IBM Security

Можно ли эффективно использовать большие данные для безопасности и есть ли примеры этого?

Олег Бакшинский
Ведущий советник по вопросам информационной безопасности
IBM в России и СНГ

IBM

Безопасность Дата Центров

- СТАНДАРТЫ
- ТРЕБОВАНИЯ
- ЛУЧШИЕ ПРАКТИКИ

Много Людей

Много Данных

Много Приложений

Много Инфраструктуры

Определим Большие Данные

- ОБЪЕМ — Огромный
- СКОРОСТЬ — В реальном времени
- РАЗНООБРАЗИЕ — Все типы данных

- ИЗМЕНЧИВОСТЬ — Не всегда периодичны
- СЛОЖНОСТЬ — Трудно коррелировать

Определим цели использования Больших Данных в ИБ

Используя инструменты Аналитики постараться

- Выявлять угрозы быстрее и точнее
- Реагировать быстрее и эффективнее
- Сэкономить

На чем строится Аналитика Больших Данных ?

- Данные
- Методы и алгоритмы
- Цели и выводы

Почему Большие Данные не взлетают ?

1. Свалка данных
2. Проблемы со сбором данных
3. Проблемы с доступом к данным
4. Ничего, кроме сбора
5. Ничего, кроме поиска по ключевым словам
6. Никакой пользы в выявлении угроз
7. Неспособность в определении сценариев для аналитики
8. Очень трудоемкая разработка сценариев
9. Отсутствие квалифицированных аналитиков

(c) Антон Чувакин, Gartner

Примеры использования Аналитики Больших Данных в ИБ

Сетевой и хост трафик. Аналитика безопасности оценивает аномалии в трафике данных на серверы и кластеры и обратно, ищем шифрование или подозрительные адресаты. Аналитика берется из источников данных, таких как SIEM, мониторинг сети или мониторинг приложений.

Веб-транзакции. Наблюдается ли подозрительная активность у критичных приложений или чувствительных активов? Аналитика будет использовать данные аутентификации, мониторинг транзакций, журналы приложений, журналы SQL-сервера и данные сетевых сессий для выявления мошеннической деятельности.

Инфраструктура. Работает ли сервер? Произошло ли последнее изменение конфигурации? Соблюдение политики и правил ИБ? Чтобы проверить изменения инфраструктуры будут использоваться данные из ИТ-активов; сверимся с GRC, и используем системы управления конфигурациями.

Данные. Какие типы данных хранятся, передаются или обрабатываются системой? Это регулируемые данные? Это ценный IP-адрес? Чтобы оценить риск безопасности от информации, большая аналитика безопасности данных основана на GRC, классификации данных и DLP.

Люди. Какие пользователи вошли в систему? Являются ли их привилегии актуальными или они были эскалированы? Когда они в последний раз вошли? Какими активами они пользовались? Для отслеживания аналитики активности пользователя будут использоваться данные аутентификации, журналы сервера, управление активами, SIEM и мониторинг сети.

Точнее и Эффективнее

- Определите правильные источники данных
- В качестве коллекторов можно использовать настроенные ранее LM или SIEM
- Начните с NBAD (NTA) и UBA (UEBA)
- Постепенно расширяйте список сценариев
- Аналитика не заменит Аналитиков

Люди – Процессы – Технологии

IBM Security

СПАСИБО

FOLLOW US ON:

ibm.com/security

securityintelligence.com

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM