

Table of Contents

Table of Contents	1
Введение	2
Введение	3

Введение

Documentation: 

Product: LogAn

Version: 7.0.1

UserGate Log Analyzer (LogAn) — это решение, реализующее функции систем SIEM (Security Information and Event Management) и IRP (Incident Response Platform).

SIEM — система управления информацией о безопасности и событиями информационной безопасности. LogAn собирает в себе данные, получаемые из различных источников (сенсоров), например, таких как, межсетевые экраны UserGate, системы управления и контроля конечных устройств UserGate, сенсоры SNMP, сенсоры WMI. Результат обработки данных предоставляется в едином интерфейсе, доступном для аналитиков безопасности, что облегчает изучение характерных особенностей, соответствующих инцидентам безопасности. На основе получаемых данных (событий) LogAn в реальном времени с помощью правил аналитики осуществляет агрегацию повторяющихся событий и их корреляцию (связывание разрозненных событий между собой), создавая инциденты кибербезопасности. Правила реагирования позволяют автоматически определить методы реагирования на инциденты информационной безопасности.

Для проведения расследований инцидентов кибербезопасности используется встроенная в LogAn система IRP. IRP — это платформа управления процессами реагирования на инциденты информационной безопасности. LogAn позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании.

LogAn поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде.

