transmosis ONE

transmosisONE For

NIST CYBER SECURITY FRAMEWORK

EXECUTIVE SUMMARY

The National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) establishes information security standards and guidelines for critical infrastructure and is in wide use by organizations of all verticals. NIST CSF breaks down cyber resilience to 5 categories: Identify, Protect, Detect, Respond and Recover.

This document details how the transmosisONE platform maps to the various NIST categories and controls. When properly installed and configured, transmosisONE provides both supplemental and direct support across all categories:

Identify

Direct support via vulnerability assessment and risk ranking, as well as supplemental support via log collection, aggregation and contextualization, File Integrity Monitoring and File Activity Monitoring.

Protect

Direct support via attack prevention technologies such as Antivirus, Next-Generation Antivirus, Threat Intelligence and automated prevention for network-based attack.

Detect

Direct support via attack detection technologies such as Endpoint Detection & Response, Network Analytics, User Behavior Analysis and Deception.

Respond

Direct support via local/global remediation actions for infected hosts, compromised user accounts, malicious files/processes and attacker-controlled traffic. These actions can be applied manually or as automated playbooks.

Recover

Supplemental support via log collection and analysis.

NIST CYBER SECURITY FRAMEWORK REQUIREMENTS

Requirement	Testing Requirements	Comments
Asset Management (ID.AM-3, ID.AM-4, ID.AM-6)	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	transmosisONE provides supplemental support for NISTCSF control requirements ID.AM-3, ID.AM-4 and ID.AM-6 by collecting and analyzing all account management, access granting/revoking, and access/authentication logs. transmosisONE correlation rules provide alerting on account authentication failures. transmosisONE investigations provide evidence of authorized/unauthorized network access. transmosisONE creates visibility into all assets in the organization and can divide them into different groups by their respective business profile and customize the security level to align with perceived business risk.
Governance (ID.GV-1, ID.GV-2, ID.GV-3)	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	transmosisONE provides supplemental support for NISTCSF control requirement ID.GV-1, ID.GV-2, and ID.GV-3 by collecting and analyzing all account management and access/authentication logs. transmosisONE correlation rules provide alerting on account authentication failures. transmosisONE investigations, reports, and tails provide evidence of account management activity (account creation, deletion, and modification) and account access/authentication activity to support efforts of enforcing security policies within the organization.

Requirement	Testing Requirements	Comments
Risk Assessment (ID.RA-1)	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	transmosisONE provides direct support for NISTCF control requirements ID RA 1 -6 and supplemental support for NISTCSF control requirements ID.RA-1. transmosisONE provides full vulnerability assessment and risk ranking along with assigning risk rank to all entities within the environment. transmosisONE identifies all entities (hosts, files, user accounts, network traffic and destinations) that introduce a likely threat to the environment. transmosisONE provides supplemental support for NISTCSF control requirements ID.RA-1 by collecting and analyzing all suspicious network activity or activities indicative of cybersecurity risks. transmosisONE correlation rules provide alerting on events indicative of potential cybersecurity threats or attacks on the network. transmosisONE investigations, reports, and tails provide evidence of cybersecurity events in support of early detection and incident response.
Access Control (PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, PR.AC-5)	Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	transmosisONE provides supplemental support for NIST-CSF control requirements PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, PR.AC-5 by collecting and analyzing all account management, and network access/authentication logs. transmosisONE correlation rules provide alerting on account authentication failures. transmosisONE User Behavior Analytics profiles user activity and alerts upon anomalies that are indicative of malicious presence. transmosisONE investigations, reports, and tails provide evidence of account access/authentication activity.
Awareness and Training (PR.AT-3)	The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	transmosisONE provides supplemental support for NIST-CSF control requirement PR.AT-3 by collecting and analyzing all third-party accounts or process activities within the environment to ensure third-parties are performing activities according to defined roles and responsibilities. transmosisONE correlation rules provide alerting on account authentication failures. transmosisONE investigations and reports provide evidence of vendor account management and authentication (success/failure) activities.

Requirement	Testing Requirements	Comments
Data Security (PR.DS-1, PR.DS-4, PR.DS-5, PR.DS-6)	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	transmosisONE provides direct support for NIST-CSF control requirements PR.DS-1 and supplemental support for NIST-CSF control requirements PR.DS-4, PR.DS-5, PR.DS-6 by collecting and analyzing all system logs relating to the protection of data integrity, availability, and mobility. transmosisONE's File Integrity Monitor (FIM) tracks file changes, while transmosisONE File Activity Monitoring monitors all creation, deletion, access and modifications. transmosisONE correlation rules provide alerting on remote account authentication failures. transmosisONE's investigations, reports, and tails provide evidence of remote account access/ authentication activity.
Information Protection Processes and Procedures (PR.IP-1, PR.IP-3, PR.IP-4, PR.IP-7, PR.IP-8, PR.IP-11, PR.IP-12)	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	transmosisONE provides supplemental support for NIST-CSF control requirements PR.IP-1, PR.IP-3, PR.IP-4, PR.IP-7, PR.IP-8, PR.IP-11, PR.IP-12 by collecting and analyzing all transmosisONE correlation rules provide alerting on account management activities. transmosisONE investigations, reports, and tails provide evidence of account management and authentication (success/failure) activities.
Maintenance (PR.MA-1)	Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	transmosisONE provides supplemental support for NIST-CSF control requirement PR.MA-1 by collecting and analyzing all logs from HMI, engineering work-stations and servers. transmosisONE correlation rules provide alerting on critical and error conditions within the environment. transmosisONE investigations, reports and tails provide evidence of environment conditions as well as process and system start-ups/shut-downs.

Requirement	Testing Requirements	Comments
Protective Technology (PR.PT-1, PR.PT-2, PR.PT-3, PR.PT-4)	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	transmosisONE provides supplemental support for NIST-CSF control requirement PR.PT-1, PR.PT-2, PR.PT-3, PR.PT-4 by collecting logs relating to technical security solution access management and authentication activities. transmosisONE correlation rules provide alerting on audit logging events (log cleared, stopped), FIM, software installations, access provisioning and authentication activities. transmosisONE deploys its own AV/NGAV to proactively protect against execution of malware, exploits, fileless and other malicious processes. Lastly, transmosisONE investigations, reports and tails provide evidence around the aforementioned activities.
Anomalies and Events (DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5)	Anomalous activity is detected in a timely manner and the potential impact of events is understood.	transmosisONE provides direct support of NIST-CSF control requirements DE.AE-3 and DE.AE-5, while providing supplemental support for NIST-CSF control requirement DE.AE-1, DE.AE-2, DE.AE-4 by collecting and analyzing logs related to security events throughout the environment. An inherent function to transmosisONE is the ability to correlate and aggregate event data across the environment. transmosisONE monitors user activity, network traffic and process behavior and employs various technologies to detect and alert upon any anomalies, indicative of malicious activity and presence. transmosisONE includes Deception technology which plants decoys across the environment and alerts upon malicious interaction.
Security Continuous Monitoring (DE.CM-5, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.CM-8)	The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	transmosisONE provides direct support of NIST-CSF control requirements DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, and DE.CM-7 as well as supplemental support for NIST-CSF control requirements DE.CM-4, DE.CM-4 AND DE.CM-4 by providing continuous monitoring, analysis, and reporting of network, physical access and other events indicative of malicious cyber activities.

Requirement	Testing Requirements	Comments
Detection Processes (DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5)	Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	transmosisONE provides direct support of NIST-CSF control requirement DE.DP-4 and supplemental support of NIST-CSF control requirement DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-5 by logging and monitoring around process and procedures in the environment. Further, transmosisONE correlation engine provides alerting on activities to assigned individuals. transmosisONE reporting, investigations and tails provide evidence around these activities as well as support maintenance of processes and procedures.
Response Planning (RS.RP-1)	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	transmosisONE provides supplemental support for NIST-CSF control requirement RS.RP-1 by collecting and analyzing all cybersecurity events from transmosisONE attack protection technologies: AV, NGAV, EDR, UBA, Network Analytics and Deception, and providing notifications to assigned personnel. transmosisONE correlation rules provide alerting on cybersecurity events while investigations, reports, and tails provide evidence behind cybersecurity events. transmosisONE provides a wide set of remediation actions to eliminate attackers' presence and activity from infected hosts, malicious processes, compromised user accounts and attacker-controlled traffic. Additionally, transmosisONE supports creation of a response playbook that automates the triggering of a set of remediation actions per malicious activity in respect to the organization's policies and procedures.

Requirement	Testing Requirements	Comments
Communications (RS.CO-3, RS.CO-4)	Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	transmosisONE provides supplemental support for NIST-CSF control requirement RS.CO-3 and RS.CO-4 by collecting and analyzing all cybersecurity events from transmosisONE attack protection technologies: AV, NGAV, EDR, UBA, Network Analytics and Deception, and providing notifications to assigned personnel. transmosisONE correlation rules provide alerting on cybersecurity events while investigations, reports, and tails provide evidence behind cybersecurity events. transmosisONE supports creation of a response playbook that automates the triggering of a set of remediation actions per malicious activity in respect to the organization's policies and procedures. transmosisONE supports creation of various reports in respect to the organization's policies and procedures.
Analysis (RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4)	Analysis is conducted to ensure adequate response and support recovery activities.	transmosisONE provides supplemental support for NIST-CSF control requirements RS.AN-1, RS.AN-2, RS.AN-3 and RS.AN-4 by collecting and analyzing logs to categorize events and allow for forensics to be performed. transmosisONE correlation engine provides alerts and notifications to assigned personnel. transmosisONE investigations, reports, and tails provide evidence of security and other events of interest throughout the environment. transmosisONE provides a wide set of remediation actions to eliminate attackers' presence and activity from infected hosts, malicious processes, compromised user accounts and attacker-controlled traffic. Additionally, transmosisONE supports creation of a response playbook that automates the triggering of a set of remediation actions per malicious activity in respect to the organization's policies and procedures.

Requirement	Testing Requirements	Comments
Analysis (RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4)	Analysis is conducted to ensure adequate response and support recovery activities.	transmosisONE provides supplemental support for NIST-CSF control requirements RS.AN-1, RS.AN-2, RS.AN-3 and RS.AN-4 by collecting and analyzing logs to categorize events and allow for forensics to be performed. transmosisONE correlation engine provides alerts and notifications to assigned personnel. transmosisONE investigations, reports, and tails provide evidence of security and other events of interest throughout the environment. transmosisONE provides a wide set of remediation actions to eliminate attackers' presence and activity from infected hosts, malicious processes, compromised user accounts and attacker-controlled traffic. Additionally, transmosisONE supports creation of a response playbook that automates the triggering of a set of remediation actions per malicious activity in respect to the organization's policies and procedures.
Mitigation (RS.MI-1, RS.MI-2, RS.MI-3)	Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	transmosisONE provides direct support for NISTCSF control requirements RS.MI-1, RS.MI-2, RS.MI-3 by three types of mitigation actions: 1. **Preset remediations:** direct removal of malicious activity and presence across infected hosts, compromised user accounts, malicious files/processes and attacker-controlled traffic. 2. **Custom remediations:** user defined remediation which optionally chain together several preset remediations, and/or join a custom script that communicates with other environment components such as AD, firewall, proxy, etc. to expand the mitigation across the entire environment. 3. **Automated playbooks:** selecting a group of preset/custom remediations and set them to get triggered automatically per a chosen malicious activity. Additionally transmosisONE provides collecting and analyzing logs related to incident response. transmosisONE correlation engine provides alerting on vulnerabilities within the environment. transmosisONE investigations, reports and tails provide evidence to support incident analysis and remediation of exposure or vulnerabilities.

Requirement	Testing Requirements	Comments
Mitigation (RS.MI-1, RS.MI-2, RS.MI-3)	Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	transmosisONE provides a wide set of remediation actions to eliminate attackers' presence and activity from infected hosts, malicious processes, compromised user accounts and attacker-controlled traffic. Additionally, transmosisONE supports creation of a response playbook that automates the triggering of a set of remediation actions per malicious activity in respect to the organization's policies and procedures.
Improvements (RS.IM-1, RS.IM-2)	Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	transmosisONE provides supplemental support for NISTCSF control requirements RS.IM-1, RS.IM-2 by collecting and analyzing logs related to incident response. transmosisONE reports provide evidence to support incident analysis and remediation of exposure or vulnerabilities.
Improvements (RC.IM-1, RC.IM-2)	Recovery planning and processes are improved by incorporating lessons learned into future activities.	transmosisONE provides supplemental support of NIST-CSF control requirements RC.IM-1 and RC.IM-2 by collecting and analyzing logs relating to recovery operations. transmosisONE reports provide evidence around the recovery operation events.
Communications (RC.CO-3)	Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	transmosisONE provides supplemental support of NISTCSF control requirement RC.CO-3 by collecting and analyzing logs relating to recovery operations. transmosisONE reports provide evidence around the recovery operation events.