MYTHOS-GUIDE-NETSEC-0002

Network And Security Engineering Library Guide

Integrated engineering guide connecting the relevant Mythos standards, implementation patterns, operating procedures, architecture decisions, evidence expectations, and maturity path for network and security engineering library.

38	12	2026-09-17
CORE STANDARDS	RELATED ARCHITECTURES	BASELINE

CANDIDATE ENGINEERING GUIDE

Mythos Systems | Permanent ID | 17 September 2026

PERMANENT PUBLICATION IDENTITY

Network And Security Engineering Library Guide

MYTHOS-GUIDE-NETSEC-0002 / Engineering Guide

Field	Value
Document ID	MYTHOS-GUIDE-NETSEC-0002
Publication class	Engineering Guide
Status	Candidate Engineering Guide
Release date	2026-09-17
Canonical route	/library/guides/mythos-guide-netsec-0002/
Refresh cadence	180 days
Public identity	Permanent ID; production workflow metadata excluded

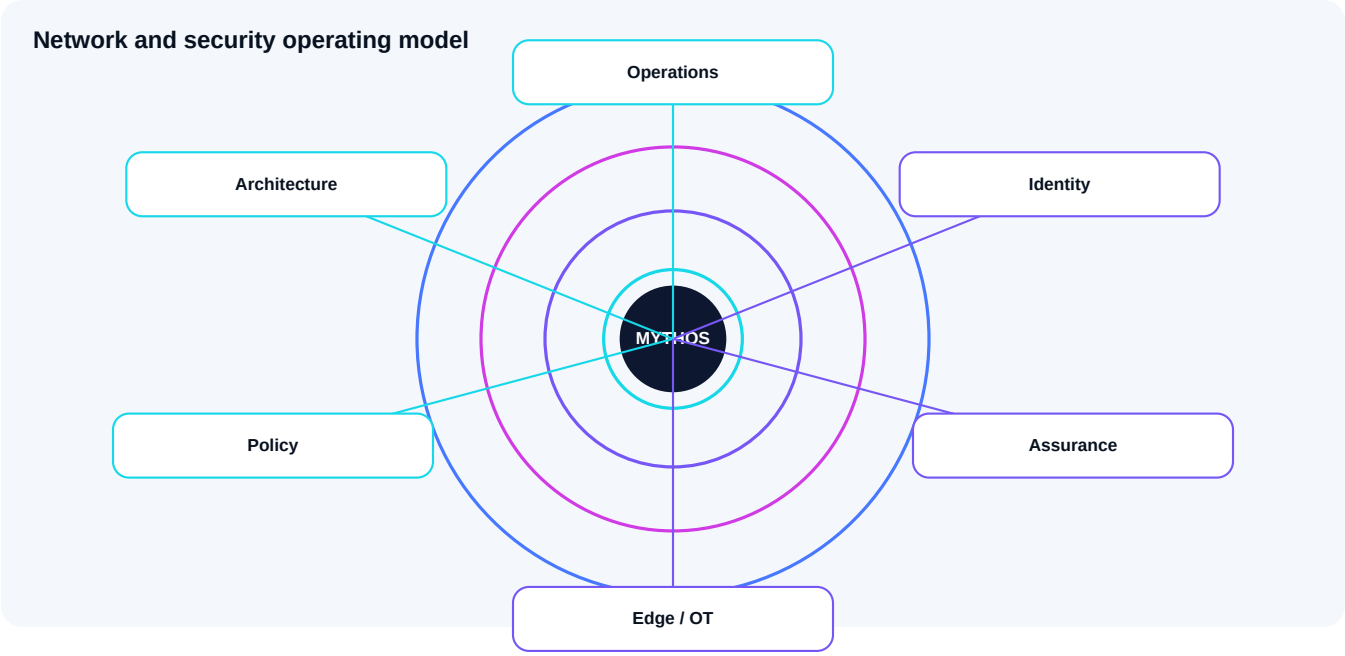
Publication position

This candidate publication is complete for structured technical review. It does not by itself establish certification, legal compliance, implementation conformance, benchmark reproduction, or final approval.

Contents

1. Guide purpose

This guide is the primary navigation and operating companion for its selected library domains. It does not replace the component standards. It explains how to select, sequence, combine, implement, verify, and operate them as one engineering program against the locked permanent-library baseline.



2. Domain operating model

Foundation and scope

Start with service criticality, environment classification, owner, identity boundary, evidence obligation, and explicit trust assumptions.

Topology and source of truth

Model physical/logical topology, routes, addressing, policy, dependencies, and desired-versus-observed state before automating change.

Identity and trust

Bind human, device, workload, and service identity to narrowly scoped authority and auditable lifecycle controls.

Security policy and segmentation

Treat policy as an attributable engineering artifact with positive and negative reachability proof, blast-radius analysis, and rollback.

Assured change

Use simulation/digital twins, pre-change validation, immutable approval context, post-change evidence, drift reconciliation, and safe rollback.

Threat and detection

Connect exposure, adversary behavior, telemetry, detection logic, incident response, and corrective action without replacing evidence with scoring alone.

Edge, OT, and telecom

Tailor timing, safety, radio, disconnected-operation, physical, and local-authority constraints rather than projecting data-center assumptions onto the edge.

End-to-end engineering sequence

3. Current standard register

38 permanent candidate standards form the primary scope of this guide. Foundation standards apply as inherited library controls even when they are not repeated below.

ID	Title	Domain	Refresh
MYTHOS-END-0001	Endpoint OS, Fleet Management & MDM Standard	Endpoint Engineering	120d
MYTHOS-GRC-0001	Federal, DoD, and Sovereign Compliance Standard	Governance, Risk, and Compliance	90d
MYTHOS-GRC-0002	AI Governance, Privacy, and Risk Management Standard	Governance, Risk, and Compliance	90d
MYTHOS-ID-0001	Workload, Agent & Human Identity Standard	Identity and Access	180d
MYTHOS-ID-0002	Public Key Infrastructure (PKI) & Attribute-Based Access Control (ABAC) Standard	Identity and Access	180d
MYTHOS-IOT-0001	IoT, Matter & Edge Sensor Standard	IoT and Edge Sensors	120d
MYTHOS-NET-0001	Network Architecture & Design Topology Standard	Network Engineering	180d
MYTHOS-NET-0002	Network Engineering & Multi-Vendor Automation Standard	Network Engineering	180d
MYTHOS-NET-0003	Network Digital Twin & Simulation Verification Standard	Network Engineering	180d
MYTHOS-NET-0004	Network Security Architecture & Zero-Trust Networking Standard	Network Engineering	180d
MYTHOS-NET-0005	Source-of-Truth (SoT) & Drift Reconciliation Standard	Network Engineering	180d
MYTHOS-NET-0006	Segment Routing (SRv6) & Next-Gen Transport Standard	Network Engineering	180d
MYTHOS-NET-0007	5G/6G RAN Automation & Network Slicing Standard	Network Engineering	180d
MYTHOS-NET-0008	OSI Troubleshooting & Core Network Infrastructure Standard	Network Engineering	180d
MYTHOS-NET-0009	Physical Layer, Cabling & Datacenter Topology Standard	Network Engineering	180d
MYTHOS-NET-0010	Routing, DNS & IPAM Standard	Network Engineering	180d
MYTHOS-NET-0011	Access, NAC & Wireless Engineering Standard	Network Engineering	180d
MYTHOS-OT-0001	ICS, Critical Infrastructure & OT Segmentation Standard	Operational Technology	180d
MYTHOS-SEC-0001	Post-Quantum Cryptography (PQC) & Crypto-Agility Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0002	AI Supply Chain, SBOM/AIBOM, & Artifact Provenance Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0003	Zero-Trust Policy, Authority Separation, & Capability Grant Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0004	Security Architecture & Advanced Design Principles Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0005	Security Engineering & SOC Automation (SOAR) Governance Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0006	Firewall Engineering, Policy Architecture, & Blast Radius Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0007	Network Security Architecture & Microsegmentation Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0008	Vulnerability Management & Exposure Assessment Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0009	Confidential Computing & Trusted Execution Environments (TEE) Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0010	Fully Homomorphic Encryption (FHE) & Zero-Knowledge Proof (ZKP) Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0011	API Security & Token Lifecycle Management Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0012	Virtualization, Hypervisor & Container Security Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0013	Adversary Tactics & Attack Methodology Standard (Vol 1: Web & Client-Side)	Cybersecurity and Network Security	90d
MYTHOS-SEC-0014	Adversary Tactics & Attack Methodology Standard (Vol 2: Network, Wireless & Supply Chain)	Cybersecurity and Network Security	90d
MYTHOS-SEC-0015	Penetration Testing & Ethical Hacking Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0016	SIEM, Threat Hunting & Detection Engineering Standard	Cybersecurity and Network Security	90d
MYTHOS-SEC-0017	DMZ Architecture & Perimeter Isolation Standard	Cybersecurity and Network Security	90d
MYTHOS-TEL-0001	5G/6G Core, Open RAN & Slicing Standard	Telecommunications	90d
MYTHOS-TEL-0002	Distributed Antenna Systems (DAS) & Indoor RF Standard	Telecommunications	90d
MYTHOS-TEL-0003	Enterprise Telephony, VoIP & Call Manager Standard	Telecommunications	90d

4. Architecture relationships

Reference architectures are implementation patterns, not mandatory products. Use them to make trust boundaries, state/data flows, failure assumptions, deployment profiles, observability, and verification concrete.

ID	Reference architecture	Use in this guide
RA-003	Enterprise Campus and Branch Network	An identity-driven, observable, programmable campus, branch, wireless, WAN, and security architecture with explicit sou...
RA-015	Edge, OT, IoT, and Telecommunications Convergence	A safety-aware architecture for distributed edge compute, industrial systems, sensors, wireless, telecom, local autonom...
RA-002	SIEM, SOAR, NDR, and Security Operations Center	A modern security-operations architecture that unifies telemetry, detection engineering, investigation, response, threa...
RA-006	Local-First AI Inference Cluster and Edge Node	A sovereign inference architecture for local models, multimodal processing, memory, routing, observability, and optiona...
RA-008	Multi-Cloud Landing Zone and Internal Developer Platform	A governed enterprise foundation for accounts, subscriptions, identity, networking, policy, platform services, golden p...
RA-009	Zero-Trust Identity, Policy, Secrets, and Access Fabric	A unified authority architecture for human, workload, agent, device, and service identity with capability grants, polic...
RA-019	Sovereign Browser, Remote Access, and Web Automation	A privacy-first browser and remote-access architecture that isolates identities, sessions, credentials, automation, dow...
RA-004	Network Source of Truth Implementation Pipeline	A closed-loop implementation pipeline that separates declarative intent, authoritative operational state, generated con...
RA-005	Secure Prosumer and Sovereign Home Network	A privacy-focused, segmented, observable, and locally controlled architecture for advanced home, laboratory, creator, a...
RA-007	AI-Assisted Software Engineering Pipeline	A governed software-engineering pipeline that combines repository intelligence, isolated agent work, model routing, det...
RA-010	Local-First Knowledge, Memory, and Evidence Platform	A source-linked architecture for document intelligence, retrieval, temporal memory, knowledge graphs, durable evidence,...
RA-014	Enterprise Data, API, Event, and Integration Fabric	A governed integration architecture for APIs, events, data products, schemas, workflows, identity, quality, lineage, re...

5. Research and adoption intelligence

Research material is time-bounded evidence. Adoption posture should follow reproduced evidence, stated limitations, readiness gates, and review triggers rather than novelty.

ID	Research publication	Refresh
RES-027	AI-Driven Radio Access Networks (RAN) & vRAN Orchestration	120d
MYTHOS-RES-ANNEX-AIKDIL-0001	AI Knowledge Data Identity And Learning Research Annex	90d
MYTHOS-RES-ANNEX-CLOUDEDGE-0001	Cloud Edge Telecom Hardware Media And Web Research Annex	90d
MYTHOS-RES-ANNEX-CRYPTO-0001	Advanced Cryptography PQC FHE ZKP And Quantum Networking Research Annex	90d
MYTHOS-RES-ANNEX-EMT-0001	Neuromorphic Npu Silicon Photonics And Edge Compute Research Annex	90d
MYTHOS-RES-ANNEX-NETSEC-0001	Network And Security Research Annex	90d
RES-015	Liquid Neural Networks (LNNs)	180d
RES-024	Zero-Knowledge Proofs (ZKPs) for Verifiable Agent Compute	120d
RES-025	Decentralized Physical Infrastructure Networks (DePIN) Compute Models	90d
RES-033	Photonic Quantum Networking & Entanglement Distribution	180d
RES-001	Desired vs. Observed Network State (Drift Dynamics)	180d
RES-003	Credential Brokering for Agents (Zero-Knowledge Secrets)	180d
RES-005	Network Digital Twin Limitations (Batfish/Containerlabs constraints)	180d
RES-006	Browser-Local WebLLM (Architecture, Constraints, and WebGPU bindings)	90d

6. Comparative evaluation and authority support

ID	Publication	Class
AUTH-008	MITRE and FIRST Threat, Defense, and Vulnerability Crosswalk	Authority Crosswalk
CMP-005	Modern Private Networking and Zero-Trust Overlay Platforms	Comparative Evaluation
AUTH-001	NIST Current-Version Authority Crosswalk	Authority Crosswalk
AUTH-002	CISA Directives, Catalogs, and Operational Guidance Crosswalk	Authority Crosswalk
AUTH-003	CIS Controls and Benchmarks Crosswalk	Authority Crosswalk
AUTH-004	IETF, RFC, IANA, and OpenID Protocol Crosswalk	Authority Crosswalk
AUTH-005	IEEE, Wi-Fi Alliance, Thread, and Matter Crosswalk	Authority Crosswalk
AUTH-006	OWASP and CERT Application, API, AI, Mobile, and Disclosure Crosswalk	Authority Crosswalk
AUTH-007	DoD, DISA, DFARS, and CMMC Crosswalk	Authority Crosswalk
AUTH-009	External Benchmark and Industry Measurement Crosswalk	Authority Crosswalk
CMP-001	NetBox and Nautobot	Comparative Evaluation
CMP-002	Enterprise Next-Generation Firewall Platforms	Comparative Evaluation

7. Evidence and assurance model

Minimum evidence coverage

Evidence layer	Minimum retained evidence
Intent	Owner, scope, requirements, exceptions, risk, expected state.
Architecture	Boundaries, identities, dependencies, state/data flows, failure domains.
Pre-change / pre-release	Static analysis, simulation, policy checks, negative tests, versioned candidate.
Execution	Stable change/release ID, actor, authorization, timestamps, commands/actions, outcome codes.
Observed result	Telemetry, traces/logs/metrics, path or transaction evidence, health and correctness checks.
Recovery	Rollback/forward-recovery evidence, restored state, residual risk, post-incident learning.

8. Implementation sequence

Controlled implementation and operations loop

Expand blast radius only after the preceding stage has retained evidence. Automation should encode a proven manual or modeled process; it should not make an undocumented process execute faster.

9. Maturity path

Stage	Demonstrated capability
Foundation	Explain critical state and failure behavior from first principles; identify owners and authorities.
Build	Implement the smallest representative system with typed boundaries, tests, and telemetry.
Operate	Diagnose and recover from injected failure while preserving causal evidence.
Automate	Convert repeatable work into idempotent, policy-bound, observable automation.
Architect	Design for scale, security, resilience, lifecycle change, interoperability, and governance.
Explore	Evaluate emerging techniques using hypotheses, limitations, reproduced evidence, and adoption gates.

10. Review gate

Advance a design or operating pattern only when another qualified engineer can reproduce the evidence, explain the architecture and authority boundaries, identify likely failure modes, distinguish measured facts from assumptions, and execute or validate recovery within the declared scope.

11. Limitations

This guide is an integration and navigation publication. Component standards remain authoritative for their Mythos requirements. External authorities remain with their issuers, and environment-specific product behavior must be revalidated against current versions and observed evidence.