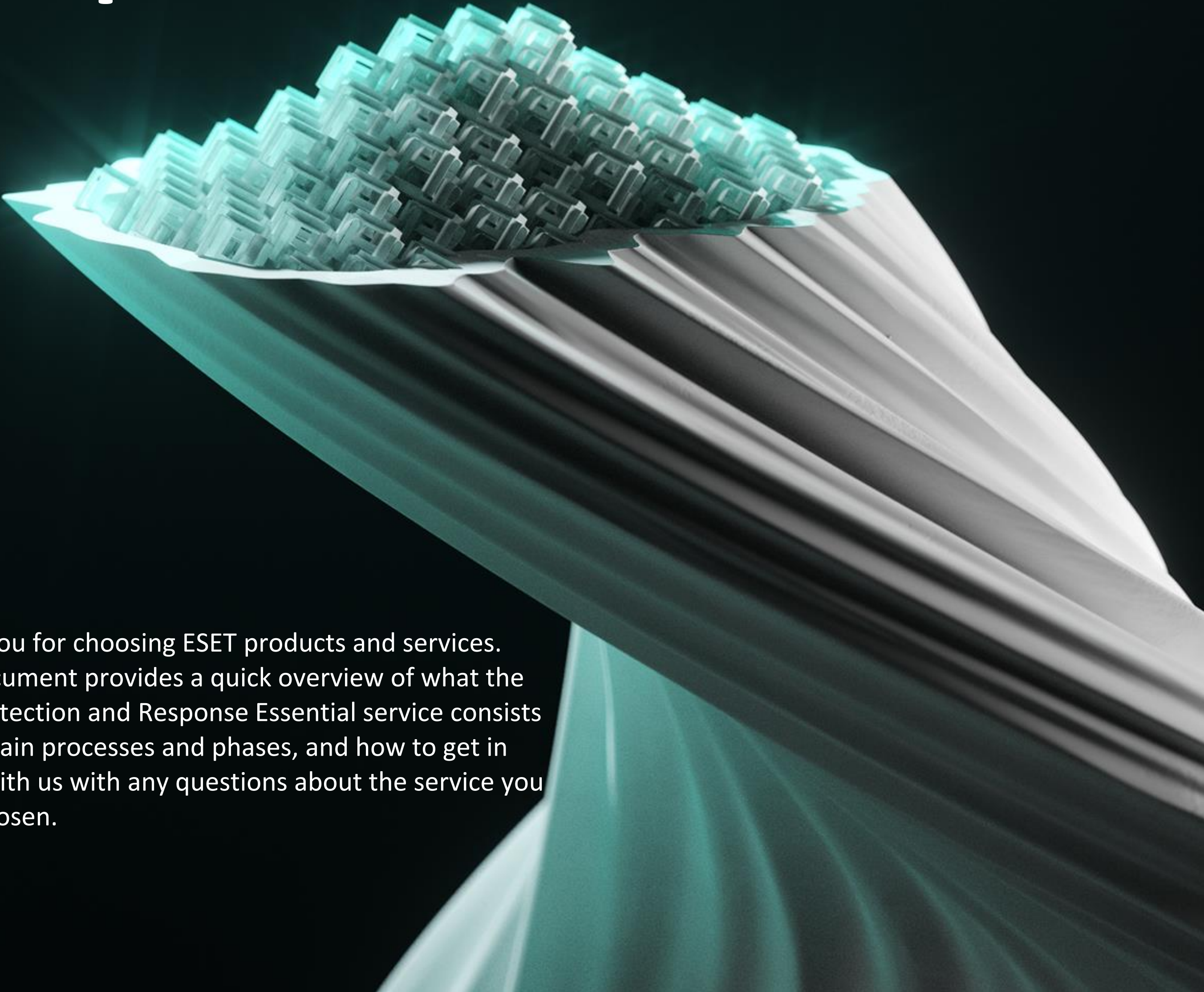
Service Specification

ESET Detection and Response Essential



Thank you for choosing ESET products and services. This document provides a quick overview of what the ESET Detection and Response Essential service consists of, its main processes and phases, and how to get in touch with us with any questions about the service you have chosen.

SERVICE SUMMARY

ESET Detection and Response Essential is a step above standard product support, thanks to its focus on security-related challenges that customers face. Designed to complement our endpoint product platform and general product ecosystem, it gives organisations the peace of mind that, in the event of a security issue, ESET cybersecurity experts are always on hand to help investigate, identify and resolve any threats that might infiltrate standard defences. The service covers everything from primary malware investigation and removal to automated and manual file analysis, to incident investigation and response, and digital forensics.

Whilst our award-winning ESET Endpoint Security product is widely recognised as one of the best in the industry, the highest level of security can only be achieved by a combination of robust technology and human expertise. No preventive layer can be 100% effective and organisations are increasingly recognising the need for a backup plan if an incident occurs. This is where ESET Detection and Response Essential comes into play.

SERVICE PHASES

1. Initial assessment and enrolment phase

Each service begins with an assessment of the customer's environment, infrastructure, organisational composition and general cybersecurity attitude. This is done by completing the service-specific Assessment Form.

Should some of the information required for effective decision-making during investigations of potential threats be missing, the Security Services team performs a full interview with the customer's designated staff until they have obtained all the necessary information.

The result of this phase is the creation of an Organisation Security Profile, which can be consulted in the future by our Security Services operators should they require information about any specifics related to the customer's environment, infrastructure, organisational structure or general cybersecurity attitude.

The final step is the verification of contact details and communication channels on both sides (see Contact Guidelines).

2. Standard operational phase

After the initial assessment and enrolment phase has been completed, our Security Services team is on standby to respond to any potential security issues and incidents reported via the defined communication channels (see the section Contacts and communication channels). Tickets should be submitted via the designated web contact form and must include a valid ESET product licence, so they can be correctly associated with the customer account.

The scope of support during the standard operational phase is described in the section below.

Response and resolution (if applicable) times are based on the SLAs defined in this document (see the section SLA).

The service availability is 24 hours per day, seven days a week and 365 per year.

SCOPE OF SERVICE

The focus of this service is primarily on digital security-related issues and questions. The primary goal is to determine maliciousness and, if confirmed, to provide suggestions for mitigation and resolution in general. The scope of the service includes support for the following main areas and issue types:

Issue Type	Issue Description	Activity Description	Required Inputs and Resulting Outputs
Malware: Missing detection	Malware is not detected	Submitted file, URL, domain or IP is analysed and, if found to be malicious, detection is added, and information about malware family is provided.	**Input:** product version, file/URL/domain/IP **Output:** if input is found to be malicious, information about added detection (incl. detection name); otherwise clean status is confirmed
Malware: Cleaning problem	Malware is detected but cannot be cleaned	Cleaning of submitted file is tested and improved if found problematic. In special cases, standalone cleaner application might be provided.	**Input:** product version, file, logs, information about the environment **Output:** if cleaning improved, information about planned fix is provided; standalone cleaner application/procedure if applicable
Malware: Ransomware infection	System is infected with ransomware	Ransomware infection is evaluated and, if decryption is possible, a decryptor is provided (existing or new). Otherwise, basic mitigation and prevention hints are provided.	**Input:** product version, examples of encrypted files, payment info file, logs, malware sample (if indicated so in GPC table) **Output:** decryptor (if possible); otherwise, basic mitigation and prevention hints
False positive	File, URL, domain or IP is falsely detected	Submitted file, URL, domain or IP is analysed and, if found falsely detected, the detection is removed.	**Input:** product version, file/URL/domain/IP, logs, screenshots **Output:** if input is found malicious, information about removed detection
General: Suspicious behaviour investigation	Suspicious behaviour not linked to any other listed category	Based on description of suspicious behaviour as well as other provided data, behaviour is analysed, and a potential solution is suggested.	**Input:** product version, suspicious behaviour description, logs, information about environment, additional data on request, incl. remote connection in specific cases **Output:** if possible, problem resolution along with basic information
Basic file analysis	Basic info about file is needed	Is submitted file clean or malicious? If clean, basic info is provided. If malicious, reasons for detection, malware family and basic info about functionality are provided.	**Input:** file; questions are specified **Output:** analysis result, along with basic information
Detailed file analysis	Detailed info about malware is needed	Is submitted file clean or malicious? If clean, basic info is provided. If malicious, reasons for detection, malware family and detailed info about functionality are provided.	**Input:** file **Output:** analysis result, along with detailed information
Digital forensic analysis	An incident needs to be investigated, all data will be submitted, no live interaction is needed. It's a post-incident investigation	Data from the affected environment is analysed. Requested level of information is provided.	**Input:** data from the environment: disk clone, memory dump, files, etc.; questions or/and level of detail is specified **Output:** analysis result
Digital forensic incident response assistance / DFIR assistance	An incident needs to be investigated, it's an ongoing incident, interaction is provided (phone call, remote connection). This is not full DFIR, it's DFIR assistance	Incident is investigated online. Consultation is provided. This may lead to file analysis and/or digital forensics.	**Input:** data from the environment, access to the environment; questions or/and level of detail is specified; info about already investigated/identified facts **Output:** any of the following: consultation, changes in the environment, report, redirection to another service

SERVICE LEVEL AGREEMENT (SLA)

Service Activity Group	Service Activity	Issue / Request Type	Static SLA and Dynamic SLA based on Severity A/B/C
Endpoint Security Support	Malware: Missing detection	Malware is not detected	**2/4/24 hours**
	Malware: Cleaning problem	Malware is detected but cannot be cleaned	**2/4/24 hours**
	Malware: Ransomware infection	System is infected with ransomware	**2/4/24 hours**
	False positive	File, URL, domain or IP is falsely detected	**2/4/24 hours**
	General: Suspicious behaviour investigation	Suspicious behaviour not linked to any other listed category	**2/4/24 hours**
Incident investigation & response assistance	Basic file analysis	Basic info about file is needed	**2/4/24 hours**
	Detailed file analysis	Detailed info about malware is needed	**2/4/24 hours**
	Digital forensic analysis	An incident needs to be investigated, all data will be submitted, no live interaction is needed. It's a post-incident investigation	**2/4/24 hours**
	Digital forensic incident response assistance / DFIR assistance	An incident needs to be investigated, it's an ongoing incident, interaction is provided (phone call, remote connection). This is not full DFIR, it's more of a DFIR assistance	**2/4/24 hours**

SEVERITY LEVELS

Severity levels are used to specify the nature and urgency of reported issues/requests and apply only to some specific issue/activity sub-types.

A. Critical

Issues and requests of a critical nature – especially ones that have been confirmed to affect business continuity. Typical examples of critical issues are live ransomware infection, live incident response and similar. Critical severity issues/requests have a guaranteed **two hour SLA** for the Initial Human Response.

B. Serious

Issues and requests of a serious nature where there is a strong suspicion that business continuity might be affected. Typical examples are reporting false positives, investigation of potentially suspicious behaviour etc. Serious severity issues/requests have a guaranteed **four hour SLA** for the Initial Human Response.

C. Common

Issues and requests of a common nature where the initial response time does not affect the final output and business continuity. Typical examples are a retrospective investigation of a historical incident, planned detailed malware analysis etc. Common severity issues/requests have a guaranteed **twenty-four hour SLA** for the Initial Human Response.

RESPONSE TYPES

1. Automated System Response

Automated email generated by the system. This email is generated within a few minutes at most and simply serves the purpose of confirming that the ticket has been created correctly.

2. Initial Human Response

This is the primary response to which SLAs apply. It is the first response generated by a human operator who performs a basic check of the reported issue/question and provides one, or a combination of, the below items:

- Severity check – when a ticket is created an issue severity should be selected as this can affect the actual SLA times. However,please note that the initially selected severity can change dependent on the initial analysis (e.g. an issue that was considered A. Critical might prove to be only B. Serious or C. Common and vice versa). ESET reserves the right to change the severity based on the outcomes of the initial analysis.

- Solution and/or workaround – often the reported issue is known and a solution or temporary workaround exists and can be provided right away.

- Initial analysis – basic analysis of the reported issue.

- Data integrity check – for issues where additional contextual data (sample file, system log, endpoint product log etc.) is required, the operator checks the integrity and completeness of the provided data.

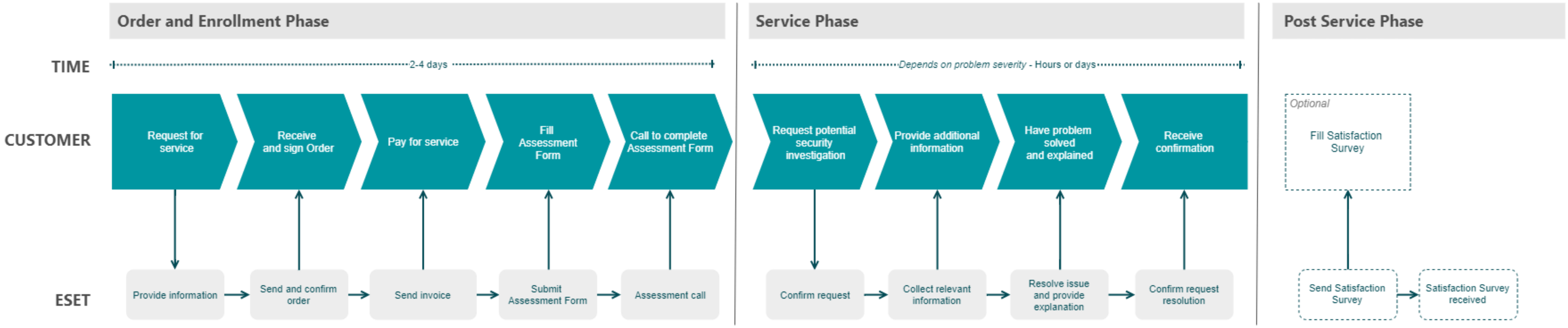
- Request for additional data – if the above mentioned integrity check and basic analysis shows that the data provided in the ticket is incomplete or insufficient for further investigation, then operators can request additional data to be provided.

- Estimated time required for final output – the SLA guarantees times only for the Initial Human Response, as the time required for the actual final output varies case by case depending on the reported issue/request. If operators will try to provide an estimated time required to complete, however this is not a guarantee and in some cases it is not possible to provide an accurate estimate.

3. Final Output

This is the final output and/or solution provided as a response to the reported issue/request within the scope of the specific service. The type of output varies based on the activities related to different issue types (e.g. a report, recommendation etc.).

PROCESS HIGH-LEVEL OVERVIEW


Order and Enrollment Phase
Service Phase
Post Service Phase
TIME
2-4 days
Depends on problem severity - Hours or days
CUSTOMER
Request for service
Receive and sign Order
Pay for service
Fill Assessment Form
Call to complete Assessment Form
Request potential security investigation
Provide additional information
Have problem solved and explained
Receive confirmation
Optional
Fill Satisfaction Survey
ESET
Provide information
Send and confirm order
Send invoice
Submit Assessment Form
Assessment call
Confirm request
Collect relevant information
Resolve issue and provide explanation
Confirm request resolution
Send Satisfaction Survey
Satisfaction Survey received