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.

Advanced Persistent Threats (APT) 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 detection and prevention of Advanced Persistent Threats (APT). These requirements will assist in reducing the cybersecurity risks and protecting from related internal and external threats to preserve the availability, integrity and confidentiality of <organization name>'s assets.

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

This sمtandard covers <organization name>'s information and technology assets and applies to all personnel (employees and contractors) in <organization name>.

Standards

1	Security environment configuration
Objective	Ensure the successful deployment of security mechanisms to strengthen the environment against Advanced Persistent Threats for complete threat detection and prevention measures.
Risk Implication	Without a properly working and managed SOC team, <organization name>'s resources are exposed to APT, what could have severe consequences for <organization name>'s compliance, business continuity and may result in new possible security incidents caused by attacks performed by APT groups.
Requirements	

1-1	<organization name> must implement Threat Intelligence Service which identifies attacks that allow unauthorized access to a computer network for an extended period of time without being detected.
1-2	<organization name> must investigate what tactics and techniques are used during the attacks performed by identified APT groups.
1-3	<organization name> must assure that logging configuration in each system contains attributes that allows identifying specified behavior (e.g. severity, associated user name, hostname, time, executed command and other dependent data). All of them must be described in SIEM correlation rules.
1-4	<organization name> must define and maintain a list of incident types which may confirm or decline connection to the APT. This list should include at least all incidents related to unauthorized access or malware infection.
2	Confirmation of APT
Objective	All security incidents which appeared in <organization name> environment must be verified in terms of connection with APT
Risk Implication	Ignoring the signs of the APT could lead to the further persistence of the threat actor and may lead to information theft, unauthorized access, and information disclosure.
Requirements	
2-1	<organization name> must carefully investigate all listed types of incidents to confirm or decline that investigated event has any sign of APT. Tactics used by APT groups according to MITRE Attack Framework are described in Table A
2-2	<organization name> must implement mechanisms to securely analyze samples and indicate that they can be associated with APT, using periodically updated two kinds of antivirus/EDR

	and sandbox engines (this capability can be outsourced if needed).
2-3	<organization name> must determine all indicators of compromise (IoCs) associated with the analyzed incident. Table B describes examples of potential IoCs.
2-4	<organization name> must have an isolated environment to detonate analyzed malicious files to describe all actions performed by malware and specify potential new IoC. This environment must be located in a dedicated network segment and deployed on dedicated server groups which are carefully monitored by security solutions. Sandbox solution must be an important part of this environment. (this capability can be outsourced if needed).
2-5	<organization name> must check all found IoC in threat intelligence database. All URLs, IP addresses, hash of suspicious files might be used by threat actor in the past and based on them, <organization name>'s SOC team can identify if this threat actor is a known APT group.
2-6	<organization name> must check with national level cybersecurity incident response team (CSIRT) tactics and techniques used by threat actor if identified APT group is currently performing the attacks in any other organization in <organization name>'s business sector.
3	Attack mitigation
Objective	After successful detection and confirmation of APT, it is crucial to mitigate risk and share an information about an attack with national level CSIRT.
Risk Implication	Without proper mitigation and sharing knowledge about the characteristics of an attack, APT groups may easily cause malware propagation, phishing exposure and information leakage.

Requirements	
3-1	<organization name> must investigate all gathered historical events to determine persistence methods used by found threat actor.
3-2	<organization name> must share knowledge about an attack with national and sector level CSIRT.
3-3	<organization name> must monitor its internal systems to identify all infected endpoints and servers and isolate them.
3-4	Each infected system must be analyzed by the <organization name> to perform actions to mitigate risk or restore disk space from backup file after its removal.
3-5	After threat mitigation on a specific system, <organization name> must monitor its behavior to determine if mitigation was successful.
3-6	<organization name> must take into account that despite taking action to recover the system, its analysis must be carried out each time in the case of detecting new IoC related to the analyzed APT.
4	Other Standards
Objective	Cybersecurity of entire <organization name> is based on built according to best practices and compliant to standards and relevant policies security environment.
Risk Implication	If <organization name> is not compliant with all applicable and mandatory standards and requirements, it could be exposed to severe threat rise specific to the areas covered by below mentioned standards.
Requirements	

4-1	The following standards must be implemented to efficiently detect and prevent APT: 1. Event and Audit Logging 2. Event Log Management and Monitoring 3. Endpoint Detection and Response 4. Network Detection and Response 5. User Behavior Analysis 6. Security Information and Event Management 7. Penetration Testing 8. Web Applications Protection 9. Vulnerability Management 10. Data Loss Prevention

Table A – Tactics used during an Attacks according to MITRE Attack framework

Phase of attack tactics	Description
Reconnaissance	The adversary is gathering data that will be used when planning future actions. This phase refers to tactics in which adversaries acquire information that may be used to support targeting, either actively or passively. Details on the victim department infrastructure and staff/personnel are examples of such information.
Resource Development	The adversary is attempting to gather resources to assist operations. Adversaries create purchase or compromise/steal resources (infrastructure, accounts or capabilities) that can be utilized to enable targeting as part of resource development tactics.
Initial Access	The adversary is attempting to gain access to your network. Initial Access is a set of approaches that employ a variety of entrance vectors to get a foothold in a network. Targeted spear phishing and exploiting vulnerabilities on public-facing web servers are two methods used to get a foothold. Initial access footholds

	may allow sustaining access (for ex. valid accounts and use of external remote services).
Execution	The adversary is trying to run malicious code. Techniques that result in adversary-controlled code running on a local or remote system are referred to as execution. Malicious code execution techniques are frequently combined with techniques from other tactics to achieve broader goals, such as network exploration or data theft.
Persistence	The adversary is attempting to keep their foothold. Adversaries utilize persistence strategies to maintain access to systems despite restarts, altered credentials, and other disruptions. Persistence techniques include changing or hijacking legitimate code or adding startup code, as well as any access, action, or configuration modifications that allow adversaries to keep their grip on systems.
Privilege Escalation	The adversary is attempting to obtain access to higher-level privileges. Adversaries utilize Privileged Escalation strategies to get higher-level permissions on a system or network. Adversaries can often gain unprivileged access to a network and explore it, but they need elevated permissions to complete their tasks. Taking advantage of flaws in the system, misconfigurations and vulnerabilities is a common strategy.
Defense Evasion	The adversary is attempting to evade detection. Defense evasion refers to the strategies used by the adversaries to escape discovery during a compromise. Uninstalling/disabling security software or obfuscating/encrypting data and scripts are examples of defense evasion techniques. Adversaries utilize and misuse trusted processes to conceal and disguise their malware.
Credential Access	The attacker is attempting to steal account names and passwords. Techniques for stealing credentials such as account names and passwords are referred to as credential access. Keylogging and credential dumping

	are two methods of obtaining credentials. Using authentic credentials can offer attackers access to systems, make them harder to detect, and allow them to create new accounts to further their objectives.
Discovery	The adversary is attempting to ascertain your surroundings. Discovery refers to ways that an adversary might employ to learn more about the system and internal network. These strategies aid adversaries in observing their surroundings and orienting themselves before deciding how to respond. They also allow enemies to investigate what they can influence and what is around their entrance point to see whether it can help them achieve their current goal. This post-compromise information gathering goal is frequently accomplished using native operating system technologies.
Lateral Movement	The adversary is attempting to navigate through your surroundings. Adversaries utilize lateral movement tactics to gain access to and control remote systems on the network. Exploring the network to discover their target and then obtaining access to it is a common requirement for completing their primary goal. Gaining access to their goal frequently necessitates pivoting across numerous systems and accounts. To perform Lateral Movement, adversaries may install their own remote access tools or utilize valid credentials using native network and operating system capabilities, which may be stealthier.
Collection	The adversary is attempting to collect data relevant to their goal. Collection refers to the strategies adversaries may employ to gather information as well as the sources from which the information is gathered that are relevant to achieving the adversary's goals. After acquiring data, the following step is often to steal (exfiltrate) it. Various disk kinds, browsers, audio, video and email are all common target sources. Screenshots and keyboard input are two common techniques of data collection.
Command and Control	The adversary is attempting to communicate with infected systems in order to gain control of them.

	Adversaries may employ command and control tactics to communicate with computers under their control within a victim network. To escape detection, adversaries frequently try to imitate normal, expected traffic. Depending on the victim's network structure and protections, the adversary can establish command and control in a variety of ways with varying levels of stealth.
Exfiltration	The adversary is attempting to steal information. Exfiltration refers to the methods that intruders can employ to steal data from your network. Adversaries frequently bundle data after collecting it in order to escape discovery while discarding it. Compression and encryption are examples of this. Transferring data out of a target network using their command and control channel or an alternate channel, as well as imposing size constraints on the transmission, are common techniques.
Impact	The adversary is attempting to alter, disrupt or destroy your data and systems. Adversaries utilize impact approaches (like data destruction or manipulation) to interrupt availability or undermine integrity by altering business and operational processes. Business procedures may appear normal on the surface, but they may have been altered to suit the adversaries' objectives. Adversaries may utilize these strategies to achieve their end purpose or to offer cover for a confidentiality breach.

Table B – Examples of indicators of compromise

Indicator of compromise	Description
Unusual outbound network traffic	Anomalies in the network traffic patterns and volumes are one of the most common signs of a security breach. Although keeping intruders out of the network is becoming increasingly difficult, it may be easier to monitor outgoing traffic for potential Indicators of Compromise. When an intruder tries to extract data from the network or when an infected system relays information to a command-and-control server, unusual outbound network traffic may be detected.
Activity from strange geographic areas	If the business is centered in a certain country and there is a user connecting to the network from a different location, it should be investigated. Logs should show an account logging in from multiple IPs in a short time period, particularly when paired with geolocation tagging. More often than not, this is a symptom of an attacker using a compromised set of credentials to log into confidential systems. Monitoring IP addresses on the network and where they come from is an easy way to detect cyber-attacks before they can do real damage to the department.
Unexplained activity by Privileged User Accounts	In complex cyberattacks, such as advanced persistent threats, a common method is to compromise low-privileged user accounts before escalating their privileges and authorizations or exposing the attack vector to accounts with more privileges. When security operators notice suspicious behavior from privileged user accounts, this may be evidence of internal or external attacks on the department's systems and data.

Substantial rise in database read volume	Most of the organizations store their most personal and confidential data in database format. Therefore, the databases will always be a prime target for attackers. A spike in database read volume represents a good indicator that an attacker is trying to infiltrate data.
High authentication failures	In account takeovers, attackers use automation to authenticate using phished credentials. A high rate of authentication attempts might indicate that someone has stolen credentials and is attempting to find an account that gives access to the network.
Lots of requests on important files	An attacker without a high-privileged account is forced to use various methods to find a vulnerability to access files. When the attackers find signs that an exploit might be successful, they often use different permutations to launch it. For instance it is abnormal when a single user or IP is discovered to make a dozen times more requests than normally.
Suspicious configuration changes	Changing configurations on files, servers, and devices could give the attacker a second backdoor to the network. Changes could also add vulnerabilities for malware to exploit.
Indicators of DDoS attacks (Distributed Denial of Service)	DDoS attacks happen when a malicious actor tries to shut down a service by flooding it with traffic and requests from a network of a controlled machine, called a botnet. DDoS attacks are frequently used as smokescreens to camouflage other more harmful attacks. The signs of DDoS are: slow network performance, unavailability of websites, firewall failover, back-end systems working at maximum capacity for unknown reasons.

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.