SILVERFORT

Comply with CCOP Identity Protection Requirements with Silverfort

What is CCOP and what are its Objectives?

The Cybersecurity Code of Practice for Critical Information Infrastructure 2.0 is an enhancement of the first version that was released in 2018 and will **become effective Date 4 July 2023.** This Code is intended to specify the minimum cybersecurity requirements that organizations that operate Critical Information Infrastructure (CII) should implement. This applies to all components of an IT or OT system and/or network infrastructure of a CII and includes physical devices and systems, software platforms and applications of the CII.

What are CCOP Identity Protection Requirements?

Cyber resilience has many aspects that address various attack surfaces. The **identity protection** aspect refers to all types of attacks that involve the compromise of user credentials and using them for either initial access, persistence, or lateral movement. This subset of attacks is often the that can potentially escalate a local security event to a systemic risk, making their mitigation a key necessity.

Silverfort Platform: Gain Full Coverage of CCOP Identity Protection Requirements

Silverfort's platform enables to implement the defense-in-depth, least privileged access, and zero trust principals the CCOP outlines within the following requirements' groups:

Protection requirements

Enforce access controls via MFA protection on all internal and remote administrative access to all resources, from workstations to databases, monitoring all logon sessions for anomalies with specific emphasis on Domain Controllers, and enforcement of least privileged access policies for all users, including service accounts.

Detection requirements

Continuous, automated monitoring of all user accounts' access attempts employing a muti-layered risk engine to detect authentication anomalies, protocol anomalies, and behavioral patterns associated with account takeover and lateral movement, as well as enabling proactive threat hunting based on each user's full authentication trail.

Response and Recovery requirements

Availability of all access logs to all OT, IT and cloud resources, to accelerate and optimize forensic investigations of identity threats, with a single click to view all authentications and access attempts that were made by a compromised account, providing rapid insight into the attack's root cause and identify the machines and users that require remediation.

Compliance Table: Silverfort Alignment to CCOP Requirements

CCOP Requirement	Details	SILVERFORT
5: PROTECTION REQUIREMENTS: Silverfort's protection applies to these requirements directly		
5.2 Account Management	5.2.1 With respect to accounts that have access to the CII, including any user, application, service or system account:	
	(a) Grant to each account only the minimum privileges necessary for its assigned functions and uses;	✓
	(d) Establish mechanisms and processes to monitor the activities of each account, including behavioural patterns, for any anomalies and to trigger an alert for investigation when any anomaly is detected; and	✓
	(e) Delete or disable any account that is no longer necessary or is inactive.	✓
5.3 Privileged Access Management	5.3.1 With respect to privileged accounts, the CIIO shall:	
	(a) Ensure that privileged access (i.e., administrative access) is granted only to selected accounts authorised to have such access;	✓
	(b) Maintain an updated inventory of privileged accounts including details of the permissions and privileges assigned to each account;	✓
	(c) Implement multi-factor authentication where privileged accounts are used to access the CII, and where privileges are to be escalated to the level of privileged access (e.g., where the user seeks to obtain additional permissions on a system or network after an initial log-in); and	✓
	(d) Ensure that privileged access is initiated from a cybersecurity hardened environment and transfer of data	✓
5.4 Domain Controller	5.4.1 The CIIO shall implement mechanisms and processes to:	
	(a) Monitor for changes to the trust relationships established between domains; and	✓
	(b) Identify anomalies in the trust relationships and trigger an alert for investigation when any anomaly is detected.	✓
5.7 Remote Connection	5.7.1 The CIIO shall put in place effective cybersecurity measures for all remote connections to the CII to prevent and detect unauthorised access, and to validate that all such remote connections are authorised.	✓
	5.7.2 The CIIO shall ensure that	
	(a) Remote connections to the CII are disabled except where necessary for operating the CII;	✓
	(b) Multi-factor authentication is required for the establishing a remote connectionto the CII;	✓

CCOP Requirement	Details	SILVERFORT
5.13 Database Security	5.13.1 The CIIO shall ensure that only authorised accounts can connect to and query databases in a CII.	✓
	5.13.3 The CIIO shall establish policies to secure databases in a CII, including policies for:	✓
	(c) Restricting access to sensitive data to authorised persons.	✓
6: DETECTION REQUIREMENTS Silverfort protection applies to the identity aspect of all the following requirements, i.e., authentication logs, identity threats (account takeover, lateral movement, etc.)		
6.1 Logging	6.1.1 The CIIO shall generate, collect and store logs of the following:	
	(a) All access and attempts to access the CII and the activities during such access, including application and database activities, and access to data in the CII;	✓
6.2 Monitoring and Detection	6.2.1 The CIIO shall establish and implement mechanisms and processes for the purposes of: (a) Monitoring and detecting all cybersecurity events in respect of the CII;	
	(a) Monitoring and detecting all cybersecurity events in respect of the CII;	✓
	(b) Collecting and storing records of all such cybersecurity events (including, where available, logs relating to the cybersecurity event);	✓
	(c) Analysing all such cybersecurity events, including correlating between cybersecurity events, and determining whether there is or has been any cybersecurity incident; and	✓
	(d) Triggering applicable incident reporting, response and recovery plans if there is or has been any cybersecurity incident	✓
	6.2.2 For the purposes of monitoring and detecting cybersecurity events, the mechanisms and processes established by the CIIO shall include:	
	(a) Scanning for indicators of compromise (IOCs), including IP addresses, Uniform Resource Locator (URL), domains and hashes;	✓
	(b) Establishing the normal day-to-day operational activities and network traffic in the CII, and using this as a baseline against which the CIIO is to monitor for deviations and anomalous activities; and	✓
	(c) Ensuring that alerts for further investigation are triggered for all deviations and anomalous activities that are detected.	✓
	6.3.1 The CIIO shall conduct threat hunting for the CII to search for and identify cybersecurity threats to the CII at least once every 24 months. The first instance of threat hunting is to be completed no later than 12 months after the Compliance Date.	✓
	6.3.2 The CIIO shall include cybersecurity threats identified from threat hunting in cybersecurity risk assessments to ensure that the risks derived from the threats are assessed, mitigated, and tracked throughout the CII's system development lifecycle.	✓
	6.3.3 The CIIO shall analyse all threats identified from threat hunting to determine if there is or has been any cybersecurity incident in respect of the CII, and shall trigger the applicable incident reporting, response and recovery plans if there is or has been a cybersecurity incident.	✓

CCOP Requirement	**Details**	SILVERFORT
7: RESPONSE AND RECOVERY REQUIREMENTS Silverfort protection applies to the identity aspect of all the following requirements, i.e., authentication logs, identity threats (account takeover, lateral movement, etc.)		
7.1 Incident Management	7.1.3 The CIIO shall establish procedures to reset the Kerberos Ticket Granting Ticket account for CII assets that use the Kerberos authentication protocol for the domain controller, and shall reset the Kerberos Ticket Granting Ticket account in the event that the CII domain controller is compromised.	✓
	7.1.4 The CIIO shall establish and implement processes to identify, investigate and address the root causes that contributed to each cybersecurity incident, including any structural, behavioural, managerial, technical or systemic factors, so as to prevent recurrence of similar incidents. This shall include processes to identify, investigate and address:	
	(a) Gaps in the existing cybersecurity governance structure that may have led to ineffective cybersecurity risk management and oversight efforts;	✓
	(b) Gaps in and failure to comply with policies, standards and procedures which may have contributed to the cybersecurity incident; and	✓
	(c) Gaps in the audit process and the remediation of audit findings which may have contributed to the cybersecurity incident.	✓