PRODUCT OVERVIEW

THREAT MONITORING

Be proactively contacted by ESET experts whenever a security anomaly or possible breach is detected in real time

ENJOY SAFER TECHNOLOGY™

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ESET Threat Monitoring service helps customers navigate the large amount of gathered data, events and alarms generated by ESET's endpoint detection and response solution—ESET Enterprise Inspector—and harness the tool's full potential without having to change their existing IT priorities.

Why **ESET Threat Monitoring service?**

GET THE MOST OUT OF ESET'S EDR

ESET Enterprise Inspector is a sophisticated EDR tool for identification of anomalous behavior and breaches, risk assessment, incident response, investigation and remediation.

It monitors and evaluates all the activities happening in the network in real time and allows organizations to take immediate action if needed.

ESET Enterprise Inspector is a prerequisite for ESET Threat Monitoring service.

LACK OF PRODUCT KNOWLEDGE

Utilizing new products without any previous knowledge can become tricky even for organizations with dedicated security or IT teams. In addition, keeping up with the rapidly changing cyber threat landscape can be challenging and sometimes best left to experts.

LACK OF MANPOWER

Helps security teams and IT administrators prioritize their workload by pinpointing only the important events. In addition, an organization can take months to hire and train a team to implement and monitor an endpoint detection and response platform.

REST EASY

Organizations can rest easy knowing that security experts are monitoring their environment daily for any anomalies or potential breaches. If any are identified, organizations are contacted proactively so they can quickly remediate the issues that were found.

LONG-TERM COSTS

Creating dedicated teams and/or hiring specialists to perform niche occasional tasks can incur high long-term costs. Purchasing products and services from a single vendor provides accounting departments peace of mind, especially for multinational corporations.

ESET Threat Monitoring service technical features

DAILY MONITORING

Organization's threat console will be checked by a live operator from ESET at least once every 24 hours within regular business days.

COMPILED REPORT

Threat Monitoring operators compile their findings into clear and comprehensible status reports, then reach out to the organization's contact to alert them of any critical events that warrant immediate attention.

ONGOING FINE-TUNING

After a report has been created, threat monitoring operators create new rules and/or exclusions as well as recommendations on how to proceed in case of a real threat.

ON-PREMISE DATA

All threat and organization data continues to stay on-premise by setting up a secure VPN connection between ESET and the organization.

INITIAL ASSESSMENT

A thorough initial assessment is completed to assess the specific organization's security policies as well as develop an internal profile.

If any anomalies or potential breaches are identified, organizations are contacted proactively so they can quickly remediate the issues that were found.

The stages

Initial assessment

- Each service starts with an assessment of not just the customer's environment, but organizational composition and general cyber security attitude.
- A full interview is completed with relevant organizational staff members to collect all required information.
- The result of this phase is an Organization Security Profile, which can be consulted in the future by any Threat Monitoring operator that requires specifics related to the organization to make correct judgments.

Regular operation

- ESET Threat Monitoring operators log in daily to check events and alarms and subsequently adjust the internal rules and settings as needed.
- Findings from each investigation are compiled into comprehensible status reports that express technical details in human-readable language.
- Organizations are contacted to alert them of any critical events that warrant immediate attention.

Optimization

- This phase begins after a few consecutive days of running ESET's EDR—ESET Enterprise Inspector—in the organization's live environment.
- During this phase, operators review the generated alarms and the rules that triggered them.
- Taking into account the organization's environment and initial assessment, exclusions are created for all false positives and events that are harmless.

ESET IN NUMBERS

110m+ users worldwide

400k+ business customers

200+ countries & territories

13 global R&D centers