От аудита до контроля, или Особенности украинского SOC

Андрей Слободяник, коммерческий директор компании ISSP

Услуги управления безопасностью по понятным причинам наиболее интересны банкам.

Компания ISSP имеет реальный опыт построения центра управления безопасностью и обслуживания заказчиков (Security Operation Center). О том, как устроен SOC и чем он занимается, журналу «СиБ» рассказал коммерческий директор ISSP Андрей Слободяник.

— Как давно ISSP предоставляет услуги SOC?

— С 2014 года. Сам SOC представляет собой некий симбиоз из людей, технологий и процессов. Кроме Украины, мы ведем бизнес еще в шести странах.

— Какие технические решения лежат в основе центра реагирования ISSP?

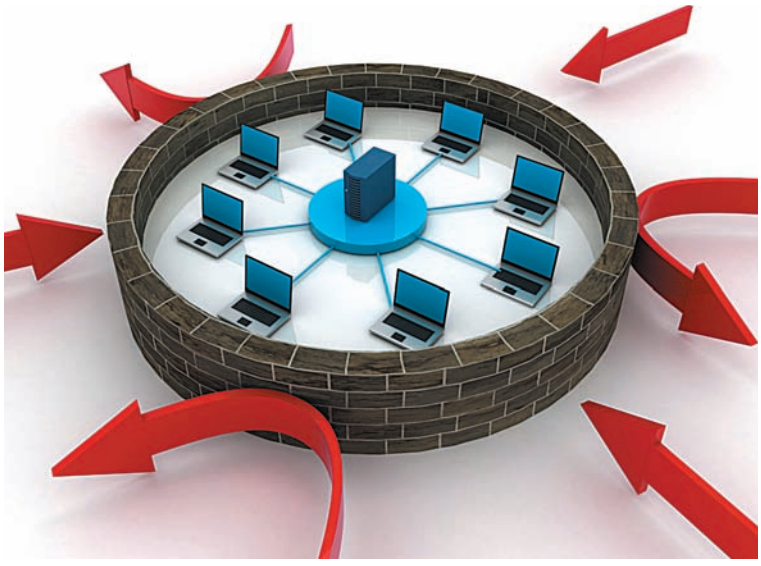
— Сердце SOC, которое осуществляет корреляцию событий и принимает решение о том, имеет место нормальная активность или аномальная, — это классы решений SIEM. Помимо SIEM, работает система мониторинга сетевой активности, различные «продвинутые» песочницы, такие как Lastline, хранилища данных и многие другие технологии, которые базируются на отраслевых стандартах.В нашу систему подключены различные потоки индикаторов компрометации (Threat Streams). На данный момент мы используем платформу MISP. Поиском индикаторов компрометации также заняты сотрудники нашего подразделения ISSP Labs, налажены партнерские отношения с разными центрами кибербезопасности (CERT), в том числе отраслевыми.

— Пожалуйста, опишите типичный сценарий обслуживания. Что наиболее интересно и нужно клиентам?

— Первый этап при внедрении SOC — это ряд аудитов, который позволяет выяснить, скомпрометирована сеть на данный момент или нет. Просматриваются журналы событий, идет поиск и анализ индикаторов компрометации и тд. Также проведение аудитов дает полное представление о том, насколько сеть уязвима, какие векторы атаки возможны и как потенциально от них защищаться. Дальше, как правило, мы проводим аудит доменной инфраструктуры и технический аудит сети, что позволяет создать картину практически о каждом узле в сети организации. После этого мы понимаем, какие процессы являются типичными и нормальными, и на основе эталонной картины можем выявлять аномалии, которые происходят внутри организации. Созданные контроли имплементируются в SIEM, которая далее в автоматическом режиме уведомляет об аномальных событиях. Анализируя их, наши специалисты могут сделать заключение, имеет место разрешенная или подозрительная активность. Варианты взаимодействия с заказчиком могут быть разными. Есть контракты, по которым наш аналитик находится на территории заказчика — обычно крупной организации — и работает вместе с ее сотрудниками. В других ситуациях клиенту достаточно получать уведомления от SIEM, на которые он реагирует самостоятельно.

— Какие компании являются заказчиками услуг SOC и какие сервисы SOC наиболее популярны?

— Более 60% заказчиков относятся к финансовому сектору. Логично, что именно они прежде всего заинтересованы в подобном сервисе. В списке немало холдинговых структур, где управление ИТ-инфраструктурой в силу масштаба затруднено, и векторов проникновения из-за этого может быть очень много. В государственном сегменте есть большая инертность, несмотря на атаки, которые раз за разом прокатываются по Украине и уничтожают инфраструктуру. Из услуг наиболее популярны различного рода аудиты, которые позволяют заказчикам отследить текущее состояние инфраструктуры. Мы консультируем, каким образом усилить ИТ-безопасность, построить защищенную сеть, оптимизировать сервисы и процессы внутри организации.



— Какие международные стандарты определяют правила построения SOC?

— Это стандарты NIST, ISO и ENSIA, которые прежде всего сосредоточены на процессной составляющей SOC. Они регламентируют, каким образом нужно проводить мониторинг, детектирование угроз, их описание, каким образом должно происходить удаление зловредной активности, восстановление после атаки. Важный этап — что необходимо сделать, чтобы защититься от выявленного вектора атак.

— В каких направлениях будут развиваться технологии SOC в ближайшем будущем?

— Дальнейшее развитие SOC-сервиса лежит в области «Интернета вещей» и промышленной безопасности потому что на данный момент мало кто задумывается о защите критической инфраструктуры — по крайней мере, в нашей стране. В Европе и Северной Америке создаются специализированные SOC для защиты такой инфраструктуры. IoT-устройств появляется все больше и больше, и они очень уязвимы, потому что нет стандартов, регламентирующих их защиту. Одно дело, например, взломать фитнес-браслет, и совсем другое — кардиостимулятор, передающий информацию в облачный сервис.

— Назовите какие-нибудь наиболее серьезные атаки, которые удалось предотвратить.

— Мы не можем раскрывать детали, так как со всеми клиентами подписываем соглашение о неразглашении. С атаками на наших заказчиков мы сталкиваемся каждый день. Это могут быть как публичные, громкие атаки, так и целенаправленные взломы при помощи специальных механизмов, разработанных для проникновения в тот или иной банк. По нашей статистике, более 80% сетей являются скомпрометированными. Атаки становятся все более автоматизированными и целенаправленными, противостоять этому можно с помощью введения автоматических процедур, которые хорошо понимают, какое состояние для организации является эталонным, и могут быстро выявлять аномалии. Собственно, в этом и состоит специфика нашей работы: держать руку на пульсе и вовремя предотвращать атаки, которым ежеминутно подвергаются наши клиенты.

— Что Вы можете сказать об опыте борьбы с недавними вымогателями?

— Те организации, где ИТ-безопасность была на должном уровне, не пострадали или же смогли быстро восстановиться и не допустили распространения вируса вглубь сети. Необходимо соблюдать определенные правила: сегментировать сеть, управлять политиками доступа, запрещать администраторам работать под административными аккаунтами. Это правила, которые зачастую не требуют никаких крупных капиталовложений, это просто соблюдение определенных политик. К сожалению, зачастую даже в крупных организациях, где есть отдел ИТ-безопасности, эти правила часто игнорируются, потому что механизмы их контроля отсутствуют.

— Сейчас многие говорят, что за кибератаками на нашу страну стоит северный сосед. Насколько это верно?

— Мы не делаем таких заявлений, потому что выступаем как экспертная организация и не можем утверждать того, чего не можем подтвердить. Но, например, компания Lockheed Martin рассматривает киберпространство как четвертую площадку для ведения войны наряду с землей, воздухом и морем. Стоит классическая военная задача захвата территории, в том числе и в киберпространстве, и атаковать нас могут не только северные соседи, но и другие крупные страны, у которых есть глобальные интересы. К сожалению, Украина на данный момент — это тестовая площадка для обкатки кибероружия, потому что мы не состоим ни в каких блоках и киберзащита у нас пока на зачаточном уровне, отчего все желающие чувствуют себя на нашей территории довольно вольготно.

Беседовал **Василий ТКАЧЕНКО**, **СиБ**