

SEARCHINFORM
INFORMATION SECURITY

Интеграции с DLP: как закрыть «слепые пятна» в ИБ



Алексей Дрозд,
начальник отдела безопасности «СёрчИнформ»

Зачем?

Если DLP не интегрируется с бизнес-системами, вы видите **только 30% информации**.

Основные бизнес-системы **не имеют** замкнутого контура.

Подключение облачных платформ бесконечно **размывает** периметр.

Сегодня нет заказчиков, которые используют классический «Network с зеркалированием трафика».

**Минимум каналов связи и бизнес-систем
находятся в замкнутом контуре и привязаны к ПК**



Интеграции с документооборотом, порталами и работой над проектами

- ✔ Jira/Confluence
- ✔ Сфера
- ✔ 1С ЗУП
- ✔ Битрикс24
- ✔ Контур.Диадок



Как это сделать?

- ▶ REST API
- ▶ SYSLOG/CEF
- ▶ SMTPs
- ▶ ICAP
- ▶ Агент драйверного уровня

УНИВЕРСАЛЬНЫЕ ТЕХНОЛОГИИ

ИНФРАСТРУКТУРНЫЕ ТЕХНОЛОГИИ

БИЗНЕС-ПЛАТФОРМЫ

Как это сделать?

- ▶ Динамическая сборка агента под разные ядра
- ▶ SMB/DFS
- ▶ ODBC
- ▶ (Power)Shell/SSH
- ▶ «Золотой образ»

УНИВЕРСАЛЬНЫЕ ТЕХНОЛОГИИ

ИНФРАСТРУКТУРНЫЕ ТЕХНОЛОГИИ

БИЗНЕС-ПЛАТФОРМЫ

Как это сделать?

- ▶ Поддержка отечественных ОС (РЕД ОС, Astra Linux, ROSA Linux, SberOS и т.д.)
- ▶ Поддержка отечественных СУБД (Postgres, Jatoba, Pangolin)
- ▶ Поддержка продуктов в защищенном исполнении (Astra Linux, PostgreSQL Pro)
- ▶ Поддержка платформ (Колибри-АРМ и т.д.)
- ▶ Поддержка PaaS-провайдеров (МТС, Яндекс, Selectel, VK Cloud)

УНИВЕРСАЛЬНЫЕ ТЕХНОЛОГИИ

ИНФРАСТРУКТУРНЫЕ ТЕХНОЛОГИИ

БИЗНЕС-ПЛАТФОРМЫ

Как это сделать?

- ▶ VK Workspace
- ▶ Государственные коммуникационные сервисы
- ▶ Microsoft 365
- ▶ Яндекс 360

УНИВЕРСАЛЬНЫЕ ТЕХНОЛОГИИ

ИНФРАСТРУКТУРНЫЕ ТЕХНОЛОГИИ

БИЗНЕС-ПЛАТФОРМЫ

Профит заказчика

С огромной вероятностью интеграция с необходимой вам типовой системой уже есть.

С нетиповой системой можно начать с применения универсальных технологий интеграции.

В сложных случаях придется запрашивать доработку функционала – сначала запрашиваем у автора прикладного ПО!

В особо сложных случаях доработку делает разработчик DLP.



Спасибо за внимание!

SEARCHINFORM
INFORMATION SECURITY

Про ИБ без воды:
Практика. Тренды. Решения



<https://searchinform.ru/landing/securityconf/>