Security Lab GRC Documentation

NIST Cybersecurity Framework 2.0

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



Created By: Paul Leone

April 3, 2026

Table of Contents

NIST Cybersecurity Framework 2.0 2
Overview 2
GOVERN (GV) — Tier 3 2
GV.OC — Organizational Context 2
GV.RM — Risk Management Strategy 3
GV.PO — Policy 4
GV.SC — Cybersecurity Supply Chain Risk Management 4
IDENTIFY (ID) — Tier 4 5
ID.AM — Asset Management 5
ID.RA — Risk Assessment 7
ID.IM — Improvement 9
PROTECT (PR) — Tier 4 9
PR.AA — Identity Management, Authentication and Access Control 10
PR.DS — Data Security 11
PR.IR — Technology Infrastructure Resilience 12
PR.PS — Platform Security 14
DETECT (DE) — Tier 3 15
DE.AE — Adverse Event Analysis 15
DE.CM — Continuous Monitoring 17
RESPOND (RS) — Tier 3 19
RS.AN — Analysis 19
RS.MA — Incident Management 20
RECOVER (RC) — Tier 3 21
RC.HL — Incident Recovery Plan Execution 21
RC.RP — Recovery Planning 22
Key Achievements — v2.0 22
Remaining Gaps — Tier 4 Advancement 23
Version History 23

NIST Cybersecurity Framework 2.0

Document Control:

Version:	**2.0**
Last Updated:	**April 2026**
Owner:	**Paul Leone**
Prior Version:	**1.1 — March 2026**

Overview

This document details implementation of NIST Cybersecurity Framework 2.0 across the security lab environment. Version 2.0 extends the prior assessment to include multi-cloud hybrid infrastructure spanning AWS (us-east-2), Azure (North Central US), and GCP (us-central1), connected via Tailscale WireGuard mesh VPN. All cloud nodes are integrated with the on-premises management toolchain (Wazuh EDR, PatchMon, Checkmk, Ansible, Uptime Kuma) and subject to the same security baselines applied to Proxmox-hosted workloads.

Overall Maturity: Tier 3 (Repeatable), Approaching Tier 4 (Adaptive). Cloud integration strengthens evidence across IDENTIFY, PROTECT, DETECT, and RECOVER functions with cloud-native security services (GuardDuty, Security Command Center, Defender for Cloud/Sentinel) augmenting on-premises controls.

GOVERN (GV) — Tier 3

Implementation: Risk management strategy established with documented CVSS-based prioritization, defined risk tolerances (Critical CVEs <72h MTTR, High <7d), and comprehensive security policies. Extended in v2.0 to cover cloud workload security baselines across AWS, Azure, and GCP. Cloud policy enforcement: no public management port exposure, Tailscale-only access, CIS SCA enforcement via Wazuh, and IAM least-privilege per provider.

GV.OC — Organizational Context

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
GV.OC-01	Lab mission statement defines security-first architecture principles; security objectives documented and aligned with learning goals.	Mission statement references SecOps, Systems Engineering, Network Defense, and Cloud Security as core focus areas. Compliance requirements documented across NIST, CIS, ISO 27001,	Cloud scope included in mission documentation: multi-cloud hybrid architecture (AWS/Azure/GCP) added as a demonstrated capability alongside on-

		and PCI-DSS frameworks.	premises SOC operations.
GV.OC-03	Legal/regulatory/contractual requirements understood.	Conceptual compliance with NIST, CIS, ISO 27001, PCI-DSS frameworks. No actual regulatory obligations (personal lab).	Cloud provider terms of service acknowledged. AWS, Azure, and GCP free-tier and pay-as-you-go usage governed by provider agreements. No cardholder data processed on cloud nodes.
GV.OC-04	Critical objectives, capabilities, and services understood.	Core services documented with criticality tiers: Tier 1 (SIEM/EDR), Tier 2 (Firewalls/DNS/Identity), Tier 3 (Supporting services).	Cloud nodes classified as Tier 2: AWS EC2 subnet router, Azure VMs, GCP Compute nodes. Cloud-native security services (GuardDuty, SCC, Defender for Cloud) classified as Tier 1 detection controls alongside Splunk and Wazuh.
GV.OC-05	Outcomes of cybersecurity strategy communicated.	Security metrics tracked in Grafana dashboards (20+). Quarterly reviews conducted against documented objectives.	Cloud security posture included in dashboard scope: Checkmk cloud node health, PatchMon cloud patch compliance, Uptime Kuma cloud tunnel availability.

GV.RM — Risk Management Strategy

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
GV.RM-01	Risk management objectives established.	Risk-based vulnerability prioritization via CVSS scoring. Patch management SLAs by severity: Critical <72h, High	Cloud risk management: same CVSS-based SLAs applied to cloud node findings from PatchMon, AWS Inspector, GCP

		<7d. Threat-informed architecture.	SCC, and Azure Defender for Cloud.
GV.RM-02	Risk appetite and tolerance defined.	Critical CVEs: MTTR <72h; High CVEs: MTTR <7d; acceptable false positive rate <5%; 95% patch compliance target.	Cloud node patch SLAs enforced identically to on-premises. Azure Spot instance eviction risk accepted with documented Deallocate policy and restart runbook.

GV.PO — Policy

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
GV.PO-01	Policy establishes behavioral expectations.	SSH hardening policy (CIS Benchmark), TLS 1.3 minimum policy, vulnerability remediation SLAs, comprehensive logging policy (100% security event coverage). Policies documented and version-controlled in Git.	Cloud policies appended: no public management ports on any cloud instance; all SSH/RDP restricted to homelab subnets (192.168.0.0/16) via provider-native firewall rules; Tailscale WireGuard mandatory for all management paths; CIS SCA enforcement via Wazuh on all cloud nodes.

GV.SC — Cybersecurity Supply Chain Risk Management

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
GV.SC-02	Suppliers and third parties included in risk management.	Vetted open-source projects used; trusted Docker Hub publishers; official OS repositories. GitHub security alerts monitored; software update frequency tracked.	Cloud provider supply chain: AWS IAM instance profiles with least-privilege roles (no long-lived access keys on EC2); GCP service accounts with minimal IAM role assignments, no owner/editor on compute instances; Azure VMs provisioned via ARM template with securestring parameters. Provider-native signing and verification for AMIs, GCP images, and Azure Marketplace images.

GV.SC-04	Suppliers and partners routinely assessed.	GitHub security alerts monitored; software update frequency tracked; planned CVE monitoring for dependencies.	Cloud provider security posture assessed continuously: AWS GuardDuty and Security Hub findings reviewed; GCP SCC security health analytics checked monthly; Azure Defender for Cloud Secure Score monitored. Cloud provider SOC 2 and ISO 27001 certifications acknowledged.
GV.SC-05	Response and recovery planning for supply chain incidents.	Snapshot-before-update strategy; rollback procedures documented.	Cloud node recovery: ARM template (Azure) and Ansible playbooks enable rebuild from code. Tailscale re-enrollment and Wazuh agent reinstallation documented in runbooks. Cloud node images (AMIs, GCP disk snapshots) available for rapid recovery.

IDENTIFY (ID) — Tier 4

Implementation: Comprehensive automated asset discovery and continuous risk assessment extended in v2.0 to include 8 cloud nodes across AWS (2 EC2), Azure (2 VMs), and GCP (2 Compute) enrolled in the common management toolchain. Cloud asset inventory, network topology, threat intelligence, and vulnerability disclosure workflows now span on-premises and hybrid cloud scope.

ID.AM — Asset Management

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
ID.AM-01	Inventories of hardware managed.	Checkmk infrastructure monitoring; Prometheus node exporters (30+ hosts); Proxmox asset database; external Excel inventory. Physical servers, network devices, and storage tracked.	Cloud hardware inventory added: AWS EC2 (i-0204e2e26d7f30631 t3.micro Amazon Linux 2, i-03e9efec4fa3fe644 c7i-flex.large Windows Server 2025); GCP (2x e2.micro, us-central1-c); Azure (Standard_B2ats_v2 Ubuntu 24.04, Standard_E2s_v3

			Windows Server 2025). All 8 cloud nodes enrolled in Checkmk via Tailscale.
ID.AM-02	Inventories of software and applications managed.	PatchMon tracks 5,000+ packages across 30+ on-premises hosts; WUD tracks 50+ containers; Nessus software inventory; Wazuh agent inventory (25+ endpoints).	PatchMon extended to 6 Linux cloud nodes (Amazon Linux 2, Debian 13.4, Ubuntu 24.04 LTS) with daily NVD CVE correlation. Windows cloud nodes (AWS, Azure) tracked via WSUS with automated approval workflows. Wazuh agents on all 8 cloud nodes provide real-time package and process inventory.
ID.AM-03	Network diagrams and organizational communication flows documented.	Network topology documented; Traefik routing architecture; VLAN segmentation diagrams; data flow maps maintained in Git.	Cloud topology added: Tailscale mesh routing tables (9 enrolled nodes, tailf07c05.ts.net), per-provider VPC/VNet CIDR allocations (AWS 172.31.0.0/16, GCP 10.128.0.0/16, Azure 10.130.0.0/16), subnet router configurations, and cloud-to-on-premises routing tables documented.
ID.AM-04	External systems and network connections catalogued.	VPN connections documented (Tailscale, PIA, Cloudflare Tunnels); external DNS resolvers tracked; internet egress points mapped.	Cloud VPC/VNet connections catalogued: AWS VPC (vpc-07db6afa9c6097fe4), internet gateway (igw-0d9a301fe45791b9b); GCP default VPC (10.128.0.0/16, us-central1); Azure homelab-vnet2 (10.130.0.0/16, North Central US). Tailscale subnet routers advertising cloud CIDRs into homelab documented.
ID.AM-05	Resources prioritized by classification and criticality.	Tier 1: SIEM, EDR, firewalls. Tier 2: DNS, identity management. Tier 3: Supporting services.	Cloud nodes classified as Tier 2. Cloud-native security services (GuardDuty, SCC, Defender for Cloud,

			Sentinel) classified as Tier 1 alongside on-premises Splunk and Wazuh. Azure Spot instance (Standard_E2s_v3) noted as lower-availability Tier 2 with documented restart procedure.
ID.AM-07	Inventories of data and information managed.	Sensitive data classification (logs, credentials, backups); data flow mapping; retention policies documented.	Cloud data inventory: AWS S3 CloudTrail log buckets (SSE enabled); GCP Cloud Storage (default encryption, audit logging enabled); Azure Log Analytics workspace homelab-log (90-day retention). All 8 cloud nodes included in Wazuh FIM monitoring scope via Tailscale.
ID.AM-08	Systems, hardware, software, and services authorized.	Authorized software list maintained; unauthorized application detection via Nessus/Wazuh; procurement approval process.	Cloud resources authorized: AWS EC2 instances in us-east-2 under documented IAM roles; GCP Compute in us-central1-c under minimal service accounts; Azure VMs in North Central US provisioned via ARM template. All cloud nodes enrolled in Tailscale tailnet with ACL-enforced access policy.

ID.RA — Risk Assessment

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
ID.RA-01	Vulnerabilities identified and documented.	OpenVAS + Nessus vulnerability scanning; CVSS scoring; CVE correlation with NVD; TheHive vulnerability tracking.	Cloud vulnerability identification: Wazuh CIS SCA on all 8 cloud nodes daily; PatchMon CVE correlation for 6 Linux cloud nodes; AWS Inspector findings; GCP SCC vulnerability assessment for Compute instances; Azure Defender for Cloud recommendations. All

			cloud findings visible in unified PatchMon dashboard.
ID.RA-02	Cyber threat intelligence received.	MISP threat intelligence platform; CrowdSec community feeds; AlienVault OTX, abuse.ch, Emerging Threats; Shuffle threat aggregation.	Cloud-native threat intelligence added: AWS GuardDuty ML-based behavioral detection (VPC flow logs, CloudTrail, DNS query logs); GCP Security Command Center asset and threat findings; Azure Sentinel KQL detection rules (NSG deny spikes, new-location sign-ins, domain join anomalies, AMA data gaps). Cloud findings forwarded to on-premises SIEM via Wazuh agents.
ID.RA-04	Potential impacts and likelihoods identified.	Risk-based remediation prioritization; exploit availability assessed; CVSS temporal scoring; asset criticality factored.	Cloud risk factors: cloud node internet-accessible public IPs (used only for Tailscale UDP handshake) assessed as low-risk given no inbound management ports. Azure Spot instance eviction risk documented with Deallocate policy. GCP e2.micro resource constraints factored into availability risk assessment.
ID.RA-08	Processes for receiving and analyzing vulnerability disclosures established.	Shuffle vulnerability disclosure workflow; NIST NVD monitoring; vendor advisory tracking; CVE analysis pipeline.	Cloud vulnerability disclosure: AWS Inspector findings routed to CloudWatch Events; GCP SCC findings generate alerting policy notifications; Azure Defender for Cloud recommendations surfaced in homelab-log and Sentinel. All cloud findings fed into TheHive for tracking against same MTTR SLAs as on-premises.

ID.RA-10	Critical suppliers and dependencies included in risk assessments.	Planned SBOM tracking; dependency vulnerability scanning; third-party risk assessments.	Cloud provider dependency risk: AWS, Azure, and GCP availability tracked via Uptime Kuma. Tailscale (WireGuard mesh VPN) identified as critical dependency for all cloud management access; dual on-premises pfSense nodes (primary and secondary Tailscale subnet routers) provide redundancy.

ID.IM — Improvement

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
ID.IM-01	Improvements identified from detection and response activities.	Vulnerability trends tracked in Grafana; CIS Benchmark compliance scores monitored; patch compliance dashboard; continuous security posture improvement.	Cloud security posture improvements tracked: PatchMon cloud patch compliance trends; Checkmk cloud node health trending; cloud-native security score tracking (AWS Security Hub score, GCP SCC findings trend, Azure Defender for Cloud Secure Score).
ID.IM-03	Response and recovery plans incorporate lessons learned.	Post-incident reviews drive playbook updates; TheHive lessons learned tracking; Shuffle workflow optimization based on execution data.	Cloud incident lessons: Azure Spot instance eviction experience documented; Tailscale tunnel recovery procedure refined; cloud node Wazuh re-enrollment runbook tested and updated following agent version upgrades.

PROTECT (PR) — Tier 4

Implementation: Defense-in-depth architecture extended in v2.0 to cloud nodes. Patch management, centralized identity, data protection, and infrastructure resilience capabilities now cover AWS, Azure, and GCP workloads using the same toolchain applied to on-premises infrastructure. No public management ports exposed on any cloud instance; all access via Tailscale.

PR.AA — Identity Management, Authentication and Access Control

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
PR.AA-01	Identities and credentials issued, managed, and verified.	Authentik SSO integration; centralized SSH key management via Ansible; individual user accounts; MFA enforcement via Authentik TOTP.	Cloud node identity: Linux cloud nodes use SSH Ed25519 keys managed via Ansible (same key distribution playbook as on-premises). AWS Windows Server 2025 and Azure Windows Server 2025 domain-joined to home.com via Tailscale — Kerberos authentication, Group Policy, and WSUS patch management extended to cloud workloads.
PR.AA-02	Identities authenticated.	SSH key-based authentication; Authentik SSO; MFA enforcement; certificate-based authentication (Step-CA).	Cloud authentication: SSH key-only access for all Linux cloud nodes (passwords disabled globally, consistent with on-premises). No public management ports on any cloud instance — all SSH/RDP access via Tailscale with device-bound WireGuard authentication. Windows cloud nodes authenticate via domain Kerberos.
PR.AA-05	Access permissions and authorizations managed.	Authentik RBAC groups; SSH sudo enforcement; Traefik middleware access control; least-privilege principle.	Cloud access control: AWS Security Groups (tailscale-access + lab-services) restrict all inbound management to homelab subnets and Tailnet CGNAT (100.64.0.0/10). GCP VPC firewall policy restricts SSH to 192.168.0.0/16. Azure NSG homelab-nsg2 explicit allow-list with DenyAllInBound at priority 65500. AWS IAM

			instance profiles scoped to minimum required actions.
PR.AA-06	Physical access managed.	Physical security (personal lab): locked server rack, limited access; environmental monitoring; backup power (UPS).	Cloud physical security delegated to provider (AWS, GCP, Azure maintain SOC 2 / ISO 27001 certified data centers). No additional on-premises physical controls required for cloud nodes.

PR.DS — Data Security

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
PR.DS-01	Data at rest protected.	Encrypted backups (AES-256); TLS in transit; scan credential encryption; SSH private keys encrypted; encrypted log transmission (syslog-ng TLS); immutable SIEM indexes.	Cloud data at rest: AWS S3 CloudTrail log buckets with SSE (server-side encryption); GCP persistent disks encrypted by default (Google-managed keys); Azure Managed Disks encrypted at rest by default; Azure Log Analytics homelab-log data encrypted at rest. All 8 cloud nodes included in Wazuh FIM monitoring scope.
PR.DS-02	Data in transit protected.	TLS 1.3 encryption (Traefik); Ed25519 SSH keys; DNSSEC validation; encrypted VPN tunnels (Tailscale, WireGuard).	Cloud data in transit: All management traffic between cloud nodes and on-premises encrypted via Tailscale WireGuard (ChaCha20-Poly1305). SSH AES-256-GCM for Linux terminal access. Cloud-to-cloud communication routes through Tailscale overlay, not public internet. Provider-native VPC/VNet internal traffic uses provider-encrypted private networking.

PR.DS-10	Integrity and authenticity of hardware and software verified.	Package signature verification; container image verification (SHA-256); Step-CA certificate validation.	Cloud software verification: AWS AMI and GCP Compute image provenance tracked; Azure Marketplace image signatures verified. Ansible new_install_baseline_roles.yml playbook validates package signatures on cloud nodes at provisioning time.
PR.DS-11	Data disposal practices established.	Secure deletion procedures; backup rotation policies; log retention limits; expired certificate cleanup.	Cloud data disposal: AWS EC2 EBS volumes deleted on instance termination (documented in runbook). GCP persistent disk deletion policy documented. Azure Managed Disk cleanup included in decommissioning checklist. Cloud-native audit logs subject to 90-day retention policy consistent with on-premises SIEM.

PR.IR — Technology Infrastructure Resilience

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
PR.IR-01	Networks and environments protected.	HA DNS failover (dual Unbound and Technitium); Traefik zero-downtime reloads; firewall clustering; network segmentation.	Cloud network resilience: AWS VPC Security Groups restrict all inbound to Tailnet and homelab subnets. GCP VPC firewall policy (homelab) with Google Threat Intelligence blocking — TOR exit nodes, known malicious IPs, sanctioned countries (CU, IR, KP, SY, Crimea, Donetsk/Luhansk). Azure NSG homelab-nsg2 default-deny. GCP Cloud Armor 3-tier WAF/DDoS policies (edge, backend,

			application) protect GCP workloads.
PR.IR-02	Security architectures established and maintained.	Defense-in-depth architecture; zero-trust principles; documented security controls; continuous assessment.	Cloud architecture: Tailscale ACL-enforced mesh (default deny, explicit allow policy) extends zero-trust posture to cloud nodes. Per-provider enclave gateway model: AWS Security Groups, GCP VPC firewall policy, Azure NSG. Cloud Armor application-level WAF (SQLi/XSS blocking via preconfigured expression sets v33-stable).
PR.IR-04	Adequate capacity ensured.	Prometheus capacity monitoring; Pulse hypervisor monitoring; disk space alerts; resource trending.	Cloud capacity monitoring: AWS CloudWatch Agent (CPU, memory, disk, network per EC2 instance); GCP Cloud Monitoring Ops Agent metrics for Compute nodes; Azure Monitor VM metric alert rules (7 active: Available Memory Bytes, Data Disk IOPS Consumed %, Network In/Out Total, OS Disk IOPS, Percentage CPU, VM Availability). All feed Checkmk on-premises dashboard and Discord alerting.
PR.IR-05	Continuity prioritized by business criticality.	Service prioritization (Tier 1-3); documented recovery priorities; RTO/RPO defined.	Cloud continuity: Tailscale subnet router redundancy — dual on-premises pfSense nodes provide alternate paths if single cloud node is unavailable. Azure Spot instance eviction

			handled by Deallocate policy with documented restart procedure. Cloud node RTO target <2hr via Ansible rebuild playbooks.

PR.PS — Platform Security

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
PR.PS-01	Configuration management practices established.	SSH config via Ansible; Traefik YAML in Git; DNS zones version-controlled; PatchMon configuration tracking; CIS Benchmark audits; Terraform IaC; configuration drift detection.	Cloud configuration management: Ansible linux_hardening.yml and new_install_baseline_roles.yml applied to all 6 Linux cloud nodes via SSH over Tailscale. Windows cloud nodes managed via GPO (domain-joined to home.com). Azure ARM template (azuredeploy.json) version-controlled for VM provisioning. All cloud configurations stored in Git.
PR.PS-03	Hardware and software maintained.	Multi-platform patch management (PatchMon, WSUS, WUD, Watchtower); vulnerability remediation workflows; automated updates where appropriate.	Cloud patch management: PatchMon daily checks on 3 Linux cloud nodes (Amazon Linux 2, Debian 13.4, Ubuntu 24.04 LTS). WSUS manages Windows cloud nodes (AWS, Azure Windows Server 2025) with automated approval workflows. Critical <72h MTTR SLA maintained across all cloud nodes.
PR.PS-04	Log records generated and managed.	100% security event logging to SIEM; 90-day retention; structured JSON format; comprehensive audit trails.	Cloud logging: AWS CloudTrail (all management events, delivered to S3 with SSE); GCP Admin Activity logs (always-on, cannot be disabled) and Data Access audit logs; Azure Activity Log and Monitor; all supplemented by Wazuh

			agent event forwarding from cloud nodes to on-premises Splunk. Cloud-native logs retained in provider storage (S3, GCS, Log Analytics Workspace homelab-log) with 90-day retention matching on-premises policy.

DETECT (DE) — Tier 3

Implementation: Continuous monitoring extended in v2.0 to cloud nodes with cloud-native behavioral detection augmenting on-premises SIEM/EDR. AWS GuardDuty, GCP Security Command Center, and Azure Defender for Cloud/Sentinel provide provider-specific threat detection operating in parallel with Wazuh EDR and Suricata/Snort IDS. Gap remains: ML-based anomaly detection for Tier 4 advancement.

DE.AE — Adverse Event Analysis

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
DE.AE-02	Potentially adverse events analyzed.	Vulnerability trending; exploit likelihood assessment; Cortex automated enrichment; MISP threat intelligence correlation; Shuffle orchestrated analysis workflows.	Cloud adverse event analysis: AWS GuardDuty findings enriched with threat intelligence and routed to CloudWatch Events; GCP SCC findings generate alerting policy notifications; Azure Sentinel KQL rules trigger incidents routed to Shuffle SOAR webhook for on-premises SOAR processing.
DE.AE-03	Information on adverse events correlated.	Multi-source correlation (Splunk + Elastic + Wazuh + network logs); TheHive aggregates alerts from SIEM, EDR, IDS; Shuffle orchestrates cross-platform queries.	Cloud event correlation: Wazuh agents on all 8 cloud nodes forward security events to on-premises Splunk and Elastic, enabling unified timeline correlation across on-premises and cloud sources. Azure Sentinel aggregates

			Windows Security Events (via AMA DCR home-lab-endpoints) and Syslog (az-ubuntu, gcp-debian-host1) in homelab-log workspace.
DE.AE-05	Incident alert thresholds established.	Splunk correlation search thresholds; Wazuh rule severity levels; TheHive case severity matrix; Prometheus alert thresholds; Grafana panel thresholds.	Cloud alert thresholds: AWS CloudWatch Alarms on GuardDuty high/medium findings; GCP Cloud Monitoring alerting policies (CPU >85%, disk <15%); Azure Monitor metric alert rules (7 active for az-win2025-dc). Azure Sentinel KQL rule: NSG deny-inbound spike >20 events/hour from single source IP triggers incident.
DE.AE-07	Cyber threat intelligence integrated.	MISP threat intelligence feeds; CrowdSec community intelligence; Cortex enrichment; Shuffle threat aggregation workflows.	Cloud threat intelligence: AWS GuardDuty ML-based detection integrated with VPC flow, CloudTrail, and DNS query logs — no manual rule maintenance required. GCP VPC network firewall policy embeds Google Cloud Threat Intelligence (TOR exit nodes, malicious IPs, geo-blocking of sanctioned countries) as priority 100-130 rules. Azure Sentinel threat intelligence connectors feed KQL detection rules.

DE.CM — Continuous Monitoring

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
DE.CM-01	Networks and network services monitored.	DNS query logging; Traefik access logs to SIEM; pfSense flow logs; Suricata/Snort IDS; NetAlertX network monitoring; 100% network traffic visibility.	Cloud network monitoring: AWS VPC flow logs (fl-03179f74e54bf1aa4) delivered to CloudWatch Logs group, capturing accepted and rejected traffic with ENI, source/destination, ports, and action. GCP VPC flow logs enabled on default network (Flow Analyzer). Azure NSG flow logs via Network Watcher (homelab-nsg2). Tailscale tunnel telemetry for all cloud-to-on-premises management paths.
DE.CM-04	Malicious code activity monitored.	Wazuh FIM; Yara rules; Cortex file analysis; Suricata IDS signatures; ClamAV/Microsoft Defender.	Cloud malware monitoring: Wazuh FIM and rootkit detection deployed on all 8 cloud nodes with same monitored path configuration as on-premises Linux/Windows hosts. Microsoft Defender active on Windows Server 2025 (AWS, Azure). ClamAV on Linux cloud nodes (Amazon Linux 2, Debian 13.4, Ubuntu 24.04 LTS). GuardDuty, GCP SCC, and Azure Defender for Cloud provide behavioral detection independent of signature-based tools.

DE.CM-06	External service provider activity monitored.	Limited: Cloudflare analytics; VPN logs; public service monitoring; API usage tracking.	Cloud provider activity monitoring: AWS CloudTrail captures all API calls including IAM role assumptions, security group modifications, and EC2 lifecycle events. GCP Admin Activity audit logs (always-on) capture all resource changes. Azure Activity Log records all ARM deployments and resource modifications. All cloud control-plane activity available for audit and correlation.
DE.CM-07	Monitoring for unauthorized activity performed.	Failed authentication tracking; privilege escalation detection; lateral movement monitoring; Shuffle automated analysis.	Cloud unauthorized activity detection: AWS GuardDuty ML detects credential misuse, port scanning, C2 callbacks, and cryptocurrency mining (VPC flow + CloudTrail + DNS). Azure Sentinel KQL rules detect: NSG deny-inbound spike (active scanning indicator), Entra ID sign-in from new geographic location, unexpected Windows domain join events, AMA data collection gaps. GCP SCC security health analytics flags open firewall rules and IAM misconfigurations.
DE.CM-09	Vulnerability scans performed.	Weekly OpenVAS network scans; monthly Nessus authenticated scans; daily PatchMon checks; continuous Wazuh SCA;	Cloud vulnerability scanning: Wazuh agents run CIS SCA on all 8 cloud nodes daily (CIS Amazon Linux, Debian 12/13, Ubuntu

		SIEM correlation of scan results.	22.04/24.04, Windows Server 2025). PatchMon daily CVE correlation for 6 Linux cloud nodes. AWS Inspector provides agent-based vulnerability assessment for EC2. GCP SCC vulnerability assessment for Compute Engine instances. Azure Defender for Cloud recommendations for Azure VMs. All cloud findings visible in unified PatchMon and Wazuh dashboards.
DE.CM-10	Threat hunting performed.	Wazuh threat hunting queries; Splunk SPL searches; Elastic KQL queries; MITRE ATT&CK-based hunting; Cortex IOC pivoting.	Cloud threat hunting: CloudWatch Logs Insights queries against CloudTrail and VPC flow logs. GCP Cloud Logging advanced queries for Admin Activity and Data Access anomalies. Azure Sentinel hunting queries (KQL) for cloud-specific TTPs. Cloud Wazuh agent telemetry included in on-premises Splunk SPL correlation searches.

RESPOND (RS) — Tier 3

Implementation: Documented IR procedures with TheHive playbooks, automated orchestration via Shuffle, and multi-engine analysis through Cortex. Cloud nodes integrated into the same incident response pipeline — Wazuh Active Response applies automated containment (firewall-drop, host-deny, account-disable) on cloud nodes via Tailscale. Gap: lacks tabletop exercises and formal BC/DR drills for Tier 4 maturity.

RS.AN — Analysis

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
RS.AN-01	Notifications investigated.	Cortex multi-engine analysis;	Cloud incident investigation: AWS GuardDuty findings forwarded to CloudWatch Events and

		MISP correlation; Splunk queries; Wazuh forensic data; TheHive case investigation.	SNS — can trigger Lambda-based automated response or Shuffle SOAR webhook. GCP SCC findings generate alerting policy notifications routed to Cloud Monitoring. Azure Sentinel incidents automatically created from KQL rule hits, routed to Shuffle SOAR webhook for on-premises TheHive case creation.
RS.AN-03	Forensics performed.	Wazuh forensic data collection; memory dumps; network captures; Shuffle automated forensic workflows; evidence preservation.	Cloud forensics: Wazuh agents on cloud nodes collect forensic data (process trees, file hashes, network connections) forwarded to on-premises SIEM. AWS VPC flow logs and CloudTrail provide control-plane forensic trail. GCP Admin Activity logs provide immutable audit trail. Azure Sentinel workspace retains logs for investigation. Cloud node disk snapshots available for offline forensic analysis.
RS.AN-04	Incidents categorized.	TheHive taxonomy; MITRE ATT&CK mapping; severity scoring; incident classification.	Cloud incident classification: AWS GuardDuty finding types mapped to MITRE ATT&CK (e.g., Recon:EC2/Portscan, Impact:EC2/BitcoinDomainRequest, CredentialAccess:IAMUser/AnomalousBehavior). GCP SCC finding categories aligned to cloud attack taxonomy. Azure Sentinel analytics rules tagged with MITRE ATT&CK techniques.

RS.MA — Incident Management

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
RS.MA-03	Incidents contained.	Wazuh Active Response; Cortex responders; Shuffle automated containment workflows; pfSense API firewall rules; network isolation.	Cloud containment: Wazuh Active Response (firewall-drop, host-deny, disable-account) executes on cloud nodes via Tailscale — same containment playbooks as on-premises. AWS Security Group modifications via CloudWatch Events + Lambda can isolate EC2 instances. GCP VPC firewall rule updates via Terraform for rapid containment. Azure NSG

			rule modification via ARM template or CLI for Azure VM isolation.
RS.MI-01	Vulnerabilities mitigated and documented.	Virtual patching (SafeLine WAF); IDS signatures; emergency patching via Ansible; TheHive vulnerability tracking.	Cloud vulnerability mitigation: Ansible linux_hardening.yml and update_linux_hosts.yml applied to cloud Linux nodes via Tailscale for emergency patching. GCP Cloud Armor virtual patching capability (WAF rule updates without instance restart). AWS Security Hub findings tracked with remediation status. Azure Defender for Cloud recommendations tracked in homelab-log.

RECOVER (RC) — Tier 3

Implementation: Backup/restore procedures with encrypted backups (AES-256), snapshot-based rollback, HA DNS failover, and documented RTO/RPO targets. Extended in v2.0 with cloud node recovery runbooks: ARM template (Azure), Ansible provisioning, and Tailscale re-enrollment enable cloud node rebuild from code with RTO target <2hr. Gap: requires formal BC/DR exercises and recovery plan testing for Tier 4.

RC.HL — Incident Recovery Plan Execution

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
RC.HL-01	Recovery plan executed.	Backup restoration procedures; system rebuild playbooks; service validation checklists; snapshot rollback.	Cloud recovery execution: Ansible new_install_baseline_roles.yml provisions replacement cloud nodes from scratch. Tailscale re-enrollment via pre-authorized key. Wazuh agent reinstallation via Ansible playbook. Azure Spot instance restart procedure: start via Azure portal or CLI after Deallocate event. AWS EC2 stop/start preserves

			Elastic IP association for subnet router continuity.
RC.HL-02	Recovery activities completed.	Verification testing; service health checks; performance validation; security posture confirmation.	Cloud recovery verification: Uptime Kuma tunnel health checks confirm Tailscale connectivity restored. Checkmk agent registration confirmed in on-premises dashboard. PatchMon agent check-in verified. Wazuh agent active status confirmed in manager. CIS SCA scan run to confirm security baseline compliance post-rebuild.

RC.RP — Recovery Planning

Subcategory	Description	Implementation	Cloud Extension (AWS / Azure / GCP)
RC.RP-01	Recovery plan exercised.	Recovery procedure testing; RTO/RPO validation.	Cloud recovery planning: Azure Spot instance eviction scenario documented and validated (Deallocate policy, restart procedure). AWS EC2 and GCP Compute instance stop/start tested. Tailscale re-enrollment from pre-authorized key tested. Cloud node RTO target <2hr validated via Ansible rebuild timing. Uptime Kuma alert-to-recovery time documented.

Key Achievements — v2.0

- 100% Function Coverage: All six CSF 2.0 functions implemented with documented processes and automated controls, now spanning on-premises and multi-cloud (AWS/Azure/GCP) scope.

- Multi-Cloud EDR: Wazuh agents deployed on all 8 cloud nodes (AWS, GCP, Azure) with CIS SCA policies matching on-premises baselines; unified vulnerability and compliance dashboards.
- Zero Public Management Exposure: No public management ports on any cloud instance — all SSH/RDP access via Tailscale WireGuard with device-bound authentication and ACL enforcement.
- Cloud-Native Threat Detection: AWS GuardDuty (ML, VPC flow/CloudTrail/DNS), GCP Security Command Center (asset inventory, vulnerability, network IDS), Azure Defender for Cloud + Sentinel (KQL detection rules, automated incident creation) operating in parallel with on-premises SIEM/EDR.
- Advanced Detection (on-premises): Multi-SIEM architecture (Splunk + Elastic + Wazuh) provides <5min MTTD for critical events.
- Automated Response: Shuffle orchestration reduces MTTR by 70% compared to manual workflows; Wazuh Active Response containment extended to cloud nodes via Tailscale.
- Risk-Based Approach: CVSS environmental scoring integrates asset criticality and exploit maturity; same SLAs (Critical <72h, High <7d) enforced across on-premises and cloud scope.
- Cloud Recovery Validated: Cloud node rebuild from Ansible playbooks tested; RTO target <2hr achieved; Azure Spot instance eviction/restart procedure documented.

Remaining Gaps — Tier 4 Advancement

- ML-based anomaly detection / UEBA: No behavioral baseline ML on on-premises or cloud nodes. Cloud-native ML (GuardDuty, Sentinel) partially fills this gap for cloud-specific behavior.
- Formal tabletop exercises and BC/DR drills: No scheduled cross-function exercises. Cloud recovery procedures validated informally.
- Mutual TLS (mTLS): Not fully deployed for all service-to-service communication, including cloud workloads.
- Comprehensive DLP: Egress filtering and bandwidth monitoring in place; formal DLP solution not deployed (cloud egress paths not covered). Planned Q2 2026.
- Full FIDO2/WebAuthn: TOTP MFA enforced; passwordless WebAuthn not yet deployed.
- SBOM tracking: Trivy/Grype implementation planned Q1 2026 for cloud node container and dependency scanning.
- Azure Spot eviction automation: Manual restart procedure documented; automated restart workflow not yet implemented.
- Cloud UEBA: Azure Sentinel and GCP SCC provide partial behavioral analytics; comprehensive UEBA platform not deployed.

Version History

Version	Date	Changes

1.0	January 2026	Initial assessment and summary statistics.
1.1	March 2026	Minor updates and formatting corrections.
2.0	April 2026	Cloud IaaS integration (AWS, Azure, GCP - 6 nodes total). Cloud content integrated