SECURITY CANON

2026-03-18

Dexter Hadley, MD/PhD

Hadley Lab CANONIC

Abstract

Example

Contents

Threats MUST be identified, categorized, and assessed before controls are applied.

Example: STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) Microsofts threat categorization framework. MITRE ATT&CK knowledge base of adversary tactics, techniques, and procedures (TTPs) organized by platform (Enterprise, Mobile, ICS). Cyber Kill Chain (Lockheed Martin) 7 phases: reconnaissance, weaponization, delivery, exploitation, installation, C2, actions on objectives. Threat intelligence sharing: STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information) standards. Diamond Model adversary, capability, infrastructure, victim relationship analysis.

0.1 2. Access Control

Access MUST follow the principle of least privilege. Authentication and authorization MUST be enforced at every boundary.

Example: RBAC (Role-Based Access Control) permissions assigned to roles, users assigned to roles. ABAC (Attribute-Based Access Control) policy decisions based on user/resource/environment attributes. Zero Trust Architecture (NIST SP 800-207) never trust, always verify. No implicit trust based on network location. PAM (Privileged Access Management) vaulting, session recording, just-in-time access for admin credentials. MFA standards: FIDO2/WebAuthn (phishing-resistant), TOTP (time-based one-time passwords), push notification. OAuth 2.0/OIDC for delegated authorization and identity federation.

0.2 3. Incident Response

Security incidents MUST be detected, contained, eradicated, and recovered from with doc-

umented lessons learned.

Example: NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide. Four phases: preparation, detection & analysis, containment/eradication/recovery, post-incident activity. CISA incident reporting critical infrastructure entities must report significant cyber incidents within 72 hours and ransomware payments within 24 hours (CIRCIA, 2022). State breach notification laws all 50 states + DC/territories require notification for PII breaches (notification timelines vary: 30-60 days typical). Forensic chain of custody digital evidence must be preserved, hashed (SHA-256), and documented for potential litigation.

0.3 4. Compliance Frameworks

Security programs MUST satisfy applicable compliance frameworks and demonstrate continuous conformance.

Example: ISO 27001:2022 ISMS (Information Security Management System) requirements. 93 controls in Annex A organized by themes (organizational, people, physical, technological). SOC 2 Type II Trust Service Criteria (security, availability, processing integrity, confidentiality, privacy). 6-12 month observation period. PCI-DSS v4.0 12 requirements for cardholder data protection, self-assessment or QSA audit depending on volume. HITRUST CSF healthcare-specific framework harmonizing HIPAA, NIST, ISO, and other standards. NIST Cybersecurity Framework (CSF) 2.0 Govern, Identify, Protect, Detect, Respond, Recover functions.

0.4 5. Application Security

Software MUST be developed, tested, and maintained according to secure development lifecycle practices.

Example: OWASP Top 10 (2021) broken access control, cryptographic failures, injection, insecure design, security misconfiguration, vulnerable components, authentication failures, integrity failures, logging/monitoring failures, SSRF. Testing: SAST (Static Application Security Testing code analysis), DAST (Dynamic runtime testing), SCA (Software Composition Analysis dependency vulnerabilities), IAST (Interactive instrumented testing). CVE (Common Vulnerabilities and Exposures) standardized identifiers. CWE (Common Weakness Enumeration) categorizes software weaknesses. Secure SDLC: threat modeling in design, secure coding standards, security testing in CI/CD, vulnerability management post-release.

0.5 6. Data Protection

Data at rest and in transit MUST be protected using approved cryptographic standards.

Example: Encryption standards: AES-256 (NIST FIPS 197) for data at rest, TLS 1.3 (RFC 8446) for data in transit. Key management: NIST SP 800-57 key lifecycle (generation, distribution, storage, rotation, destruction). HSMs (Hardware Security Modules) for key protection. DLP (Data Loss Prevention) content inspection, endpoint agents, network monitoring. Data classification: public, internal, confidential, restricted/regulated. NIST SP 800-88 Rev. 1 media sanitization guidelines (clear, purge, destroy). Certificate management: PKI, certificate transparency, ACME protocol for automated issuance.

1. Constraints

```
MUST:     Cite specific framework control or standard
MUST:     Distinguish between compliance frameworks by
MUST NOT: Present compliance as equivalent to security
```

SECURITY | CANON | HORIZONTAL