SOC, или Наука управления безопасностью

Задача SOC — отследить и пресечь любой инцидент или атаку, лучше всего еще до ее начала. В будущем это будет происходить автоматически, но пока основная проблема — кадры.

Центры управления кибербезопасностью (SOC) — следующий этап организации защиты от атак, которые становятся все многочисленнее и изощреннее. SOC объединяет в себе технические решения (сенсоры, систему сбора информации — SIEM, средства аналитики) и квалифицированный персонал, который обрабатывает информацию об аномалиях в сети и принимает меры в зависимости от ситуации. Передать киберзащиту на аутсорсинг в SOC — неплохой выход для компаний, которые не могут себе позволить необходимых расходов на это направление.

Коммерческих SOC, берущих на себя защиту других компаний, в мире уже столько, что составляются рейтинги типа первой сотни. За последние годы несколько таких организаций открылось и в Украине. «СиБ» выясняет, чем они оснащены, какие услуги предлагают и вообще как устроен типичный день в SOC.

SOC как услуга

Исследовательская организация ***SANS Institute*** определяет SOC как «*сочетание людей, процессов и технологий, защищающих информационные системы организаций посредством упреждающего проектирования и конфигурирования, постоянного мониторинга состояния систем, выявления непредусмотренных действий или нежелательных состояний, а также минимизации ущерба от нежелательных последствий*».

Есть несколько моделей работы центров кибербезопасности. Самый дешевый вариант — «виртуальный SOC», когда функции киберзащиты возлагаются на существующий персонал (например, ИТ-отдел), выделенного помещения может и не быть, а под SOC понимаются скорее процессы обеспечения безопасности. Возможен и гибридный вариант, когда часть функций защиты обеспечивается на месте, а другие передаются на аутсорсинг в какой-нибудь коммерческий SOC. Если компания строит свой собственный, т.н. «выделенный» SOC, это уже сопряжено с серьезными затратами на закупку технических решений, набор и содержание команды специалистов, а также разработку и внедрение процессов, хотя такой центр, конечно, обеспечивает полный контроль за безопасностью предприятия. Крупные географически разнесенные организации, а также холдинги, включающие бизнесы разной направленности, могут иметь несколько центров кибербезопасности, управляемых из т.н. «командного SOC».

Собственно коммерческие SOC также называются ***провайдерами управляемого сервиса безопасности*** (Managed Security Service, MSS). Gartner определяет MSS как услугу, удовлетворяющую трем требованиям:

- круглосуточный удаленный мониторинг событий и источников данных, имеющих отношение к безопасности;
- обеспечение защиты удаленно из SOC, а не сотрудниками на месте, и как коммерчески доступный сервис, а не услуга для единственного потребителя;
- администрирование и управление техническими средствами ИТ-безопасности.

Кроме мониторинга событий, SOC может предоставлять другие услуги. Например, управление межсетевыми экранами, системами IDS/IPS и другими устройствами, реагирование на инциденты (удаленно или с выездом на место), оценку уязвимостей с сопутствующими действиями (сканирование, анализ и выработка рекомендаций). Возможен и сервис киберразведки — Cyber Threat Intelligence, CTI (например, мониторинг Dark Web и социальных сетей на предмет специфичных для заказчика угроз). По мере того как компании внедряют облачные

технологии, расширяется и охват услуг удаленного мониторинга, который теперь распространяется на сервисы, предоставляемые из облака и на среду «Интернета вещей».

Gartner в своем майском отчете ***Magic Quadrant for Managed Security Services, Worldwide*** отмечает, что поставщики MSS-услуг постоянно расширяют спектр своих предложений. Реально наибольшим спросом пользуются базовый сервис мониторинга и блокирование атак. При этом простого оповещения об инцидентах уже недостаточно. Даже организации, у которых есть свои отделы ИТ-безопасности, хотят получать расширенные сведения (например, идет речь об обычном заражении или о целенаправленной атаке, были ли на пораженном компьютере незакрытые уязвимости и т.д.). Те, у которых система безопасности не выстроена, а сотрудников мало, хотят, чтобы SOC принимал более активное участие в диагностике, локализации и расследовании инцидентов. Среди других технологических тенденций Gartner отмечает выпуск провайдерами SOC-услуг собственных мобильных приложений, что упрощает доступ к информации. Например, аналитик или офицер безопасности может оперативно получать все данные об инциденте, даже когда под рукой нет компьютера, чтобы зайти на веб-портал SOC.

Заказчиков интересуют сервисы, закрывающие бреши в защите предприятия; многие видят потребность в «гигиене безопасности», привлекая MSS-провайдеров для управления уязвимостями. В то же время услуги удаленного управления и администрирования все менее актуальны, поскольку они покрываются более широким кругом провайдеров (например, управление межсетевыми экранами берут на себя операторы связи, также многие сервисы безопасности поставляются из облака). С другой стороны, MSS-провайдеры ищут варианты управления системами, которые обычно не предлагаются «как услуга» (например, SIEM и EDR).

Мировой рынок SOC

Gartner в упомянутом выше отчете оценивает рынок MSSP 2018 года в $10,9 млрд. В Интернете можно найти пресс-релизы многочисленных исследований, посвященных оценкам и прогнозам развития этого сегмента на ближайшие годы.

Например, согласно свежему отчету Kenneth Research, объем мирового рынка SOC в нынешнем году составит почти $31,8 млрд, а к 2025-му достигнет почти $61,2 млрд при среднегодовом росте на уровне 11,5%. Наибольшая доля принадлежит Северной Америке благодаря как сильной экономике, так и принимаемым мерам по внедрению киберзащиты на предприятиях. Азиатско-Тихоокеанский регион будет демонстрировать наиболее высокий рост благодаря развивающимся экономикам. Среди типов SOC преобладают внутренние (in-house), хотя все большей популярностью пользуется гибридная модель. Market Research Future прогнозирует, что к 2025-му рынок достигнет $52,81 млрд при годовом росте 10,4%.

Компания Mordor Intelligence рассматривает рынок коммерческих центров кибербезопасности (SOC as a service), прогнозируя в ближайшей перспективе (до 2024 года) среднегодовой рост на уровне 25%, что является очень солидным показателем. При этом рынок сильно фрагментирован — сколько-либо доминирующих игроков на нем нет. В региональном разрезе агентство также выделяет Северную Америку, что объясняется присутствием там нескольких сильных игроков в сочетании с ростом числа кибератак (в частности, на США приходится более 18% числа атак вымогателей). Кроме того, агентство обращает

PRIME PC™

Зроблено без компромісів

Потужні, надійні, функціональні сервери і ПК

it-integrator.ua

внимание на намерение администрации Дональда Трампа выделить более $19 млрд на инициативы, связанные с кибербезопасностью.

Из секторов экономики наиболее существенный рост прогнозируется в сферах банковских, финансовых и страховых услуг, поскольку эти предприятия имеют дело с большими объемами чувствительной информации и терпят самые крупные убытки от киберпреступности (в среднем порядка $18,3 млн на компанию). Кроме того, в этих отраслях действует жесткое государственное регулирование.

Факторы, сдерживающие развитие SOC, так или иначе связаны с высокой стоимостью их организации и поддержки. Компания, предоставляющая услуги SOC, должна вложиться не только в приобретение технических решений, но и в постоянную адаптацию к изменяющейся обстановке, в том числе покупку дополнительных технологий для противостояния новым угрозам. Также для эффективной работы SOC нужны квалифицированные специалисты из разных областей — телекоммуникаций, ИТ и информационной безопасности. При этом компании сталкиваются с высокой текучестью кадров, а это негативно сказывается на росте рынка услуг коммерческих SOC. Однако выгоды оправдывают все эти затраты, особенно для крупных компаний, заключает Mordor Intelligence

В июле SANS Institute опубликовал ежегодный отчет, посвященный лучшим практикам SOC. Из результатов опроса следует, что почти 80% центров кибербезопасности не занимаются аутсорсингом: 58% заявили, что не предоставляют услуг сторонним организациям, и еще 22% охарактеризовался себя как внутренних провайдеров (что не соответствует критерию Gartner для MSSP). Большинство компаний, в которых есть SOC, относятся к сфере кибербезопасности, государственным организациям или банковскому сектору (**рис. 1**).

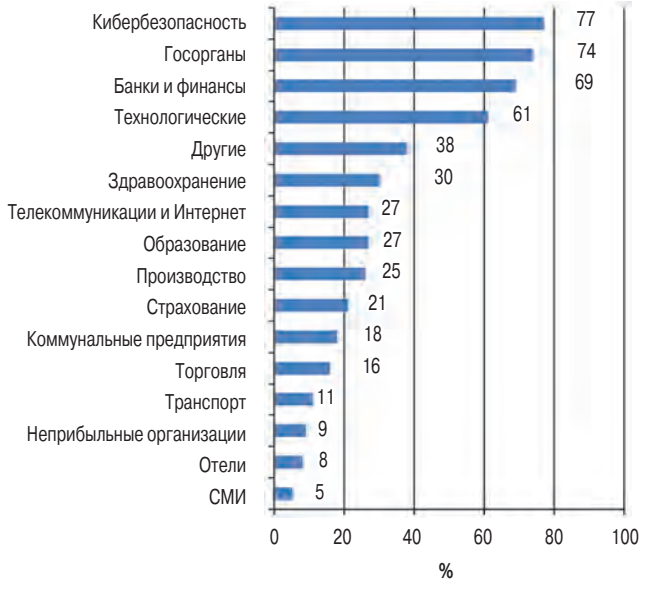

Рис. 1. Сферы деятельности предприятий, в составе которых есть SOC (по ответам респондентов SANS Institute, 2019 год)

А вот еще несколько интересных цифр. Географически больше всего SOC находится опять-таки в Северной Америке (57% в США + 4% в Канаде), на втором месте Европа (17%), на третьем Юго-Восточная Азия (10%). Число сотрудников в большей части SOC составляет 2–5 человек. Для сопоставления и анализа данных в основном используется SIEM, хотя также в ходу платформы Threat Intelligence, системы управления журналами, решения для автоматизации и оркестрации, и даже «самописные» панели мониторинга.

SANS Institute также спрашивал о проблемах и препятствиях, с которыми сталкиваются SOC (**рис. 2**). Чаще всего жалобы связаны с нехваткой квалифицированного персонала, недостаточной интеграцией различных инструментов и малым уровнем автоматизации.

Рис. 2. Основные проблемы, с которыми сталкиваются SOC (источник: SANS Institute, 2019 год)

Гуру рекомендуют

В начале года сайт Digital Guardian опросил экспертов в отрасли кибербезопасности относительно того, какие сотрудники, технологии и процессы необходимы для построения SOC. Если свести воедино высказанные рекомендации, то общие правила в итоге таковы.

Сотрудников SOC рекомендуется разделить на три линии. Первая занимается выявлением и идентификацией проблем и инцидентов, а также поиском решений для их устранения. Обычно именно эти сотрудники взаимодействуют с заказчиком. Вторая линия отвечает за собственно нейтрализацию атак, выявленных первой. Третью линию составляют самые опытные и технически подкованные специалисты, которые также занимаются разработкой процессов и инструментов для поиска угроз (Threat Hunting). Для работы в SOC нужен высококвалифицированный персонал, который хорошо разбирается в базовых событиях и сценариях безопасности, а также умеет адаптироваться и находить нестандартные решения, поскольку ландшафт угроз постоянно меняется, а атаки могут приобретать разные формы.

Если SOC имеет несколько площадок или удаленных сотрудников, находящихся в разных временных зонах,

19-дюймові пристрої безпеки

Пристрої безпеки mGuard в 19-дюймовому форматі від Phoenix Contact

Пристрій mGuard centerport — це комбінація сучасного брандмауера і високопродуктивних шлюзів VPN в 19-дюймовому форматі. Пристрій включає в себе Gigabit Ethernet, багатоядерну архітектуру та великий резерв потужності. Таким чином mGuard centerport без проблем масштабується з постійно зростаючим числом VPN-з'єднань та захищених сегментів мережі. Постійна якість передачі для критично важливих IP-служб забезпечується навіть при максимальному навантаженні.

ТОВ "Фенікс Контакт" (Україна)
+38 044 594 55 22
phoenixcontact.ua/cybersecurity

PHOENIX CONTACT
INSPIRING INNOVATIONS

его персонал может работать в режиме «следования за солнцем» (то есть в локальные рабочие часы). Если офис один, инженеры работают посменно. При восьмичасовом рабочем дне, с учетом выходных, отпусков и т.д., для круглосуточной работы на одно рабочее место нужно 4,5 сотрудника.

Технические средства SOC также могут быть разбиты на три части. Первая — это источники данных: сетевые устройства (IDS/IPS, межсетевые экраны, сканеры уязвимостей), рабочие станции (антивирусы, журналы ОС и т.д.), системы авторизации (LDAP, Active Directory), внутренние и внешние источники данных об угрозах. Вторая часть — SIEM, которая сопоставляет приходящие данные, выявляет инциденты и оповещает инженеров. Наконец, третья составляющая — система сопровождения инцидентов (ticketing system), которая используется для отслеживания истории событий и взаимодействия с клиентом. В SOC должен быть составлен набор инструментов для проведения аудита инфраструктуры, тестов на проникновение и различного анализа.

Здание SOC должно быть запитано от нескольких источников (например, в дополнение к электросети должны быть установлены дизель-генератор или солнечно-аккумуляторная система). Нужно также резервировать каналы интернет-доступа. Рекомендуется хранить копии данных где-нибудь за пределами центра.

Особое внимание следует уделять безопасности самого SOC, прежде всего допуску в здание центра. Тщательная проверка необходима и при подборе сотрудников. Также обязательно соблюдение политики «чистого стола» (на рабочем месте не должно оставаться никаких бумаг). Кроме того, персонал нужно научить распознавать атаки с применением методов социальной инженерии.

С другой стороны, SOC должен обеспечивать комфортные условия для людей, которые в нем работают. «Слишком многие SOC как будто построены главным образом для руководителя, который заходит в комнату пару раз в день и хочет видеть стену экранов и табло с метриками безопасности, KPI и оперативными сводками, — высказался один из консультантов. — Проектируя SOC, позаботьтесь об эргономических потребностях операторов, которые будут работать в нем круглые сутки».

Инструменты для SOC будущего

Независимо от направленности любой SOC выполняет ряд задач, базовой из которых является мониторинг событий и реагирование на них (***Managed Detection & Response, MDR***). Основной инструмент для этой цели — SIEM, система управления информационной безопасностью, которая собирает информацию от разных устройств, анализирует ее, представляет в удобном для восприятия виде и выдает уведомления о событиях. SIEM является «сердцем» SOC, обеспечивающим возможности MDR.

АВТОМАТИЗАЦИЯ — ПАЛКА О ДВУХ КОНЦАХ

В сфере кибербезопасности, как собственно и везде, недостаточно купить технологию – надо еще найти специалистов с нужными компетенциями. Затем возникают две серьезные проблемы: удержание этих сотрудников, потому что на них идет охота, да им и самим неинтересно сидеть на одном месте и защищать одну и ту же инфраструктуру, не развивая свои навыки и не получая опыт в полном объеме; а вторая – все-таки нужно выстроить устойчивый процесс взаимодействия всей команды. Среди клиентов наших SOC-сервисов – компании, у которых есть средства, но нет времени и концентрации ресурсов на данном направлении; они составляют один тип клиентов. С такими компаниями мы детально прорабатываем те контроли информационной безопасности, которые они бы хотели отдать нам на аутсорсинг. Зачастую для отработки большинства начальных контролей не нужно обладать какими-то особенными технологиями и знаниями, это довольно тривиальные вещи, но они задействуют большую часть ресурса клиентов, после чего не остается времени на стратегическое развитие кибербезопасности. Другая категория – когда уже случился некий инцидент и компании начинают понимать, что по кибербезопасности у них не все гладко. Первым делом они заказывают расследование, если факт инцидента подтвержден, или анализ компрометации, если наблюдаются аномалии в поведении инфраструктуры. И если действительно целенаправленная атака имеет место быть, то когда мы объясняем, как происходила атака, глаза часто округляются: «Как, у нас тут проходной двор?».

Такие примеры, как NotPetya, BlackEnergy, уже являются хрестоматийными, их проходят даже в западных институтах, куда мы ездим с открытыми лекциями. Нужно отметить, что уровень автоматизации большинства этапов атаки, включая проникновение и захват инфраструктуры за последние 3–4 года, значительно вырос. Мы со своей стороны внедряем ИИ, машинное обучение, глубокий анализ данных (Data Mining) и т.д., в то время как преступники делают то же самое. И часто они на шаг впереди, потому что у них ресурс куда солиднее, черный рынок оценивается как минимум в 6 раз больше, чем белый.

Благодаря высокому уровню автоматизации снизился и порог входа хакеров на рынок кибератак. Если вчера злоумышленник грабил магазины, то сейчас после непродолжительного обучения уже может заниматься обналичиванием «белого пластика», выполнять заказы на составление фишинговых писем или обслуживание бот-сетей. Каких-то особо глубоких компетенций уже не нужно – достаточно быть опытным пользователем ПК. И для нас, специалистов кибер-безопасности, это большая проблема.

Артем МИХАЙЛОВ,
директор по коммерческим решениям компании ISSP

К счастью или к сожалению, но банальных нарушений политик безопасности самими пользователями больше, чем элементов реальных атак в общем количестве фиксируемых инцидентов. Но все эти нарушения, которые выглядят некритично, создают туман в профилировании поведения ИТ-сервисов и учетных записей, хаос, в котором легко затеряться хакеру, потому что его поведение не покажется аномальным, а скорее будет выглядеть в точности как действия легитимного администратора, систематически нарушающего определенную политику. Если заказчик не старается решить проблему, это мешает качественному выявлению.

Сейчас затишье в информационном поле и вроде как нет информации о громких взломах. Это не в последнюю очередь благодаря тому, что и мы работаем, и наши конкуренты-партнеры, и CERT-UA, и СБУ, и Киберполиция. Но это не значит, что все позади. Речь не только о криминалитете: у наших недругов официальная доктрина гибридной войны подразумевает активные кибероперации. Поэтому не поддавайтесь на иллюзию безопасности, не полагайтесь на то, что если все тихо, то все хорошо. Если посмотреть на траекторию всех предыдущих атак, то сейчас как раз время, когда активно идет захват, как мы это называем, высот в киберпространстве. Причем ведь хакеры взламывают организации не потому, что есть заказ на них, а потому, что в условиях безнаказанности идет война, как когда-то за территории. А любая захваченная компания либо может участвовать в цепочке атаки, либо сама относится к критической инфраструктуре (телекоммуникации, энергетика, ключевые банки). Если нарушить их работу, это может дестабилизировать ситуацию в Украине.

Но одного SIEM уже недостаточно, поскольку атаки становятся все более изощренными, технологии и процессы у заказчиков — тоже; все это банально увеличивает нагрузку на инженеров SOC. Чтобы отсеять ложные срабатывания, упростить реагирование и обезопасить доселе незакрытые направления, в SOC используется множество других инструментов.

Например, не так давно Gartner ввел термин ***SOAR*** (***Security Orchestration, Automation and Response***). Он описывает набор решений, предназначенных для автоматического (без участия человека) выявления малозначимых событий безопасности и реагирования на них. Это освобождает инженеров от рутинной работы и оставляет больше времени на анализ инцидентов. Сейчас эти решения используются для дополнения возможностей SIEM, но ожидается, что в будущем SOAR будут прямо интегрироваться в них и как отдельный класс продуктов исчезнут. К примеру, система IBM QRadar уже дополнена SOAR-платформой Resilient, Splunk — решением Phantom. Gartner отмечает, что MSS-провайдеры уже начали внедрять технологии SOAR, и ожидает, что в течение трех лет их будут использовать все.

Для обнаружения инцидентов на рабочих станциях и серверах используются решения ***EDR*** (***Endpoint Detection and Response***) — системы обнаружения и устранения угроз для конечных точек. Их создали для борьбы с угрозами, которым обычные антивирусы противостоять не могут (таким как APT, бесфайловые атаки и вообще новые вредоносные программы). Эти решения используют различные механизмы: песочницы, приманки, эвристический анализ и т.д., позволяющие предотвращать или быстро блокировать атаки. Кроме того, такие системы

действуют на опережение — непрерывно ищут индикаторы компрометации на всех устройствах, а также собирают информацию для расследования инцидентов.

Уведомления EDR могут направляться в SIEM. Вдобавок система улучшает видимость всех устройств, процессов, и файлов в сети организации, что полезно при расследовании инцидентов. Некоторые решения сохраняют и архивные данные — это позволяет отслеживать атаки в ретроспективе. Наконец, EDR дают возможность удаленного воздействия (например, отправка файлов в карантин, принудительное прекращение процессов и изоляция устройств от сети).

Относительно новым типом решения являются ***UEBA*** (***User and Entity Behavioral Analysis*** — системы анализа поведения пользователей и объектов). Под объектами понимаются устройства, сети, приложения и т.д. UEBA обрабатывает не только данные SIEM и журналов, но и информацию о перемещении пользователей (например, записи о выданных пропусках), о контактах между сотрудниками (чаты, электронная почта) и вообще обо всем, что нужно отслеживать. Используя статические правила, UEBA находит аномалии в поведении пользователей и объектов (например, одновременные подключения из двух разных точек или в нестандартное время). А алгоритмы машинного обучения позволяют выявлять изменение поведения; если кто-то обратится к важным данным, которые его ранее не интересовали, это будет замечено.

Сейчас системы UEBA позиционируются как дополнение к SIEM. Считается, что в будущем они тоже вольются в SIEM или EDR и прекратят существование как отдельный класс решений.

Существуют и отдельные детекторы с использованием машинного обучения, которые наблюдают за трафиком в сети и учатся распознавать признаки атак. После обучения они тоже могут обнаруживать аномалии в сети. Такие системы способны выявлять неизвестные атаки, в том числе использующие уязвимости нулевого дня. Предполагается, что они придут на смену традиционным системам IDS/IPS.

Излюбленной целью хакеров является служба каталогов (Active Directory), поскольку через нее можно получить доступ к учетным записям и ресурсам сети. Поэтому существуют специализированные решения, которые в реальном времени, но чаще во время аудита, контролируют состояние каталогов и выявляют уязвимости, которые могут привести к компрометации, и уведомляют о них через SIEM. Также эти средства мониторинга могут обнаруживать изменения в конфигурации, будь то непреднамеренные или сделанные со злым умыслом.

CASB (***Cloud Access Security Broker*** — брокер безопасности облачного доступа) — это инструмент, призванный обеспечить безопасность при работе с услугами и ресурсами, расположенными в облаке. CASB служит централизованной точкой входа в облака с соблюдением корпоративных политик безопасности. Также эта система компенсирует недостаток видимости в облачных средах, например, позволяя обнаруживать «теневые ИТ» (приложения, используемые сотрудниками без ведома организации) и распознавая аномальное поведение программ. Кроме того, CASB передает сводные данные в SIEM для анализа. Возможны две модели использования CASB: проксирование (когда решение располагается между облаком и пользователями) и доступ через API (вход в облако происходит напрямую, но при каждом обращении облачный сервис запрашивает разрешение у CASB, который оценивает риски и выдает подтверждение или запрет). Решения CASB предлагают в том числе сами провайдеры облачных платформ.

В каждом SOC так или иначе должны быть инструменты упреждающего действия — ***CTI***. Это целое направление деятельности, которым занимаются производители решений в сфере кибербезопасности, специализированные компании, а также отделы самих SOC. При этом используются любые методы, позволяющие добывать информацию о киберугрозах, включая разведку по открытым источникам (OSINT) и в Dark Web, где продаются данные об уязвимостях. SOC может искать и анализировать угрозы и риски, специфичные для заказчика, и на базе этого строить его защиту. Аналогичным образом собираются сведения о тактиках и методах работы злоумышленников. Данные, полученные благодаря кибермразведке, обеспечивают более точное распознавание атак.

К кому обращаться

Если говорить конкретно о коммерческих SOC, то американский портал MSSP Alert в прошлом году публиковал рейтинг 100 ведущих провайдеров управляемого сервиса безопасности. В основном это американские же компании; первые места занимают IBM Security Services, MSS-структуры операторов Verizon и AT&T, также в десятку вошли еще четыре компании из США, по одной из Канады, Индии и Японии. Gartner в своем отчете отнес к квадранту лидеров 5 компаний: на первом месте Secureworks, на втором Trustwave (обе также из первой десятки MSSP Alert), также в этой группе Symantec, Verizon и с большим отставанием IBM.

Gartner отмечает, что на рынке представлены как компании, для которых MSS является основным бизнесом, так и другие, для которых это лишь одно из направлений деятельности (аутсорсеры ИТ-услуг, интеграторы, телеком-операторы). При этом существуют сотни маленьких компаний, предлагающих SOC-услуги на региональном уровне; каждую неделю появляется новый провайдер, будь то специализированный или пришедший из смежной сферы.

Что касается лидеров рейтингов, то ***Secureworks***, помимо США, имеет офисы в Лондоне, Сиднее, Токио и Эдинбурге. Три площадки SOC расположены на территории Америки, по одной — в Японии, Великобритании и Индии. Собственная разработка под названием

КИБЕРБЕЗОПАСНОСТЬ — ЭТО УЖЕ НЕОБХОДИМОСТЬ

По нашим оценкам, сейчас в Украине действует около 20 как коммерческих, так и государственных SOC. В основном они предоставляют услуги мониторинга и аудита событий информационной безопасности. Технологии при этом используются разные; все зависит от направлений, которые тот или иной SOC обслуживает. Хорошая практика – применение систем предотвращения вторжений, решений по защите конечных точек, анализаторов сетевых потоков и различных систем контроля доступа.

Александр ПРИХОДЬКО,
директор департамента
по информационной безопасности
«Датагруп»

Количество киберугроз в мире продолжает увеличиваться: например, за последние 6 месяцев 2019 года произошло свыше 4 млн DDoS-атак, а их частота выросла на 39%. При этом атаки усиливаются с ростом количества подключенных к сети IoT-устройств, которое увеличивается на 7,7 млн каждый день. По данным компании NetScout Arbor, одновременно с этим существенно выросло количество респондентов (с 38% до 50%), которые осознали реальные угрозы и негативные последствия от кибератак для бизнеса. К последним по-прежнему относятся DDoS, фишинг и иные действия, нацеленные на получение доступа к различным системам, в том числе с целью вымогательства. Интенсивность этих угроз будет только нарастать.

Поэтому очень важно, чтобы у топ-менеджмента компаний было понимание того, что на сегодня кибербезопасность – это уже обязательный элемент корпоративной ИТ-инфраструктуры. Тормозит же развитие SOC нехватка высококвалифицированного персонала по этому направлению, а также стоимость решений, которые необходимы для эффективной работы полноценного центра кибербезопасности.

Counter Threat Platform обеспечивает сбор и анализ данных, включая методы машинного обучения, а также доступ к информации через портал. ***Trustwave*** — это подразделение азиатского телеком-оператора Singtel Group, круглосуточные SOC-площадки находятся в США, Сингапуре, на Филиппинах и в Польше, также есть несколько SOC, работающих в дневные часы. Также в составе оператора имеется собственная группа Threat Intelligence — SpiderLabs. На ведущих ролях в том числе и американская компания ***AlertLogic***, в прошлом году представившая решение, получившее название SIEMless Threat Management.

Говоря о коммерческих SOC в Украине, нужно упомянуть, прежде всего, компанию ***ISSP***, которая занимается этим бизнесом уже более пяти лет. Кроме Украины, ISSP имеет офисы в Вашингтоне, Вроцлаве, Тбилиси и Алматы. Основные SOC-мощности собраны в Киеве, тогда как площадку во Вроцлаве компания характеризует как точку концентрации SOC-компетенций в восточной части Евросоюза. Также ISSP сейчас занята продвижением в Северной Америке.

Клиентами ISSP являются крупные компании со средним количеством сотрудников на уровне 2–4 тысяч, основные заказчики — финансовые учреждения, госорганы, торговые сети, хотя не так давно оператор запустил пакет услуг для малого бизнеса. Наиболее распространенной услугой является мониторинг и выявление, хотя некоторое количество компаний уже подписалось и на услугу активного реагирования на выявленные угрозы. Одной из ключевых услуг перед подключением к SOC-сервисам нам назвали анализ компрометации инфраструктуры заказчика, для чего разработана собственная платформа GuardYoo. Также у ISSP есть своя кибер-лаборатория.

В прошлом году открылся SOC компании ***«Октава Кіберзахист»***, рассчитанный на компании уровня SMB. Техническая часть включает в себя, среди прочего, SIEM ***Splunk***, «ловушки» TrapX, позволяющие обнаруживать неизвестные атаки, и безагентное решение для защиты рабочих станций Promisec Endpoint Manager. В качестве детекторов используются межсетевые экраны Cisco, которые могут предоставляться в аренду заказчикам и разворачиваться на их территории, передавая телеметрию для анализа в SOC.

Infopulse — компания, имеющая представительства в нескольких странах Европы, — занимается строительством SOC у заказчиков, а также предлагает услуги на базе собственного центра кибербезопасности. В их число входят защита от атак нулевого дня, анализ поведения пользователей и выявление аномалий, защита Active Directory, мониторинг действий администраторов и другие функции. Также компания проводит аудиты безопасности на предприятии, оценку уязвимостей и тесты на проникновение.

Omega Security Service имеет в Украине три площадки SOC, работающие круглосуточно. Предлагаемые услуги включают в себя защиту от DDoS-атак, сканирование инфраструктуры на уязвимости и испытания на проникновение, в том числе с использованием методов социальной инженерии и Threat Intelligence для упреждающего выявления угроз. Также компания устанавливает системы видеонаблюдения и предоставляет сервис видеоаналитики. Кроме Украины, компания имеет офис в Канаде.

В начале прошлого года систему SIEM для мониторинга и раннего обнаружения потенциальных атак внедрил у себя оператор ***«Датагруп»***. На ее базе был создан собственный SOC, и по состоянию на первую половину года уже имелось несколько клиентов. Но так как SOC только недавно запустился, об опыте работы наверняка стоит спрашивать уже в следующем году.

Обязательно спросим — и непременно к тому времени появятся еще компании, предлагающие сервисы киберзащиты.

Василий ТКАЧЕНКО, СиБ