Киберпреступники постоянно находят новые способы, как обойти защиту разных компаний и предприятий. Однако, в России уже сейчас есть много решений, которые помогут обеспечить безопасность любого бизнеса. Но есть ли какие-то системы, которые точно смогут побороть уловки киберпреступников?

Что такое SIEM-системы?

Каждый день в новостях мы слышим о новых киберпреступлениях: то пенсионер перевёл крупную сумму мошенникам, то персональные данные тысяч пользователей оказались в открытом доступе. В наше время грабители предпочитают действовать не в подворотне, а в интернете.

Существует множество способов защитить себя от кибератак: от соблюдения простых правил цифровой гигиены до использования антивирусных программ. Однако, иногда даже этих мер бывает недостаточно, и требуется комплексный подход. И тут на помощь приходят SIEM-системы.

pinterest.com

Все права защищены

SIEM-системы — это мощный инструмент, который объединяет функции мониторинга событий безопасности и управление информацией о них. С помощью таких систем можно собирать и анализировать важные данные, отслеживать события и хранить информацию. В будущем это может пригодиться при проведении расследований или аудита.

Если система обнаружит подозрительную или аномальную активность, она незамедлительно сообщит об этом специалисту или же примет меры самостоятельно.

Результат опроса «Какую SIEM-систему вы используете?»
anti-malware.ru

До февраля 2022 года не все компании использовали SIEM-системы, но сейчас, когда Россия оказалась в числе стран, которые подвергаются наиболее интенсивным атакам хакеров, внедрение таких систем может стать критически важным шагом к обеспечению безопасности.

Все права защищены

save pdf date >>> 14.12.2025

forbes.com

Отечественный рынок кибербезопасности предлагает много продуктов, которые были адаптированы к условиям российской реальности. О некоторых мы сейчас расскажем.

KUMA

«Лаборатория Касперского» — это первый российский бренд, который приходит на ум, когда речь заходит о кибербезопасности. Помимо классического антивируса и других продуктов, компания предлагает свою собственную SIEM-систему — KUMA (Kaspersky Unified Monitoring and Analysis Platform).

KUMA объединяет продукты компании и сторонних поставщиков в единую систему информационной безопасности (ИБ). Гибкий API позволяет взаимодействовать с продуктами других поставщиков.

Все права защищены

Kaspersky Unified Monitoring and Analysis Platform

dialognauka.ru

> API (Application Programming Interface) — это программный интерфейс приложения, набор правил и протоколов, который позволяет различным программным приложениям взаимодействовать друг с другом.

KUMA построена по принципу микросервисов, что позволяет легко менять её настройки. Благодаря этому она может переключаться на разный объём работ без сбоев, а область её применения почти безгранична.

RuSIEM

Разработка от российской компании, участницы проекта «Сколково». Обрабатывает до 90 000 событий в секунду на одном компьютере. Может сохранять данные в сыром виде, что полезно при расследовании киберпреступлений. Есть бесплатная версия программы, которая, конечно, имеет более ограниченный функционал, чем платная.

Все права защищены

dzen.ru

Ankey SIEM

Российский продукт от компании «Газинформсервис». Эта система, как и предыдущие, следит за безопасностью и информацией. Она оперативно выявляет проблемы, анализирует их и управляет событиями, которые связаны с безопасностью IT-инфраструктуры.

Нацелена, в первую очередь, на крупные организации, такие как госорганы, предприятия добывающей промышленности и предприятия с разветвлённой инфраструктурой.

Все права защищены

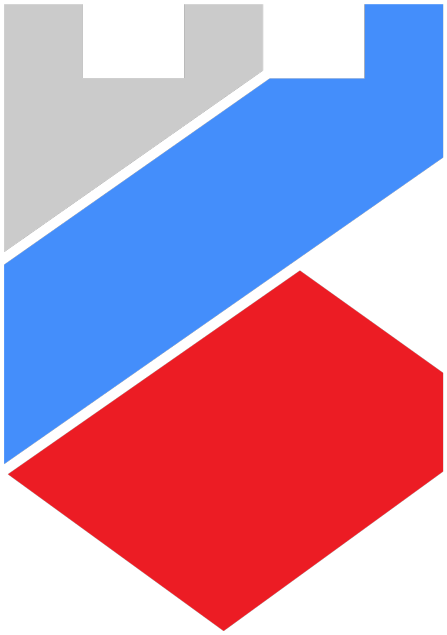
behance.net

Пангео Радар

Отечественное решение, разработчик которого также является участником проекта «Сколково». В систему уже встроена база знаний, которая поможет в обнаружении сложных хакерских атак. В целом, эта платформа способна удовлетворить основные потребности в работе с инцидентами, а также поможет в выявлении и устранении последствий киберугроз.

Все права защищены

save pdf date >>> 14.12.2025



ПАНГЕО РАДАР

cnews.ru

MaxPatrol

Флагман российских SIEM-систем. Кроме того, что система мониторит и выявляет угрозы, она также может адаптироваться к изменениям в архитектуре кода без внесение правок самим человеком.

Конечно, продукт можно совмещать с другими решениями компании, что позволит создать многоуровневые системы защиты. У MaxPatrol SIEM очень много клиентов (более 600) и применяют её в абсолютно разных отраслях: от госсектора до промышленности.

Все права защищены

whalenet.ru

Киберпреступники больше не страшны?

Как мы видим, российская кибербезопасность продолжает развиваться, и на рынке появляются новые предложения. Российские SIEM-системы — достойные конкуренты

Все права защищены

иностранным продуктам сразу по нескольким причинам.

Во-первых, отечественные SIEM-системы уже адаптированы под российского пользователя и под многие российские ОС, а это огромный плюс.

culture.ru

Во-вторых, иностранный софт в современных условиях и при текущей геополитической обстановке нельзя считать надёжным. В любой момент может появиться запрет на поставку в Россию SIEM-систем, и тогда вся инфраструктура окажется беззащитна перед лицом злоумышленников.

Таким образом, уповать остаётся только на отечественных кибербезопасников и их системы. К тому же, вариантов на российском рынке хватает, и каждая компания сможет выбрать именно то, что подходит ей больше всего. Это ли не здорово?

Все права защищены

save pdf date >>> 14.12.2025