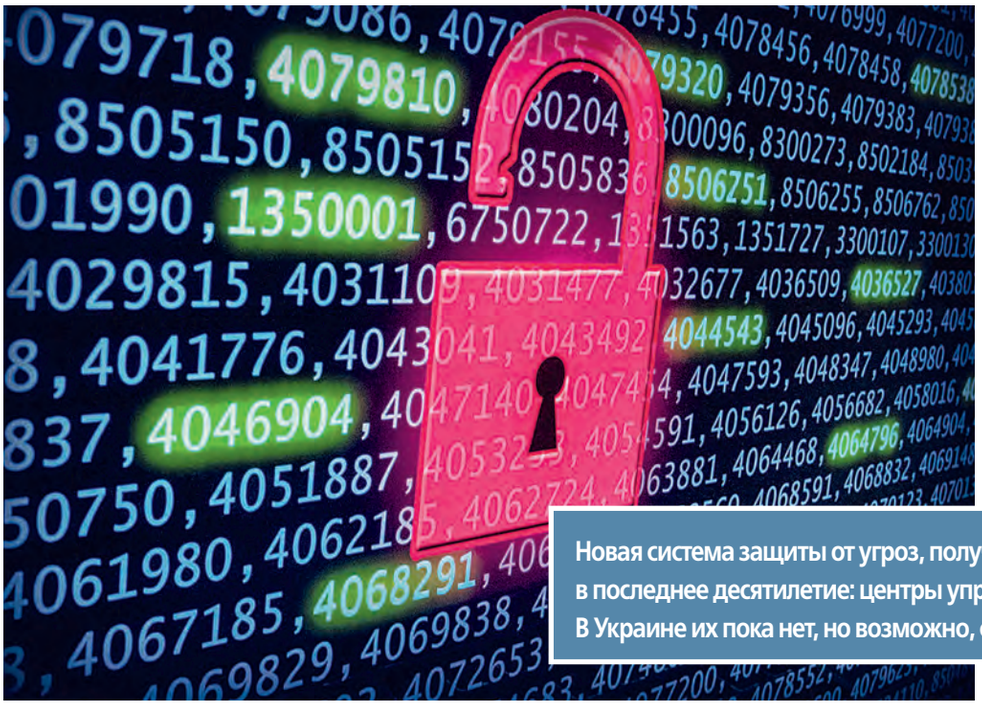
Не грози киберзащитному централу, или зачем нужен SOC



Новая система защиты от угроз, получившая распространение в последнее десятилетие: центры управления безопасностью (SOC). В Украине их пока нет, но возможно, скоро появятся.

Сакраментальная фраза, что компании должны больше внимания уделять информационной безопасности, уже доходит до самих адресатов. Эпидемии шифровальщиков, которые мы видели на примере Petya.A и WannaCry; целенаправленные атаки, которые могут готовиться месяцами; проникновения с помощью методов социальной инженерии, — словом, ландшафт угроз богат и разнообразен, и с годами ситуация будет только ухудшаться. При этом аналитики говорят о том, что множество случаев взлома так и остаются незамеченными или обнаруживаются спустя значительное время, которое может измеряться неделями. Можно услышать и более радикальное мнение: абсолютной защиты не существует, при желании взломают любого, а потому нужно действовать на опережение.

Видимость сети обеспечивает система управления событиями безопасности (SIEM), ведущая мониторинг в реальном времени и уведомляющая ИТ-персонал об инцидентах. Однако и этого уже недостаточно: определяющую роль играет время реакции — нужно успеть остановить атаку до того, как вред нанесен, и тут не обойтись без специализированного персонала, который отвечает за безопасность в круглосуточном режиме.

Эту задачу выполняют центры управления безопасностью (Security Operations Center — SOC), иначе «центры мониторинга и реагирования». Ключевое слово здесь — «реагирование»: персонал SOC должен не только выявить аномалию, но и оперативно уведомить соответствующих сотрудников, которые и примут меры для нейтрализации угрозы.

Анатомия SOC

Существуют разные модели построения SOC. В больших корпорациях он может функционировать как выделенное подразделение со штатными сотрудниками. Преимущество такого подхода заключается в том, что персонал внутреннего SOC наиболее близко знаком с инфраструктурой предприятия и получает наиболее полную информацию обо всех событиях. Обратная сторона медали — высокие начальные затраты на организацию центра и возможные трудности с набором квалифицированного персонала. Кроме того, построение собственного SOC может растянуться во времени.

Альтернативный подход, как обычно в наше время, — это виртуальный SOC. Существуют специализированные компании, предоставляющие услуги контроля безопасности. Виртуальный SOC — это бюджетный вариант, организациям не нужно тратиться на создание и круглосуточную работу собственных центров. При этом к их услугам персонал с высокой квалификацией, который имеет опыт работы с предприятиями разных сфер деятельности и имеет доступ к большим объемам данных об угрозах. Недостатки этого варианта типичны для аутсорсинговых сценариев — это меньшая гибкость и ограниченная возможность учета специфических запросов клиента, а также то, что чужие сотрудники хуже знают специфику предприятия, в силу чего передача оповещения нужным специалистам может занимать больше времени. Кроме того, обслуживающая компания имеет доступ к данным заказчика.

Возможна и промежуточная (гибридная) схема, когда имеется небольшой внутренний SOC, дополняемый поддержкой со стороны аутсорсера. Это обеспечивает экономию средств, быстрое реагирование на инциденты, а также дополнительное обучение для персонала заказчика благодаря совместной работе со специалистами обслуживающей фирмы. При этом остается необходимость обработки данных на стороне, и еще одним недостатком по сравнению с «виртуальным» SOC могут быть более высокие расходы в долгосрочной перспективе, поскольку нужно тратиться и на оснащение собственного подразделения, и на услуги сторонней компании.

Схему организации и функциональность центра управления безопасностью можно рассмотреть на примере одного из существующих аутсорсинговых SOC. На низовом уровне обслуживающая компания обеспечивает эксплуатацию и администрирование систем информационной безопасности заказчика (анти-DDoS, анти-APT, NGFW, IPS, «песочницы», системы контентной фильтрации и т.д.), осуществляя настройку, удаленную профилактику, проведение обновлений и прочие работы. Также возможна аренда лицензий на функции защиты по схеме SaaS.

В случае инцидента сотрудники SOC проводят его анализ, собирая информацию с серверов, рабочих станций и сетевого оборудования, формируют выводы о его причине, сопутствующих последствиях, а также выдают рекомендации по блокированию развития инцидента и его возможного повторения. Компания проводит исследование скомпрометированных компьютеров и самих вредоносных программ, выявляя механизм их работы.

Для анализа внешней обстановки используются репутационные базы данных — как внутренние, так и сторонние (в том числе полученные от групп реагирования на компьютерные чрезвычайные ситуации — CERT), а также партнерских сервисов по OSINT-оценке интереса к компании со стороны киберпреступников.

Большой блок функций контроля защищенности включает в себя ряд услуг. Управление уязвимостями инфраструктуры предусматривает сканирование и сопровождение их устранения (приоритизация исходя из особенностей инфраструктуры клиента, разработка рекомендаций для ИТ-специалистов относительно закрытия наиболее критичных «дыр» и контроль этого процесса). Возможно и подтверждение актуальности выявленных уязвимостей путем их контролируемой эксплуатации. SOC берет на себя анализ уровня защищенности периметра и веб-сервисов от атак, по итогам которого готовит рекомендации относительно улучшения защиты. Также специалисты обслуживающей организации могут провести аудит состояния информационной безопасности, подключив инфраструктуру заказчика к своей системе мониторинга. Возможен и тест на проникновение с целью выявления брешей в защите инфраструктуры, в том числе в рамках «оценки зрелости» внутреннего SOC.

Ключевая группа функций SOC — мониторинг инцидентов информационной безопасности. Центр обеспечивает круглосуточный сбор, корреляцию и анализ данных о событиях информбезопасности как в сети, так и на уровне пользователей. SOC выявляет аномалии в работе бизнес-приложений, идентифицирует изменение критичных файлов на рабочих станциях. SOC также собирает журнальные данные с ключевых систем, средств защиты и сетевой инфраструктуры, эти данные недоступны сотрудникам заказчика и могут использоваться для отчетности и расследования инцидентов. Сводная информация об уровне защищенности организации, «слабых местах» в системе и обнаруженным инцидентам выводится в графическом виде.

Статистика потребностей

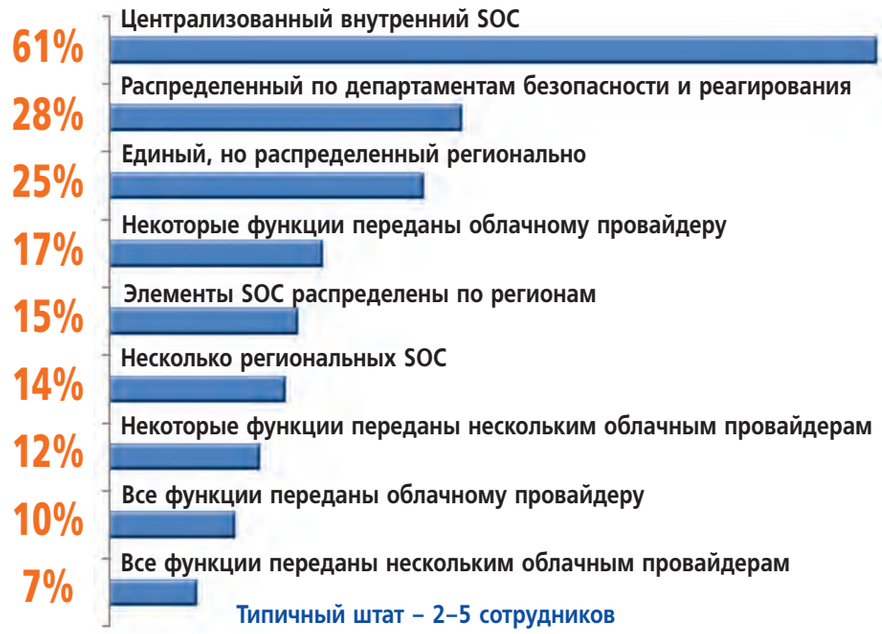
По данным организации ***SANS Institute***, которые приводятся в тематическом отчете, вышедшем в мае, большинство организаций предпочитают иметь свой собственный SOC, сосредоточенный в одном месте (которое, впрочем, не обязательно совпадает со штаб-квартирой). Однако возможные типы архитектур не ограничиваются тремя сценариями: есть и переходные формы. Так, второй по популярности вариант — тоже внутренний SOC, но с разделением функций между различными департаментами (информационной безопасности, реагирования на инциденты, контроля за соблюдением нормативно-правовым документам и т.д.). В ином случае SOC может быть распределен территориально между региональными подразделениями компании, либо это могут быть несколько полноценных центров в регионах. Варианты аутсорсинга также разнообразны: частичная или полная передача функций сторонней организации или нескольким «облачным» SOC.

При этом 78% респондентов (а это чуть более трех сотен компаний, представляющих разные сферы экономики, от кибербезопасности до отельно-ресторанного бизнеса и прессы) сообщили, что такие стратегические элементы, как планирование «дорожной карты» и построение архитектуры безопасности, они оставляют в ведении собственных служб безопасности. На аутсорсинг — полностью или частично — чаще всего передаются такие функции, как исследование угроз, цифровая криминалистика (расследование инцидентов — кстати, самый популярный вид деятельности, к которой привлекают сторонние организации) и поиск доказательств в электронных данных для использования в суде.

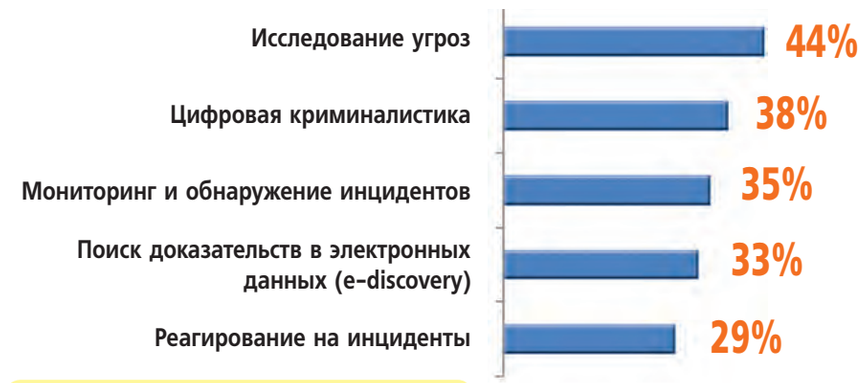
Еще одним важным аспектом функционирования SOC названо взаимодействие с центром управления сетью (Network Operations Center — NOC), обеспечивающим контроль инфраструктуры связи. Большинство компаний, опрошенных SANS, заявили, что у них либо вовсе нет NOC, либо он никак не связан с SOC, а взаимодействие бывает в случае чрезвычайных ситуаций, и лишь у 12% респондентов оба центра технически интегрированы. Между тем взаимодействие между SOC и NOC должно улучшить возможности обнаружения и реагирования на инциденты, поскольку оба имеют одну цель — защиту информационной инфраструктуры и обеспечение работы сети.

Изначально центры управления безопасностью создавались из расчета предотвращения атак и быстрого реагирования на инциденты. Однако, как отмечает вице-президент компании ***FourV Systems*** Кейси Коркоран, поскольку ИТ-безопасность традиционно финансировалась по остаточному принципу, производители наводнили рынок множеством специализированных продуктов, способных обнаруживать даже самые скрытые вирусы. В результате SOC вынуждены обрабатывать многочисленные потоки данных и формировать отчеты, которые никто не читает из-за их избыточности. Поэтому путь развития SOC может лежать в сторону внедрения концепции обеспечения, анализа и отчетности в сфере безопасности (Security Operations, Analysis and Reporting — SOAR), которую представил Gartner в прошлом году. SOAR призван упорядочить данные, генерируемые

Наиболее распространенные функции и архитектуры SOC (по данным института SANS)



Самые популярные архитектуры SOC (по данным института SANS)



Функции SOC, которые чаще всего полностью или частично передаются сторонним провайдерам (по данным института SANS)

разными системами безопасности, приоритизировать меры по обеспечению безопасности и автоматизировать меры по ликвидации последствий.

Продукты и решения

Услуги SOC предоставляют некоторые производители решений информационной безопасности. Такие компании обладают опытом противодействия угрозам и специализированными командами, которые собирают и анализируют данные о вредоносном коде, а потому могут взять на себя функции контроля безопасности других организаций.

Например, у ***Cisco*** такое подразделение носит название Incident Response Retainer Service. Для сбора информации об угрозах и их анализа компания использует свою службу расследования угроз Talos. Компания обещает, что в течение 4 часов после проникновения в систему ее специалисты свяжутся с заказчиком, а в течение 24 часов — прибудут на место происшествия.

Центр управления безопасностью компании ***Symantec*** входит в состав подразделения внешнего управления Symantec Managed Security Services. В его работе задействованы специализированные группы: DeepInsight Intelligence (сбор и анализ информации об угрозах), Incident Response Services (собственно реагирование на инциденты) и Security Simulation (тестирование на реальных атаках и моделирование угроз).

F5 может предложить такие услуги, как оповещение о подозрительной активности в реальном времени, «облачные» службы Silverline (защита от DDoS-атак и шлюз контроля приложений), получение информации о серверах, куда злоумышленники загружают украденные учетные данные (Drop Zone Analysis), мониторинг угроз в реальном времени и даже закрытие фишинговых и других злонамеренных сайтов. Сервис включает в себя пользовательский портал, где можно просмотреть отчеты и пообщаться со специалистом компании.

Виртуальный центр обеспечения безопасности ***Raytheon*** (V-SOC), по заявлению компании, специализируется на выявлении продвинутых угроз, тогда как традиционные атаки, не сопряженные с большими рисками, обрабатываются автоматически с помощью платформы Automated Threat

Intelligence Platform (ATIP) с технологией машинного обучения. Система не ограничивается генерацией уведомлений об инцидентах, а анализирует тактику, приемы и процедуры, применяемые злоумышленниками, что позволяет выявлять атаки через «уязвимости нулевого дня», новые продвинутые угрозы, утечку данных, подозрительное поведение сотрудников и другие опасные явления. При этом для каждого клиента создается виртуальный рабочий стол, который изолирован от других заказчиков и уничтожается при разъединении, тем самым обеспечивается сохранность данных, которые не покидают сети заказчика. Кроме того, Raytheon предлагает поддержку персонала заказчика в ночные часы, во время выходных, праздников и т.д.

Из разработчиков решений для SOC можно выделить компанию ***SOC Prime***, которая на них и специализируется. SOC Prime предлагает несколько продуктов, ключевые из них — система автоматизации управления Predictive Maintenance и платформа аналитики и визуализации угроз CyberView. Партнером SOC Prime в Украине является компания Integrity Vision.

Fortinet предлагает аппаратное решение для построения центров управления безопасности, делая упор на организации взаимодействия между SOC и NOC. В основе решения лежит система управления событиями FortiSIEM, тогда как FortiAnalyzer отвечает за аналитику, отчетность и оповещение об инцидентах, а FortiManager — за управление устройствами, тогда как данные об угрозах доступны благодаря команде «цифровой разведки» FortiGuard.

Добавим, что услуги SOC или решения для их организации предлагают и другие компании, известные и не очень.

А что у нас?

Насколько удалось установить, полноценных SOC в Украине пока нет. Нередко под этим термином понимают само ядро такой структуры, то есть SIEM, однако настоящих центров управления безопасностью, по-видимому, не создано. Правда, известно, что своими SOC владеют международные компании, работающие в Украине, но они ориентированы на обслуживание клиентов в других странах, хотя физически персонал находится здесь.

В июле СБУ подписало с НАТО соглашение «О реализации трастового фонда Украина–НАТО по вопросам кибербезопасности». Документ предусматривает построение сети ситуационных центров реагирования на компьютерные инциденты, а также создание центров кибербезопасности Вооруженных сил Украины и Национальной полиции с их последующей интеграцией в общегосударственную сеть ситуационных центров.

Кроме того, есть мнение, что местный бизнес также проявляет интерес к SOC. Данных о конкретных проектах пока нет, но если будет и дальше штормить, появление таких объектов не за горами.

Василий ТКАЧЕНКО, СиБ

НОВОСТИ
ВИДЕОКОНФЕРЕНЦСВЯЗЬ

Первая киевская конференция Trend Micro по кибербезопасности

Компания Trend Micro 26 сентября 2017 года провела в Киеве конференцию Security TRENDS 2017, посвященную проблемам кибербезопасности. Как известно, в июле начало работать представительство вендора в нашей стране, региональным менеджером которого стал Роман Черненький.

Открыл конференцию управляющий директор Trend Micro в Тихоокеанском регионе и странах Азии Даня Таккар, который говорил о новых вызовах, возникающих в связи с цифровой трансформацией. К примеру, стремясь обеспечить сохранность ценной информации, которая является «нефтью» цифровой экономики, компании тратят много усилий на предотвращение вторжений. Однако в реальности периметр сети как таковой больше не существует, данные могут находиться где угодно, а вредоносный код способен проникнуть в сеть незаметно. В среднем факт целенаправленной атаки обнаруживается в течение пяти месяцев, причем только в 53% случаев благодаря действиям подразделения ИБ самой компании.

Современный ландшафт угроз обрисовал Михаил Кондрашин, технический директор Trend Micro в СНГ, Грузии и Монголии. Он сообщил, что альянс Zero Day Initiative, основанный в свое время еще компанией TippingPoint (ныне в составе Trend Micro), за первое полугодие выявил 382 уязвимости, информация о которых передана разработчикам. Главным же провалом на рынке стала атака вируса WannaCry, ущерб от которого достиг $4 млрд. Еще $5,3 млрд на сегодняшний день составляют потери от нового вида кибератаки – Business Email Compromise, когда финансовые отделы получают поддельные письма от руководства с распоряжением о переводе денег. Такие атаки трудно опознать, поскольку злоумышленники тщательно копируют стиль переписки. Появились и новые вымогатели – Cerber, который избегает обнаружения механизмами машинного обучения, и поражающая Android-устройства программа Slocker, которая не только блокирует телефон, но и шифрует файлы. Опасность представляют и подключенные к Интернету устройства, которые легко взломать – от IP-камер до промышленных маршрутизаторов и роботов. Например, удаленное изменение программы калибровочных параметров механизмов может вылиться в выпуск продукции с микродефектами. Специалисты Trend Micro также ознакомили посетителей с решениями производителя и их возможностями по защите инфраструктуры сетей.

Даня Таккар во время выступления на конференции Security TRENDS 2017 в Киеве