

Централизованное управление угрозами и инцидентами. Eventia Suite

13 ноября 2007

Игорь Левен

Директор учебного центра

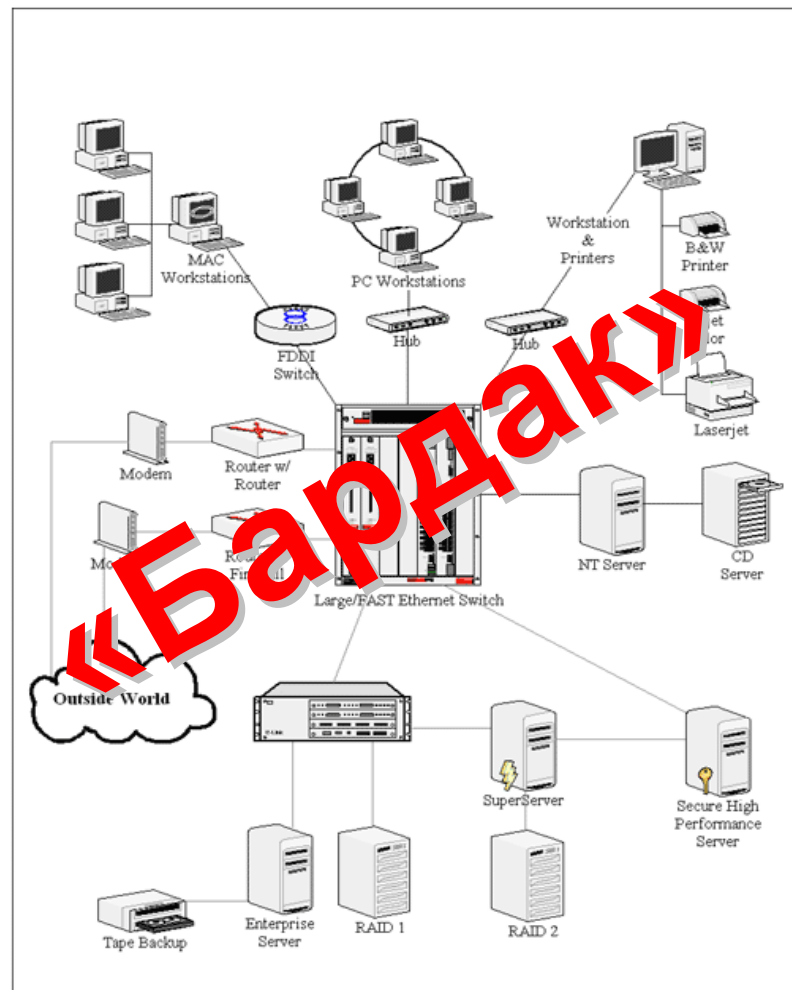
iloewen@ntc.ru

+7 (495) 580 9902

С точки зрения компании...



- Слишком много устройств безопасности в инфраструктуре
 - FireWalls, VPn devices, Anti-Virus, IPS, end-point security solutions, Application FireWalls, etc.
- Слишком много продуктов, выдающих события, связанные с безопасностью :
 - Routers and Switches with ACLs, OS, Web Applications, etc.



С точки зрения администратора...



- Устройства протоколируют миллионы записей в день/неделю
 - Как узнать, что произошло событие, важное для безопасности ?
 - Как автоматически получать уведомление?
- Как часто администратор просматривает такие журналы ?
- Описаны ли процедуры и выделены люди, чтобы важная информация не была пропущена?



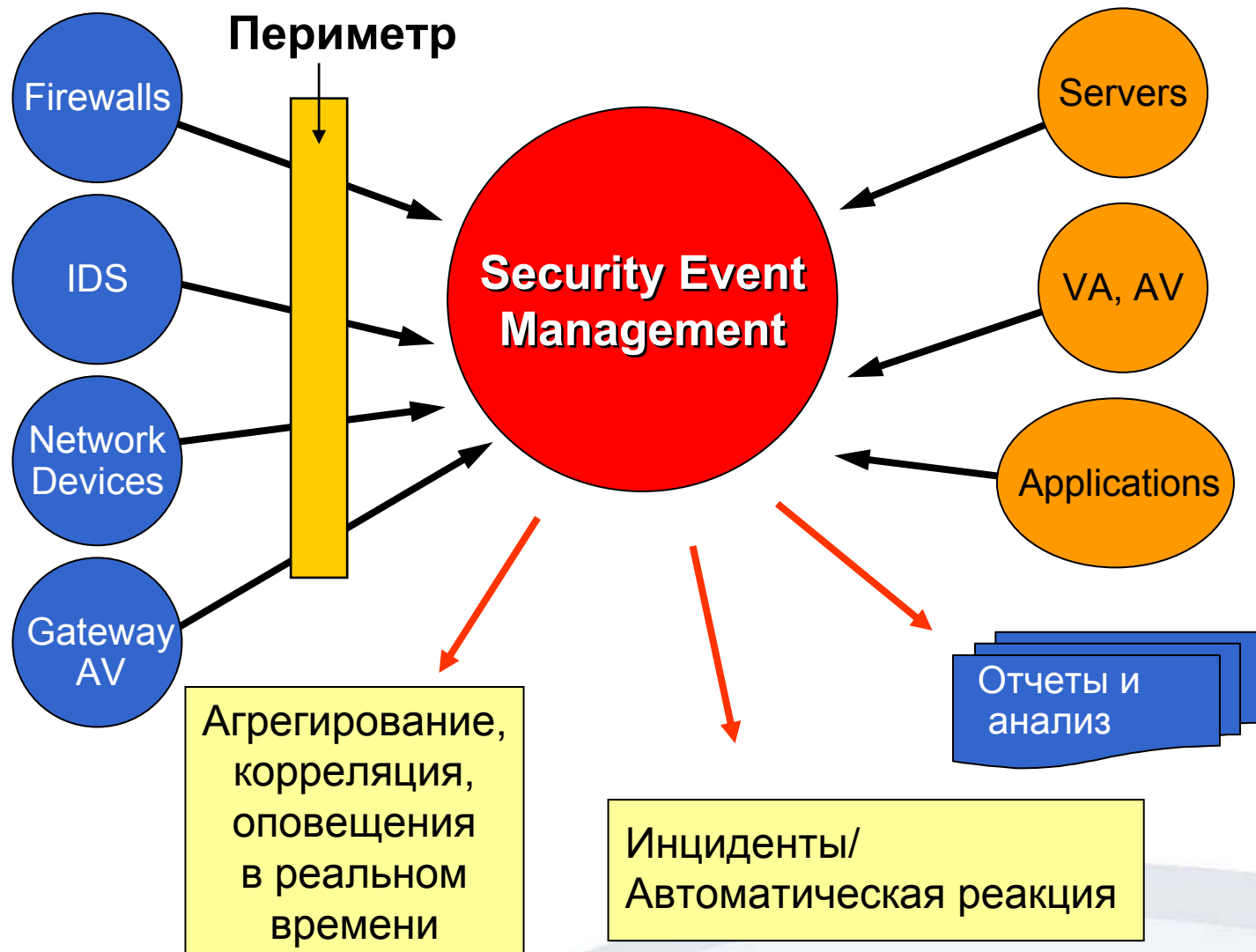
С точки зрения руководителя IT...



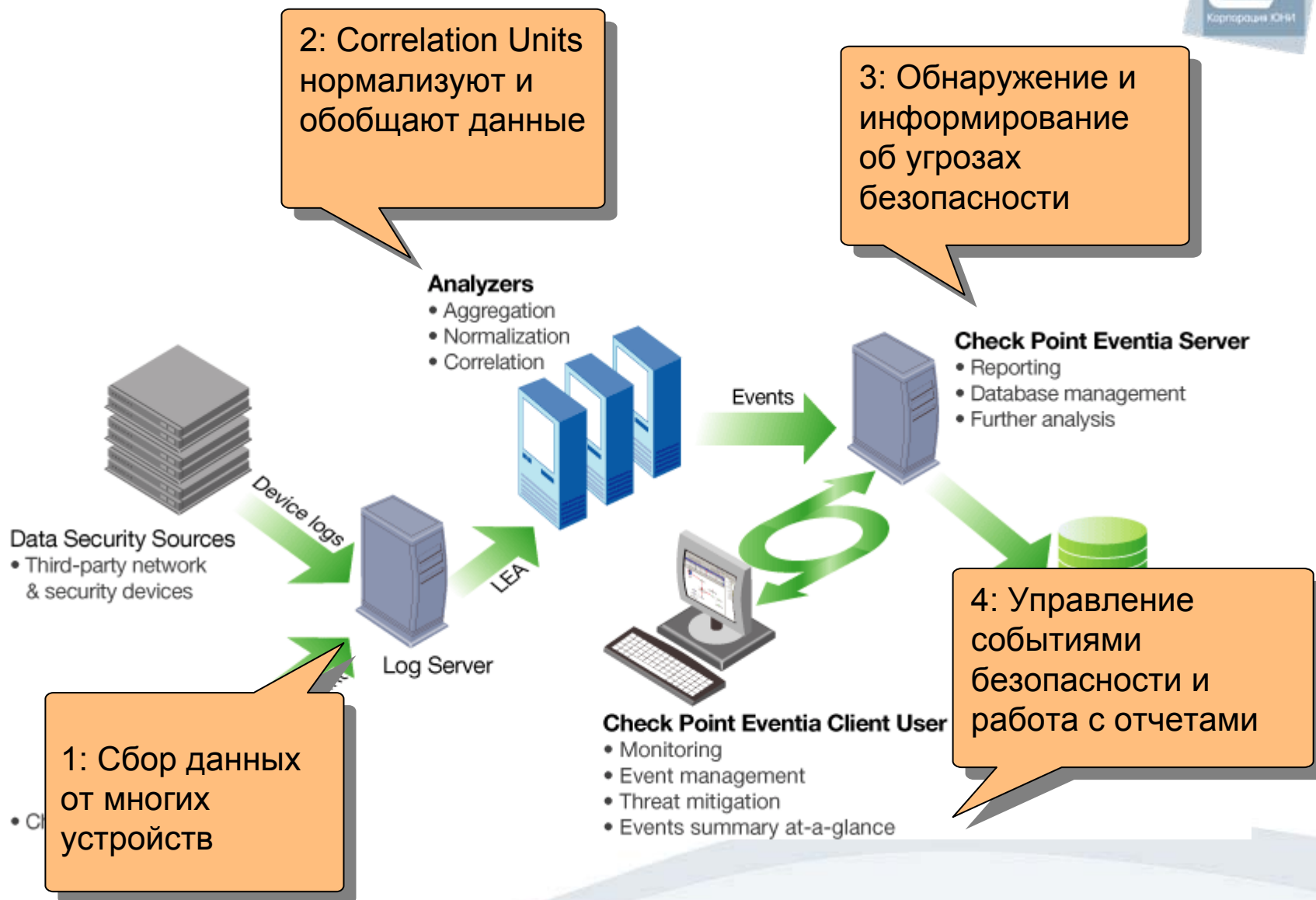
- На IT безопасность тратятся существенные средства
- Безопасность IT важна для компании
- А есть ли уверенность, что в случае инцидента с безопасностью о нем станет известно раньше, чем будет нанесен ущерб?
- Регулярно ли формируются и анализируются отчеты о произошедших инцидентах с безопасностью?
 - Иными словами, есть ли осведомленность о том, что происходит?
- Предоставляется ли руководству реальная информация для подтверждения/обоснования бюджета на IT безопасность?

SIM (Security Information Management)

SEM (Security Event Management)



Обзор Eventia Analyzer



Check Point Eventia Analyzer

помогает снизить риски



Анализ угроз в реальном времени

Глубокий анализ критичных событий

***local - Check Point Eventia Analyzer Client**
File View Actions Query Help

Overview Events Policy Reports

Custom
Untitled
Predefined
All Events
By ID
By Severity
By State
By Time
Current hour's events
Today's events
Current week's events
By Type
Scans
Probes
Denial Of Service
Unauthorized Entry
Anomalies
Host Based Events
Externally Identified
Informational

Current hour's events

ID	Start Time	End Time	Severity	Name	State	Source	Destination
EN0000...	10:28:57...	10:29:00...	Low	Alert from gateway	Open		
EN0000...	10:28:09...	10:28:59...	Low	Port scan from external ...	Open	client1 (10.0.0.1)	SmartCenter_s...
EN0000...	10:26:38...	10:26:38...	Low	Alert from gateway	Open		
EN0000...	16:53:18...	17:29:00...	Low	Alert from gateway	Open		
EN0000...	14:37:55...	14:39:29...	Critical	Check Point administrator credential query	Open		
EN0000...	18:11:11...	18:11:11...	Low	Alert from gateway	Open		
EN0000...	17:15:02...	17:19:26...	Critical	Check Point administrator credential query	Open		
EN0000...	17:07:12...	18:39:23...	Low	Check Point administrator credential query	Open		
EN0000...	16:54:50...	17:23:52...	Low	Alert from gateway	Open		
EN0000...	15:03:41...	15:03:45...	Low	Alert from gateway	Open	client2 (10.0.0.2)	SmartCenter_s...
EN0000...	15:03:41...	15:03:41...	Low	Alert from gateway	Open	client2 (10.0.0.2)	SmartCenter_s...
EN0000...	15:03:36...	15:03:44...	Low	Port scan from external ...	Open	client2 (10.0.0.2)	SmartCenter_s...

Previous Next Copy Raw data Change State

Critical Check Point administrator credential query
A suspicious user (N/A) is trying to login to Check Point Eventia Analyzer Client time (5 failures in 1 minute and 34 seconds).

Field	Value	Field	Value
Start Time	14:37:55 21 Nov 2004	Source	N/A
End Time	14:39:29 21 Nov 2004	Description	N/A
Update Time	15:09:57 21 Nov 2004	User	N/A
Origin	SmartCenter_station (10.0.0.0)	Service	N/A
Detected By	10.0.0.2	Direction	N/A
Event State	Open	Num Conns	5 (5 accepted by the firewall)
Product Name	Eventia Analyzer Client	Peak Conns	5 conns within 600 seconds
Additional Info	N/A		

Ready Demo Mode Number of records in grid: 16 No new Events

Check Point Eventia Analyzer облегчает управление безопасностью



Предопределенные события

Легко настраивать политики

Event policy

- Global Exclusions
- Scans
- Third Party Devices - User Configured Events
 - ☒ User configured Snort events
 - ☒ User configured Cisco events according to m
 - ☒ User configured Cisco events according to m
 - ☒ User configured NetScreen events
 - ☒ User configured ISS Proventia events
 - ☒ User configured IntruShield events
- Denial Of Service
 - ☒ High rate of blocked connections
 - ☒ High connection rate to internal host on serv
 - ☒ High connection rate to external host on ser
 - ☒ LAND attack
 - ☒ Ping of death attack
 - ☒ Teardrop attack
 - ☒ Winnuke attack
 - ☒ VPN - SSL Null pointer assignment
 - ☒ Malicious code detected
 - ☒ Potential resource abuse
 - ☒ Badly fragmented packets
 - ☒ Other denial of service
- Unauthorized Entry
- Virus Alert
 - ☒ Viruses and worms
 - ☒ Attempt to send virus past firewall
 - ☒ Virus Alert
 - ☒ Virus Outbreak
- Anomalies
 - ☒ High connection rate from internal host on se
 - ☒ High connection rate from external host on s
 - ☒ High connection rate from internal host
 - ☒ High connection rate from external host
 - ☒ High connection rate from interface
 - ☒ High connection rate to interface
 - ☒ Abnormal activity on service
 - ☒ High connection rate on rule
 - ☐ High error rate on web server from internal t
 - ☐ High error rate on web server from external
 - ☒ High mail rate from user
 - ☒ Bad/non-standard packet
 - ☒ Insecure options/variants of protocols
 - ☒ Abnormal connection - possible attack
 - ☒ Insecure protocols
 - ☒ High report rate from important facility
- Host Based Events

Exclude the following events:

Filter: All

Customer	Source	Destination	Scan Direction	Scan Result	Origin Type

Add... Edit... Remove

Apply the following exceptions to the event definition:

Filter: All

Customer	Source	Destination	Scan Direction	Virus Name	Scan Result	Origin Type

Attempt to send virus past firewall

Description: An attempt was made to send a virus through the firewall.

Supported devices: • Express CI Anti Virus

Last Update: 18-Jan-2006

Ready Demo Mode NUM

Поддерживаемые ИСТОЧНИКИ



- All Check Point Perimeter, Internal and Web security gateways
- Cisco Routers & Switches
- 3rd party firewalls - CiscoPIX, Juniper
- IDS devices such as Snort & ISS Proventia, Cisco IDS, McAfee Intrushield
- Unix operating systems (Solaris, Linux, Windows)
- Web application servers (Apache)
- Anti-virus devices (Trend Micro)

Поддерживаемые источники

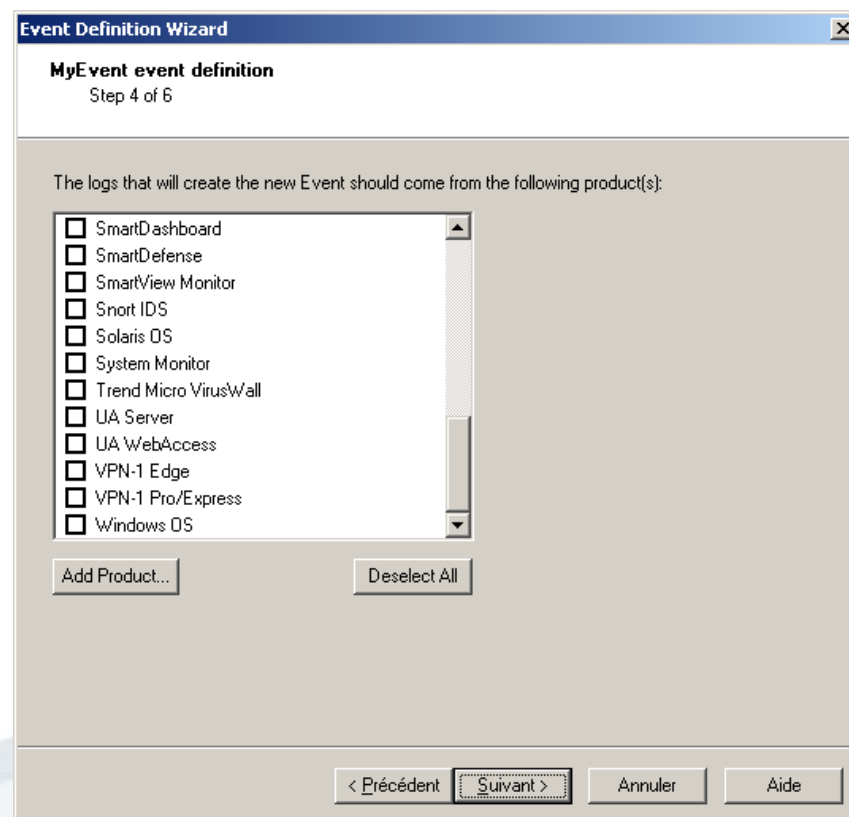
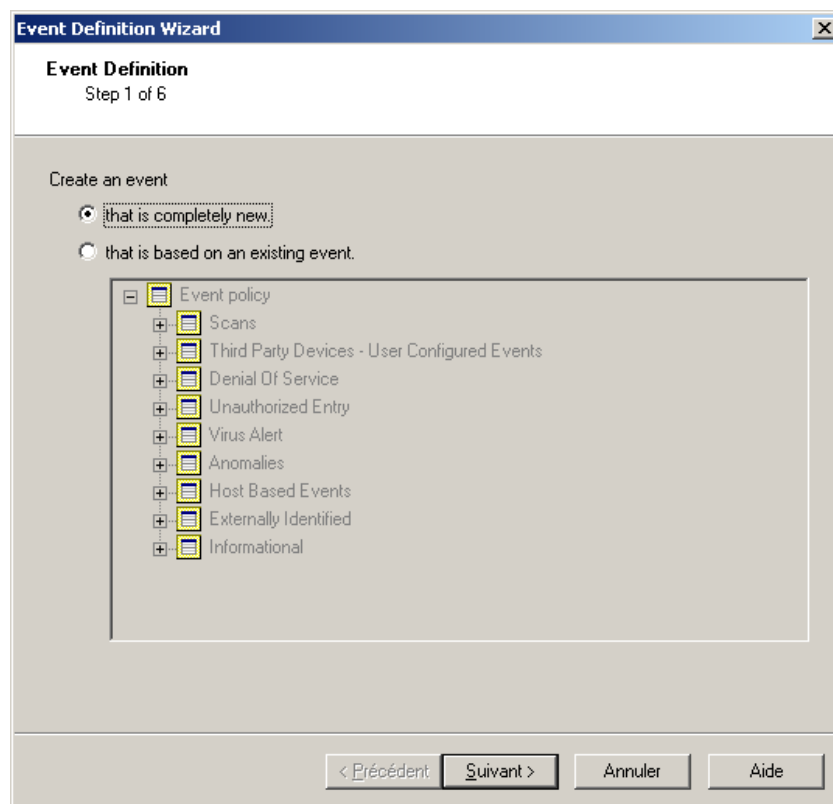


Product Category	Vendor	Product Name	Via
Anti-Virus	Check Point	Express Cl	Native
	Symantec	Symantec Anti-Virus	SNMP Traps
	TrendMicro	Trend Micro Anti Virus	SNMP Traps
Application Gateway	NetContinuum	NetContinuum Application Security Gateway	Syslog
End Point FW	Check Point	Integrity	Native
Firewall	Check Point	VPN-1	Native
	Check Point	VPN-1 Edge	Native
	Cisco	PIX	Syslog
	Juniper	Netscreen	Syslog
IDS/IPS	TippingPoint	TippingPoint	Syslog
	Open source	SNORT	Syslog
	Check Point	InterSpect	Native
	Cisco	Cisco IDS/IPS on router	Syslog
	ISS	Proventia	SNMP Traps
	McAfee	IntruShield	Syslog
Mail Server	Open source	Sendmail	Syslog
Network Monitoring	Standard	RMON	SNMP Traps
OS	Check Point	SecurePlatform	Syslog
	Microsoft	Windows	Remote Agent
	Nokia	IPSO	Syslog
	Open source	Linux	Syslog
	Sun	Solaris	Syslog
Remote Access	Check Point	Connectra	Native
Router	Cisco	Cisco Router	Syslog
Switch	Cisco	Catalyst	Syslog
	Cisco	Cisco	Syslog
	Nortel	BayStack	SNMP Traps
Web Server	Open source	Apache	Syslog

Настраиваемые события



- Администратор может создавать собственные события безопасности



Режим самообучения



- В каждой компании своя собственная структура сети, архитектура безопасности
 - Например, в DMZ может стоять сканер безопасности и т.п.
- Решение SEM должно легко обрабатывать такие исключения
- Так называемый режим самообучения «self-learning mode»
 - Дайте Analyzer поработать несколько дней
 - Self-Learning Mode предложит оптимальную политику для вашего окружения
 - Можете выполнить тонкую настройку

Автоматические реакции на события



- Администратор безопасности будет извещен о событии
 - Также предусмотрена автоматическая реакция
 - Может настраиваться индивидуально для каждого события

Attempt to send virus past firewall

Severity: High

Automatic Reactions: [] [+]

Exclude the following combinations:

Filter: All

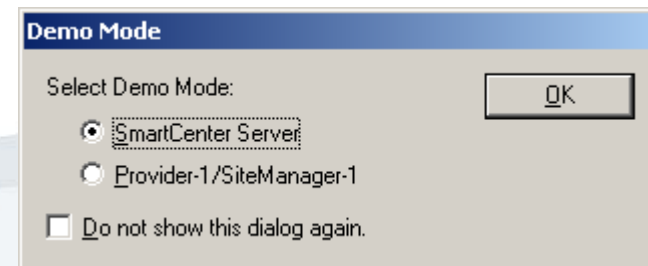
Customer	Source	Destination	Sc...
----------	--------	-------------	-------

Automatic Reactions		
Name	Type	Comment
<input checked="" type="checkbox"/> Block Source example	Block Source	Example for Block Source automatic reaction.
<input checked="" type="checkbox"/> Block Event Activity example	Block Event Activity	Example for Block Event Activity automatic reaction.
<input checked="" type="checkbox"/> Mail example	Mail	Example for Mail automatic reaction.
<input checked="" type="checkbox"/> External Script example	External Script	Example for External Script automatic reaction.
<input checked="" type="checkbox"/> Snmp Trap example	SNMP Trap	Example for Snmp Trap automatic reaction.

Интеграция с Provider-1



- Analyzer читает объекты и записи из протоколов работы Provider-1
 - Подключается к MDS и получает Global Objects, равно как и CMAs Objects
- SIC устанавливается с MDS
- Может использовать Provider-1 “Customers” в описании события
- Дополнительные настройки «Enterprise»



Отчеты



1. Security Events By Severity




Security event occurrence

Severity	Event	Number of Events	Average Daily Events (since system
Critical	SecureClient authentication failure	1	This table shows security event occurrence, sorted by severity
	All Events	1	
High	High connection rate from internal host on service	155	13
	Port scan from internal network	106	9
	IP sweep from internal network	102	9
	Port scan from external network	49	4
	IP sweep from external network	36	3
	All Events	448	37
Medium	Bad/non-standard packet	111	9
	High connection rate from internal host on service	65	5
	Connection from blocked source (SAM)	59	5
	Insecure options/variants of protocols	33	3
	Abnormal activity on service	15	1
	High connection rate from external host on service	8	1
	Multiple user access from single IP	6	1
	Policy installation	2	0
	All Events	299	25
Low	All Events	3	0
Informational	All Events	0	0

События Windows



- Analyzer читает события Windows
- Для этого требуется агент, установленный на машину с Windows
 - Достаточно единственной машины с Windows, которая будет мониторить остальные

Software Subscription Downloads			
Eventia Analyzer, v2.0 on Windows			
Software			
	Eventia Analyzer 2.0 SmartConsole Installation Package for Windows		
MD5:	5ded93fee66d0474d49028248c289e7f	Last updated:	15-Mar-2006
SHA1:	7564e5a8fe9566705c6c22961c7ecb57d36b0b8e	File size:	35.79 MB
	Eventia Analyzer 2.0 Software Installation Package for Windows		
MD5:	6137349a6e0c46fe96dd5bdce2082c20	Last updated:	08-Mar-2006
SHA1:	cf0121ca92c2473be10bd232e8bf335212187c77	File size:	34.05 MB
	Eventia Analyzer 2.0 WinEventToCPLLog Software Installation Package for Windows		
MD5:	f341bdfae8a5b8b8cbb649512f0ed844	Last updated:	08-Mar-2006
SHA1:	06dbc118c6e1dfa8434c434e3d72d76690856f8d	File size:	8.26 MB

События Windows

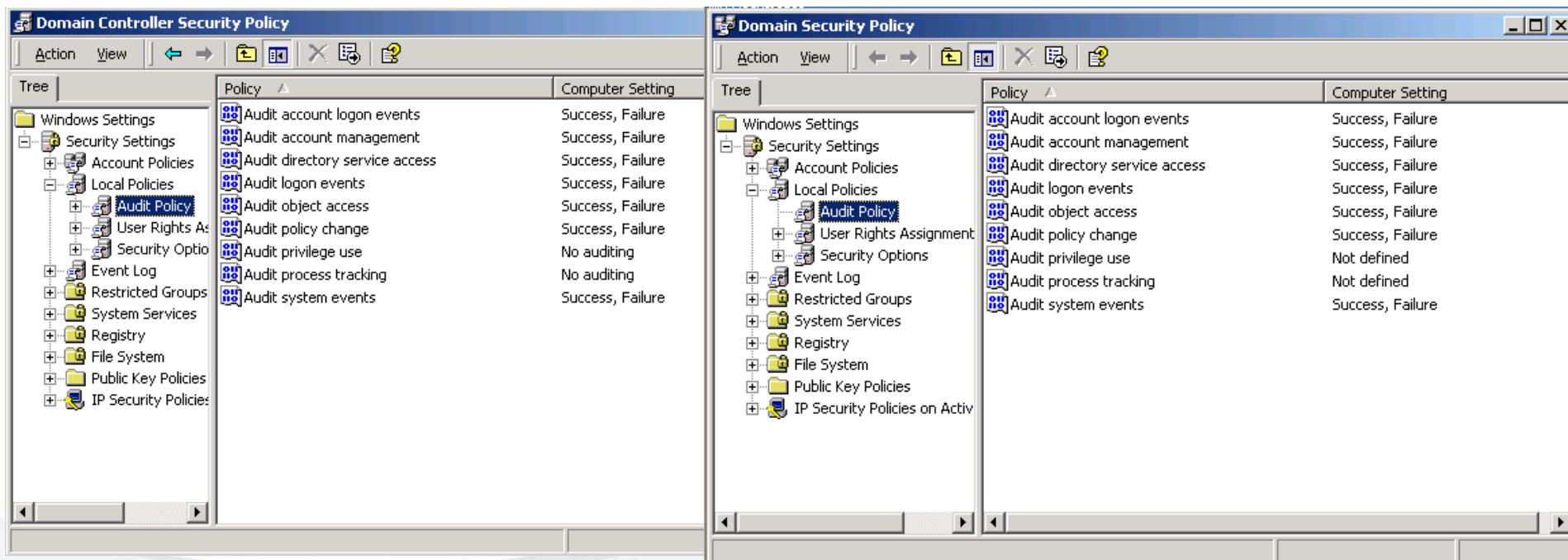


- Последовательность действий
 - Установить агента на Windows
 - Ввести активационный код
 - Лицензия не требуется
 - Reboot & cpstart
 - Создать на SmartCenter объект для этой Windows машины
 - Push policy & Install database
 - Настроить сервис Check Point на Windows машине
 - Запустить `windowEventToCPLog -s`
 - Domain\username & Password
 - Cpstop / cpstart
 - Запустить `windowEventToCPLog -a IPaddress`
 - IP Address машин, которые нужно мониторить
 - Запустить `windowEventToCPLog -l LogServerIPaddress`
 - LogServerIPaddress = Eventia IP
 - Cpstop / Cpstart

События Windows



- Убедитесь, что Windows протоколирует в Events Log события, которые нужно анализировать и коррелировать
 - Audit Policy in the Windows Domain Controller Security Policy and Domain Security Policy



События Windows



192.168.1.63 - Check Point Eventia Analyzer Client

File View Actions Query Help

Overview Events Policy Reports

Custom

- Predefined
 - All Events
 - By ID
 - By Severity
 - By State
- By Time
 - Last Hour's events
 - Today's events
 - Current week's events
- By Type
 - Scans
 - Third Party Device
 - Denial Of Service
 - Unauthorized Entry
 - Anomalies
 - Virus Alert
 - Host Based Events
 - Externally Identified
 - Informational
 - User Defined Events

Last Hour's events

ID	Start Time	End Time	Severity	Name	Source	Destination	Severity
EN0000...	17:09:36...	Not comp...	Warning	Audit Policy changed	WinBox (192.1...		
EN0000...	16:55:57...	16:55:57...	Warning	User account password reset	WinBox (192.1...		
EN0000...	16:53:55...	16:55:57...	Warning	Change in users or groups	WinBox (192.1...		

Previous Next Copy Raw data Change State

Audit Policy changed EN00000010

All Events EN0000... 15:08:13... Not comp... dns service stopped WinBox (192.1...

All Events EN0000... 14:25:34... Not comp... Credentials guessing WinBox (192.1...

FAQ



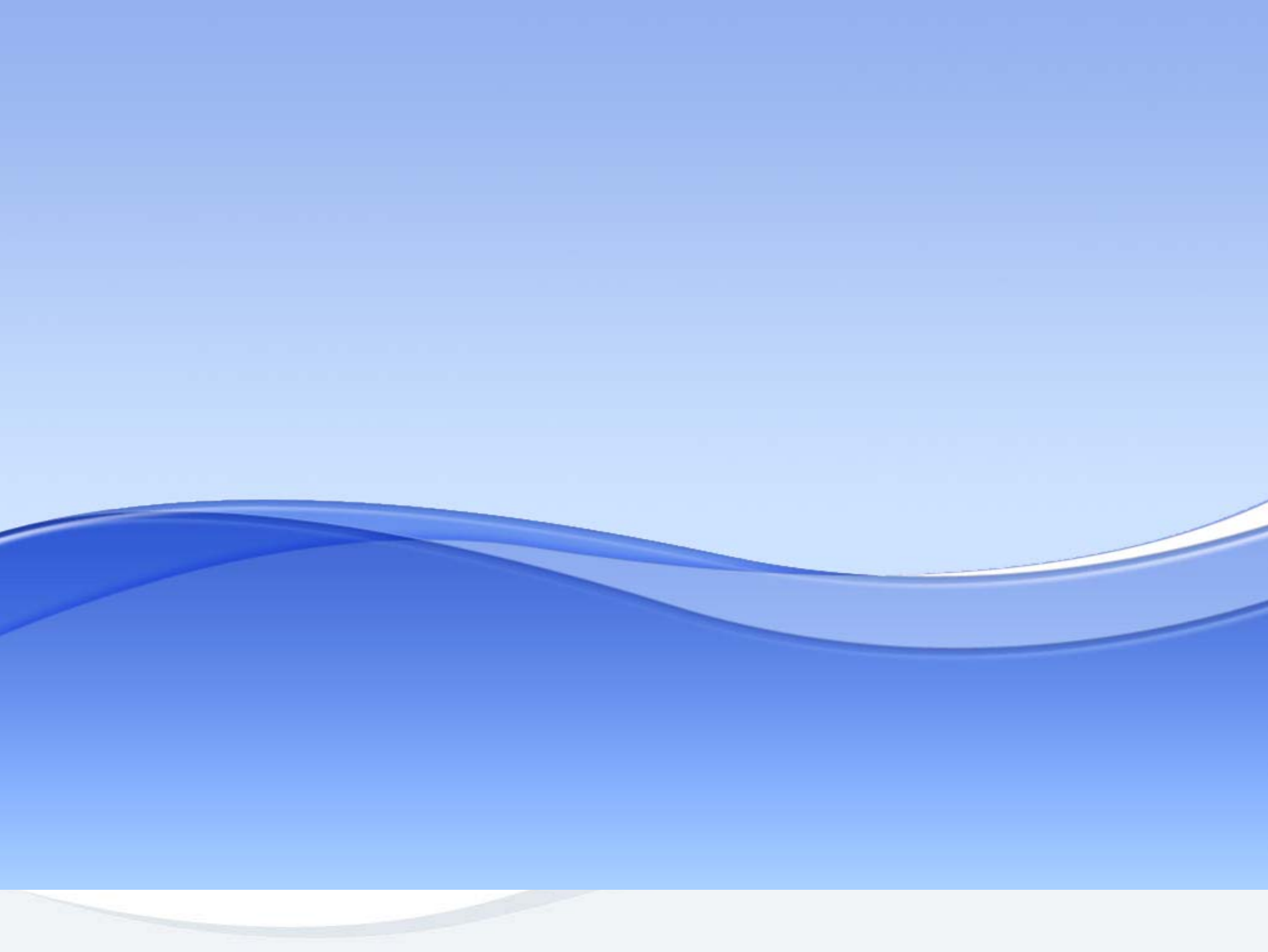
- В чем отличие от Reporter ?
 - Reporter читает только Check Point Logs (Analyzer может обрабатывать 3rd party logs)
 - Reporter дает отчеты о прошлых событиях
 - Включая и не связанные с безопасностью (top X users, top Y applications, etc.)
 - Analyzer фокусируется на событиях безопасности в реальном времени

FAQ



- Платформы для Analyzer
 - Windows 2003, 2000 Advanced Server and Server (SP1 to SP4)
 - Solaris 9
 - SPLAT
 - RHEL 3.0
- Версии SmartCenter / Provider-1
 - SmartCenter R54, R55, R60, R61
 - Provider-1 / SiteManager-1 R55, R60*, R61*

* : recommended



Конфигурации Eventia



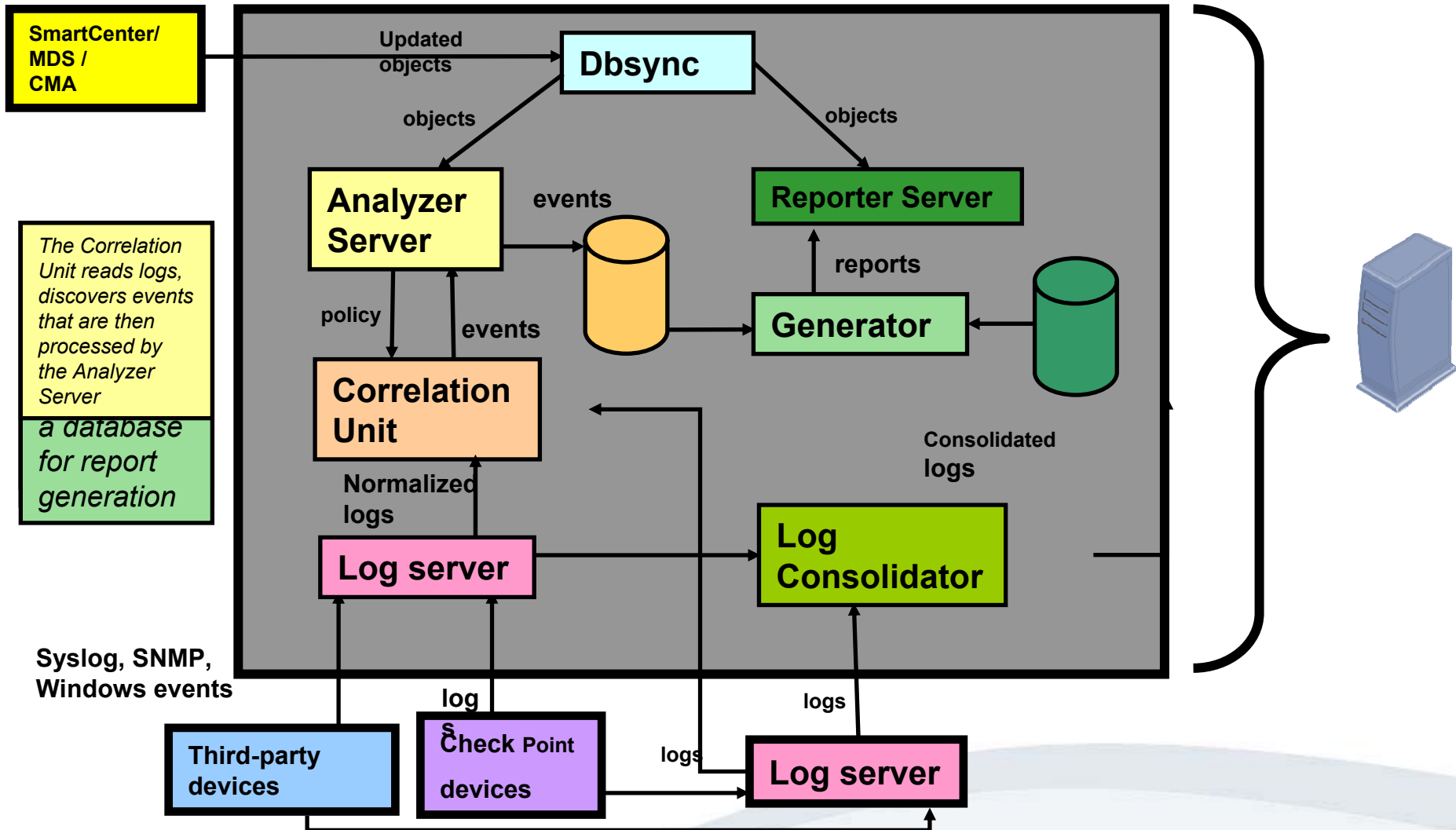
- Eventia Suite это комбинация Eventia Analyzer и Eventia Reporter.
- Eventia Suite включает log server. С R65 будет полная поддержка log server, включая database installation

Eventia Suite: Analyzer и Reporter вместе



- Analyzer и Reporter могут устанавливаться как на одну машину, так и порознь
- Сервер от Reporter всегда должен быть установлен, если ставится Analyzer. При наличии лицензии только от Analyzer Reporter будет создавать отчеты только для Analyzer. Консолидация не будет доступна.

Eventia Suite: Components and Data Flows



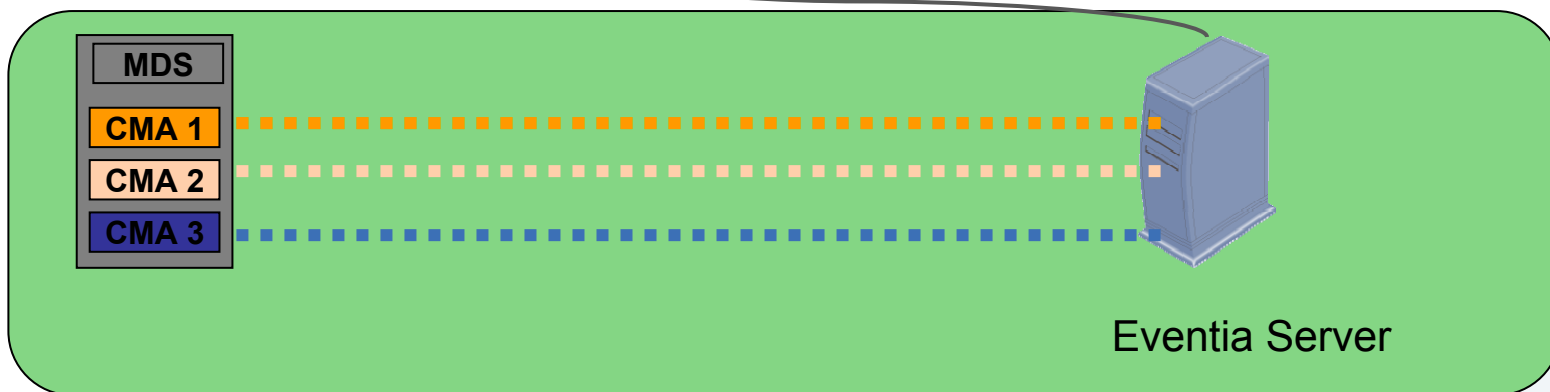
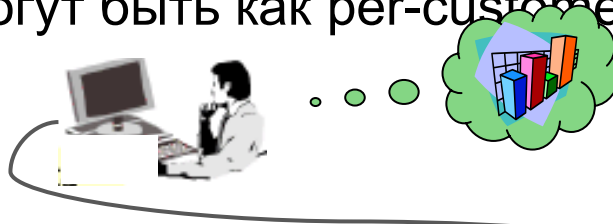
Eventia Suite в среде Provider-1



- Eventia поддерживает Provider-1, синхронизируя базу данных объектов с каждой СМА, которую администратор решил поддерживать.
- События Report'ера, как и Analyzer'а могут быть для каждого СМА, а могут и для всей платформы.
- Analyzer поддерживает профили администраторов, т.е. на уровне СМА можно задавать соответствующие разрешения администраторам: администратор может иметь доступ к одним СМА, но не иметь к другим

Eventia Reporter/Analyzer и Provider-1

- Eventia Reporter/Analyzer устанавливается на отдельный сервер
- Устанавливается Trust между MDS и Eventia Server, что позволяет Eventia подключаться к разным СМА на этом MDS и получать с них логи для генерации событий/отчетов
- Eventia использует dbsync – технологию для синхронизации баз данных объектов с MDS и выбранных администратором СМА. Это дает возможность Eventia получать объекты даже со старых версий Provider-1 (начиная с R55).
- Отчеты и события могут быть как per-customer так и cross-customer





Производительность Eventia



- Основные цифры
 - Один Reporter может консолидировать до 32 GB журналов в сутки
 - Один Analyzer Correlation Unit может анализировать 15 GB журналов в сутки. Многопроцессорность существенно помогает.
 - Сервер Syslog может получать 500 записей в секунду.

Производительность Eventia



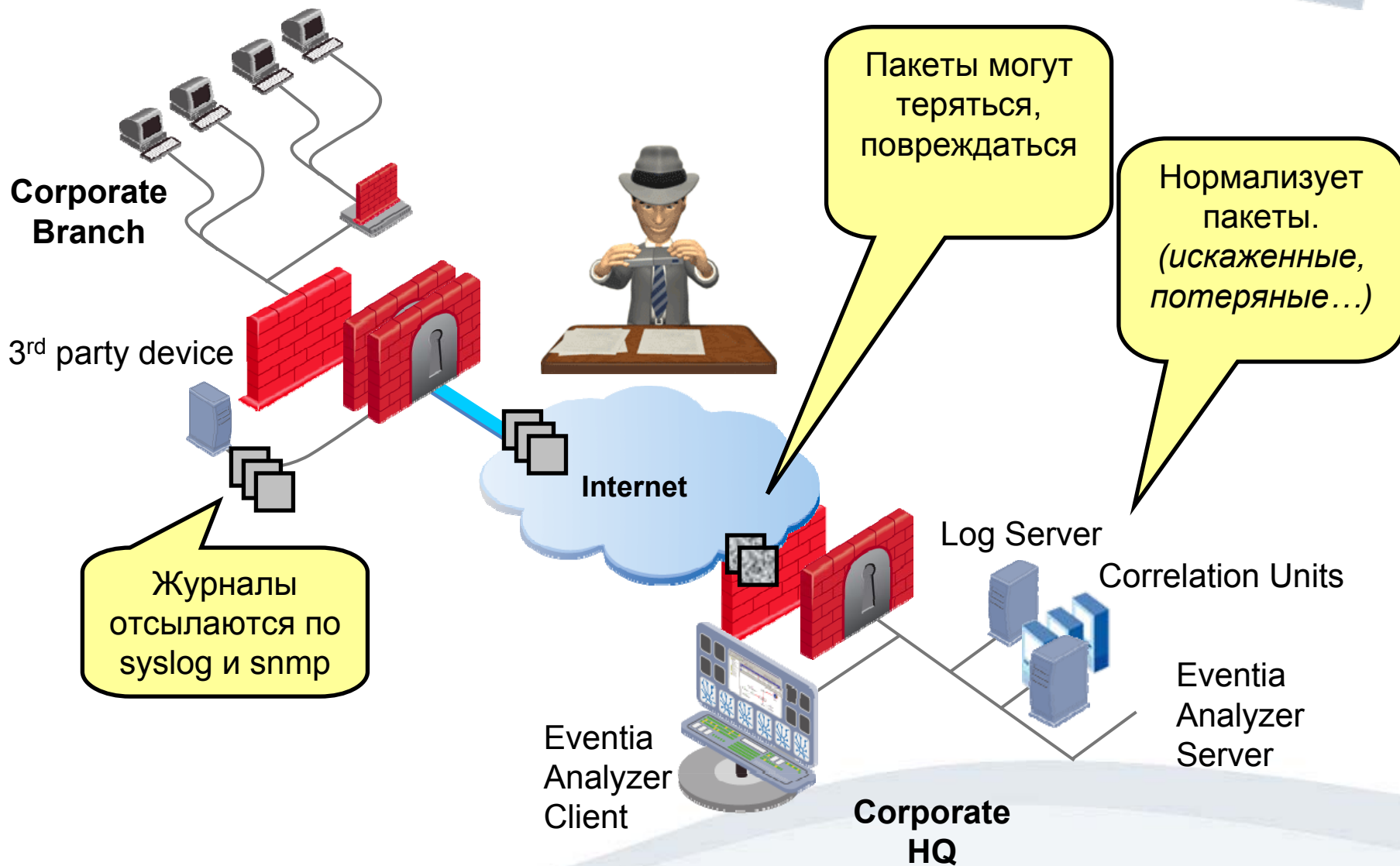
- Основные положения
 - Reporter имеет два основных (для производительности) процесса:
 - Для Log Consolidator важна скорость обработки журналов
 - Для Генератора отчетов важен диск
 - У Analyzer основное:
 - Для Correlation Unit важно быстродействие CPU и память. Несколько процессоров и 2 GB RAM приветствуются
 - Если производительности все же не хватает, можно разделить Analyzer и Reporter. Более того, log server также может устанавливаться отдельно.

Масштабируемость Eventia

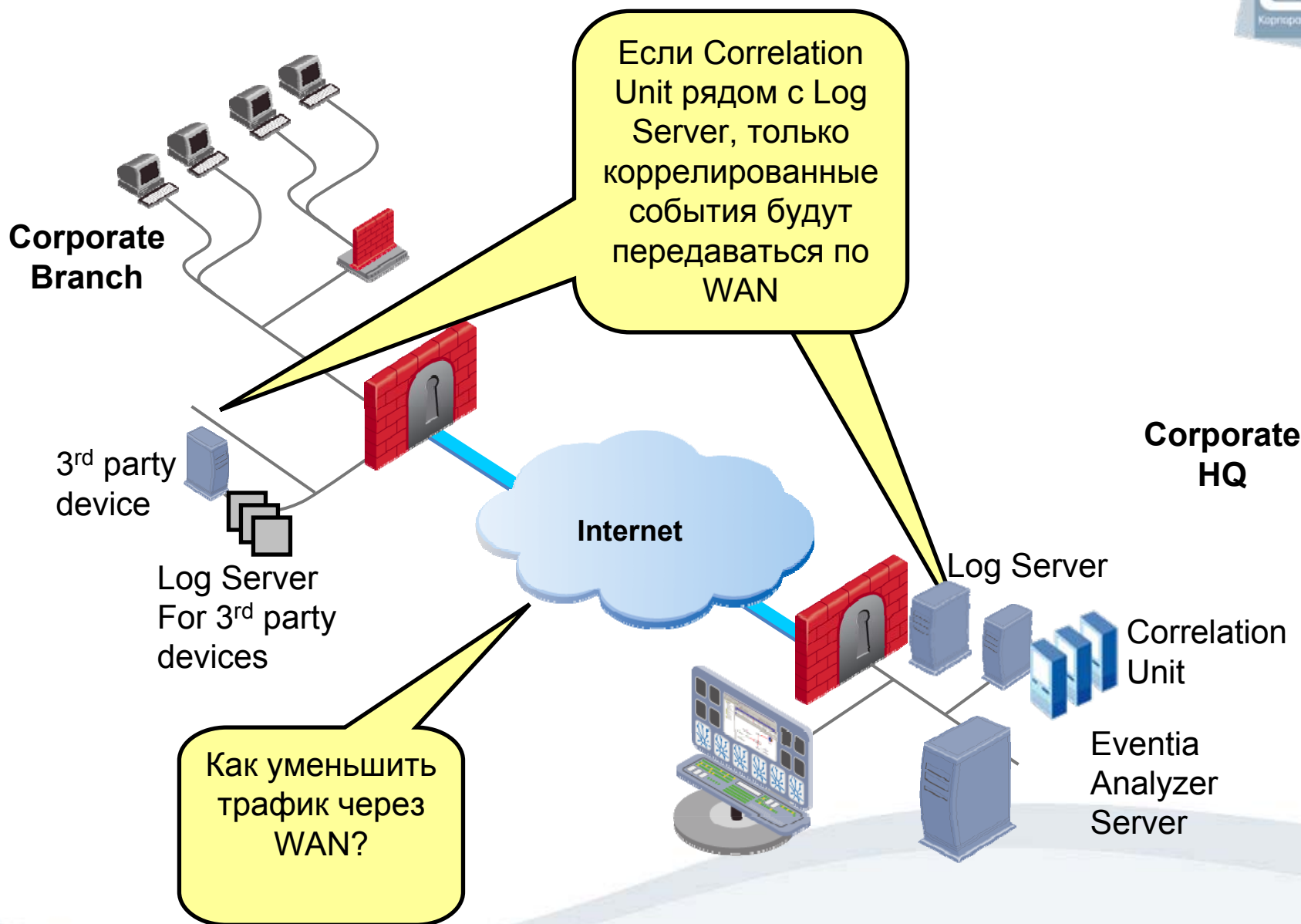


- Reporter
 - Несколько Reporter'ов могут подключаться к одному SmartCenter или MDS.
- Analyzer
 - Несколько Analyzer Correlation Units могут подключаться к одному Analyzer Server. Analyzer Server собирает информацию от всех Correlation Units в единую базу данных, т.е. все данные в результате собираются вместе. Однако Correlation Unit не взаимодействует с другим Correlation Units в процессе восстановления событий из данных, обрабатываемых другими Correlation Unit.

Особенности топологии



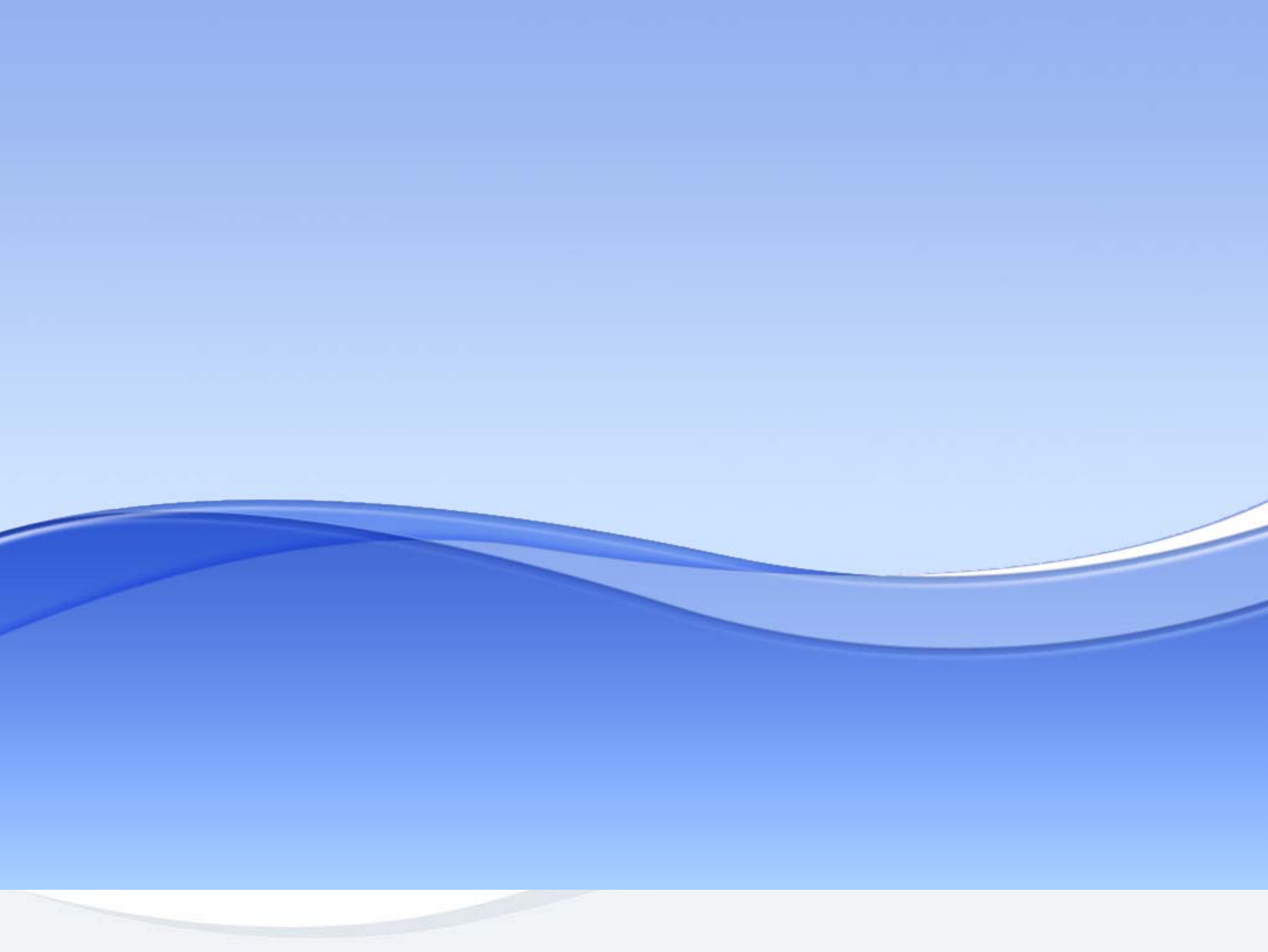
Особенности топологии (улучшения)



Ограничения распределенной топологии



- Дополнительные затраты
 - Correlation unit \$10,000
 - Log Server \$1,000
- Корреляция событий между несколькими Correlation unit не поддерживается.
2 Log Server должны обрабатываться одним Correlation Unit, если мы хотим, чтобы комбинации важных событий, пришедших на эти Log Servers, могли быть обнаружены.



Новые возможности Eventia R63/R65



- Общий функционал
 - Reporter и Analyzer могут устанавливаться на одной платформе
 - Reporter, подобно Analyzer, может поддерживать SmartCenter и Provider старых версий (от R55 до R65)
 - Reporter и Analyzer поддерживает функции динамического обновления описаний отчетов и событий соответственно

НОВЫЕ ВОЗМОЖНОСТИ Eventia R63/R65



- Особенности Analyzer
 - Analyzer поддерживает профили администраторов – администратор может видеть только «свои» СМА
 - Analyzer поддерживает SmartCenter и Provider-1 НА
 - Analyzer может читать старые журналы offline
 - Analyzer создает отчеты через Reporter. Отчеты могут создаваться по расписанию, распространяться различными способами, настраиваться мощным механизмом фильтрации Reporter'a
 - Поддержка большого количества продуктов других фирм: Symantec Anti-virus, Tipping Point SMS, NetContinuum Application Security Gateway, sendmail...

НОВЫЕ ВОЗМОЖНОСТИ Eventia R63/R65



- Особенности Reporter:
 - Несколько Reporter могут подключаться к одному SmartCenter или MDS для масштабируемости. Напротив, Reporter может подключаться к единственной CMA
 - Политика консолидации Reporter'а может редактироваться через утилиты Provider-1 в дополнение к существующим возможностям SmartCenter
 - Отчеты могут рассылаться как один MHTML файл
 - Reporter поддерживает offline dynamic update

Новые и планируемые возможности Eventia R63/R65



- Динамические обновления:
 - Дополнительные продукты и возможности Check Point
 - Устройства других фирм
 - Дополнительные события и отчеты
- Расширенный Correlation Engine
- Визуализация событий, навигация, переходы
- Улучшенные возможности автонастройки
 - Более детальные рекомендации
 - Обновляемый механизм самообучения для новых событий

Новые и планируемые возможности Eventia R63/R65



- Ввод данных из текстовых файлов событий
 - Получение при рассинхронизации
 - Повторное проигрывание журналов
 - Проверка после изменения политики
- Поддержка в GUI настройки пользовательских правил разбора событий
 - Дополнительные возможности для партнеров
 - Адаптация к существующему окружению
- Расширения в части управления
- Отчеты о соответствии требованиям стандартов
- Отчеты о событиях Audit logs

Спасибо!