Требования регуляторов и(или) бизнес-риски. Адаптация единых инструментов под две задачи.

Леонид Чуриков

Ведущий аналитик «СерчИнформ»

SEARCHINFORM
INFORMATION SECURITY

Необходимость SIEM для обеспечения нормативных требований по защищенности организации

SEARCHINFORM
INFORMATION SECURITY

Подход к вопросу с позиции регулятора

- Отчитаться об инциденте в течение суток, расследовать инцидент за трое суток (нововведение).
- Выполнять регламент по ИБ (приказы ФСТЭК: 239, 17, 21, 31 и т.д.).
- Быть в контакте с НКЦКИ*.
- Оборотный штраф (этап публичного обсуждения).
- Переход на отечественное ПО (для объектов КИИ и госорганизаций – прямой запрет, для частного сектора – уход иностранных компаний, несоблюдение договоров).

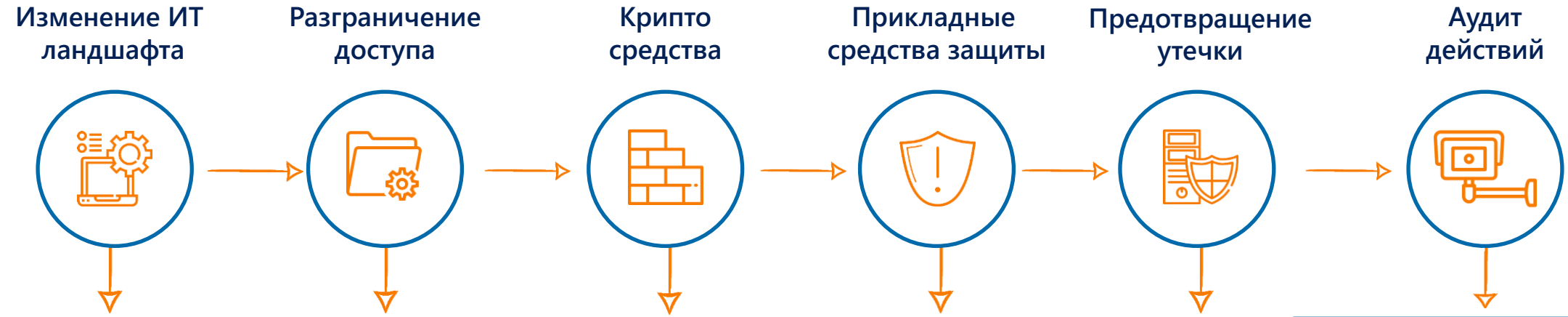
SEARCHINFORM
INFORMATION SECURITY

Подход к вопросу с позиции здравого смысла

- Не допустить прерывания бизнес-процессов, обеспечить стабильную работоспособность.
- Защитить конфиденциальную информацию для бизнеса.
- Избежать нарушений законодательства.
- Тратить меньше ресурсов и оптимизировать процессы ИБ.

SEARCHINFORM
INFORMATION SECURITY

Типовые проблемы классических подходов

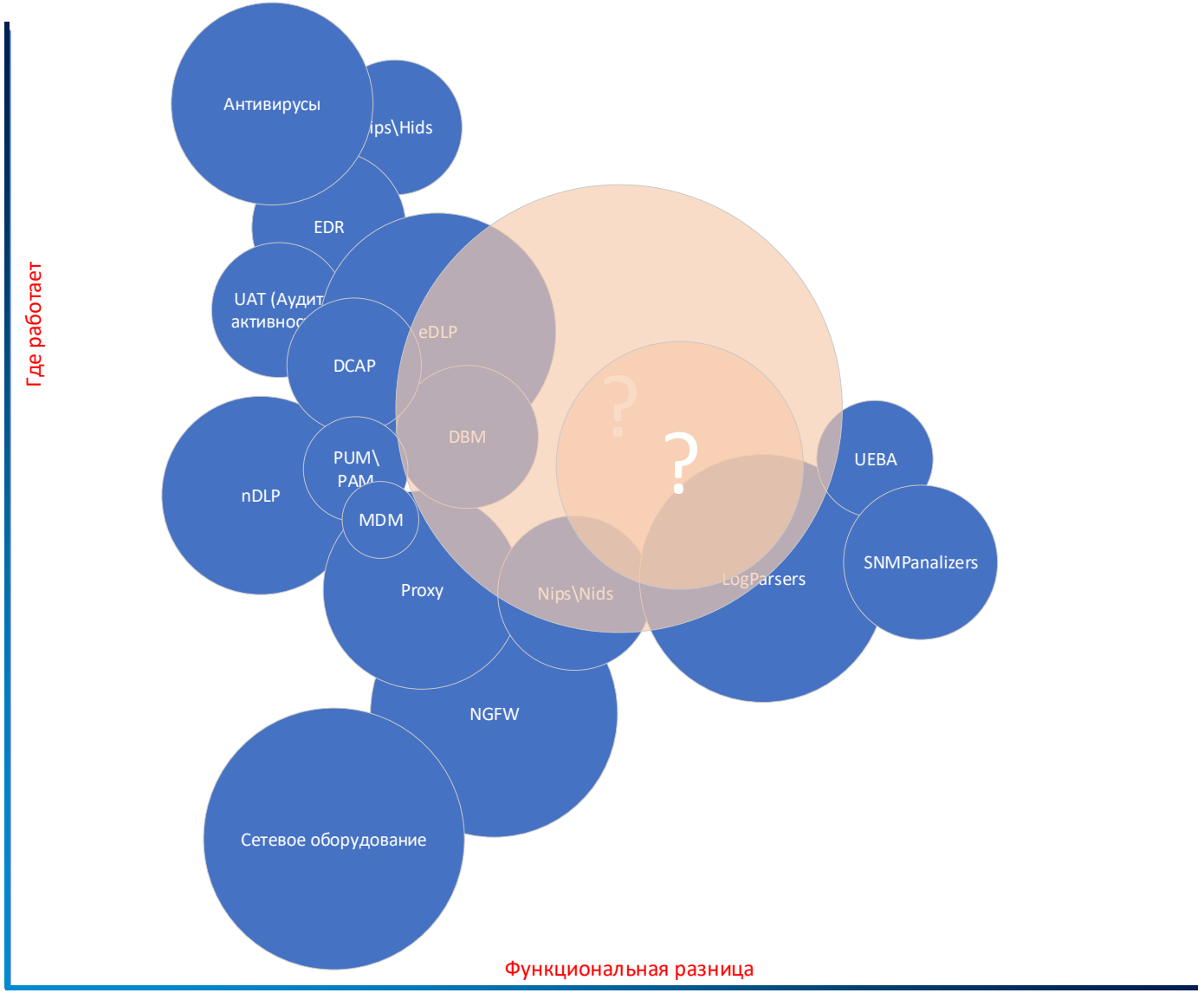


Нерешенные проблемы

- Непонимание ландшафта
- Разграничение доступа не всегда разграничивает
- Шифрование не всегда эффективно
- За предотвращение утечек часто выдают выявление утечек
- Частичный аудит выдается за полный

Итог – хорошее решение прикладных задач, но отсутствие комплексного понимания

ИТОГО


Антивирусы
ips\Hids
EDR
UAT (Аудит
активнос
eDLP
DCAP
DBM
?
?
PUM\
PAM
nDLP
MDM
UEBA
SNMPanalizers
Proxy
Nips\Nids
LogParsers
NGFW
Сетевое оборудование
Где работает
Функциональная разница

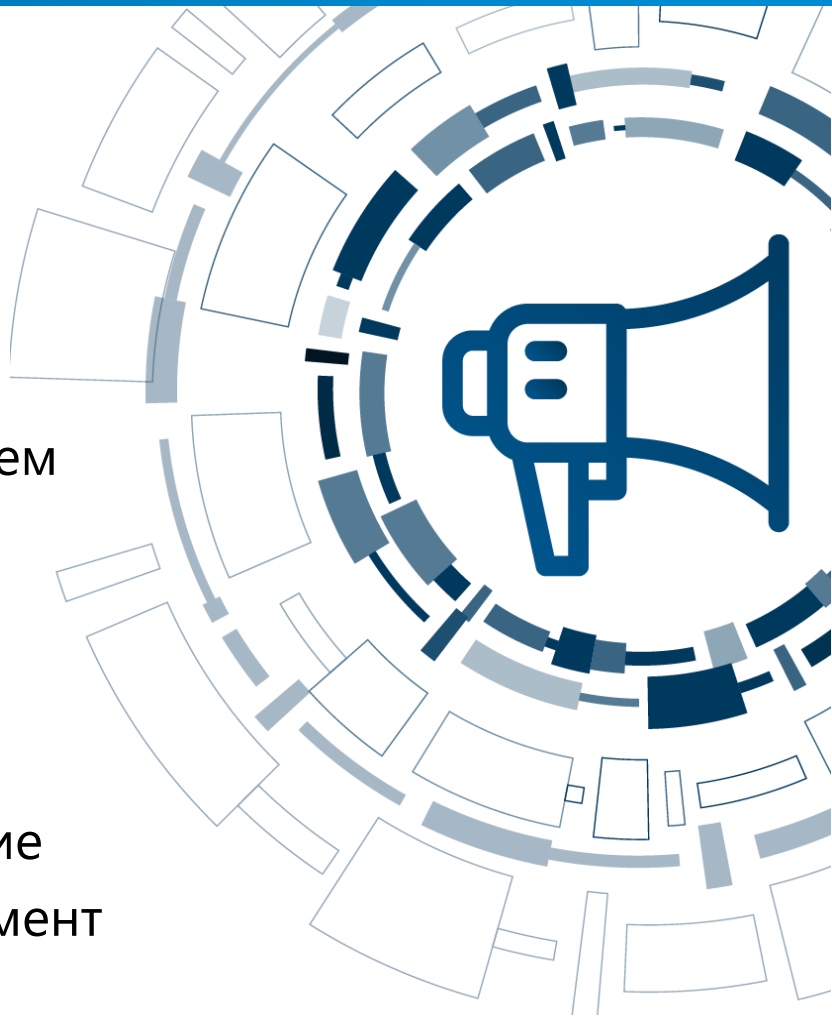
Особенности подхода

- SIEM и SOC имеют ряд идентичных функций.
- Детектирование – лишь часть решения проблемы. Не все SIEM умеют реагировать на инцидент и предотвращать его.
- Не все SIEM и SOC имеют автоматизированные функции аудита инфраструктуры.
- Не все SIEM умеют прогнозировать проблемы, некоторые подходят к этому с неправильной стороны.
- Функция кросс-корреляции может отсутствовать или не использоваться.
- Не все продукты бесшовно совместимы с НКЦКИ.

SEARCHINFORM
INFORMATION SECURITY

Итоговые рекомендации

- Обращайте внимание не только на формальную поддержу отечественного ПО и оборудования, но и на состав технологий внутри продукта.
- Пытайтесь минимизировать количество решений.
- Продукт с проработанными функциями из «коробки» лучше, чем продукт с проработанной кастомизацией.
- Продукт должен закрывать проблемы в моменте и минимизировать потенциальные риски.
- Чем больший цикл проблем закрывается, тем лучше (выделение события, выявление инцидента, реакция на инцидент, менеджмент инцидента, исключение повторного инцидента).



SEARCHINFORM
INFORMATION SECURITY

Спасибо за внимание! Вопросы?

https://t.me/searchinform

https://vk.com/securityinform

https://www.youtube.com/user/SearchInform

Практика и аналитика

https://searchinform.ru/practice-and-analytics/

SEARCHINFORM
INFORMATION SECURITY