SCOPE Framework: Network & Security Architecture Control Domain

Table of Contents

Originating Component	SCOPE Framework Governance Committee
Releasability	Cleared for public distribution. Available in the SCOPE Framework Hub at [https://timtiptonjr.com/scope-hub].

Purpose: The Network Security & Architecture domain defines the structural and technical blueprint for securing enterprise network environments across traditional, cloud, hybrid, and software-defined infrastructures. This domain ensures the confidentiality, integrity, and availability of data in motion by enforcing controls around network segmentation, perimeter defenses, trust modeling, protocol governance, and adaptive access enforcement. By architecting resilient, compartmentalized, and policy-driven network layers, the organization reduces attack surfaces, impedes lateral movement, and enables dynamic response to emerging threats—ultimately fortifying the enterprise against both internal compromise and external adversaries.

Section 1. Zero Trust Architecture (ZTA)

Zero Trust Architecture (ZTA) redefines traditional perimeter-based security models by adopting a “never trust, always verify” posture across identity, devices, networks, applications, and data. This control family establishes the foundational principles, mechanisms, and governance required to design, implement, and sustain a Zero Trust Architecture that supports adaptive access decisions, minimizes lateral movement, and enforces continuous verification of trust.

1.1 ZTA-01: Define and Document a Zero Trust Strategy

Organizations shall develop and maintain a formal Zero Trust Architecture (ZTA) strategy that aligns with enterprise security objectives, business priorities, and threat landscape, including a phased implementation roadmap and governance structure.

1.2 ZTA-02: Establish Trust Zones and Segmentation Boundaries

Trust zones shall be defined and enforced to separate network segments, workloads, or user groups based on sensitivity, criticality, and trust requirements, with clearly documented rules governing allowed inter-zone communications.

1.3 ZTA-03: Implement Context-Aware Access Policies

Access decisions shall incorporate contextual attributes such as device posture, user role, geolocation, and behavioral baselines to dynamically determine access permissions.

1.4 ZTA-04: Enforce Continuous Authentication and Authorization

All users, devices, and services shall undergo continuous authentication and authorization checks throughout a session, not solely at the initial point of access.

1.5 ZTA-05: Require Device Posture Assessment Prior to Access

Access to enterprise resources shall be restricted to devices that meet predefined security posture baselines (e.g., patch level, endpoint protection status), with real-time posture validation integrated into access control flows.

1.6 ZTA-06: Centralize Policy Decision and Enforcement Points (PDP/PEP)

Organizations shall architect their ZTA to include centralized Policy Decision Points (PDPs) and distributed Policy Enforcement Points (PEPs) to ensure scalable, consistent access control.

1.7 ZTA-07: Implement Resource-Based Access Control

Each enterprise resource (e.g., application, database, service) shall have granular, identity-aware access policies enforced directly at the resource layer, independent of the network perimeter.

1.8 ZTA-08: Enable East-West Traffic Visibility

Mechanisms shall be deployed to monitor and analyze East-West (internal) traffic to detect anomalous behaviors, lateral movement attempts, and policy violations within segmented zones.

1.9 ZTA-09: Ensure Identity Binding to Sessions and Transactions

All sessions and transactions shall be cryptographically or logically bound to the initiating identity to ensure traceability and prevent session hijacking.

1.10 ZTA-10: Integrate Telemetry for Trust Evaluation

Continuous telemetry from endpoints, user activity, network traffic, and security tools shall feed into trust algorithms to dynamically adjust access decisions and risk scoring.

1.11 ZTA-11: Apply Just-In-Time (JIT) Access Principles

Access to sensitive resources shall be provisioned using just-in-time (JIT) models to reduce standing privileges and limit exposure windows.

1.12 ZTA-12: Enforce Least Privilege at All Layers

Zero Trust implementations shall enforce the principle of least privilege across user, service, network, and data layers, ensuring entities only access the minimum necessary resources.

1.13 ZTA-13: Support ZTA Through Secure Software-Defined Perimeters

ZTA architectures shall leverage software-defined perimeter (SDP) technologies to obfuscate resource locations and only reveal them upon successful authentication and authorization.

1.14 ZTA-14: Automate Policy Updates Based on Risk Indicators

Access policies shall be dynamically adjusted through automation based on threat intelligence, risk indicators, and environmental changes (e.g., CVE publication, breach reports).

1.15 ZTA-15: Implement Continuous Trust Validation for Devices and Services

Trust assigned to devices, services, and identities shall decay over time and require periodic revalidation based on activity, security posture, and policy compliance.

1.16 ZTA-16: Establish Governance for ZTA Roles and Responsibilities

Roles and responsibilities for Zero Trust implementation, maintenance, and oversight shall be clearly defined, including cross-functional collaboration between security, IT, and business units.

1.17 ZTA-17: Conduct Regular Zero Trust Readiness Assessments

Organizations shall perform periodic assessments of their Zero Trust maturity and readiness using defined benchmarks, frameworks, or third-party evaluations.

1.18 ZTA-18: Monitor for Policy Drift and Configuration Deviations

Controls shall be in place to detect, alert, and remediate deviations from defined ZTA policies or configurations that could undermine trust boundaries or enforcement.

1.19 ZTA-19: Integrate Zero Trust with Cloud and Hybrid Environments

ZTA policies and enforcement mechanisms shall extend consistently across on-premise, cloud, and hybrid environments, accounting for different trust models and control capabilities.

1.20 ZTA-20: Maintain an Inventory of Trust Relationships

Organizations shall maintain an up-to-date inventory of all trust relationships across systems, services, and users, including documented rationale, risk level, and expiration criteria.

1.21 ZTA-21: Validate Third-Party Compliance with Zero Trust Principles

Third-party integrations shall be reviewed to ensure compatibility with ZTA principles, including identity federation, segmentation enforcement, and contextual access control.

1.22 ZTA-22: Conduct Simulated Breach Scenarios to Test ZTA Resilience

Regular simulated breach and lateral movement exercises shall be conducted to test the effectiveness of ZTA segmentation, detection, and trust revalidation mechanisms.

Section 2. Micro-Segmentation & Network Access Control (MSN)

Micro-Segmentation and Network Access Control (NAC) form the enforcement backbone of east-west traffic restrictions, dynamic network trust zones, and host-to-host isolation. While Zero Trust defines the strategic model, this control family addresses the technical and operational enforcement of that model through fine-grained segmentation, real-time access decisions, and adaptive network controls. These controls ensure containment, limit lateral movement, and maintain network integrity based on identity, context, and behavioral baselines.

2.1 MSN-01: Define Logical Segmentation Boundaries at the Network Layer

Organizations shall document and implement logical segmentation boundaries that separate users, devices, and workloads based on sensitivity, function, or risk level, using VLANs, VRFs, or overlay networks.

2.2 MSN-02: Enforce Host-Level Micro-Segmentation

Host-based firewalls or agent-based enforcement mechanisms shall be deployed to enable micro-segmentation directly at the workload or endpoint level, enforcing process-to-process or application-level communication controls.

2.3 MSN-03: Implement Policy-Driven NAC Enforcement

Network Access Control policies shall be enforced dynamically based on user role, device posture, location, and time of access, leveraging 802.1X, MACsec, or software-defined enforcement technologies.

2.4 MSN-04: Tag and Classify Network Assets for Segmentation Alignment

All network-connected assets shall be tagged and classified by function, criticality, and ownership to support dynamic segmentation policies and enforcement logic.

2.5 MSN-05: Monitor and Alert on Segmentation Violations

Systems shall generate real-time alerts and logs when unauthorized or anomalous traffic attempts to traverse defined segmentation or access boundaries.

2.6 MSN-06: Restrict East-West Traffic Using Granular ACLs

East-west network traffic shall be restricted using Access Control Lists (ACLs) or software-defined rules, ensuring only approved communications are allowed between trust zones or network segments.

2.7 MSN-07: Apply Network Segmentation to Third-Party Connections

Third-party access (e.g., contractors, partners, MSPs) shall be isolated into dedicated segments with strictly limited and monitored access paths, independent of internal network resources.

2.8 MSN-08: Enforce NAC on Wireless and Remote Connections

Wireless and remote endpoints shall be subject to NAC policies equivalent in rigor to wired access points, using VPN-based or agent-based posture verification.

2.9 MSN-09: Integrate NAC with Endpoint Detection Systems

NAC solutions shall be integrated with endpoint protection platforms (e.g., EDR, antivirus) to factor real-time endpoint health into access control decisions.

2.10 MSN-10: Utilize Software-Defined Network (SDN) Controls for Segmentation

SDN or controller-based solutions shall be used to create dynamic, policy-driven segmentation that can adapt to changes in environment, threat level, or business context.

2.11 MSN-11: Implement Time-Bound Access for Network Connections

Temporary access to sensitive network segments shall be automatically revoked after a defined time interval or activity completion to reduce persistent exposure.

2.12 MSN-12: Quarantine Non-Compliant or Infected Devices Automatically

Devices that fail posture assessment or exhibit indicators of compromise shall be dynamically quarantined or redirected to remediation zones via NAC or SDN controls.

2.13 MSN-13: Enforce Network Access Controls Across Data Center Fabrics

Segmentation policies and enforcement shall extend uniformly across physical and virtual data center fabrics, including container networking and hypervisor-level segmentation.

2.14 MSN-14: Maintain a Dynamic Map of Authorized Communication Paths

Organizations shall maintain and regularly update a visual or logical map of authorized communication flows between network zones and segments to support enforcement and auditability.

2.15 MSN-15: Use Identity-Based Network Access Policies

NAC policies shall be tied to identity attributes (e.g., AD group, role, department) rather than static IPs or MAC addresses to support flexibility and alignment with IAM governance.

2.16 MSN-16: Restrict Lateral Movement Within User Access Segments

Even within the same user segment or VLAN, controls shall prevent or restrict lateral movement (e.g., user-to-user traffic) unless explicitly authorized.

2.17 MSN-17: Require Segmentation Reviews During System Changes

Any system, application, or infrastructure change that affects network connectivity shall require a segmentation impact analysis and validation of compliance with segmentation policy.

2.18 MSN-18: Log All Network Access Control Decisions

All access control decisions made by NAC systems (e.g., allow, deny, quarantine) shall be logged with metadata to support forensic analysis and access reviews.

2.19 MSN-19: Perform Periodic NAC and Segmentation Testing

Organizations shall conduct periodic validation and penetration testing of NAC enforcement and segmentation policies to identify bypass methods or misconfigurations.

2.20 MSN-20: Maintain an Exception Process for Segmentation Controls

A formalized, time-limited exception process shall exist for segmentation and access control requests that require deviations from defined policies, with full audit trails and approval workflows.

2.21 MSN-21: Align Segmentation Enforcement with Data Sensitivity Zones

Segmentation shall correlate directly with data classification, ensuring that sensitive or regulated data resides within restricted zones with enforced access boundaries.

Section 3. Firewalls & Intrusion Detection/Prevention Systems (IDS/IPS) (IPS)

Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) form a critical part of an organization's perimeter and internal defense infrastructure. This control family focuses on the detection, prevention, and control of unauthorized or anomalous traffic at ingress, egress, and internal chokepoints. These controls ensure consistent enforcement of security policy, visibility into network-layer threats, and rapid mitigation of known and emerging attack vectors without duplicating broader segmentation or monitoring responsibilities assigned elsewhere.

3.1 IPS-01: Deploy Layered Firewalls Across Network Tiers

Organizations shall implement firewalls at all critical network junctures—including perimeter, DMZ, internal zones, and cloud gateways—ensuring layered traffic inspection and policy enforcement.

3.2 IPS-02: Maintain a Rule Review and Optimization Process

A documented process shall be in place to periodically review, validate, and optimize firewall and IPS rule sets, removing obsolete, overly permissive, or unused rules.

3.3 IPS-03: Enforce Default-Deny Policies on All Firewalls

All firewalls shall operate on a "default deny" basis, explicitly permitting only known, necessary, and authorized traffic, with all other traffic denied by default.

3.4 IPS-04: Deploy IDS/IPS Capabilities at High-Risk Network Points

Intrusion Detection and/or Prevention Systems shall be deployed at points where critical systems reside, where traffic enters/exits the network, or where sensitive data is processed.

3.5 IPS-05: Enable Deep Packet Inspection (DPI) Where Feasible

Where system performance permits, IDS/IPS systems shall be configured for deep packet inspection to identify application-layer threats and evasive attack techniques.

3.6 IPS-06: Integrate Threat Intelligence into IPS Signatures

Organizations shall configure IPS devices to ingest and apply external and internal threat intelligence feeds for timely detection of known attack indicators.

3.7 IPS-07: Segregate Management Interfaces for Security Appliances

Firewall and IDS/IPS management interfaces shall be logically or physically isolated from production networks and accessible only through secured administrative zones.

3.8 IPS-08: Alert on and Block Known Malicious Payloads

IPS configurations shall include signature-based and behavior-based mechanisms to detect and block known malicious payloads, including exploits, malware, and command-and-control traffic.

3.9 IPS-09: Use Firewall Zones and Interfaces to Enforce Policy

Firewall interfaces shall be logically segmented into distinct security zones (e.g., internal, external, DMZ) with policies uniquely defined for each zone-to-zone interaction.

3.10 IPS-10: Log All Allowed and Denied Connections

Firewalls and IDS/IPS systems shall log all allowed and denied connection attempts with full metadata, enabling detailed event reconstruction and forensic analysis.

3.11 IPS-11: Implement Egress Filtering for Data Exfiltration Prevention

Outbound traffic from enterprise networks shall be filtered through firewalls to restrict unauthorized destinations, prevent tunneling, and detect exfiltration attempts.

3.12 IPS-12: Maintain Real-Time IDS/IPS Signature Updates

All IDS/IPS platforms shall be configured to automatically download and apply the latest vendor and community-driven signature updates on a scheduled or real-time basis.

3.13 IPS-13: Test IPS Policies in Detection Mode Prior to Prevention

New or updated IPS policies shall be tested in detection mode to assess potential impact on legitimate traffic before enabling blocking or prevention actions.

3.14 IPS-14: Enable Geo-IP Filtering Where Applicable

Organizations shall use firewall capabilities to enforce geo-IP restrictions, blocking or monitoring traffic from regions with no business necessity or elevated threat risk.

3.15 IPS-15: Use Application-Layer Gateways (ALGs) for Specific Protocols

For protocols that require inspection beyond layer 4 (e.g., SIP, FTP), firewalls shall use application-layer gateways or equivalent mechanisms to manage dynamic port behavior securely.

3.16 IPS-16: Restrict Administrative Access by Source IP and Method

Access to firewall and IDS/IPS management consoles shall be limited by source IP, protocol, and method (e.g., SSH with MFA only from jump hosts) to reduce attack surface.

3.17 IPS-17: Conduct Rule Impact Simulations Before Deployment

Firewall rule changes shall undergo simulation or staging to validate expected behavior, avoid unintentional service disruption, and identify conflict with existing rules.

3.18 IPS-18: Tune IDS/IPS for Environment-Specific Noise Reduction

IDS/IPS systems shall be tuned regularly to suppress benign or expected alerts (false positives) based on contextual awareness of the organization's systems and applications.

3.19 IPS-19: Monitor Encrypted Traffic at Ingress and Egress Points

Where feasible, encrypted traffic shall be decrypted and inspected at firewall or proxy layers to detect threats otherwise hidden from IDS/IPS visibility.

3.20 IPS-20: Document All Approved Services and Ports Per Zone

All allowed ports, protocols, and services for each security zone shall be documented, reviewed quarterly, and aligned with business and security requirements.

3.21 IPS-21: Establish Firewall Rule Lifecycle Management Procedures

Firewall rules shall include metadata such as owner, purpose, expiration date, and review schedule to enforce governance and prevent rule sprawl.

3.22 IPS-22: Integrate IDS/IPS Alerts with Centralized SIEM

All IDS/IPS alerts shall be forwarded to a centralized security information and event management (SIEM) platform with appropriate tagging for correlation and incident triage.

Section 4. Software-Defined Networking Security (SDN)

Software-Defined Networking (SDN) enables centralized control over network traffic flows, abstracting hardware control planes to enhance agility and automation. However, SDN also introduces novel security challenges such as controller compromise, insecure APIs, and lateral policy misconfigurations. This control family addresses the unique security requirements for protecting SDN architectures, including controller security, flow rule integrity, orchestration layer protections, and tenant isolation in dynamic, programmable network environments.

4.1 SDN-01: Secure the SDN Controller as a High-Value Asset

The SDN controller shall be treated as a mission-critical asset, with hardened configurations, access controls, and monitoring mechanisms to detect compromise or unauthorized modifications.

4.2 SDN-02: Enforce Mutual Authentication Between Controller and Switches

All communications between SDN controllers and data plane devices (e.g., switches, routers) shall be mutually authenticated using certificates or cryptographic keys.

4.3 SDN-03: Isolate SDN Control Traffic from Production Networks

Control plane communications between the SDN controller and network devices shall be logically or physically isolated from data plane and management plane traffic.

4.4 SDN-04: Implement RBAC for Controller API Access

Role-Based Access Control shall be enforced on all northbound and southbound controller APIs, limiting access based on user roles, job function, and administrative scope.

4.5 SDN-05: Monitor for Unauthorized Flow Rule Injection

Mechanisms shall be in place to detect and alert on unauthorized or anomalous flow rule insertions or deletions within the SDN environment.

4.6 SDN-06: Encrypt Controller-to-Application and Controller-to-Device Communications

All API and messaging communications between the controller and applications (northbound) and between controller and switches (southbound) shall be encrypted using TLS or equivalent protocols.

4.7 SDN-07: Apply Policy Validation Before Flow Rule Deployment

All flow rules shall be validated against defined network security policies before being pushed to data plane devices to prevent rule conflicts or unauthorized access paths.

4.8 SDN-08: Log All Controller API Interactions

Comprehensive logging shall be enabled for all interactions with the SDN controller's APIs, including configuration changes, authentication attempts, and flow deployments.

4.9 SDN-09: Implement High Availability for SDN Controllers

Redundant controller nodes shall be deployed to ensure failover capability, eliminate single points of failure, and protect against availability-based attacks.

4.10 SDN-10: Segregate Tenants in Multi-Tenant SDN Environments

Multi-tenant SDN deployments shall enforce strict logical isolation between tenants at both the orchestration and data plane levels to prevent unauthorized access or leakage.

4.11 SDN-11: Validate Controller Software Integrity

All controller software images and updates shall be verified via cryptographic hash or signature validation to prevent installation of tampered or malicious code.

4.12 SDN-12: Define and Enforce Flow Timeout Policies

Flow rules shall have defined timeout periods and automatic expiry parameters to reduce stale rule accumulation and eliminate unauthorized persistent paths.

4.13 SDN-13: Limit Controller Exposure to Management Interfaces

Controller management interfaces shall be restricted to secure administrative zones and accessible only through hardened jump servers or bastion hosts.

4.14 SDN-14: Conduct Static and Dynamic Analysis of Controller Code

Where custom or open-source controllers are used, both static and dynamic application security testing shall be conducted to identify vulnerabilities prior to deployment.

4.15 SDN-15: Implement Application Whitelisting for Controller Extensions

Only approved, signed, and vetted applications or plug-ins shall be allowed to interact with the SDN controller to prevent introduction of malicious or unvetted code.

4.16 SDN-16: Integrate Flow Policy Auditing Mechanisms

Organizations shall deploy tools or processes that audit active flow rules across the network and identify deviations from the intended security posture.

4.17 SDN-17: Detect and Alert on Lateral Movement Within the Control Plane

Anomaly detection systems shall monitor the SDN control plane for signs of lateral movement, controller compromise, or suspicious propagation of flow instructions.

4.18 SDN-18: Separate Development and Production SDN Controllers

SDN environments shall maintain a strict separation between development, test, and production controllers to prevent configuration bleed-over or unauthorized deployments.

4.19 SDN-19: Perform Real-Time Flow Visualization and Mapping

Real-time flow visualization tools shall be implemented to map, monitor, and validate the actual traffic paths created by SDN controllers against intended policies.

4.20 SDN-20: Enforce Northbound API Rate Limiting and Throttling

Rate limiting and throttling shall be enforced on SDN controller northbound APIs to prevent abuse or denial-of-service scenarios from orchestration or automation layers.

4.21 SDN-21: Conduct Periodic SDN Configuration Drift Assessments

Regular assessments shall be conducted to detect and correct configuration drift across SDN controllers, flow rules, and network device states to maintain integrity and compliance.

4.22 SDN-22: Harden and Patch All SDN Components Regularly

All components within the SDN ecosystem—including controllers, orchestration platforms, and virtual switches—shall be regularly patched, hardened, and monitored for known vulnerabilities.

Section 5. Cloud & Hybrid Environment Security (CHE)

Cloud and hybrid environments introduce dynamic, distributed architectures where traditional perimeter-based controls no longer suffice. This control family establishes safeguards tailored to public, private, and hybrid cloud infrastructures, emphasizing security posture visibility, interconnect governance, and secure orchestration across cloud-native services, virtualization layers, and on-prem integration points. These controls ensure that cloud usage aligns with organizational security requirements without duplicating zero trust, SDN, or segmentation-specific controls defined elsewhere.

5.1 CHE-01: Define a Cloud & Hybrid Security Governance Framework

Organizations shall establish a governance model for cloud and hybrid environments, including defined roles, responsibilities, and accountability for infrastructure, platform, and software layers.

5.2 CHE-02: Establish Approved Cloud Service Provider (CSP) Usage Criteria

Formalized evaluation criteria shall be defined to assess and approve cloud service providers (CSPs), including security certifications, compliance posture, data residency, and shared responsibility model clarity.

5.3 CHE-03: Require Explicit Security Architecture for Hybrid Connectivity

All hybrid cloud connections (e.g., VPNs, Direct Connect, ExpressRoute) shall be designed with layered security controls including encryption, segmentation, and monitoring at ingress/egress points.

5.4 CHE-04: Enforce Least Privilege Across Cloud Console and APIs

Administrative access to cloud management consoles and APIs shall be tightly controlled using least privilege principles, identity-bound access, and scoped permissions.

5.5 CHE-05: Maintain Cloud-Specific Asset and Resource Inventory

Organizations shall maintain a continuously updated inventory of all cloud assets, including instances, services, containers, and APIs, enriched with metadata for classification and risk.

5.6 CHE-06: Isolate Production, Development, and Test Cloud Environments

Cloud environments for development, staging, and production shall be isolated at the account, subscription, or project level to reduce risk of cross-environment access or misconfiguration.

5.7 CHE-07: Require Security Baselines for Cloud Resources

All cloud resources (e.g., VMs, containers, databases, storage) shall adhere to organization-approved security baselines for hardening, access, and monitoring prior to deployment.

5.8 CHE-08: Configure Cloud-Native Network Controls

Cloud-native firewalls, security groups, and route tables shall be configured to restrict access to resources based on source, destination, protocol, and application-layer context.

5.9 CHE-09: Monitor for Misconfigurations Across Cloud Accounts

Automated tools shall be deployed to continuously scan for and alert on misconfigurations such as open storage buckets, overly permissive IAM roles, or exposed management interfaces.

5.10 CHE-10: Enforce Secure Defaults for Cloud Resource Provisioning

Infrastructure-as-Code (IaC) templates and cloud blueprints shall enforce secure defaults for encryption, logging, access control, and resource lifecycle management.

5.11 CHE-11: Control Inter-Region and Inter-Cloud Communications

Traffic between cloud regions or across multiple cloud service providers shall be governed by explicit policies, with inspection and logging at all interconnect points.

5.12 CHE-12: Restrict Use of Root and Break-Glass Cloud Accounts

Use of root, global admin, or break-glass accounts shall be tightly controlled, logged, and limited to emergency use with multi-factor authentication and post-use review.

5.13 CHE-13: Ensure Encryption of Data-in-Transit and Data-at-Rest by Default

All cloud-hosted data shall be encrypted both in transit and at rest using CSP-native encryption services or customer-managed keys, with default enforcement across services.

5.14 CHE-14: Validate Cloud Service Configurations Before Deployment

Configuration validation shall be performed on all cloud service deployments (e.g., via policy-as-code or automated checks) to detect security violations or noncompliance.

5.15 CHE-15: Limit Cloud Service Exposure to Public Internet

Cloud services shall not be directly exposed to the public internet unless explicitly required, in which case compensating controls (e.g., WAF, access control lists) must be implemented.

5.16 CHE-16: Require Logging of All Cloud Administrative Activities

All administrative actions taken via cloud consoles, CLIs, or APIs shall be logged in a centralized and tamper-evident manner, with retention aligned to legal and regulatory requirements.

5.17 CHE-17: Use Secure Workload Identities for Service Interactions

Workloads interacting with cloud services shall use managed identities, service accounts, or workload identity federation mechanisms rather than static credentials or keys.

5.18 CHE-18: Perform Cloud-Specific Threat Modeling

Threat models tailored to cloud-native attack vectors (e.g., container escape, metadata service abuse, IAM misconfigurations) shall be developed and regularly reviewed.

5.19 CHE-19: Monitor Cloud Provider Security Bulletins and Advisories

Organizations shall continuously monitor CSP security advisories and implement patches or configuration changes based on published threats or vulnerabilities in cloud services.

5.20 CHE-20: Validate Tenant and Container Isolation in Shared Environments

In multi-tenant cloud or containerized architectures, controls shall be in place to enforce tenant isolation and prevent cross-tenant data access or resource interference.

5.21 CHE-21: Apply Governance Controls to Cloud Marketplace and SaaS Integrations

All third-party services or integrations procured via cloud marketplaces or external SaaS providers shall undergo security assessment and approval prior to use.

5.22 CHE-22: Enforce Cloud Resource Lifecycle Policies

Cloud resource provisioning, usage, and decommissioning shall follow documented lifecycle policies, including tagging, expiration dates, and post-termination data sanitization.