

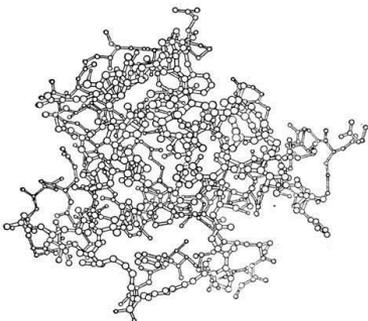
Гибкое решение для анализа данных и мониторинга

Pete Kuzeev, Security Presale Engineer, RRC Moscow



Основные возможности продукта, области применения, детали внедрения и доработки

Обзор продукта



SPLUNK - это система обработки данных



Поиск и устранение проблем



Получение данных
о несовместимости
продуктов

Оценка
воздействия одного
продукта на другой



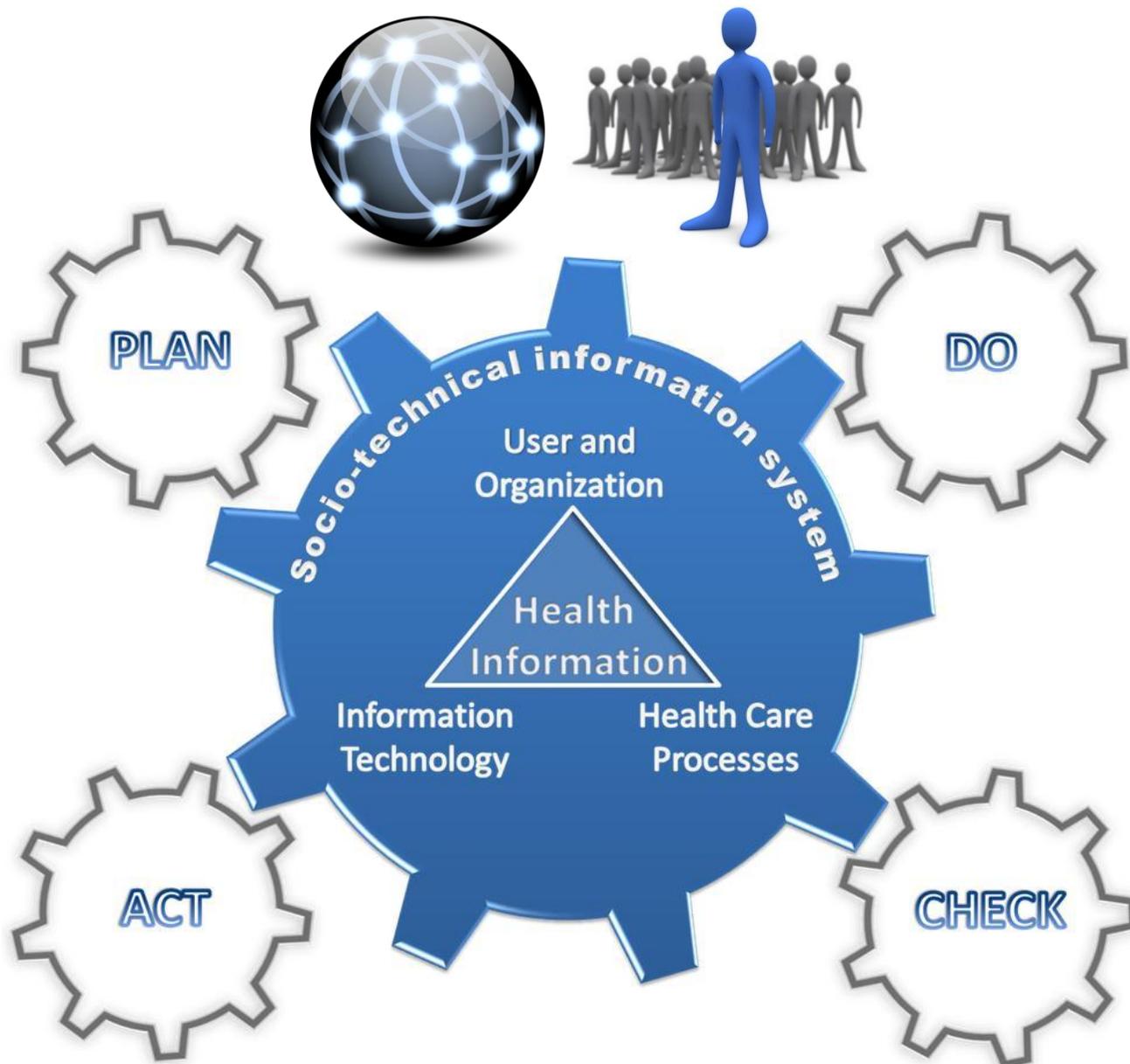
Масштабируемость
от небольшой сети
до сети ЦОД



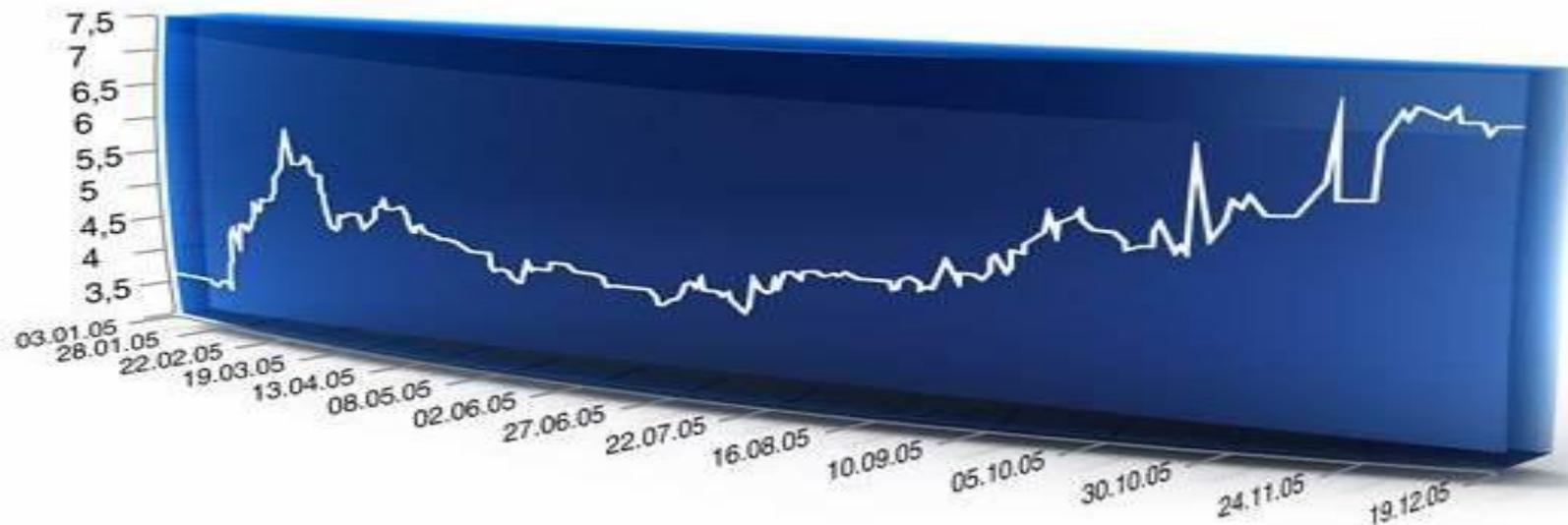
Мониторинг в
режиме реального
времени



Аналитика для
решения скрытых
проблем







Автоматизация

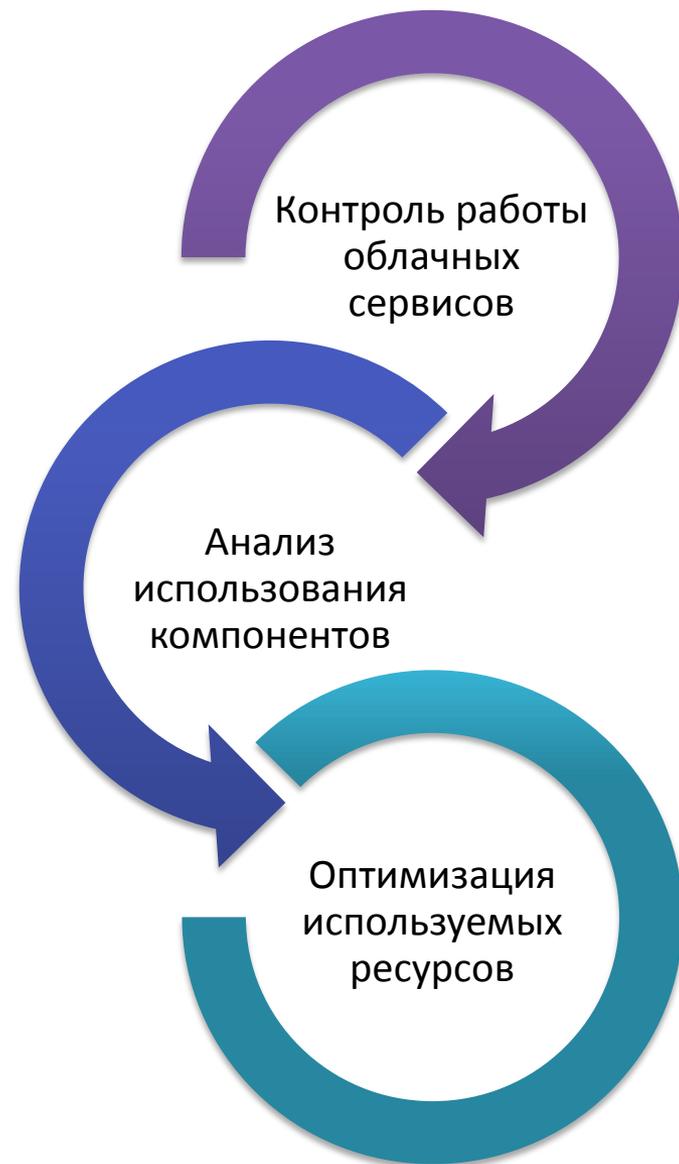
Торговые
роботы

Аналитика

Анализ
трендов

Прогнозирование

Прогноз
роста



next! 

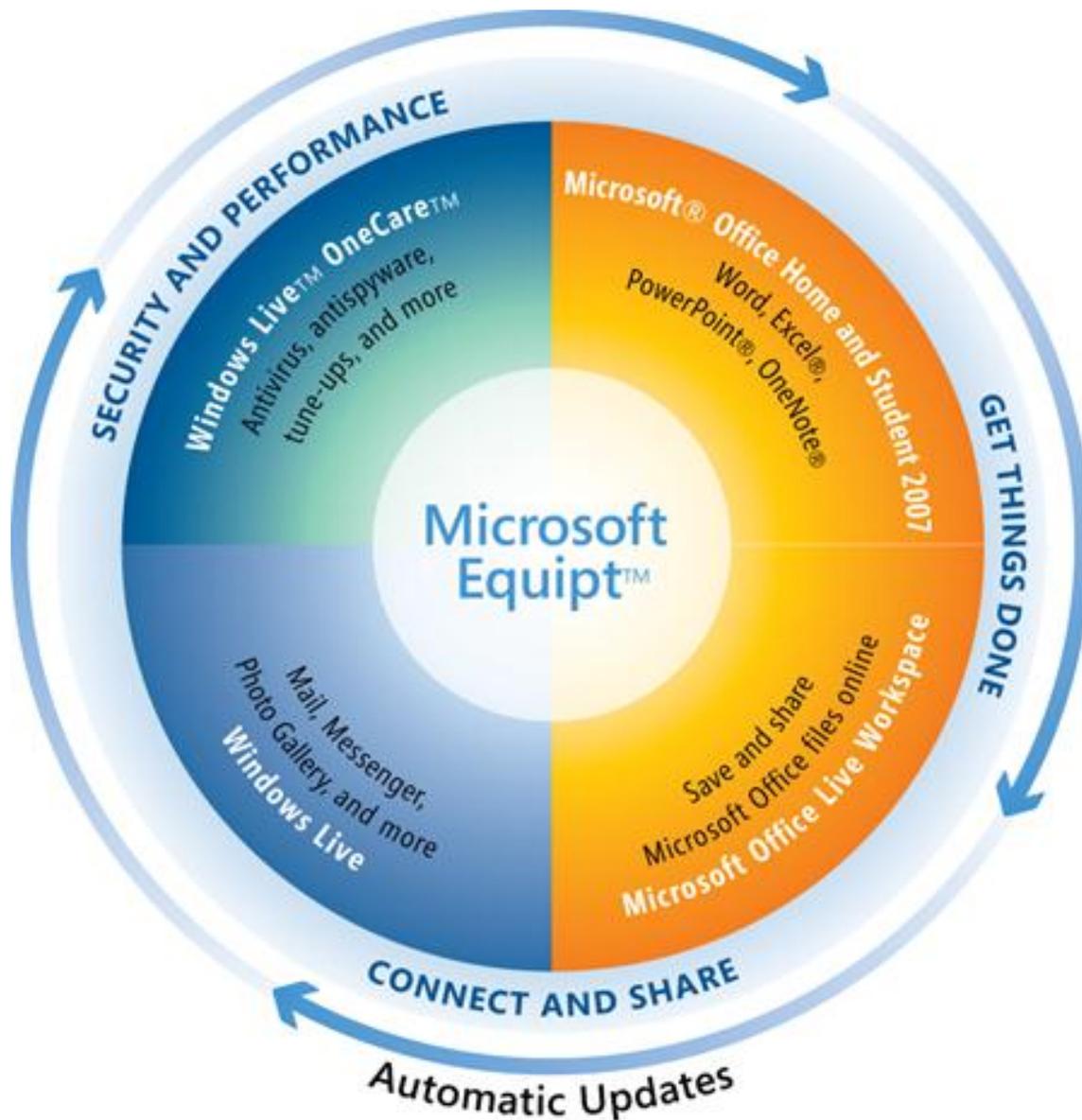
Поддержка
широкого спектра
ПО

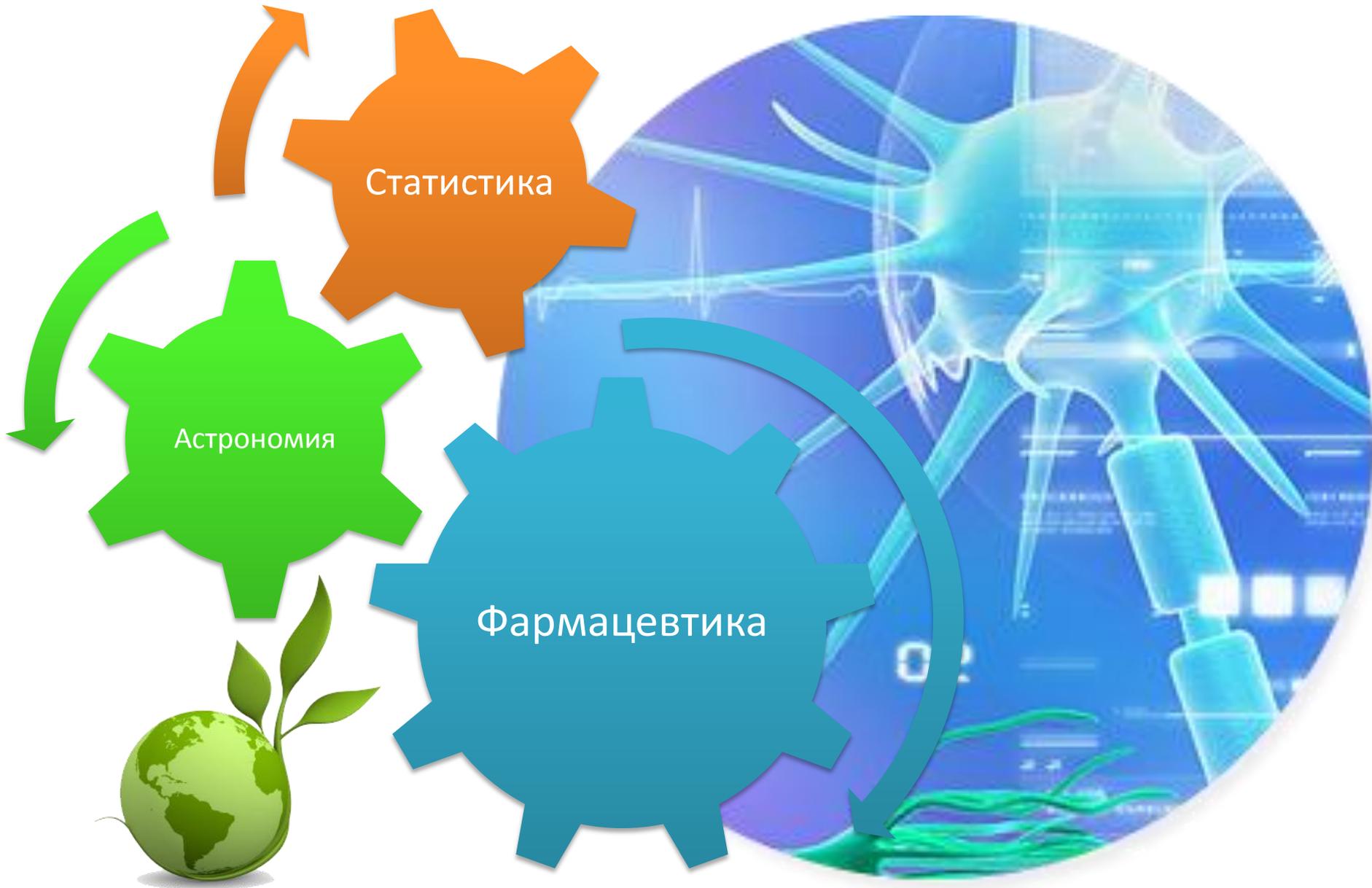


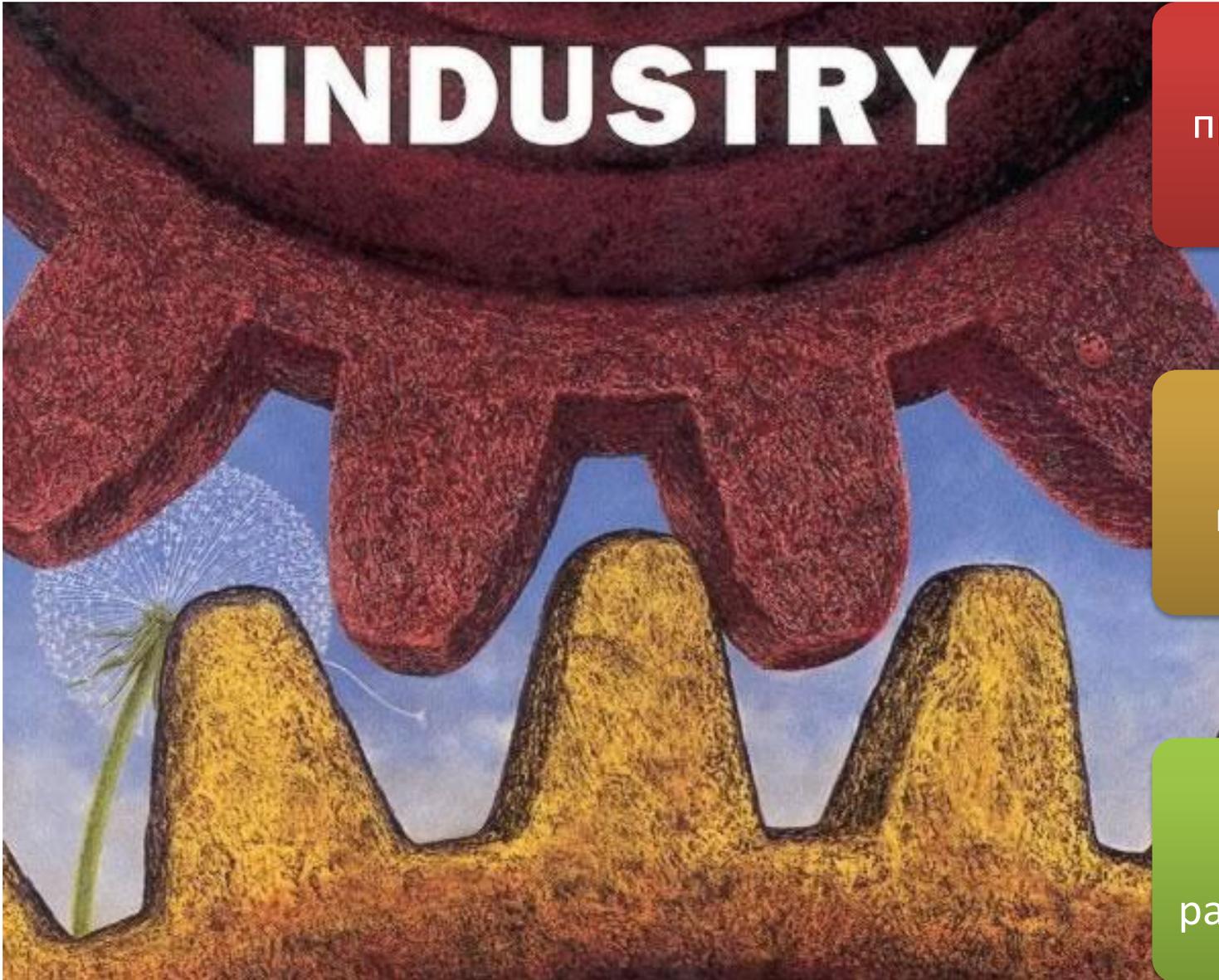
Возможность
работы с логами в
кириллице



Варианты
использование в
качестве Help Desk







INDUSTRY

Контроль
промышленных
линий

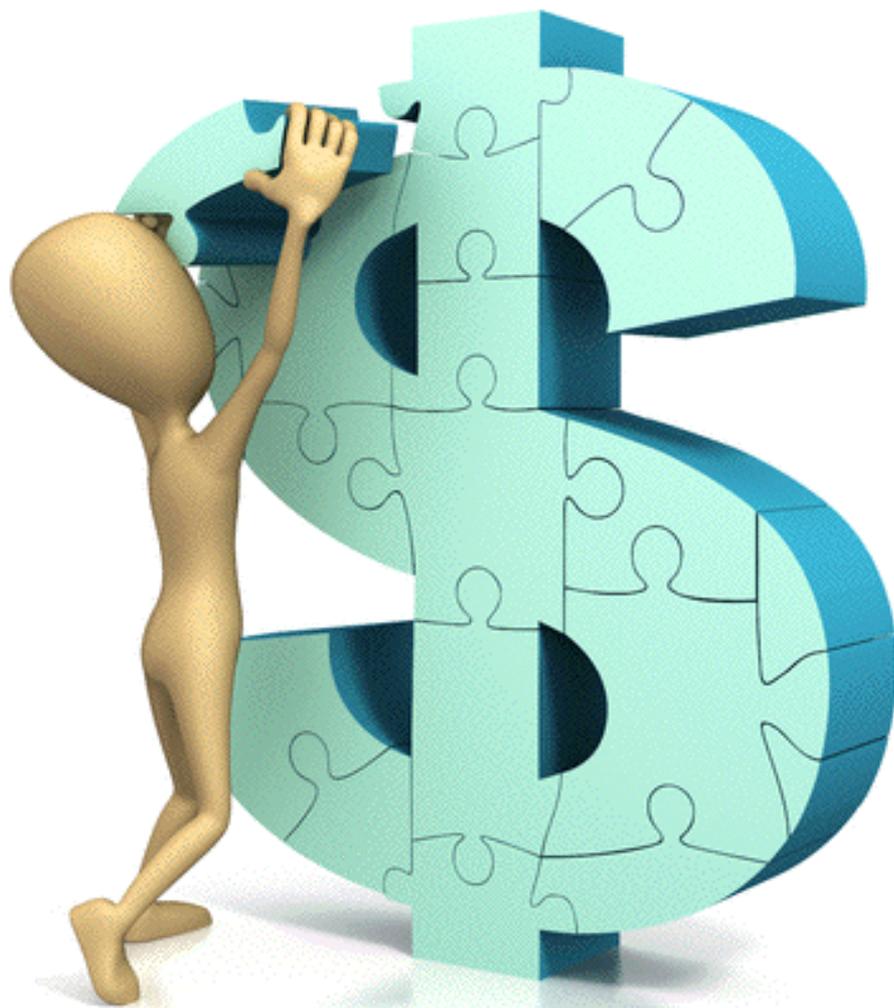


Мониторинг
производства



Обработка
данных от
разных вендоров





Деятельность
компании

Работа
ритейловых
сетей

Качество
автоматизац
ии





Анализ
действий
пользователя



Статистика по
покупкам



Статистика по
переходам

Логи любых устройств или приложений в формате plaintext

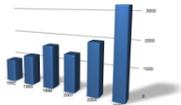


Данные полученные по сети – SNMP, Syslog

Данные полученные приложением в любом формате

Информация полученная с помощью Web-login

Информация полученная от коннекторов или агентов



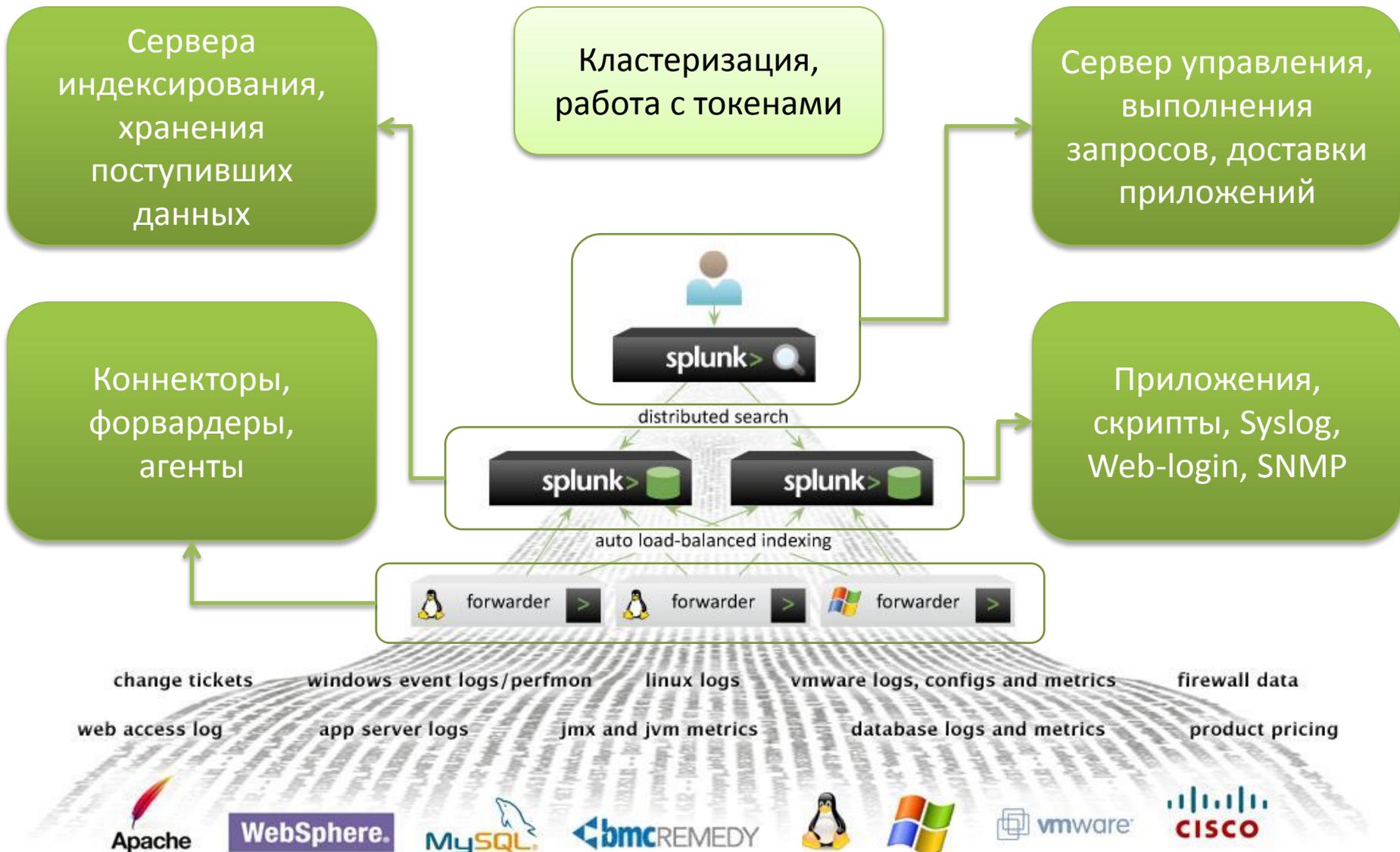
Архивы систем мониторинга – Cisco MARS

Любые любых логов, даже без поля времени и даты



Результаты работы скрипта

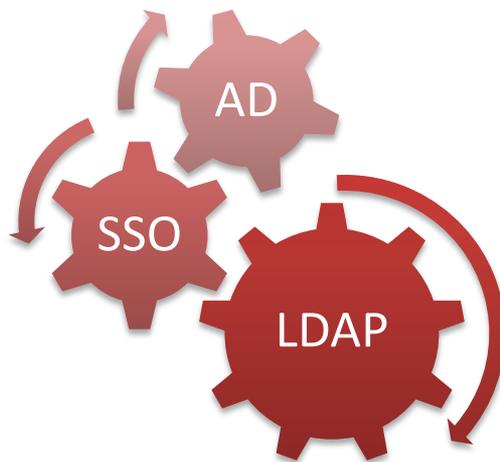
Архитектура приложения



Установка

Поддержка
любой ОСВидео по
установкеАдминистратор
любого уровня

splunk >



You have been logged out. Log in to return to the system.

USERNAME

PASSWORD

Sign in

[First time logging in?](#)

Настройка

Просто указать
путь к логамНастроить
ожидание
данных на
портуДобавить
приложение
через Web

Apps



Apps

Edit permissions for installed apps. Create a new app, or browse Splunkbase for apps created by the community.

Knowledge



Searches and reports

View and edit saved searches and reports. Set permissions. Set up alerts and summary indexing.



Event types

View and edit event types. Set permissions.



Tags

Create, view and edit tags. Set permissions.



Fields

View and edit fields. Set permissions. Define event workflow actions and field aliases. Rename sourcetypes.



Lookups

Create, view and edit lookup definitions. Create and list lookup tables. Set permissions.



User interface

Create, view and edit views, dashboards, and navigation menus.



Advanced search

Create, view and edit search macros. Set permission for search macros and search commands.



All configurations

See all configurations across all apps.

System



System settings

Manage system settings including ports, host name, index path, email server, and system logging.



Server controls

Restart Splunk.



Licensing

Manage license volume, stacking, and pooling. View licensing alerts. Designate this host as the license manager or a license slave.

Data



Data inputs

Add data to Splunk from scripts, files, directories and network ports.



Forwarding and receiving

Configure this host to send and receive data.



Indexes

Create new indexes and manage index size preferences.

Deployment



Distributed search

Set up distributed search across multiple Splunk instances.



Deployment

View deployment client and server status.

Users and authentication

Поиск

Простота
выполнения
запросаКорреляция
по времениСохранение
запросов

Search

* | Last 15 minutes

✓ 24,081 matching events

Hide Zoom out Zoom to selection Deselect Linear scale 1 bar = 1 minute

2,000
1,000
7:20 AM Thu Feb 23 2012
7:25 AM
7:30 AM

24,081 events in the last 15 minutes (from 7:19:00 AM to 7:34:33 AM on Thursday, February 23, 2012)

Field discovery is: On

3 selected fields Edit

- host (19)
- source (31)
- sourcetype (30)

7 interesting fields

- eventtype (45)
- index (2)
- linecount (70)
- punct (≥100)
- splunk_server (2)
- timeendpos (15)
- timestartpos (10)

View all 266 fields

Export Options

prev 1 2 3 4 5 6 7 8 9 10 next 10 per page

1	2/23/12 7:34:32.619 AM	20120223073432.619612 PercentProcessorTime=19 PercentUserTime=9 wmi_type=CPUTime host=panda sourcetype=WMI:CPUTime source=WMI:CPUTime
2	2/23/12 7:34:32.030 AM	1330004072.03 88 1.16.0.0 TCP_REFRESH_HIT/200 412 GET http://www.askmehelpdesk.com/amhd_imgs/style2/menu_divider2.gif "doc@demo" DIRECT/www.askmehelpdesk.com image/gif DEFAULT_CASE-DefaultGroup-Demo_Clients-NONE-NONE-DefaultRouting <IW_ref,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-,-,-,-,IW_ref,-> - http://www.askmehelpdesk.com/ host=ironport.safeweb.acme sourcetype=cisco_wsa_squid source=/var/log/ironport_web.log
3	2/23/12 7:34:32.030 AM	1330004072.03 87 130.253.37.97 TCP_REFRESH_HIT/200 822 GET http://www.askmehelpdesk.com/amhd_imgs/style2/footbg.gif "doc@demo" DIRECT/www.askmehelpdesk.com image/gif DEFAULT_CASE-DefaultGroup-Demo_Clients-NONE-NONE-DefaultRouting <IW_ref,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-,-,-,-,IW_ref,-> - http://www.askmehelpdesk.com/ host=ironport.safeweb.acme sourcetype=cisco_wsa_squid source=/var/log/ironport_web.log
4	2/23/12 7:34:32.030 AM	1330004072.03 87 27.101.11.11 TCP_REFRESH_HIT/200 449 GET http://www.askmehelpdesk.com/amhd_imgs/buttons/collapse_thead.gif "doc@demo" DIRECT/www.askmehelpdesk.com image/gif DEFAULT_CASE-DefaultGroup-Demo_Clients-NONE-NONE-DefaultRouting <IW_ref,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-,-,-,-,IW_ref,-> - http://www.askmehelpdesk.com/ host=ironport.safeweb.acme sourcetype=cisco_wsa_squid source=/var/log/ironport_web.log
5	2/23/12 7:34:32.000 AM	Thu Feb 23 08:34:32 2012 Info: ICID 743930 REJECT SG BLACKLIST match sbrs[-10.0:-3.0] SBRS -10.0 host=ironport.mail.acme sourcetype=cisco_esa source=/var/log/cisco_ironport_mail.log

Оповещения

Из
сохранённых
запросовОтображение
на рабочем
столеОтправка
уведомлений

splunk> Windows Management Administrator | App | Manager | Alerts | Jobs | Logout

Search Overview Performance Management System Management Searches & Reports Setup Help About

Search

source=wineventlog:* "Type=Error" earliest_time=-24h in the last 24 hours

26 matching events ? || ✓ ✕ i 🖨 Save Create

Your timerange was substituted based on your search string

Hide Zoom out Zoom to selection Deselect Linear scale 1 bar = 1 hour

26 events in the last 24 hours (from 7:58:59.000 AM February 22 to 7:59:00.103 AM February 23, 2012)

Field discovery is: On Off Export Options

3 selected fields Edit

- host (3)
- source (2)
- sourcetype (3)

24 interesting fields

- Category (1)
- CategoryString (1)
- ComputerName (3)
- dest (2)
- dvc (3)

System Management 2m ago

In the past 24 hours, your Windows Event Logs recorded:

269210 Events **14 Errors** **1304 Warnings**

Event ID	Time	Log Name	Source Name	Event Code	Event Type	Message
1	2/22/12 3:48:01.000 PM	02/22/2012 03:48:01 PM	Microsoft-Windows-Winlogon	4005	Error	ComputerName=panda.techservices.splunk.com TaskCategory=None OpCode=None RecordNumber=20687 Show all 13 lines host=panda sourcetype=WinEventLog:Application source=WinEventLog:Application
2	2/22/12 12:42:10.000 PM	02/22/12 12:42:10 PM	Sophos Anti-Virus	1	Warning	

Отчёты

Рассылка
pdf, csv, RSSПростота
генерацииЛюбое
приложение

Шаг 1

Выбираете данные для
аналитики

Шаг 2

Выбираете тип
представления запросов
– график, таблица

Шаг 3

Генерируете требуемый
вариант отчёта

Splunk.com | Documentation | Splunkbase | Answers | Wiki | Blogs | Developers Sign Up | Login | FAQ

splunkbase

Home | Answers | Apps upload an app | ask a question | badges | tags | users

Do More with Splunk

Apps and add-ons extend the capabilities of Splunk and make it easier to use. Download a few or share your own creations.



Learn
about apps & add-ons



Share
your apps & add-ons

Featured



Cisco Security Suite

The Cisco Security Suite app is an umbrella app providing a single pane of glass interface into data provided by the other apps and add-ons in the Cisco ... [More »](#)

Recent Uploads

[See all »](#)

5
votes

10
reviews

Splunk App for Windows

windows splunk-supported perfmon
windows-event-logs



Jan 18 splunk 6.4k

15
votes

12
reviews

Splunk for Unix and Linux

splunk-supported performance unix
linux



Nov 07 '11 splunk 6.4k

20
votes

6
reviews

Google Maps

geolocation commands geo
custom-module



May 31 '11 ziegfried 5.8k

Recent Uploads

[See all »](#)

8
votes

2
reviews

Splunk for Excel Export

export excel spreadsheet add-on



yesterday araitz 5.6k

0
votes

0
reviews

Field extractions for Microsoft IAS

Feb 04 southeringtonp 4.3k

1
vote

1
review

Splunk for Cisco CDR

cisco cdr

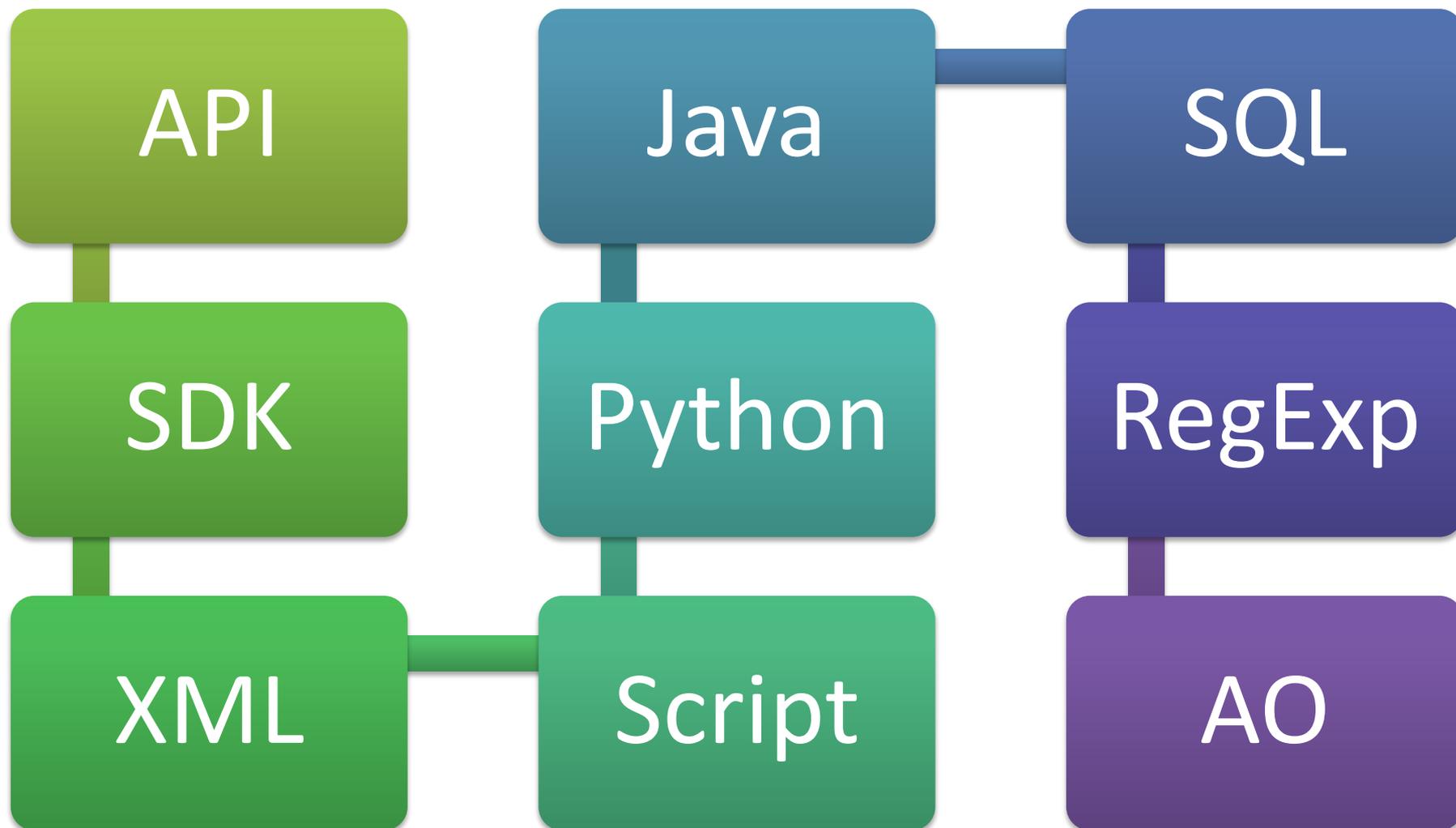


Feb 02 nick 13.1k

0
votes

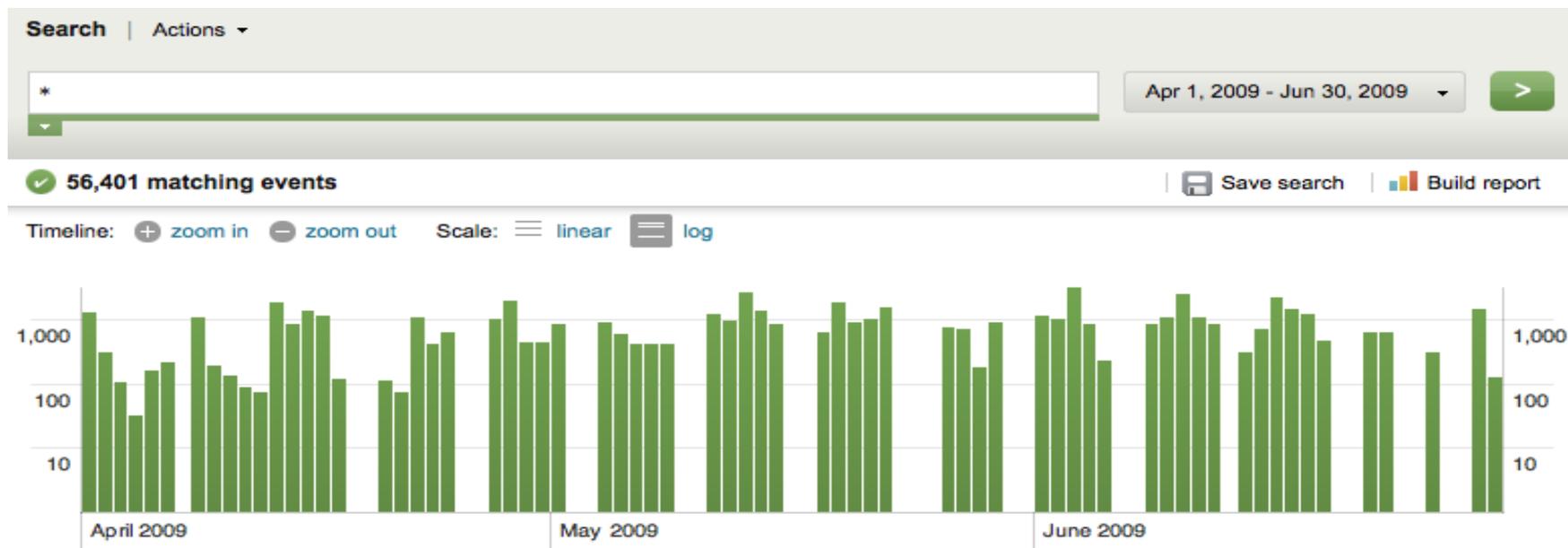
4
reviews

Splunk App for Enterprise Security



- Для удобства анализа и временной корреляции существует timeline, позволяющий связать несколько событий из разных источников для выявления возникшей проблемы и оценки её масштабов

Time Line



- Позволяет пользователям, создавать требуемые выборки данных полей из логов без специальных знаний

Конструктор
RegExp



Splunk

Документация,
база знаний



Splunk Storm

Сервис анализа работы
облачных приложений



Splunk App for Enterprise Security

Пакет Информационной
Безопасности



Splunk for WebSphere Application Server

Анализ данных WebSphere



Splunk App for Web Intelligence

Приложение для изучения
веб-трафика



Splunk MySQL Connector

MySQL коннектор



Splunk App for Microsoft Exchange

Анализатор MS Exchange



Splunk App for Unix and Linux

Набор аналитики для
Unix и Linux

Features	Splunk Free	Splunk Enterprise
Maximum indexing volume per day	500MB	Unlimited (based on license)
Universal, real-time indexing	•	•
Real-time and historical search	•	•
Reporting	•	•
Knowledge mapping	•	•
Dashboards	•	•
Monitoring and alerting		•
Distributed search		•
Data forwarding and receiving	•	•
Role-based access controls		•
Single sign-on		•
Developer APIs	•	•
Community Apps	•	•
Enterprise Apps		•
Standard support	•	
Enterprise support		•

Splunk сжимает поступившие данные до 10ти раз

Учитывается только объём индексов по заданным полям

Пробная лицензия на 500 Мб/день действует 60 дней

Не включает распределённый поиск, мониторинг и оповещения

Ограничена локальным использованием и не поддерживает работу ряда приложений



Графический
интерфейс
более не
привязан к Flash,
используется
HTML 5

Создание
рабочих столов
на лету

Splunk 4.3

Увеличение
скорости поиска
в 10 раз

Увеличение
количества
одновременных
пользователей в
10 раз

Процесс
управления
большими
объёмами
данных стал
более лёгким

Спасибо за внимание!

pkuzeev@rrc.ru

Skype – zerottl

+7 985 9994824