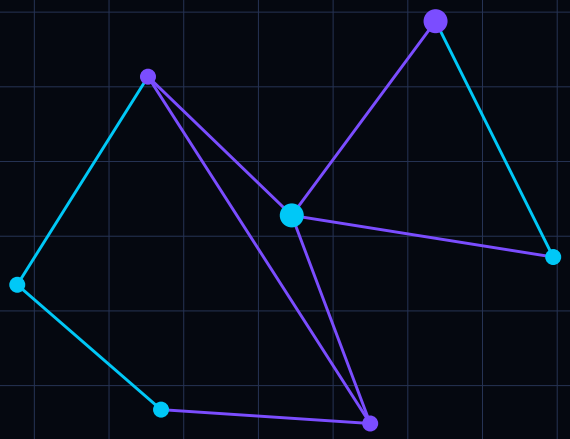
M MYTHOS SYSTEMS

ENGINEERING STANDARDS LIBRARY / NETWORK + SECURITY

Network and Security Standards Executive Portfolio

Permanent publication map for network engineering, cybersecurity, focused practitioner guides, research intelligence, and reference architectures.



PERMANENT ID	STANDARDS	FOCUSED GUIDES	RESEARCH / ARCH
MYTHOS-NETSEC-EXEC-0001	28	41	15 / 9

Permanent publication architecture

The network and security library is not one report. It is a graph of independent permanent publications with stable identities.

28 **NORMATIVE STANDARDS**

NET-0001..0011 + SEC-0001..0017

5 **LIVING OVERVIEWS**

Network / network security / security / cyber ops / PQC

41 **FOCUSED GUIDES**

22 network + 19 security

15 **RESEARCH REPORTS**

Evidence, limitations, adoption, freshness

9 **REFERENCE ARCHITECTURES**

Topology, trust, automation, observability

Network engineering standards

MYTHOS-NET-0001	Network Architecture, Design, and Topology Standard
MYTHOS-NET-0002	Network Engineering and Multi-Vendor Automation Standard
MYTHOS-NET-0003	Network Digital Twin and Simulation Verification Standard
MYTHOS-NET-0004	Network Security Architecture and Zero-Trust Networking Standard
MYTHOS-NET-0005	Network Source of Truth and Drift Reconciliation Standard
MYTHOS-NET-0006	Segment Routing and Next-Generation Transport Standard
MYTHOS-NET-0007	5G, 6G, RAN Automation, and Network Slicing Standard
MYTHOS-NET-0008	OSI Troubleshooting and Core Infrastructure Standard
MYTHOS-NET-0009	Physical Layer, Cabling, Optics, and Data-Center Topology Standard
MYTHOS-NET-0010	Routing, DNS, DHCP, and IPAM Standard
MYTHOS-NET-0011	Access, NAC, Wireless, and RF Engineering Standard

Cybersecurity standards

MYTHOS-SEC-0001	Post-Quantum Cryptography and Crypto-Agility Standard
MYTHOS-SEC-0002	AI Supply Chain, SBOM, AIBOM, and Artifact Provenance Standard
MYTHOS-SEC-0003	Zero-Trust Policy, Authority Separation, and Capability Grant Standard
MYTHOS-SEC-0004	Security Architecture and Advanced Design Principles Standard
MYTHOS-SEC-0005	Security Engineering and SOC Automation Governance Standard
MYTHOS-SEC-0006	Firewall Engineering, Policy Architecture, and Blast-Radius Standard
MYTHOS-SEC-0007	Network Security Architecture and Microsegmentation Standard
MYTHOS-SEC-0008	Vulnerability Management and Exposure Assessment Standard
MYTHOS-SEC-0009	Confidential Computing and Trusted Execution Environment Standard

Cybersecurity standards / continued

MYTHOS-SEC-0010	Fully Homomorphic Encryption and Zero-Knowledge Proof Standard
MYTHOS-SEC-0011	API Security and Token Lifecycle Standard
MYTHOS-SEC-0012	Virtualization, Hypervisor, Container, and Workload Security Standard
MYTHOS-SEC-0013	Adversary Tactics and Attack Methodology - Web and Client Standard
MYTHOS-SEC-0014	Adversary Tactics and Attack Methodology - Network, Wireless, and Supply Chain Standard
MYTHOS-SEC-0015	Penetration Testing and Ethical Hacking Standard
MYTHOS-SEC-0016	SIEM, Threat Hunting, and Detection Engineering Standard
MYTHOS-SEC-0017	DMZ, Perimeter, Remote Access, and Isolation Standard

Guide decomposition is a publication se

The source guides decompose into permanent living overviews plus focused practitioner field guides. They are not replaced by a synthetic umbrella guide.

MYTHOS-GUIDE-NET-0001	Network Engineering: Foundations, Architecture, Automation, an
MYTHOS-GUIDE-NETSEC-0001	Network Security Engineering: Policy, Segmentation, Identity,
MYTHOS-GUIDE-SEC-0001	Security Engineering and Information Security
MYTHOS-GUIDE-CYOPS-0001	Cybersecurity Operations, Detection, Response, and Threat Hunt
MYTHOS-GUIDE-PQC-0001	Modern Cryptography and Post-Quantum Migration

Focused decomposition

22 **NETWORK ENGINEERING**

MYTHOS-FG-NET-0001 through MYTHOS-FG-NET-0022

19 **CYBERSECURITY**

MYTHOS-FG-SEC-0001 through MYTHOS-FG-SEC-0019

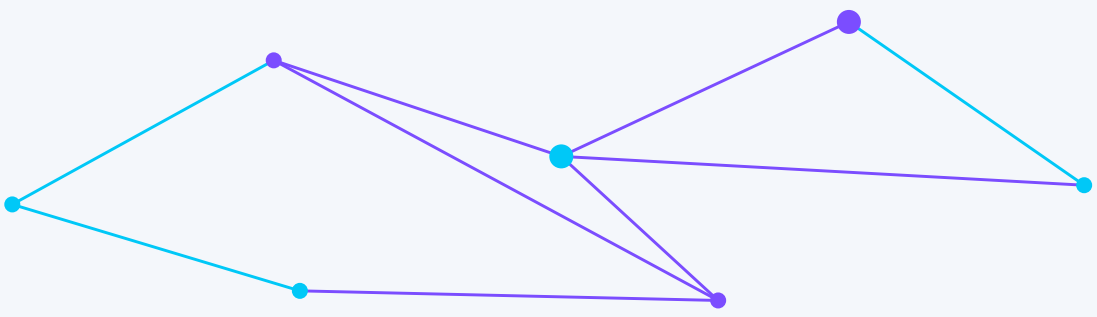
Research intelligence + reference archi

15 research reports

RES-001 Desired vs. Observed Network Stat
RES-003 Credential Brokering for Agents (
RES-004 CISA KEV + EPSS + CVSS (Exploitab
RES-005 Network Digital Twin Limitations
RES-008 Post-Quantum Network Migration (H
RES-009 Evidence Bundles (Cryptographic P
RES-011 Developing an Attack: OWASP Top 1
RES-023 Trusted Execution Environments (T
RES-024 Zero-Knowledge Proofs (ZKPs) for
RES-026 Segment Routing (SRv6) Programmab
RES-027 AI-Driven Radio Access Networks (
RES-028 5G/6G Network Slicing & QoS Enfor
RES-029 TLA+ Formal Verification for Dist
RES-032 Local-First SQLite Event Sourcing
RES-034 NIST FIPS 203/204/205 PQC Integra

9 reference architectures

RA-002 SIEM, SOAR, NDR, and Security O
RA-003 Enterprise Campus and Branch Ne
RA-004 Network Source-of-Truth and Imp
RA-005 Secure Prosumer and Sovereign H
RA-009 Zero-Trust Identity, Policy, Se
RA-011 Digital Twin, Infrastructure Au
RA-012 Enterprise Observability, SRE,
RA-015 Edge, OT, IoT, and Telecommunic
RA-019 Sovereign Browser, Remote Acces



Publication acceptance model

IDENTITY

Permanent IDs and canonical titles govern every public artifact.

EVIDENCE

Assessment claims remain bounded by evidence and validation windows.

VISUAL SYSTEM

Topology, packet/control flow, attack path, enforcement and evidence-chain visuals are semantic, not decorative.

FRESHNESS

Research preserves validation dates and review windows; candidate status remains explicit.

QA

Searchability, bookmarks, metadata, forbidden-label scans, page rendering, and archive integrity are release gates.