Построение центра мониторинга и управления безопасностью Cisco
Архитектура, процессы и результаты

Обзор

Центр мониторинга и управления безопасностью (Security Operations Center; SOC) Cisco® поможет защитить вашу сеть, сети ваших клиентов и трафик, связанный с деловой активностью. Организуя разумный баланс технологий, процессов и людских ресурсов, Cisco SOC предоставляет возможность непрерывного мониторинга сетей с отслеживанием инцидентов в сфере безопасности и быстрого принятия ответных мер при возникновении угроз.

Фактически, скорость реакции – это основное преимущество центра Cisco SOC. Компьютерные черви способны распространяться в сети Интернет в течение минут или даже секунд, выводить из строя сети ваших клиентов или замедлять передачу трафика до черепашьих скоростей. Поэтому для выявления таких атак и их отражения еще до того, как они смогут причинить существенный ущерб, важна каждая секунда. Cisco SOC предназначен для решения именно таких задач.

На практике Cisco SOC выполняет мониторинг состояния безопасности сети и мгновенно реагирует на возникновение критических ситуаций в сфере безопасности проблемы и появление новых уязвимостей.

В этом документе обосновывается необходимость создания центра SOC, описана его роль, функции и преимущества. Рассмотрены этапы построения архитектуры Cisco SOC и шесть стадий эффективных мер по обработке инцидентов в сфере безопасности. Наконец, речь идет о том, как собрать команду Cisco SOC, и перечислены ожидаемые результаты работы Cisco SOC.

Вашей организации, как и любому провайдеру услуг, необходима политика безопасности для вашей собственной сети. Хотя многие из описанных в данном документе принципов и приемов могут быть уже отражены в такой политике, вернитесь к ним при рассмотрении вопросов создания и настройки Cisco SOC для мониторинга и защиты сетей и трафика клиентов.

Необходимость создания Cisco SOC

Когда сеть организации подвергается атаке вирусов, червей или распределенной атаке типа «отказ в обслуживании» (DDoS), издержки могут оказаться весьма значительными. Это упущенные прибыли. Это недовольные клиенты. Это разочарованные сотрудники. Это подмоченная репутация. Но при этом у многих организаций нет адекватных программ и процедур обеспечения безопасности для обработки таких инцидентов. Как правило, этим организациям также не хватает профессионального опыта и инструментов для устранения последствий нарушений информационной безопасности. Организации простодушно рассчитывают на то, что такие атаки их не коснутся. Такая шаткая вера - это, скорее, принятие желаемого за действительное, а не реалистичный взгляд на вещи.

Несмотря на это, организации хотят избежать потери и порчи своих данных, в том числе и важных объектов интеллектуальной собственности. Они хотят защищать критически важные ресурсы. Они хотят «оставаться на связи»… поддерживать работоспособность важных сервисов... защищать деловые операции от убытков и задержек... и обеспечивать обслуживание клиентов. Существенное нарушение безопасности сети может поставить под угрозу реализацию всех этих задач.

Благодаря Cisco SOC, вы сможете в полном объеме удовлетворить потребности ваших клиентов в сфере обеспечения безопасности и внедрить архитектуры и процессы, которые защитят их организации. Одним словом, при активном участии клиентов вводятся программы, процедуры и инструменты обеспечения безопасности и применяются профессиональные навыки ваших специалистов, которые необходимы сегодня для надлежащего контроля за состоянием сетей.

Общие задачи и функции Cisco SOC

Для обеспечения защиты такого уровня центр SOC должен обеспечить решение следующих задач:

- Управление следующими объектами и мониторинг их состояния в режиме реального времени: виртуальные частные сети, межсетевые экраны, системы обнаружения и предотвращения вторжений, системы отражения DDoS-атак, решения для борьбы с вирусами, шпионскими программами и другим вредоносным кодом, обновления программного обеспечения, персональные и портативные компьютеры, серверы и другие продукты, имеющие отношение к сфере безопасности.
- Анализ данных журнала безопасности, сведений об уязвимостях, информации о ресурсах и сигналов тревоги.
- Немедленное принятие ответных мер при возникновении потенциальных угроз нарушения безопасности и быстрое разрешение проблемных ситуаций в сфере безопасности.
- Мониторинг состояния безопасности ваших клиентов в режиме реального времени.
- Защита клиентов от возникающих сетевых атак.
- Защита инвестиций организаций в технологии обеспечения информационной безопасности.

Для успешного решения этих задач центру SOC необходимо выполнять мониторинг сетей клиентов, отслеживая возникающие угрозы безопасности. Эта функция, так называемый «мониторинг безопасности для оценки риска», подразумевает выполнение следующих действий:

- Получение подробного обзора состояния сети путем сбора данных, в частности, результатов опроса по протоколу SNMP, сообщений SNMP-trap, syslog-сообщений и данных NetFlow.
- Применение приемов и инструментов интеллектуального анализа и корреляции для выявления инцидентов в сфере безопасности на базе собранной информации.
- Тщательный мониторинг возникающих угроз и единые правила реакции на эти угрозы в сети коллективного пользования наряду с применением индивидуальной политики безопасности для каждого клиента.
- Применение сложной методики анализа трафика для обнаружения аномалий,

потенциально связанных с инцидентами в сфере безопасности.

- Привлечение экспертов по безопасности для анализа и помощи в разрешении инцидентов в сфере безопасности.
- Непрерывный мониторинг уязвимостей и нарушений в сфере безопасности; осуществление таких мероприятий на самом раннем этапе, выявление инцидентов в сфере информационной безопасности в самом начале, позволяет устранить угрозу до того момента, как будет нанесен реальный ущерб.
- Периодическое сканирование вашей сети и сетей ваших клиентов для проверки соответствия мер обеспечения информационной безопасности принятым политикам безопасности и условиям договоров об уровне обслуживания (SLA).
- Мониторинг вашей сети для отслеживания сигналов тревоги, контроль и тестирование элементов сети.
- Удаленное обслуживание, конфигурирование и резервное копирование файлов для оперативного восстановления работоспособности сервисов.
- Модернизация устройств обеспечения безопасности с применением протестированного программного обеспечения, которое содержит исправления, устраняющие уязвимости, текущие обновления и новые функции.
- Сбор данных об использовании ресурсов клиентами для биллинга.
- Помощь в генерировании отчетов о соблюдении нормативных требований для аудиторов с использованием обширного хранилища собранных данных.

Преимущества Cisco SOC

Задачи и функции, решаемые центром Cisco SOC, обеспечивают целый ряд преимуществ:

Эффективная реакция на инциденты в сфере информационной безопасности
При использовании Cisco SOC осуществляется переход от реактивного подхода к профилактическим мерам.
Вместо акцента на ответных мерах, реализуемых при угрозе безопасности, вводится продуманный процесс, который предоставляет возможность быстро и эффективно перейти к обнаружению, локализации и уничтожению угрозы.
Помимо этого, достигается возможность ориентировать экспертов по безопасности на разработку сетевых стратегий, а не на поиск применимых решений каждый раз, когда будет возникать новая угроза. В дополнение к этому, появляется возможность предлагать защиту от злоумышленников, которые атакуют сети или web-сайты ваших клиентов.

Снижение риска для ваших клиентов
С помощью Cisco SOC можно свести к минимуму перерывы в работе сети, связанные с событиями в сфере информационной безопасности. «Шагая в ногу» с эволюционирующими глобальными угрозами, вы можете более эффективно защищать трафик ваших клиентов от потерь и манипулирования данными и устанавливить более эффективный контроль над вашими сервисами обеспечения безопасности.

Усовершенствование ответных мер для обеспечения безопасности
Что вызвало всплеск трафика электронной почты клиента? Этот всплеск аномален, но не криминален? Или это предвестник разрушительной сетевой атаки? Используя Cisco SOC, вы получаете на вооружение алгоритм привлечения различных функциональных подразделений для анализа подобных случаев. Это алгоритм систематизированного анализа потенциальных причин возникновения аномалий трафика и соответствующей

передачи инцидента на следующий уровень анализа. Действуя быстро, вы устраняете инциденты в сфере безопасности за считанные минуты, а не часы или дни, что значительно сокращает возможные перерывы в работе критически важных сервисов и в бизнес-процессах.

Повышение эффективности работы

Определив правила и введя политику безопасности, специалисты вашего центра SOC получат возможность быстро выявлять угрозы и применять средства их устранения в зонах риска еще до того, как на них обрушатся сетевые атаки. В дополнение к этому, за счет выделения угроз безопасности из колоссального объема данных, которые поступают в центр SOC, можно снизить коэффициент «сигнал-шум», при больших значения которого способность принимать ответные меры существенно ухудшается.

Более того, при совместной работе SOC с центром управления сетью (NOC) достигается такая эффективность работы, которая была бы невозможна при изолированной работе этих двух составляющих. Совместная работа двух центров предоставляет вашим экспертам в области функционирования сетей и в сфере безопасности возможность более четко контролировать ситуацию, обмениваться доступными инструментами, интегрировать процедуры принятия ответных мер для обеспечения безопасности и действовать более сплоченно.

Сокращение затрат

Поскольку Cisco SOC в значительной мере опирается на технологии, инструменты и процедуры обеспечения безопасности, обеспечивающие «первый уровень защиты», можно эффективно использовать всегда недостаточные ресурсы обеспечения безопасности без ущерба для качества результатов работы SOC. Давая таким специалистам возможность сконцентрировать внимание на угрозах, не обнаруживаемых автоматически в рамках контроля выполнения политики безопасности, вы оптимальным образом используете их профессиональные навыки. Другими словами, Cisco SOC позволяет опереться на процессы и технологии, которые станут весомым подспорьем в работе, выполняемой, как правило, специалистами по безопасности. Это поможет вам обслуживать большее количество клиентов, не раздувая штат организации.

Помощь клиентам в соблюдении нормативных требований

Во многих случаях клиенты должны соблюдать требования нормативных документов и политик, регламентирующих использование, защиту и конфиденциальность информации. Клиенты могут использовать отчеты, генерируемые центром SOC, для помощи в соблюдении таких требований и правил, включая Закон Сайрбенса-Оксли (SOX), Закон о прибылях и отчетности в сфере здравоохранения (HIPAA) и требования к безопасному хранению данных, которые действуют в сфере обращения платежных карт (PCIDSS).

Вопросы, на которые следует ответить перед внедрением Cisco SOC

Возможно, ваше предприятие до сегодняшнего дня достаточно хорошо работало и без SOC. Зачем вкладывать в него деньги сейчас? Ответ прост: скорость распространения современных Интернет-червей и и потенциальный ущерб, который могут причинить атаки в масштабе всей сети Интернет, делают SOC необходимым атрибутом, а не предметом роскоши. Короче говоря, нельзя позволить отказаться от его создания, если необходимо обеспечить адекватную защиту своих клиентов и своего предприятия.

Перед тем как приступить к настройке SOC необходимо ответить на следующие вопросы:

- Как можно защитить критически важные ресурсы и операции наших клиентов перед лицом постоянно меняющихся угроз?
- Как гарантируется конфиденциальность информации для наших сотрудников, партнеров, поставщиков и клиентов?
- Как разрабатывается политика безопасности и как она реализуется?
- Как управляются колоссальные объемы данных, которые поступают в результате работы технологий мониторинга безопасности, технологий, которые сами по себе создают сложные задачи эксплуатационной поддержки?
- Как поддерживаются подотчетность и регламентация целевых задач на корпоративном уровне?

Ответив на эти вопросы, выполните действия, описанные в следующем разделе.

Архитектура Cisco SOC

В этом разделе описывается построение архитектуры Cisco SOC, и рассмотрены шесть стадий принятия ответных мер при возникновении инцидентов. Выполнив эти действия и пройдя эти стадии, вы разработаете важнейшие процедуры для идентификации, разрешения и нейтрализации инцидентов в сфере информационной безопасности.

Построение своей архитектуры центра Cisco SOC

Архитектура Cisco SOC предписывает, какую информацию о безопасности следует собирать, и определяет правила анализа, обработки и распространения этой информации. Выполните нижеописанные действия для построения надлежащей архитектуры Cisco SOC в вашей фирме. Соответствующие этапы перечислены на стрелках в верхней части рисунка 1.

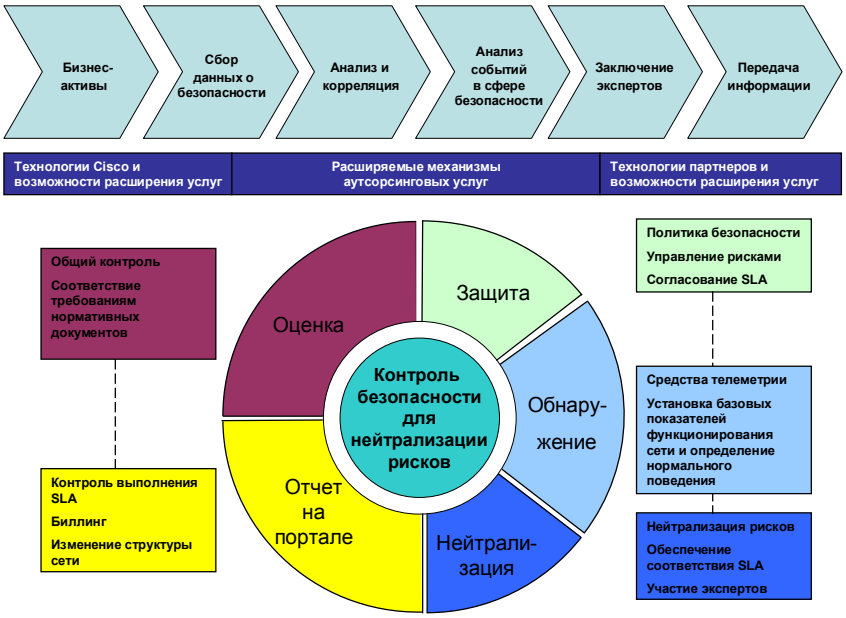

Рисунок 1. Архитектура Cisco SOC

1. Определите, для каких бизнес-активов необходимы мониторинг и защита.

В некоторых случаях ваши клиенты знают, защита каких маршрутизаторов, коммутаторов, серверов, компьютеров, баз данных и других бизнес-активов им необходима. В других

ситуациях вам, возможно, потребуется дать им определенные рекомендации.

Определив, на какие бизнес-активы будет распространяться мониторинг, вы и ваши клиенты должны ответить на два вопроса:

- Какая политика безопасности требуется для защиты этих активов?
- Какой договор об уровне обслуживания (SLA) необходим?

Ответив на эти вопросы, вы можете перейти к следующему этапу.

2. Определите, какие данные о безопасности следует собирать.
В соответствии с политикой безопасности и условиями договоров SLA необходимо получать от ваших клиентов определенные данные. Как правило, чем шире масштабы мониторинга безопасности, тем более подробны эти данные. Другими словами, возможны существенные различия в характере и объеме собираемых вами данных, зависящие от конкретного клиента.

3. Определите, по каким данным следует проводить анализ и определять корреляцию.
Анализировать весь трафик, поступающий от клиента, нецелесообразно. Даже малые и средние предприятия могут выдавать поистине колоссальные объемы данных. Можно упростить этот процесс, проводя анализ и корреляцию только тех данных, которые созданы в результате анализа результатов опросов по протоколу SNMP, сообщений SNMP-trap, syslog-сообщений и данных NetFlow. *Средства анализа и механизмы корреляции мгновенно идентифицируют потенциальные инциденты в сфере безопасности, и эти функции исключительно важны для обеспечения надлежащего качества сервисов*.

Анализ и определение корреляции могут выполняться как в центре Cisco SOC, так и на площадках клиентов. Большинство провайдеров выбирают первый вариант, но из-за ограниченности полосы пропускания более привлекательным может стать второй. В любом случае, сообщите вашим клиентам, какими данными вы пользуетесь для сбора информации об инцидентах в сфере безопасностью. Вы можете гарантировать клиентам, что никакая конфиденциальная информация, т.е. информация, связанная с их текущей деловой активностью, не попадает в центр SOC. Это послужит дополнительным аргументом для представителей руководства организаций.

4. Проанализируйте соответствующие события в сфере безопасности.
Выполнив анализ и определив корреляцию информационного трафика клиента, выделите инциденты в сфере безопасности из корректного трафика и сконцентрируйте свое внимание на них. Важно выделять только те инциденты, которые являются фактическим нарушением политики безопасности каждого клиента. Например, нереально выполнить проверку каждой строки из двух миллионов syslog-сообщений, созданных межсетевым экраном клиента. Выделив только те строки, которые соответствуют угрозе безопасности, вы сможете эффективно использовать дефицитные ресурсы в сфере информационных технологий.

5. Привлеките ваших экспертов по безопасности.
После того как SOC выделит потенциальный инцидент в сфере безопасности, к работе приступают эксперты по безопасности. Эти люди обладают профессиональными навыками и опытом для анализа потенциального нарушения безопасности и быстрого и эффективного устранения последствий нарушения безопасности.

6. Передайте информацию клиентам.
Последний этап в построении архитектуры Cisco SOC – формирование процесса, с помощью которого клиенты смогут получать информацию о каждом инциденте в сфере безопасности и

контролировать процесс его устранения. При возникновении инцидента необходимо генерировать учетную карточку (так называемый Trouble Ticket) и предоставлять клиентам, которых затронул этот инцидент, доступ к этой карточке в соответствии с условиями договора SLA или политикой безопасности. Кроме этого, можно составлять подробные еженедельные, ежемесячные и годовые отчеты, что позволяет дополнительно укрепить взаимоотношения с клиентами.

Шесть этапов принятия ответных мер при возникновении инцидентов

Итак, архитектура центра Cisco SOC сформирована, но вам по-прежнему необходимы эффективные и результативные ответные меры на случай выявления угрозы безопасности. Для этого служат шесть этапов принятия ответных мер при возникновении инцидентов (см. рис. 2), подробное описание которых приведено ниже.

Рисунок 2. Шесть этапов реакции на инцидент

1. Подготовка

Продуманная подготовка – важный элемент продуманной реакции на инциденты. Если вы хорошо подготовлены, вы знаете, что и как делать, если возникнет инцидент в сфере безопасности. Хорошая подготовка – это:

- Привлечение опытных дипломированных специалистов.
- Разработка и оформление плана обеспечения безопасности.
- Разработка договоров SLA с клиентами и организациями-партнерами.
- Приобретение необходимых инструментов.
- Внедрение процедур обеспечения безопасности.
- Обучение персонала центра SOC работе с инструментами и процедурами.
- Регулярная проверка непрерывности эксплуатации.
- Наличие постоянно действующих договоров о сопровождении с производителями/поставщиками.
- Экспертная оценка и количественное измерение степени улучшения процесса.

Когда эти действия будут выполнены, центр Cisco SOC сможет быстро и эффективно

реагировать на возникающие сетевые угрозы. Убедитесь в том, что весь персонал хорошо знаком с задачами центра и с предусмотренными процедурами. Безусловно, вы не хотите, чтобы первый практический опыт возник на почве реального инцидента. Другими словами, тщательное планирование, обеспечивающее готовность, и внедрение надежных базовых параметров для принятия ответных мер избавят вас от ошибок и пропусков, которые могут ощутимо снизить эффективность ваших действий в критических ситуациях.

2. Идентификация
Безусловно, вы хотите выявлять инциденты в сфере безопасность, до того, как они затронут сети ваших клиентов. Для того чтобы получить такую ценную возможность, используйте аналитические инструменты и данные мониторинга, получаемые с помощью NetFlow, опросов по протоколу SNMP, сообщений SNMP-trap и syslog-сообщений.

3. Классификация
После того как атака идентифицирована, необходимо оценить степень ее серьезности и масштаб: затрагивает ли атака одного клиента, нескольких клиентов или всю инфраструктуру?

4. Отслеживание источника
У атаки есть жертва и источник. После того как угроза классифицирована, ваши специалисты должны найти точку ее проникновения: это может быть сеть организации-партнера, сервер в сети более высокого уровня, сервер в сети более низкого уровня или взломанное сетевое устройство в центре обработки данных.

5. Ответные меры
Классифицировав атаку и выявив ее источник, специалисты центра Cisco SOC применяют инструменты и процедуры подавления атаки. Для того чтобы эта работа была успешной, необходима наглядная картина состояния сети и хорошо прописанные стандартные операционные процедуры. Придерживаясь этих процедур, вы не рискуете усугубить проблему.

6. Анализ
Ваши специалисты по безопасности должны анализировать исходные причины каждого инцидента и вносить найденные новые решения в рабочие инструкции по разрешению инцидентов, чтобы использовать их для справки при возникновении очередного инцидента.

Команда центра обеспечения безопасности

Даже безупречные процедуры реакции на инциденты принесут мало пользы, если у ваших специалистов нет достаточных профессиональных навыков или опыта правильного применения таких процедур. Поэтому необходимо собрать команду специалистов центра Cisco SOC и создать оперативную группу для разрешения инцидентов.

Требования к профессиональным навыкам команды специалистов Cisco SOC

Работники центра Cisco SOC должны быть специалистами одновременно и по магистральным сетям провайдеров услуг, и по обеспечению безопасности. Фактически, специалисты вашего центра Cisco SOC должны быть знакомы со следующими аспектами функционирования сетей провайдеров:

- Функционирование ядра и магистральной сети.
- Подсоединение клиентской сети к ядру или магистральной сети.

- Управление сетью, включая системы поддержки функционирования (OSS).
- Системы хостинга и хранения контента.
- Деятельность сообществ, например, по безопасности провайдеров сетевых сервисов (NSP-SEC).
- Система доменных имен (DNS), протокол DHCP, схемы адресации и процедуры обеспечения безопасности.
- Функционирование группы реагирования на чрезвычайные ситуации (CERT).

Специалисты центра Cisco SOC также должны обладать знаниями, которые необходимы обычному техническому специалисту по безопасности. Возможно, такие одаренные специалисты запросят высокие оклады, но, опираясь на надлежащие инструменты и процедуры, вы можете оптимизировать и масштабировать профессиональные навыки таких работников. Кроме этого, вы, возможно, захотите командировать специалистов по безопасности для работы на площадках ваших клиентов. В этом случае обеспечивается максимальная степень безопасности.

Создание оперативной группы для разрешения инцидентов
Специалисты центра Cisco SOC обеспечивают его повседневную работу, но на случай реальных атак, возможно, следует создать специальную оперативную группу для разрешения инцидентов. Такая специальная оперативная группа потребуется, если центр Cisco SOC действует независимо от центра NOC. Если эти два центра работают как единое подразделение, специалисты центра Cisco SOC формируют оперативную группу, при этом к ним присоединяется ряд нетехнических специалистов, упомянутых ниже. В любом случае, размер такой оперативной группы, как правило, будет меняться в зависимости от количества и размера контролируемых сетей.

Если центры Cisco SOC и NOC работают раздельно, в оперативную группу по разрешению инцидентов должны входить представители и Cisco SOC, и NOC. Почему? Это предоставляет возможность оперативно определить, что является источником инцидента - сеть или межсетевой экран – и можно ли отнести инцидет к сфере информационной безопасности. Например, если оформляется учетная карточка, возможно, в первую очередь ее следует направить в центр NOC. Если центр NOC установит, что с сетью все в порядке, карточка будет перенаправлена в центр Cisco SOC. Если специалисты Cisco SOC ответят, что межсетевой экран функционирует исправно, учетная карточка будет передана в оперативную группу разрешения инцидентов. Благодаря привлечению специалистов из центра Cisco SOC и NOC, эта команда обладает концептуальным видением и профессиональными навыками, которые необходимы для системного подхода к решению проблемы, для применения инструментов, приемов и процессов идентификации инцидентов, отслеживания их источников и принятия надлежащих ответных мер.

Вам также следует включить в оперативную группу по разрешению инцидентов ведущего специалиста по информационной безопасности, ведущего специалиста по информационным технологиям, главного юрисконсульта, менеджера по связям с общественностью и, возможно, других работников. Хотя члены вашего Корпоративного комитета по защите и безопасности (CIRC) и ведущий специалист по информационной безопасности, вероятно, будут принимать участие в реализации ответных мер, для успешной работы им необходима поддержка, профессиональные знания, а также полномочия других подразделений организации.

Аттестация готовности работников и сетей

Если обе команды специалистов и сеть подготовлены, вы можете дать ответы на следующие вопросы:

- Нормальны ли эти шаблоны трафика для нашей сети?
- Что занимает всю нашу полосу пропускания?
- Звонят рассерженные клиенты. Что стряслось?
- Почему сервер, сеть или автономная система недоступны?
- Не произошел ли незаконный захват наших маршрутизаторов другим провайдером?
- Необходимо ли нам изменить атрибуты или политику BGP?

Контактные данные и каналы коммуникаций

В центре Cisco SOC должны существовать установленные процедуры связи с работниками, клиентами и взаимодействующими провайдерами на случай, если вы или ваши клиенты подвергнетесь атаке. Фактически, вам необходимо применять шестиэтапный процесс реакции на инциденты, описанный ранее. Точная контактная информация поможет вам пройти эти шесть этапов быстрее и эффективнее. Поэтому необходимо собрать и своевременно обновлять следующую информацию:

- Все важнейшие адреса электронной почты, номера телефонов и пейджеров, URL-адреса Web-страниц.
- Контактные лица всех взаимосвязанных провайдеров – одного уровня с вашей организацией и более высокого уровня – а также производителей, поставщиков и клиентов.
- Контактные лица ваших поставщиков из оперативных групп обеспечения безопасности продуктов и лица, ответственные за принятие ответных мер.
- Политики, которые устанавливают уровень поддержки клиентов, порядок классификации и отслеживания источников атак, методы принятия ответных мер (например, будет ли применяться в вашей инфраструктуре сброс пакетов, формирующих атаку?).
- Процедуры ответов на вопросы и процедуры взаимодействия.

Результаты внедрения Cisco SOC

В результате функционирования центра Cisco SOC должны появляться следующие результаты, многие из которых будут выдаваться в форме отчетов:

- Мониторинг безопасности в целях управления рисками.
- Анализ рисков для определения состояния безопасности.
- Надежный доступ к порталу мониторинга безопасности с использованием ролевой модели контроля доступа.
- Мониторинг в режиме реального времени; установление состояния обработки инцидентов и ведение учетных карточек.
- Отчеты о политике безопасности.
- Отчеты об инцидентах в сфере безопасности.
- Экспертиза инцидентов в режиме реального времени, а также оформление еженедельных и ежемесячных отчетов.

- Информация, требуемая для подготовки к аудиторской проверке соблюдения нормативных требований.
- Отчеты по договорам SLA.
- Подтверждение соблюдения политики безопасности.
- Динамика инцидентов и событий в сфере информационной безопасности.

Важная роль отчетности

Как можно заключить на основании перечисленных результатов, отчетность играет исключительно важную роль в эффективной работе вашего центра Cisco SOC. В конечном итоге, вы разработаете собственные стандарты отчетности об инцидентах, но, в соответствии с накопленным практическим опытом, в ваших отчетах должны присутствовать некоторые общие составляющие, в частности, время и дата реакции на инцидент, идентификационные данные и результаты классификации атаки, основная причина, метод обнаружения, метод отражения и результаты анализа рисков (т.е. как можно избежать возникновения этой проблемы в будущем).

Кроме этого, не следует обнародовать информацию, которая может негативно отразиться на функционировании центра Cisco SOC или сделать вас уязвимой мишенью для хакеров. Другими словами, проявите надлежащее внимание на этапе окончательного оформления отчетов. В дополнение к этому, если ваши отчеты об инцидентах могут быть преданы гласности (как это происходит при предоставлении отчетов федеральным и местным органам власти), перед публикацией содержание этих отчетов должен оценить ваш специалист по связям с общественностью или юрисконсульт.

Содержание отчетов об инцидентах

Для того чтобы повысить ценность ваших отчетов об инцидентах, по возможности указывайте время в стандарте UTC (по Гринвичу) применительно ко всей инфраструктуре маршрутизации и коммутации, инструментам обеспечения безопасности и критически важным серверам. Стандартизация по UTC предоставит вам возможность сформировать общий временной базис для простой консолидации и объединения данных, поступающих от сенсоров. Сведя к минимуму пересчет времени, вы устраните риск случайного искажения собранных сведений.

Проследите за тем, чтобы в списки контактных лиц были включены все люди, которые участвовали в обработке с инцидентом, и указаны их роли. Эта информация исключительно важна для анализа инцидентов и борьбы с инцидентами сходного характера. И, наконец, предоставьте доступ к вашим отчетам через портал мониторинга безопасности. На этом портале должна быть отражена последовательная картина состояния безопасности в масштабах всей сети.

Заключение

Центр мониторинга и управления безопасностью Cisco поможет вам защитить сети и информационный трафик ваших клиентов от угроз в сфере информационной безопасности. Cisco SOC объединяет технологии, процессы и человеческие ресурсы, формируя комплексную систему защиты. Высокая степень готовности и соблюдение систематического процесса реакции на инциденты в сфере безопасности, поможет избежать или сгладить последствия потенциально разрушительных атак, которые обрушиваются на сети ваших клиентов.

Узнайте у представителя Cisco о выгодах, которые может принести внедрение центра мониторинга и управления безопасностью вам и вашим клиентам.

Cisco Systems
Россия, 115054, Москва,
бизнес-центр
«Риверсайд Тауерс»
Космодамианская наб., 52,
стр. 1, этаж 4
Тел.: +7 (495) 961 14 10
Факс: +7 (495) 961 14 60
www.cisco.ru
www.cisco.com

Cisco Systems
Россия, 191186,
Санкт-Петербург,
бизнес-центр «Регус»
Невский проспект, 25,
этаж 2, офис 30
Тел.: +7 (812) 346 77 17,
Факс: +7 (812) 346 78 00
www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099,
Алматы,
бизнес-центр «Самал 2»
Ул. О. Жолдасбекова, 97,
блок А2, этаж 14
Тел.: + 7 (3272) 58 46 58
Факс: + 7 (3272) 58 46 60
www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004, Киев,
бизнес-центр
«Горайзон Тауерс»
Ул. Шовковична, 42-44,
этаж 9
Тел.: + 7 (38044) 490 36 00
Факс: + 7 (38044) 490 56 66
www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • SAR • Hungary • India • Indonesia • Ireland • Israel •Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe