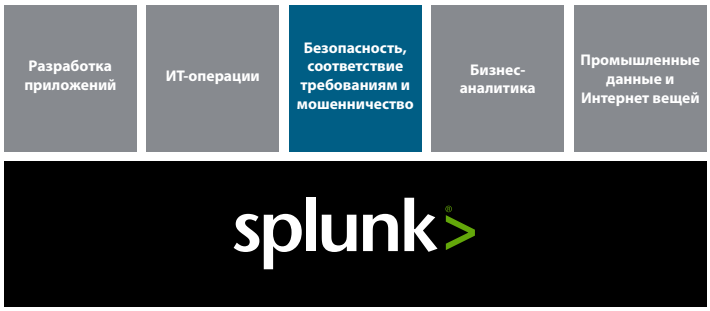
SPLUNK® ДЛЯ БЕЗОПАСНОСТИ

Обеспечение безопасности на основе аналитики

- **Комплексная аналитика безопасности** для данных из секретных и несекретных источников
- **Улучшение сложных расследований в сфере безопасности** с использованием методологии описания этапов атак (kill chain)
- **Быстрый анализ инцидентов** с коротким временем ответа (time-to-answer) и упреждающим обнаружением угроз
- **Использование современной аналитики на основе данных** для быстрого обнаружения отклонений и угроз и смягчения последствий внутренних и внешних атак
- **Адаптивная реакция** для лучшего отражения современных атак с унифицированной защитой во всей экосистеме безопасности



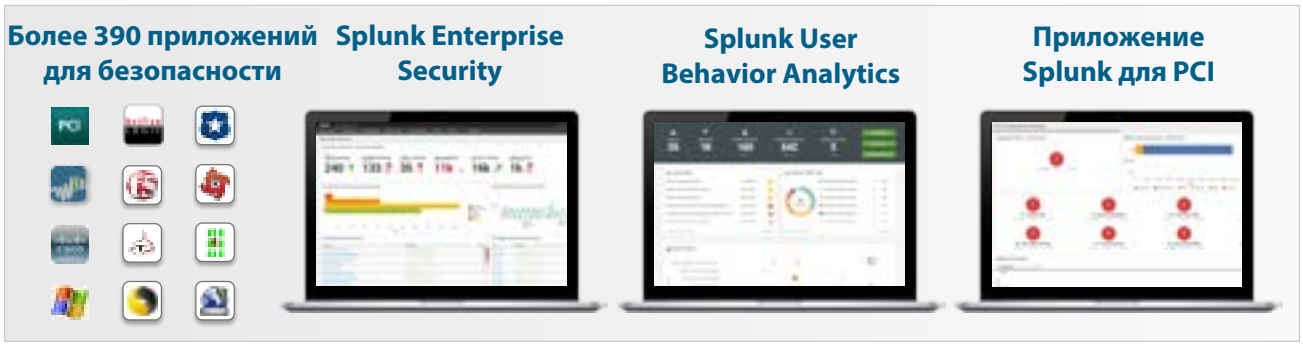
Сложность современных кибератак, устойчивость серьезных угроз и важность преодоления рисков для бизнеса на постоянной основе заставляют организации пересматривать всю экосистему безопасности. Чрезвычайно важно, чтобы аналитика безопасности включала подробный анализ информации о пользователях, атаках, контексте, времени и местоположении от систем идентификации, конечных точек, серверов, приложений, веб-серверов, почтовых сервером и нетрадиционных систем.

Принятие на вооружение облака, мобильных рабочих нагрузок и гибридных систем увеличило потребность в облачных службах и приложениях. Требуется динамическое представление инфраструктуры и целых приложений для выявления, расследования внутренних и внешних угроз и реакции на них в реальном времени.

Решения Splunk для обеспечения безопасности на основе аналитики обеспечивают комплексный подход к кибербезопасности, включая такие современные методы, как машинное обучение и аналитика поведения. Эти методы помогают группам безопасности быстро выявлять, изучать угрозы и реагировать на них в более широком контексте безопасности, чем с традиционными средствами обеспечения безопасности. Решения Splunk могут быть развернуты локально, в облаке или гибридном облаке.

Splunk как центр обеспечения безопасности

Программа Adaptive Response Initiative компании Splunk использует машинные данные из всей экосистемы безопасности для объединения аналитических данных по ней и всем технологическим решениям. Безопасность организации повышается благодаря быстрой проверке угроз и методичному прерыванию кибератак на разных этапах цепи. Эта модель совмещает предупреждения и информацию об угрозах по разным аспектам безопасности и технологий. Совокупный анализ помогает принимать более взвешенные решения на всех этапах цепи атак — особенно при проверке угроз и применении директив по реагированию, основанных на аналитических данных, в среде безопасности.



Обнаружение внутренних угроз

Можно автоматически выявлять внутренние угрозы с помощью машинного обучения, базовых характеристик поведения, средств анализа одноранговых групп и анализа поведения.

Обнаружение сложных угроз

Использование методологии цепи атаки (kill chain) для отслеживания различных этапов сложной угрозы, объединения событий в последовательность и целевые усилия по решению проблемы.

Обнаружение и расследование мошенничества

Обнаружение и расследование различных видов мошенничества, краж и нарушений системы безопасности и отчетность по ним в реальном времени. Splunk дополняет существующие средства борьбы с мошенничеством, индексируя данные о событиях для получения общего представления по случаям мошенничества во всей организации или создания агрегированных показателей безопасности для отдельной транзакции.

Система управления информационной безопасностью и событиями (SIEM)

SIEM используется в организациях для таких целей, как анализ и обработка инцидентов, аналитика и создание профилей поведения, анализ угроз и специальный поиск. Крупные организации используют весь набор операций с данными по безопасности, включая оценку состояния безопасности, мониторинг, предупреждения и обработку инцидентов, CSIRT, анализ нарушений и реакция на них и корреляцию событий. Splunk может использоваться в качестве системы SIEM для операционных центров защиты (SOC) любого размера.

Быстрое расследование инцидентов

Совместная работа дает возможность аналитикам операционных центров защиты и специалистам по выявлению нарушений в организации быстро расследовать инциденты с помощью специального поиска с уже существующими корреляциями на основе актуальных данных. Для определения первопричины и последующих шагов можно использовать данные за прошлые периоды.

Отчетность о соответствии требованиям

Создание правил корреляции и отчетов в целях выявления угроз для секретных данных или в отношении важных сотрудников, автоматическая демонстрация соответствия требованиям и выявление областей несоответствия по таким требованиям и стандартам, как PCI, HIPAA, FISMA, GLBA, NERC, SOX, EU Data Directive, ISO, COBIT и CIS Top 20.

Управление журналами

Возможность консолидации, сбора, хранения, индексации, поиска, корреляции, визуализации и анализа машинных данных, связанных с безопасностью, а также составления отчетов по ним для быстрого выявления и устранения проблем безопасности. Специальные запросы и отчетность на основе данных за прошлые периоды не требуют использования каких-либо сторонних программных средств отчетности. ПО Splunk дает возможность расширить данные журналов и обеспечить гибкий доступ к реляционным базам данных, данным в конкретных полях CSV-файлов и другим хранилищам корпоративных данных, таким как Hadoop или NoSQL.

Попробуйте решение Splunk Enterprise Security сейчас Испытайте возможности Splunk Enterprise Security — без дополнительного ПО, настройки оборудования или конфигурации. Splunk Enterprise Security Online Sandbox — это пробная среда с уже загруженными данными, предоставляемая на срок 7 дней в облаке. Вы получаете возможность поиска, визуализации, анализа данных и тщательного расследования инцидентов в многочисленных сценариях использования в системе безопасности. Также можно воспользоваться пошаговым руководством по мощным средствам визуализации и анализа, доступным с помощью ПО Splunk. **Подробнее.**

splunk> sales@splunk.com www.splunk.com