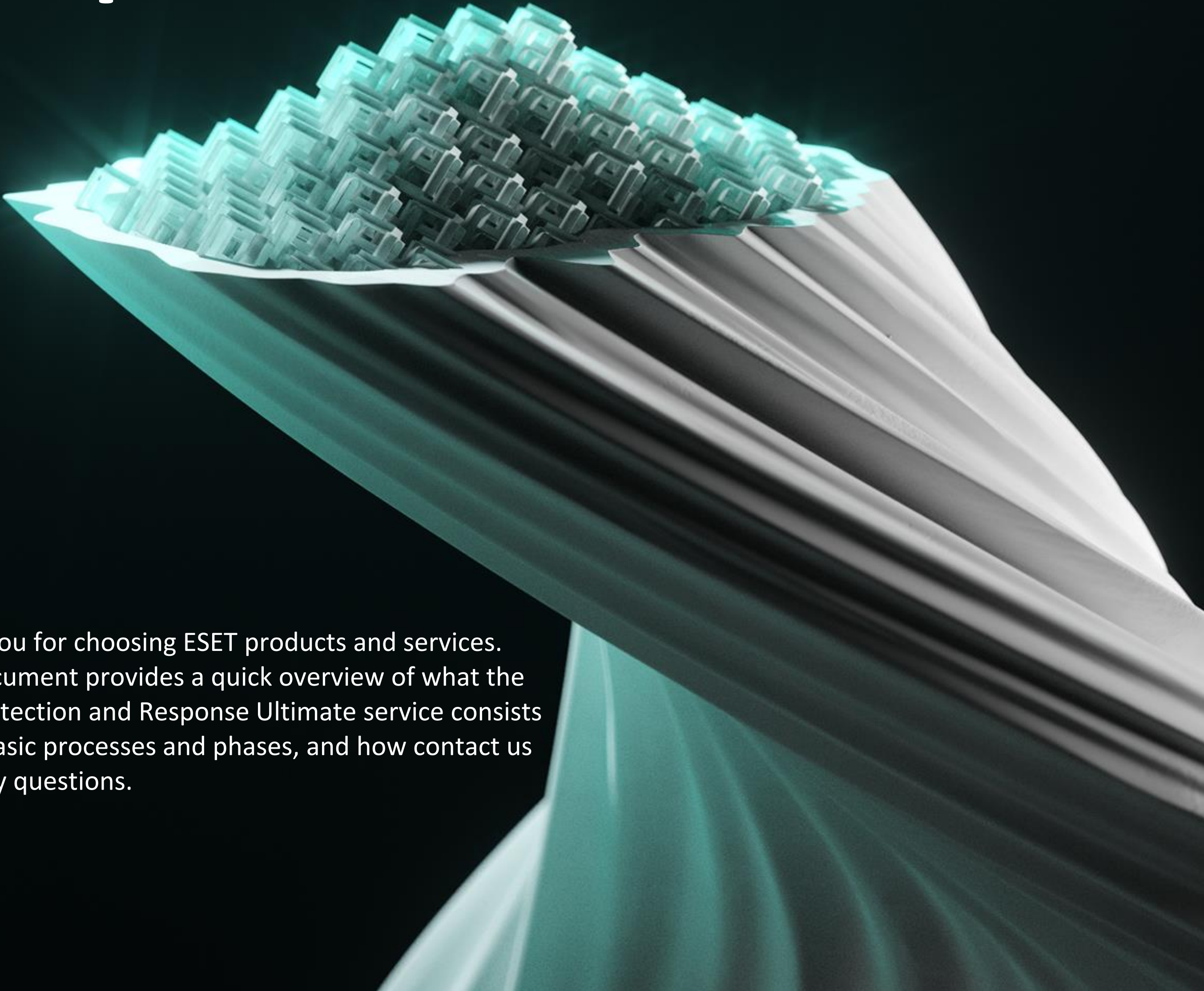
Service Specification
ESET Detection and Response Ultimate



Thank you for choosing ESET products and services. This document provides a quick overview of what the ESET Detection and Response Ultimate service consists of, its basic processes and phases, and how contact us with any questions.

SERVICE SUMMARY

ESET Detection and Response Ultimate goes a step beyond standard product support and is built to provide effective help in the investigation of incidents and security challenges, analyse potentially harmful files and propose response and remediation steps to ensure business continuity. Furthermore, Detection and Response Ultimate has been designed specifically to address the needs of organisations which decide to elevate their security by adding our XDR enabling solution, ESET Inspect (EI), to their stack and want to ensure they can reap the maximum benefit from it immediately after its deployment. This is achieved thanks to daily proactive monitoring of the customers' EI consoles and periodical threat hunting by ESET security experts.

It is best suited for organisations which do not have the personnel to manage the daily operations of ESET Inspect on their own, but wish to significantly increase their security stack thanks to the many benefits that XDR and ESET Inspect offers. Thanks to ESET Detection and Response Ultimate customers can be sure that their new product is correctly optimised and customised to their organisation, and that they can consult ESET cybersecurity experts if needed.   Whilst our award-winning products are widely recognised as some 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 preventative layer can ever be 100% effective, and organisations are increasingly recognising the need for a strong backup plan, should an incident occur. This is where ESET Detection and Response Ultimate comes into play – assuring organisations that ESET cybersecurity experts are always on hand to help investigate, identify and resolve any potentially harmful events.

SERVICE PHASES

1. Initial assessment and enrolment phase

ESET Detection and Response Ultimate is truly a complete solution. ESET engineers also take care of the initial deployment and make sure that the product is always kept on the latest available version, thanks the inclusion of ESET Deployment and Upgrade services.

Each service starts with an assessment of the customer's environment, infrastructure, organisational composition and general digital security attitude. This is carried out by completing a service specific Assessment Form.

If information required for effective decision making during investigations of potential threats is missing, the Security Services team performs a full interview with the customer's designated staff until they have obtained all 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 composition or general digital security attitude.

The final step is the verification of contact details and communication channels on both sides (see the section Contacts and communication channels). This final part also includes the verification of the connection method to the environment itself, which is normally done via the customer's VPN (access is required purely to the IP addresses of the EI and ESMC web consoles).

2. Standard operational phase

The primary proactive part of the service is the daily monitoring and management of the EI web console. This activity, labelled Threat Monitoring in the Service Scope overview table below, should be understood as an overall check of the console - especially triggered alarms, further investigation of potential threats and subsequently the prioritisation of alarms that require an intervention on the customer’s side.

Threat Monitoring operators a) compile their findings into clear and comprehensible bi-weekly Status Reports and b) reach out to the customer’s designated point of contact to alert them of any critical events that warrant immediate attention. Any detected anomalies, pinpointed for further investigation on the customer’s side, are addressed by ESET with recommendations on how to proceed in case the anomaly would prove to be a real threat. In case Threat Monitoring operators create new rules and/or exclusions, they document this in the next Status Report to be created.

The security services team is focused primarily on Detections with a Severity Score of above 70 (EI metric to categorise the potential harmfulness of Detections). Detections of a lower severity and/or Informational Alarms are checked only to provide further context in case an incident is identified. EI itself works in tandem with our ESET Endpoint Security solution so standard threats are stopped preventively, already on this level, and the focus on Detections of above 70 within EI is sufficient in ensuring that even advanced persistent threats which evade standard detection methods are captured.

On top of the daily proactive Threat Monitoring, more thorough Threat Hunting activities are also performed on a quarterly basis by ESET security experts.

Furthermore, a reactive service is also offered; whereby, following completion of the initial assessment and enrolment phase, our Security Services team waits 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 that it can be correctly associated with the customer’s account.

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

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

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 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, 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 potential solution is suggested.	**Input:** product version, suspicious behaviour description, logs, information about environment, additional data on request, including 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 is 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 is 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 are analysed. Requested level of information is provided.	**Input:** Data from the environment: disk clone, memory dump, files, 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-blown DFIR, it's DFIR assistance	Incident is investigated online. Consultation is provided. This may lead to file analysis and/or digital forensic.	**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
EI: rules support	Support related to rule creation, modification or disfunction, e.g. to detect specific malware behaviour	Specified rule or behaviour is analysed and consultation is provided.	**Input:** version of EI, rule, specification of the problem, in cases it turns out to be a bug logs, database/database access **Output:** consultation and recommendation on how to set up desired rule
EI: exclusions support	Support related to exclusion creation, modification or disfunction is needed	Specified exclusion or behaviour is analysed and consultation is provided.	**Input:** version of EI, exclusion, specification of the problem, in cases it turns out to be a bug logs, database/database access **Output:** consultation and recommendation on how to set up desired exclusion
EI: general security related question	EI security related question not linked to any other listed category	Specified behaviour is analysed. Result may be advice to the customer or bug/ improvement for developers.	**Input:** version of EI, specification of the problem, in cases it turns out to be a bug – logs, database/database access **Output:** consultation and recommendation on how to achieve desired outcome
EI: Initial optimization	After installation to new environment, EI generates large number of false positives	One-time action (may contain several rounds). Most frequent FP detections in EI environment are checked. Exclusions are created. Custom rules may be created, or rules may be modified to reflect expectations.	**Input:** assessment form, access to the environment or exported data **Output:** optimisation report, changes within EI environment such as creation/modification of rules and exclusions
EI: Threat Hunting (proactive)	Customer wants to have their environment inspected proactively for the latest threat using ESET's righ knowledge of IOCs (one-time inspection on a quarterly basis)	One-time action. Environment is inspected using EI. Information will be provided about found threats or weaknesses. Advice will be provided. Individual steps will be defined in checklist.	**Input:** assessment form, access to the environment **Output:** Threat Hunting report
EI: Threat Monitoring	Customer wants to have their environment monitored by security professionals	Continuous action. Customers environment is checked each day (using EI console). Suspicious EI detections are verified, only detections with severity 70 and higher are actively investigated and resolved. False positive detections are resolved. Correct detections are reported to the customer (reports sent in specified intervals). In cases where detection is significant and urgent, customer is notified immediatelly through emergency contact.	**Input**: assesment form, access to the environment **Output**: periodic reports, periodic sync calls, emergency reports, changes to the EI environment
EI: Threat Hunting	Customer wants to have his environment inspected, if	Periodic action. Environment is inspected using EI. Cutomer will be informed about found	**Input:** assesment form, access to the

	there are any threats present (periodic inspection)	threats or weaknesses. Advice will be provided. Individual steps will be defined in checklist.	environment **Output**: periodic reports, periodic sync calls, emergency reports, changes to the EI environment"
Deployment & Upgrade	Customer wants EI to be deployed and kept up to date on the latest version.	One time action. ESET team will deploy or upgrade the EI console and related ESET Products/components specified in this Annex, Art. 2 C, section 1.2. (as agreed with the customer). Deployment & Upgrade will be carried out by ESET by deploying/upgrading of 100 units of Products/components. Manual on how to finish these deployments and upgrades is shared with customers.	**Input:** assesment form, access to the environment **Output:** correctly deployed and setup EI Server and EI Agent on a sample of 100 endpoints

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	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-blown DFIR, it's more of a DFIR assistance.	**2 / 4 / 24 hours**
EI Security Support	EI: rules support	Support related to rule creation, modification or disfunction, e.g. to detect specific malware behaviour, is needed	**2 / 4 / 24 hours**
	EI: exclusions support	Support related to exclusion creation, modification or disfunction is needed	**2 / 4 / 24 hours**
	EI: general security related question	EI security- related question not linked to any other listed category	**2 / 4 / 24 hours**
	EI: Initial Optimisation	After installation to new environment, EI generates large number of false positives.	**N/A** (planned activity performed by ESET experts)
	EI: Threat Hunting (on-demand)	Customer wants to have their environment inspected, if there are any threats present (one time inspection)	**2 / 4 / 24 hours**
EI Security Service	EI: Threat Monitoring	Customer wants to have their environment monitored by security professionals	**N/A (customer expects only continuous monitoring to be achieved but does not report issues as this is a proactive type activity - SLA applies only from L1/2 towards L3 for help)**
	EI: Threat Hunting (proactive)	Pro-active inspection of environment for any threats	**N/A** (planned activity performed by ESET experts)
EI Deployment & Upgrade	EI: Deployment & Upgrade	Complimentary professional service to perform initial deployment of EI and related products/components required for proper EI operation. Subsequent upgrades to their latest version	**N/A** (planned activity performed by ESET experts)

SEVERITY LEVELS

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

A. Critical

Issue and requests of a critical nature – especially ones that have been confirmed to affect business continuity. Common examples of critical issues are a 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. Common examples include the reporting of false positives, or the 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. Common examples include a retrospective investigation of a historical incident, help with setup of ESET Inspect rules/exclusions, planned detailed malware analysis etc. This severity also includes activities which are planned in advance (e.g. scheduled Threat Hunting) and any issues/requests that might arise during their delivery. 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

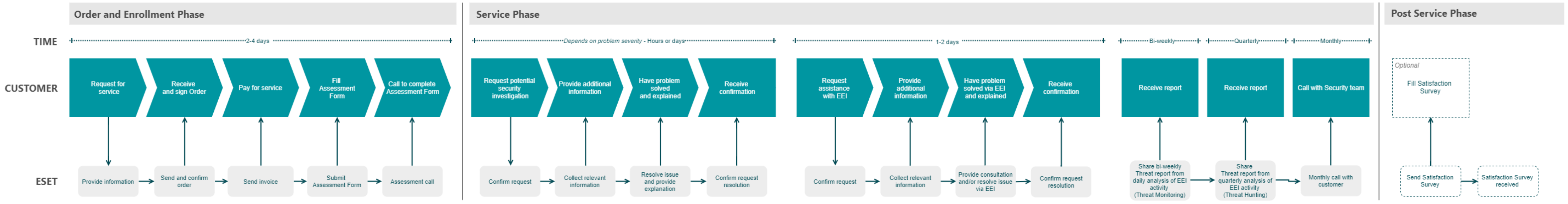
This is the primary response to which SLAs apply. It is the first response generated by a human operator who performs a basic check of the reported issue/question and provides one, or a combination of, the below items:

- 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 depending based 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 possible, 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 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
CUSTOMER
ESET
2-4 days
Request for service
Receive and sign Order
Pay for service
Fill Assessment Form
Call to complete Assessment Form
Provide information
Send and confirm order
Send invoice
Submit Assessment Form
Assessment call
Depends on problem severity - Hours or days
Request potential security investigation
Provide additional information
Have problem solved and explained
Receive confirmation
Confirm request
Collect relevant information
Resolve issue and provide explanation
Confirm request resolution
1-2 days
Request assistance with EEI
Provide additional information
Have problem solved via EEI and explained
Receive confirmation
Confirm request
Collect relevant information
Provide consultation and/or resolve issue via EEI
Confirm request resolution
Bi-weekly
Quarterly
Monthly
Receive report
Receive report
Call with Security team
Share bi-weekly Threat report from daily analysis of EEI activity (Threat Monitoring)
Share Threat report from quarterly analysis of EEI activity (Threat Hunting)
Monthly call with customer
Optional
Fill Satisfaction Survey
Send Satisfaction Survey
Satisfaction Survey received