# Безопасность корпоративных сетей: мониторинг, анализ, управление

***Обзор систем мониторинга, анализа и управления безопасностью корпоративных IT-инфраструктур, представленных на российском рынке.***

## *Введение*

*За последнее десятилетие в решении проблемы защиты доступа к ресурсам корпоративной сети можно отметить существенные изменения. Еще совсем недавно безопасность информационных систем можно было с высокой степенью надежности обеспечить при помощи таких традиционных защитных механизмов, как идентификация и аутентификация, разграничение доступа, шифрование и т.п. Однако с появлением и развитием открытых компьютерных сетей ситуация резко изменилась. Подключение корпоративной сети к интернету, построение распределенных сетей, появление огромного количества компьютерных вирусов способствовали активному внедрению технических средств для защиты периметра корпоративных информационных систем. Результаты последних исследований показывают, что сегодня подавляющее большинство компаний имеют такие системы: 90% компаний используют межсетевые экраны и антивирусные программы, а 40% – системы обнаружения вторжений (IDS).*

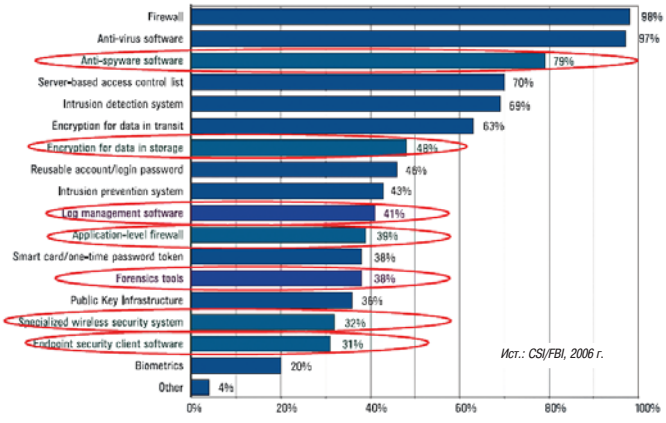



**Рис. 1.** Распределение трендов, волнующих пользователей по данным опроса CSI/FBI в 2006 г. *(красным отмечены новые тренды).*

*Однако сейчас средства безопасности устанавливаются повсеместно, реализуя уже стратегии защиты как от внешних нарушителей, так и от внутренних. Время, когда уровень безопасности измерялся количеством установленных систем безопасности, проходит. Например, согласно отчету CSI/FBI (рис. 1), появились новые тренды в обеспечении информационной безопасности (ИБ). Фирмы начали уделять серьезное внимание как системам журналирования событий безопасности и автоматизированных систем (Log management), так и системам, которые позволяют проводить анализ событий в "ретроспективном плане" (forensics), т.е. расследовать инциденты.*

*Сегодня, с точки зрения ИБ, уровень зрелости компании определяется уже не количеством установленных в ее сети устройств безопасности, а умением управлять тем огромным количеством сигналов и сообщений, которые они порождают.*

*В потоке информации, постоянно поступающей на экран консоли администратора безопасности, есть множество предупреждений и сообщений от установленных в сети средств защиты. Это и диагностика от систем сканирования периметра сети, и обнаруженные попытки подбора пароля на узлах, видимых из интернета, и выявленные атаки "червей", и злонамеренное использование уязвимостей web-сервера, и многое другое. Несколько сотен тысяч событий в день и больше – это, увы, реальность наших дней. А в крупных сетях ежедневная порция информации, которая "сваливается" на администратора, может превысить миллионы сообщений. Например, только один межсетевой экран может генерировать за день более 1 Гбайт данных в Log-файле, а один сенсор IDS за это же время может выдавать до 500 тыс. сообщений. Справиться с такими объемами информации не под силу ни одному человеку.*

*Ситуация осложняется еще и тем, что далеко не все сообщения, сгенерированные средствами защиты, соответствуют реальным атакам – у всех средств безопасности в той или иной степени случаются ложные срабатывания. Например, по статистике, число ложных срабатываний для сенсоров IDS может достигать 90%. Это приводит к тому, что администраторы безопасности часто вынуждены рассматривать только события высшего приоритета, оставляя практически все события, кроме наиболее критичных, незамеченными, и, таким образом, пропускать реальные атаки на информационную систему.*

*Наличие большого количества разных средств безопасности порождает большое количество журналов от разных систем, каждая из которых выдает события на своем языке и, кроме того, выдает много ненужной информации, а также иногда срабатывает на события не совсем адекватно.*

*В связи с этим, одной из актуальных задач представляется построение единой, централизованной системы мониторинга событий информационной безопасности.*

## Классификация и рынок систем мониторинга и управления событиями безопасности

Как показывает практика, эффективная система мониторинга и управления событиями безопасности должна объединять события, собираемые со всех используемых защитных средств, в единую

управляемую систему информационной безопасности, причем из огромного числа сообщений, генерируемых различными системами безопасности, оставлять только те, в которых может содержаться полезная информация. Основываясь на опыте, из миллиона генерируемых записей интерес для администратора безопасности представляют только сотни, если не десятки из них.

Одним их эффективных решений проблемы являются системы управления событиями информационной безопасности (Security Information Management), которые позволяют связать все используемые в сети защитные средства в единый управляемый комплекс.

Здесь эксперты разделяют системы на разные классы: работающие в реальном режиме времени или системы, осуществляющие журналирование всей информации и позволяющие в дальнейшем проводить "ретроспективный" анализ событий. Кроме того, делят системы на SIM- и SEM-решения.

*Security information management (SIM)* решение обеспечивает создание отчетов и анализ данных, большей частью, из серверных систем и приложений и, во вторую очередь, из систем безопасности для обеспечения анализа на соответствие системы заданной политике безопасности защите от внутренних угроз и осуществление анализа на соответствие различным законодательным актам и стандартам.

*Security event management (SEM)* решения улучшают возможности систем безопасности по реагированию на инциденты безопасности. SEM обрабатывают данные практически в реальном режиме времени, получаемые с систем защиты, сетевых устройств и систем для обеспечения управления событиями безопасности в целях обеспечения непрерывной эксплуатации информационной системы. SEM помогают IT персоналу более эффективно реагировать на внутренние и внешние угрозы.

По данным аналитических агентств, 70% покупателей требуют и SIM, и SEM. Соответственно, класс систем, объединяющий указанную функциональность, будем обозначать как SIEM (SIM + SEM).

Все методы обработки событий можно разбить на 5 групп, каждая из которых занимает свою нишу, с точки зрения числа обрабатываемых событий (рис. 2).

*Фильтрация событий* – устранение избыточной информации, основываясь на критериях, заданных администратором или определенных в системе.

*Нормализация событий* – данные от различных средств защиты приводятся к единому виду, единым показателям значимости события. Нормализация также подразумевает устранение избыточной информации.

*Агрегирование событий* – объединение однотипных событий в одно.

*Корреляция событий* – позволяет выявлять наличие комплексных атак, т.е. атак, которые не могут быть обнаружены одним устройством с использованием известных сигнатур IDS, так как фактически обрабатывают комплекс событий,

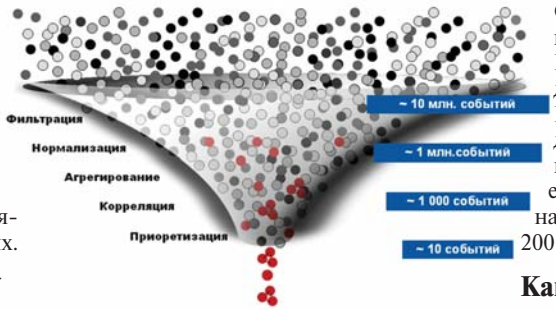



**Рис. 2.** Каждый из методов обработки событий занимает свою нишу, с точки зрения возможного числа обрабатываемых событий.

которые по отдельности не говорят о реальной атаке.

*Приоритезация событий* – автоматическое присвоение событиям соответствующего уровня, исходя из заданных администратором или определенных в системе критериев.

На сегодняшний момент рынок систем SIEM переваливает за несколько сотен миллионов долларов. На рынке присутствует несколько десятков компаний, наиболее известны следующие компании (средства): Arcsight (*Enterprise Security Manager)*; Network Intelligence *(enVision, куплена EMC)*; Novell *(Sentinel)*; Cisco *(MARS – Monitoring, Analysis and Response System)*; Symantec *(Security Information Manager)*; NetForensics *(nFX Open Security Platform)*; CA *(eTrust Security Command Center)*; Intellitactics *(Security Manager)*; ActiveWorx; IBM *(Tivoli Risk Manager, скорее всего, будет прекращена поддержка ввиду покупки NeuSecure)*; NetIQ *(Security Manager)*; LogLogic; Sensage; NeuSecure (куплена IBM); Checkpoint *(Eventia)*; LogLogic.

Все системы принадлежат к разным классам: если Cisco MARS – к системам SEM (в основном ранее нацеленной на SME-рынок), то LogLogic или Net IQ в большей степени – к системе управления Log-информацией, а, например, Arcsight – это одна из самых мощных систем SIEM, позволяющая работать компаниям самого большого размера и выполняющая огромное количество работы по управлению событиями безопасности.

Если посмотреть на несколько устаревшую, однако отражающую текущее состояние дел диаграмму, рынок выглядит следующим образом (рис. 3): впереди 5 наиболее сильных игроков, получивших наиболее большие доли рынка.

На российском рынке присутствует достаточно ограниченное количество систем SIEM: IBM Tivoli Risk manager, Computer Associates, Netforensics SIM (часто под маркой Cisco SIMS), Net IQ,

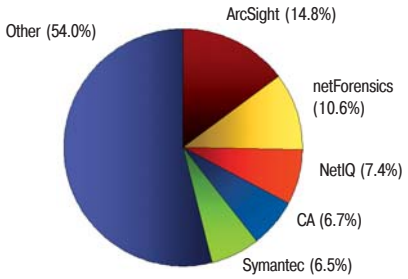



**Рис. 3.** Распределение общемирового рынка ($209,9 млрд) между основными производителями SIEM-систем, *по данным IDC, 2005 г.*

Cisco MARS, остальные игроки пока мало заметны на российском рынке. Например, сильно рекламируется недавно вышедшая система Checkpoint Eventia, однако ее функционал пока далек от лидеров (например, список поддерживаемых устройств у Eventia едва переваливает за десятку, против, например, Arcsight, у которого более 200 типов поддерживаемых устройств).

## Как строятся системы управления событиями безопасности?

Типичное построение – трехуровневая архитектура – *агенты*, собирающие данные с устройств, *engine*, обрабатывающий информацию, и *база данных*, куда информация складывается, а также *управляющий интерфейс*. Отдельные системы, например, Cisco MARS, выпускаются в виде аппаратных устройств и собирают всю информацию непосредственно в аппаратно-программный комплекс, что может оказаться недостаточно гибкой системой при сложной сетевой инфраструктуре, поскольку при большом разветвлении приходится ставить такие устройства в каждом сегменте, что часто усложняет применение системы в целом.

Рассмотрим наиболее известные системы:

*1. eTrust Security Command Center (SCC)*

eTrust SCC – программно-аппаратное решение, состоящее из двух основных подсистем:

- CleverPath Portal – веб-портал и система генерации отчетов;
- eTrust Audit – сбор и анализ логов.

Процедуру сбора и обработки логов в eTrust SCC можно разделить на несколько этапов. На первом этапе коллекторы eTrust Audit собирают логи различных систем и преобразовывают их к единому формату. После того, как коллекторы обработали первичные данные, они поступают на другой компонент eTrust Audit, называемый маршрутизатором. В его задачу входит обработка сообщений, согласно заданным правилам, и их последующая маршрутизация в единую базу eTrust SCC. Правила, по которым маршрутизатор обрабатывает сообщения, задаются централизованно через единую консоль eTrust Audit и распространяются на выбранные маршрутизаторы автоматически. eTrust Audit на основании поступивших к нему событий может выполнять различные управляющие команды. По аналитическим отчетам компании Gartner, eTrust SCC является одним из лидеров рынка наряду с Arcsight.

*2. NetForensics*

Система управления информационной безопасностью NetForensics предназначена для работы с гетерогенной средой продуктов обеспечения информационной безопасности и реализует непрерывный сбор, обработку и отображение событий безопасности. Система работает под управлением ОС Windows, Linux или Solaris, используя в качестве хранилища данных полнофункциональную СУБД Oracle 9. Система имеет широкие возможности работы в распределенном ре-

жиме, поддержку различных отказоустойчивых конфигураций и реализована на базе технологии Java по модульному принципу.

Алгоритм работы системы NetForensics чем-то похож на алгоритм, используемый, например, в Tivoli, но дополнен рядом полезных функционалов. Агенты собирают данные с устройств и пересылают их компоненту nF Engine, который фильтрует их в соответствии с заданными правилами, приводит их к единому виду и пересылает их компоненту nF Master, который выполняет корреляцию, агрегацию и приоритезацию данных, и после этого в режиме реального времени выводит их на консоль администратора безопасности. В отличие от системы Tivoli Risk Manager, а также от eTrust SCC, система NetForensics обладает несколькими полезными подсистемами. Система Rule Based Correlation предоставляет дополнительные возможности корреляции данных. С помощью удобного механизма пользователь может создавать собственные правила корреляции и редактировать существующие.

Модуль Incident Resolution Manager помогает при расследовании, систематизации и документировании произошедших инцидентов.

*3. IBM Tivoli Risk Manager*

Это программное решение является открытым, межплатформенным приложением, построенным на базе стандартных решений по управлению безопасностью предприятия, и базируется на продукте Tivoli Enterprise Console. IBM Tivoli Risk Manager позволяет решать проблемы, связанные с нарушением системы безопасности и выявлением уязвимых мест с помощью единой консоли безопасности. Решение уделяет первостепенное внимание событиям, связанным с безопасностью приложений, операционных систем и сетевых устройств, обеспечивая всестороннее представление об архитектуре системы безопасности. Используя возможности формирования отчетов, администраторы могут выявлять уязвимые места в системе безопасности и предпринимать корректирующие меры.

В целом, алгоритм работы системы заключается в следующем: агенты собирают данные с подвергаемых мониторингу устройств и пересылают их на Tivoli Risk Manager Event Server. Данные подвергаются фильтрации, приводятся к единому виду. Далее происходит объединение однотипных событий, корреляция данных и присвоение им определенного веса. “Очищенные от мусора” данные пересылаются в режиме реального времени на консоль администратора безопасности, а также помещаются в базу данных, что дает возможность в последствии создавать аналитические отчеты, необходимые для более четкого понимания уровня информационной безопасности в компании.

*4. ArcSight*

Пока эта система управления информационной безопасностью и рисками не очень известна на российском рынке, но она занимает ведущие позиции в мире (по аналитическим данным, ~ 50% всех проектов по построению систем мониторинга сетевой активности в Европе, выполнены с использованием продуктов ArcSight). На сегодняшний день она обладает наиболее мощными механизмами, позволяющими централизованно управлять рисками и реагировать на различные угрозы и попытки несанкционированного проникновения в информационную систему предприятия.

Архитектура решения позволяет создавать распределенные структуры и регулировать отношения между подсистемами, как на уровне каналов связи, так и по составу модулей и поддерживаемых систем.

Кроме того, на мой взгляд, наиболее простой в управлении и реализующий максимальное количество полезных функций интерфейс представлен в системе ArcSight. Консоль администратора реализована не только в виде web-приложения, но и в виде отдельного приложения.

## Выбор решения

При выборе решения всегда существует проблема, что выбрать и какими должны быть критерии. При выборе данного решения необходимо помнить как о возможностях системы, которые в период маркетинговых войн становятся часто “дутыми”, так и о необходимом функционале и эксплуатационных характеристиках.

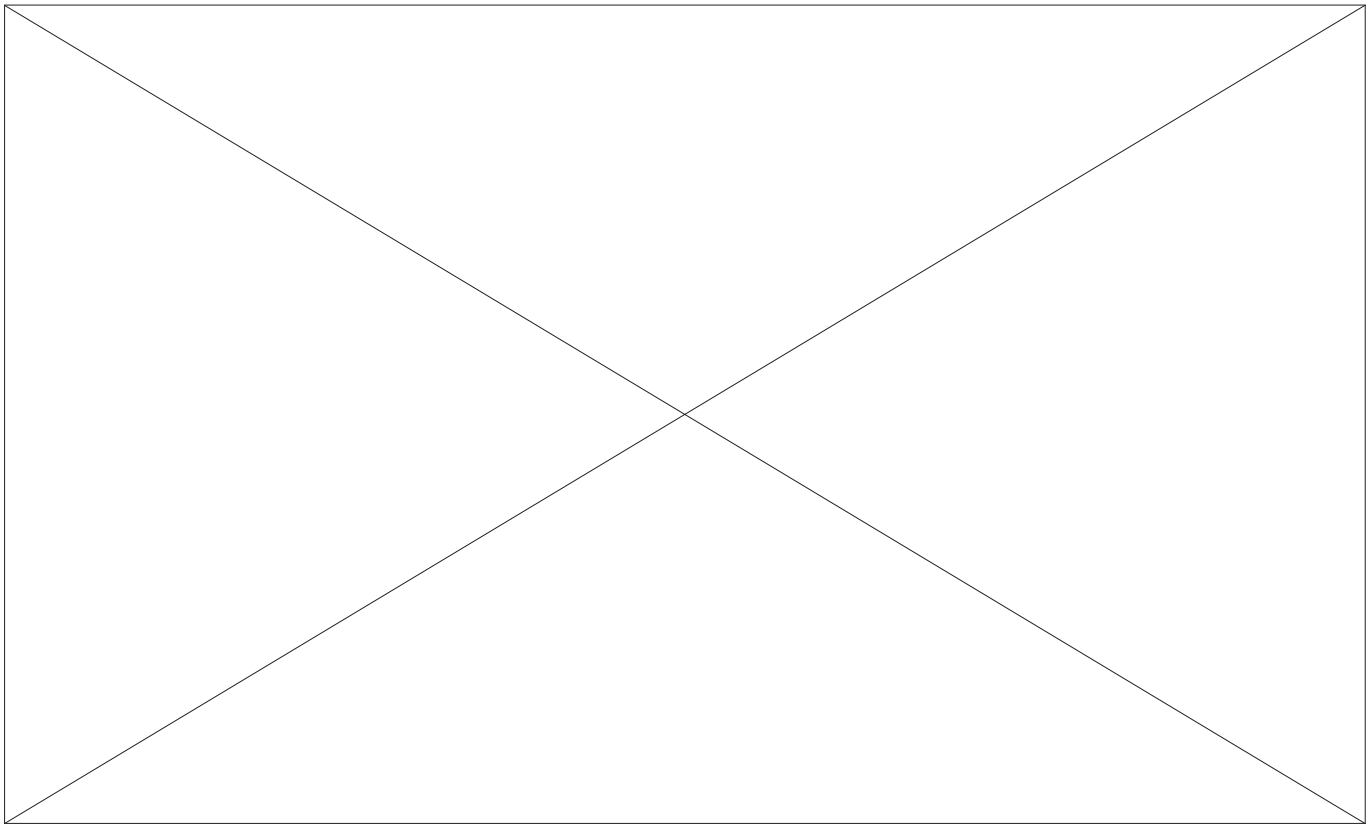
*1. Получение на консоль только значимых событий.* При этом необходимо понимать, как эта информация будет представлена: только в виде скоррелированных событий или же с возможностью получения в дальнейшем всей информации о том, как все было.

*2. Наличие централизованного хранилища данных от всех систем.* Самое неудобное это большая база данных, с которой непросто обращаться, соответственно, работа с базой событий должна быть по возможности простой.

*3. Возможность ранжирования угроз, основанного на серьезности ущерба,* что позволяет администратору сфокусировать внимание на реальных угрозах, исключая ложные, поэтому система должна учитывать анализ рисков, проведенный в компании, и получать информацию от систем анализа безопасности;

*4. Система должна быть масштабируемой и при необходимости распределенной* – не каждый вендор может предоставить действительно масштабируемую систему.

*5. Необходимость мониторинга на уровне приложений (например, SAP и т.п.)* – во-



просы работы с приложениями являются одними из самых трудных в таких системах.

*6. Наличие решений по мониторингу инсайдерской активности* – должны поддерживаться системы анализа контента, а также специфические функции отдельных приложений.

*7. Решение должно иметь возможность анализировать поддерживаемый уровень безопасности, сравнивать его с нормативными требованиями законодательства или отраслевыми и международными нормами (ISO 27001 и др.)*

Первое, что надо отметить при сравнении данных продуктов, это то, что при их общей схожести, цели, возложенные на них, все-таки отличаются друг от друга. Схожесть заключается в том, что все эти системы собирают и обрабатывают некоторым образом события с различных устройств, обеспечивая унифицированное управление защитой периметра и внутренней безопасностью сети. Это позволяет администраторам единообразно задавать и контролировать выполнение правил безопасности при меньших затратах на управление. С другой стороны, принципы обнаружения и управления событиями безопасности совершенно разные – соответственно, отличаются и результаты.

Главное отличие заключается в том, что системы Arcsite, NetForensics и Tivoli Risk Manager в основном предназначены для того, чтобы из тысяч событий безопасности выделить единицы действительно важных событий и тем самым привлечь внимание администратора к тем событиям, на которые необходимо реагировать.

Основной задачей eTrust SCC является обработка сообщений, согласно заданным правилам, и последующее выполнение различных управляющих действий, таких как: отправка почты, блокировка учетной записи пользователя, закрытие на активном сетевом оборудовании определенного IP-адреса и т.п. Другими словами, это расширенная SEM-система, обладающая возможностью обрабатывать и хранить события и проводить анализ с использованием дополнительного ПО Network Forensics, но предоставляющая широкие возможности по работе в реальном режиме времени и способностью немедленного реагирования на события безопасности. Система же Netforensics это SIM-система, которая позволяет выявлять нарушителей, но не обладающая ответной реакцией на события безопасности – считается, что решения должен принимать человек.

Arcsight как представитель SIEM позволяет как в реальном режиме времени, так и в режиме forensics анализировать события безопасности и реагировать на ситуации и инциденты, а кроме того, подключать модули анализа соответствия различными событиям, политикам безопасности и др.

Рассмотрим типичную функциональность таких систем.

### *1) Корреляция событий*

Подход, реализуемый в системе Tivoli, существенно отличается от подхода, реализуемого в системе NetForensics и

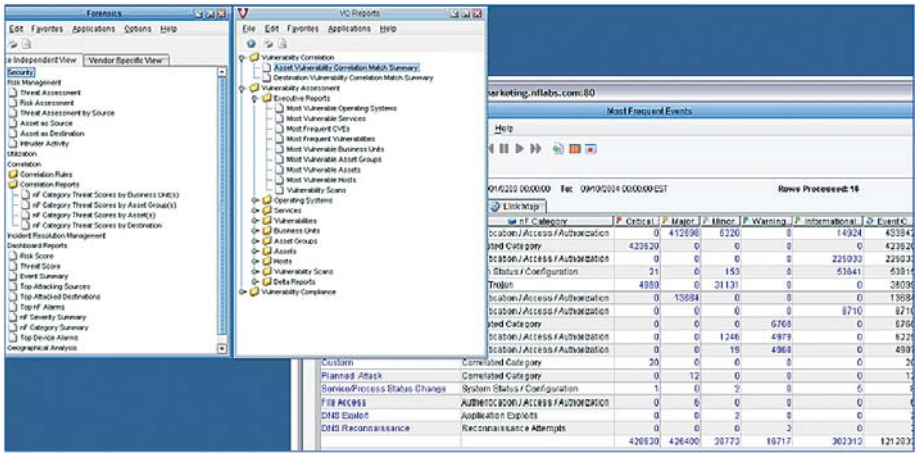


**Рис. 4.** Пример отчета системы NetForensics с визуализацией только событий от определенного уровня критичности или событий от определенных агентов.

ArcSight. Если в Tivoli для корреляции используется алгоритм, выявляющий совокупность связанных между собою событий, то в NetForensics используется алгоритм выявления последовательности определенных событий. То есть, если системой зафиксированы в течение определенного времени несколько событий, описанных в правилах корреляции, то NetForensics и ArcSight скоррелирует их только в том случае, если порядок их возникновения соответствует порядку, описанному в правилах. Система Tivoli скоррелирует эти события в независимости от последовательности их возникновения, понятно, что при определенных условиях это приведет к ложным срабатываниям.

Каждая из систем предоставляет несколько предопределенных правил корреляции, но в Tivoli создание новых правил выполняется вручную, путем редактирования XML-файлов, что представляет довольно-таки трудоемкую задачу. Система NetForensics предоставляет для этих целей достаточно удобный графический интерфейс. При этом, например, в Netforensics достаточно мало предустановленных правил корреляции (порядка 30), в Arcsight их более 250 уже предустановленно, причем, разных – как общего плана, так и спроектированных для конкретного типа атак.

### *2) Агрегация событий*

В Tivoli правила агрегации определены только для Cisco PIX, Cisco IDS и CheckPoint. Правила агрегации для остальных агентов пишутся вручную на XML. Системы ArcSight и NetForensics предоставляют готовые правила для всех поддерживаемых агентов. В eTrust SCC агрегация предусмотрена для ряда поддерживаемых продуктов и для не поддерживаемых в данный момент, используется специальный коллектор, где правила прописываются вручную.

### *3) Хранилище информации*

В NetForensics в качестве хранилища информации используется база данных Oracle. Система ArcSight, кроме Oracle, позволяет использовать в качестве хранилища DB2, а Tivoli в дополнение к этому – еще Sybase и Microsoft SQL Server. В Tivoli все работы связанные с обслуживанием базы данных (архивирование, удаление устаревших записей и т.д.), выполняются в ручном режиме, к тому же, в Tivoli используется несколько баз данных, что требует дополнительных расходов на их обслуживание. Системы NetForensics и ArcSight представляют механизмы, позволяющие автоматизировать обслуживание базы данных. E-trust обладает встроенной базой данных.

### *4) Отчеты*

В данном компоненте Tivoli также существенно уступает двум другим продуктам. В Tivoli отсутствует возможность создания отчетов по расписанию, имеется меньшее количество предопределенных шаблонов (около двух десятков), которые не настраиваются.

Система NetForensics предоставляет порядка 250 предопределенных отчетов с возможностью настройки определенных параметров, например выводить в отчет только события от определенного уровня критичности или – только события от определенных агентов (рис. 4).

Количество предопределенных отчетов в системе ArcSight более 300, но в отли-

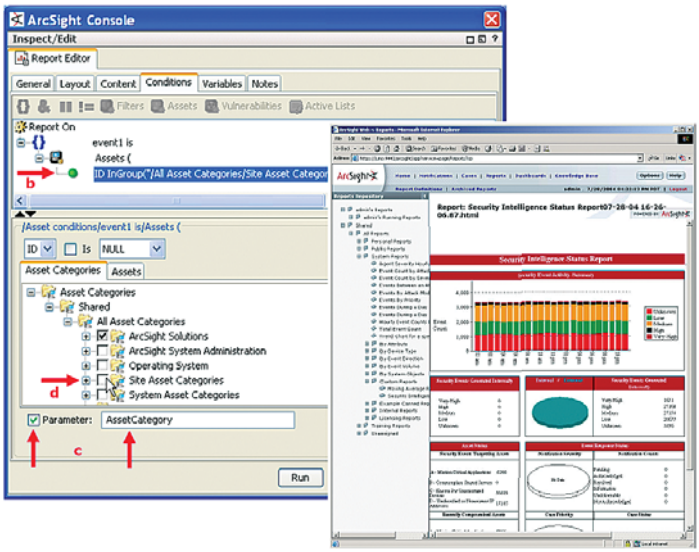



**Рис. 5.** Пример отчета – Top Vulnerable Systems – в ArcSight, привязанного к стандартам: ISO 17799 секция 5.2.1, NIST 800-53 секция RA-5 и др.

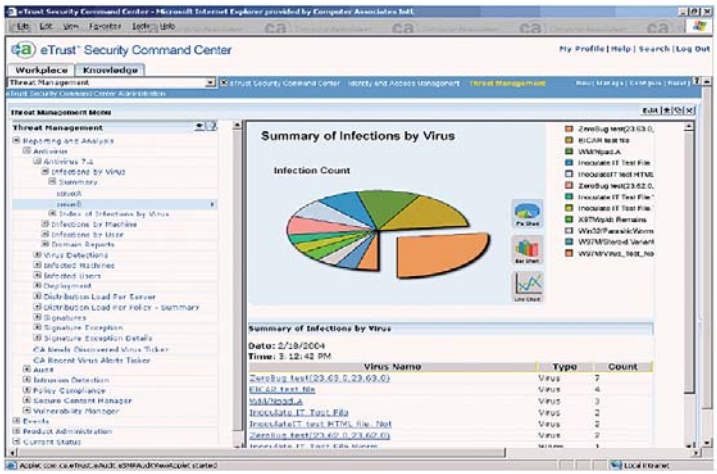



**Рис. 6.** Пример отчета eTrust Security Command Center.

чие от ранее рассмотренных систем, предоставляется удобный инструмент для создания отчетов по любым критериям, определенным пользователем (рис. 5). Предопределенные отчеты в ArcSight привязаны к определенным стандартам, например отчет Top Vulnerable Systems к ISO 17799 (секция 5.2.1), NIST 800-53 (секция RA-5) и др.

В eTrust Security Command Center существует более 200 предустановленных отчетов, которые могут быть как высокого уровня, так и уровня инженерного состава (рис. 6).

***5) Оповещение администратора о критичных событиях***

Единственная возможность оповещения администратора в Tivoli – отправить заранее сконфигурированное электронное сообщение.

NetForensics и ArcSight и eTrust SCC поддерживают несколько механизмов оповещения администратора в экстренных случаях: e-mail, SNMP и др. Существует возможность создания собственных механизмов оповещения.

***6) Совместная работа со сканерами***

Эта функциональность поддерживается в системах ArcSight и NetForensics, а также в новой версии MARS. К eTrust SCC имеется дополнительная подсистема анализа уязвимостей, которая используется в комплексе для анализа уязвимостей. Формат работы со сканерами у всех систем разный – если, например, Netforensics требует четкой привязки, поддерживаемой IPS с конкретным поддерживаемым сканером по сигнатурам, то в Arcsight возможны корреляции с приложениями и др.

***7) Поддерживаемые технологии и продукты***

Одним из немаловажных моментов использования системы мониторинга и управления является поддерживаемое оборудование, поскольку система, которая понимает только половину оборудования, это пустая трата средств и времени. Здесь важно понимать, насколько вендор готов поддержать оборудование, которое стоит в сети. Разработка агента под новые технологии может вестись годами.

Таким образом, у Tivoli с поддерживаемыми продуктами не все хорошо, мне удалось найти агенты только для самых популярных продуктов, а их не более 30. А остальное можно только подключить, используя библиотеки разработчика. eTrust SCC позволяет подключать достаточно большой спектр оборудования порядка 80 типов, Netforensics – 90 типов, Arcsight – более 200 типов оборудования и, что наиболее интересно – большое количество приложений (например SAP R/3).

## *Выводы*

*В настоящее время появились достаточно надежные и мощные системы управления безопасностью. Однако это не упрощает, а усложняет выбор решения.*

*Часто эксплуатационные характеристики имеют решающее значение. Например, несмотря на несомненные достоинства NetForensics, инсталляция и настройка этой системы представляют определенные трудности. Если есть грамотный Unix-администратор, то они не страшны, в противном случае – следует присмотреться к другим продуктам. К сожалению, в системе NetForensics, как впрочем, и в Tivoli, отсутствуют полноценные механизмы контроля работы и диагностики агентов, что при установке системы в распределенном режиме также может создать трудности.*

*К несомненным плюсам систем NetForensics и ArcSight можно отнести механизм анализа ценностей ресурсов (Assets). Данный механизм позволяет присвоить каждому узлу сети определенные значения ценности, на основе которых при попытках вторжения можно присваивать событиям определенный уровень критичности. В системе ArcSight существует механизм автоматической настройки данного функционала с привязкой к стандартам ISO 17799 и NIST 800-53.*

*В результате, если вы хотите построить SOC, который будет анализировать и выполнять автоматические действия по блокировке и др., то следует поближе ознакомиться с продуктом eTrust SCC. Если вы собираетесь выполнять все действия сами, и мгновенная автоматическая реакция на нарушения не нужна, но требуется детально разбираться, что же произошло в результате инцидента, вам поможет Netforensics.*

*А если необходимо создать мощную систему безопасности, выполняющую не только функции мониторинга и управления безопасностью, проводить анализ в соответствии с политикой безопасности, международными нормами и др., ваш выбор – Arcsight.*

***Михаил Романов,***
*начальник отдела информационной безопасности и планирования непрерывности бизнеса, компания "ТехноСерв А/С"*

# Теперь не страшно терять ноутбук

***Март 2007 г.*** – Компания Seagate Technology объявила о начале поставок жестких дисков Momentus® 5400 FDE.2 (Full Disk Encryption – полное аппаратное шифрование данных) компании ASI Computer Technologies для производства ноутбуков с высоким уровнем безопасности, которые также будут оснащены ПО для управления безопасностью информации от корпорации Wave Systems Corp.

Согласно недавнему отчету Института Понемона, 35% всех случаев потери компьютерных данных было связано с потерей ноутбуков и других портативных устройств. По данным опроса того же института за 2005 г., основными причинами, в силу которых организации отказываются от шифрования конфиденциальной информации, являются боязнь потери производительности жесткого диска (69% опрошенных), сложность (44%) и затратность (25%) подобных внедрений.

Seagate Momentus® 5400 FDE.2 – это 2,5" SATA-диск с использованием технологии перпендикулярной записи имеет объем 160 Гбайт, а также шифрование данных на основе протокола AES, который позволяет автоматически шифровать полностью все данные, записанные на диск (а не только к отдельным файлам и партициям), предотвращая неавторизованный доступ к информации в случае потери или кражи ноутбука.

Компания ASI Computer Technologies будет инсталлировать Momentus 5400 FDE.2 в ноутбуки серии ASI C8015, получившие название "вайт-бук" (whitebook system). Для обеспечения дополнительной безопасности данных и для более надежной аутентификации пользователя на ноутбуках ASI C8015, которые появятся уже в апреле с.г., будет установлен биометрический считыватель опечатка пальца. В ноутбуке ASI C8015 будет использоваться программный пакет от Wave Systems, призванный упростить установку и конфигурацию диска Momentus 5400 FDE.2. Drive Manager из пакета Wave Systems Embassy Security Center также упростит для администраторов и пользователей процесс создания и хранения паролей, а для администраторов – процесс установки и контроля политик безопасности диска. Технология DriveTrust от Seagate также дает возможность быстро и легко стирать данные с диска. Новая платформа Seagate DriveTrust Technology объединяет мощную, полностью автоматизированную интегрированную аппаратную безопасность с программной платформой, которая позволяет легко добавлять программные компоненты для управления ключами шифрования в масштабах всей организации, обеспечения многоуровневой аутентификации пользователей, а также другие функции, которые делают недоступными данные, находящиеся на хранении.