

# Организация хранения данных с помощью Symantec DLP

Суязов Александр

Руководитель отдела защиты от утечек



# ЧТО ТАКОЕ DLP ?



## Отправка по электронной Почте



## Ошибка в назначении прав доступа



- **Контроль хранения данных - важен**
- **Есть у многих DLP систем**
- **Обнаружение КИ в общем доступе – половина решения**
- **Вы знаете, кто воспользовался данной информацией ?**

## Контроль доступа к данным – Symantec Data Insight Enterprise

### Сценарии использования



**Сотрудник скачал все доступные ему данные**

**DLP бесполезна**

**Необходим контроль поведения пользователей**

## Symantec Data Insight – уведомление о необычном поведении пользователя



# КОНТРОЛЬ ПОВЕДЕНИЯ - КАК РАБОТАЕТ

The screenshot displays a web-based interface for managing security policies. At the top, there are buttons for 'Update Resolution', 'Delete', and 'Send Email'. Below is a table with columns: Policy Name, Policy Type, User, Reason, Generated On, and Resolution. A 'Policy Details' dialog box is open over the table, showing the configuration for a selected policy. The 'Threshold' field is highlighted with a red box.

Policy Name	Policy Type	User	Reason	Generated On	Resolution
DeviationPolicy	User Activity Deviation ...				
DeviationPolicy	User Activity Deviation ...				
DeviationPolicy	User Activity Deviation ...				
PreserveAccesstoConfidentialDocuments	Data Activity User Whit...				
PreserveAccesstoConfidentialDocuments	Data Activity User Whit...				
PreserveAccesstoConfidentialDocuments	Data Activity User Whit...				
AccesstoConfidential	Data Activity Trigger P...				
AccesstoConfidential	Data Activity Trigger P...				
AccesstoConfidential	Data Activity Trigger P...				
DeviationPolicy	User Activity Deviation ...				
<input checked="" type="checkbox"/> DeviationPolicy	User Activity Deviation ...				
DeviationPolicy	User Activity Deviation ...				
PreserveAccesstoConfidentialDocuments	Data Activity User Whit...				
PreserveAccesstoConfidentialDocuments	Data Activity User Whit...				
PreserveAccesstoConfidentialDocuments	Data Activity User Whit...				
PreserveAccesstoConfidentialDocuments	Data Activity User Whit...				
AccesstoConfidential	Data Activity Trigger P...	User1	Today's Access Count:391. De...	2011-05-26 00:00:41 +...	
AccesstoConfidential	Data Activity Trigger P...	User2	Today's Access Count:304. De...	2011-05-26 00:00:41 +...	
AccesstoConfidential	Data Activity Trigger P...	User3	Today's Access Count:300. De...	2011-05-26 00:00:41 +...	

**Policy Details**

**Description:**

**Policy Type:** User Activity Deviation Policy

**Severity:** HIGH

**Enabled:** true

**Created By:** Administrator@STD

**Baseline:** Last 1 weeks

**Threshold:** 3 times of standard deviation

**Minumum Accesses:** 100 accesses per day

**Selected Paths:**

- \\STD-DC-FS.STD.local

**Selected Users/Groups:**

- User1
- User2
- User3

Close

Был выявлен инцидент, связанный с неправильным назначением прав доступа.

**Неизвестно, кто просматривал данные документы.**

Необходим периодический аудит прав доступа к данным

Необходим контроль доступа сотрудников к файлам с КИ

Необходим процесс исправления выявленных проблем

**Symantec Network Discover – обнаружение КИ в общем доступе**

**Symantec Network Protect – защита КИ**

**Symantec Data Insight – отчет о правах доступа**

**Symantec Data Insight – отчет о доступе к обнаруженным данным**

Symantec DLP  
Network  
Discover  
Обнаружение  
важных  
данных

Symantec Data Insight  
Access Detail Reports  
Формирование  
отчетов о правах  
доступа отделов к  
данным

Заявка на  
изменение  
прав  
доступа в  
ИБ

Изменение  
прав IT  
службой

Data Insight  
Выявление владельцев  
информации  
Network Discover  
Уведомление  
владельцев  
информации

Анализ  
отчета  
Владельце  
м  
информаци  
и

Подтверждени  
е на  
изменение  
прав доступа

# АУДИТ ДОСТУПА К ДАННЫМ

USER	ACCOUNT NAME	TOTAL ACCESS	READ
User1	User1@STD.local	1056	1051
User2	user2@STD.local	855	855
User3	user3@STD.local	828	818
S-1-5-21-3230055797-3765554450-811187041-500	Administrator@STD.local	224	191

FILE SERVER	ACCESS PATH
STD-DC-FS.STD.local	\\STD-DC-FS.STD.local\Confidential\

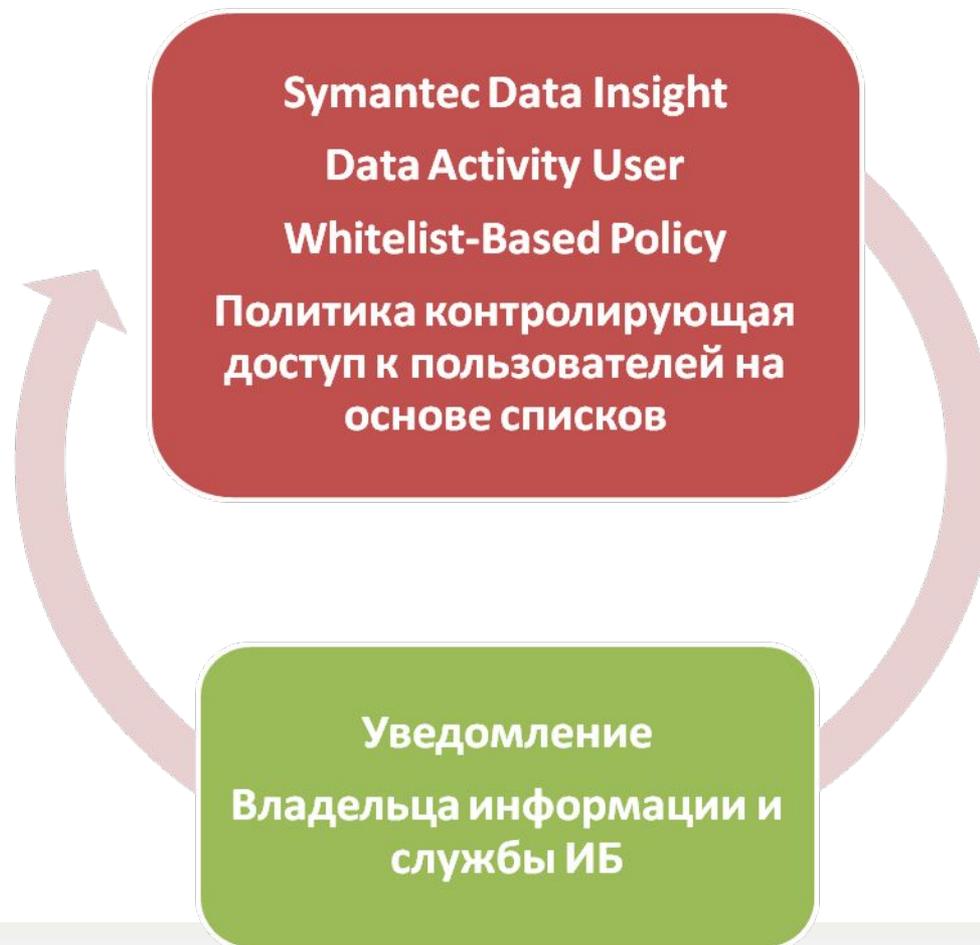
BU NAME	BU OWNER
Юридический отдел	Алексей Иванов
Техподдержка	Александр Кнопкин
Служебная запись	Александр Иванов

# КОНТРОЛЬ ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ

**В компании был выявлен инцидент, связанный с доступом Администраторов к важным данным**

**Необходимо контролировать несанкционированный доступ привилегированных пользователей к важным данным**

## Symantec Data Insight – уведомление о несанкционированном доступе пользователей к файлам





## Контроль использования файловых серверов:

**Capacity Reports – Отчеты по использованию файловых серверов**

**Data Lifecycle Reports – Отчеты по неиспользуемым данным**

**Consumption Reports – отчеты о размере пользовательских данных**

## ИБ Процессы

Проведение аудита  
прав доступа  
Контроль доступа  
привилегированных  
пользователей  
Контроль действий  
пользователей  
Выявление  
нарушения  
регламентов ИБ

## ИТ Процессы

Управление  
хранением данных

## Александр Суязов

Главный менеджер по продуктам направления DLP.

Моб. тел.: +7 (965) 132-0770

e-mail: [asuyazov@leta.ru](mailto:asuyazov@leta.ru)

e-mail: [dlp@leta.ru](mailto:dlp@leta.ru)

## LETA

109129, Россия, Москва, ул. 8-я Текстильщиков, д.11, стр. 2

Тел./факс: +7 (495) 921-1410

Единая служба сервисной поддержки: + 7 (495) 921-1410

[www.leta.ru](http://www.leta.ru)

