Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Преврати
Информацию
в
Действие

ОПИСАНИЕ ПРОДУКТА

Программный блейд SmartEvent – первое и единственное решение, объединяющее анализ событий и управление, которое в режиме реального времени обеспечивает полезной информацией по управлению угрозами.

Программный блейд SmartEvent

Переводит информацию, относящуюся к безопасности, в действие

ВАША ПРОБЛЕМА

Обеспечить более полную и активную защиту при помощи готового решения в области безопасности, поскольку новые и более изощренные угрозы держат под прицелом предприятия в попытке украсть ценную информацию. Вредоносная активность может легко затеряться среди тысяч событий, создаваемых каждую секунду сетевым оборудованием и устройствами безопасности, а интервал между началом атаки и ее обнаружением и удалением становится все более критическим. Задача состоит в требовании наглядности, чтобы отсортировать лишнее, точно определить реальную угрозу и активно устранить атаку до того, как сеть или данные будут скомпрометированы.

НАШЕ РЕШЕНИЕ

Программный блейд SmartEvent превращает информацию, относящуюся к безопасности, в действие – с помощью корреляции событий безопасности и управления в реальном времени для шлюзов безопасности Check Point и устройств сторонних производителей. Единый анализ событий блейда SmartEvent выделяет критические события безопасности из общей массы во время корреляции событий со всех систем безопасности. Его автоматическая агрегация и корреляция данных не только сводит к минимуму время, затрачиваемое на анализ данных журнала, но и изолирует и приоретизирует реальные угрозы безопасности.

С программным блейдом SmartEvent, группе, отвечающей за безопасность больше не нужно прочесывать массу данных, генерируемых устройствами. Вместо этого, ресурсы теперь могут быть направлены на угрозы, которые представляют наибольший риск для бизнеса.

Превратить информацию в действие

Большая наглядность | Быстрое восстановление | Улучшенная интеграция | Элементарность

ФУНКЦИИ ПРОДУКТА

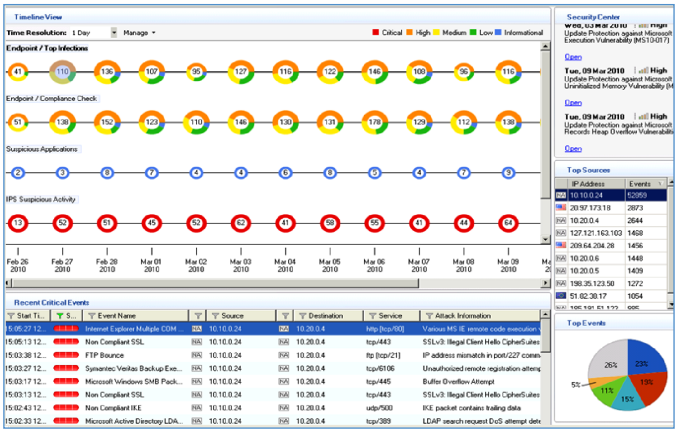
- Коррелировать события межсетевого экрана, IPS, DLP, конечных точек и систем сторонних производителей
- Отображать информацию о событиях и тенденциях в реальном времени и использованием графиков, диаграмм и карт
- Добавлять защиту на лету для устранения атак
- Блокировать вредоносный трафик из стран нарушителей с помощью Geo-Protection
- Отслеживать разрешение событий с помощью встроенной системы заявок

ПРЕИМУЩЕСТВА ПРОДУКТА

- Быстро выявить угрозы безопасности из потока регистрируемых событий с устройств
- Снизить бизнес-риски в режиме реального времени, интеллектуальное определение угроз
- Задать приоритеты ресурсам для эффективного решения наиболее серьезных угроз
- Выполение сводных отчетов по соответствию требованиям
- Усилить имеющиеся инвестиции в защиту за дополнительные деньги

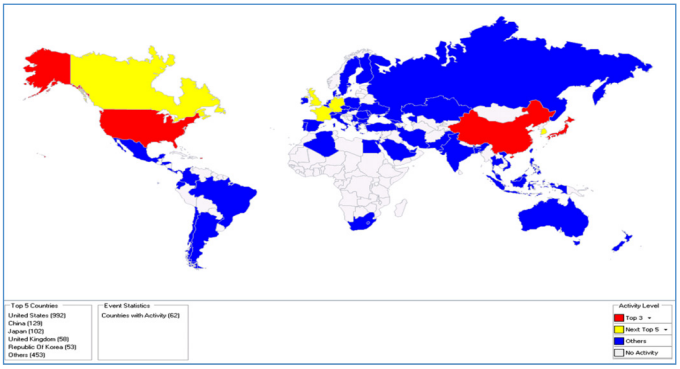
Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Мониторинг только важных событий



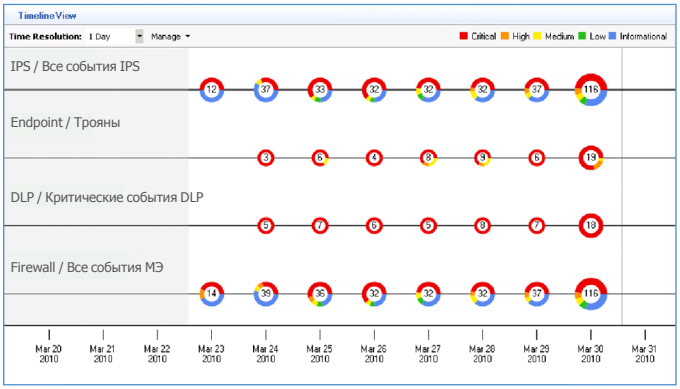
Легкое выявление критических событий безопасности из общей массы.

Просмотр угроз по стране происхождения



Блокировка вредоносного трафика из стран нарушителей с Geo-Protection.

Единый анализ событий



Корреляция событий со всех систем безопасности: межсетевой экран, IPS, Endpoint, DLP.

Лучшая наглядность

SmartEvent предоставляет несколько обзоров в реальном времени, чтобы помочь вам быстро осознать ситуацию с безопасностью и действовать в основе увиденного. Временная шкала позволяет увидеть тенденции и развитие атак. Изображение диаграмм предоставляет статистику событий в виде круговой диаграммы или в формате гистограммы. Изображение карты позволяет идентифицировать потенциальные угрозы с разбивкой по странам.

Быстрое восстановление

Для проведения быстрого анализа событий SmartEvent предоставляет различные инструменты. События могут быть динамически отфильтрованы, найдены, отсортированы и сгруппированы, чтобы быстро понять состояние безопасности вашей сети. На основании увиденного, вы можете остановить атаки прямо с экрана событий. Устранение атак производится добавлением дополнительной защиты на лету. С Geo-Protection блокируется вредоносный трафик из стран нарушителей.

Единая унифицированная консоль событий

Консоль SmartEvent обеспечивает централизованные корреляцию событий и управление для всех продуктов Check Point, включая IPS, DLP и Endpoint Security, а также систем безопасности сторонних производителей. Тот же интерфейс позволяет управлять аудитом и отчетностью для выполения сводных отчетов по соответствию требованиям.

Лучшая интеграция

Программный блейд SmartEvent, работающий совместно с имеющимися серверами регистрации событий Security Management и Provider-1®, избавляет пользователя от необходимости настройки каждого сервера регистрации событий в отдельности для сбора и анализа журналов. Все объекты, заданные в Security Management или Provider-1, будут автоматически доступны с сервера SmartEvent для задания политики событий и принудительного применения.

Простота развертывания

Для быстрого развертывания блейд SmartEvent предоставляет большое количество предопределенных, но легко настраиваемых событий безопасности. Используя мастер администраторы IT безопасности могут легко создавать свои собственные события под индивидуальные потребности.

Масштабируемая распределенная архитектура

Программный блейд SmartEvent предоставляет гибкую, масштабируемую платформу, способную управлять миллионами журналов в день на сервер корреляции. Благодаря распределенной архитектуре, блейд SmartEvent может быть установлен на одном сервере, но гибко распределять вычислительную нагрузку между несколькими серверами корреляции.

Устройства Smart-1 SmartEvent для полнофункционального управления

- Готовое решение для управления событиями всех продуктов Check Point
- Встроенная расширяемая Архитектура «Программные блейды» компании Check Point
- Лидирующее на рынке хранение журналов событий и управление по дополнительному каналу

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

УСТРОЙСТВА SMART-1 SMARTEVENT



	Smart-1 SmartEvent 5	Smart-1 SmartEvent 25	Smart-1 SmartEvent 50
Установленные программные блейды	SmartEvent, Reporting, Logging and Status		
Хранилище	1 x 0.5 TB	4 x 0.5 TB, RAID 10	4 x 1 TB, RAID 10
Fiber Channel SAN Card	-	-	Опционально
Управление по дополнительному каналу	-	Интегрировано	Интегрировано
Управляемых шлюзов (рекомендуется)	5	25	50
Максимальное количество управляемых шлюзов	25	50	150
Объем протоколирования (рекомендуется)	2Гб в день	10Гб в день	25Гб в день

ХАРАКТЕРИСТИКИ ПРОГРАММНОГО БЛЕЙДА SMARTEVENT

Свойства	Описание
Источники данных	
Продукты CheckPoint	Интегрировано, предопределенные правила и корреляция событий
Продукты безопасности сторонних производителей	Поддерживается множество форматов протоколирования от сторонних производителей
Графический анализатор журналов регистрации	Анализ вручную и подготовка любого журнала от сторонних производителей
Несколько методов сбора журналов	Сбор журналов с агентом и без
Наглядность	
Отображение временной шкалы	Графический просмотр в режиме реального времени информации о событиях, тенденциях и аномалиях
Отображение графиков	Отображение статистики событий в виде полосы и круговой диаграммы
Карты	Географическое местоположение источника события и IP адрес назначения
Быстрый просмотр событий	Быстрая группировка событий по типу, источнику, месту назначения, пользователю или стране
Анализ событий	
Предопределенные правила корреляции событий	Основана на передовой практике CheckPoint по общим проблемам в отрасли безопасности
Настраиваемые события безопасности	Пользовательские правила корреляции событий для мониторинга любых событий безопасности
Расследование	Двойной щелчок по временной шкале события, графики и карты для быстрой детализации на уровне пакетов
Группировка и поиск событий	Удобный для использования поиск и группировка данных для анализа событий
Особенность протоколирования	Преобразует IP-адреса в имена пользователей на основе Active Directory
Приложение ClientInfo	Щелчек правой кнопкой мыши на любом устройстве для доступа к критически важной информации, такой как процессы, заплатки и уязвимости
Интеллектуальный режим обучения	Базовые уровни работы для обнаружения тенденций
Оценка уязвимости	Встроенное оценивание событий безопасности
Информация к действиям	
Помеченные события	Назначение событий для администраторов с обработкой по системе заявок
Глобальные и характерные для события исключения	Настройка оповещений для исключения событий по продукту, источнику, месту назначения и сервису
Функции восстановления	Назначение автоматического или ручного восстановления, чтобы изменить политику безопасности на основе анализа событий
Другое	
Масштабируемая распределенная архитектура	Сервер протоколирования, сервер корреляции событий и сервер событий могут быть развернуты на отдельных системах

АДРЕСА И ТЕЛЕФОНЫ CHECK POINT

Международная штаб-квартира
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Телефон: 972-3-753-4555 | Факс: 972-3-575-9256 | Эл. почта: info@checkpoint.com
Представительство в России и СНГ
Check Point Software Technologies (Russia) ООО | 109240, Москва, ул. Николоямская, д. 13, стр. 17 | Тел./факс: +7 495 967 7444 | http://rus.checkpoint.com