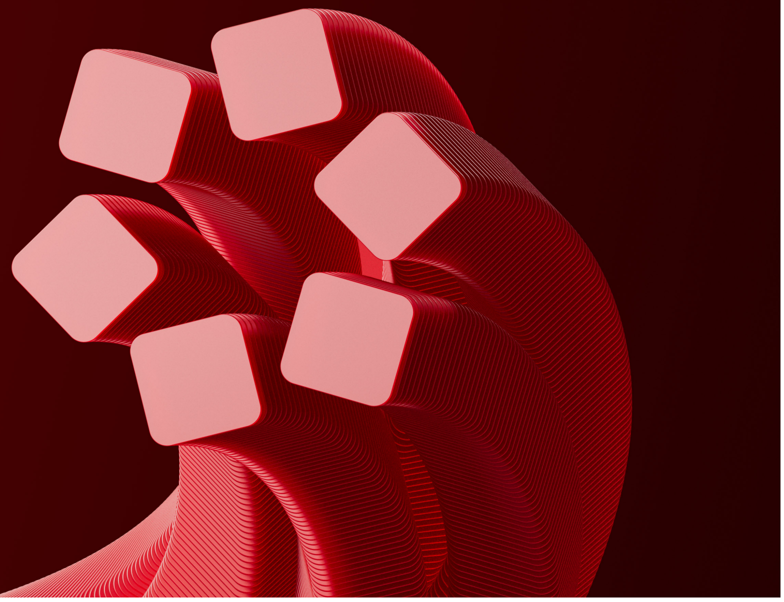
positive
technologies



MaxPatrol O2

Autopilot for result-driven cybersecurity

90%

of companies have a shortage of infosec professionals

71%

of non-tolerable events can be realized by attackers within one month

100%

of infrastructures can be fully taken over by internal attackers

93%

of network perimeters can be crossed by attackers to obtain local network access

MaxPatrol O2 detects attackers, determines the breached assets, predicts the attack scenario considering company-specific non-tolerable events, and stops the attack before irreparable damage is done.

Models potential attacker actions

Predicts the non-tolerable events that suspicious activity may lead to and how many steps are left until risks are realized.

Detects hacker activity chains

Analyzes data from Positive Technologies sensors in the metaproduct and demarcates attacking, targeted, and captured resources. Correlates resources to build activity chains informed by knowledge of malicious actor TPPs. Each chain contains a visualization of the attackers' path, plus a prediction of where they will move next.

Automates investigations

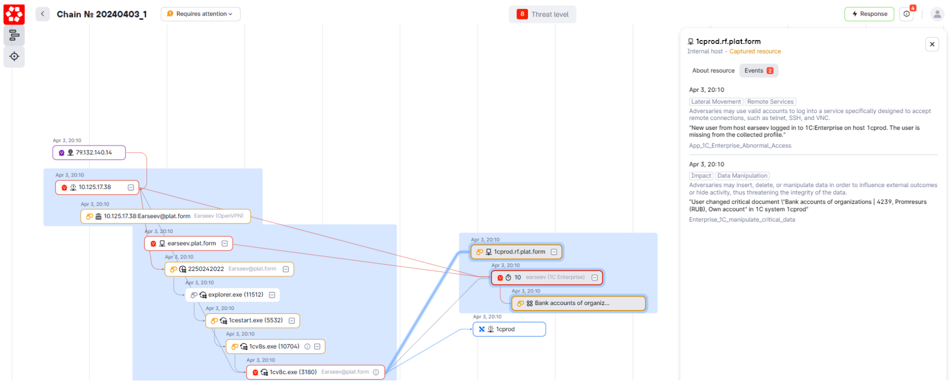
Uses data from Positive Technologies sensors to build a full attack context and investigate.

Assesses threat severity

MaxPatrol O2 views captured resources and assesses the proximity of a non-tolerable event. Upon receiving this information, the system escalates attack chain status to «Attention required» before stopping the hacker or prompting the operator to make a decision.

Stops the attacker

Considers risks to business processes and suggests the ideal response scenario. The scenario can be implemented automatically or manually if adjustments are needed



1cprod.rf.plat.form

Internal host · Captured resource

About resource | Events 2

Apr 3, 20:10

Lateral Movement | Remote Services

Adversaries may use valid accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC.

"New user from host earseev logged in to 1C:Enterprise on host 1cprod. The user is missing from the collected profile."

App_1C_Enterprise_Abnormal_Access

Apr 3, 20:10

Impact | Data Manipulation

Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data.

"User changed critical document \"Bank accounts of organizations | 4239, Promresurs (RUB), Own account" in 1C system 1cprod"

Enterprise_1C_manipulate_critical_data

Learn more about
cybersecurity on
autopilot

Positive Technologies ecosystem

Rules out

non-tolerable events
for business.

Automates SOC activities

for the detection,
investigation, and reaction
to incidents

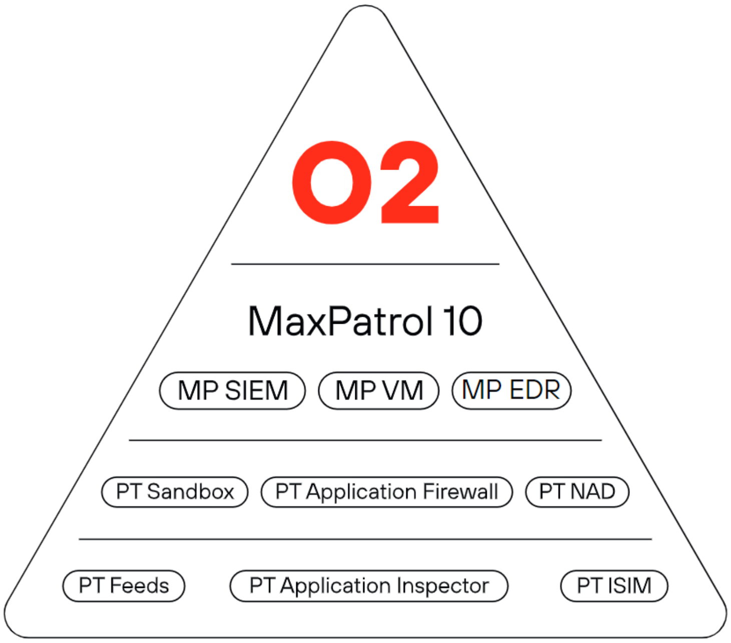
Knows how attackers act

thanks to the experience
of Positive Technologies in
regular cyberexercises, the
Positive Dream Hunting
Bug Bounty, and Standoff

No niche skills required

for the metaproducts
to be effective

Brings together Positive Technologies products that function as sensors, exchange knowledge, and provide comprehensive IT system protection with minimal human involvement.



O2

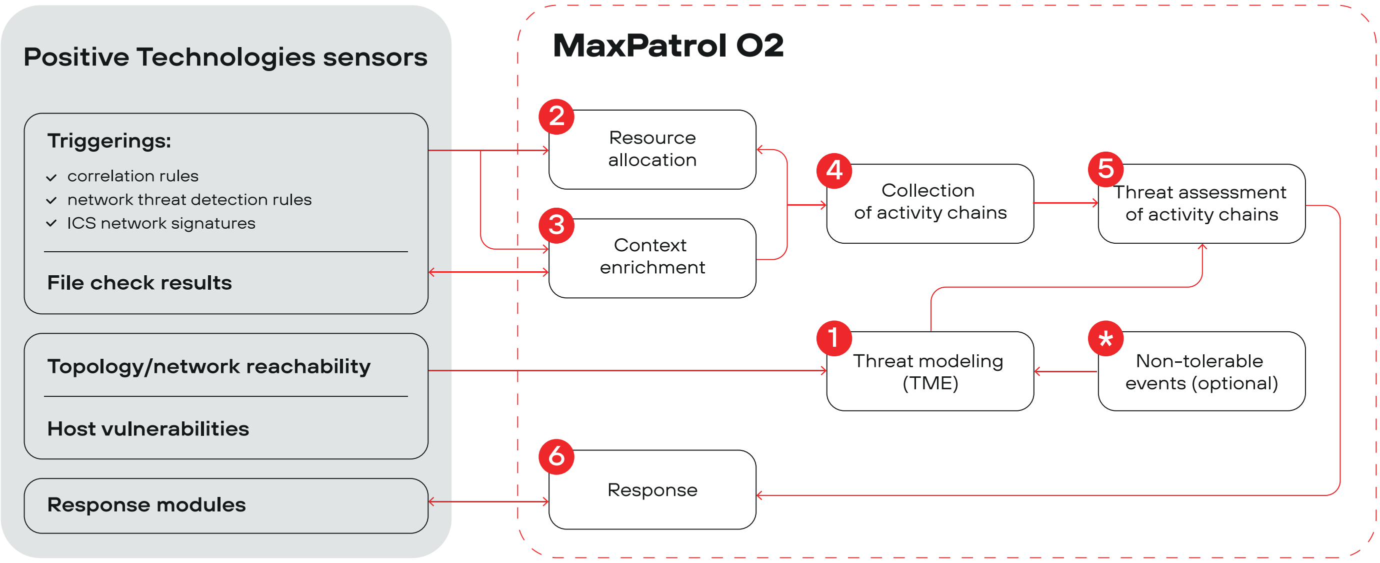
MaxPatrol 10

MP SIEM · MP VM · MP EDR

PT Sandbox · PT Application Firewall · PT NAD

PT Feeds · PT Application Inspector · PT ISIM

How MaxPatrol O2 works



Positive Technologies sensors

Triggerings:

- correlation rules
- network threat detection rules
- ICS network signatures

File check results

Topology/network reachability

Host vulnerabilities

Response modules

MaxPatrol O2

2 Resource allocation

3 Context enrichment

4 Collection of activity chains

5 Threat assessment of activity chains

1 Threat modeling (TME)

* Non-tolerable events (optional)

6 Response

global.ptsecurity.com
info@ptsecurity.com

Positive Technologies is an industry leader in result-driven cybersecurity and a major global provider of information security solutions. Our mission is to safeguard businesses and entire industries against cyberattacks and non-tolerable damage. Over 4,000 organizations worldwide use technologies and services developed by our company.