ОСОБЕННОСТИ

Акцент на реальных задачах
MaxPatrol SIEM был разработан для решения насущных задач: универсальный сбор событий, простота представления данных, легкость работы с новыми источниками, богатые и постоянно развивающиеся функции корреляции, эффективная работа с большими объемами данных, автоматизация процессов администрирования.

Всесторонний анализ
Система оперирует не только событиями ИБ, но и состояниями активов в любой момент времени. Это позволяет связывать события со свойствами элементов инфраструктуры, выявляя действительно опасные инциденты.

Понимание инфраструктуры
Система MaxPatrol SIEM собирает не только события, но и всю информацию о сети, узлах, конфигурациях и т. п., позволяя воссоздать виртуальную копию инфраструктуры организации, увидеть полную картину происходящего и использовать эти данные для выявления инцидентов.

Надежность и масштабируемость
MaxPatrol SIEM имеет понятный интерфейс и обеспечивает стабильную работу в распределенной сети крупной компании. Наличие единой платформы MaxPatrol позволяет строить на основе продуктов Positive Technologies корпоративный центр мониторинга безопасности.

MAXPATROL SIEM: ПОЛНАЯ КАРТИНА БЕЗОПАСНОСТИ

Современные корпоративные системы сложнее и крупнее, чем когда-либо, и обеспечение их безопасности — непрекращающийся процесс. Любая компания стремится защитить свою интеллектуальную собственность, клиентскую информацию, финансовые документы и использует для этого целый комплекс программно-аппаратных средств. Однако в реальности степень защищенности компаний от киберпреступников остается низкой. Так, согласно данным Positive Research 2016, 76% корпоративных систем, находящихся в коммерческой эксплуатации, содержат уязвимости разной степени риска, позволяющие злоумышленникам получить полный контроль над системой или отдельными ее узлами.

Как правило, IT-инфраструктура компании гетерогенна, состоит из большого количества элементов разных производителей. При работе этих элементов — устройств и приложений — формируются журналы событий различных форматов, с разной интенсивностью поступления данных. Информация из журналов служит основой для выявления инцидентов ИБ, а также обнаружения и прогнозирования сбоев в работе оборудования.

Для обработки потока событий с целью выявления инцидентов и реагирования на них применяют специализированный класс решений SIEM (security information and event management). Однако на практике эффективность большинства систем SIEM остается низкой из-за следующих факторов:

+ комплексность систем SIEM и многообразие настроек значительно осложняют их использование массовыми пользователями и требуют привлечения высококвалифицированного и дорогостоящего персонала;
+ отчеты, формируемые SIEM-системами, плохо структурированы и трудны для восприятия, поэтому зачастую возникает необходимость корректировать их вручную перед представлением руководству или нетехническим специалистам;
+ «удаленность» производителя систем SIEM от заказчика и, как следствие, слабое покрытие источников данных, разрозненность и низкое качество обрабатываемой в SIEM-системах информации.

Компания Positive Technologies, опираясь на собственный экспертный опыт в области противодействия кибератакам, разработала систему сбора и анализа событий информационной безопасности MaxPatrol SIEM.

ПРЕИМУЩЕСТВА

Гибкость платформы
Модульная архитектура позволяет построить любую конфигурацию системы, которая отвечает требованиям заказчика и не содержит избыточной функциональности, что дает существенную экономию средств при внедрении.

Легкая миграция
Благодаря поддержке экспертов компании-разработчика, а также техническим инновациям, заложенным в продукте, внедрение и переход с других решений на MaxPatrol SIEM осуществляются безболезненно и незаметно для бизнес-процессов.

Российское решение высокого класса
Система MaxPatrol SIEM целиком спроектирована в России, с учетом специфики решаемых задач и требований регулирующих организаций. Специалисты Positive Technologies участвуют в работе технических комитетов Росстандарта и входят в рабочие группы ФСТЭК России, оказывая экспертную помощь в формировании требований безопасности.

15 лет опыта — на страже вашего бизнеса
В основе продукта лежит уникальная база знаний, включающая в себя многолетний опыт проведения масштабных тестов на проникновение, расследования сложных инцидентов и экспертного сопровождения таких мероприятий, как Универсиада в Казани и Олимпийские игры в Сочи.

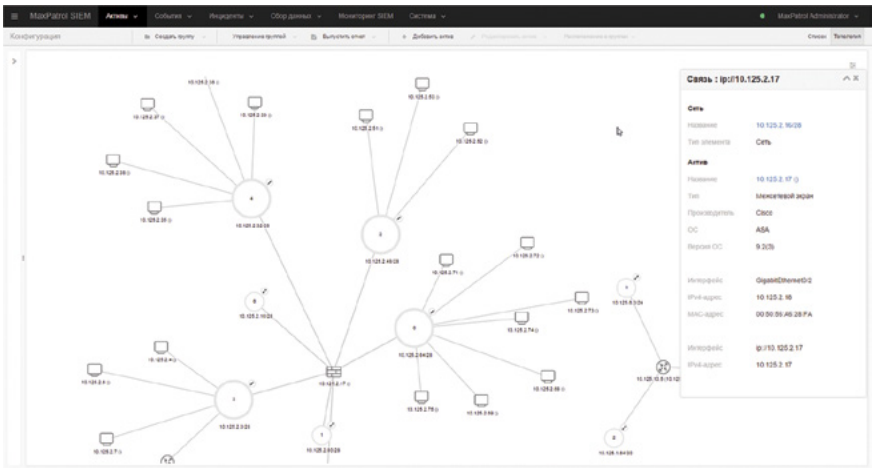
ПРИНЦИП РАБОТЫ MAXPATROL SIEM

MaxPatol SIEM работает на базе высокопроизводительной и гибкой платформы MaxPatrol. Ключевые особенности MaxPatrol SIEM:

- удаленный сбор данных, не требующий установки агентов на целевые системы;
- сбор данных не только о событиях, но и о конфигурациях, результатах сканирования, состоянии узлов, сетевой активности;
- постоянное обогащение активов данными из событий и в то же время обогащение событий данными об активах.

Платформа MaxPatrol позволяет реализовать как классические функции SIEM-решений, так и ряд уникальных технологий:

- **Активоцентрическая модель.** Любой элемент инфраструктуры — сетевой узел, сегмент сети, виртуальная машина — являются активами MaxPatrol SIEM. Информация о них собирается активными и пассивными методами, а также путем анализа сетевого трафика. Это позволяет оперировать реальными сущностями инфраструктуры, а не абстрактными событиями безопасности.
- **Модельные корреляции.** MaxPatrol SIEM использует любую информацию об активах в правилах корреляции, начиная с перечня установленного ПО, прав доступа и открытых портов, заканчивая списком уязвимостей. Это помогает максимально точно выявлять инциденты безопасности и минимизировать ложные срабатывания.
- **Гибкий язык описания корреляционных правил.** MaxPatrol SIEM позволяет описывать логику работы правил корреляции на специализированном декларативном языке. Язык постоянно развивается и позволяет решить задачу любой сложности.
- **Гибкий конструктор отчетов.** Помогает получить наглядные и информативные отчеты.
- **Интеграция с порталом аналитической отчетности.** Позволяет наглядно визуализировать любой набор метрик для оценки реального состояния безопасности организации в удобном представлении, которое отвечает требованиям руководства.



О компании Positive Technologies

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Деятельность компании лицензирована Минобороны РФ, ФСБ и ФСТЭК, продукция сертифицирована «Газпромом» и ФСТЭК. Более 3000 организаций из 30 стран мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телекомов. В 2013 году компания заняла третье место на российском рынке ПО для безопасности и стала лидером по темпам роста на международном рынке систем управления уязвимостями. В 2015 году Gartner назвал Positive Technologies «визионером» в своем рейтинге Magic Quadrant for Web Application Firewalls.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.ru