Организация оперативного управления кибербезопасностью на производстве

Алексей Демидов, Владимир Караваев

Кафедра безопасности информационных технологий,
Харьковский национальный университет радиоэлектроники,
УКРАИНА, г. Харьков, пр. Науки, 14,
E-mail: alexdemydov96@gmail.com,
E-mail: volodymyr.karavaiev@nure.ua

Abstract – Models of Security Operations Center are analyzed, their comparative characteristics are given. The basic components, tasks, processes and order of their deployment are considered. The practical value lies in developing recommendations for the enterprise to build Security Operations Center and to deploy them. The results of the research can be applied at Ukrainian enterprises. The scientific novelty lies in the factors that determine the model and architecture of Security Operations Center.

Keywords – SIEM; SOC; Security operations center.

I. Введение

В Украине за последние годы увеличилось количество кибер-атак в корпоративном секторе так и государственном, а сами хакеры уже не работают в одиночку, как 20 лет назад, а работают в крупных или не больших группах хорошо организованных как техническим оснащением так и огромными многомиллионными вложениями средств со стороны государств или средств которые были полученные незаконным путем.

Высокая интенсивность кибер-атак по всей Украине статистика приведена за 2019 год в Рис.1.

Рис. 1 - Статистика кибер-атак по Украине за 2019 год

При этом в корпоративном секторе работают специалисты по кибербезопасности, а в государственном секторе работает Киберполиция, СБУ ДКИБ, которые имеют в своем арсенале программно-технические комплексы в области защиты информации (DLP, SIEM, IDS/IPS, WAF/FW, EDR). При всей организации защиты информации в Украине, все равно происходят кибер-атаки с большим убытком государству.

Специалисты в сфере кибербезопасности давно осознали, то что необходимо создание единого централизированного комплексного решения в сфере реагирования на кибер-атак и других инцидентов связанных с информацией с возможностью расследования инцидентов. Основным решением является создание центра мониторинга и оперативного реагирования кибер-атак, который поможет избежать кибер-атак но и противостоять атакам в режиме реального времени а так же расследовать их после. Для обеспечения целостного и комплексного подхода мониторинга и реагирования на кибер-атаки, согласно всем стандартам регулирующим кибербезопасноть, например ISO IEC 27035, ISO IEC 27001. SOC объединяет все данные технологии а так же процессы и професиональные навыки сотрудников в сфере кибербезопасности, формируя комплексную систему защиты. Что позволяет получить высокую степень готовности и реагирования на инциденты в сфере кибербезопасности, что позволит избежать критических последствии от потенциальных кибер-атак, нацеленных на разные секторы в государстве.

II. Варианты SOC и их сравнение

Существуют три модели SOC:

- собственный SOC;
- SOC как сервис;
- гибридный SOC.

Их можно сравнить по следующим показателям:

- размещение технического оборудования;
- размещение персонала;
- уровень зрелости ИБ;
- структура расходов.

В Таблице 1. сравнивается место размещения технического оснащения.

Сравнивая эти типы можно выделить следующие преимущества и недостатки каждой из систем, которые приведены в сравнительной Таблице 2.

ТАБЛИЦА 1

Сравнение места размещения технического оснащения

	Собствен-ный SOC	SOC как сервис	Гибридный SOC
Оборудование для системы	*	+	*
Техническая поддержка	*	+	+
Серверы для сбора данных	*	*	*
Серверы для хранения данных	*	+	+
Серверы резервного копирования	*	+	+
Лицензирование (SIEM, Service Desk)	*	+	*

* - расположены в организации
\+ - расположены у интегратора

ТАБЛИЦА 2

Недостатки и преимущества различных типов SOC

	Собственный SOC	SOC как сервис	Гибридный SOC
Преиму-щества	Собственный процесс контролиру-емого самой организацией	Готовый процесс как услуга Сравнительно небольшая стоимость	Сравнительно небольшая стоимость готов процесс как услуга Возможность развернуть собственный SOC
Недос-татки	Высокая стоимость и сложность организации, построения и поддержки	Выход информации за рамки организации	Выход информации за рамки организации

III. Проблемы и их решение

Основные проблемы SOC:

- люди ;
- реагирование;
- обнаружение;
- расследование;
- поиск (Threat hunting);
- кадры.

Пути решения проблем SOC:

- использовать только лучшие решения SIEM для высокого уровня автоматизации, которые могут позволить создавать сложные правила корреляции и автоматизации с возможностью использования машинного обучения;
- обучение сотрудников, включая экспертов и специалистов в SOC;
- постоянный поведенческий анализ пользователей и систем таких как UBA и UEBA;
- использовать Threat Intelligence от вендоров и сообществ которые предаставляют Threat feeds и IOCs;
- постоянно искать новые API сервисы для интергации с SIEM;
- автоматизация повторяющихся инцидентов в SOC, для увелечения эффективности действий центра;
- постоянно искать лучшие варианты для улучшения политик и правил;
- чем выше осведомленность сотрудников, тем ниже загрузка аналитиков SOC.

Выводы

В статье рассмотрены варианты центров, их проблемы и решения. Были проанализированы их модели и предоставлена сравнительная характеристика. Центр реагирования на кибер-атаки может быть собственным или аутсорсинговым. В любом случае, внедряя SOC, организация одновременно реализует часть процессов системы управления информационной безопасности в соответствии со стандартом ISO 27001 процесс управления инцидентами ИБ, управления уязвимостями и изменениями, контроль соответствия законодательным и отраслевым требованиям, а также выполняет часть требований стандарта PCI DSS.

Литература

[1] S. David. A Practical Application of SIM/SEM/SIEM / Automating Threat Identification. SANS Institute, 2006. p.3. [Электронный ресурс]. - Режим доступа: https://www.sans.org/reading-room/whitepapers/logging/practical- application-sim-sem-siem-automating-threat-identification-1781.pdf

[2] Международный стандарт ISO / IEC 27001: 2013 «Система управления информационной безопасностью. Требования». [Электронный ресурс]. - Режим доступа: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56742 .

[3] Интерактивная карта киберугроз. [Электронный ресурс]. - Режим доступа: https://cybermap.kaspersky.com/ru/