Новые продукты для обеспечения информационной безопасности

Михаил Кадер

Positive Technologies

18.04.2023

Время возможностей?

- МСЭ нового поколения (NGFW)
- Защита контейнеров (container security)
- Автоматизация (SOAR/IRP)
- Контроль доступа к облачным приложениям (CASB)

Межсетевые экраны нового поколения (NGFW)

- Огромный кусок «пирога»
- ФСТЭК
  - Железо
  - Граница с Интернет
- Несколько подходов
  - Напишем сами
  - Слепим из СРПО

Межсетевые экраны нового поколения
Функциональность

- Режимы внедрения – маршрутизируемый или прозрачный
- Кластеризация и/или горячее резервирование
- Пользователи
- Приложения, включая облачные
- Расшифрование TLS
- Сигнатуры СОВ
- Антивирус
- Производительность
- Централизованное управление

Время возможностей?

- МСЭ нового поколения (NGFW)
- Защита контейнеров (container security)
- Автоматизация (SOAR/IRP)
- Контроль доступа к облачным приложениям (CASB)

Защита контейнеров

- Контейнеры – основа разработки и выполнения современных приложений
- О чем подумать
  - Реестр ПО
  - Защита оркестровки
  - Уязвимости операционных систем
  - Уязвимости образов
  - Уязвимости прикладного ПО
  - Аномалии поведения
  - Микросегментация/МСЭ

Время возможностей?

- МСЭ нового поколения (NGFW)
- Защита контейнеров (container security)
- Автоматизация (SOAR/IRP)
- Контроль доступа к облачным приложениям (CASB)

Автоматизация

- Людей нет
- Людей нет
- Людей нет
- …
- Интеграция процессов ИТ/ИБ
  - Скорость реагирования
  - Точность реагирования
  - Ложное реагирование
  - Моральная готовность
  - Услуги

Время возможностей?

- МСЭ нового поколения (NGFW)
- Защита контейнеров (container security)
- Автоматизация (SOAR/IRP)
- Контроль доступа к облачным приложениям (CASB)

Контроль доступа к облачным приложениям

- Яндекс
- VK
- И многие другие
- Решений нет?
  - 2018 год ☹
  - 2022 год ☹
  - Может быть не нужны?
  - Хотя бы мониторинг

Немного общего

- Экспертиза
- Интеграции
- Сопровождение

Спасибо
за внимание

ptsecurity.com