Security Lab GRC Documentation

NIST SP 800-53, Rev 5 Framework

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



Created By: Paul Leone

April 7, 2026

Table of Contents

NIST SP 800-53, Rev 5 Framework 2
Version 2.0: Change Log (from v1.0, January 2026) 2
Overview 4
Overall Maturity: High (Technical Controls) / Moderate (Administrative Controls) 4
Control Family Implementation Detail 4
Access Control (AC): 90% Compliant (27/30 Implemented) 4
Audit and Accountability (AU): 100% Compliant (18/18 Implemented) 7
Assessment, Authorization, and Monitoring (CA): 80% Compliant (8/10 Implemented) 10
Configuration Management (CM): 95% Compliant (15/16 Implemented) 11
Contingency Planning (CP): 75% Compliant (6/8 Implemented) 13
Identification and Authentication (IA): 95% Compliant (17/18 Implemented) 13
Incident Response (IR): 90% Compliant (11/13 Implemented) 15
Maintenance (MA): 60% Compliant (4/6 Implemented) 16
Media Protection (MP): 40% Compliant 17
Physical and Environmental Protection (PE): N/A (Residential Homelab) 17
Planning (PL): 60% Compliant 17
Program Management (PM): 40% Compliant 17
Risk Assessment (RA): 85% Compliant (10/12 Implemented) 18
System and Communications Protection (SC): 95% Compliant (24/25 Implemented) 19
System and Information Integrity (SI): 90% Compliant (25/28 Implemented) 22
Supply Chain Risk Management (SR): 40% Compliant 25

NIST SP 800-53, Rev 5 Framework

Document Control:

Version:	2.0
Last Updated:	April 2026
Owner:	Paul Leone
Prior Version:	1.0: January 2026

Version 2.0: Change Log (from v1.0, January 2026)

Cloud workload content integrated directly into each control's Notes column. Cloud node inventory: AWS (2 nodes: Amazon Linux 2, Windows Server 2025), Azure (2 nodes: Ubuntu 24.04 LTS, Windows Server 2025), GCP (2 nodes: Debian 13.4, Ubuntu): 6 nodes total. All nodes connected via Tailscale WireGuard mesh VPN with no public management ports.

Control	Control Name	Change	Status Impact
AC-17	**Remote Access**	Cloud node remote access added: SSH (Linux) and RDP (Windows) restricted to homelab subnets (192.168.0.0/16) via provider-native firewall rules (AWS Security Groups, GCP VPC firewall policy, Azure NSG); all management traffic routed through Tailscale WireGuard with no public internet exposure.	Implemented
AU-2	**Event Logging**	Cloud audit logging added: AWS CloudTrail (all management events, S3 with SSE); GCP Admin Activity logs (always-on) and Data Access audit logs; Azure Activity Log and Monitor (homelab-log workspace); Wazuh agent forwarding from all 6 cloud nodes to on-premises Splunk.	Implemented
AU-6	**Audit Record Review**	Cloud-native alerting added: CloudWatch Alarms (AWS), GCP Cloud Monitoring alerting policies, Azure Monitor alert rules (7 VM metric alerts active); all feed on-premises SOC dashboards.	Implemented
CA-7	**Continuous Monitoring**	Cloud continuous monitoring added: AWS GuardDuty (VPC flow, CloudTrail, DNS: real-time ML detection), GCP SCC (asset inventory, vulnerability assessment, network IDS endpoint), Azure Defender for Cloud and Sentinel (KQL rules, automated response); all integrated with on-premises SIEM via Wazuh agent telemetry.	Implemented
CM-8	**System Component Inventory**	Cloud component inventory added: 6 nodes across AWS, GCP, and Azure tracked in PatchMon, Wazuh,	Implemented

		Checkmk, and Tailscale admin console. Wazuh endpoint count updated to 31+.	
IA-2	**Identification and Authentication**	Cloud identity added: Windows cloud nodes domain-joined to home.com via Tailscale (Kerberos, GPO, WSUS); Linux cloud nodes use SSH Ed25519 key-based auth with centralized Ansible key management.	Implemented
IA-3	**Device Identification**	Cloud device identification added: all 6 cloud nodes enrolled in Tailscale tailnet (tailf07c05.ts.net) with device-bound WireGuard keys; Wazuh agent IDs serve as device identifiers in SIEM.	Implemented
RA-5	**Vulnerability Monitoring and Scanning**	Cloud vulnerability scanning added: Wazuh CIS SCA and vulnerability assessment on all 6 cloud nodes daily; PatchMon tracks 4 Linux cloud nodes against NVD; AWS Inspector, GCP SCC, Azure Defender for Cloud provide provider-native scanning.	Implemented
SC-7	**Boundary Protection**	Cloud boundary protection added: AWS Security Groups (tailscale-access + lab-services), GCP VPC network firewall policy homelab (17 rules, Google Threat Intelligence blocking for TOR exit nodes, malicious IPs, sanctioned countries), Azure NSG homelab-nsg2 (explicit allow-list, deny-all defaults), GCP Cloud Armor three-tier WAF/DDoS.	Implemented
SC-8	**Transmission Confidentiality and Integrity**	Cloud transmission controls added: all management traffic via Tailscale WireGuard (ChaCha20-Poly1305); cloud VPC/VNet internal traffic uses provider-encrypted private networking; SSH AES-256-GCM for Linux nodes; RDP over Tailscale for Windows nodes.	Implemented
SI-3	**Malicious Code Protection**	Cloud malware protection added: Wazuh FIM and rootkit detection on all 6 cloud nodes; Microsoft Defender on Windows Server 2025 (AWS and Azure); ClamAV on all 4 Linux cloud nodes; GuardDuty, SCC, Defender for Cloud provide behavioral detection layer.	Implemented
SI-4	**System Monitoring**	Cloud monitoring added: CloudWatch Agent (AWS), GCP Cloud Monitoring Ops Agent, Azure Monitor VM metric alert rules (7 active); Checkmk agent on all 6 cloud nodes; Uptime Kuma monitors Tailscale tunnel health.	Implemented
SR-3	**Supply Chain Controls**	Cloud supply chain controls added: AWS IAM instance profiles (least-privilege, no long-lived keys on EC2); GCP service accounts (minimal roles, no	Partial

	owner/editor on Compute); Azure VMs provisioned via ARM template with securestring parameters; all nodes enrolled in same on-premises management stack.		

Overview

324+ individual requirements across 18 control families. Strong compliance in technical families (AC, AU, IA, SC, SI) at 85%+ implementation. Version 2.0 integrates cloud workload coverage across AWS, GCP, and Azure: 6 nodes total connected via Tailscale WireGuard mesh VPN. Cloud-native security services (GuardDuty, Security Command Center, Defender for Cloud/Sentinel) augment on-premises controls across all relevant families.

Overall Maturity: High (Technical Controls) / Moderate (Administrative Controls)

Maturity Assessment by Control Family

Tier	Families	Rationale
Tier 4 (Adaptive)	AU, IA, SI, CM	Automated correlation, PKI automation, multi-layered detection including NSM and cloud-native tools, IaC drift detection
Tier 3 (Defined)	AC, IR, RA, SC	Documented policies, centralized enforcement, behavioral monitoring, cloud boundary protection, IPSec/PA-VM additions
Tier 2 (Managed)	CP, CA, MA	Scheduled scanning, restore testing, change control
N/A	PE, PS, PM, PL, MP	Constrained by single-user homelab context

Control Family Implementation Detail

Access Control (AC): 90% Compliant (27/30 Implemented)

AC-1	Policy and Procedures: Lab mission statement defines security-first architecture; documented access control requirements.	**Implemented**	
AC-2	Account Management: Authentik user lifecycle management; SSH individual user accounts; Wazuh tracks active sessions; no shared credentials.	**Implemented**	Cloud: Linux cloud node accounts managed via Ansible SSH key distribution; Windows cloud nodes managed via Active Directory (domain-joined over Tailscale); cloud IAM service accounts inventoried with minimal role assignments.

AC-2(1)	Automated System Account Management: Authentik automated provisioning/deprovisioning.	**Implemented**	
AC-2(3)	Disable Accounts: Authentik automated account disabling after 90 days inactivity.	**Partial**	Cloud: AWS IAM access keys reviewed quarterly (no long-lived keys on EC2); GCP IAM recommender audits service accounts; Azure Entra ID 45-day dormancy policy applied.
AC-2(4)	Automated Audit Actions: SIEM tracks all account creation/modification/deletion.	**Implemented**	Cloud: CloudTrail, GCP Admin Activity, Azure Activity Log capture all cloud IAM events.
AC-2(5)	Inactivity Logout: Authentik 30-min idle timeout; SSH ClientAliveInterval=300.	**Implemented**	
AC-2(7)	Privileged User Accounts: Separate admin accounts; monitored via SIEM; MFA enforced.	**Implemented**	Cloud: AWS IAM instance profiles scoped to minimum required actions; GCP service accounts use minimal roles; Azure subscription admin access MFA-enforced via Entra Conditional Access.
AC-2(12)	Account Monitoring Atypical Usage: Splunk behavioral analysis; unusual login times/geoIP tracking.	**Partial**	Cloud: Azure Sentinel KQL rule detects sign-in from new geographic location; GuardDuty CredentialAccess findings; GCP SCC IAM anomaly detection.
AC-2(13)	Disable High-Risk Accounts: Wazuh Active Response disables compromised accounts.	**Implemented**	Cloud: Wazuh Active Response (disable-account) executes on cloud nodes via Tailscale using same playbooks as on-premises.
AC-3	Access Enforcement: Authentik/AD RBAC groups; SSH sudo enforcement; Traefik middleware access control.	**Implemented**	Cloud: Tailscale ACL policy enforces per-device/per-subnet explicit allow rules (default deny); Palo Alto User-ID AD group enforcement extended to cloud-adjacent resources.
AC-3(7)	Role-Based Access Control: Authentik groups map to	**Implemented**	

	application permissions; AD OUs for Windows.		
AC-3(8)	Revocation of Access: Centralized SSH key revocation via Ansible; Authentik account deactivation.	**Implemented**	Cloud: Tailscale node key revocation; AWS IAM role disassociation; GCP service account removal; Azure Entra ID account deactivation: all documented in decommissioning runbook.
AC-6	Least Privilege: SSH sudo policies; Authentik role-based permissions; minimal access granted.	**Implemented**	Cloud: AWS IAM instance profiles (no wildcard actions); GCP minimal role assignments (no owner/editor on Compute); Azure RBAC scoped per resource group.
AC-6(1)	Authorize Access to Security Functions: Security tool access restricted to SOC role; documented in Authentik.	**Implemented**	
AC-6(2)	Non-Privileged Access for Non-Security Functions: Standard user accounts for daily operations.	**Implemented**	
AC-6(5)	Privileged Accounts: Separate privileged accounts; monitored; MFA enforced.	**Implemented**	
AC-6(9)	Log Use of Privileged Functions: All sudo commands logged to SIEM; Windows privileged operations audited.	**Implemented**	Cloud: cloud console admin actions logged via CloudTrail, GCP Audit Logs, Azure Activity Log.
AC-7	Unsuccessful Logon Attempts: SSH MaxAuthTries=5; Authentik lockout after 5 failures; Wazuh active-response.	**Implemented**	
AC-8	System Use Notification: SSH banner configured; Authentik login notice.	**Implemented**	
AC-12	Session Termination: Authentik session timeout; SSH automatic disconnect.	**Implemented**	
AC-17	Remote Access: SSH hardening; IP restrictions (firewall + Traefik);	**Implemented**	Cloud: SSH (Linux) and RDP (Windows) restricted to homelab

	MFA for admin access; Tailscale VPN.		subnets (192.168.0.0/16) via AWS Security Groups, GCP VPC firewall policy, Azure NSG; all access via Tailscale WireGuard: no public management ports on any cloud instance.
AC-17(1)	Monitoring and Control: VPN connections logged; SSH sessions monitored; Traefik access logs.	**Implemented**	Cloud: Tailscale tunnel telemetry; cloud provider flow logs (VPC flow logs, NSG flow logs) supplement on-premises monitoring.
AC-17(2)	Protection via Encryption: SSH AES-256-GCM; TLS 1.3 (Traefik); Tailscale WireGuard.	**Implemented**	Cloud: all cloud management traffic via Tailscale WireGuard (ChaCha20-Poly1305); no plaintext management paths.
AC-17(4)	Privileged Commands via Remote Access: Privileged SSH sessions logged separately; sudo usage tracked.	**Implemented**	
AC-17(9)	Disconnect or Disable Access: Remote access can be disabled via firewall rules; Tailscale ACLs.	**Partial**	Cloud: Tailscale node key revocation immediately removes cloud node access; provider-native security group/NSG modification available for emergency lockout.
AC-17(10)	Authenticate Remote Commands: SSH key-based authentication; command verification via logging.	**Implemented**	

Audit and Accountability (AU): 100% Compliant (18/18 Implemented)

AU-1	Policy and Procedures: Comprehensive logging policy documented; 100% security event coverage requirement.	**Implemented**	Cloud: cloud audit logging policy extended to AWS CloudTrail, GCP Admin Activity, Azure Activity Log with 90-day retention requirement.
AU-2	Event Logging: DNS queries, SSH sessions, Traefik requests, patch events, scan activity, Wazuh events logged.	**Implemented**	Cloud: AWS CloudTrail (all management events to S3 with SSE); GCP Admin Activity logs (always-on) and Data Access audit logs; Azure Activity Log and Monitor; Wazuh agents on all 6 cloud nodes forward endpoint

			security events to on-premises Splunk.
AU-3	Content of Audit Records: Logs include: timestamp, user, source IP, action, result; Wazuh includes file hashes, process trees.	**Implemented**	Cloud: CloudTrail includes IAM identity, source IP, user agent, request/response detail; GCP audit logs include principal identity, resource, method, source IP; Azure Activity Log includes caller identity, resource, operation.
AU-3(1)	Additional Audit Information: SSH key fingerprints, DNS query details, Traefik request/response, Sysmon process telemetry.	**Implemented**	
AU-4	Audit Log Storage Capacity: 90-day retention; auto-archival to cold storage; capacity monitoring via Prometheus.	**Implemented**	Cloud: AWS S3 lifecycle policy (90-day); GCP Cloud Logging retention per GCP defaults (400 days for admin activity); Azure Log Analytics homelab-log 90-day retention.
AU-5	Response to Audit Logging Process Failures: SIEM alerts on logging failures; redundant log paths (local + remote).	**Implemented**	Cloud: Azure Sentinel AMA data gap detection rule alerts when cloud agent heartbeat absent for 15+ minutes.
AU-5(1)	Storage Capacity Warning: Prometheus/alerts at 80% capacity; automated archival triggers.	**Implemented**	
AU-5(2)	Real-Time Alerts: Splunk/Elastic real-time correlation; Wazuh instant alerts; sub-60s notification latency.	**Implemented**	
AU-6	Audit Record Review: Splunk/Elastic dashboards (DNS/SSH/Traefik); automated correlation; vulnerability trending.	**Implemented**	Cloud: CloudWatch Alarms (AWS), GCP Cloud Monitoring alerting policies, Azure Monitor alert rules (7 active VM metric alerts); all feed Discord/email notification channels.
AU-6(1)	Automated Process Integration: SIEM correlation across Splunk/Elastic/Wazuh; TheHive case aggregation; n8n/Shuffle workflows.	**Implemented**	

AU-6(3)	Correlate Audit Record Repositories: Multi-source correlation: Splunk + Elastic + Wazuh + network logs; unified timeline analysis.	**Implemented**	Cloud: Wazuh agents on all 6 cloud nodes forward endpoint events to on-premises Splunk for unified cross-environment correlation.
AU-6(5)	Integrated Analysis: Cortex multi-engine analysis; MISP threat intelligence; Shuffle enrichment pipelines.	**Implemented**	
AU-7	Audit Record Reduction: Splunk SPL queries; Elastic KQL; Wazuh filters; automated report generation.	**Implemented**	
AU-7(1)	Automatic Processing: Scheduled Splunk searches; Elastic detection rules; automated dashboards.	**Implemented**	
AU-9	Protection of Audit Information: Logs forwarded to immutable SIEM; Splunk read-only indexes; syslog-ng TLS encryption.	**Implemented**	Cloud: AWS S3 CloudTrail bucket with SSE; GCP Admin Activity logs (cannot be disabled); Azure Log Analytics immutable data retention.
AU-11	Audit Record Retention: 90-day hot retention; 1-year cold storage; automated lifecycle management.	**Implemented**	Cloud: all cloud audit sources maintain 90-day minimum retention matching on-premises SIEM policy.
AU-12	Audit Record Generation: Universal Forwarders (30+ hosts); Elastic Agents; Wazuh agents (31+ including 6 cloud); structured JSON format.	**Implemented**	Cloud: Wazuh agents on all 6 cloud nodes; AWS CloudTrail; GCP Audit Logs; Azure Monitor all feed on-premises Splunk indexer.
AU-12(1)	System-Wide Audit Trail: Centralized logging across all infrastructure; time-correlated via NTP (SC-45).	**Implemented**	Cloud: cloud nodes NTP-synced (time.google.com, time.cloudflare.com via Ansible) ensuring consistent timestamps across on-premises and cloud audit trails.
AU-12(2)	Standardized Formats: JSON/CEF formats; normalized in SIEM; CIM-compliant (Splunk).	**Implemented**	

Assessment, Authorization, and Monitoring (CA): 80% Compliant (8/10 Implemented)

CA-1	Policy and Procedures: Assessment and authorization policy documented; continuous monitoring strategy defined.	**Implemented**	
CA-2	Control Assessments: Weekly OpenVAS scans; monthly Nessus authenticated scans; CIS Benchmark audits; Wazuh SCA.	**Implemented**	Cloud: Wazuh CIS SCA on all 6 cloud nodes daily; AWS Inspector, GCP SCC vulnerability assessment, Azure Defender for Cloud recommendations provide supplemental cloud-native assessment.
CA-2(1)	Independent Assessors: N/A: Single user homelab.	**N/A**	
CA-3	Information Exchange: Documented interconnections; firewall rules for external connections.	**Partial**	Cloud: Tailscale mesh topology documented; VPC/VNet CIDR allocations and subnet router configurations documented.
CA-5	Plan of Action and Milestones: Vulnerability tracking in TheHive; remediation SLAs documented.	**Partial**	Cloud: cloud node findings tracked in same TheHive instance as on-premises; Critical less than 72h, High less than 7d MTTR SLAs apply to cloud scope.
CA-6	Authorization: N/A: Single user homelab.	**N/A**	
CA-7	Continuous Monitoring: Automated vulnerability scanning; real-time patch status; security posture dashboards; Wazuh real-time FIM.	**Implemented**	Cloud: AWS GuardDuty (VPC flow, CloudTrail, DNS: real-time ML detection), GCP SCC (asset inventory, vulnerability assessment, network IDS endpoint), Azure Defender for Cloud (CSPM Secure Score) and Sentinel (KQL detection rules, automated response); all integrated with on-premises SIEM via Wazuh agent telemetry.
CA-7(1)	Independent Assessment: N/A: Single user homelab.	**N/A**	
CA-7(3)	Trend Analyses: Grafana dashboards track vulnerability trends over time.	**Implemented**	Cloud: PatchMon cloud patch compliance trending; AWS Security Hub score trending; GCP SCC

			findings trend; Azure Defender Secure Score monitored.
CA-8	Penetration Testing: Informal testing: scanning, enumeration, vulnerability assessments.	**Partial**	
CA-9	Internal System Connections: Network diagram documents internal connections; firewall rules enforce segmentation.	**Implemented**	Cloud: Tailscale mesh routing tables, VPC/VNet topology, and cloud-to-on-premises routing documented.

Configuration Management (CM): 95% Compliant (15/16 Implemented)

CM-1	Policy and Procedures: Configuration management policy documented; IaC standards defined.	**Implemented**	
CM-2	Baseline Configuration: Ansible playbooks define baselines; PatchMon baseline tracking; CIS Benchmark baselines audited via Nessus.	**Implemented**	Cloud: Ansible linux_hardening.yml and new_install_baseline_roles.yml applied to all 4 Linux cloud nodes; Windows cloud nodes managed via GPO (domain-joined); Azure ARM template version-controlled in Git.
CM-2(2)	Automation Support: Ansible automation; Terraform IaC; automated baseline verification.	**Implemented**	Cloud: Terraform manages AWS Security Groups, GCP VPC firewall policy, Azure NSG rules as IaC; Git commit required for all cloud network changes.
CM-2(3)	Retention of Previous Configurations: Git version control; snapshot-before-patch; configuration history retained.	**Implemented**	Cloud: cloud infrastructure change history in CloudTrail, GCP Audit Logs, Azure Activity Log; Terraform state versioned.
CM-3	Configuration Change Control: Snapshot-before-patch; WSUS approval workflows; pre-scan snapshots; Git pull requests.	**Implemented**	Cloud: Terraform plan review required before cloud infrastructure changes; ARM template parameter validation before Azure deployment; no ad-hoc console changes.
CM-3(2)	Testing and Validation: WSUS test deployments; Ansible dry-run; patch validation before production.	**Implemented**	Cloud: Wazuh SCA post-rebuild validates CIS baseline compliance for cloud nodes; cloud node rebuild timing validated against RTO target.

CM-5	Access Restrictions for Change: Ansible playbook execution restricted; WSUS approval required; Git branch protection.	**Implemented**	
CM-6	Configuration Settings: CIS Benchmark compliance audits; hardened SSH/Traefik configs; configuration deviations detected.	**Implemented**	Cloud: Wazuh SCA applies CIS benchmarks (CIS Amazon Linux, Debian 12/13, Ubuntu 22.04/24.04, Windows Server 2025) to all 6 cloud nodes daily.
CM-6(1)	Automated Management: Ansible automation; configuration drift detection; automated remediation.	**Implemented**	Cloud: Ansible drift detection runs against cloud nodes via Tailscale SSH; non-compliant findings trigger Discord alerts.
CM-7	Least Functionality: Unnecessary services disabled; verified via authenticated Nessus scans.	**Implemented**	Cloud: cloud nodes provisioned with minimal base images; Wazuh SCA validates running services against CIS benchmarks on all 6 cloud nodes.
CM-8	System Component Inventory: PatchMon (5,000+ packages, 30+ hosts); WUD (50+ containers); OpenVAS/Nessus asset databases; Wazuh agent inventory; NetAlert Inventory.	**Implemented**	Cloud: 6 cloud nodes across AWS, GCP, Azure tracked in PatchMon, Wazuh (31+ agents), Checkmk, and Tailscale admin console (tailf07c05.ts.net). Per-provider instance IDs documented.
CM-8(1)	Updates During Install/Removal: Inventory updated automatically and manually; Wazuh tracks software changes.	**Implemented**	
CM-8(2)	Automated Maintenance: PatchMon daily updates; WUD container tracking; automated inventory reconciliation.	**Implemented**	
CM-8(3)	Automated Unauthorized Component Detection: Nessus compliance scans detect unauthorized software; Wazuh FIM alerts on new executables; NetAlert new device notifications.	**Implemented**	
CM-9	Configuration Management Plan: IaC strategy documented; Ansible	**Partial**	

	playbook standards; Git workflow defined.		
CM-14	Signed Components: Docker image signature verification (SHA-256); Step-CA signed certificates.	**Implemented**	

Contingency Planning (CP): 75% Compliant (6/8 Implemented)

CP-1	Policy and Procedures: Backup procedures documented; failover strategies defined.	**Partial**	
CP-9	System Backup: Proxmox automated backups bi-weekly; encrypted backups; dual backup solutions.	**Implemented**	Cloud: AWS EBS snapshots (encrypted); GCP disk snapshots (encrypted at rest); Azure VM snapshots (encrypted); cloud node rebuild from Git + Ansible provides IaC recovery path. Cloud node RTO less than 2 hours validated.
CP-9(1)	Testing for Reliability: Quarterly restore testing documented.	**Implemented**	Cloud: Azure Spot instance eviction/restart scenario tested; cloud node Ansible rebuild timing validated.
CP-9(3)	Separate Storage: Off-host encrypted backups; physically separate storage.	**Implemented**	
CP-9(8)	Cryptographic Protection: Encrypted backups via Proxmox Backup Server.	**Implemented**	Cloud: AWS S3 SSE; GCP persistent disk default encryption; Azure Managed Disk encryption.
CP-10	System Recovery: Documented restore procedures; IaC enables rapid rebuild.	**Partial**	Cloud: cloud node rebuild runbooks (Tailscale enrollment, Wazuh agent reinstallation, Ansible baseline) documented and tested.

Identification and Authentication (IA): 95% Compliant (17/18 Implemented)

IA-1	Policy and Procedures: Authentication policy documented; MFA requirements defined.	**Implemented**	
IA-2	Identification and Authentication: SSH keys; Authentik SSO; unique user identities required.	**Implemented**	Cloud: Linux cloud nodes use SSH Ed25519 key-based authentication (passwords disabled globally via Ansible). Windows cloud nodes (AWS Windows Server 2025, Azure

			Windows Server 2025) domain-joined to home.com via Tailscale: Kerberos authentication, Group Policy, and WSUS extended to cloud.
IA-2(1)	MFA to Privileged Accounts: Authentik TOTP enforced for all admin accounts; SSH key + passphrase.	**Implemented**	Cloud: AWS console MFA enforced via IAM policy; GCP console requires Google MFA; Azure admin access enforced via Entra Conditional Access.
IA-2(2)	MFA to Non-Privileged Accounts: Authentik TOTP available; SSH keys only (equivalent to 2FA).	**Implemented**	
IA-2(8)	Replay Resistant: SSH session tokens; Authentik session cookies with CSRF protection.	**Implemented**	
IA-2(10)	Single Sign-On: Authentik SSO integration; Traefik ForwardAuth; OAuth2 provider.	**Implemented**	
IA-3	Device Identification: SSH host keys; device certificates via Step-CA.	**Implemented**	Cloud: all 6 cloud nodes enrolled in Tailscale tailnet (tailf07c05.ts.net) with device-bound WireGuard keys serving as cryptographic device identifiers; Wazuh agent IDs provide device identity in SIEM.
IA-4	Identifier Management: Centralized user management via Authentik/AD; SSH keys tracked in Ansible.	**Implemented**	Cloud: AWS IAM instance profiles, GCP service accounts, Azure Managed Identity inventoried; cloud node local user accounts tracked via Wazuh agent inventory.
IA-5	Authenticator Management: SSH keys managed via Ansible; Authentik credential policies; centralized key distribution.	**Implemented**	Cloud: SSH key distribution to cloud nodes via Ansible new_install_baseline_roles.yml; quarterly key rotation playbook.
IA-5(1)	Password-Based Authentication: SSH passwords disabled globally; Authentik enforces complexity requirements.	**Implemented**	
IA-5(2)	PKI-Based Authentication: Step-CA two-tier PKI; SSH Ed25519 keys; automated certificate issuance.	**Implemented**	

IA-5(7)	No Embedded Unencrypted Authenticators: Vaultwarden secrets management; Ansible Vault encrypted vars; no hardcoded credentials.	**Implemented**	Cloud: no credentials embedded in cloud node configurations; Ansible Vault protects all cloud node credentials; cloud IAM uses instance profiles/service accounts (no hardcoded keys).
IA-5(14)	Managing PKI Trust Stores: Step-CA root/intermediate CA management; automated trust distribution.	**Implemented**	
IA-5(18)	Password Managers: Vaultwarden deployed; biometric unlock; zero-knowledge encryption.	**Implemented**	
IA-11	Re-authentication: Authentik session timeout requires re-auth; SSH session timeout.	**Implemented**	

Incident Response (IR): 90% Compliant (11/13 Implemented)

IR-1	Policy and Procedures: Incident response policy documented; SOC procedures defined.	**Implemented**	
IR-4	Incident Handling: TheHive case management; Wazuh Active Response; Splunk correlation; n8n/Shuffle SOAR orchestration.	**Implemented**	Cloud: Wazuh Active Response (firewall-drop, host-deny, account-disable) executes on cloud nodes via Tailscale. AWS GuardDuty and Azure Sentinel incidents auto-create TheHive cases via Shuffle SOAR webhook. GCP SCC findings trigger alerting policy notifications.
IR-4(1)	Automated Incident Handling: Wazuh Active Response (firewall-drop, host-deny); VirusTotal quarantine; Shuffle workflows; sub-30-min MTTR.	**Implemented**	
IR-4(4)	Information Correlation: TheHive correlates Splunk/Wazuh/Suricata/scanners; Cortex enrichment; MISP threat context.	**Implemented**	Cloud: cloud node Wazuh agent telemetry included in TheHive case correlation; GuardDuty finding types mapped to MITRE ATT&CK in Shuffle SOAR workflow.
IR-5	Incident Monitoring: Real-time SIEM dashboards; Discord notifications;	**Implemented**	

	TheHive case tracking; 100% security event visibility.		
IR-5(1)	Automated Tracking: TheHive automated case creation; Shuffle orchestration; Cortex job tracking; Wazuh forensic data collection.	**Implemented**	
IR-6	Incident Reporting: TheHive case documentation; Shuffle notifications; Discord/email alerting; Splunk executive reports.	**Implemented**	
IR-6(1)	Automated Reporting: Shuffle automated notifications (Discord, email, PagerDuty); TheHive status updates; Splunk scheduled reports.	**Implemented**	
IR-7	Incident Response Assistance: TheHive knowledge base; documented playbooks (15+); Shuffle workflow library; Cortex analyzer catalog.	**Implemented**	Cloud: cloud node IR runbooks (Tailscale containment, Security Group/NSG modification, Wazuh Active Response) documented.
IR-8	Incident Response Plan: Comprehensive IR plan; TheHive playbooks; Shuffle workflows; multi-channel alerting.	**Implemented**	
IR-8(1)	Breaches: Limited: Wazuh automated alerting and active response; TheHive automated case creation.	**Partial**	

Maintenance (MA): 60% Compliant (4/6 Implemented)

MA-1	Policy and Procedures: Maintenance policy informal: personal lab environment.	**Partial**	
MA-2	Controlled Maintenance: Change control via Git; snapshot-before-patch.	**Partial**	
MA-3	Maintenance Tools: Ansible automation tools version controlled.	**Partial**	
MA-4	Nonlocal Maintenance: SSH remote maintenance logged; session monitoring.	**Implemented**	Cloud: all cloud node maintenance via SSH over Tailscale with session logging; Windows cloud node maintenance via RDP over

			Tailscale; all maintenance actions logged via CloudTrail/GCP Audit Logs/Azure Activity Log.
MA-4(6)	Cryptographic Protection: SSH encryption for remote maintenance; TLS for web-based tools.	**Implemented**	Cloud: all cloud maintenance traffic encrypted via Tailscale WireGuard (ChaCha20-Poly1305).
MA-6	Timely Maintenance: Patch SLAs defined and tracked.	**Partial**	Cloud: same Critical less than 72h, High less than 7d MTTR SLAs applied to cloud nodes; PatchMon dashboard tracks cloud patch compliance.

Media Protection (MP): 40% Compliant

MP-4	Media Storage: Backup media stored securely; encrypted.	**Implemented**	
MP-7	Media Use: Removable media disabled via GPO (Windows).	**Partial**	

Physical and Environmental Protection (PE): N/A (Residential Homelab)

PE-9	Power Equipment and Cabling: UPS battery backup for critical systems.	**N/A**	Cloud: physical infrastructure managed by cloud provider (AWS, GCP, Azure maintain SOC 2 certified data centers).
PE-11	Emergency Power: UPS provides temporary power.	**N/A**	

Planning (PL): 60% Compliant

PL-2	System Security Plans: GRC documentation serves as security plan.	**Implemented**	
PL-8	Security Architecture: Defense-in-depth architecture documented; network diagrams maintained.	**Implemented**	Cloud: multi-cloud hybrid architecture documented in GRC documents; Tailscale mesh topology, VPC/VNet diagrams, and routing tables maintained.
PL-8(1)	Defense in Depth: Multi-layer security controls across network/application/data layers.	**Implemented**	

Program Management (PM): 40% Compliant

PM-5	System Inventory: Comprehensive asset inventory maintained	**Implemented**	Cloud: 6 cloud nodes tracked in PatchMon, Wazuh (31+ agents),

	(PatchMon, Wazuh, OpenVAS, Nessus, NetAlert).		Checkmk, and Tailscale admin console.
PM-9	Risk Management Strategy: Risk-based vulnerability prioritization; CVSS scoring.	**Implemented**	
PM-16(1)	Automated Threat Intelligence Sharing: MISP automated feed synchronization; Shuffle vulnerability aggregation.	**Implemented**	Cloud: AWS GuardDuty, GCP SCC, Azure Sentinel findings available to MISP for IOC correlation.

Risk Assessment (RA): 85% Compliant (10/12 Implemented)

RA-1	Policy and Procedures: Risk assessment policy documented; CVSS scoring methodology defined.	**Implemented**	
RA-3	Risk Assessment: CVSS scoring of vulnerabilities; exploit likelihood assessment; risk-based remediation prioritization.	**Implemented**	Cloud: same CVSS-based risk assessment applied to cloud node findings from PatchMon, AWS Inspector, GCP SCC, Azure Defender for Cloud.
RA-3(1)	Supply Chain Risk Assessment: MISP vendor compromise tracking; limited supply chain visibility.	**Partial**	Cloud: AWS IAM instance profiles (no long-lived keys), GCP minimal service account roles, Azure securestring ARM parameters reduce supply chain risk on cloud nodes.
RA-5	Vulnerability Monitoring and Scanning: Weekly OpenVAS network scans; monthly Nessus authenticated scans; daily PatchMon package checks; CVE correlation with NVD.	**Implemented**	Cloud: Wazuh CIS SCA and vulnerability assessment on all 6 cloud nodes daily; PatchMon CVE correlation for 4 Linux cloud nodes; AWS Inspector EC2 agent-based assessment; GCP SCC vulnerability findings for Compute instances; Azure Defender for Cloud recommendations for Azure VMs.
RA-5(2)	Update Vulnerabilities to Be Scanned: Daily NVT updates (OpenVAS); plugin updates (Nessus); MISP feed sync; Shuffle CVE aggregation.	**Implemented**	

RA-5(3)	Breadth and Depth of Coverage: Network scans (OpenVAS); authenticated OS scans (Nessus); compliance audits (CIS); 75+ assets covered.	**Implemented**	Cloud: cloud nodes added to asset count; provider-native tools supplement on-premises scans.
RA-5(5)	Privileged Access: Authenticated scans via SSH keys (Linux); domain service accounts (Windows); SNMP v3 (network devices).	**Implemented**	Cloud: Wazuh agents provide authenticated host-level visibility on all cloud nodes without network credentials.
RA-5(8)	Review Historic Audit Logs: Vulnerability trends tracked in Grafana; historical scan results archived; MTTR calculated over time.	**Implemented**	
RA-5(10)	Correlate Scanning Information: SIEM correlates vulnerability scans with exploit databases; Wazuh links vulnerabilities to installed software.	**Implemented**	
RA-10	Threat Hunting: Wazuh threat hunting queries; Splunk investigation searches; MITRE ATT&CK mapping.	**Implemented**	

System and Communications Protection (SC): 95% Compliant (24/25 Implemented)

SC-7	Boundary Protection: DNS at edge (Unbound); SSH firewall rules; Traefik ingress controller; pfSense ACLs; IDS/IPS.	**Implemented**	Cloud: AWS Security Groups (tailscale-access + lab-services, default-deny), GCP VPC network firewall policy homelab (17 rules, Google Threat Intelligence blocking: TOR exit nodes, malicious IPs, sanctioned countries at priority 100-130), Azure NSG homelab-nsg2 (explicit allow-list with DenyAllInBound at priority 65500). GCP Cloud Armor three-tier WAF/DDoS policies (edge, backend, application-level with SQLi/XSS blocking via v33-stable expression sets). Azure DDoS Protection plan homelab-ddos.
SC-7(3)	Access Points: Managed access points via Traefik/Nginx Ingress;	**Implemented**	

	SafeLine WAF; Cloudflare/Tailscale RBAC.		
SC-7(4)	External Telecommunications: Verizon; VPN services (Tailscale, PIA); Cloudflare Tunnels.	**Implemented**	
SC-7(5)	Deny by Default / Allow by Exception: pfSense/OPNsense default-deny rules; Traefik explicit route definitions; firewall whitelist approach.	**Implemented**	Cloud: AWS Security Groups default-deny; GCP VPC firewall policy default pass with explicit deny rules for threat intelligence; Azure NSG DenyAllInBound default; Tailscale ACL default-deny.
SC-7(8)	Route Traffic to Authenticated Proxy: Traefik reverse proxy with Authentik authentication.	**Implemented**	
SC-7(21)	Isolation of System Components: Traefik isolates backend services; NGINX Ingress isolates K3s pods; network segmentation.	**Implemented**	Cloud: per-provider VPC/VNet isolation (AWS 172.31.0.0/16, GCP 10.128.0.0/16, Azure 10.130.0.0/16); inter-cloud communication only via Tailscale overlay with ACL enforcement.
SC-8	Transmission Confidentiality and Integrity: TLS 1.3 (Traefik); SSH encryption; DNS-over-TLS (future); encrypted scan credentials.	**Implemented**	Cloud: all cloud management traffic via Tailscale WireGuard (ChaCha20-Poly1305); SSH AES-256-GCM for Linux cloud node terminal access; RDP over Tailscale tunnel for Windows nodes; cloud VPC/VNet internal traffic uses provider-encrypted private networking.
SC-8(1)	Cryptographic Protection: AES-256-GCM (SSH/Traefik); Ed25519 keys; TLS 1.3 ciphersuites.	**Implemented**	Cloud: Tailscale WireGuard (ChaCha20-Poly1305); AWS S3 SSE (SSE-S3); GCP persistent disk and GCS default encryption; Azure Managed Disk and Log Analytics workspace encrypted at rest.
SC-12	Cryptographic Key Establishment and Management: Step-CA automated certificate issuance; SSH key generation (ed25519); centralized key management.	**Implemented**	
SC-13	Cryptographic Protection: Modern algorithms only (Ed25519, AES-256-	**Implemented**	

	GCM, TLS 1.3); weak cipher detection via vulnerability scans.		
SC-17	Public Key Infrastructure Certificates: Step-CA PKI (Root + Intermediate CA); Traefik cert distribution; automated renewal.	**Implemented**	
SC-17(1)	Certificate Validation: OCSP validation; CRL distribution; client certificate validation.	**Implemented**	
SC-20	Secure Name/Address Resolution (Authoritative): Technitium DNS authoritative DNS; DNSSEC signing.	**Implemented**	Cloud: all cloud nodes resolve via on-premises Unbound (192.168.1.153/154) over Tailscale with DNSSEC validation and malware domain blocking.
SC-21	Secure Name/Address Resolution (Recursive): Unbound recursive resolver; DNSSEC validation enabled.	**Implemented**	
SC-23	Session Authenticity: Authentik session tokens; SSH session IDs; TLS session tickets.	**Implemented**	
SC-28	Protection of Information at Rest: Encrypted backups; TLS in transit; scan credential encryption; SSH private keys encrypted.	**Implemented**	Cloud: AWS S3 SSE; GCP persistent disk and GCS default encryption; Azure Managed Disk and Log Analytics workspace encrypted at rest.
SC-28(1)	Cryptographic Protection at Rest: AES-256 encrypted backups.	**Partial**	
SC-28(3)	Cryptographic Keys: Step-CA offline root CA; SSH keys encrypted; Vaultwarden secrets management.	**Implemented**	
SC-39	Process Isolation: Container isolation (Docker); VM isolation (Proxmox); process separation.	**Implemented**	
SC-45	System Time Synchronization: NTP time synchronization across infrastructure; centralized time source.	**Implemented**	Cloud: all 4 Linux cloud nodes configured with NTP (time.google.com, time.cloudflare.com) via Ansible; Windows cloud nodes sync via domain NTP policy over Tailscale.

SC-45(1)	Synchronization with Authoritative Time Source: Chrony NTP client; Internet time servers (pool.ntp.org).	**Implemented**	

System and Information Integrity (SI): 90% Compliant (25/28 Implemented)

SI-2	Flaw Remediation: Multi-platform patch management; MTTR less than 72h for Critical CVEs; remediation verified via re-scans.	**Implemented**	Cloud: same MTTR SLAs (Critical less than 72h, High less than 7d) applied to cloud nodes; PatchMon tracks cloud Linux node CVEs; WSUS manages Windows cloud nodes; Ansible update_linux_hosts.yml provides emergency patching via Tailscale.
SI-2(2)	Automated Flaw Remediation Status: Watchtower auto-updates; WSUS auto-approval rules; n8n orchestration; Wazuh alerts on unpatched systems.	**Implemented**	
SI-2(4)	Automated Patch Management Tools: PatchMon (Linux); WSUS (Windows); Watchtower (containers); OpenVAS/Nessus verification.	**Implemented**	Cloud: PatchMon on 4 Linux cloud nodes; WSUS on 2 Windows cloud nodes; Wazuh vulnerability assessment on all 6 cloud nodes.
SI-2(6)	Removal of Previous Versions: Old container images pruned after Watchtower updates; superseded patches cleaned via WSUS.	**Implemented**	
SI-3	Malicious Code Protection: Wazuh FIM with VirusTotal; Suricata/Snort signatures; ClamAV/Microsoft Defender; rootkit detection.	**Implemented**	Cloud: Wazuh FIM and rootkit detection on all 6 cloud nodes; Microsoft Defender active on Windows Server 2025 (AWS and Azure); ClamAV freshclam on all 4 Linux cloud nodes; AWS GuardDuty ML-based behavioral detection, GCP SCC threat detection, Azure Defender for Cloud behavioral analytics provide cloud-native malware detection layer.
SI-3(4)	Updates Only by Privileged Users: AV signature updates restricted to admin accounts; WSUS authorization.	**Implemented**	

SI-3(10)	Malicious Code Analysis: Cortex multi-engine analysis (VirusTotal, Yara); Shuffle malware workflow; TheHive case management.	**Implemented**	
SI-4	System Monitoring: Prometheus; Uptime Kuma; Splunk/Elastic SIEM; Wazuh EDR; Suricata/Snort IDS; NetAlert; multi-layered detection.	**Implemented**	Cloud: AWS CloudWatch Agent (CPU, memory, disk, network per EC2 instance) and GuardDuty behavioral detection; GCP Cloud Monitoring Ops Agent and SCC threat detection and VPC network IDS endpoint; Azure Monitor VM metric alert rules (7 active: Available Memory Bytes, Data Disk IOPS, Network In/Out, OS Disk IOPS, Percentage CPU, VM Availability) and Sentinel KQL detection rules; all 6 cloud nodes enrolled in Checkmk on-premises dashboard; Uptime Kuma monitors Tailscale tunnel health.
SI-4(1)	System-Wide Intrusion Detection: Suricata/Snort on all network segments; centralized SIEM correlation.	**Implemented**	
SI-4(2)	Automated Tools for Real-Time Analysis: Splunk real-time correlation; Wazuh real-time FIM; Elastic SIEM; Suricata inline blocking; Cortex automation.	**Implemented**	
SI-4(4)	Inbound and Outbound Communications Traffic: Suricata/Snort IDS on all segments; pfSense flow logs; Traefik access logs; DNS query logging; complete visibility.	**Implemented**	Cloud: AWS VPC flow logs (fl-03179f74e54bf1aa4, CloudWatch Logs); GCP VPC flow logs (default network, Flow Analyzer); Azure NSG flow logs (Network Watcher homelab-nsg2); Tailscale tunnel telemetry for all cloud-to-on-premises paths.
SI-4(5)	System-Generated Alerts: Discord webhooks; Splunk scheduled alerts; Wazuh Discord/email; Prometheus Alertmanager; CVSS-based routing.	**Implemented**	

SI-4(12)	Automated Alerts: Prometheus Alertmanager; Grafana automated alerts; Splunk real-time searches; Wazuh Active Response triggers.	**Implemented**	
SI-4(16)	Correlate Monitoring Information: Multi-source correlation across Splunk/Elastic/Wazuh/network logs; TheHive aggregation.	**Implemented**	Cloud: cloud node Wazuh agent telemetry included in on-premises Splunk SPL correlation searches; GuardDuty and Sentinel findings auto-create TheHive cases via Shuffle SOAR for unified case management.
SI-4(18)	Analyze Traffic/Event Patterns: Cortex pattern recognition; MISP campaign correlation.	**Partial**	
SI-4(23)	Host-Based Devices: Wazuh EDR on 25+ on-premises endpoints; FIM real-time monitoring; rootkit detection; process monitoring; Sysmon integration.	**Implemented**	Cloud: Wazuh EDR deployed on all 6 cloud nodes with same FIM, rootkit detection, process monitoring, and CIS SCA configuration as on-premises (31+ total agents).
SI-5	Security Alerts, Advisories, and Directives: PatchMon CVE alerts; WUD update notifications; Discord webhooks; OpenVAS/Nessus scan completion alerts.	**Implemented**	
SI-5(1)	Automated Alerts and Advisories: Discord webhooks for scan completion; CVSS-based alert routing; TheHive case auto-creation.	**Implemented**	
SI-7	Software, Firmware, and Information Integrity: Docker image SHA-256 verification; Step-CA certificate validation; Wazuh FIM integrity monitoring.	**Implemented**	
SI-7(1)	Integrity Checks: Wazuh FIM real-time integrity monitoring; file hash verification; registry monitoring (Windows).	**Implemented**	Cloud: Wazuh FIM on all 6 cloud nodes monitors same critical paths as on-premises (Linux: /etc, /bin, /sbin; Windows: System32, registry keys).

SI-7(6)	Cryptographic Protection: SHA-256 image signatures; TLS certificate validation; file integrity checksums.	**Implemented**	
SI-7(7)	Integration of Detection and Response: Wazuh FIM triggers Active Response; SIEM correlation with integrity violations.	**Implemented**	Cloud: Wazuh Active Response on cloud nodes triggers firewall-drop, host-deny, account-disable in response to integrity violations.
SI-10	Information Input Validation: WAF input validation (SafeLine); Traefik header validation; DNS query sanitization.	**Implemented**	
SI-12	Information Management and Retention: 90-day log retention; 30-day backup retention; automated lifecycle management.	**Implemented**	Cloud: cloud audit log retention policy (AWS S3 90-day lifecycle; GCP 400-day Admin Activity; Azure Log Analytics 90-day) consistent with on-premises SIEM policy.

Supply Chain Risk Management (SR): 40% Compliant

SR-3	Supply Chain Controls and Processes: Vetted open-source projects; trusted Docker registries; official package repositories.	**Partial**	Cloud: AWS IAM instance profiles (least-privilege, no long-lived access keys on EC2); GCP service accounts (minimal roles, no owner/editor on Compute instances); Azure VMs provisioned via ARM template with securestring parameters; all 6 cloud nodes enrolled in same vetted open-source management stack (Wazuh, Ansible, Checkmk, PatchMon) as on-premises hosts.
SR-10	Inspection of Systems or Components: Visual inspection of hardware; no formal process.	**Partial**	
SR-11	Component Authenticity: Docker image signature verification; package signature validation.	**Implemented**	Cloud: cloud provider base images (AMIs, GCP Compute images, Azure Marketplace images) tracked by version; provider-maintained images used with same-day security patch availability.
SR-12	Component Disposal: Secure deletion procedures; encrypted storage wiping.	**Implemented**	Cloud: AWS EBS volume deletion on instance termination; GCP persistent disk deletion; Azure Managed Disk cleanup: all

	documented in decommissioning runbook.

Version History

Version	Date	Changes
1.0	January 2026	Initial release.
2.0	April 2026	Cloud IaaS integration (AWS, Azure, GCP: 6 nodes). Cloud content integrated into Notes column of all relevant controls. Change log added.