

"Бумажная безопасность" - как угроза информационному обществу

Борис Симис
Директор по развитию
Positive Technologies



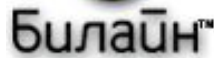
POSITIVE TECHNOLOGIES

О компании Positive Technologies

- Специализация компании – анализ и поиск уязвимостей компьютерных систем.
- Лицензиат ФСТЭК, ФСБ, Минобороны РФ.
- Российский разработчик ПО
 - Сканер безопасности XSPider
 - Система MaxPatrol
- Поддержка портала SecurityLab.ru
- Проведение работ по анализу защищенности:
 - Более 20 Заказчиков в 2009 году (ТЭК, Телеком, Банки, Государственные структуры)



Клиенты компании



ПРАКТИКА АНАЛИЗА ЗАЩИЩЕННОСТИ



Наиболее вероятные пути проникновения

- **Социальная инженерия в сочетании с уязвимостями рабочих мест пользователей**
- **Использование уязвимостей в Web-приложениях**
- **Слабости парольной защиты**
- **Уязвимости и ошибки конфигурации:**
 - сетевых устройств,
 - средств защиты периметра
 - информационных ресурсов в демилитаризованных зонах



Люди и их рабочие места

- **Письма с интересным заголовком**
 - Список увольняемых 2009 год.doc
 - Премияльные выплаты.pdf
- **100 процентно «дырявое» ПО:**
 - Acrodat reader
 - Видео кодеки
 - ICQ, Java



Защищенность Web-приложений

- **1,5 процента легальных сайтов в интернете взломано и используется для установки вредоносного ПО.**
- **Более 10% Интернет-сайтов может быть взломано полностью автоматически.**



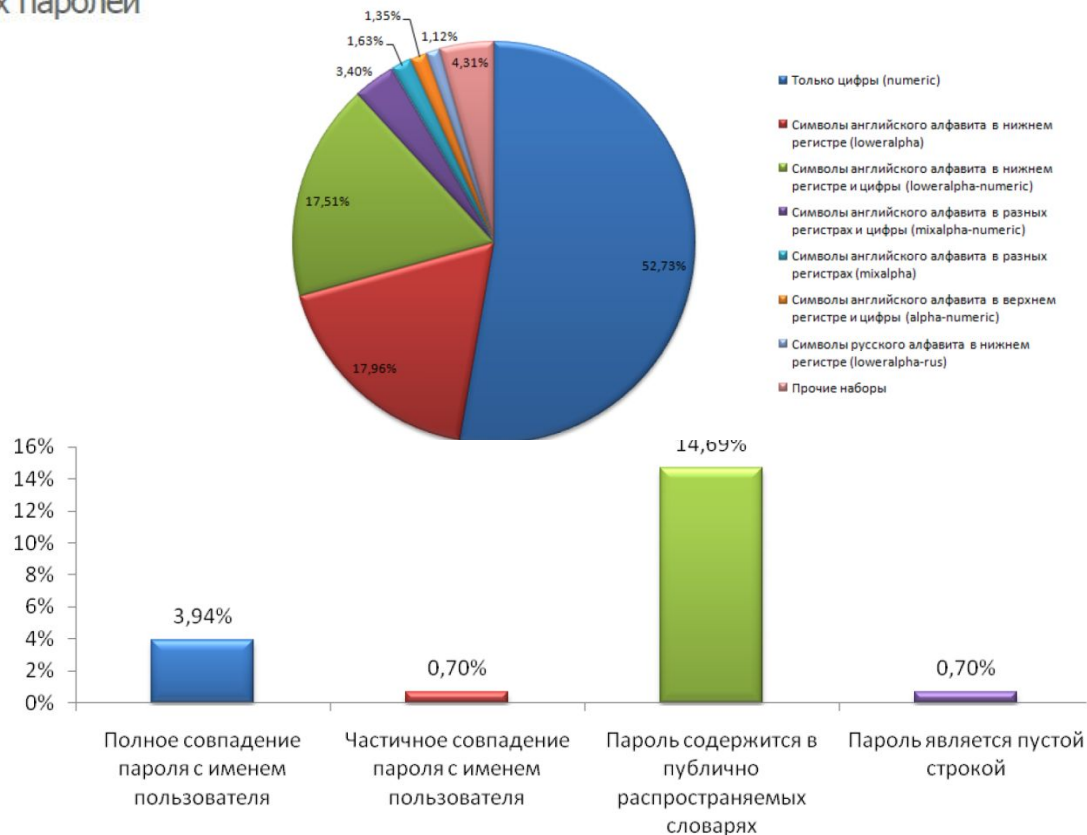
- **Порядка трети web-сайтов российских крупных компаний имеет уязвимости высокой степени критичности.**



Наиболее часто используемые пароли в России

Таблица 2. TOP 10 наиболее часто используемых паролей

Пароль	Позиция	Доля, %
1234567	1	3,36%
12345678	2	1,65%
123456	3	1,02%
Пустая строка	4	0,72%
12345	5	0,47%
7654321	6	0,31%



По материалам исследований компании Positive Technologies: «Анализ проблем парольной защиты в российских компаниях»



Мировая статистика

- **74% инцидентов – результат внешних атак**
- **83% атак не требовало высокой квалификации нарушителя**
- **В 67% инцидентов стали успешны благодаря серьезным ошибкам в защите**
- **87% атак могли бы быть предотвращены стандартными решениями**

По материалам «2009 Data Breach Investigations Report» - Verizon Business



В чем причина?

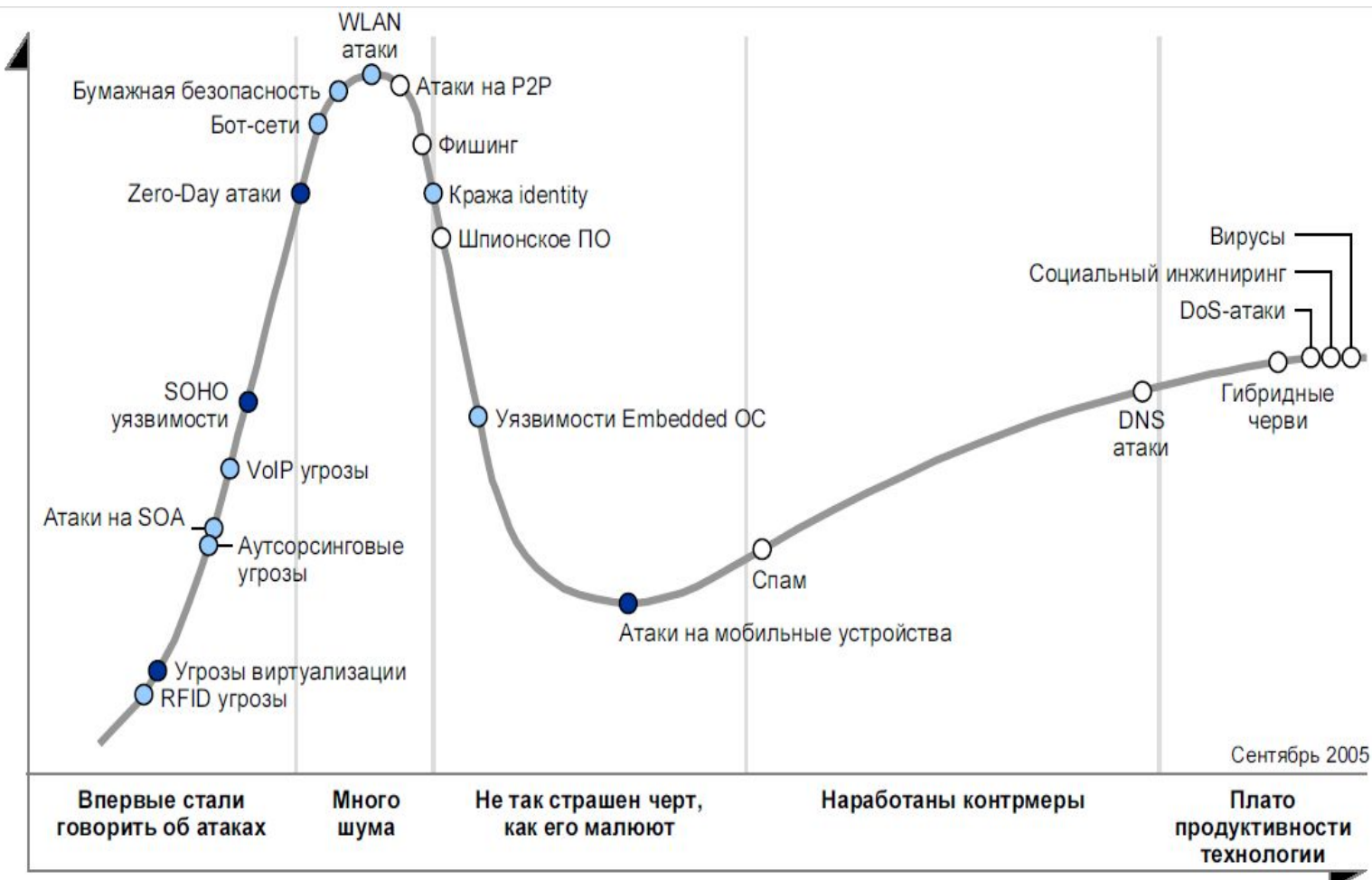


Признаки «бумажной безопасности»

- **Отсутствует контроль настроек ИТ-систем.** Политики реализованы только в виде регламентирующих документов. Как они реализованы никто не знает.
- **Отсутствует процесс управления защищенностью.** Ежедневно появляются новые уязвимости и никто в Компании не знает, какие есть бреши в их системе.



Прогнозирование угроз. Gartner - 2005 Год.



Резюме.

- Преобладание «бумажной» безопасности над реальной
- Обеспечение «реальной» безопасности не является первостепенным вопросом для руководства служб ИБ



Основная предпосылка

- **Безопасность невозможна без порядка в ИТ**
- **Порядок в ИТ трудно навести без технических стандартов для конкретных ИТ систем**
- **Технические стандарты без контроля – фикция**
- **Контроль без автоматизации – нереализуем**



Концепция

**Инвентаризация
технических активов**

**Контроль
защищенности**

**Реальная
безопасность**

**Контроль
технических политик**

**Контроль
изменений, КРІ**



MaxPatrol

**СИСТЕМА КОНТРОЛЯ
ЗАЩИЩЕННОСТИ И СООТВЕТСТВИЯ
ТЕХНИЧЕСКИМ ПОЛИТИКАМ**



Подход к «реальной безопасности» на базе MaxPatrol



ИНВЕНТАРИЗАЦИЯ ТЕХНИЧЕСКИХ АКТИВОВ



Инвентаризация.

- **Внешний периметр:**
 - **Определить перечень узлов и приложений**
 - **Выявить нелегитимные службы (Web-сервера, сетевое оборудование)**
 - **Инвентаризировать внешние ресурсы дочерних организаций**



Инвентаризация.

- **Собрать конфигурацию всех узлов сети:**
 - **Рабочие станции** (перечень установленного ПО, лицензионность ПО, локальные администраторы, внешние модемы...)
 - **Сетевое оборудование** (настроенные access-list, правила авторизации)
 - **Базы данных** (перечень таблиц, пользователи с административными правами)



КОНТРОЛЬ ЗАЩИЩЕННОСТИ



Контроль защищенности – 5 в одном

- **Сетевой сканнер
Network scanner**
- **Тестирование на проникновение
Penetration test**
- **Сканер баз данных
Database scanner**
- **Сканер Web-приложений
Web application scanner**
- **Системные проверки
System audit**



Контроль защищенности

- **Vulnerability management. Контроль управления уязвимостями.**
 - Порядка 15000 уязвимостей в Базе Знаний
 - Ежедневное обновление БД уязвимостей
 - Выявление уязвимостей в ИТ системе
 - Формирование отчетов о необходимости устранения уязвимостями
 - Контроль как ИТ службы устранили уязвимости
- **Результат: ИТ система без уязвимостей.**



КОНТРОЛЬ ПОЛИТИК



- **Встроенные технические стандарты**
 - Cisco, Nortel...
 - MS Windows, Active Directory, Exchange...
 - Linux, Solaris, HP-UX...
 - Microsoft SQL, Oracle...
 - SAP...
- **Возможность разработки собственных стандартов на базе встроенных**



MaxPatrol. Технические политики

02.2009 16:21, длится 00:01:55] - Документ сканирования

Compliances

- [-] CIS - Cisco Firewall
- [-] CIS - Cisco IOS
 - [X] Необходимо настроить EIGRP-аутентификацию, если и
 - [X] Необходимо настроить централизованную аутентифика
 - [X] Необходима локальная аутентификация для управлени
 - [X] Необходима локальная аутентификация AAA при входе
 - [X] Необходима централизованная аутентификация AAA пр
 - [X] Необходимо задать локального пользователя
 - [X] Необходимо задать уровень регистрируемых событий д
 - [X] Необходимо запретить доступ с правами на запись по S
 - [X] Необходимо запретить использование протокола CDP в
 - [X] Необходимо запретить использование TFTP-сервера
 - [X] Необходимо запретить маршрутизацию от исходного IP
 - [X] Необходимо запретить множественные loopback-интерф
 - [X] Необходимо запретить направленную широковещатель
 - [X] Необходимо запретить пароль протокола SNMP "private
 - [X] Необходимо запретить пароль протокола SNMP "public"
 - [X] Необходимо запретить сервис Finger
 - [X] Необходимо запретить BOOTP-сервер
 - [X] Необходимо запретить IP Proxu ARP
 - [X] Необходимо использовать SSH-транспорт для линий VT
 - [X] Необходимо назначить вторичный NTP-сервер
 - [X] Необходимо назначить первичный NTP-сервер
 - [X] Необходимо назначить третичный NTP-сервер
 - [X] Необходимо настроить временные метки в сообщениях
 - [X] Необходимо настроить пароли, привязанные к линиям (
 - [X] Необходимо настроить AAA-учет для команд
 - [X] Необходимо настроить AAA-учет для режима Ehex
 - [X] Необходимо настроить AAA-учет для сетевых событий
 - [X] Необходимо настроить AAA-учет для системных событ
 - [X] Необходимо настроить AAA-учет для соединений
 - [X] Необходимо настроить сервис шифрования паролей

Информация

Результаты проверки

Сервис AAA : Вкл.
[hostname(config)#aaa new-model]

Список групп учета событий commands

Группа учета	Уровень привилегий	Процесс	Группа AAA
default	1	start-stop	group AAA

[hostname(config)#aaa accounting {commands 15} {default} {start-stop} {group tacacs+} [local-case ...]]

Список серверов TACACS+

Сервер TACACS+	Группа AAA	Сервер задан командой "tacacs-server host"
1.1.1.1	AAA	Нет
7.7.7.7	AAA	Да
2.3.4.5	tacacs+ (стандартная группа)	Да
7.7.7.7	tacacs+ (стандартная группа)	Да

[hostname(config)#tacacs-server host {ip-address server}]
[hostname(config)#aaa group server tacacs+ {name_group}]
[hostname(config)-sg-tacacs+)#server {ip-address server}]

Как исправить

Настройте AAA-учет для команд, используя следующие команды:
hostname(config)#aaa new-model
hostname(config)#tacacs-server host {ip-address server}



УПРАВЛЕНИЕ СООТВЕТСТВИЕМ



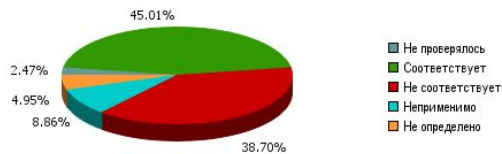
Контроль соблюдения стандартов

- **Compliance management. Контроль соответствия стандартам.**
 - Определили технические стандарты для ключевых систем
 - Согласовали их внутри организации
 - Контролируем их соответствие
- **Прозрачный контроль ERP систем, биллинга**
- **Контроль регионов, дочерних предприятий**
- **Результат: ИТ система в порядке с точки зрения ИБ.**



Результат сканирования в режиме "Compliance"

Compliance	Microsoft Windows XP
Задача	PCI DSS
Всего хостов	11
Начало сканирования	25.07.2008 09:11:50
Завершение сканирования	25.07.2008 09:56:03



хост	начало	конец	задача	результат
192.168.0.10	25.07.2008 09:12:31	25.07.2008 09:24:42	PCI DSS	Соответствует
192.168.0.11	25.07.2008 09:12:31	25.07.2008 09:24:07	PCI DSS	Соответствует
192.168.0.12	25.07.2008 09:12:31	25.07.2008 09:26:47	PCI DSS	Соответствует
192.168.0.13	25.07.2008 09:12:31	25.07.2008 09:25:02	PCI DSS	Соответствует
192.168.0.16	25.07.2008 09:22:22	25.07.2008 09:30:52	PCI DSS	Не соответствует
192.168.0.21	25.07.2008 09:23:10	25.07.2008 09:27:21	PCI DSS	Соответствует
192.168.0.22	25.07.2008 09:24:24	25.07.2008 09:36:39	PCI DSS	Не соответствует
192.168.0.52	25.07.2008 09:28:13	25.07.2008 09:55:58	PCI DSS	Соответствует
192.168.0.56	25.07.2008 09:28:20	25.07.2008 09:42:09	PCI DSS	Соответствует
192.168.0.55	25.07.2008 09:28:20	25.07.2008 09:38:51	PCI DSS	Соответствует
192.168.0.59	25.07.2008 09:28:52	25.07.2008 09:40:55	PCI DSS	Соответствует

Compliances

- Все Compliances
- Контрольный список проверок для коммутаторов
- Контрольный список проверок для маршрутизаторов
- Контрольный список проверок для протоколов маршрутизации
- Контрольный список проверок для Active Directory 2003
- Контрольный список проверок для Checkpoint Firewall-1
- Контрольный список проверок для Exchange 2003
- Контрольный список проверок для MS Office 2000/XP/2003
- Контрольный список проверок для Oracle 9i Server
- Контрольный список проверок для SAP R/3
- Контрольный список проверок для Solaris 8
- Контрольный список проверок для Solaris 9
- Контрольный список проверок для Windows 2000 Professional
- Контрольный список проверок для Windows XP Professional
- CIS - Cisco Firewall
- CIS - Cisco IOS
- CIS - Microsoft SQL Server 2000
- CIS - Microsoft SQL Server 2005
- CIS - Microsoft SQL Server 2008
- CIS - Microsoft Windows 2003**
- CIS - Sun Solaris 10
- PT - Microsoft Active Directory 2003
- PT - Microsoft Exchange 2003
- PT - Microsoft Office
- PT - Microsoft Windows 2000 Professional
- PT - Microsoft Windows XP
- PT - Oracle 9i Server
- PT - Sun Solaris 8
- PT - Sun Solaris 9

Информация

CIS - Microsoft Windows 2003

Контрольный список проверок для Microsoft Windows 2003

По всем хостам

Статус	Процент
Соответствует	55.42%
Не соответствует	33.47%
Неприменимо	10.01%
Не определено	1.10%

10.111.113.64 / IVANOVAVIN2K3 / IVANOVAVIN2K3

Статус	Процент
Соответствует	53.09%
Не соответствует	36.21%
Неприменимо	9.88%
Не определено	0.82%

10.111.113.45 / PT / PT

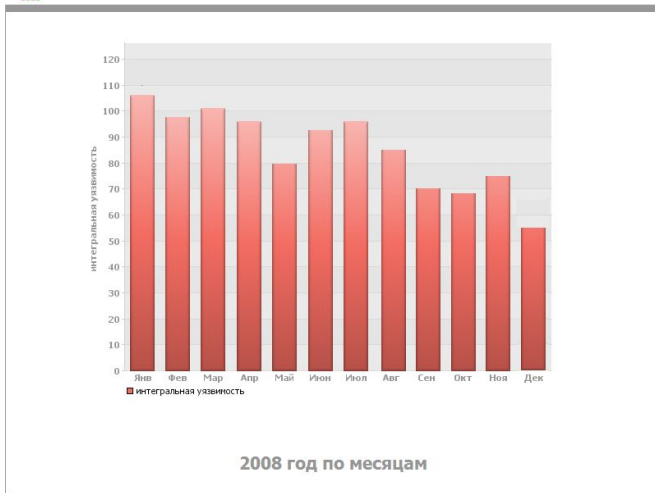
Статус	Процент
Соответствует	57.20%
Не соответствует	32.10%
Неприменимо	9.88%
Не определено	0.82%



Контроль эффективности. КРІ

- **Конфигурируемый набор метрик безопасности**
- **Метрики могут рассчитываться для различных групп узлов и подразделений**
- **Исторический анализ данных**

Финансовый отдел

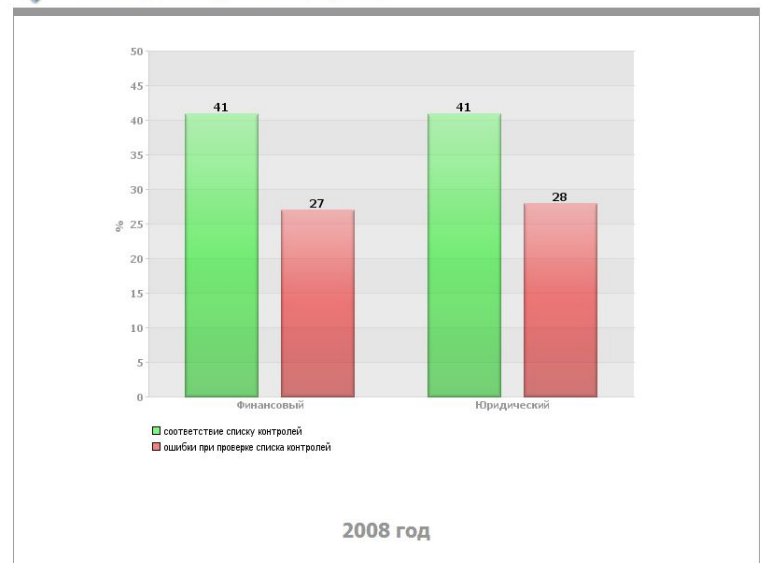


Расчет интегральной узвимости

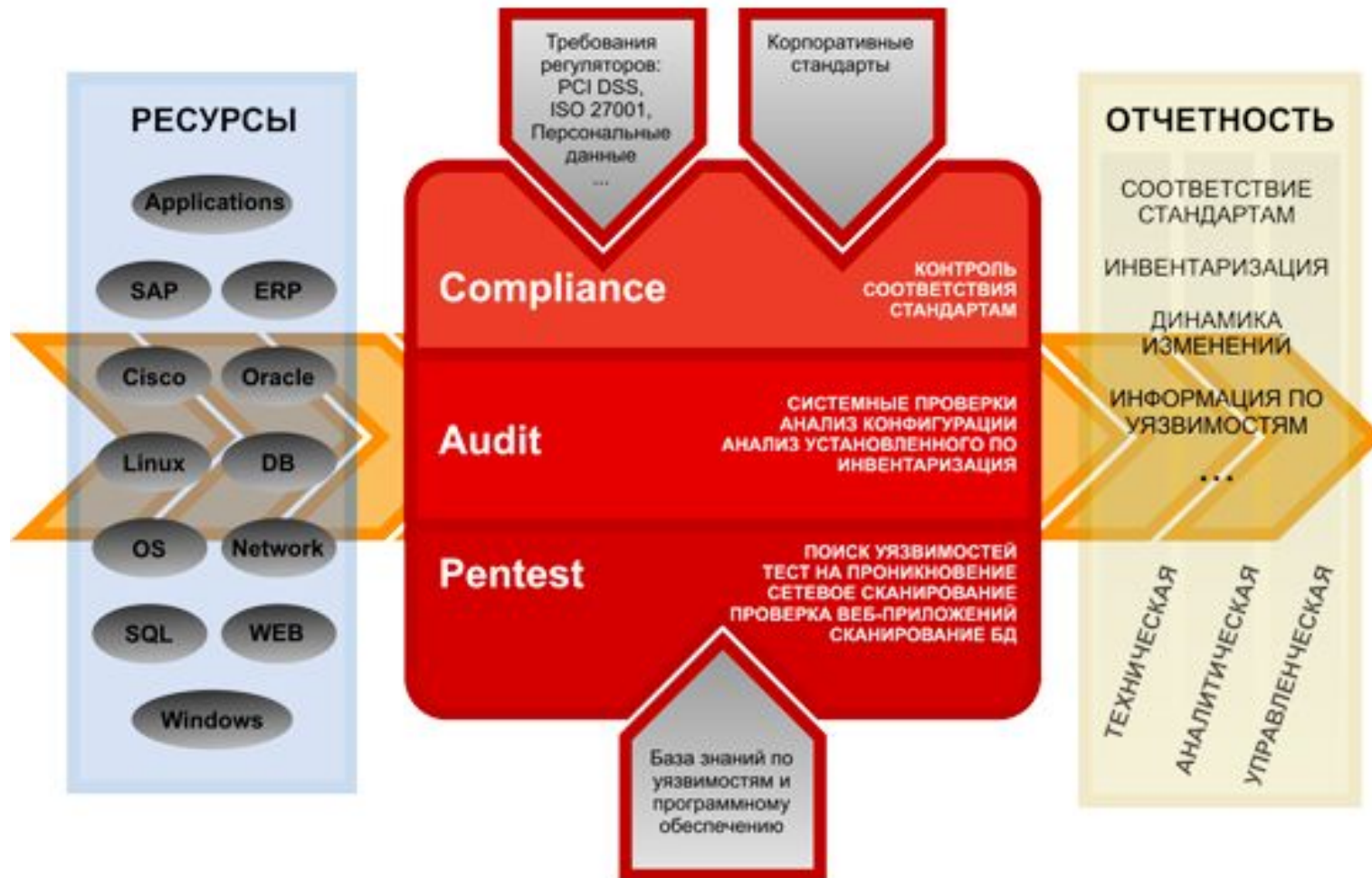
$$\text{Интегральная узвимость} = N_{\diamond} + 3 \cdot (N_{\diamond} + N_{\blacklozenge}) + 5 \cdot (N_{\blacklozenge} + N_{\blacklozenge})$$

N_i — число узвимостей соответствующего уровня

Статистика по заданным метрикам



Центр контроля защищенности на основе MaxPatrol



Спасибо за внимание!

Симис Борис Борисович
bsimis@ptsecurity.ru



POSITIVE TECHNOLOGIES