Эффективная защита в режиме реального времени

Обзор тенденций эволюции современных угроз безопасности и развития SIEM-решений (на примере RSA Security Analytics), призванных противостоять этим угрозам.

Андрей Перкунов – руководитель направления информационной безопасности компании "СТЭП ЛОДЖИК".

Павел Коростелев – эксперт по информационной безопасности компании "СТЭП ЛОДЖИК".

Введение

ИТ-системы крупных предприятий постоянно подвергаются риску атак со стороны злоумышленников. Оставляя в стороне мотивировку этих атак (идейную, государственную или финансовую), уверенно можно сказать, что их сложность растет.

Характерным для злоумышленников является использование ботнетов и вредоносного ПО с модулями обхода антивирусных систем. Ботнет – сеть, состоящая из компьютеров, зараженных специализированным вредоносным ПО. Зараженный компьютер находится полностью под контролем злоумышленника – из него могут быть извлечены данные, на компьютер могут быть установлены дополнительные вредоносные модули, он может участвовать в спам-рассылках и DDoS-атаках. Заражение компьютера и деятельность вредоносного ПО происходит незаметно для пользователя, что затрудняет обнаружение проблемы и ее решение. Взаимодействие с оператором происходит по зашифрованному каналу связи через открытые сетевые порты (80, 443 и т.д.). В последнее время разработчикам вредоносного кода и операторам ботнетов стали доступны сервисы, которые позволяют автоматически отслеживать обнаружение образцов вредоносного ПО с помощью различных антивирусных систем, а также вносить незначительные изменения в код вредоносного ПО, делая уже созданные антивирусные сигнатуры неактуальными. Это значительно снижает эффективность антивирусных систем и повышает риски для стабильности инфраструктуры и безопасности корпоративных данных.

Инвестиции в ИБ, как правило, направлены в большей степени на защиту от проникновения злоумышленника в сеть компании, а также на пресечение несанкционированного доступа к ценным ресурсам. Однако если злоумышленник применит принципиально новый способ атаки, то существующие средства защиты уже не смогут его остановить. Кроме того, корпоративная система ИБ будет все время запаздывать, так как внедрение новых средств защиты привязано к общекорпоративному циклу бюджетирования и закупок.

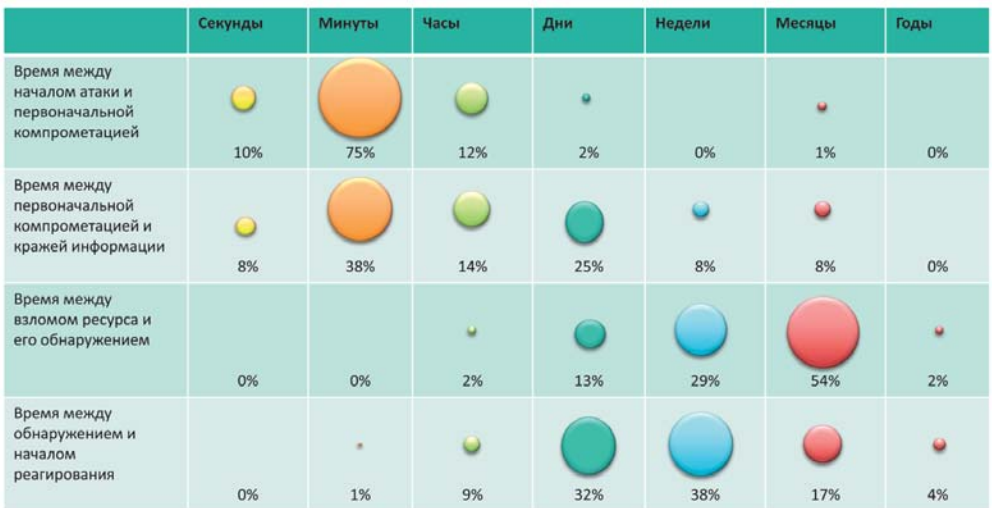
Таким образом, при использовании злоумышленником принципиально нового способа атаки, все предыдущие инвестиции в средства ИБ предприятия мгновенно обесцениваются.

Следующим важным фактом является невозможность своевременно отследить момент проникновения злоумышленника в сеть предприятия и его действия, если они не носят открыто деструктивный характер. Соответственно, все процедуры, связанные с расследованием таких действий, запускаются, только когда (если) их все же засекли. К сожалению, к этому времени минимизировать ущерб уже невозможно (рис. 1).

Для того чтобы бороться со сложными атаками, предприятию нужны не только средства защиты информации, но и система, способная отслеживать аномальное поведение пользователей и ИТ-систем, а также своевременно оповещать об этом профильных сотрудников, осуществляя проактивный подход к работе системы защиты корпоративных ресурсов.

Механизмы работы SIEM-систем

Прародителями современных SIEM систем являлись два разных класса систем – SIM (Security Information Management) и SEM (Security Event Management). Системы класса SIM отвечали за агрегацию данных из множества различных источников (логи серверов, приложений, сетевого оборудования, средств защиты, приложений, СУБД и проч.), их унификацию, анализ и долговременное хранение (рис. 2). Появление та-



Источник – Verizon Data Breach Investigation 2012

Рис. 1. Длительность периодов между этапами инцидента.

Рис. 2. Архитектура потоков данных в SIEM-решениях.

Рис. 3. Интеграция функционала SIM- и SEM-систем привела к возникновению SIEM-решений.

ких систем было обусловлено не только потребностями бизнеса, но и жесткими требованиями американского законодательства (в частности, актом Sarbanes-Oxley, GLBA и др.). SEM системы отвечали за мониторинг в режиме реального времени, корреляцию событий, оповещение и отчетность.

Взаимная интеграция этих систем (рис. 3) и привела к образованию аббревиатуры – SIEM (Security Information and Event Management).

Агрегация логов

Одним из ключевых механизмов, которые использует SIEM, является механизм сбора и агрегации логов (рис. 4). Эта информация поступает из множества различных источников – сетевое оборудование, средства защиты информации, приложения, СУБД и др. Информация попадает в SIEM либо напрямую из отслеживаемых систем (как правило, используется syslog для информации о состоянии системы и C-flow/J-flow – о характеристиках сетевого трафика), либо через парсинг лог-файлов. В последнем случае на отслеживаемую систему ставится SIEM-агент, который отправляет информацию на сервер агрегации данных.

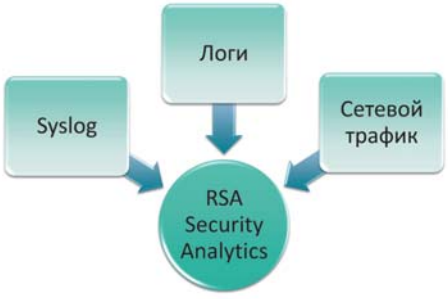


Рис. 4. Механизмы получения данных для RSA Security Analytics.

Несмотря на то, что для современных систем написано очень много коннекторов, на предприятиях могут использоваться различные "самописные" приложения, которые также необходимо отслеживать. Для включения их в контур мониторинга существует возможность написания собственных правил парсинга (при условии, конечно, что приложение пишет информацию о своем состоянии в лог-файл). В общем случае информация о том или ином событии содержит отметку о времени (т.н. timestamp), код события, а также набор произвольных полей данных, часть которых встречается очень часто (IP-адрес источника события, имя пользователя и т.д.). Задав в правилах парсинга формат логов и назначение полей данных, мы сможем использовать эти данные в SIEM-системе.

Одним из ключевых показателей производительности SIEM-системы является количество обрабатываемых событий (например, строк в лог-файлах) в единицу времени. Чем большее количество систем мы отслеживаем, тем выше этот показатель, и, соответственно, серьезнее требования к SIEM-системе в части процессинга и хранения этой информации.

Для территориально-распределенных компаний очень важным является вопрос масштабирования системы, так как источники данных могут находиться на удаленных площадках и использовать "узкие" каналы связи. В этом случае используются модули "препроцессинга", которые разворачиваются на удаленных площадках, собирают информацию и отправляют ее на сервер агрегации в оптимизированном виде.

После обработки информация становится доступна оператору, который может ее использовать для расследования инцидентов, статистического анализа работы ИТ-систем или аудита.

Корреляция событий

При подключении большого количества источников данных неизбежно возникает вопрос анализа получаемой информации. Ручная обработка потока данных даже средней системы (3–5 тысяч событий в минуту) невозможна, поэтому для мониторинга работы систем используются различные способы корреляции событий, обеспечивающие автоматизированный анализ поступающих событий и привлекающие оператора только в случае явной необходимости.

Можно выделить два основных способа корреляции:

- корреляция на базе правил (Rule based correlation);
- корреляция без использования правил (Rule-lesscorrelation).

Каждый из этих способов имеет как достоинства, так и определенные недостатки.

Классическим является способ корреляции событий на базе правил. В этом случае при внедрении системы мы описываем определенную последовательность логических действий, которые характеризуют действия злоумышленника. Например, большое количество попыток входа в какую-либо систему, напоминающее процесс подбора пароля, которое заканчивается успешным входом в эту систему. Преимуществом этого способа является высокая точность обнаружения злоумышленника. К недостаткам можно отнести необходимость периодического обновления правил корреляции и невозможность реагировать на последовательность событий, не описанную в правилах.

Корреляция без использования правил использует риск-ориентированный подход, подобный банковским скоринговым системам. В рамках этого подхода все события имеют определенный рейтинг, и, когда уровень рейтинга последовательности событий с одним параметром (исходящий IP-адрес, целевой IP-адрес, пользователь и т.д.) превышает установленный, происходит оповещение оператора. Преимуществом этого способа является отсутствие зависимости от написанных правил и возможность обнаружения новых векторов атак. К недостаткам относится меньший уровень точности, потому что существует вероятность того, что необычные действия выполняет легитимный пользователь. Также можно выделить статистический анализ событий, когда работающие системы создают стандартный профиль событий (например, большое количество успешных авторизаций в Active Directory утром в будний день). Таким образом, нестандартное событие (например, авторизация ночью или попытка удаленного доступа с территории другого государства) также может означать вероятность инцидента ИБ.

Индексация сетевого трафика

В ряде систем, в частности, в RSA Security Analytics (за счет интеграции с NetWitness и с увеличением производительности SIEM-системы) появилась возможность сбора и хранения копии сетевого трафика, что позволяет значительно повысить эффективность расследования инцидентов ИБ. После выявления подозрительной активности в сети предприятия сетевой трафик между злоумышленником и целевой системой представляет особый интерес. При этом для ряда протоколов существует возможность его просмотра на уровне приложения. Например, для SMTP-трафика есть возможность просмотра писем, для telnet-сессии – последовательность введенных команд и т.д. Все это дает аналитику широкие возможности для расследования инцидентов и выявления ущерба.

Использование внешних источников данных

Многие компании, работающие в сфере ИБ, производят постоянный мониторинг угроз в сети. Этот процесс включает в себя отслеживание активности ботсетей, новых видов вредоносного ПО, инструментов для взлома информационных систем и методов атак. Работа с такими источниками данных является ключевой для современных систем ИБ, в том числе и для SIEM. Их интеграция заключается в придании контекста информации, попадающей в SIEM-систему. Например, попытка удаленного доступа с внешнего IP-адреса, с которого была зарегистрирована подозрительная активность в отношении другой компании, должна сразу заинтересовать оператора SIEM-системы.

Расследование инцидентов

Так как SIEM-система является центром агрегации всех данных, объем событий, требующих дополнительного анализа, в ней всегда выше, чем в обычных средствах ИБ. В связи с этим, SIEM-системы располагают встроенным механизмом построения процессов расследования инцидентов ИБ. Например, в случае появления инцидента, связанного с работой сетевого оборудования, будет создан инцидент и назначен ответственный сотрудник. В итоге система позволит строить процессы, аналогичные ITSM, например, назначать специалистов, отвечающих за выполнение задач, а также определять максимальный срок реакции, отслеживать статистику по инцидентам и т.д.

Соответствие требованиям

Благодаря уникальной архитектуре SIEM-систему удобно использовать при проведении аудитов на соответствие требованиям различных стандартов безопасности, как внешних (PCI DSS, SOX), так и внутренних. Одним из требований к SIEM-системе является наличие механизмов отчетности и преднастроенных шаблонов отчетов, соответствующих различным мировым стандартам. Кроме этого, важно иметь возможность создавать отчеты в различных форматах – для аудиторов, ИТ-персонала и бизнес-руководства.

Что необходимо для успешного внедрения

Для успешного внедрения SIEM-системы необходим не только опыт реализации подобных проектов, но и экспертиза по всем системам, которые будут включены в контур мониторинга. Кроме того, для эффективной эксплуатации систем необходимо наличие корпоративных процедур и ресурсов, задействованных в расследовании инцидентов ИБ.

Специалисты СТЭП ЛОДЖИК готовы предложить заказчикам комплексное решение, включающее в себя внедрение SIEM-системы, а также разработку всех необходимых документов, связанных с порядком расследования инцидентов ИБ.

Решение

Для реализации SIEM-системы мы предлагаем решение на базе продукта RSA Security Analytics. Продукт предоставляет инструментарий для анализа различных источников информации, а также данных, передаваемых по сети. Для внедрения системы мы используем уникальную экспертизу СТЭП ЛОДЖИК в области построения систем передачи данных, внедрения средств защиты информации, а также создания корпоративных политик и процедур ИБ. Это позволит заказчику получить эффективную и полнофункциональную систему в кратчайшие сроки.

RSA Security Analytics обладает рядом преимуществ перед аналогами других производителей:

- инфраструктура хранения данных, спроектированная для обработки больших объемов данных в масштабе времени, близкому к реальному;
- интеграция с облачным сервисом RSA, предоставляющим актуальную информацию о новых угрозах ИБ;
- возможность анализа сетевых сессий и трафика;
- расширенный инструментарий для расследования инцидентов;
- возможность работы с учетом ценности различных корпоративных ИТ-активов;
- дополнительные механизмы выявления вредоносного ПО.

Инфраструктура хранения данных

В силу особенностей архитектуры SIEM-систем к подсистеме хранения данных всегда предъявляются особые требования. Система должна обеспечивать обработку большого объема данных, а также, при необходимости, быстро извлекать их из хранилища. Решение этой сложной задачи требует использования специализированных СУБД, которые доступны в решениях не всех производителей SIEM-систем. Работа с хранилищем данных в режиме времени, близком к реальному – это отличительная особенность продукта RSA.

Интеграция с облачным сервисом RSA Threat Intelligence

Использование внешнего источника данных о новых угрозах в сфере ИТ значительно повышает эффективность обнаружения инцидентов и работы системы в целом. Оператору всегда доступна актуальная информация о новых уязвимостях, угрозах, активности ботнетов применительно к активам конкретной компании.

Возможность анализа сетевых сессий и трафика

Анализ сетевого трафика значительно повышает эффективность SIEM-системы. Аналитик может не только установить факт передачи информации по какому-либо протоколу, но и просмотреть эти данные как на уровне отдельных пакетов, так и на уровне сессии в целом, например, установив последовательность команд, передающихся по telnet, или восстановив файл, передававшийся по FTP.

Расширенный инструментарий для расследования инцидентов

За счет использования платформы RSA NetWitness Security Analytics предоставляет аналитику широкий инструментарий для расследования инцидентов. Аналитик может быстро получить полный доступ к любой информации, касающейся активности того или иного сервиса, пользователя или IP-адреса. Совместно с возможностью анализа сетевого трафика это значительно повышает эффективность работы системы в целом. Без применения этого инструментария расследование инцидентов занимало бы значительно больше времени, так как информацию необходимо было бы запрашивать у других подразделений.

Возможность работы с учетом различной степени ценности корпоративных активов

Ценность и важность информации, хранящейся в ИТ-активах компании, различна. Безусловно, в первую очередь необходимо реагировать на инциденты, вследствие которых могут пострадать более ценные данные. Использование такого подхода дает возможность оптимально перераспределять ресурсы департамента безопасности и, в первую очередь, уделять внимание более приоритетным задачам.

Дополнительные механизмы выявления вредоносного ПО

Зачастую вредоносное ПО способно обходить традиционные антивирусные системы, использующие сигнатурный, эвристический подход. Security Analytics использует метод "Sandboxing". В рамках этого подхода подозрительный файл помещается в виртуальную "идеальную среду", где система анализирует его активность. Если активность напоминает вредоносную, то файл соответствующим образом помечается. Это позволяет выявлять вредоносное ПО без использования традиционного анализа, который злоумышленники уже научились обходить.

Пример расследования инцидента ИБ средствами RSA Security Analytics

Аналитику приходит оповещение о потенциальном подборе пароля пользователя (несколько записей в логе сервера удаленного доступа, затем сообщение об удачном входе этого пользователя). Аналитик в режиме реального времени получает данные об активности удаленного пользователя во внутренней сети предприятия. В рамках отчета фиксируется использование сетевых эксплоитов по отношению к серверу, содержащему критичную информацию. Далее аналитик запрашивает информацию по активности на сервере, фиксирует вход удаленного пользователя с правами администратора и передачу с сервера некоего архива, запрашивает информацию по сессии, в рамках которой был передан этот архив, и восстанавливает передаваемый архив. В архиве может содержаться, например, файл с конфиденциальным годовым отчетом о деятельности компании.

В описанном сценарии видно, что аналитик зафиксировал вторжение, в течение короткого времени проанализировал вовлеченные в инцидент ИТ-активы и отследил, какая информация была похищена. Средства, предоставляемые RSA Security Analytics, позволяют полностью реализовать данный процесс.

Заключение

Наличие только средств защиты информации не является гарантией сохранности корпоративных ресурсов. Для обеспечения оптимального уровня защиты необходима система мониторинга ИБ, работающая в режиме реального времени.

Не все SIEM-системы обладают уровнем производительности, достаточным для обеспечения расследования инцидентов в реальном времени, что значительно снижает эффективность их работы.

Специалисты СТЭП ЛОДЖИК предлагают универсальное решение – систему RSA Security Analytics. Внедрение RSA Security Analytics обеспечит сбор и анализ данных журналов безопасности ИТ-систем, а также индексацию общего сетевого трафика. Уникальная экспертиза СТЭП ЛОДЖИК позволит сократить сроки внедрения решения и создать все необходимые процедуры для обеспечения эффективной работы системы.

Внедрение SIEM-системы значительно повысит уровень безопасности ресурсов, позволит упорядочить процесс расследования инцидентов и сократить расходы на обеспечение ИБ.

Андрей Перкунов,
Павел Коростелев,
компания "СТЭП ЛОДЖИК"