Обзор платформы Seceon OTM - быстрое и точное выявление угроз в Вашей сети.

Краткое изложение

Изощренность и объем внутренних угроз, а также, направленных на сетевые ресурсы кибератак на данный момент больше, чем когда-либо раньше. Несмотря на значительные инвестиции в безопасность, компании подвергаются риску катастрофических нарушений конфиденциальности. Эти нарушения вредят бизнесу компаний и приводят как к прямым, так и к косвенным убыткам. Недавние опубликованные отчёты о взломах ресурсов компаний показали, что эти убытки могут достигать сотен миллионов, если учесть ликвидацию последствий, штрафы и потери в стоимости бренда. Руководители компаний и советы директоров стали обращать внимание на проблемы, которые ранее считались зоной ответственности директоров по ИТ-безопасности и руководителей ИТ-отделов.

Как мы видим, компании проигрывают хакерам, постоянно изобретающим новые методы несанкционированного доступа, потому что применяемые методы защиты непрерывно устаревают. Традиционные технологии безопасности неспособны остановить современные точечно направленные угрозы. Снова и снова хакеры демонстрируют свою способность проскользнуть мимо охраны даже наиболее укрепленных периметров. Киберпреступники и кибер шпионы теперь почти не используют известные уязвимости и распространённые вредоносные программы. Теперь они действуют неизвестными доселе способами: изучая Ваших людей, процессы управления предприятием, технологии и системы поставок; и исполняя роль зарегистрированных пользователей - иногда вообще не используя вредоносное программное обеспечение.

Эти методы позволяют хакерам проходить через защиту периметра, уклоняться от технологий обнаружения атак, таких как IDS, IPS и NGFW, и обойти контроль конфигурации, контроль соблюдения политик, проверки систем на уязвимости и т.д. Они могут обойти SIEM и Log аналитические продукты, которые не могут правильно приоритезировать угрозы и часто пропускают важные события безопасности, даже когда они уже произошли.

Тихая угроза: Ни одно из сегодняшних традиционных решений не имеет дело с одной из самых вредных угроз: внутренняя угроза. Verizon опросил крупные и средние предприятия в своем Отчете Угроз[4] 2015 и определил, что внутренние угрозы составляют до 40% от всех обнаруженных угроз. Это только лишь известные угрозы, большинство из этих внутренних угроз до сих пор не обнаружено. Инсайдер, используя свои или чьи-либо учётные данные, как правило, знает, где искать самую ценную информацию, и при использовании актуальных учётных данных не будет остановлен ни SIEM, ни DLP, ни мониторингом активности пользователей или другими традиционными инструментами контроля безопасности.

Очевидно, внутренняя и кибер-безопасность находится в переломном моменте. Чтобы побороть сегодняшние и завтрашние угрозы, предприятия должны начать мыслить по другому. Seceon полагает, что пора “изменить ход событий”. Это означает, что необходимо анализировать ситуацию с точки зрения нападающего, понимая его цели, тактику и методы, и в соответствие этой новой точке зрения строить Вашу защиту.

Эта стратегия воплощена в платформе Seceon OTM - первая поведенческая платформа обнаружения и реагирования, которая сразу информирует, мгновенно обнаруживает и активно устраняет все угрозы.
Используя методы раннего обнаружения, современные алгоритмы обнаружения угрозы и управляемое блокирование, а также, устраняя последствия инцидента, Платформа Seceon OTM заранее обнаруживает и активно отвечает на угрозы.

Этот обзор детализирует современные проблемы безопасности и описывает, как Платформа Seceon OTM позволяет нашим клиентам своевременно выявлять угрозы и автоматически отвечать на них в режиме реального времени.

Введение

В то время, когда такие громкие имена как Anthem, Sony, Scottrade, Erade, Home Depot, JPMorgan Chase и Target заполонили заголовки СМИ после обширных нарушений конфиденциальности данных, правда состоит в том, что более 80% компаний в США подверглись успешным атакам инсайдеров или кибератакам[1]. Кибератаки стали столь широко распространенными, что фактически никакая промышленность сегодня не защищена от этой новой действительности. Банковское дело, производство, розничная торговля, здравоохранение, туризм и другие отрасли стоят перед компромиссом и следующими репутационными и финансовыми убытками.

Проще говоря, злоумышленники постоянно опережают службы безопасности корпораций и их меры безопасности. По общему мнению экспертов по безопасности, число нападений продолжит расти. На данный момент и в обозримом будущем, хакеры сильнее многих организаций, они проводят направленные, сложные нападения, которые часто остаются не обнаруженными существующими технологиями безопасности.

Считавшаяся ранее исключительно проблемой IT кибербезопасность теперь стала проблемой высшего менеджмента и правления корпорации. Так как усиленное внимание уделяется риску кибератаки, правления, топ-менеджеры, принимающие решения, как и директора по ИТ-безопасности, теперь ставят кибер-безопасность наивысшим приоритетом. Обзор Piper Jaffray показывает, что это главный приоритет при формировании бюджетов для правления: 75% респондентов обзора ответили, что они увеличили бы расходы на кибер-безопасность в наступающем году[2] . Однако, если эти расходы не станут новой философией, они, вероятно, просто добавят новый слой к существующей груде неэффективных продуктов безопасности.

---

1 CFO Survey June 2015 - http://www.cfosurvey.org/2015q2/press-release-hacking.pdf

2 Piper Jaffray 2015 CIO Survey

Чтобы быть эффективными, инвестиции должны включать разработку новых методов для защиты цифровых активов от внутренних, а также, от внешних киберугроз. Статус-кво традиционной, основанной на подписи или вредоносного анализа защиты, оказался совершенно несоответствующим для предотвращения успешных нападений.

Рост направленных атак

В 2015, впервые, кибер-безопасность была главной темой в ежегодном докладе президента США конгрессу о положении в стране.
Несанкционированные проникновения сложного характера доминировали в заголовках СМИ в течение прошлых 18 месяцев, выдвигая на первый план тревожную картину катастрофически успешных кибератак. Худшее то, что эти нападения — не обычные взломы, которые производятся при помощи вредоносных программ. Это специально направленные нападения с целью кражи конфиденциальных данных или нанесения урона бизнес-процессам. В результате чего, убытки, причиненные направленными нападениями, могут быть огромными, включая финансовые потери и угрозу репутации. Согласно Институту Ponemon, средняя стоимость повреждения данных в 2014 составила $3.5 миллиона. После того, как нарушение было обнародовано, Target указала на убытки в размере более чем $148 миллионов, что является оптимистической оценкой[3].

Сегодняшние продвинутые злоумышленники создают средства нападения, специально предназначенные для того, чтобы обойти защиту конкретной выбранной цели. Эти нападения хорошо замаскированы, и разработаны так, чтобы перемещать точку воздействия внутри организации в течение многих недель или месяцев перед тем, как проникнуть сквозь охраняемый периметр. Согласно отчетам о нарушении[4], их присутствие остается не обнаруженным, в среднем, в течение 200 дней.

Обход безопасности конечной точки

Несмотря на наличие свежих сигнатур вирусов, выполнение надлежащего управления обновлениями ПО и закупку новейших средства обнаружения вредоносных программ, даже самые подготовленные организации пали жертвой направленных нападений. Почему?

Ответ заключается в том, что изощренность хакеров продолжает опережать способности так называемой защиты следующего поколения. Методы, которые были когда-то доступны только спонсируемым государством хакерам, теперь легко используются преступными синдикатами и группами хакеров. Трояны и эксплойты, которые становятся все популярнее и доступнее, предоставляют хакерам легкие методы для подбора и подстановки сетевых атрибутов атакующего таким образом, чтобы обойти меры безопасности, основанные на контроле этих данных, а также,

---

3 “Cybersecurity Hindsight and a Look Ahead at 2015,” Yoav Leitersdorf and Ofer Schreiber, TechCrunch, Декабрь 28, 2014

4 2015 Verizon Threat Report

простейшие аналитические решения. Комбинация этих методов с вновь обнаруженными уязвимостями ПО предоставляет злоумышленникам полную свободу действий.

Непрерывная изменение местоположения источника атаки позволяет хакерам оставаться фактически не обнаружимыми большинством обычных средств защиты, из-за их уверенности в устаревших методах обнаружения, таких как hashes и помещение IP в черный список. Избежать обнаружение в пределах песочниц или виртуальных решений может большинство хакерских программ.

Измени игру; Думай как хакер

Не удивительно, что недавние опросы показывают: две трети респондентов думают, что новые решения могут пополнить или заменить их существующую защиту. Но какая новая защита действительно является эффективной против этих более сложных нападений? Как директора по ИТ-безопасности и CIO могут улучшить защиту своих компаний, обнаружить угрозы быстрее и более точно и остановить нападения, прежде чем реальный ущерб будет нанесен?

Ответ заключается в том, чтобы начать думать как хакер и использовать в своих интересах уроки, полученные от тех, кто изучил опытных хакеров. Когда большинство экспертов по безопасности говорят: “думай как хакер”, они защищают от проникновения, повторяя действия хакеров, чтобы определить слабые места в системах безопасности. Однако, чтобы быть действительно эффективными при блокировании направленных нападений, мы должны быть на шаг впереди. Мы должны проникнуть в мысли хакера и понять его цели, тактику и методы – в сущности их поведение.

Во время обучения и практических занятий военачальников учат представить себя противником, чтобы понять любую ситуацию с его точки зрения. Делая так, можно начать понимать достоинства и недостатки противника и предпринимать действия, основанные на этом понимании. В кибер области та же самая стратегия является подходящей при защите информационных ресурсов.

Борясь с “темной стороной” Интернета, эксперты по кибер-безопасности могут лучше понять намерения, методы, инструменты и цели атакующих. От подпольных хакерских форумов до онлайн рынков, распродающих платформы киберпреступности в Китае, России или Бразилии, эти эксперты учатся думать как хакер.
С интеллектом “инсайдера” и лучшим пониманием преимуществ атакующего, они могут помочь своим организациям определить неизвестные угрозы, которые пропущены устаревшей защитой, более быстро и эффективно отреагировать, оказаться между атакующим и его целью или между активом и точкой утечки.

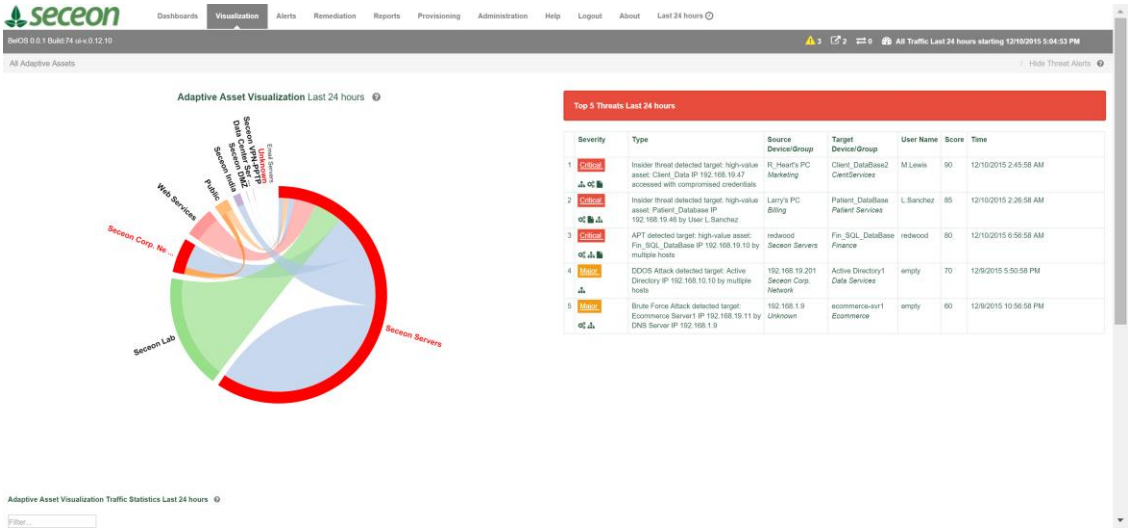
В то время, когда этот подход, несомненно, является необходимым для противостояния сегодняшним направленным нападениям, не верно думать, что наем десятков или сотен специально обученных и опытных экспертов по кибер-безопасности является правильным методом для предприятий. Если не так, то как тогда может ритейлер, производитель, финансовая организация, провайдер телекоммуникаций, учреждение здравоохранения, поставщик

энергоресурсов или другой тип компании использовать этот метод борьбы для защиты своих информационных ресурсов от злоумышленников во всем мире? Для этого есть Платформа Seceon OTM.

Развитие платформы Seceon OTM

С платформой Seceon OTM, Вы получаете обнаружение угрозы на базе поведенческого анализа, которое объединяет глубокую и многоплановую аналитику для обнаружения сложных угроз и быстрой реакции на внутренние угрозы и кибератаки.

Думая как хакер, Платформа Seceon OTM ищет угрозы способами, которые другие продукты не используют, предугадывая выбор поведения нападающих; решение резко уменьшает преимущество хакера. Результат - мгновенное обнаружение и ответная реакция в реальном времени с указанием мер противодействия.



Платформа Seceon OTM анализирует ресурсы серверов, сетевые устройства, приложения и поведение пользователей, чтобы быстро обнаружить присутствие внутреннего риска и внешних киберугроз, таким образом ускоряя ответную реакцию, предотвращая повреждение данных и их потерю. Вот так она работает:

1. Датчик Сбора и Контроля (CCE): датчик Seceon может находиться непосредственно на контролируемых конечных точках или на отдельном сервере для удаленного сбора данных, с минимальным воздействием на производительность сети, устройства или приложения. Датчики Seceon CCE наблюдают тысячи действий наряду с различными признаками, включая пользователя, систему, приложение, файл и сетевые соединения, направляя наблюдения в APE Seceon. CCE способен принимать меры в отношении внутренней или кибер угрозы после получения инструкции от APE.

2. Analytic Processing Engine (APE): облачный аналитический сервер Seceon собирает детальную информацию о приложениях, сетях, файлах и конфигурациях от всех датчиков и устройств. Используя основанный на контексте поведенческий анализ и элементы

искусственного интеллекта, он быстро обнаруживает подозрительное поведение в режиме реального времени, по мере развития событий. Этот механизм основан на корреляции событий, составляющих последовательность действий, представляющих угрозу. Визуализация в реальном времени показывает злонамеренное поведение, аномальные или направленные хосты, приложения и устройства, позволяя оператору своевременно отреагировать.

3. Автоматизированный Ответ Seceon: Платформа Seceon OTM позволяет Вашей службе безопасности быстро и эффективно расследовать инциденты и реагировать на них, не требуя навыков и знаний опытного эксперта. Она реализует механизмы, которые существенно уменьшают вероятность ложных тревог, давая возможность службам безопасности взять на себя управление в режиме реального времени.

4. Разведка Угроз Seceon: Платформа Seceon OTM подключена к более чем 40 лучшими источникам анализа угроз. У нашей платформы есть способность в режиме реального времени находить самый лучший источник сведений о потенциальных угрозах заданного вида, находить развивающиеся угрозы, заранее предупреждая наших клиентов о новых методах атак и их технологиях, для каждой специфической области деятельности предприятия и его местонахождении. Эти источники информации используются в качестве модели возможных угроз, используемой Обработкой Аналитики Seceon, чтобы находить и распределять по приоритетам известные и неизвестные угрозы, которые способны обходить традиционную защиту.

Почему Seceon

С Платформой Seceon OTM вы можете защититься от направленных атак с помощью:

Широкая наблюдаемость ресурсов организации

Подход Seceon начинается со способности контролировать всю деятельность в сети и в критических устройствах, которые разрешают или обеспечивают доступ к ценной информации. Приложение Seceon CCE собирает, составляет и превращает проверенную регистрацию устройств и поток сетевых данных в важную информацию. Оно суммирует действия и передает эту информацию централизованному APE, чтобы выполнить обнаружение угрозы и аналитические процессы предсказания. Лёгкое приложение CCE может также работать в виртуальных или облачных средах. CCE может контролировать тысячи действий и признаков, включая пользователя, систему, приложение, файл и сетевые соединения, с минимальным воздействием на производительность сети.

Определение в режиме реального времени

Облачная Аналитическая обработка Seceon (APE) объединяет приложение, сеть, хост, файл, пользователя и детали конфигурации от датчика CCE. Машинное обучение формирует модели угрозы, которые коррелируют события, и проводит основанный на контексте поведенческий анализ; подозрительное поведение быстро определяется и прослеживается в режиме реального времени, по мере развития событий. Визуализация определяет злонамеренное поведение и

аномальные или атакованные хосты, устройства, приложения и пользователей, позволяя оператору предпринять своевременные действия.

Ответ в режиме реального времени

Платформа Seceon OTM позволяет Вашей службе безопасности быстро, эффективно расследовать и реагировать, не требуя навыков и знания опытного эксперта. Она реализует механизмы, которые существенно уменьшают вероятность ложных тревог, давая возможность службам безопасности взять на себя управление в режиме реального времени. Это устраняет подавляющее число ложных и повторяющихся тревог, производимыми традиционными продуктами безопасности.

Продвинутая разведка угроз

Платформа Seceon OTM подключена к более чем 40 лучшими источникам анализа угроз. У нашей платформы есть способность в режиме реального времени находить самый лучший источник сведений о потенциальных угрозах заданного вида, находить развивающиеся угрозы, заранее предупреждая наших клиентов о новых методах атак и их технологиях, для каждой специфической области деятельности предприятия и его местонахождении.

Вывод

Хакеры продолжают достигать новых уровней инноваций и изобретательности, поскольку они преследуют цели воровства или нанесения ущерба. Они обучены виртуозно обходить уровни защиты современных организаций. Основанные на сетевых атрибутах технологии и, так называемая, защита следующего поколения оказались не соответствующими текущим задачам. В результате, жертвы обнаруживали угрозу или сильный ущерб своей репутации, а также прямые финансовые потери. Наконец, и самое главное, истинные внутренние угрозы необходимо обнаруживать и останавливать, прежде чем критическая информация поставлена под угрозу или стала доступна посторонним. Сегодня, как правило, такая потеря остается не обнаруженной.

Чтобы полностью изменить эти тенденции, защитникам нужны лучшие инструменты, которые не только обнаруживают такие угрозы, прежде чем реальный ущерб будет нанесен, но и делают это автоматически, за считанные секунды, без потребности в анализе опытным специалистом, чтобы установить количество и объем таких угроз. Инструменты, которые позволяют значительно улучшить положение безопасности организации, позволяют сотрудникам тратить меньше времени на реагирование и больше времени - на превентивные действия. Меняя ход событий, организации будут в состоянии быстро обнаружить и отвечать противникам, уменьшая потенциальные потери и вред. Seceon использует современные, основанные на поведении алгоритмы обнаружения угрозы, чтобы обнаружить новейшие или ещё не известные угрозы, которые традиционная защита пропускает. С Платформой Seceon OTM Вы можете взять всё под контроль.

Узнать больше о Платформе Seceon OTM можно посетив: www.seceon.com