Security Documentation - Phase 2 Day 2

Overview

This document provides comprehensive security documentation for the HX Infrastructure Ansible project, covering all security measures, configurations, and procedures implemented in Phase 2 Day 2.

Security Framework

1. Multi-Layer Security Approach

Our security implementation follows a defense-in-depth strategy with multiple layers:

- **Infrastructure Security**: Network segmentation, firewall rules, VPC security
- **Access Control**: SSH key management, role-based access, principle of least privilege
- **Operational Security**: Safety procedures, dangerous command protection, audit logging
- **Data Security**: Encryption at rest and in transit, secrets management
- **Application Security**: Secure configurations, input validation, security headers
- **Monitoring & Detection**: Security monitoring, intrusion detection, audit trails

2. Security Controls Matrix

Control Category	Implementation	Status	Priority
Authentication	SSH Key-based	✅ Complete	Critical
Authorization	Role-based Access	✅ Complete	Critical
Encryption	TLS 1.2+, SSH, Vault	✅ Complete	Critical
Network Security	Firewall, Segmentation	✅ Complete	High
Audit Logging	Comprehensive Logs	✅ Complete	High
Vulnerability Management	Automated Scanning	✅ Complete	High
Incident Response	Procedures & Tools	✅ Complete	Medium
Backup & Recovery	Automated Backups	✅ Complete	Medium

Authentication & Access Control

1. SSH Key Management

Key Generation Standards

- **Algorithm**: ED25519 (preferred) or RSA 4096-bit minimum

- **Key Rotation**: Every 90 days for production environments
- **Key Storage**: Encrypted storage with restricted access
- **Key Distribution**: Automated via Ansible with verification

SSH Security Configuration

```
# SSH Hardening Settings
Protocol: 2
PermitRootLogin: no
PasswordAuthentication: no
PubkeyAuthentication: yes
PermitEmptyPasswords: no
ChallengeResponseAuthentication: no
X11Forwarding: no
ClientAliveInterval: 300
ClientAliveCountMax: 2
MaxAuthTries: 3
LoginGraceTime: 60
```

Key Management Procedures

1. **Key Generation**: Automated via `ssh_key_management` role
2. **Key Distribution**: Secure distribution to authorized hosts
3. **Key Rotation**: Scheduled rotation with rollback capability
4. **Key Revocation**: Immediate removal from all systems
5. **Key Audit**: Regular audit of key usage and access

2. Role-Based Access Control (RBAC)

User Roles

- **Production Admin**: Full production access with safety controls
- **Application Deployer**: Application deployment permissions
- **Database Admin**: Database-specific access
- **Monitoring User**: Read-only monitoring access
- **Backup Operator**: Backup and restore operations

Permission Matrix

```
production_admin:
  - all_hosts: ["*"]
  - operations: ["deploy", "configure", "maintain", "backup", "restore"]
  - safety_required: true
  - approval_required: true

app_deployer:
  - hosts: ["production_app_servers"]
  - operations: ["deploy", "restart", "configure"]
  - safety_required: true
  - approval_required: false

db_admin:
  - hosts: ["production_database_servers"]
  - operations: ["backup", "restore", "configure", "maintain"]
  - safety_required: true
  - approval_required: true
```

Network Security

1. Network Segmentation

Network Architecture

```
┌─────────────────┐    ┌─────────────────┐    ┌─────────────────┐
│   DMZ Network   │    │ Application Net │    │ Database Net    │
│  10.0.100.0/24  │    │  10.0.1.0/24    │    │  10.0.2.0/24    │
│                 │    │                 │    │                 │
│ Load Balancers  │    │ App Servers     │    │ DB Servers      │
│ Web Servers     │    │ API Servers     │    │ Cache Servers   │
└─────────────────┘    └─────────────────┘    └─────────────────┘
         │                       │                       │
         └───────────────────────┼───────────────────────┘
                                 │
                    ┌─────────────────┐
                    │ Management Net  │
                    │  10.0.200.0/24  │
                    │                 │
                    │ Ansible Control │
                    │ Monitoring      │
                    │ Logging         │
                    └─────────────────┘
```

Firewall Rules

```yaml
# Web Tier (DMZ)
web_tier_rules:
  inbound:
    - { port: 80, protocol: tcp, source: "0.0.0.0/0", action: allow }
    - { port: 443, protocol: tcp, source: "0.0.0.0/0", action: allow }
    - { port: 22, protocol: tcp, source: "10.0.200.0/24", action: allow }
  outbound:
    - { port: 8080, protocol: tcp, destination: "10.0.1.0/24", action: allow }
    - { port: 443, protocol: tcp, destination: "0.0.0.0/0", action: allow }

# Application Tier
app_tier_rules:
  inbound:
    - { port: 8080, protocol: tcp, source: "10.0.100.0/24", action: allow }
    - { port: 22, protocol: tcp, source: "10.0.200.0/24", action: allow }
  outbound:
    - { port: 5432, protocol: tcp, destination: "10.0.2.0/24", action: allow }
    - { port: 443, protocol: tcp, destination: "0.0.0.0/0", action: allow }

# Database Tier
db_tier_rules:
  inbound:
    - { port: 5432, protocol: tcp, source: "10.0.1.0/24", action: allow }
    - { port: 22, protocol: tcp, source: "10.0.200.0/24", action: allow }
  outbound:
    - { port: 443, protocol: tcp, destination: "0.0.0.0/0", action: allow }
```

2. SSL/TLS Configuration

TLS Standards

- **Minimum Version**: TLS 1.2
- **Preferred Version**: TLS 1.3

- **Certificate Authority**: Let’s Encrypt with automated renewal
- **Key Exchange**: ECDHE (Perfect Forward Secrecy)
- **Cipher Suites**: Strong ciphers only

SSL Configuration

```
# Nginx SSL Configuration
ssl_protocols TLSv1.2 TLSv1.3;
ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384;
ssl_prefer_server_ciphers off;
ssl_session_cache shared:SSL:10m;
ssl_session_timeout 10m;
ssl_stapling on;
ssl_stapling_verify on;

# Security Headers
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
add_header X-Frame-Options DENY always;
add_header X-Content-Type-Options nosniff always;
add_header X-XSS-Protection "1; mode=block" always;
add_header Referrer-Policy "strict-origin-when-cross-origin" always;
```

Secrets Management

1. Ansible Vault Integration

Vault Configuration

```
# Vault settings
vault_enabled: true
vault_url: "{{ lookup('env', 'HX_VAULT_URL') }}"
vault_auth_method: "{{ lookup('env', 'HX_VAULT_AUTH_METHOD') }}"
vault_token_ttl: 3600
vault_renewal_threshold: 300

# Secret paths
vault_secret_paths:
  database: "secret/production/database"
  application: "secret/production/application"
  ssl_certificates: "secret/production/ssl"
  api_keys: "secret/production/api"
```

Secret Encryption

All sensitive data is encrypted using Ansible Vault:

```
# Encrypt sensitive variables
ansible-vault encrypt_string 'secret_password' --name 'db_password'

# Encrypt entire files
ansible-vault encrypt group_vars/production/vault.yml

# Edit encrypted files
ansible-vault edit group_vars/production/vault.yml
```

2. Environment Variable Management

Secure Environment Variables

```
# Production environment variables
export HX_VAULT_URL="https://vault.hana-x.ai:8200"
export HX_VAULT_AUTH_METHOD="aws"
export HX_DB_PASSWORD_FILE="/secure/db_password"
export HX_API_KEY_FILE="/secure/api_key"
export HX_SSL_CERT_PATH="/secure/ssl/cert.pem"
export HX_SSL_KEY_PATH="/secure/ssl/key.pem"
```

Operational Security

1. Dangerous Command Protection

Protected Commands

The system automatically protects against dangerous operations:

```
dangerous_commands:
  filesystem:
    - "rm -rf /"
    - "dd if=/dev/zero"
    - "mkfs.*"
    - "fdisk"
    - "parted"
    - "wipefs"

  database:
    - "DROP DATABASE"
    - "TRUNCATE TABLE"
    - "DELETE FROM .* WHERE"

  system:
    - "shutdown"
    - "reboot"
    - "halt"
    - "init 0"
```

Safety Procedures

1. **Pre-operation Backup**: Automatic backup before destructive operations
2. **Confirmation Prompts**: Interactive confirmation for critical operations
3. **Maintenance Windows**: Restricted operation times for production
4. **Rollback Scripts**: Automatic generation of rollback procedures
5. **Audit Logging**: Complete audit trail of all operations

2. Security Monitoring

Log Sources

- **System Logs**: `/var/log/syslog`, `/var/log/auth.log`
- **Application Logs**: Application-specific log files
- **Security Logs**: `/var/log/ansible-safety/`, `/var/log/security/`
- **Audit Logs**: `/var/log/audit/audit.log`
- **Network Logs**: Firewall and network device logs

Monitoring Rules

```yaml
security_alerts:
  authentication_failures:
    threshold: 5
    window: 300  # 5 minutes
    action: "block_ip"

  privilege_escalation:
    pattern: "sudo.*root"
    action: "alert_admin"

  dangerous_commands:
    pattern: "rm -rf|dd if=|mkfs"
    action: "alert_security_team"

  unauthorized_access:
    pattern: "authentication failure"
    threshold: 10
    window: 600  # 10 minutes
    action: "lock_account"
```

Vulnerability Management

1. Automated Security Scanning

Security Scanner Features

- **Static Analysis**: Code and configuration analysis
- **Dependency Scanning**: Third-party library vulnerabilities
- **Configuration Assessment**: Security misconfigurations
- **Compliance Checking**: Industry standard compliance
- **Continuous Monitoring**: Regular automated scans

Scan Schedule

```yaml
security_scans:
  daily:
    - vulnerability_scan
    - configuration_check
    - log_analysis

  weekly:
    - full_system_scan
    - dependency_audit
    - compliance_check

  monthly:
    - penetration_test
    - security_review
    - policy_update
```

2. Patch Management

Patching Strategy

1. **Critical Patches**: Applied within 24 hours
2. **Security Patches**: Applied within 7 days

3. **Regular Updates**: Applied during maintenance windows
4. **Testing**: All patches tested in staging first
5. **Rollback**: Automatic rollback on failure

Patch Automation

```yaml
patch_management:
  auto_security_updates: true
  maintenance_window: "02:00-06:00 UTC"
  testing_required: true
  rollback_enabled: true
  notification_channels:
    - email
    - slack
    - pagerduty
```

Incident Response

1. Security Incident Classification

Severity Levels

- **Critical**: Active security breach, data compromise
- **High**: Potential security breach, system compromise
- **Medium**: Security policy violation, suspicious activity
- **Low**: Security configuration issue, minor policy violation

Response Times

- **Critical**: Immediate response (< 15 minutes)
- **High**: Urgent response (< 1 hour)
- **Medium**: Standard response (< 4 hours)
- **Low**: Routine response (< 24 hours)

2. Incident Response Procedures

Response Team

- **Incident Commander**: Overall incident coordination
- **Security Analyst**: Security investigation and analysis
- **System Administrator**: System remediation and recovery
- **Communications Lead**: Stakeholder communication
- **Legal/Compliance**: Legal and regulatory requirements

Response Workflow

1. **Detection**: Automated alerts or manual reporting
2. **Assessment**: Initial impact and severity assessment
3. **Containment**: Immediate containment of the incident
4. **Investigation**: Detailed forensic investigation
5. **Eradication**: Remove the root cause
6. **Recovery**: Restore normal operations
7. **Lessons Learned**: Post-incident review and improvements

Compliance & Auditing

1. Compliance Frameworks

Supported Standards

- **SOC 2 Type II**: Security, availability, processing integrity
- **ISO 27001**: Information security management
- **CIS Controls**: Center for Internet Security benchmarks
- **NIST Cybersecurity Framework**: Risk-based approach
- **GDPR**: Data protection and privacy (where applicable)

Compliance Monitoring

```yaml
compliance_checks:
  access_control:
    - user_access_review
    - privilege_escalation_audit
    - ssh_key_rotation_check

  data_protection:
    - encryption_verification
    - backup_integrity_check
    - data_retention_compliance

  system_security:
    - vulnerability_assessment
    - configuration_compliance
    - patch_management_audit
```

2. Audit Trail

Audit Log Requirements

- **User Authentication**: All login attempts and outcomes
- **Privilege Usage**: All sudo and administrative actions
- **Data Access**: Database queries and file access
- **Configuration Changes**: All system and application changes
- **Security Events**: All security-related activities

Log Retention

- **Security Logs**: 7 years retention
- **Audit Logs**: 7 years retention
- **System Logs**: 1 year retention
- **Application Logs**: 90 days retention
- **Debug Logs**: 30 days retention

Security Testing

1. Automated Security Testing

Test Types

- **Static Application Security Testing (SAST)**: Code analysis
- **Dynamic Application Security Testing (DAST)**: Runtime testing

- **Interactive Application Security Testing (IAST)**: Hybrid approach
- **Software Composition Analysis (SCA)**: Dependency scanning
- **Infrastructure as Code (IaC) Scanning**: Configuration testing

Testing Pipeline

```yaml
security_testing:
  pre_commit:
    - secret_scanning
    - static_analysis
    - policy_validation

  ci_pipeline:
    - dependency_check
    - container_scanning
    - configuration_audit

  pre_deployment:
    - dynamic_testing
    - penetration_testing
    - compliance_check

  post_deployment:
    - runtime_monitoring
    - behavioral_analysis
    - continuous_assessment
```

2. Penetration Testing

Testing Scope

- **External Testing**: Internet-facing systems
- **Internal Testing**: Internal network and systems
- **Web Application Testing**: Application security
- **Wireless Testing**: Wireless network security
- **Social Engineering**: Human factor testing

Testing Schedule

- **Quarterly**: External penetration testing
- **Semi-annually**: Internal penetration testing
- **Annually**: Comprehensive security assessment
- **Ad-hoc**: After major changes or incidents

Security Metrics & KPIs

1. Security Metrics

Key Performance Indicators

```yaml
security_kpis:
  vulnerability_management:
    - mean_time_to_patch: "< 7 days"
    - critical_vulnerabilities: "0"
    - vulnerability_scan_coverage: "> 95%"

  incident_response:
    - mean_time_to_detection: "< 15 minutes"
    - mean_time_to_containment: "< 1 hour"
    - incident_recurrence_rate: "< 5%"

  access_control:
    - failed_login_attempts: "< 1% of total"
    - privileged_account_usage: "monitored 100%"
    - ssh_key_rotation_compliance: "> 95%"

  compliance:
    - audit_findings: "0 critical"
    - policy_compliance: "> 98%"
    - training_completion: "> 95%"
```

2. Security Dashboard

Monitoring Dashboards

- **Security Overview**: High-level security status
- **Threat Intelligence**: Current threat landscape
- **Vulnerability Management**: Patch status and trends
- **Incident Response**: Active incidents and response times
- **Compliance Status**: Compliance posture and gaps

Training & Awareness

1. Security Training Program

Training Components

- **Security Awareness**: General security principles
- **Role-specific Training**: Job-specific security requirements
- **Incident Response**: Response procedures and tools
- **Compliance Training**: Regulatory requirements
- **Technical Training**: Security tools and technologies

Training Schedule

- **New Employee**: Within first week
- **Annual Refresher**: All employees
- **Quarterly Updates**: Security team
- **Ad-hoc Training**: After incidents or changes

2. Security Policies

Policy Framework

- **Information Security Policy**: Overall security governance
- **Access Control Policy**: User access and authentication
- **Data Protection Policy**: Data handling and privacy
- **Incident Response Policy**: Security incident procedures
- **Acceptable Use Policy**: System and resource usage

Contact Information

Security Team Contacts

- **Security Officer**: security@hana-x.ai
- **Incident Response**: incident@hana-x.ai
- **Compliance Officer**: compliance@hana-x.ai
- **Emergency Hotline**: +1-XXX-XXX-XXXX

External Contacts

- **Security Vendor**: vendor-security@example.com
- **Legal Counsel**: legal@hana-x.ai
- **Regulatory Authority**: As required by jurisdiction
- **Law Enforcement**: As required by incident type

Document Version: 1.0
Last Updated: 2025-09-18
Next Review: 2025-12-18
Owner: Security Team
Approved By: CISO