positive technologies

MaxPatrol SIEM

Knows your infrastructure in detail and accurately detects incidents

DO IT ALL WITH MAXPATROL SIEM

- **Monitors information security** in large hierarchical infrastructures
- **See** IT infrastructure
- **Verify** system configuration using a checklist
- **Create your** own correlation rules with a flexible constructor
- **Automatically add** legitimate triggers to the whitelist
- **Check hypotheses** by viewing linked correlated events
- **Find data** in third-party systems and services directly in the event card

MaxPatrol SIEM detects information security incidents leading to non-tolerable events and any attempts to compromise the company's cyberresilience.

Fast results

No additional investments or changes needed. Deploys fast so you can launch infrastructure monitoring with out-of-the-box expertise

Updated expertise

MaxPatrol SIEM is updated automatically every month with a new expertise pack, and we consistently update and improve previous rules.

Adaptable to changes

Fast adaptation to infrastructure changes and clear identification of IT assets. Classifying assets into groups makes it easier to configure correlation rules.

Decision making help

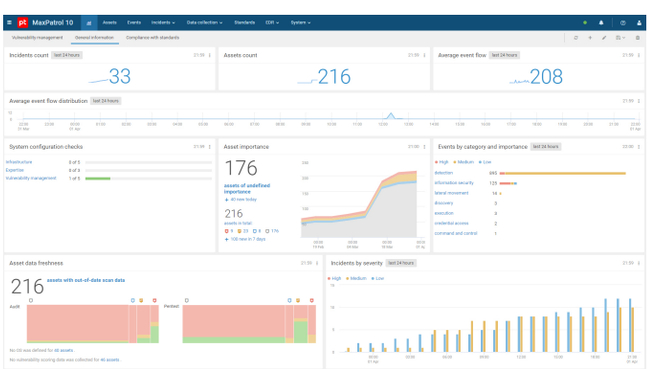
MaxPatrol SIEM features the Behavioral Anomaly Detection (BAD) ML assistant as a second opinion system to increase attack detection effectiveness with an alternative event assessment method.

Simple and easy

We focus efforts to improve analyst experience (AX). Convenient event cards help detect linked events, check potentially dangerous files, and respond to incidents all in the same window.

Enterprise monitoring

MaxPatrol SIEM can handle more than 540K EPS on a single core with full expertise. Thanks to our proprietary LogSpace database management system, only half the resources are consumed compared to similar open source solutions.



Custom dashboards help monitor the organization's overall state of information security

REQUEST A PILOT PROJECT

Find out how your infrastructure can benefit from MaxPatrol SIEM

Domestic SIEM solution leader	The product is used by more than 600 industrial, transport, and financial companies, as well as in the private and public sectors and by state authorities.
Regular expertise pack updates to detect threats	Expertise in MaxPatrol SIEM comes from our investigations of complex incidents, research into emerging threats and hacking methods used against companies and monitoring activities of all major hacker groups worldwide.
Community and independent developments	The extension directory contains extensions, rules, and connectors for MaxPatrol SIEM developed by the expert community to simplify the solution of a variety of problems.
Fast growth	With two releases a year, we regularly introduce new technologies and are constantly expanding our product development team.

global.ptsecurity.com
info@ptsecurity.com

MP-SIEM_A4.ENG.0001.09.APR.2024