Концепция настройки политик в InfoWatch Traffic Monitor 6 для «ОАО Банк»

1. Концепция

Настоящий документ содержит правила реагирования Системы на перехваченные объекты, в зависимости от принадлежности объекта к одной из категорий защищаемых данных. К защищаемым данным могут относиться:

- Термины (слова или их сочетаний);
- Тестовые объекты (регулярные выражений) определённого формата;
- Эталонные документы (цифровые отпечатки документов фиксированной структуры)
- Эталонные выгрузки из баз данных (цифровые отпечатки эталонных выгрузок – определённые столбцы или их сочетания)

В рамках текущего этапа внедрения необходимо реализовать детектирование фактов передачи за периметр Компании следующих категорий документов:

1. Строго конфиденциальная информация;
2. Конфиденциальная информация;
3. PCI DSS;
4. Персональные данные;

В таблице ниже описаны правила реагирования Системы на вышеуказанные категории информации, включая:

- Правила передачи – пересылка объекта, содержащего определённую политикой информацию по любому из контролируемых каналов;
- Правила копирования – копирование объекта, содержащего определённую политикой информацию на съемное устройство;
- Правила хранения – размещение объекта, содержащего определённую политикой информацию на рабочей станции пользователя/ разделяемом сетевом ресурсе.
- Правила буфера обмена – копирование объекта, содержащего определённую политикой информацию из одного приложения в другое.
- Правила защиты данных на агенте при передачи – пересылка объекта, содержащего определённую политикой информацию по любому из контролируемых каналов;
- Правила защиты данных на агенте при копировании - копирование объекта, содержащего определённую политикой информацию на съемное устройство;

2. Политики защиты данных (в соответствии со стандартом PCI DSS)

Название политики	Правила реагирования	Пояснение

1. PCI DSS	• Категории
	  ○ PCI DSS: CVV, криптопериод, ключи шифрования
	• Текстовый объект
	  ○ Номер кредитной карты
	• Эталонные документы
	  ○ Выгрузка из БД с данными держателей карт
	1.1. Правило передачи 1:
	• Каналы: все
	• Отправители – любой отправитель, получатели – любой получатель, кроме «Внутренний периметр»
	• Уровень угрозы – высокий
	1.2. Правило передачи 2:
	• Канал: Исходящая почта
	• Отправители – любой отправитель, получатели – @sentinelcredit.ru
	• Уровень угрозы – средний
	1.3. Правило передачи 3:
	• Каналы: все
	• Отправители – «группа e-business», получатели – любой внутренний получатель, кроме «группа e-business»;
	• Уровень угрозы - низкий
	1.4. Правило копирования:
	• Уровень угрозы – высокий
	1.5. Правило хранения:
	• Любой сотрудник, кроме «группа e-business»
	• Уровень угрозы – средний
	1.6. Правило буфера обмена
		1.1. При отправке сообщения, содержащего в теле объекта или вложении информацию категории PCI DSS на внешний адрес, в консоли Traffic Monitor появится событие с высоким уровнем угрозы.
		1.2. При отправке сообщения, содержащего в теле объекта или вложении информацию категории PCI DSS на внешний адрес «@sentinelcredit.ru», в консоли Traffic Monitor появится событие со средним уровнем угрозы.
		1.3. При отправке сотрудником, входящим в группу Процессинга сообщения, содержащего в теле объекта или вложении информацию категории PCI DSS любому получателю, кроме сотрудников группы Процессинга, в консоли Traffic Monitor появится событие со средним уровнем угрозы.
		1.4. При копировании на съемный носитель файла, содержащего информацию категории PCI DSS, в консоли Traffic Monitor появится событие с высоким уровнем угрозы.
		1.5. При обнаружении файлов, содержащих информацию категории PCI DSS на рабочих станциях сотрудников, не входящих в группу Процессинга, в консоли Traffic Monitor появится событие со средним уровнем угрозы.

	• Уровень угрозы – высокий • Назначить событию теги: Подозреваемый 1.7. Правило защиты данных на агенте при передачи • Каналы: Все • Отправители – «группа e-business», получатели - @enemy.com • Назначить событию вердикт: Заблокировать • Уровень угрозы: Высокий • Назначить инициатору статус: Под наблюдением	