Архитектура и основные подсистемы SOC,
применяемые решения и продукты

Антон ЮДАКОВ,
начальник отдела решений по управлению ИБ, ОАО «ЭЛВИС-ПЛЮС»

Планирование, внедрение и обеспечение деятельности Security Operations Center (SOC) в его традиционном понимании – как ситуационного центра мониторинга и управления инцидентами ИБ – остается сегодня одной из актуальных задач для множества российских и зарубежных компаний. Согласно отчету компании Verizon «2013 Data Breach Investigation Report», около 70% проникновений в корпоративные сети компаний было обнаружено не самостоятельно, а внешними по отношению к ним организациями, уведомившими о соответствующих утечках. Одним из громких примеров может служить проникновение во внутреннюю сеть компании Target в конце 2013 г., повлекшее утечку данных кредитных карт более 40 млн клиентов компании и прочих нефинансовых данных примерно 70 млн клиентов. При этом важно понимать, что одномоментного внедрения средств мониторинга, даже сопровождаемых набором документации и выделенным персоналом, недостаточно для решения поставленной задачи (что также подтверждает случай компании Target). И речь не только о постоянном развитии и внедрении новых технологий, а также сопутствующем развитии угроз ИБ. Обеспечение деятельности по информационной безопасности также должно быть динамичным и, кроме того, в целом управление информационной безопасностью должно являться частью системы управления компанией.

Современный SOC

При анализе развития и внедрения новых технологий можно отметить существенное эволюционирование SOC вследствие тенденций двух последних десятилетий (последовательно: эпоха появления и расцвета вредоносного ПО, IDS, ботнетов, IPS и Compliance, кибервойн, хактивизма, APT).

Общемировые тенденции развития технологий, а также количественного и качественного роста угроз ИБ оказали существенное влияние на требования к современным SOC, как и в целом на вопросы обеспечения ИБ в компаниях. При этом не имеет значения, идет ли речь о собственном или внутреннем (in-house) SOC либо об использовании SOC как сервиса (as a service). Однако при рассмотрении архитектуры современного SOC в первую очередь будет анализироваться модель собственного SOC.

Стоит отметить, что создание, поддержка и развитие современного собственного SOC не всегда целесообразны. И не только по причине высоких для большинства компаний затрат (для крупных организаций они ниже стоимости последствий возможных инцидентов ИБ), но и вследствие обязательного требования наличия в компании хорошо выстроенных и отработанных процессов управления ИБ.

В то же время стоит помнить, что даже в случае использования аутсорсинговых моделей SOC критически значимые составляющие SOC остаются внутри компании – примером может служить непосредственно реагирование на выявляемые инциденты ИБ.

Создаваемый SOC может выполнять довольно широкий набор функций: мониторинг и управление инцидентами ИБ, управление уязвимостями, управление рисками ИБ, управление соответствием стандартам и т. д. Решение этого вопроса напрямую зависит от возлагаемых компанией на SOC целей и задач.

Как показывает практика, основой для принятия решения о возлагаемых на SOC функциях в том числе служат такие факторы, как:

- отрасль и специфика бизнеса компании;
- структура и территориальная распределенность компании;
- зрелость компании в целом с точки зрения вопросов обеспечения ИБ.

Как следствие, в одних компаниях происходит процесс внедрения ситуационных центров мониторинга и управления инцидентами ИБ (SOC в его традиционном понимании), в других – полнофункциональных центров управления и мониторинга ИБ. При этом для зрелых с точки зрения вопросов обеспечения ИБ отраслей и компаний (например, банковской отрасли) процесс внедрения по любому из указанных вариантов требует, как правило, меньших затрат.

Вне зависимости от выбранного пути и решаемых задач, важно помнить, что SOC, как и обеспечение ИБ в целом, – это не проект и не продукт, а совокупность используемых решений/продуктов, персонала и процессов.

Решения и продукты

Практически каждая российская компания при планировании собственного SOC в первую очередь возлагает на него функции мониторинга и управления инцидентами ИБ. Этот подход полностью соответствует мировой практике: основной подсистемой в составе SOC традиционно считаются решения классов Log Management и Security Information and Event Management (SIEM).

Подобные решения предназначены в первую очередь для централизованного сбора и анализа событий от различных источников, предоставляя (в зависимости от класса системы) возможность выявления инцидентов ИБ и инструментарий для их расследования.

Вне SOC, как правило, данная подсистема строится при наличии в компании множества разнородных средств ИТ-инфраструктуры и средств управления подсистемами ИБ, анализ журналов регистрации событий которых становится трудоемкой задачей для персонала соответствующих ИТ-/ИБ-подразделений. Для решения задачи централизации событий из различных журналов выбирается либо продукт с базовыми функциями централизованного управления событиями (Log Management), либо более продвинутые системы, обладающие возможностями по корреляции – взаимной обработке поступающих событий ИБ в режиме, близком к реальному времени (SIEM). Как вариант в компании также могут одновременно использоваться системы обоих классов.

Кроме того, современные SIEM-системы обладают широкими возможностями по управлению инцидентами ИБ и наращиванию их функциональности с помощью отдельно лицензируемых модулей, что будет подробно рассмотрено далее.

Выбор класса системы и конкретного продукта для реализации LM- и/или SIEM-системы при построении SOC – весьма ответственная задача, решение которой требует серьезных компетенций специалистов заказчика и возможно привлекаемого интегратора. В качестве продуктов систем данного класса могут использоваться как коммерческие продукты зарубежных вендоров, так и свободно распространяемое ПО, а также основанные на нем российские разработки.

На российском рынке активно работают постоянные игроки LM- и SIEM-рынка, широко распространены:

- продукты линейки HP ArcSight (HP ArcSight Logger, HP ArcSight ESM/Express);
- продукты линейки IBM QRadar SIEM;
- продукты линейки McAfee SIEM;
- в некоторых компаниях – решение Splunk.

Ограниченно встречаются продукты и других зарубежных вендоров – от серьезных игроков рынка (в частности, RSA Security Analytics) до нишевых (например, SolarWinds LEM).

В некоторых российских компаниях используются адаптируемые наборы свободно распространяемого ПО (OSSIM, Elasticsearch/Logstash/Kibana, SEC и др.) – как самостоятельно внедряемые и адаптируемые силами заказчика, так и, например, в виде коммерческого продукта КОМРАД, внедряемого и поддерживаемого разработчиком – НПО «Эшелон».

Функции по управлению инцидентами ИБ (ведение и эскалация инцидентов, ведение базы инцидентов и т. д.) зачастую

Рис. 1. *Высокоуровневая архитектура SOC*

отделяются компаниями от SIEM-решений. И здесь очень многое зависит от ситуации в конкретной компании, в том числе от возможности и целесообразности использования имеющейся Service Desk-системы (например, модуль Incident Management решения BMC Remedy IT Service Management Suite). Или, возможно, компания внедряет решение класса IT-GRC (Governance, Risk, Compliance), предусматривающее автоматизацию процесса управления инцидентами (например, модули Incident Management и Security Operations Management IT-GRC-платформы RSA Archer).

Тем не менее, и это особенно актуально при создании SOC, некоторым компаниям будет достаточно механизмов управления инцидентами ИБ, реализованных в SIEM-решении (например, HP ArcSight Case Management или RSA Security Analytics Security Operations Management). Если же это невозможно или для компании целесообразно совместить несколько из указанных подходов (необходимость создания и ведения инцидента может быть обусловлена не только выявленным SIEM-системой инцидентом), то практически каждое SIEM-решение позволяет организовать пересылку информации об инциденте во внешнюю систему.

Для обмена информацией, полученной при расследовании инцидентов ИБ, в составе технических средств SOC целесообразно наличие общей базы знаний, в которую будут вноситься решения

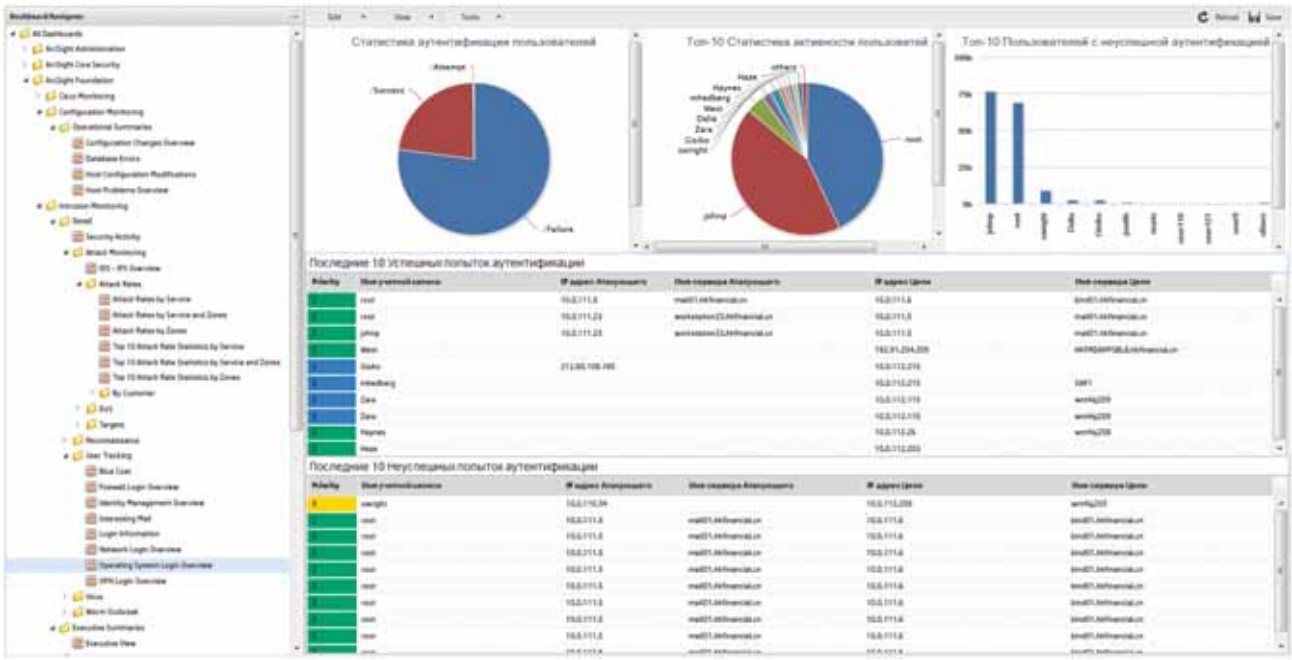

Рис. 2. *Пример рабочей панели HP ArcSight ESM/Express*

известных проблем и инцидентов. Такая база знаний необходима для SOC любого масштаба, но средства ее реализации могут варьироваться. Например, для небольшой команды это может быть файловый сервер или свободно распространяемый портал формата «Wiki». Другой вариант – средства, предлагаемые разработчиками SIEM-систем или решений класса IT-GRC.

Переходя к вопросу организации реагирования на инциденты ИБ, важно отметить возможность обеспечения доказательной базы на основе не только информации из журналов регистрации событий, но и результатов конкретных сессий передачи данных, пользовательских сессий и т. д. И что особенно актуально при создании SOC – здесь могут быть полезны решения класса Network Forensics Tool (NFT), а также класса Endpoint Threat Detection and Response (ETDR).

Инструментарий класса NFT сложно переоценить при использовании в составе SOC: в процессе восстановления цепочки событий при расследовании самых различных инцидентов такие средства позволяют восстановить конкретные сессии и передаваемые внутри них данные.

До недавнего времени на российском рынке был представлен лишь один зарубежный вендор с решением RSA Netwitness (в настоящий момент – часть SIEM-решения RSA Security Analytics), однако череда недавних поглощений привела к появлению на российском рынке сразу нескольких крупных игроков с такими решениями, как:

- FireEye Network Forensics (ранее nPulse Technologies Cyclone Network Forensics Platform);
- Arbor Pravail Security Analytics (ранее Packetloop Security Analytics);
- Blue Coat Security Analytics Platform (ранее Solera Networks DeepSee).

В дополнение к перечисленным коммерческим продуктам зарубежных вендоров существует и разработанное сотрудниками компании AOL свободно распространяемое ПО, выполняющее схожие функции, – Moloch, уже встречающееся и в российских SOC.

Функции по сохранению отдельных подозрительных или связанных с выявленным инцидентом сессий появляются и в составе SIEM-решений. Например, подобные модули уже реализованы в продуктах IBM QRadar SIEM (модуль Incident Forensics) и McAfee SIEM (модуль Application Data Monitor).

Вместе с тем не стоит забывать и о высокоуровневом анализе данных о сетевом трафике, в частности о сборе и анализе данных по протоколам NetFlow, SFlow и им подобным. Так, в составе линейки HP ArcSight предусмотрен полезный для SOC дополнительно лицензируемый модуль HP ArcSight Pattern Discovery, позволяющий выявлять поведенческие паттерны[1], в том числе возможно свидетельствующие о реализуемых незамеченных атаках.

Говоря об инструментарии класса ETDR, назовем наиболее популярные в составе SOC решения: EnCase Enterprise (компании Guidance Software); Spector CNE Investigator (компании SpectorSoft), но подробно рассматривать их не будем.

[1] *Модуль HP ArcSight Pattern Discovery позволяет выявлять поведенческие паттерны не только в событиях о сетевых взаимодействиях, но и в целом в любых имеющихся в SIEM-системе наборах событий.*

Не являются предметом данной статьи, хотя и могут рассматриваться в качестве подсистем SOC, средства централизованного управления подсистемами ИБ, используемые в инфраструктуре компании. В частности, это относится к решениям класса Vulnerability Management, Database Audit and Protection, Network IDS/IPS, Malware и Endpoint protection. При этом стоит отметить решения классов Data Loss Prevention и Next Generation Threat Protection (в частности, популярную линейку продуктов FireEye), интеграция с которыми (при их наличии) важна при создании SOC.

На практике на SOC часто возлагается и ряд организационных проактивных мер (как в явном виде, так и вследствие выполняемых задач): разработка и проведение Security Awareness тренингов, участие в разработке внутренних политик/стандартов и т. п.

При анализе проактивных функций SOC, позволяющих снизить риск возникновения инцидентов ИБ, стоит обратить внимание и на такой аспект. Современные злоумышленники создают целые сообщества экспертов своего дела, обмениваются знаниями и информацией, служащей для их незаконного обогащения. Такой подход требует соответствующих противодействующих мер и обмена знаниями экспертами в области ИБ. Широко известны различные платные и бесплатные сервисы, предоставляющие информацию об обнаруженных угрозах, уязвимостях, ботнетах и т. п. Некоторые из производителей SIEM-систем встраивают взаимодействие с подобными источниками данных на платной основе в виде соответствующих подписок или отдельно лицензируемых модулей: например, RSA Live для RSA Security Analytics, HP ArcSight RepSM для HP ArcSight и т. д.

Информация, получаемая через эти подписки, позволяет персоналу SOC более точно анализировать текущую обстановку, а в случае интеграции с SIEM в автоматическом режиме анализировать с ее учетом поступающие в систему события ИБ. Действительно, персонал SOC должен обладать актуальной информацией и предлагать изменения настроек средств защиты и обнаружения инцидентов для их соответствия актуальным угрозам ИБ. Поэтому для функционирующего SOC целесообразно обеспечить соответствующие подписки на предусмотренные в системах мониторинга и защиты информации источники данных и желательно подписки на рассылки отчетов и уведомлений от компаний, проводящих независимые исследования в этой области. Сложно назвать это отдельной подсистемой SOC, однако если недооценить важность актуальной информации об угрозах, обмена индикаторами компрометации и т. п., это может вылиться в успешно реализованную своевременно не выявленную атаку.

Немаловажными задачами SOC (вне зависимости от вкладываемого в понятие смысла, хотя указанные задачи особенно актуальны, если говорить о полнофункциональном центре управления и мониторинга ИБ) также являются:

- оценка результативности и эффективности деятельности SOC (на основе статистических данных или в динамике);
- оценка эффективности взаимодействия подразделений компании в части, касающейся деятельности SOC;
- демонстрация деятельности SOC руководству компании.

С точки зрения SOC наиболее подходящими для оценки результатов деятельности персонала и эффективности самого подразделения

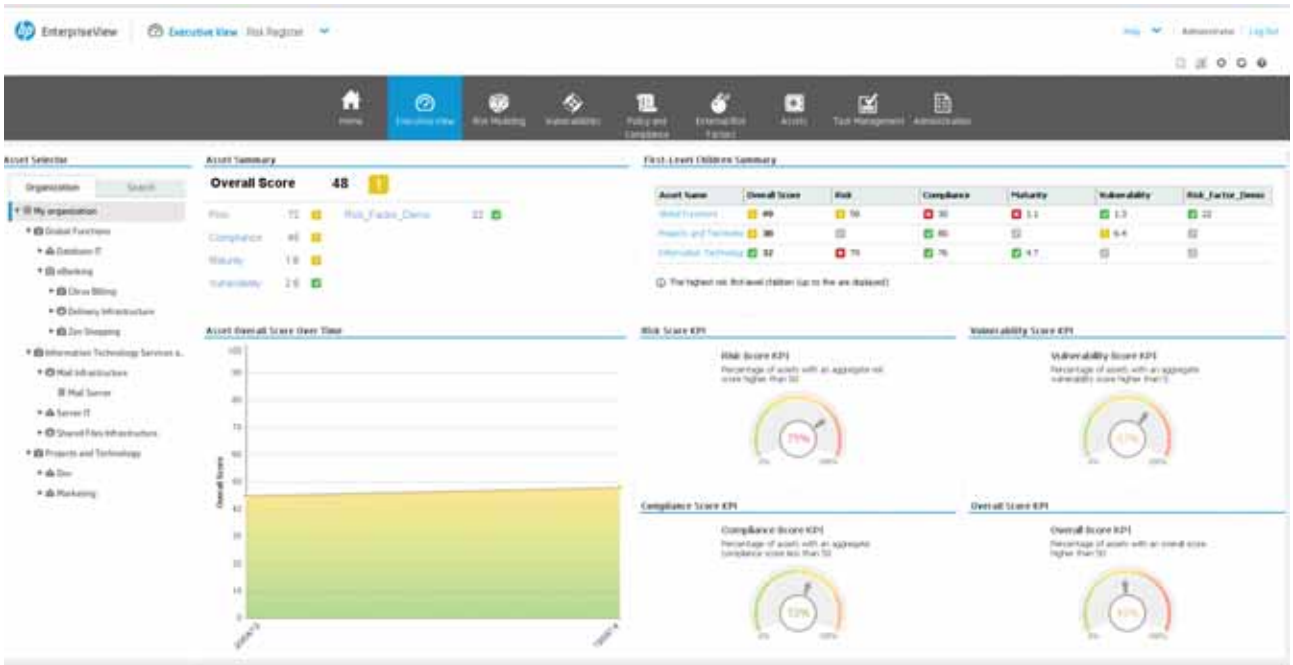

Рис. 3. *Пример интерфейса HP EnterpriseView (модуль Risk Management)*

Рис. 4. *Пример интерфейса R-Vision (модуль Incident Manager)*

являются отчеты, составленные в системах, стоящих над отдельными подсистемами ИБ, т. е. в SIEM-системах, решениях по управлению инцидентами ИБ и возможно используемых IT-GRC решениях. Для решения этой задачи могут применяться и системы класса Business Intelligence and Analytics.

Наиболее популярными представителями продуктов данного класса (в том числе на российском рынке) являются платформы Tableau (компании Tableau Software) и QlikView (компании QlikTech). На базе последней – QlikView – уже есть соответствующие предложения от нескольких ИБ-вендоров и интеграторов, например, решение Портал аналитической отчетности компании Positive Technologies.

Для решения указанной задачи могут применяться и решения класса IT-GRC либо их отдельные модули. И здесь целесообразно вновь вернуться к вопросу возлагаемых на SOC задач и подробнее рассмотреть вариант, когда компанией создается полнофункциональный центр управления и мониторинга ИБ. Помимо рассмотренных выше функций SOC центр управления и мониторинга ИБ позволяет автоматизировать такие процессы управления ИБ, как:

- управление информационными активами (Asset Management);
- управление уязвимостями (Vulnerability Management);
- управление рисками ИБ (Risk Management);
- управление соответствием стандартам регуляторов и политикам компании в области ИБ (Compliance).

На российском рынке представлено несколько зарубежных коммерческих IT-GRC платформ, позволяющих автоматизировать перечисленные процессы, – это платформа RSA Archer, на протяжении многих лет признанный лидер в области GRC-решений, а также относительно новый продукт от компании HP – HP EnterpriseView. Отличительной особенностью этих продуктов является высокая степень автоматизации процессов управления уязвимостями, рисками ИБ и соответствие стандартам, с широкими возможностями по интеграции с внешними системами, в частности решениями классов Vulnerability Management и SIEM (как собственными, так и сторонними).

В то же время на российском рынке появились и системы отечественной разработки, также предоставляющие возможности автоматизации процессов управления ИБ, при этом, что немаловажно, по умолчанию учитывающие специфику и требования российских компаний, как, например, решение R-Vision (компании ISM Systems). Подобные решения обладают как преимуществами, так и недостатками в сравнении с зарубежными аналогами, однако для ряда компаний они могут стать оптимальным и соответствующим потребностям выбором.

***

Подводя итог, можно констатировать, что для любого выбранного пути создания SOC – ситуационного центра мониторинга и управления инцидентами ИБ (SOC в его традиционном понимании) или полнофункционального центра управления и мониторинга ИБ в компании – на российском рынке предлагаются активно развивающиеся как зарубежные, так и отечественные решения и продукты, обеспечивающие реализацию соответствующих процессов мониторинга и управления, более того, в зависимости от выбранных решений позволяющие без особых затрат перейти от первого ко второму варианту создания подобного центра. ■