Центры Оперативного Управления Информационной Безопасностью

В конце 2011 г. корпорация EMC анонсировала инициативу – Advanced Security Operations, цель которой – объединить различные инструменты, а также методы контроля и управления информационными рисками, и создать возможность организации Центров Оперативного Управления Информационной Безопасностью. Публикация – обзор того, что сделано EMC для реализации этой инициативы за прошедший год.

Александр Чигвинцев – руководитель подразделения EMC RSA в регионе Россия и СНГ.

Введение

Работа по обеспечению безопасности как в крупной компании с выделенным персоналом и ресурсами, так и в небольшой организации, состоит в поддержании безопасности информационных активов на требуемом уровне посредством непрерывного наблюдения за вычислительной средой компании, предупреждения и оперативного устранения выявленных угроз и уязвимостей. Один из вариантов формализованного подхода к данной задаче сводится к созданию Центра Оперативного Управления Информационной Безопасностью (ЦОУ ИБ), или SOC (Security Operation Center). Это может быть как централизованная, так и распределенная служба, в идеале обеспечивающая выявление, контроль и устранение всех инцидентов информационной безопасности.

К сожалению, достаточно большое число специалистов по ИБ почерпнули представления о SOC из голливудских, да и отечественных блокбастеров: полутемная комната; стена с огромными экранами, на которых высвечиваются постоянно меняющиеся графики, диаграммы и таблицы; ряды сотрудников отдела ИБ, что-то пристально рассматривающих на своих индивидуальных мониторах...

Сразу следует заметить, что SOC – это не только настенные мониторы и красочные диаграммы. Это, прежде всего, хорошо разработанная, и ***формализованная политика информационной безопасности****. Наибольший эффект от внедрения данного сервиса можно получить только после классификации информации, циркулирующей внутри организации, выявления потенциальных угроз, разработки стандартных процедур реагирования на те или иные инциденты, распределения ролей и обязанностей, составления четких должностных инструкций сотрудникам отдела ИБ и дежурной смены SOC.*

Кроме того, SOC в его классическом виде (здесь правильнее использовать термин SIEM – Security Information and Event Management Solution) уже не является адекватным ответом на современные риски и угрозы информационной безопасности. Именно поэтому компания RSA (в настоящее время это подразделение информационной безопасности корпорации EMC) в конце прошлого года анонсировала инициативу – Advanced Security Operations (http://www.rsa.com/node.aspx?id=3686). Одна из основных идей, лежащих в основе данной стратегии, является идея объединения различных инструментов и методов контроля и управления информационными рисками, благодаря чему достигаются кардинальное расширение номенклатуры контролируемых параметров и возможность анализа не только событий информационной безопасности. В частности, в предложении RSA – технологии Archer, enVision (SIEM), NetWitness интегрируется с системой RSA DLP (Data Loss Prevention – система предотвращения утечки конфиденциальной информации), технологиями борьбы с on-line мошенничеством (RSA FraudAction, RSA eFraudNetwork), системами контроля и управления IT-инфраструктурой и приложениями – EMC Ionix.

При этом платформа Archer позиционируется на вершине "стека" продуктов и решений по управлению информационной безопасностью предприятия. Это связано с тем, что именно этот продукт, с одной стороны, обеспечивает разработку политик по соблюдению режима ИБ, а с другой – предоставляет возможности по эффективному и объективному контролю над выполнением этих политик в организации. Еще одна возможность платформы Archer, связанная с управлением инцидентами и "корреляцией" их с информационными активами, бизнес-процессами и оценкой рисков, позволяют предприятию приоритезировать расследование и обработку таких событий, и направлять имеющиеся (как правило, ограниченные ресурсы) на решение самых опасных, с точки зрения бизнеса, проблем. Как классические (DLP, SIEM), так и новые (NetWitness\SecurityAnalytics) технологии RSA уже интегрированы с Archer, что дает возможность продуктам RSA обмениваться необходимой информацией в реальном масштабе времени.

Технологическая основа взаимодействия продуктов – "RSA Connector Framework". Данная служба обеспечивает унифицированные базовые интерфейсы для обмена данными и командами между решениями RSA по управлению Информационной Безопасностью.

Сейчас RSA предлагает следующие варианты интеграций:

- *AssetCriticalityIntelligence;*
- *RSA Solution for Security Incident Management;*
- *DLP Risk Remediation Manager;*
- *RSA DLP Policy Workflow Manager.*

В ближайшее время предполагается существенно расширить номенклатуру решений, что позволит строить гибкие, подстраиваемые под конкретную инфраструктуру/ модель рисков и т.д. корпоративные системы управления Информационной Безопасностью.

Компоненты интеграции и анализа для создания ЦОУ ИБ

Asset Criticality Intelligence (ACI)

Одной из сложных задач, стоящих перед службой ИБ предприятия, является проблема определения опасности инцидента, исходя из возможного негативного влияния на текущие бизнес-процессы.

В качестве возможного варианта решения данной задачи RSA предлагает интеграцию платформы Archer с системой мониторинга и контроля сетевой активности RSA NetWitness.

Archer в данном контексте выступает как корпоративное, централизованное хранилище данных всех Информационных Активов предприятия и их роли в текущем бизнес-процессе.

Search Results

Drag a column name here to group the items by the values within that column

Device Name	Internal IP Address	Type	Criticality Rating	Business Unit	Facility
Client PC6	192.168.2.103	Database Server		AM Strikers	Thunder Ann Arbor
box1		Application Server		SMC SOL	
Client PC1	192.168.2.103	Desktop		Engineering	
Client PC10	192.168.2.104	File Server		CJ Thunder	Magic Columbus
Client PC11	192.168.2.101	Infrastructure Server		AM Strikers	Eagles Manchester
Client PC2	192.168.2.101	Desktop		CJ Thunder	Eagles Manchester
Client PC3	192.168.2.103	Desktop		CJ Thunder	Thunder Ann Arbor
Client PC4	192.168.2.100	Desktop		AM Strikers	Strikers Boston
Client PC5	192.168.2.104	Desktop		BG Magic	Magic Columbus
Client PC7	192.168.2.103	Database Server		AM Strikers	Thunder Ann Arbor
Client PC8	192.168.2.103	Database Server		AM Strikers	Thunder Ann Arbor
Client PC9	192.168.2.104	File Server		EC Eagles	Magic Columbus
Device2	1.1.1.1	File Server		Kiosk Centre1	

Рис. 1. Отчет с оценкой критичности устройств с привязкой к бизнес-юниту, компоненте ИТ-инфраструктуры и IP-адресу.

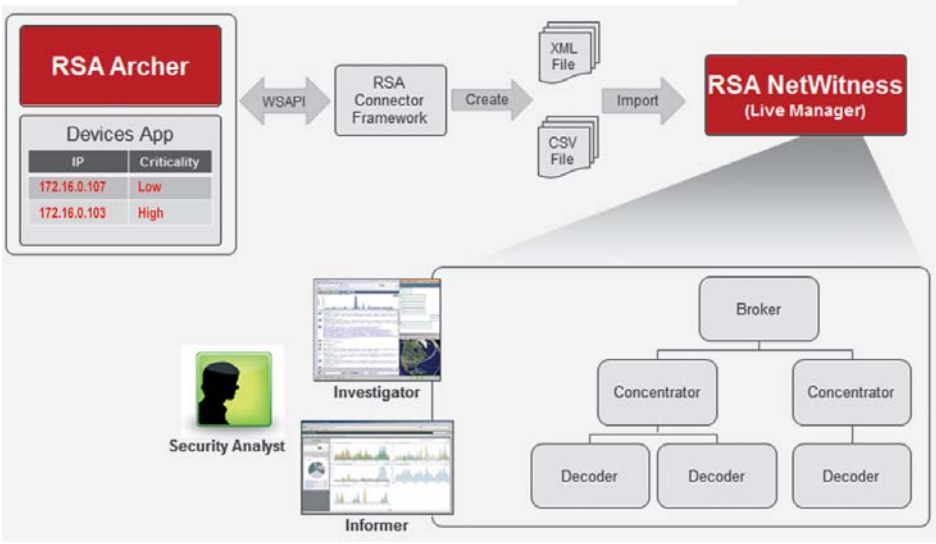

Рис. 2. Результатом работы ACI-интеграции является упрощение написания правил фильтрации, корреляции инцидентов, рассылки оповещений (Alerts), т.к. все необходимые данные становятся видны в стандартном интерфейсе NetWitness

Archer device application

Archer device application позволяет создавать отчеты по устройствам, помечая при этом каждое из них рейтингом критичности (рис. 1). Далее данная информация периодически передается в NetWitness и используется для приоритезации и оценки рисков выявленных сетевых аномалий.

Результатом работы ACI-интеграции является упрощение написания правил фильтрации, корреляции инцидентов, рассылки оповещений (Alerts), т.к. все необходимые данные становятся видны в стандартном интерфейсе NetWitness (рис. 2). Это, в свою очередь, позволяет резко сократить время для анализа возможных последствий тех или иных событий в инфраструктуре и более адекватно реагировать на угрозы ИБ.

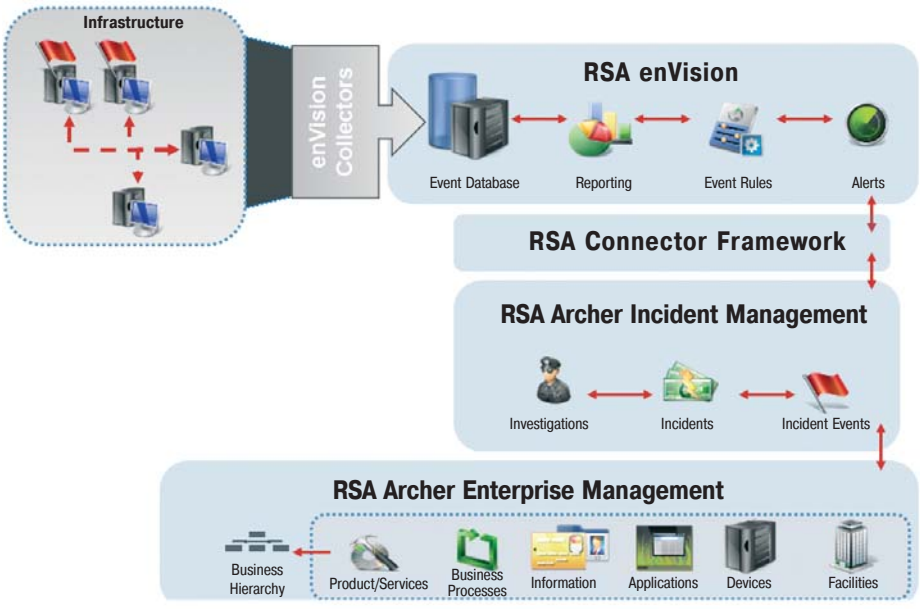

Рис. 3. RSA SSIM является одним из ключевых в цепочке решений по управлению инцидентами безопасности.

RSA Solution for Security Incident Management (RSA SSIM)

RSA SSIM является одним из ключевых в цепочке решений по управлению инцидентами безопасности (рис. 3).

После того, как идентифицированы критически важные события, указывающие на потенциальное нарушение безопасности, enVision собирает их с целью приоритизации и выдачи сообщений. RSA Connector Framework автоматически создает Инцидент в RSA Archer Incident Management, связывая с Инцидентом ассоциированные данные. Далее, администраторы безопасности, используя возможности RSA Archer Incident Management и информацию, получаемую от RSA Archer Enterprise Management, оценивают ситуацию, запускают процедуры расследования и решения инцидента.

По информации от службы EMC CIRC, им удается экономить до 1500 чел./час. ежемесячно благодаря такой интеграции систем при расследовании инцидентов.

RSA SSIM позволяет все обнаруженные "целевыми" системами инциденты ИБ передавать в реальном масштабе времени в приложение RSA Archer. Archer содержит данные о всех информационных активах предприятия, методиках оценки рисков, утвержденных процедурах обработки инцидентов и т.д. Это позволяет автоматически оценивать возможные последствия инцидента для бизнеса, а наличие дополнительной информации (владелец вовлеченного в инцидент актива, важность актива, заранее разработанные процессы обработки инцидента и т.д.) обеспечивают резкое сокращение времени между обнаружением инцидента и его обработкой.

DLP Risk Remediation Manager (RRM)

Решение RRM также использует данные об информационных активах предприятия и его организационной структуре для выявления владельцев информации (тех сотрудников организации, кто наиболее часто обращается к тем или иным файловым ресурсам). Далее, эта информация используется в стандартном бизнес-процессе, позволяющем ограничивать и контролировать доступ к конфиденциальным данным только тем сотрудникам, которые действительно в ней нуждаются по роду их деятельности в данной организации (рис. 4).

На первом этапе служба ИБ предприятия совместно с "владельцами" конфиденциальных данных разрабатывает формальные критерии, характеризующие определенный тип контролируемой информации. Эти критерии переводятся в описание политик DLP. Модуль RSA DLP Datacenter, используя данные политики, выполняет сканирование файловых ресурсов предприятия и выявляет файлы с конфиденциальной информацией, местоположение или профиль доступа к которым не соответствуют принятым в организации политикам ИБ. Далее, используя продукты и решения по мониторингу частоты обращения пользователей

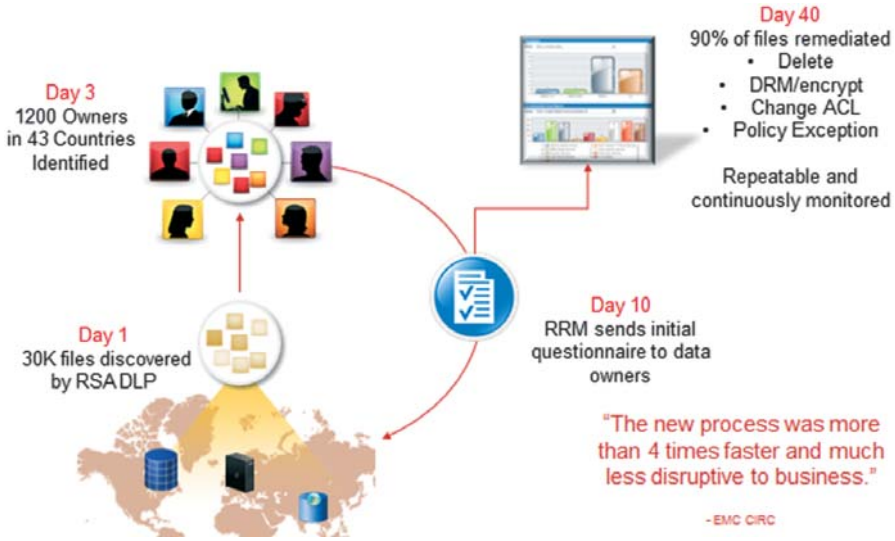

Рис. 4. Этапность приведения файловых активов предприятия в соответствие с политиками ИБ (и дальнейшего контроля их соблюдения) с помощью DLP Risk Remediation Manager.

к тем или иным файловым ресурсам (например, Varonis, Imperva и т.д.) выявляются фактические владельцы и пользователи информации. Затем полученные данные передаются в Archer, где специально разработанное приложение автоматически генерирует инцидент ИБ, опрашивает выявленных владельцев информации и предлагает им привести профиль использования конфиденциальных данных в соответствие с политикой ИБ предприятия. Описанная процедура проводится периодически в автоматизированном режиме и позволяет в непрерывном режиме контролировать соблюдения сотрудниками организации политик работы с конфиденциальными данными.

RSA DLP Policy Workflow Manager (PWM)

Решение PWM позволяет выстроить бизнес-процесс по предоставлению доступа сотрудников предприятия к конфиденциальным данным. Данное решение также поддерживает механизм (процедуру) исключений. Это позволяет автоматически документировать и отслеживать доступ к конфиденциальным данным предприятия (рис. 5).

Согласно предлагаемой методике, сотрудники бизнес-подразделений (фактически владельцы информации) используя специальное приложение в Archer, определяют, регистрируют и визируют в соответствии с принятым бизнес-процессом правила доступа к определенным конфиденциальным данным на основе действующей в организации политики ИБ. Данное приложение также позволяет определять и регистрировать исключения из принятых правил доступа к информации для конкретных сотрудников организации. На базе утвержденной схемы доступа и работы с информацией в дальнейшем специалисты отдела ИБ разрабатывают политики DLP, которые будут автоматически контролировать соблюдение сотрудниками предприятия утвержденных правил работы с конфиденциальными данными.

Заключение

К настоящему времени практически ни у кого не вызывает сомнение тот факт, что информация является самым ценным активом любого предприятия или организации. Потеря конфиденциальных данных влечет за собой как репутационные, так и финансовые издержки, а иногда может поставить коммерческую организацию даже на грань закрытия бизнеса. С другой стороны, за последнее время резко увеличилось количество хорошо подготовленных и технологически сложных кибер-атак на самые различные активы.

В связи с этим огромное значение для выживания предприятия получила задача по созданию или реорганизации службы ИБ для оперативного и эффективного противодействия современным методам обхода классических средств защиты информационных ресурсов.

Компания RSA предоставляет целый спектр продуктов и решений для построения современной эшелонированной системы ИБ предприятия. Следует отдельно отметить, что все эти решения широко используются для защиты внутренней инфраструктуры EMC (RSA – подразделение внутри корпорации EMC). Таким образом, компания фактически предоставляет уже апробированные продукты, которые хорошо зарекомендовали себя для решения актуальных задач ИБ в крупной организации.

Эксплуатация всех описанных в данной статье систем как в EMC, так и у большого числа заказчиков, продемонстрировала существенное снижение как числа инцидентов ИБ, так и времени, необходимого для расследования этих инцидентов.

Александр Чигвинцев,
EMC RSA в регионе Россия и СНГ.

Рис. 5. Этапность установления контроля по доступу сотрудников предприятия к конфиденциальной информации в соответствии с принятыми политиками ИБ с помощью RSA DLP Policy Workflow Manager.

VMware: новые решения для облаков

Декабрь 2012 г. – Компания VMware, Inc . объявила о доступности обновленной линейки решений для управления облаком, включающей значительные усовершенствования недавно выпущенного программного комплекса VMware vCloud® Suite. В его состав добавлен новый продукт VMware vCloud Automation Center™ 5.1, а в программный комплекс VMware IT Business Management Suite™ внесены изменения, позволяющие упрощать и автоматизировать процесс управления службами в разнородных облачных средах.

Решения VMware Cloud Management™ помогают построить программно-определяемый ЦОД, обеспечивающий эффективность и быстроту облачных вычислений. Подход VMware к управлению гибридными и разнородными облачными средами связан с тремя важными областями:

- *разработка облачных сервисов:* автоматизация процесса создания и управления ИТ-инфраструктурой по принципам «приложение как услуга» и «рабочее место как услуга» в соответствии с потребностями предприятия и его ИТ-политикой;
- *управление облачными вычислениями:* аналитика и другие интеллектуальные средства обеспечения эффективности облачной инфраструктуры;
- *управление облачными бизнес-процессами:* управление облачными сервисами