



УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ПО ITIL И РЕШЕНИЯ CISCO SYSTEMS

Алексей Лукацкий

Бизнес-консультант по безопасности

Содержание

- **Как правильно управлять безопасностью или что такое ITIL Security Management?**
- **Безопасность с точки зрения процесса и процесс с точки зрения безопасности**
- **Как автоматизировать процесс управления или создание ценности для клиента в единой точке контакта?**
- **Как Cisco Systems помогает найти ответы на эти вопросы?**

ПОЧЕМУ ТАК ВАЖЕН СТРУКТУРИРОВАННЫЙ ПОДХОД?



Внешние предпосылки

- **Растет число угроз безопасности**
- **Нехватка персонала для обеспечения управления безопасностью**
- **Конфликт между ИБ и ИТ**
- **Отсутствует единый центр управления ИТ-безопасностью**

Внутренние предпосылки

- **Служба ИБ хочет повысить свой статус в компании**
- **Служба ИБ борется с внешними конкурентами за право выполнять свою работу**
- **Служба ИБ хочет получать достойно за свою работу**

ЧТО ТАКОЕ ITIL?



Что такое ITIL?

- **ITIL – IT Infrastructure Library**

Это набор книг, а не методология

Собрание «best practices»

- **ИТ – это набор сервисов, которые могут предоставляться бизнес-потребителям и поддерживаться ИТ-службой в соответствии с четко описанными процессами**

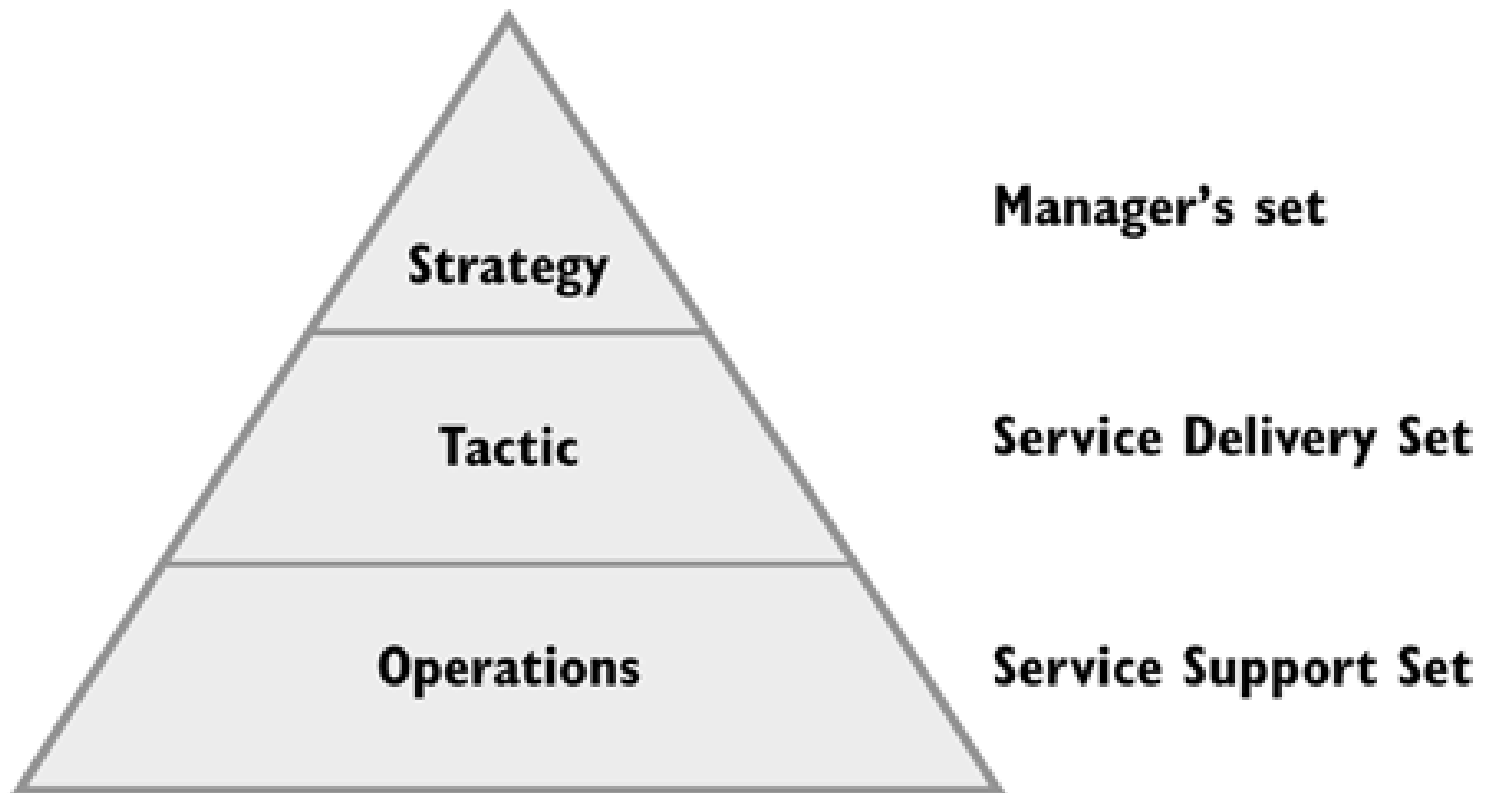
Нельзя внедрить ITIL, но можно внедрить процесс, описанный в ITIL

- **Процессы по ITIL направлены на выполнение требований заказчика/пользователя, а не просто достижение бесперебойной работы ИТ**

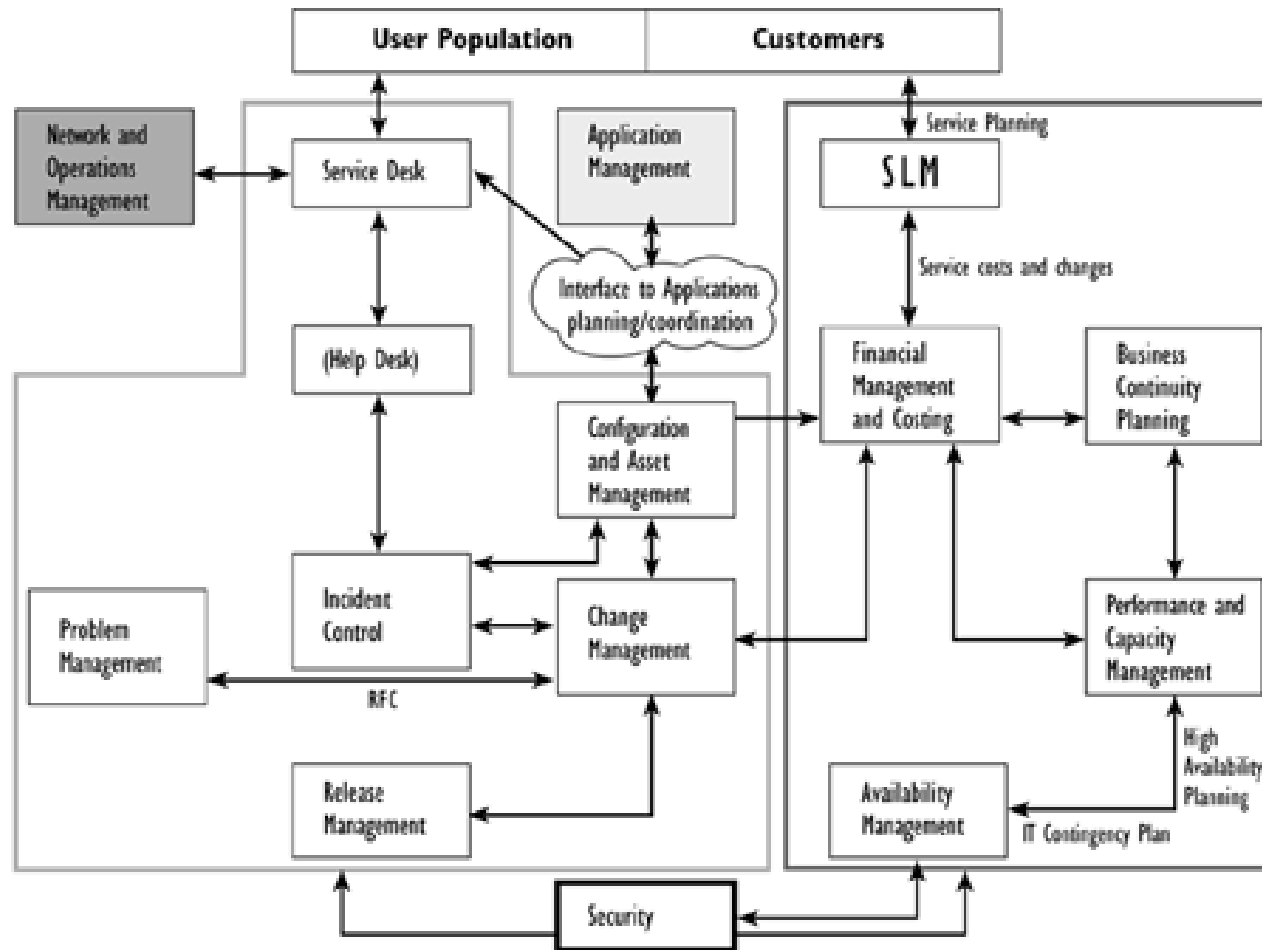
Как пришли к ITIL?

- **Главное - цель сервиса и метрики ее достижения**
Помимо метрики результативности есть еще и метрики эффективности процесса – насколько оправданы затраты
- **Улучшение процесса невозможно без регистрации информации, без которой нельзя оценить результат и эффективность процесса**
- **Имея информацию можно строить реальные планы по вносимым изменениям (изменения становятся осознанными)**
- **Результат изменений можно измерить и сравнить с исходными желаемыми результатами**
- **Процесс становится управляемым!**

Три уровня модели ITIL



Модель ITIL



Сначала был... Процесс

- **ITIL описывает цели и функции, входные и выходные параметры процессов, но не описывает способ их реализации, т.к. он может различаться от компании к компании**
- **Процесс - связанная последовательность действий, деятельности, изменений и т.д., совершаемая с целью достижения целей**
- **Управление процессом - процесс планирования и регулирования исполнения процесса эффективным способом**

Процесс



10 процессов ITSM – ядро ITIL

Предоставление сервиса

Service Level Management

ITSCM

Availability

Capacity management

Financial Management for IT Services

Service Desk

Поддержка сервиса

Incident management

Problem management

Configuration management

Change Management

Release management

Преимущества ITIL

- **Повышение удовлетворенности клиентов**
- **Увеличение возврата на инвестиции**
- **Улучшение климата в ИТ-службе**
- **Снижение текучки ИТ-кадров**
- **Понимание ролей для ИТ-персонала**
- **Снижение расходов на обучение**
- **Повышение доступности приложений и сервисов**
- **Увеличение производительности ИТ-службы**
- **Уменьшение расходов на обработку инцидентов**
- **Снижение скрытых издержек**
- **Эффективное использование ИТ-активов**
- **Снижение TCO**

ЧТО ТАКОЕ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ?



Управление безопасностью

- **Управление безопасностью – процесс управления заданным уровнем безопасности информации и сервисов**
- **Управление безопасности (по ITIL) – это**
 - с одной стороны отдельный, но не изолированный процесс (не входит в ITSM)**
 - с другой стороны процесс, очень тесно интегрируемый в другие ИТ-процессы**
- **Факторы успеха ITIL Security Management**
 - Понимание бизнеса-пользователей и их потребностей**
 - Написание и утверждение SLA**

Этапы процесса управления ИБ

- **Какие цели мы хотим достичь?**
Политика
- **Что надо сделать для достижения целей?**
Процесс
- **Кто должен это делать и когда?**
Процедуры
- **Как и где это делать?**
Инструкции

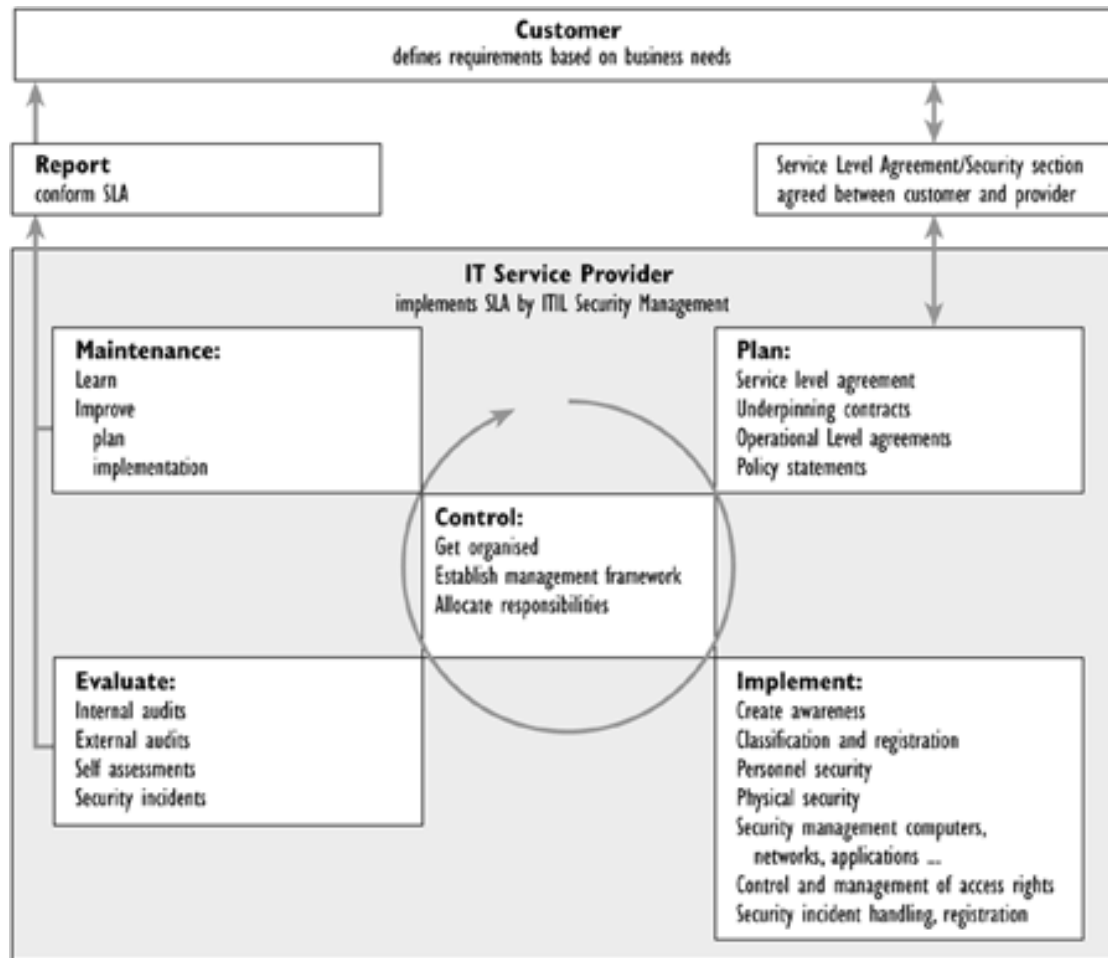
Безопасность, как процесс



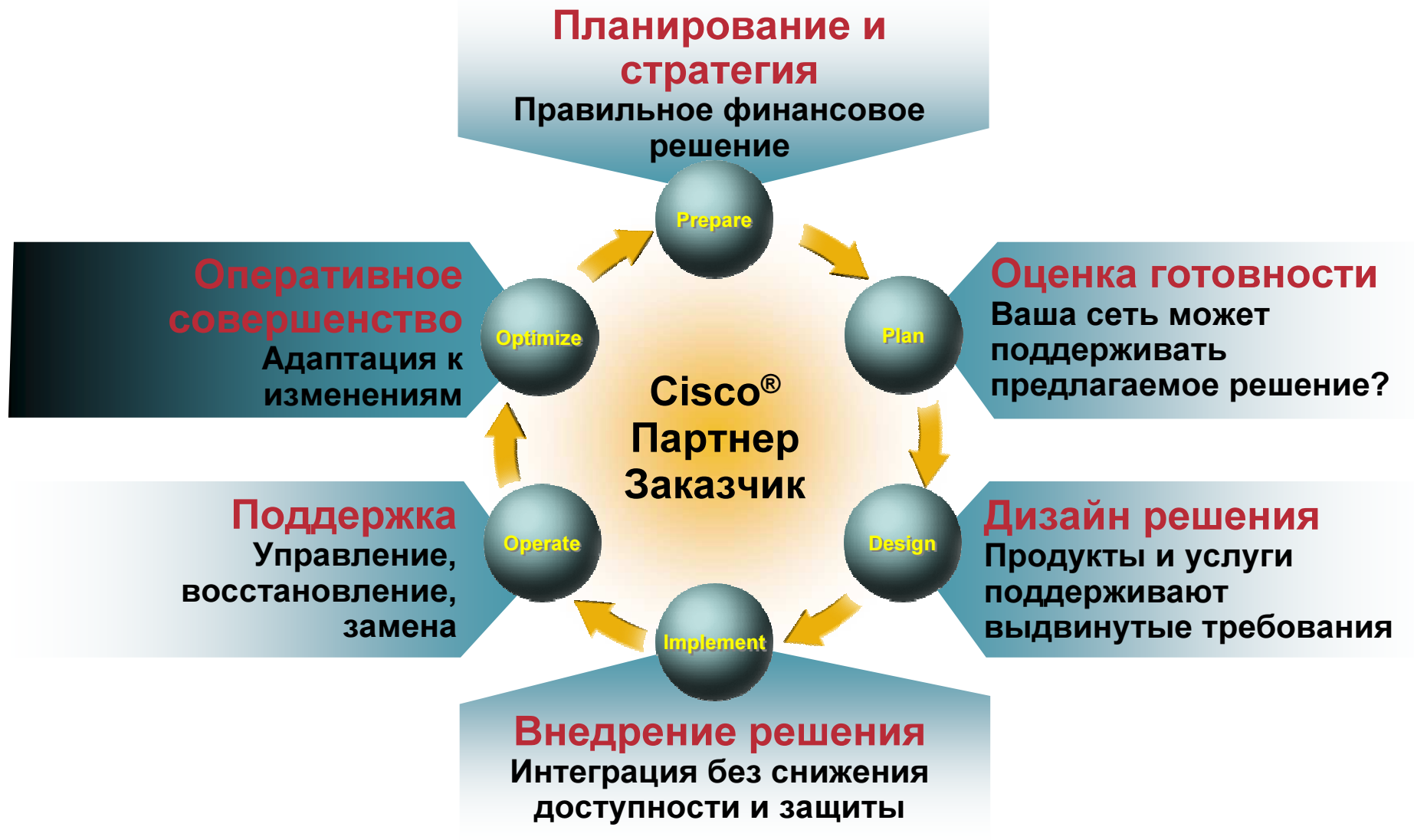
Этапы процесса

- **Переговоры с клиентом и оценка его требований**
- **Привязка специфических требований клиента к стандартным сервисам безопасности**
- **Определение необходимости создания специфического сервиса**
- **Определение и разработка SLA**
- **Разработка и поддержка каталога сервисов безопасности**
- **Анализ специфического для клиента уровня обеспечения сервисов**
- **Определение цикла обзоров уровня обеспечения сервисов**
- **Мониторинг сервиса с точки зрения клиента, создание отчетов, обзоры процесса**
- **Обсуждение результатов мониторинга с клиентом**
- **Предложения по улучшению сервисов**

Что внутри? Что клиент не видит?



Cisco Security Lifecycle (PPDIOO)



К этому надо быть готовым

- **Надо понимать, что переход на ITIL в области ИБ не только способствует улучшению качества этого сервиса, но и имеет другую сторону**

Вы должны будете оценивать стоимость своих услуг, а многие линейные руководители любят их получать «даром»

Не все готовы к формализации

Требуется совершенно иной уровень мышления и знаний

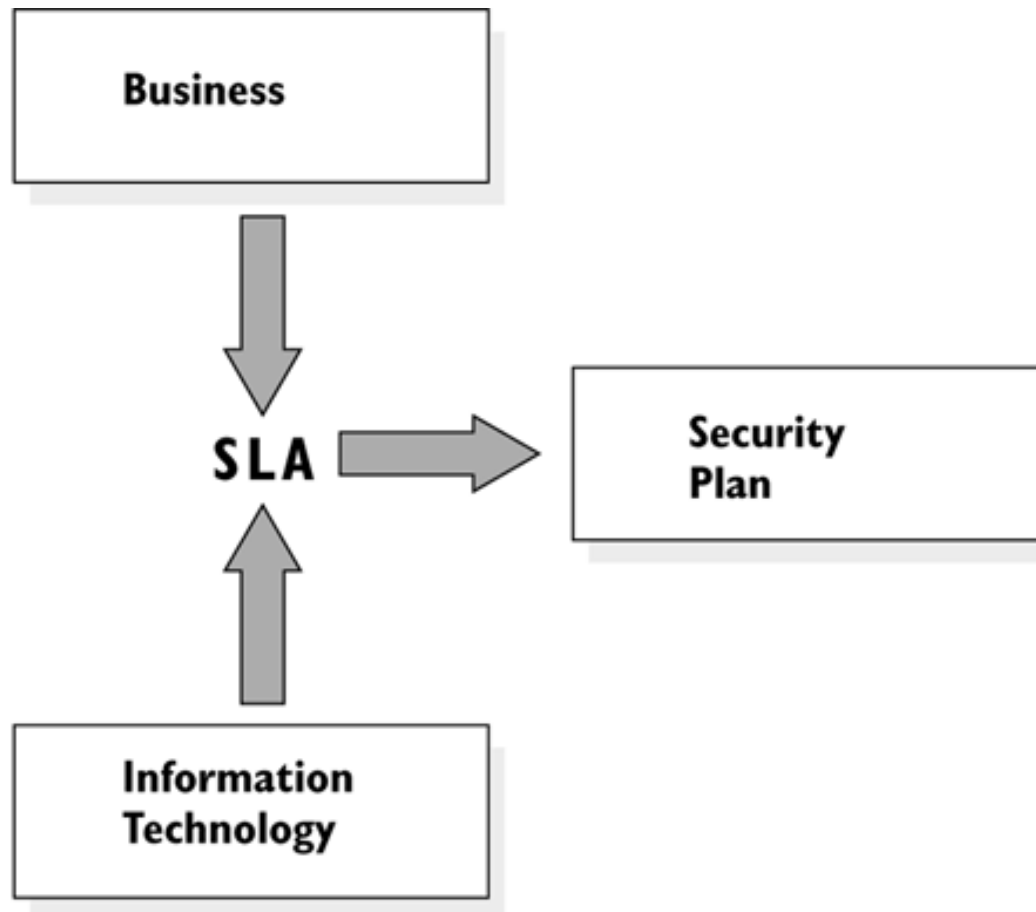
Вы должны будете соблюдать принятые обязательства и отвечать по ним

ОСОБЕННОСТИ ITIL SECURITY MANAGEMENT



Без SLA никуда

- **Качество сервиса измеримо**
- **Ключ – SLA, на основе которого сервис предоставляется бизнесу**



Как определить SLA?

- Провести анализ рисков
- Определить стоимость активов
- Определить уязвимые точки
- Оценить угрозы для бизнеса

Принципы или концепция?

Принципы

3-5 предложений или тезисов

Не требует специальных знаний

Доступно любому сотруднику

Может быть вывешено на сайте

Не меняется с течением времени

Концепция

Очень объемный документ

Мало кто читает

Требует специальных знаний

Требует изменений и повторных согласований при внедрении новых технологий, слияниях и т.п.

Российская специфика

- В России обычно нет понятия «принципы ИБ»
- В России концепцию обычно пишет не заказчик, а исполнитель, который считает, что его работу будут оценивать по объему и форме, а не содержанию
- На Западе понятие «Концепция ИБ» применяется к целому государству, а не отдельной компании
- На Западе есть понятие «политика безопасности», которая содержит набор конкретных рекомендаций

Повышение осведомленности

- **Безопасность, как культура компании**
- **Безопасность – забота каждого сотрудника**
- **Мультимедиа программы, eLearning и внутренний портал**
- **Ежегодный обязательный тренинг по безопасности для всех сотрудников**
- **Без этого внедрение процессного подхода обречено на неудачу**



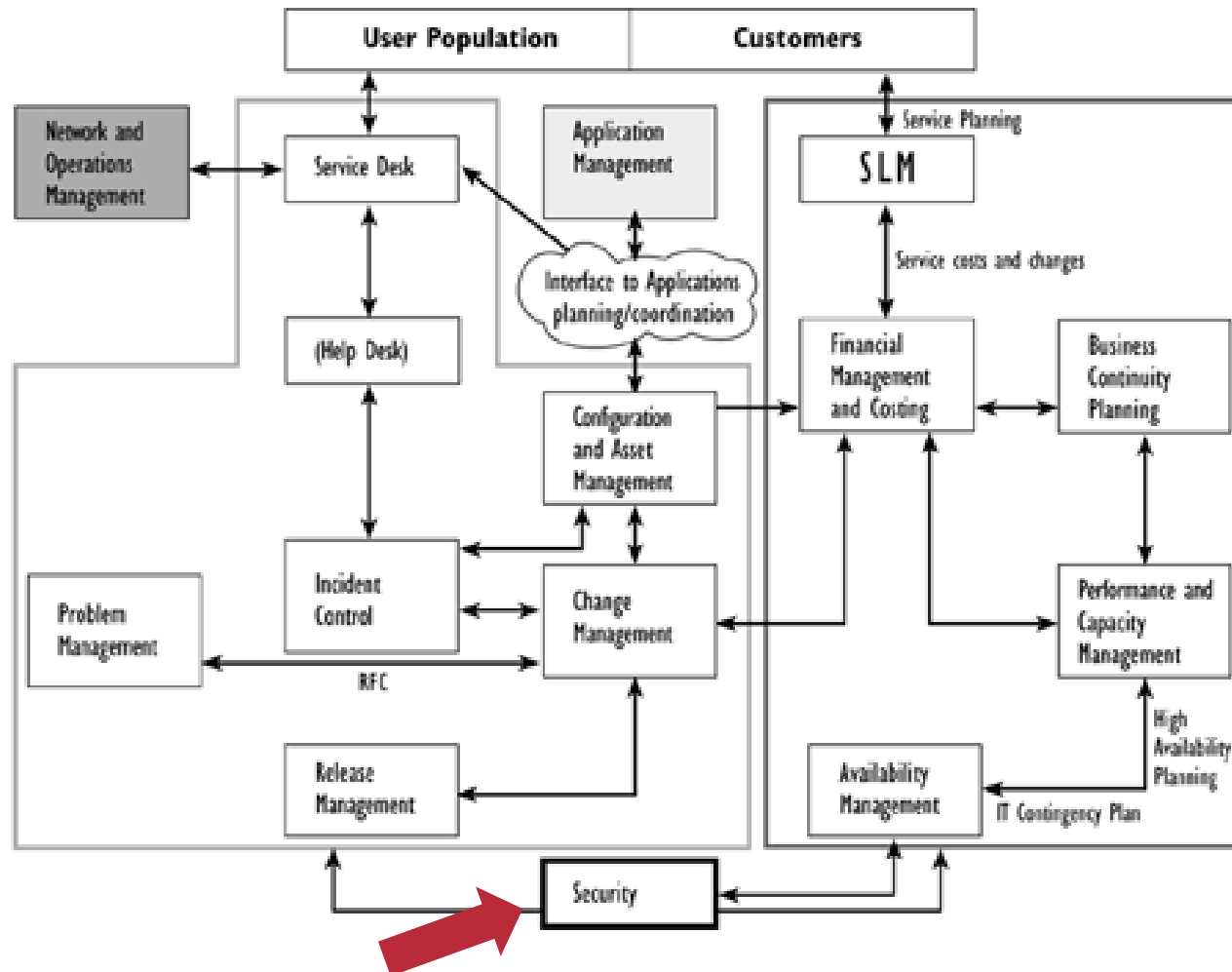
“Безопасность начинается с меня, CEO компании, и спускается вниз до каждого рядового сотрудника... это обязательно!”

**Джон Чемберс,
CEO, Cisco Systems®**

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ПО ITIL И РЕШЕНИЯ CISCO



Место безопасности в модели ITIL



Цели ITIL Security Management

- **Внешние**

 - Выполнение SLA

 - Соответствие законодательству и иным требованиям

- **Внутренние**

 - Обеспечение безопасности и непрерывности собственных сервисов службы ИБ

- **Безопасность – такой же сервис и для него необходимо соблюдать ITSM**

Безопасность – как сервис

- **Безопасность – такой же сервис и для него необходимо соблюдать ITSM**

Поддержка

Configuration & Asset
Incident Control
Problem Management
Change Management
Release Management

Предоставление

SL Management
Availability Management
Capacity Management
BCP
Finance Management

Управление инцидентами

- **Управление инцидентами**

Инцидент – любое событие, не являющее частью нормального функционирования сервиса и требующее ответной реакции

Процесс скорейшего устранения инцидентов

- **Решения Cisco**

Cisco MARS

Cisco SIMS

Решения Cisco Threat Management (например, Cisco IPS)

Этапы управления инцидентами

- Прием запросов (Accept calls)
- Регистрация инцидентов (Log incidents)
- Категоризация инцидентов (Categorize incidents)
- Приоритизация инцидентов (Prioritize incidents)
- Изоляция инцидентов (Isolate incidents)
- Эскалация инцидентов (Escalate incidents (within the process and/or to management))
- Отслеживание развития инцидента (Track incident progress)
- Разрешение инцидентов (Resolve incidents)
- Уведомление клиентов (Notify customers)
- Закрытие инцидентов (Close incidents)

Метрики управления инцидентами

- **Метрики**

Число зарегистрированных инцидентов

Продолжительность обработки и реагирования инцидента

Число инцидентов, переданных «не туда»

Число инцидентов на пользователя

Стоимость на инцидент

Customer Satisfaction Index

Self-resolution rate

Соблюдение SLA

Управление проблемами

- **Управление проблемами**

Процесс уменьшения числа инцидентов путем устранения причин их возникновения

Проблема – инцидент с неизвестной причиной

- **Решения Cisco**

Cisco SIMS

Cisco MARS

Cisco IntelliShield Alert Manager

Этапы управления проблемами

- **Анализ тенденций инцидентов (Analyze incident trends)**
- **Регистрация проблем (Log problem)**
- **Идентификация корневых причин инцидентов (Identify root cause)**
- **Отслеживание изменений проблем (Track problem progress)**
- **Выявление известных ошибок (Verify known errors)**
- **Управление известными ошибками (Control known errors)**
- **Решение проблем (Resolve problems)**
- **Закрытие проблем (Close problems/known errors)**

Управление конфигурацией

- **Управление конфигурацией**

Создание и поддержка в актуальном состоянии логической инфраструктуры

- **Решения Cisco**

Cisco MARS

CiscoWorks

Cisco IPS

Управление изменениями

- **Управление изменениями**

Допускать и контролировать только разумные изменения, невливающие негативно на бизнес

- **Решения Cisco**

Cisco Security Manager

Cisco Incident Control Manager

Cisco ACS

Cisco NAC

Управление релизами

- **Управление релизами**

Сохранить работоспособность при проведении изменений

- **Решения Cisco**

Cisco Security Manager

Cisco Incident Control Systems

Cisco MARS

Cisco Security Agent

Управление предоставлением сервиса

- **Управление уровнем сервиса**

Выявление требуемого состава и уровня ИТ-сервиса, слежение за его достижением, устранение некачественного сервиса

- **Управление финансами**

Обеспечить надежную финансовую базу для всех процессов

- **Управление мощностью**

Обеспечение компромисса между затратами и потребностями

Управление предоставлением сервиса

- **Управление непрерывностью**

Обеспечить гарантированное восстановление инфраструктуры в результате чрезвычайной ситуации

- **Управление доступностью**

Управление непрерывностью

- **Этапы обеспечения процесса**

- Анализ рисков**

- Стоимость активов**

- Выявление уязвимостей**

- Выявление угроз**

- Управление рисками**

- Разработка контрмер**

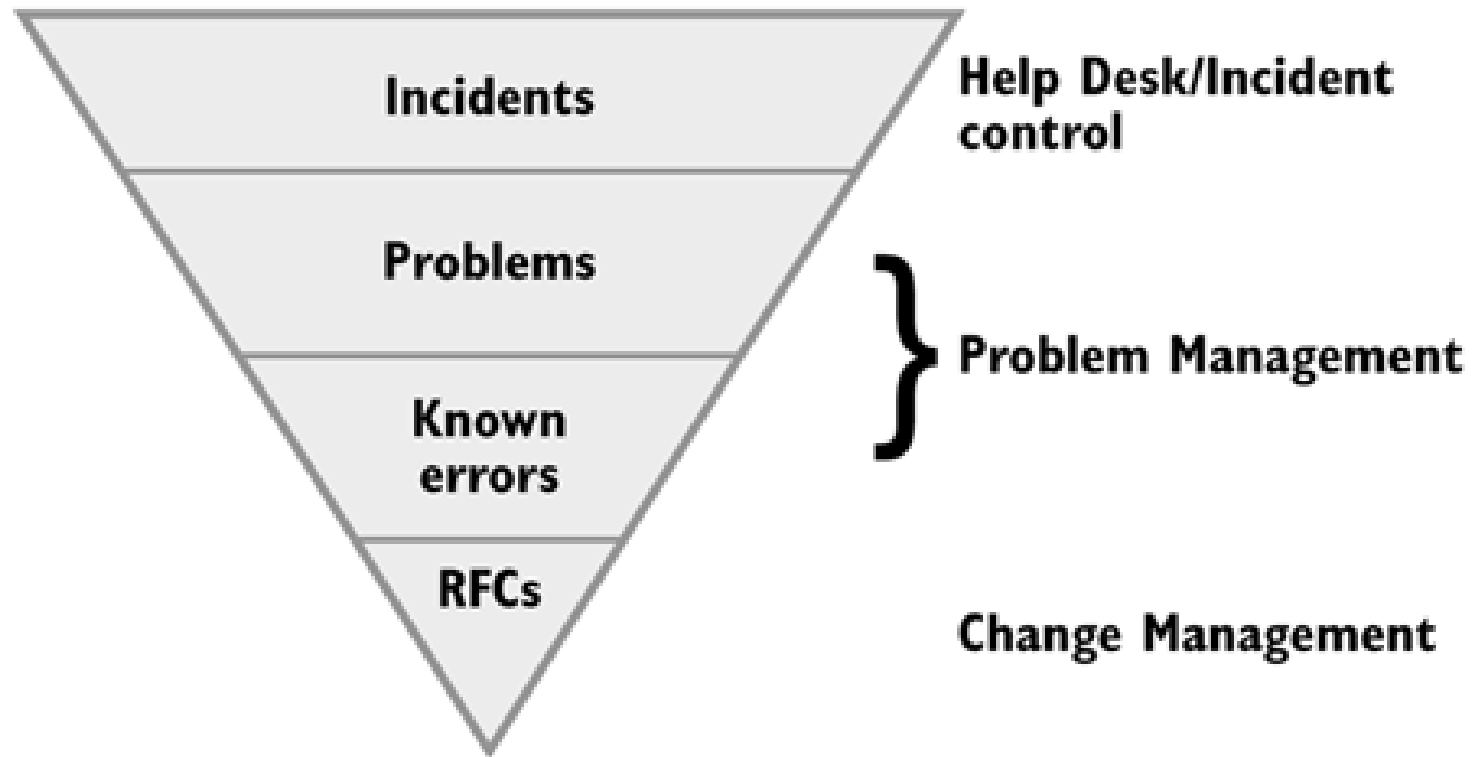
- Планирование деятельности при ЧС**

- Управление в условиях ЧС**

ОТ ХАОСА К УПРАВЛЯЕМОМУ ПРОЦЕССУ



Управляемый процесс



ИБ и ИТ – борьба и единство

Видим проблему, не понимаем причину

Снизилась скорость доступа к серверу

Web-сервер не отвечает

Высокая загрузка процессора

Непонятное сообщение на мониторе

Знаем причину, не видим проблему

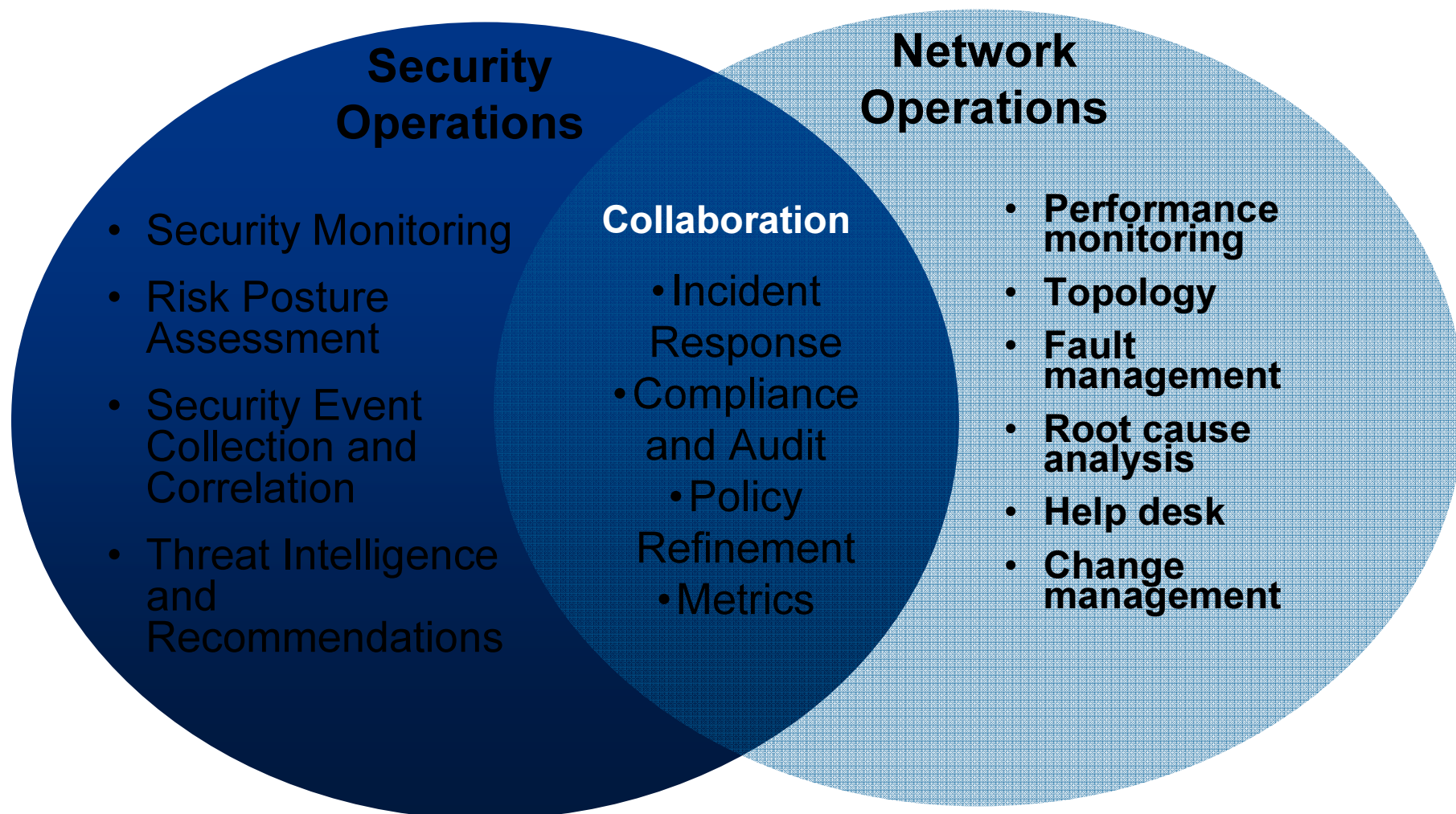
Идет эпидемия червя, а где источник?

Знаем как изолировать атаку, но не знаем где?

ИТ знали о падении Web-сервера, но ничего нам не сказали

Нам ничего не известно какие системы пострадали

Сила в партнерстве



Service Desk

- **Цели Service Desk**

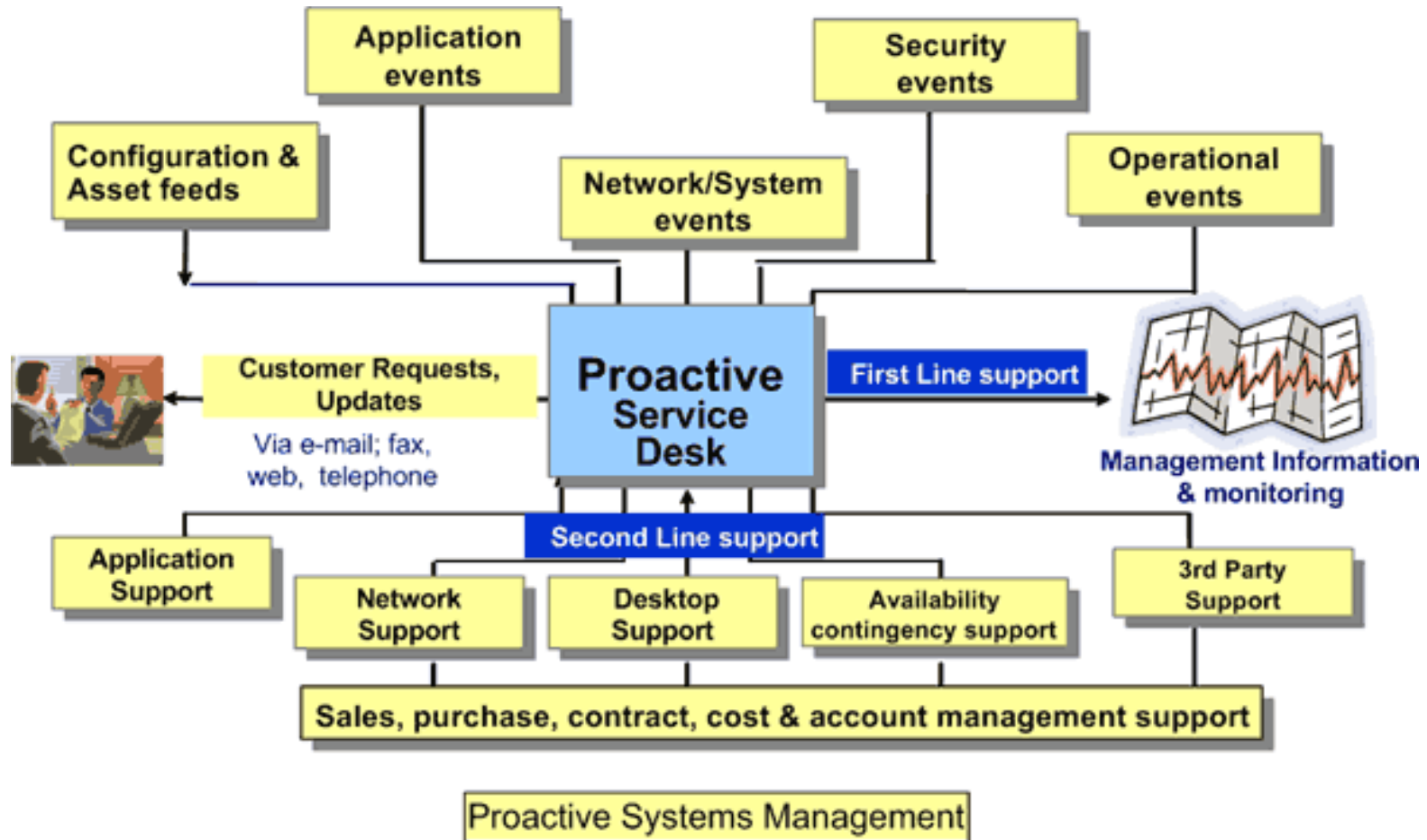
 - **обеспечивать единую точку контакта для клиентов**

 - **способствовать восстановлению нормальных действующих сервисов с минимальным влиянием на бизнес клиента в соответствии с согласованными уровнями сервисов и приоритетами бизнеса**

- **Цель SD – не установление и управление процессами, а создание ценности (не цены) для клиента (например, быстрое разрешение конфликта или устранение инцидента)**

- **Между целями SD нужно искать баланс**

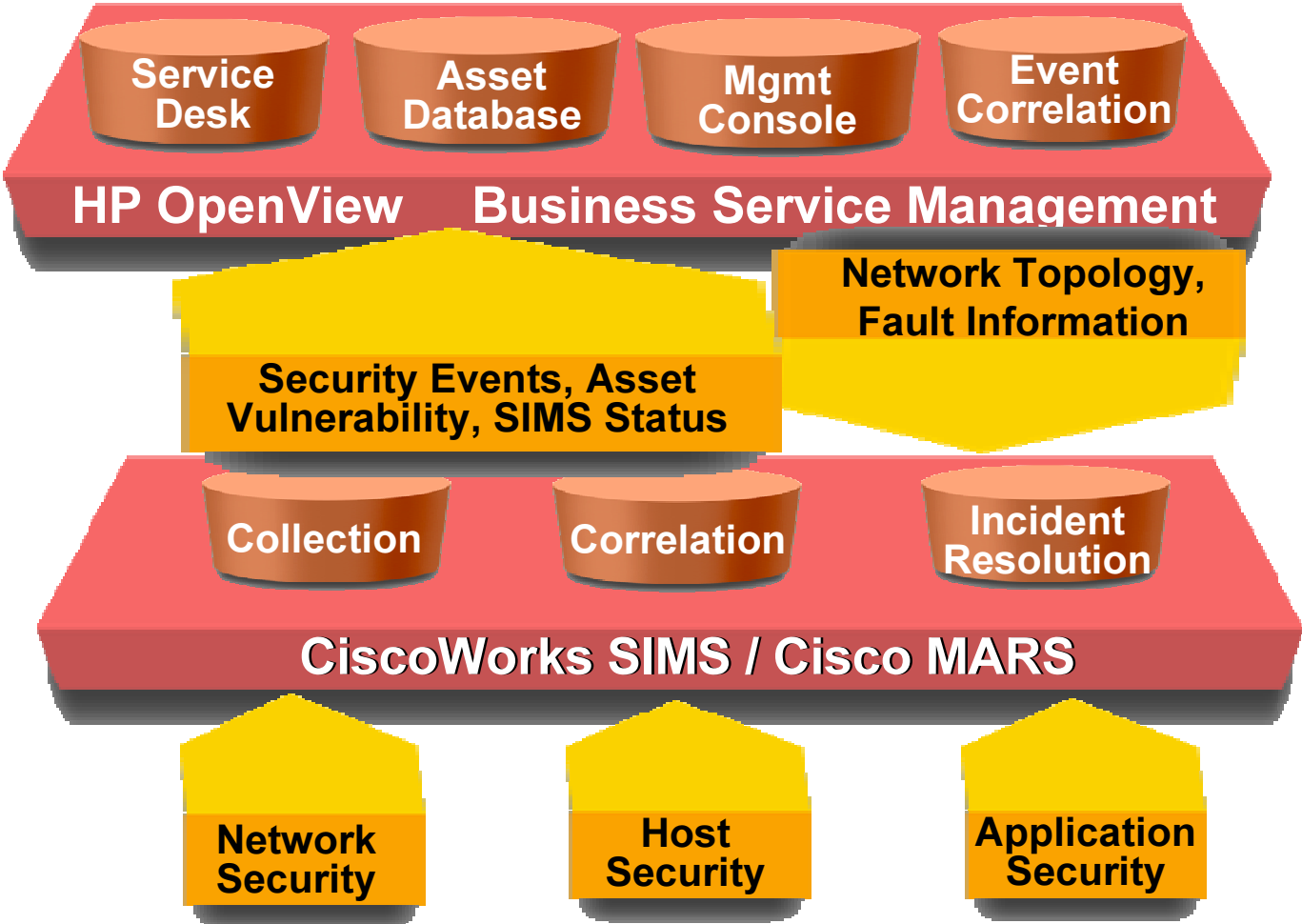
Архитектура Service Desk



ИНТЕРАЦИЯ РЕШЕНИЙ CISCO И HEWLETT-PACKARD



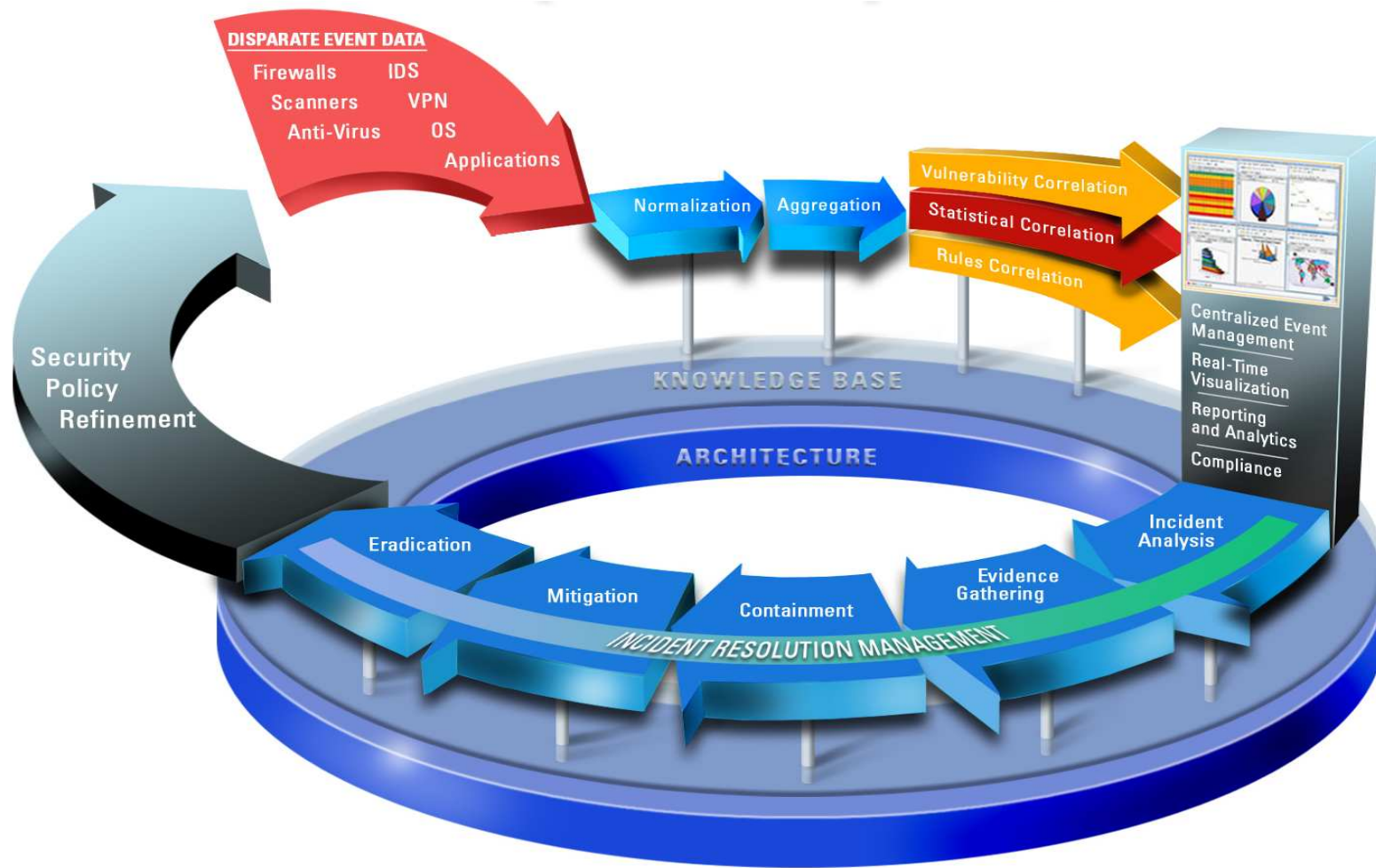
Cisco Security Management Suite и HP



Пути интеграции

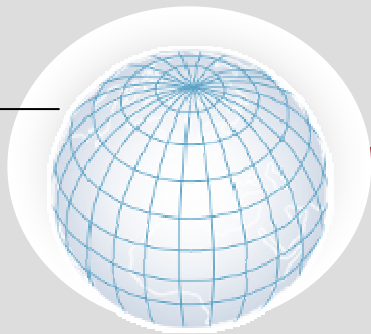
- **Cisco MARS → XML Incident Notification**
- **Cisco IntelliShield Alert Manager → XML Alert**
- **CiscoWorks SIMS → XML Notification**

CiscoWorks SIMS & Cisco MARS



Cisco IntelliShield Alert Manager

Global Source Network



- Организации по безопасности
- Государственные организации
- Производители
- «Хакерские» источники

Исследования и анализ



Сбор и оценка
Анализ и корреляция
Распространение

Генерация отчетов и бюллетеней

Cisco IntelliShield	
Linux/Unix: Xpdf Multiple Arbitrary Code Execution and Denial of Service Vulnerabilities	
Vulnerabilities: WU:ADV-2005-0428	
Threat Type: Unremediated Weakness: Multiple Vulnerabilities	Urgency: Unlikely Use
IssueID/Alert ID: 1893	Criticality: Confirmed
Version: 1	Severity: Mid Damage
First Published: Jan 18, 2005, 07:18 PM EST	
Last Published: Jan 18, 2005, 07:18 PM EST	
Ports: Not Available	
CVE: CVE-2005-0654, CVE-2005-0655, CVE-2005-0656, CVE-2005-0657	
Vendor Summary: Xpdf contains multiple vulnerabilities that could allow a remote attacker to cause a denial of service condition or execute arbitrary code. Patches are available.	
Description	Impact
Xpdf version 3.01 and prior contain vulnerabilities that could allow a remote attacker to execute arbitrary code or cause a denial of service (DoS) condition.	A remote attacker could exploit these vulnerabilities to cause a DoS condition or execute arbitrary code with privileges of the affected application.
The first vulnerability (CVE-2005-0654) results due to a lack of input validation in the COTFFactDoc class. A remote attacker could exploit this vulnerability by sending a specially crafted PDF file containing malicious parameters designed to cause an integer overflow or arithmetic overflow. This could result in a segmentation fault or allow the attacker to execute arbitrary code.	The first vulnerability (CVE-2005-0654) results due to a DoS (Denial of Service) condition. To cause an integer overflow or arithmetic overflow, a remote attacker could exploit this vulnerability by creating a PDF file with parameters containing integer overflow or negative integers. This provides the attacker with denial of service, but does not allow the attacker to execute arbitrary code.
The second vulnerability (CVE-2005-0655) results when a remote attacker sends a specially crafted PDF file to a remote system. A remote attacker could create a PDF file that forces a stream to end unexpectedly, resulting in a denial of service (DoS) condition on the affected system.	The second vulnerability (CVE-2005-0655) results when streams end unexpectedly. This vulnerability likely occurs in situations such as the COTFFactDoc and

Настраиваемые уведомления, Задачность, Аудит, Отчеты



ПРИЧИНЫ НЕУДАЧ



Причины неудач

- **Низкий уровень зрелости**
 - Люди «не готовы» (клиенты, ИТ или ИБ)
- **Люди – не автоматы и не всегда следуют «лучшим практикам»**
 - Специалист Help Desk мог не зарегистрировать инцидент, потому что он может повлиять на его друга или у него «нет времени» или не собрана полная информация
 - Зарегистрированная информация еще не значит, что в реальности все хорошо
- **Нет ресурсов для выполнения работ**
- **Не установлены цели или они не приоритезированы**

Причины неудач

- **Попытка съесть слона целиком**

Внедрение всех 10-ти процессов может занять от 3-х до 5-ти лет

- **Дело не доведено до конца**

- **Руководство компании не заинтересовано**

- **Не хватает людей для реализации «лучших практик»**

Одним-двумя людьми проблему не решить

- **Отсутствие четких инструкций**

- **Отсутствие владельца процесса**

Очень важно для безопасности, которая пересекает границы многих подразделений в компании

Причины неудач

- **Отсутствие единства между подразделениями, участвующими во внедрении**
- **Игнорирование других стандартов и практик (COBIT, ISO 27001, ISO 17799 и т.д.), а также законодательства**
- **Психология**
 - Единая точка контакта, как стена, отделяет ИТ от пользователя и он не прощает то, что простилось бы при личном контакте**
 - Формализация требует более высокого качества обслуживания**
- **Фокус на цифрах для результата, а не ценности для клиента**

Причины неудач

- **Отсутствие технологической инфраструктуры безопасности**
МСЭ, антивирусы, ID&PS и т.д.

ЗАКЛЮЧЕНИЕ



В качестве заключения

- **ITIL – это не панацея – успех зависит от множества факторов**
- **ITIL – не догма – адаптируйте и улучшайте**
- **Решения Cisco могут быть внедрение в соответствие с ITIL**



**Дополнительные вопросы Вы можете
задать по электронной почте
security-request@cisco.com
или по телефону: (495) 961-1410**

CISCO SYSTEMS

