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.

Network 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 the Network Detection and Response (NDR) for <organization name>.

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 NDR solution must be securely designed and appropriately used when required.
Risk Implication	Misconfiguration of the NDR solution may reduce the success of threat identification and result in information theft, unauthorized access, and information disclosure.
Requirements	
1-1	NDR must combine data science, machine learning and behavioral analysis with well-curated threat intelligence in order to identify in real time or near real time the intent of network traffic and reveal malicious behaviors, independent of applications and even when traffic is encrypted and provide assistance with manual incident and threat hunting response through automation.

1-2	NDR must correlate global threat intelligence to local threats in order to prevent attackers from infecting many victims with the same malware.
1-3	NDR must be deployed in various methodologies (in-line sensors, passive sensors - Table A).
1-4	Physical access to the NDR solution must be restricted to authorized employees only (least privilege assignment for different administrators).
1-5	Administrative access to the management interface of the NDR solution must be restricted for limited group of administrators.
1-6	Unused Network Interface Cards must be disconnected from any network.
1-7	NDR must support IPv4 and IPv6 stack for traffic processing and security rules and traffic policy definition.
1-8	All security updates to the NDR solution must be installed as they are released by the vendor and according to the change management procedure.
1-9	Each management communication channel must be using a dedicated management network or the management network communications which is authenticated and encrypted using validated cryptographic modules that are in line with the National Cryptography Standard's Key Lifecycle Management requirements.
1-10	Time configuration on the NDR solution must be synchronized with a trusted authoritative time server.
2	Traffic monitoring

Objective	The NDR solution must be properly configured and securely managed for proper cyber threat and anomalous behavior detection in monitored networks.
Risk Implication	Misconfiguration of the NDR solution may have severe consequences like failing to analyze network traffic and recognizing a threat, which could lead to data leakage, attack on partner enterprises or even company clients.
Requirements	
2-1	NDR must continually reveal the underlying purpose of traffic, even when the payload is not visible. This allows for protection without prying.
2-2	NDR must model a baseline of what normal network behavior looks like and alert security teams on any suspicious traffic that falls outside of that normal range.
2-3	NDR must attribute malicious behavior to a specific IP address and perform forensic analyses to determine how threats have moved laterally within an environment.
2-4	NDR must provide visibility to multiple public and private cloud environments.
2-5	NDR must be able to analyze encrypted traffic without decryption and detect threats that attempt to hide themselves in encrypted traffic.
2-6	NDR must recognize URLs, applications (based on signatures), IP addresses, TCP/UDP ports.
2-7	NDR must provide the ability to verify compliance to protocol standards and prevent traffic that is not compliant.
2-8	Incident Response team must be able to query the database with the list of “always available” or “always denied”

	resources/attacks which were verified by NDR solution during traffic monitoring.
3	Traffic detection and logging
Objective	The NDR solution must monitor and process traffic in a secure way to save any suspicious activity and notify the incident response team in case of an unknown new possible incident.
Risk Implication	Traffic detection without proper configuration may easily cause malware propagation, phishing exposure and information leak. Improperly configured NDR solution may result in not sufficiently mitigating new possible security incidents in the future.
Requirements	
3-1	NDR must detect threats (e.g. unusual remote access, port scanning, the use of restricted ports or protocols, etc.) in real-time with the use of constantly learning behavioral models derived from machine learning.
3-2	NDR must utilize advance threats detection and reduce investigation time by capturing metadata and also recognize the unique characteristics of malicious behaviors, which lead to reliable identification of network intrusions, even if the tools, malware or attack are completely unknown.
3-3	NDR must collect and enrich security metadata with deep insights and context that allows it to detect and stop a wide range of attack scenarios early and consistently.
3-4	NDR must apply algorithmic models directly to network traffic in order to reveal underlying attack behaviors and then enrich that data with secondary sources (e.g. authentication logs and threat intelligence data) automatically.

3-5	NDR must find signs of attackers who tunnel hidden communications within an SSL/TLS-encrypted web session. By analyzing tiny fluctuations in protocols like HTTPS and DNS, NDR solution must reveal when additional layers of communication are hidden within.
3-6	NDR must identify a wide range of command-and-control behaviors, including attempts to imitate browser behavior, use of hidden tunnels, peer-to-peer communication, malware updating as well as a broad variety of anonymization techniques such as TOR.
3-7	NDR must continuously monitor and alert for unusual privileged access (the complexity of access management makes it prone to misconfigurations).
3-8	NDR must divide gathered information into two sectors: user information section and diagnostic information for administration section.
3-9	NDR must analyze previously captured incidents and draw schemes to avoid them in the future with the use of machine learning and artificial intelligence (ML and AI).
3-10	NDR must gather data about incidents in a dedicated database. Each record must include information about assigned categories of incidents, like phishing emails, malicious links, etc.
3-11	The local threat intelligence database should be updated in real-time to prepare for attacks happening in local enterprises.
3-12	NDR must filter all objects transferred through the network, for instance phishing emails, malicious links, etc. It must be consistent with the requirements of <organization name>'s Malware Protection Standard.

3-13	NDR must inform users about performed actions (in particular: blocked requests or files) by configurable response web pages.
3-14	NDR must use security feeds delivered by national trusted organizations like national level CSIRT.
4	Automatic response and notification
Objective	The NDR solution must use data science and machine learning in order to detect, analyze and protect the systems against future security threats.
Risk Implication	Without proper activity analysis and providing timely alerts for incident response teams, the NDR solution may be ineffective in preventing and mitigating future incidents.
Requirements	
4-1	NDR must constantly detect network activity in order to detect ongoing attacks, while security analysts have more time to proactively hunt for threats and investigate incidents with greater success.
4-2	NDR must accelerate response time by integrating and sharing security insights with EDR, SIEMs and SOAR tools for endpoint to cloud threat management and visibility.
4-3	NDR must deny unauthorized access to prevent access to essential information which might progress attack and compromise sensitive data.
4-4	NDR must immediately inform about rejected or mitigated attacks.
4-5	NDR must gather events and information about them in its database with previously captured anomalies and prevented attacks for future relevance.

4-6	Organization should have runbook scenarios for NDR to protect from adversary threats, for instance removing and mitigation a threat by isolating affected systems, detecting and blocking the spreading of malicious links or phishing emails (detection based on local threat intelligence database with ongoing incidents).
4-7	NDR must gather all log types from <organization name>'s resources.
4-8	NDR must be consistent with the requirements of <organization name>'s Event Log Management and Monitoring Standard.
4-9	NDR must be configured to send only specific logs to the central log system e.g. using syslog protocol and CEF, LEEF or RFC 5425 specified log format.
4-10	NDR must include at least the following information: ● date and time of session ● source IP address ● user login ● destination IP ● action performed ● used traffic policy

Table A – NDR deployment methodologies

There are two major methodologies of NDR deployment:

- in-line sensors - offer direct response capabilities.
- passive sensors - rely on integrations.

In-line sensors	The method is based on placing the NDR solution directly in the path of a network segment, which allows for fast traffic inspection and dropping anomalous or malicious traffic in real-time.
Passive sensors	This option revolves around placing an NDR solution inside the network (usually by integrating with SIEM, SOAR, public/private clouds, etc.) and extracting metadata from taken snapshots, which is then sent for analysis.

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.