

Smart Monitor

Универсальная платформа для сбора и анализа машинных данных, которая позволяет решать практические задачи в области информационной безопасности, мониторинга ИТ-инфраструктуры и анализа бизнес-процессов

Компании, которые используют Smart Monitor, уже

> 1.2
млрд р.

экономят в год благодаря предотвращенному корпоративному ущербу

5.3
%

оптимизируют годовых затрат на фонд оплаты труда за счет автоматизации

2.5
млн.

генерируют событий в ИТ-инфраструктуре компании каждую секунду

950+
Тб/д

регистрируют ежесуточный поток данных в рамках нагрузочного тестирования

> 1
млн.

выявляют и предотвращают случаи корпоративного мошенничества в течение года

35K+
сотрудников

профилируют действия сотрудников и выстраивают поведенческую аналитику

Сценарии применения Smart Monitor

> Больше сценариев

Переезд SIEM с MS Sentinel на Smart Monitor за два месяца

Цели: миграция SIEM с западного решения на Smart Monitor.

Задачи: миграция с Sentinel, переезд в On-premise, реализация правил с собственной логикой, перенос SOC процессов на Smart Monitor.

Результаты: быстрое развертывание и миграция за 2 месяца своими силами, использование CI/CD для управления конфигурациями, использование workflow Incident Manager для построения процесса SOC.

- > 2000K EPS поток обрабатываемых событий в инфраструктуре
- 10K+ серверов в системе мониторинга
- интеграция с внешними системами по API для управления инцидентами

Мониторинг операционной эффективности для финансовой компании

Цели: оценка операционной эффективности сотрудников через подход, основанный на данных.

Задачи: сложности в выявлении действий сотрудников, критических для бизнеса, и эффективное построение индивидуальных и групповых профилей.

Результаты: достижение эффективного баланса рабочей нагрузки для более чем 3000 сотрудников, снижение затрат на сверхурочные работы и трудозатраты.

- на 7-10% увеличилась эффективность использования труда сотрудников
- с дней до минут сократился процесс составления кратких отчетов сотрудниками
- 8 филиалов в разных часовых поясах



SM Store | modules marketplace

> Больше модулей

Core

Основообразующий модуль Smart Monitor. Координирует взаимодействие других модулей платформы и предоставляет единую точку доступа к их функциям.

Incident Manager

Функциональное решение по управлению жизненным циклом инцидентов в области ИБ, ИТ инфраструктуры, аномального поведения пользователей и ошибок бизнес-процессов.

Compliance

Помогает выстроить автоматизированную оценку соответствия на выполнение нормативных или корпоративных требований к информационной безопасности или уровню ИТ-сервисов.

Inventory

Позволяет сформировать единую базу активов (серверы, рабочие станции, сетевые устройства, информационные системы, объекты кластерной инфраструктуры) и пользователей, а также обеспечить поддержку данной базы в актуальном состоянии.

Cyber Security

Позволяет из единой консоли получать сведения о работе всех средств защиты информации (СЗИ). Реализованы корреляционные механизмы между событиями различных СЗИ, что позволяет выявлять события ИБ, не определяемые ни одним СЗИ по отдельности.

MITRE ATT&CK

Позволяет применить в защищаемой инфраструктуре различные сценарии использования MITRE ATT&CK (оценить покрытие техник инструментальными контролями, сформировать специализированные модели угроз и применить их к компонентам ИТ-ландшафта и т.п.)

Сайт Smart Monitor

Заказать демонстрацию

Рассчитать стоимость

Документация