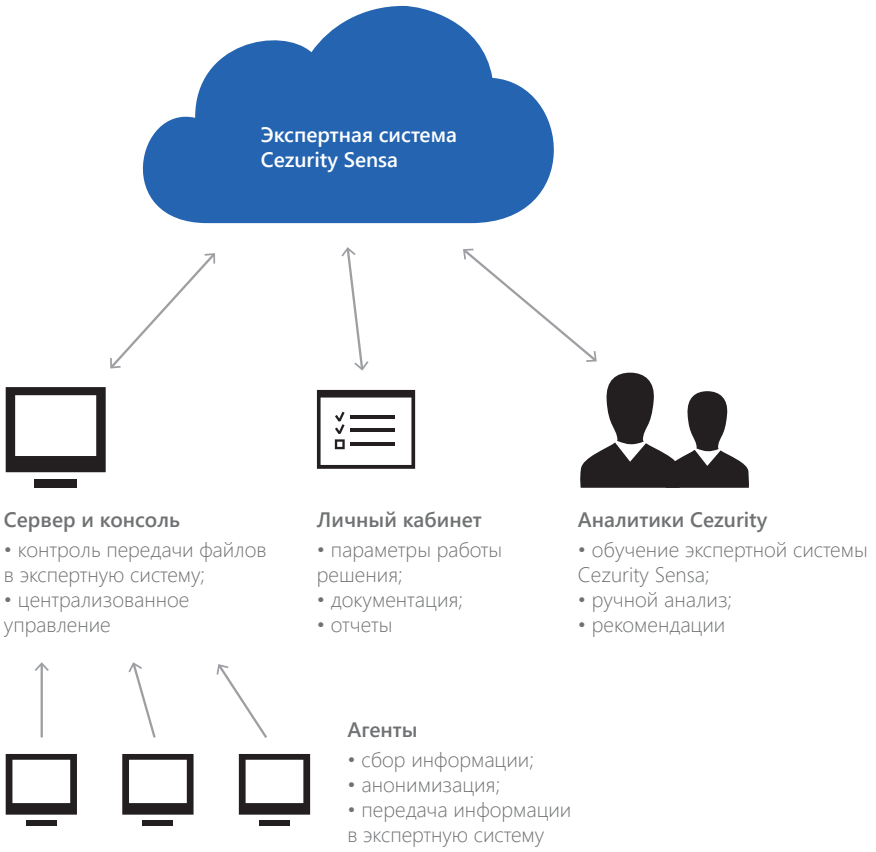
В большинстве случаев экспертная система Cezurity Sensa способна сделать вывод о наличии аномалий без участия аналитиков. Если принять однозначное решение автоматически невозможно, к анализу привлекается аналитик Cezurity.

Таким образом, может быть выявлен любой из этапов целенаправленной атаки, на котором действия злоумышленников привели к появлению аномалий в изменениях состояния хотя бы одной из систем.

В том числе это могли быть такие действия, как:
1) шаги, направленные на закрепление в системе;
2) модификация критических объектов системы;
3) компрометация данных;
4) хищение данных;
5) предоставление удаленного доступа к системе;
6) вмешательство в работу программно-аппаратных комплексов;
7) удаление следов присутствия.

Решение Cezurity COTA позволит обнаружить атаки, где применены неизвестные методы внедрения и закрепления, а также используются еще не обнаруженные (0day) уязвимости и вредоносные программы. Это становится возможным благодаря тому, что отслеживается и анализируется любое из критических изменений, а также их совокупность.

Архитектура решения Cezurity



Решение Cezurity включает 4 основных компонента:

1. Агент — программный модуль, устанавливаемый на каждый компьютер анализируемой ИТ-инфраструктуры. Модуль выполняет периодическое сканирование состояния системы, извлекает необходимый набор критических объектов и их характеристик. Полученные данные агрегируются, анонимизируются и передаются для анализа в в облачную экспертную систему Cezurity Sensa.

2. Сервер и Консоль управления сервером. На уровне Сервера осуществляется контроль передачи файлов в облачную экспертную систему Cezurity Sensa. Решение позволяет офицеру безопасности или системному администратору настроить политики передачи объектов из корпоративной сети. Также с помощью Сервера реализуется развертывание и обновление Агентов без использования средств Active Directory.

3. Экспертная система Cezurity Sensa. Система облачного хранения и анализа больших массивов данных. Система предназначена для классификации ПО, поиска вредоносного программного обеспечения и выявления целенаправленных атак или их следов. Система расположена на серверах компании Cezurity и поддерживается специалистами этой компании.

4. Личный кабинет. Для оценки хода внедрения решения офицер информационной безопасности или системный администратор могут самостоятельно получить доступ к некоторым параметрам работы решения. Это необходимо для того, чтобы обеспечить полноценное внедрение. К таким параметрам относятся:

- статистика по работе агентов;
- список машин, не выходивших на связь более 3-х суток;
- статистика сканирований;

- статистика найденных объектов;
- статистика новых объектов;
- статистика подозрительных и вредоносных объектов.

В личном кабинете доступна документация по продукту и дистрибутивы поставляемых пакетов.

Личный кабинет доступен как из локальной сети предприятия, так и снаружи.

Преимущества решения Cezurity

1. 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 с использованием сложного вредоносного программного обеспечения. Если IT-инфраструктура атакована, это на некотором этапе 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.

Использование для обнаружения атак нескольких решений параллельно зачастую сильно усложняет администрирование защиты, что в результате может негативно сказаться на общем уровне защищенности информационной системы.

2. Скорость обнаружения

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

3. 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, соответственно, доступны для анализа.

4. 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 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.

5. Низкая нагрузка на системные ресурсы

Наиболее ресурсоемкие процессы анализа происходят в облачной экспертной системе Cezurity Sensa. Это позволяет снизить нагрузку на конечные точки системы.

6. Совместимость с другими решениями

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

7. Высокая стабильность работы

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

8. 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, но, 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

Резидент IT-кластера «Сколково»

Продажей и внедрением решения для защиты от целенаправленных атак на основе разработанной Cezurity технологии динамического обнаружения занимается компания InfoWatch. Решение поставляется под торговой маркой InfoWatch Targeted Attack Detector (InfoWatch TAD). Для получения дополнительной информации обратитесь, пожалуйста, в компанию InfoWatch: +7 495 229 0022, www.infowatch.ru