This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the left.

Endpoint Detection and Response Standard Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously
- Enter “<organization name>” in the Find text box
- Enter your organization’s full name in the “Replace” text box
- Click “More”, and make sure “Match case” is ticked
- Click “Replace All”
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This standard aims to define the detailed cybersecurity requirements related to Endpoint Detection and Response (EDR) solutions for <organization name>. The ability of <organization name> to deploy and use EDR solution in accordance with this standard will assist in proper monitoring of malicious activities and detection of anomalies on all endpoints, and in preserving the availability, integrity and confidentiality of <organization name>'s assets and information.

The requirements in this standard are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to ECC-1:2018 and CSCC-1:2019, in addition to other related cybersecurity legal and regulatory requirements.

Scope

The standard covers <organization name>'s information and technology assets and applies to all personnel (employees and contractors) in <organization name> and related third parties.

Standards

1	General Requirements
Objective	The EDR solution must be securely managed and appropriately used when required.
Risk Implication	Misconfiguration of EDR solutions may reduce the chance of threat identification and result in information theft, unauthorized access, and information disclosure.
Requirements	
1-1	At the most general level, the EDR solution must provide real-time continuous security monitoring and collection of endpoint

	data with rules-based automated response and analysis capabilities.
1-2	EDR solution must be deployed as an agent mode solution.
1-3	EDR solution must provide monitoring and protection among every endpoint in the <organization name>. This requirement is independent of the endpoint's operating system. In case of particular operating systems not supporting EDR solution deployment, those must be separated into a special group and monitored in a dedicated, special manner.
1-4	EDR solution must provide information not only about techniques, tactics, and procedures that the attacker uses, but it must also provide information about how attackers break into the internal network, move to other machines, escalate on-host privilege to accomplish their goals in the attack.
1-5	All security updates to the EDR software must be installed, as they are released by the vendor.
1-6	All security updates must follow patch management and hardening policy requirements.
1-7	EDR software updates must be conducted according to the change management procedure.
1-8	EDR solution must provide abilities for deep analysis and advanced forensics examination in case of a need to conduct an investigation.
1-9	EDR solution shall be scalable to address next generation cybersecurity threats concern.
1-10	Periodic backup of relevant data and alerts, EDR configuration files (rules, reports, dashboards, groups, scheduled actions) and file storage management must be conducted according to the <organization name>'s backup policy and procedure.

1-11	A Service Level Agreement (SLA) must be defined to outline specific responsibilities of the EDR solution provider and satisfy <organization name>'s expectations.
1-12	<organization name> must verify list of permissions needed to be assigned for proper work of the EDR agent. List of permission might be different based on the EDR working mode (block or monitor) and should be adjusted accordingly using least privileges rule.
2	Data Collection and Monitoring
Objective	EDR software agents must properly monitor and collect endpoint data, such as processes, connections, volume of activity and data transfers into a central database.
Risk Implication	Improper monitoring and data collection of software agents may have severe consequences in EDR solution not detecting and reacting to threats properly.
Requirements	
2-1	EDR solution must implement a centralized management console with the following features: • simultaneous access, • monitoring of current events, • visualization of the important information, • display of particular event's details, • multi-window work mode, • advanced filtering capabilities, • automatic refreshing, • access without the need to switch interfaces, • automatic reporting.

2-2	EDR solution must monitor and collect activity data from endpoints that could indicate a threat.
2-3	EDR solution must cross-correlate data across the whole environment of its monitoring range.
2-4	EDR solution must collect and monitor data without interfering with the endpoint activities.
2-5	EDR solution must work regardless of whether there is or isn't any antivirus software on the endpoint.
2-6	EDR solution must collect and monitor relevant data to build a complete picture of endpoint activity.
2-7	Relevant data for EDR solution must include information covering the following areas: Processes, Connections, Files, Drivers, Autorun, System, Machine, Users. Additional data sources may be used, including but not limited to: • logs, • performance monitoring, • file details, • running processes, and • configuration data.
2-8	EDR solution must properly collect and monitor endpoint activity no matter where the endpoint is located.
3	Data Analysis and Threat Pattern Identification
Objective	Real time analysis for rapid diagnosis of threats that weren't foreseen in automated response tables.
Risk Implication	Improper data analysis and threat pattern identification may have severe consequences in automatic response and notification not reacting correctly.

Requirements	
3-1	EDR solution must monitor every endpoint in the organization to collect and analyze gathered data that could give indication on suspicious activities or potential threats.
3-2	EDR solution must give a clear signal of being under attack to the <organization name>'s IT staff members. EDR must provide details concerning where the attack comes from and what has the attacker managed to achieve.
3-3	EDR solution must identify threat patterns based on aggregated data from all endpoints, rather than a single one.
3-4	EDR solution must compare new dataset patterns to the previous ones, in order to identify previously unknown or known malicious activities.
3-5	EDR solution must provide behavioral threat detection capabilities.
3-6	EDR solution must use globally accessible knowledge databases concerning cybersecurity threat categorization (e.g., MITRE ATT&CK globally accessible knowledge base of adversary tactics and techniques based on real-world observations).
3-7	EDR solution must assign risk scorings and categorize cyber-threats based on criticality and confidence. Criticality estimates the impact on the cyber environment of a potentially ineffective detection. Confidence means how likely it is that the detection is valid and not a false-positive.
4	Automatic Response and Notification
Objective	Creation of pre-configured rules for rapid response in case of potential rule violation, combined with proper alarming.

Risk Implication	Misconfigured or poor automatic response and notification may have severe consequences in taking proper actions to prevent or stop potential intrusion.
Requirements	
4-1	EDR solution must provide an automatic response and alerting system, covering up-to-date attack scenarios.
4-2	EDR solution must accelerate response time by integrating and sharing security insights with Network Detection and Response (NDR), Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) tools.
4-3	EDR solution must trigger an automatic response based on previously identified threat (Table A).
4-4	EDR solution must prevent the malicious file from running and spreading throughout the network during or after your investigation.
4-5	EDR solution must automatically isolate infected hosts on finding an indicator of compromise associated with a fast-spreading threat.
4-6	EDR solution must automatically quarantine files associated with evasive threats on all endpoints.
4-7	EDR solution must automatically log and notify <organization name>'s IT staff members when the solution identifies a potential threat, triggers an automatic response or when there isn't a defined automatic response to an identified threat.
4-8	EDR solution must gather in the log file any events that may be in the scope of audit inspection (e.g., suspicious activities, threat identification, automatic action, staff notification).
5	Other Standards

Objective	The EDR solution must be securely configured and used appropriately when required.
Risk Implication	If <organization name> is not compliant with all of standards and requirements, it could be exposed to severe threat exposure.
Requirements	
5-1	The following standards must be implemented in relevance to EDR solution: 1. Identity and access Management 2. Disaster recovery and backup 3. Cryptography 4. Event and audit logging 5. Physical security 6. Secure configuration and hardening 7. Event Log Management and Monitoring 8. Malware Protection 9. Backup and Recovery Management 10. Network Detection and Response

Table A – Responding to detections

The response to a detection can take one of the following routes.

File retrieve	Retrieves files.
Process shutdown	Shuts down suspicious processes.
Thread shutdown	Shuts down suspicious threads.
Connection shutdown	Shuts down suspicious connections.
File deletion	Deletes suspicious files.
Registry deletion	Deletes suspicious register records.
Scheduled task deletion	Deletes scheduled tasks.
Service deletion	Deletes services that match particular criteria.

Roles and Responsibilities

1- **Standard Owner:** <head of the Cybersecurity function>

2- **Standard Review and Update:** <cybersecurity function>

3- **Standard Implementation and Execution:** <information technology function>

4- **Standard Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the standard at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the Cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.

2- All personnel at <organization name> must comply with this standard.

3- Any violation of this standard may be subject to disciplinary action according to <organization name>'s procedures.