Визитка

АНДРЕЙ БИРЮКОВ, специалист по информационной безопасности. Работает в крупном системном интеграторе. Занимается внедрением решений по защите корпоративных ресурсов

Средство мониторинга событий ИБ
Выбираем подходящее

«Кто предупрежден, тот вооружен» — гласит древняя мудрость. Поговорим о средствах мониторинга событий информационной безопасности

Что нам нужно?

Для начала определимся с терминологией. Решения по мониторингу событий информационной безопасности обозначаются аббревиатурой SIEM (Security Information and Event Management, управление информацией о безопасности и событиях безопасности). Такие приложения включают в себя средства автоматизированного сбора событий, их нормализации, то есть приведения текста события к некоторому общему виду (например, выделение из события имени пользователя, IP-адреса, порта соединения и т.д.). Также классический SIEM сохраняет все события в единой БД и позволяет составлять правила корреляции, выявляя статистические закономерности. С помощью этих правил специалист по безопасности может существенно автоматизировать свою работу по обнаружению и предотвращению атак. Опционально решение также содержит средства генерации отчетов и автоматизации расследования инцидентов. Как правило, присутствует возможность реагирования на события и интеграции с системами IPS.

Помимо классических SIEM, существуют также узконаправленные, осуществляющие мониторинг только специализированного типа систем, например СУБД (Guardium, Sentrigo Hedgehog и другие). В рамках данной статьи мы будем рассматривать только классические SIEM.

Продукты SIEM доступны под различными лицензиями коммерческие так и бесплатные решения. В этой статье мы рассмотрим как те, так и другие. Начнем с коммерческих.

ArcSight ESM

Данный продукт является признанным лидером на рынке коммерческих SIEM-решений. ArcSight ESM [1] позволяет собирать данные с различных сетевых устройств, операционных систем и приложений и производит корреляцию этих событий. В настоящий момент поддерживается более 275 типов источников сообщений.

Также осенью 2010 года появилась возможность мониторинга сетевых потоков с помощью NetFlow. Для этого предлагается использовать FlowSensor, устройство которое, подсоединяясь к «зеркалируемому» SPAN-порту, генерирует сообщения в формате NetFlow для последующей передачи в ArcSight. Подробнее об этом решении можно прочесть на этом сайте [2].

Операционные системы, на которых может быть развернут ArcSight, – это RedHat Linux, MS Windows Server 2003 32- или x64, IBM AIX 5L 5.3 64 bit, Solaris 9/10 32 или 64 бит. В качестве хранилища данных используется СУБД Oracle 10g.

ArcSight состоит из трех основных компонентов:

SmartConnectors – коннекторы, которые подключаются к устройствам и осуществляют сбор событий.

Manager – собственно ядро системы, осуществляющее обработку и корреляцию событий.

Data Base – база данных, в которой хранятся все события.

При использовании ArcSight все три компонента можно установить на один сервер, но я категорически не рекомендую этого делать. Как минимум разнесите коннекторы с остальными модулями. Тогда в случае выхода из строя менеджера (если не используется отказоустойчивая конфигурация) события станут кэшироваться на коннекторах, затем будут переданы в базу данных и обработаны менеджером при его включении.

Подключение нестандартных источников – это, пожалуй, важнейший вопрос, который возникает при внедрении систем SIEM. В каждой сети есть специфичные приложения, в том числе и собственной разработки. Как правило, средства SIEM их не поддерживают. Но эти системы также необходимо контролировать.

Для подключения таких источников в ArcSight предусмотрен специальный мастер FlexAgent Creation Wizard, с помощью которого в интерактивном режиме легко «обучить» ArcSight разбирать поля событий в новом источнике.

Еще одним важным преимуществом ArcSight является богатый функционал по настройке правил взаимосвязи и реагированию на события. В случае выполнения заданных условий возможны различные варианты реагирования: новое событие, отправить уведомление по электронной почте, а также выполнить сценарий или блокировку с помощью IPS. Сам ArcSight не может выступать в роли IPS, так как он

предназначен для мониторинга событий, а не для предотвращения вторжений. Для взаимодействия с IPS в ArcSight предусмотрено отдельное аппаратное решение TRM (Threat Response Module), интегрирующееся с ESM. Это устройство осуществляет взаимодействие с сетевыми устройствами и выполняет на них различные команды.

Если атака произошла, сторонние приложения не понадобятся, ArcSight ESM содержит набор средств для автоматизации расследования, которые позволят осуществлять поиск событий, связанных с ним, документировать этапы расследования инцидента.

Для лучшего понимания того, как все эти модули взаимодействуют, приведу небольшой пример. С клиентской машины злоумышленник вводит несколько неверных паролей для одной учетной записи при входе в домен Active Directory. Коннекторы ESM получают эти события непосредственно от источников, производят проверку их соответствия правилам корреляции в режиме, приближенном к реальному времени. В случае если такое совпадение имеется, на устройство TRM передается команда по блокировке атакующего хоста. Параллельно администратору отправляется уведомление на электронную почту. Теперь посмотрим, как выглядят визуальные компоненты ESM.

Сама консоль реализована в двух вариантах: веб и «толстого», устанавливающегося на рабочую станцию администратора. При использовании веб-варианта на сервере ESM необходимо установить дополнительный модуль, отвечающий за веб-доступ.

В целом ArcSight является заслуженным лидером рынка решений по мониторингу событий безопасности. Единственное, что внушает некоторые опасения по поводу будущего данного продукта, – тот факт, что недавно HP приобрела ArcSight. Насколько поглощение гигантом скажется на дальнейшем развитии продукта, покажет время.

Symantec Security Information Manager

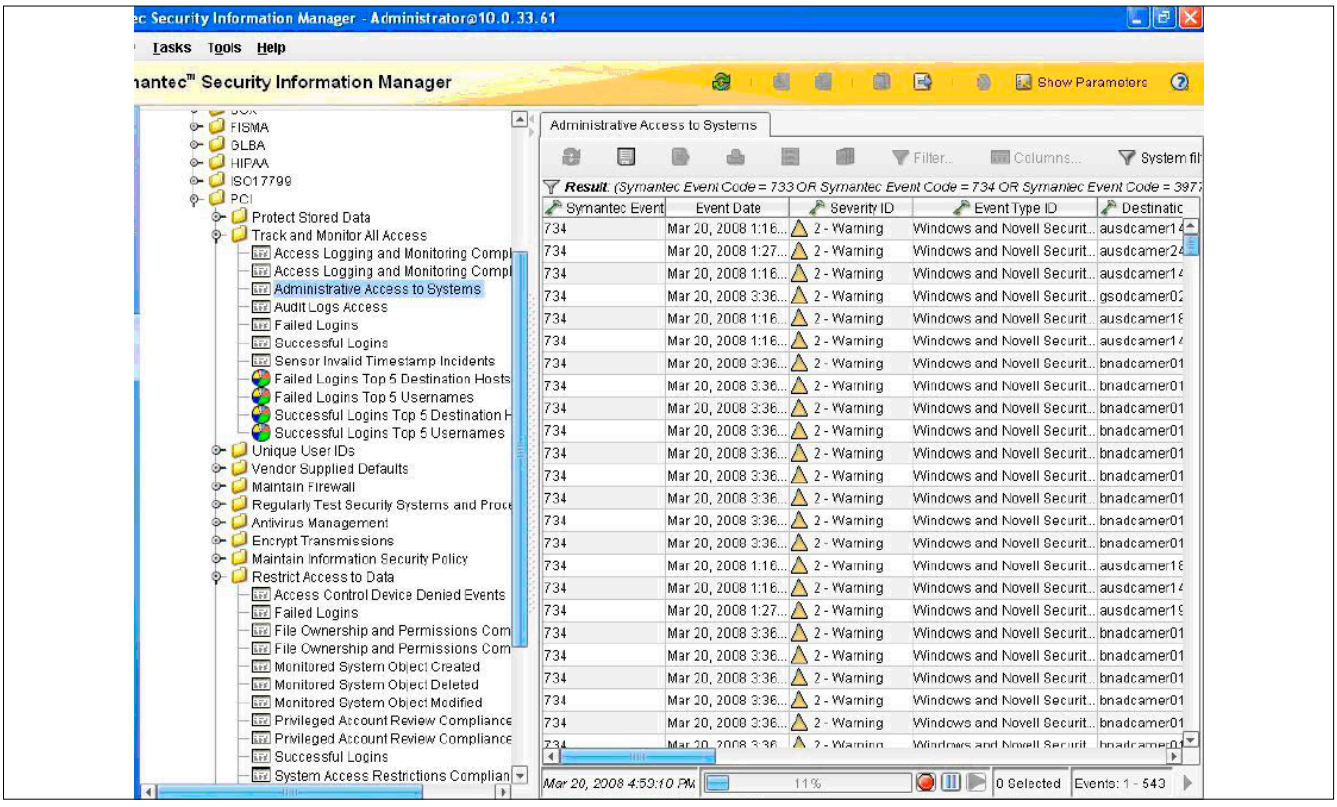
Компания Symantec обладает обширным набором решений по информационной безопасности. И хотя наиболее известными являются антивирусы и системы резервного копирования, продукт Security Information Manager [3] тоже заслуживает внимания. В списке совместимых только одна операционная система – Red Hat® Enterprise Linux 4.7 32 bit. Плюс доступен вариант под VMware ESX 3.5 и 4.

Консоль клиента SIM ставится еще на ОС Windows.

Symantec SIM позволяет собирать события ИБ со всех устройств и приложений корпоративной сети в режиме, близком к реальному времени. Получать информацию можно более чем со 100 различных источников. Для систем, которые не входят в этот список, предусмотрена возможность разработки собственных коллекторов для сбора событий ИБ с помощью специализированного программного пакета Collector Studio. Но этот пакет доступен для партнеров компании Symantec, которые предоставляют услуги по разработке коллекторов.

На основе собранных данных Symantec SIM помогает выявлять угрозы безопасности, направленные на наиболее важные бизнес-приложения, определять приоритеты угроз, автоматически создает инциденты. При выявлении какого-либо инцидента срабатывает определенный тип оповещения (в соответствии с настройками) – уведомления от-

Рисунок 1. Консоль управления Symantec SIM



правляются ответственным специалистам по электронной почте или SMS. Вся информация и результаты ее обработки хранятся в централизованной базе.

Самые разные отчеты, создаваемые SIM, помогут специалисту по безопасности получить информацию о состоянии сети в разрезе информационной безопасности.

Как видите, функционал SIM схож с ArcSight, однако по некоторым возможностям ArcSight обходит решение от Symantec. Так, SIM не отображает критичность событий, а значит, и события не могут быть отсортированы по этому критерию. К примеру, администратор безопасности, придя утром на работу, с помощью системы Symantec сможет определить только увеличение количества сообщений в определенный ночной период времени. Используя же систему ArcSight, администратор сразу же определит важность события с точки зрения безопасности.

К тому же система ArcSight позволяет просматривать все сообщения (обычные и коррелированные) в одном окне, коррелированные события помечены значком с молнией. А в системе Symantec такой просмотр можно выполнить только в двух разных окнах (Incedents и Events), что также не совсем удобно.

Приведенные доводы относятся к средствам визуализации и могут оказаться не существенными при выборе конкретного решения. Говоря о недостатках, следует также отметить, что поддержка устаревшей ОС говорит о том, что разработчик не стремится развивать продукт. Далее перейдем к обсуждению продукта от IBM.

Tivoli Security Operations Manager

Данный продукт изначально планировался как мощное SIEM-решение, обладающее всем необходимым функционалом: гибкими средствами нормализации событий, мощным функционалом построения корреляций, средствами построения отчетов, интеграцией с решениями Checkpoint и многим другим. Однако фактически дела обстоят значительно хуже. Но обо всем по порядку. Начнем с описания продукта.

TSOM поддерживает платформы Red Hat Enterprise Linux ES 4.5, Sun Solaris 10, AIX 5L V5.3. Некоторое время назад TSOM работал под ОС Windows Server 2003 64 bit, но сейчас в списке возможных ОС данная система не упоминается [4].

Состоит из трех модулей:

CMS (Central Management System) – ядро системы, осуществляющим корреляцию событий.

EAM (Event Aggregation Module) – модуль осуществляет сбор и нормализацию событий.

Data Base – база данных для хранения событий (Oracle или DB2).

Программа установки не позволяет установить EAM и CMS на одну машину. Помимо этих трех модулей, в состав дистрибутива входит UCM (Universal Collection Module), с помощью которого осуществляется сбор событий с Windows-машин, баз данных и приложений. Собранные события UCM передает в EAM, где осуществляется их нормализация.

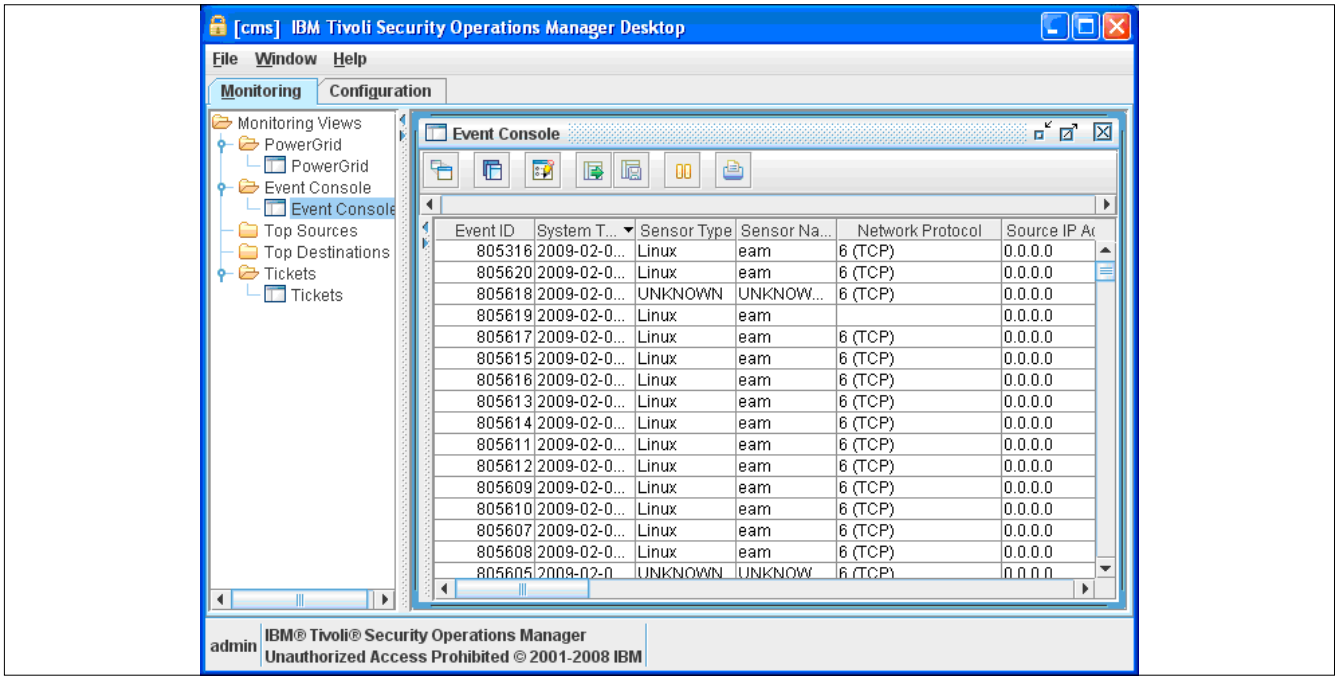
Для подключения новых источников в TSOM необходимо неплохо разбираться в программировании, для того чтобы «обучить» EAM читать журнал не поддерживаемого официально формата с помощью скриптов на Perl.

Это не так плохо, потому что можно с помощью регулярных выражений RegExp разобрать практически любой лог.

Значительно хуже дела обстоят с правилами корреляции, в особенности с их надежностью. Здесь постоянно возникают проблемы: то только что созданные в консоли правила вдруг становятся невидимыми, то правило срабатывает дважды, то вообще не срабатывает.

Средства работы с инцидентами представляют собой интерфейс, позволяющий отслеживать статус инцидента,

Рисунок 2. Консоль событий TSOM



вносить заметки об этапах расследования, менять статус и т.д.

Набор готовых шаблонов, доступных в CMS, позволяет генерировать порядка 30 видов отчетов. В случае необходимости разработки собственного шаблона можно воспользоваться ПО JReports.

Впрочем, проблемы с надежностью есть не только у отдельных компонент, но и у продукта в целом. Нередки случаи, когда соединение между модулями по непонятным причинам пропадает, и проблема решается только перезагрузкой. Для продукта, позиционирующегося как средство мониторинга событий ИБ, такое недопустимо.

Регулярная установка довольно громоздких (порядка 500 Мб) пакетов обновлений FixPack мало способствует решению проблем с надежностью. Бывали случаи, когда после установки обновления TSOM переставал функционировать.

У читателей может возникнуть вопрос, зачем я вообще включил описание данного продукта в свой обзор, если он обладает таким количеством недостатков. Хочу заметить, что в Magic Quadrant от Gartner (общемировой независимый критерий оценки различных решений) для SIEM решения от IBM по-прежнему находятся достаточно высоко. Поэтому не рассматривать этот продукт совсем было бы с моей точки зрения неправильно.

Cisco MARS

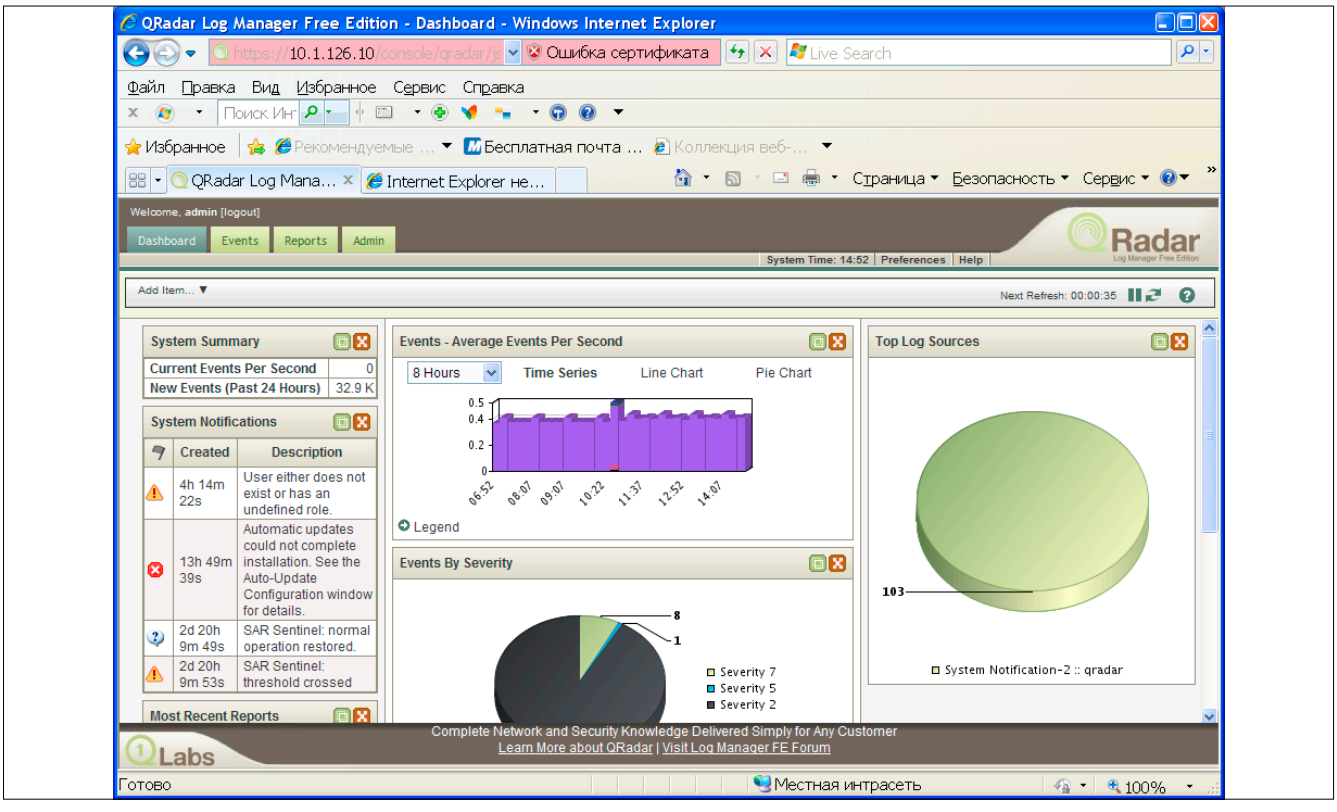
Данное аппаратное решение знакомо многим специалистам по сетевой безопасности, работающим с продуктами Cisco. Система мониторинга, анализа и ответной реакции Cisco MARS (Cisco Security Monitoring, Analysis, and Response System) является аппаратной комплексной платформой, предоставляющей возможности тщательного наблюдения и контроля существующей системы безопасности [5]. Cisco MARS ориентирован на сбор данных, прежде всего с сетевых устройств. Также возможны мониторинг приложений, обнаружение аномалий, включая анализ информации, получаемой по Cisco NetFlow, корреляция событий как на основе правил, так и анализа «поведения» объектов сети, встроенные и определяемые администратором правила, автоматическая нормализация транслированных сетевых адресов (NAT normalization).

Также Cisco MARS позволяет производить построение топологической схемы сети, как по запросу администратора, так и регулярно по графику. В частности, может автоматически обнаруживать маршрутизаторы, коммутаторы и межсетевые экраны 2 и 3 уровней, отдельные системы IDS (сетевых систем обнаружения вторжений). MARS поддерживает управление по протоколам SSH, SNMP, Telnet.

В отличие от упоминавшихся выше продуктов Cisco MARS производит анализ уязвимостей при обнаружении аномалий или угроз безопасности. Для этого выполняется анализ конфигурации коммутаторов, маршрутизаторов, межсетевых экранов и NAT. На основании полученной информации выполняется запрос к базе данных уязвимостей.

По результатам делается вывод о наличии проблемы и необходимости внедрения дополнительных средств защиты. Также имеются средства для снятия «следов», оставленных нарушителем в масштабе сети или на отдельном узле. Естественно, речь идет об оборудовании производства Cisco.

Рисунок 3. Консоль управления QRadar Log Manager



Объединение сеансовых событий с контекстом всех правил при их настройке позволяет автоматизировать расследование инцидентов.

В системе выполняется графическое представление пути атаки с подробным анализом, с помощью которого администратор может отследить, через какие устройства сети осуществлялась атака. Такая визуализация позволяет существенно упростить процесс расследования инцидента.

Создание правил осуществляется с помощью графического интерфейса. Оповещения об инцидентах ИБ Cisco MARS может отправлять на электронную почту, пейджер, системный журнал и SNMP.

В целом MARS является эффективным и производительным средством мониторинга сетевой безопасности.

Кстати, недавно стало известно, что в 2011 году Cisco Systems завершит продажи MARS. Таким образом, компания планирует покинуть рынок SIEM- решений, еще больше сконцентрировавшись на разработке сетевых и коммуникационных решений.

QRadar Log Manager Free Edition

QRadar Log Management – это средство централизованного сбора и анализа событий ИБ. Несмотря на то что решение является аппаратным, разработчики предоставляют также тестовый VMware Appliance, то есть образ виртуальной машины, обладающий всем функционалом QRadar, которую можно бесплатно загрузить с сайта разработчика [6].

QRadar Log Manager позволяет осуществлять сбор событий от различных источников (сетевое оборудование, операционные системы, приложения и т. д.), их нормализацию, сохранение во внутренней БД, а также корреляцию на соответствие различным моделям угроз. В качестве ответных реакций на угрозы QRadar Log Management создает новые события, отправляет уведомления по электронной почте и протоколу Syslog. Для управления QRadar Log Management используется веб-клиент, доступ к которому осуществляется по протоколу HTTPS.

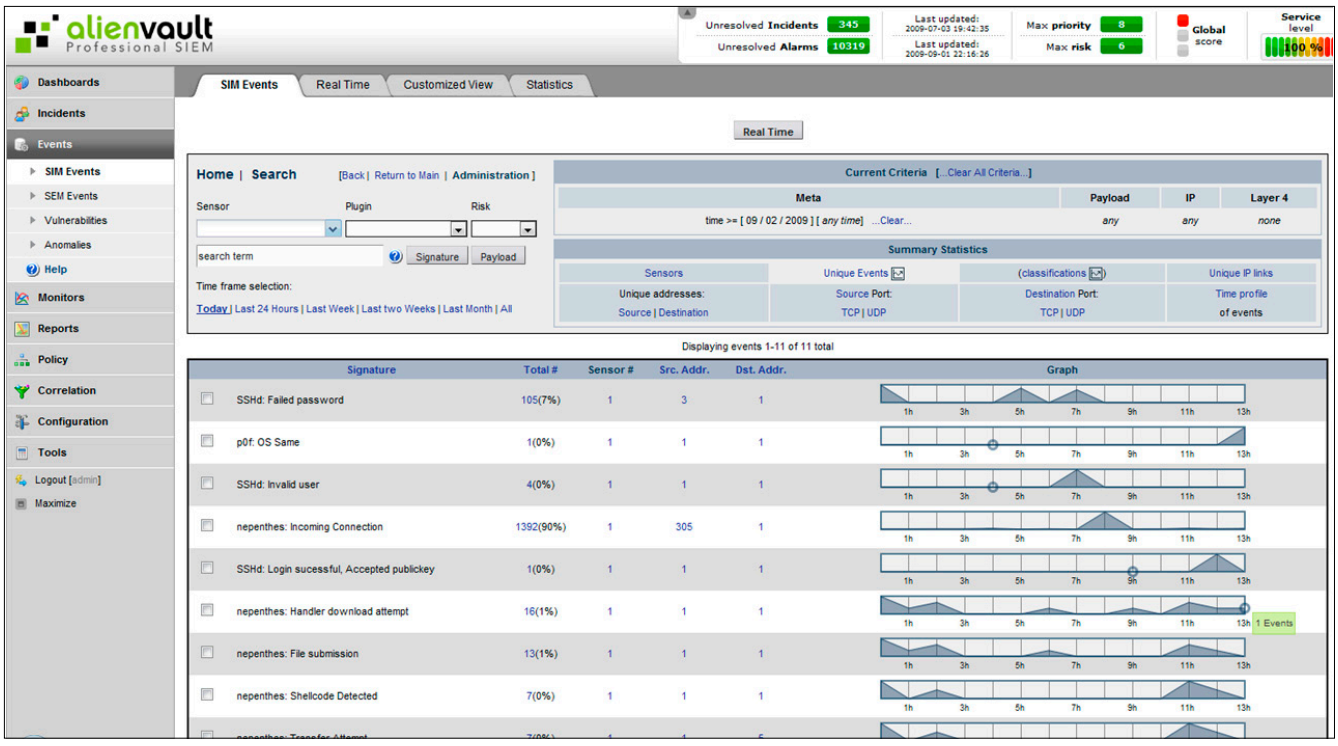
Подключение источников событий к системе осуществляется без использования агентского ПО, что позволяет избежать дополнительной нагрузки на серверы – источники событий. Причем здесь в отличие от описанных ранее решений разворачивать какие-либо промежуточные серверы (по типу EAM в системе TSOM) не требуется вовсе.

QRadar Log Manager удобен в работе, подключение источников событий не вызывает особых проблем. Для нестандартных журналов событий допустимо применить язык регулярных выражений RegExp.

Из недостатков продукта отмечу отсутствие возможности в качестве ответной реакции запускать сценарии. Конечно, в аппаратном решении выполнять полноценные скрипты на Perl вряд ли возможно, но сделать поддержку ограниченного числа команд разработчики могли бы.

Для работы QRadar Log Management Free Edition необходимо выполнение следующих аппаратных требований: двухядерный 2 ГГц или выше процессор (обязательно должна поддерживаться 64-битная архитектура), 4 Гб оперативной памяти; 300 ГБ дискового пространства; QRadar Log Manager Free Edition поддерживает VMware ESX 3.5.x и VMware Player v3.x. Собственно, с версией виртуальной среды проблем возникнуть не должно, так как на сайте VMware доступен для скачивания конвертер, позволяющий без особых трудностей конвертировать образ из одной версии виртуальной среды в другую. А вот требование 64-битной архитектуры является жестким.

Рисунок 4. Консоль событий OSSIM



Помимо QRadar, имеется еще несколько аналогичных аппаратных решений, заслуживающих внимания. Это RSA enVision [7] и LogLogic [8]. Далее мы переходим к описанию бесплатных SIEM-решений.

Open Source SIM

По заявлениям авторов, основной задачей проекта OSSIM (Open Source Security Information Management) является максимальная интеграция разнородных утилит в пределах единой открытой архитектуры. В 2005 году в нашем журнале уже была статья, посвященная OSSIM [9], однако с тех пор проект развивался, поэтому я включил его в этот обзор.

Современная версия OSSIM [10] обладает возможностями по накоплению данных, находит и отслеживет четкие взаимосвязи в собранной информации. Источниками служат практически любые утилиты, способные обрабатывать сетевую или системную информацию в режиме, приближенном к реальному времени. Сейчас список интегрированных с OSSIM инструментов довольно широк: Arpwatch, P0f, PADS, Nessus/OpenVAS, Ntop, Snort, tcptrack, tcpdump, Nmap, Spade, Nagios, Osiris, OCSInventory-NG, OSSEC, RRDTool.

Дополнительно возможен анализ данных, собираемых preludeIDS, NTsyslog, Snare, Cisco Secure IDS. Полученная информация может быть доставлена с помощью разных способов: протоколов Syslog, SNMP, OPSEC, а также сокетов, plain log и пр. В итоге и администратор может получить информацию о любом событии в сети, узле или устройстве.

Каждая отдельная система подвергается детальному анализу, для чего собирается информация о типичном ее использовании (например, средний трафик за день), активности пользователя (почта, ICQ, http, ftp и т.п.) и производится мониторинг сессии в реальном времени с возможностью отобразить характер активности машины в сети. Агенты OCSInventory-NG поставляют данные об установленном на каждом компьютере оборудовании и ПО. На основании данных мониторинга OSSIM следит за связями отдельных компьютеров и вычисляет составной риск. Для этого строятся графики постоянных TCP-сессий, изменяющихся UDP, TCP и ICMP-связей, что позволяет идентифицировать сетевые атаки, совершаемые одновременно на несколько компьютеров.

В результате OSSIM может работать как система предотвращения атак (IPS, Intrusion Prevention System), управляя поддерживаемыми сетевыми устройствами. При этом она основывается на коррелированных данных, собранных со всех источников. Естественным минусом такого подхода является необходимость установки агентов на системы, мониторинг которых ведется.

Типичная система на OSSIM состоит из следующих модулей: сервера, который производит управление корреляциями, нормализацию данных, оценку риска и приоритета событий и базы данных, которая обеспечивает занесение информации в реляционную базу данных и корреляцию данных (основные компоненты – MySQL, OSSIM, Snort/ACID и PhpGACL). Каждый из представленных компонентов OSSIM может быть установлен на отдельной системе, информация между ними в этом случае будет передаваться исключительно в зашифрованном виде (для этого используется SSL).

Реализовано три уровня доступа к настройкам и функциям – сетевой администратор, системный инженер и специалист защиты (CSO, Chief Security Officer).

Вообще в качестве системы для базирования OSSIM подойдет любая ОС, на которой могут быть запущены все или отдельные компоненты, но логичнее использовать предпочитаемый дистрибутив Linux. Проект для установки и использования OSSIM предлагает исходные тексты (архив и доступ к CVS) и установочный ISO-образ – AlienVault Open Source SIM Installer (32- и 64-битные версии размером ~600 Мб). Первый вариант подходит для случаев, когда нельзя предоставить под сервер OSSIM отдельный компьютер, установка осуществляется в рабочую систему.

Поскольку OSSIM собирает много различных данных, лучше для него выделить самостоятельную систему (разработчики рекомендуют именно этот вариант).

Несмотря на свою «бесплатность», OSSIM обладает достаточно богатым функционалом, для того чтобы использоваться в качестве полноценного средства мониторинга событий ИБ.

Панель управления визуально разбита на три области. Справа находится список функций OSSIM: Dashboards (выводятся риски, здесь видно появление новой ОС или сервиса), Incidents, Events (аномалии, события), Monitors (мониторинг сети и систем), Reports (отчеты по узлам, оборудованию, ПО, сети), Policy (настройка политик и действий, запуск программы или отправка e-mail), Correlation, Configuration, Tools (бэкап, ссылки для закачки клиентов, сканер сети).

Также OSSIM умеет самостоятельно выполнить поиск и сканирование имеющих в сети систем.

При необходимости данные о системах можно добавить вручную. Информация по сетям и хостам затем используется при настройке политик.

Отдельно хотелось бы отметить наличие достаточно подробной помощи по каждой из компонент OSSIM. В каждой вкладке доступен Help, где с иллюстрациями показано назначение основных настроек. Даже при базовом знании английского разобраться будет несложно.

SIGVI

Принцип работы этого продукта отличается от других описанных ранее SIEM-систем. По сути, SIGVI не является средством мониторинга событий в чистом виде и предназначен в большей степени для уведомления администраторов об угрозах.

SIGVI работает по следующему принципу: программа периодически загружает новые оповещения об уязвимостях (для этого используются стандарты CVE, CPE и CVSS протокола SCAP), а затем полученная информация в соответствии с настройками фильтров отправляется администратору. Источники, откуда берутся сообщения, настраиваются вручную. Чтобы не рассылать лишние данные, SIGVI должен знать об используемых сервисах. Это можно также настроить вручную или использовать инструмент NSDi (Network Services Discoverer), который автоматизирует процесс сбора данных. Для каждой уязвимости, затрагивающей одну из используемых на серверах программ, SIGVI создает сообщение тревоги (alert).

При создании тревоги принимаются во внимание фактор риска и свойства сервиса. Фактор риска рассчитывается на основании вектора CVSS. Вектор применяет классификацию по шкале критичности 0 – 10, определяющей степень риска (кстати, эти данные использует сканер Nessus и другие подобные решения). При этом учитываются доступ (локальный, удаленный), сложность атаки (квалификация атакующего, настройки систем и т.п.), аутентификация, наличие рабочего эксплоита, обновлений, закрывающих уязвимость и прочие параметры. А вот чтобы определить, в каких случаях оповещать администратора, используются фильтры. Например, их можно настроить так, что сообщение будет генерироваться только при наличии готового эксплоита. Все полученные предупреждения заносятся в базу данных и доступны в любое время. Реализован поиск по нескольким критериям и большое количество отчетов.

Подробнее о проекте SIGVI можно прочесть на сайте [11].

***

В этой статье я рассмотрел несколько решений, предназначенных для мониторинга событий ИБ. Как видите, решений много, как программных, так и аппаратных, как коммерческих, так и бесплатных. Так что администраторы смогут сами выбрать то, которое позволит им эффективно осуществлять мониторинг ИБ в корпоративной сети. EOF

1. Информация по ArcSight ESM – http://www.arcsight.com/products/products-esm.
2. ArcSight и NetFlow – http://netflowninjas.lancope.com/blog/2010/09/arcsight-adds-support-for-lancopes-flowsensor-appliance.html.
3. Информация по Symantec SIM – http://www.symantec.com/business/security-information-manager.
4. Информация по TSOM – http://www-01.ibm.com/software/tivoli/products/security-operations-mgr.
5. Информация по Cisco MARS – http://www.cisco.com/en/US/products/ps6241/tsd_products_support_series_home.html.
6. Информация по QRadar Log Manager Free Edition – http://q1labs.com/products/qradar-log-manager.aspx.
7. Страница, посвященная RSA enVision – http://www.rsa.com/node.aspx?id=3170.
8. Портал LogLogic – http://loglogic.com.
9. Яремчук С. Контролируем безопасность сети с помощью OSSIM. //«Системный администратор», № 5, 2005 г. – С. 78-85 (http://samag.ru/archive/article/482).
10. Информация по OSSIM – ossim.net.
11. Информация по SIGVI – http://sigvi.upcnet.es/index.php.

Рисунок 5. Консоль устройств ArcSight