ПЕРСПЕКТИВА ИНТЕГРАЦИИ В ОБЛАКО ПОЛНОФУНКЦИОНАЛЬНОЙ СИСТЕМЫ SIEM

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белая О. В.

Сечко Г. В. – канд. техн. наук, доцент

На сегодняшний день в мире фиксируется настоящий всплеск киберинцидентов. Руководителям отделов информационной безопасности и их сотрудникам зачастую приходится неравными силами бороться с этой угрозой. Ресурсов катастрофически не хватает. Это обязывает к разработке и применению различных средств и моделей, одной из которых является полнофункциональная облачная модель SIEM.

SIEM (security information and event management) –это система управления информацией и инцидентами в сфере безопасности. В этой системе успешно решен вопрос не только высокой капитальной стоимости, но и больших эксплуатационных затрат, кроме того она актуальна для множества случаев применения. Основная задача системы SIEM определяется спецификой организации, но спектр основных решаемых данной системой задач сводится, как правило, к выявлению фактов проникновения в систему, попыток организации утечки данных или вирусных атак. Далее идет сбор информации об инциденте и выбор адекватного средства реагирования на инцидент. На завершающем этапе происходит расследование по конкретным пользователям, причастным к инциденту, и устраняются недоработки, сделавшие этот инцидент возможным.

Интеграция в облако полнофункциональной системы SIEM позволила бы не только полностью задействовать все известные преимущества самого облака, но и качественно отразилось бы на всем цикле реагирования на киберинцидент. В конечном итоге, результатом использования системы SIEM будет являться некое событие, на базе которого специалисты по инфозащите могут расследовать киберинциденты. Когда и каким образом будет задействовано это событие — от этого и будет зависеть полезность и ценность системы SIEM, лежащая в основе принятия решения о приобретении подобной системы.

Если создать новый облачный сервис с управлением инфобезопасностью на базе системы SIEM, он будет прост в использовании и внедрении, к тому же его функционал не ограничивается простым сбором информации о событиях, здесь будет подключен новый уровень сбора и анализа данных. В то же время этот сервис не будет отличаться технической сложностью, свойственной системам управления событиями (механизмы сбора, хранения и анализа данных). Пользователям, не придется самим заниматься ни сбором, ни тем более анализом отобранных системой данных. Ответ прост — для этого есть облако. Вся сложная с технической точки зрения инфраструктура SIEM просто переносится туда, пользователю остается лишь выполнить несложную настройку функций безопасности при запуске системы и подписать соглашение о предоставлении услуг (service-level agreement, SLA),согласно которому он будет получать уведомления о произошедших в его сети событиях. В рамках этого сервиса будет функционировать круглосуточный и ежедневный центр управления безопасностью, где дежурные специалисты будут анализировать каждое отмеченное системой SIEM событие и уведомлять о нем пользователей (если это предусмотрено условиями договора SLA).

Ценность такого сервиса для пользователей существенно выше, чем у традиционных корпоративных систем SIEM. Конечной целью создания такого сервиса является полный перенос инфраструктуры SIEM в облако.

Но, как и любой продукт, функционирующий на базе сложных процессов и технологий, система SIEM при переносе ее в облако, имеет свои недостатки. Основной из них — безопасность. Ведь фактически в SIEM будут храниться, и обрабатываться конфиденциальные данные (журналы событий и информация о киберинцидентах), и даже личные данные пользователей. Получается, что пользователи «облачной» версии SIEM должны питать абсолютное доверие к провайдеру системы.

Полнофункциональная облачная модель SIEM должна отвечать следующим требованиям:

1. Вложения и расходы на содержание собственной аппаратной и программной инфраструктуры — нулевые или незначительные.

2. Простота использования: достаточно просто переслать свои журналы событий в систему для оценки.

3. Наличие круглосуточного центра операционной безопасности (SOC).

4. «Коробочная» конфигурация, подразумевающая продукт в готовом виде, рассчитанный на разную специфику применения и идущий в сочетании с договором SLA.

Остается надеяться, что в скором времени облачная полнофункциональная система SIEM будет разработана и найдет широкое применение. Пришла пора объединить технологи безопасности с прочими достижениями прогресса, вылившимися в создание инновационных сервисов и технологий, в нашем случае, извлечь максимальную пользу из таких свойств облака, как масштабируемость и ценовые преимущества.