Kyūdō

SOVEREIGNTY-GRADE AI · GRC

Microsoft Security + GRC Integration Playbook

Vigilance with Purpose. Security with Control.

PRESENTED BY

Kyūdō — a KMicro Technologies platform

3525-265 Hyland Avenue

Costa Mesa, CA 92626 · kyudo.ai

hello@kyudo.ai

kyudo.ai · April 2026

CLASSIFICATION: PUBLIC

00 · HOW TO USE THIS PLAYBOOK

Seven integrations. Five days. Defensible evidence.

This playbook is for the platform admin, the identity admin, and the SOC lead who own the Microsoft Security integrations during Kyūdō's Days 2–5 deployment arc. It documents how to connect the seven priority Microsoft Security integrations to Kyūdō's automated evidence collection — the integrations that turn Defender, Sentinel, Purview, Entra ID, and Azure Policy signals into governed assurance artifacts.

The integrations follow a consistent five-stage setup model. Once you have walked the first integration end-to-end, the rest become recognizable. The differences are scope (which permissions, which APIs, which mappings) and the prerequisites you need in place before starting.

Audience and prerequisites

This playbook assumes:

- Kyūdō is deployed in your Azure tenant and Day 1 setup (authentication, RBAC group binding, organization profile) is complete. The Quick Start Guide and 30-Day Implementation Roadmap cover those steps.
- You have Tenant Admin role in Kyūdō and Global Administrator (or equivalent for the integration in question) in your Microsoft 365 / Entra ID / Azure environment.
- Your organization's frameworks are activated in Controls Hub (typical: SOC 2, ISO 27001, NIST CSF, CMMC, HIPAA depending on profile) so evidence has somewhere to land.
- You have read access to the Microsoft Defender, Sentinel, Purview, and Entra ID portals to validate that the integrations are pulling what you expect.

The five-stage workflow (universal)

Every integration follows the same five stages. Recognizing the pattern accelerates the second integration onward.

Stage	What happens
1 — Initiate	Open Kyūdō Settings > Integrations. Select the integration you are connecting. Click Set Up. Review the description, the required permissions, and the prerequisites checklist.
2 — Authorize	Authentication and credential exchange. Three patterns depending on the integration: OAuth (Microsoft Graph and Defender), Service Principal (Azure Resource Graph and Azure Policy), or External API Key

Stage	What happens
	(non-Microsoft sources). Tokens and credentials are stored encrypted in your tenant’s Key Vault.
3 — Scope selection	Choose which resources to monitor. Subscriptions, Entra ID groups, M365 workloads, Defender plans, Sentinel workspaces. Stored as Scope Selection Groups; reusable across Kyūdō assessments.
4 — Data ingestion + control mapping	Initial inventory pull. Signals normalized into Kyūdō Assurance Control Types. AI-assisted mapping to SCF controls; you confirm or override. Mapping results saved to the Knowledge Graph.
5 — Verify + continuous sync	Review mapped controls, unmapped controls, total resources scanned. Choose sync frequency (1 hour / 4 hours / daily / weekly). Initial full sync executes. Click Finish Setup. Integration status becomes Connected.

01 · THE INTEGRATION ORDER

Seven priority integrations. Configured in sequence.

Microsoft integrations are configured in a recommended order. The order matters: each integration extends the evidence base the next ones rely on. Identity is foundation; posture is breadth; logging is continuity.

Order	Integration	Day	Why this position
1	Microsoft Entra ID	2	Identity foundation. Establishes the user-and-group base every subsequent integration maps to. Required before any access-control evidence makes sense.
2	Microsoft Defender for Cloud	3	Posture breadth. Single integration produces the largest initial evidence yield through CSPM findings across Azure subscriptions. The integration most likely to flip an organization’s framework completeness scores noticeably on Day 1.
3	Microsoft Defender XDR	3	Endpoint posture. Threat detections, device compliance, vulnerability exposure. Closes the endpoint-control gap that CSPM does not cover.
4	Microsoft Sentinel	4	Logging and monitoring continuity. Sentinel analytic rules become Continuous Monitoring evidence. SOC lead involvement essential. Higher-effort integration but high-value: every framework has a logging-and-monitoring control family.
5	Microsoft Purview	4	Data governance. Two parts: Compliance Manager (assessments, improvement actions, regulatory templates) and Data Governance (classifications, lineage, sensitivity propagation). Connect both.
6	Azure Policy + Resource Graph	5	Configuration control. Service Principal-based integration. Azure Policy compliance summary becomes infrastructure-control evidence; Resource Graph provides asset enumeration

Order	Integration	Day	Why this position
			breadth.
7	Microsoft Graph API (M365)	5	Microsoft 365 governance. Mailbox policies, SharePoint sharing, OneDrive settings, DLP rules, retention. Closes the M365 governance gap that the security-focused integrations do not cover.

If you can only connect three

If your organization’s schedule allows only the highest-priority integrations on Day 1, connect Entra ID, Defender for Cloud, and Sentinel. These three produce the bulk of evidence for the most commonly-audited control families (access control, configuration management, logging and monitoring). The remaining four can be added in subsequent weeks without rework.

What must be in place before integration day.

Before opening Kyūdō Settings > Integrations, validate the prerequisites below. A missing prerequisite is the most common reason an integration fails Stage 2 authorization.

Tenant and licensing

- Microsoft 365 E3 or E5 license (or equivalent A3/A5 for education, G3/G5 for U.S. government). E5 unlocks Defender XDR, Sentinel, and full Purview capability; E3 covers most of the rest. Defender for Cloud requires Standard tier on at least the subscriptions in scope.
- Microsoft Sentinel workspace provisioned in the tenant. Connected data sources (Microsoft 365, Entra ID, Defender XDR, Azure Activity, etc.) configured per the SOC lead's standard playbook.
- Microsoft Defender for Cloud enabled on at least the subscriptions in scope, with Standard tier active. Microsoft Cloud Security Benchmark (MCSB) baseline assessments running.
- Microsoft Purview accounts provisioned (one Compliance Manager workspace at minimum; Data Governance accounts as the customer's data residency policy requires).
- Microsoft Entra ID with Conditional Access policies in place for administrative access. Privileged Identity Management (PIM) recommended for the Tenant Admin and Global Administrator roles.

Identity and consent

- Global Administrator role available for OAuth admin consent flows (consent is one-time per integration; the Global Administrator can step out after consent is granted).
- Application Administrator role for ongoing app-registration management (recommended separation from Global Admin for least-privilege operation).
- Security Administrator role for Defender XDR consent (separate consent flow from Microsoft Graph).

Service principal (for Azure Policy + Resource Graph)

- Service principal created in your tenant with Reader and Security Reader roles assigned at the subscription scope. Some customers prefer Resource Graph Contributor for enhanced query capability; this is optional.
- Client ID, Client Secret (or certificate), and Tenant ID available for the Stage 2 authorization. Secret rotation policy in place per your secrets management standard.

Kyūdō RBAC

- Tenant Admin role assigned in Kyūdō to the platform admin executing the integrations. Kyūdō Tenant Admin maps to the `Kyudo_TenantAdmin` Entra ID security group.

- Frameworks activated in Controls Hub. Without active frameworks, the AI mapping in Stage 4 has no destination.
- Organization profile complete (industry, region, regulatory drivers). The profile drives which control mappings the AI prioritizes.

Network and connectivity

- Kyūdō services have outbound network access to the Microsoft Graph, Defender, Sentinel, Purview, and Azure Resource Manager API endpoints. The Azure Firewall Premium baseline rules allow the Microsoft service tags by default.
- If your organization uses an outbound proxy or has network egress restrictions, validate that the relevant Microsoft endpoints are reachable. The required endpoints are documented in the Reference Runbook.

Three patterns. Read-only by default. Audit-logged.

Kyūdō's integrations follow three authentication patterns depending on the source system. All three default to read-only scope; write permissions are never requested unless a specific feature requires them and explicit approval has been documented.

Pattern A — OAuth admin consent

Used by: Microsoft Graph API (M365 + Entra ID), Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Purview Compliance Manager.

Flow: A Global Administrator clicks `Sign in with Microsoft` in the Kyūdō integration setup wizard. The Microsoft consent screen displays the requested scopes. Admin grants consent on behalf of the tenant. Kyūdō receives the OAuth token and stores it encrypted in the customer's Key Vault. Tokens refresh automatically; admin re-consent is required only if scopes change.

Properties: Tenant-wide consent. Read-only scopes by default. Token refresh is automatic. Consent can be reviewed at any time in the Microsoft Entra admin center > Enterprise applications > Kyūdō > Permissions.

Pattern B — Service principal

Used by: Azure Resource Graph, Azure Policy.

Flow: The customer creates a service principal in their Entra ID tenant (one-time setup). The service principal is assigned Reader and Security Reader roles at the subscription scope. The Tenant Admin enters the Tenant ID, Client ID, Client Secret (or certificate), and selected Subscription IDs in the Kyūdō wizard. Kyūdō validates by querying the first subscription for metadata.

Properties: Scoped to specific subscriptions; never tenant-wide. Read-only via Azure RBAC roles. Credentials stored in Key Vault. Secret rotation managed by the customer per their secrets management standard.

Pattern C — External API key

Used by: AWS Config / Security Hub, GCP Security Command Center, Prowler. Not used by any Microsoft integration in the Day 2–5 priority set.

Flow: Documented in the corresponding cloud-platform integration guides. Outside the scope of this Microsoft-focused playbook.

What Kyūdō never asks for

Three things Kyūdō will never request, regardless of integration. If the consent screen ever shows any of these, stop and contact KMicro Customer Success.

- Write permissions on Microsoft Graph (e.g., `Directory.ReadWrite.All`). Kyūdō reads; it never modifies your environment.
- Owner or Contributor roles at any Azure scope. Reader and Security Reader are sufficient for evidence collection. Resource Graph Contributor is optional for enhanced query.
- Multi-factor authentication codes from your administrator. Kyūdō is not in the MFA path; MFA is between you and Microsoft Entra ID.

Audit logging on integration activity

Every integration action is logged. The integration setup audit trail includes: who initiated the integration, which scopes were granted, when consent was given, every subsequent token refresh, every sync run, every test connection, every disable or reconfigure event. Integration logs are retained per your tenant’s configured retention policy and are exported to your Sentinel workspace if your organization has the Kyūdō-to-Sentinel forwarding configured.

Identity foundation. Day 2.

Microsoft Entra ID is the foundation integration. Connect it first; every subsequent integration's access-control evidence maps to identities, roles, and Conditional Access policies that this integration surfaces.

What this integration provides

- Directory inventory: users, groups, roles, devices, Conditional Access policies.
- Identity posture signals: MFA enabled per user, privileged role assignments, guest access patterns, sign-in risk and user risk events.
- Conditional Access policy state: which policies are configured, which are enabled, which apply to administrative roles, gap detection against the customer's baseline.
- Sign-in and audit logs (when configured) for evidence of access reviews, role activations, and high-risk sign-in events.

OAuth scopes requested (read-only)

Scope	Purpose
Directory.Read.All	Read users, groups, directory objects
AuditLog.Read.All	Read sign-in logs and directory audit events
Reports.Read.All	Read identity-protection reports and risk events
Policy.Read.All	Read Conditional Access policies and tenant policy state
IdentityRiskEvent.Read.All (optional)	Read user-risk and sign-in-risk events for risk-engine input

Step by step

1. Sign into Kyūdō with your Tenant Admin role.
2. Open Settings > Integrations. Locate Microsoft Entra ID in the Available list. Click Set Up.
3. Review the integration description and the requested scopes. The wizard displays the OAuth scopes above and indicates each is read-only.
4. Click Sign in with Microsoft. The Microsoft consent screen opens. Authenticate as a Global Administrator (this is the moment that requires Global Admin; you can step away from that role afterward).
5. Review the consent screen. Confirm the application name is `Kyudo` and the publisher is verified as KMicro Technologies. Click Accept.

6. You are returned to the Kyūdō wizard at Stage 3. Select scope: which Entra ID groups, organizational units, and conditional-access policy sets to monitor. For most organizations, select all groups in scope of governance frameworks.
7. Stage 4 begins automatically. The initial inventory pull runs (typically 5–15 minutes for a mid-market tenant). The Knowledge Graph populates with users, groups, roles, and CA policies. AI suggests SCF mappings.
8. Review AI-suggested mappings in the Stage 4 summary. Common mappings: MFA enabled → SCF AC-3 (Authentication Enforcement); admin role assignments → SCF AC-5 (Privileged Account Management); guest restrictions → SCF AC-2 (Account Management). Confirm or override each.
9. Stage 5: Choose sync frequency. Recommended baseline: 4 hours for most organizations; 1 hour for high-velocity environments; daily for stable environments. Click Finish Setup.

You will know it worked when...

Within 15 minutes of completing setup, the Controls Hub Identity & Authentication assurance type populates with control completeness scores. Open any access-control framework (SOC 2 CC6.1, ISO 27001 A.5, CMMC AC-3) and the controls now show evidence-backed status with citations to specific Entra ID policy and user records.

Failure modes

Symptom	Likely cause + remediation
Consent screen shows scopes you did not expect	The consent screen is from Microsoft, not from Kyūdō. If unexpected scopes appear, do not click Accept. Cancel, contact KMicro Customer Success, and review the Kyūdō application registration in Microsoft Entra > Enterprise applications.
"Need admin approval" error after Sign in	The signed-in user does not have Global Administrator or App Administrator role. Either elevate via PIM or have a Global Administrator complete the consent flow.
Integration shows Connected but no data after 30 minutes	Initial inventory pulls can take longer for large tenants. Check the integration detail page > Sync Status. If no successful sync after 60 minutes, click Test Connection. If Test Connection fails, the integration token may need re-consent.
AI mapping suggestions look wrong	Override the suggestion. Open the unmapped or mismapped control; manually map to the correct SCF control. The AI learns from overrides; subsequent mappings improve.

Cloud security posture. Day 3.

Microsoft Defender for Cloud (CSPM) is the highest-density evidence integration. A single Defender for Cloud connection produces the most initial evidence by volume — every CSPM recommendation, every Microsoft Cloud Security Benchmark assessment, every Secure Score signal across all in-scope subscriptions.

What this integration provides

- Microsoft Cloud Security Benchmark (MCSB) regulatory compliance assessments mapped to NIST SP 800-53, NIST SP 800-171, ISO 27001, CIS Microsoft Azure Foundations.
- Per-resource CSPM recommendations: misconfigurations, missing encryption, exposed endpoints, unhardened identities, missing Defender plans.
- Secure Score: the aggregated posture metric that becomes a continuous board-ready trajectory line in the Risk Management module.
- Resource hygiene findings: vulnerability signals, exposed network paths, identity-and-access concerns at infrastructure layer.

Required Azure RBAC roles (assigned to the Kyūdō service principal at subscription scope)

Role	Required	Purpose
Reader	Yes	Enumerate Azure resources in scope
Security Reader	Yes	Read Defender for Cloud recommendations and Secure Score
Resource Graph Contributor	Optional	Enables enhanced posture queries via Azure Resource Graph

Required OAuth scopes (when using OAuth pattern)

Scope	Purpose
https://management.azure.com/.default	Access Azure Resource Manager metadata and Defender CSPM API
SecurityRecommendation.Read.All	Retrieve posture recommendations
SecurityConfiguration.Read.All	Retrieve CSPM configuration findings

Step by step

10. Confirm Defender for Cloud Standard tier is enabled on the subscriptions you intend to connect. Subscriptions on Free tier produce limited evidence yield.
11. In Kyūdō, open Settings > Integrations. Select Microsoft Defender for Cloud. Click Set Up.
12. Choose authentication pattern: OAuth (recommended for tenant-wide deployment) or Service Principal (recommended where you want subscription-by-subscription scoping with explicit role assignments).
13. If OAuth: Sign in with Microsoft as a Security Administrator. Grant consent for the SecurityRecommendation and SecurityConfiguration scopes.
14. If Service Principal: Enter Tenant ID, Client ID, Client Secret. Confirm the service principal has Reader and Security Reader at the subscription scopes you are connecting.
15. Stage 3: Select the subscriptions in scope. For most organizations, select all production subscriptions; non-production environments are typically connected later under separate Scope Selection Groups.
16. Stage 4: Initial pull runs. Defender for Cloud tenants with 50+ subscriptions can take 30–60 minutes for the first full ingestion. Subsequent syncs are incremental.
17. Review AI mappings. Common Defender for Cloud findings map to: identity hardening → SCF AC-3, AC-5; data protection → SCF DP-5; network hardening → SCF NS-1, NS-2; logging/monitoring → SCF LM-1, LM-4; threat and vulnerability → SCF TVM-1, TVM-2.
18. Stage 5: Sync frequency 4 hours is typical baseline. CSPM does not change minute-by-minute; daily is sufficient for environments with low change velocity.

You will know it worked when...

The Risk Management dashboard shows a Defender Secure Score trajectory line populated with current and historical data. The Controls Hub > Cloud Posture assurance type is fully populated with completeness scores derived from CSPM findings. Open any framework with a configuration-management control family (NIST CSF PR.IP, ISO 27001 A.8, CMMC CM-2) — the controls now show evidence-backed status.

Failure modes

Symptom	Likely cause + remediation
No Secure Score appears even after sync	Defender for Cloud is on Free tier, MCSB is not enabled, or the CSPM data connector is not enabled per subscription. Upgrade to Standard tier; confirm MCSB; check Defender for Cloud > Environment settings.
Some subscriptions show data, others do not	Service principal does not have Security Reader on the missing subscriptions, or the role assignment is at resource group scope rather than subscription scope. Add Security Reader at subscription scope; the next sync will populate.

Endpoint posture. Day 3.

Microsoft Defender XDR (which subsumes Defender for Endpoint, Defender for Office 365, Defender for Identity, and related services) closes the endpoint-control gap. Where Defender for Cloud surfaces infrastructure posture, Defender XDR surfaces device posture, threat detections, and vulnerability findings.

What this integration provides

- Endpoint inventory: registered devices, OS versions, compliance state, MDE onboarding status.
- Threat detections: alerts mapped to MITRE ATT&CK techniques, remediation status, dwell time.
- Vulnerability findings: exposure score, software inventory, configuration weaknesses, recommendations.
- Email, identity, and cloud-app threat signals (where the corresponding Defender services are enabled).

OAuth scopes requested (read-only)

Scope	Purpose
Alerts.Read.All	Retrieve endpoint and Defender XDR alerts for risk scoring
Machine.Read.All	Device inventory and endpoint posture
Software.Read.All	Software inventory and vulnerability data
Vulnerability.Read.All	Exposure score and vulnerability findings
SecurityRecommendation.Read.All (optional)	Hardening and misconfiguration findings

API endpoints used: `https://api.security.microsoft.com` (unified Defender XDR endpoint) and `https://api.securitycenter.microsoft.com` (legacy MDE endpoint, where applicable).

Step by step

19. In Kyūdō, open Settings > Integrations. Select Microsoft Defender XDR. Click Set Up.
20. Click Sign in with Microsoft. Authenticate as a Security Administrator with admin consent capability.
21. Grant consent for the requested scopes. The consent flow is separate from Microsoft Graph (Defender XDR has its own application registration in your tenant).

22. Stage 3: Select scope by device group, by Defender role, or by tenant-wide. Most organizations select tenant-wide for the initial integration; device-group scoping is useful for multi-business-unit organizations with separate device fleets.
23. Stage 4: Initial pull runs. Tenants with 10,000+ devices can take 30–60 minutes for the first ingestion.
24. Review AI mappings. Common Defender XDR findings map to: endpoint hardening → SCF END-1, END-2; threat management → SCF TVM-1, TVM-2; vulnerability management → SCF VPM-3, VPM-4; incident response signals → SCF IRO-1.
25. Stage 5: Sync frequency 1–4 hours. Endpoint state changes more frequently than CSPM; faster sync is justified.

You will know it worked when...

The Controls Hub > Endpoint Hardening and Threat & Vulnerability Management assurance types populate with completeness scores. Recent threat detections appear as Knowledge Graph entities linked to the affected devices and to the controls those detections inform. Vulnerability findings appear in the Risk Management module with treatment-tracking workflow.

Failure modes

Symptom	Likely cause + remediation
"Insufficient privilege" error after consent	The signed-in user has Security Reader but not Security Administrator. Re-attempt with Security Administrator role or escalate via PIM.
No vulnerability data after sync	Microsoft Defender Vulnerability Management add-on may not be licensed in your tenant. Vulnerability data requires either the integrated MDE Plan 2 or the standalone Defender Vulnerability Management license.
Sync runs but device count is lower than expected	Some devices may not be onboarded to MDE. Open Defender XDR > Devices; confirm onboarding status. Devices not onboarded do not surface evidence.

Logging and monitoring continuity. Day 4.

Microsoft Sentinel is the highest-effort but highest-value integration in this set. Sentinel's analytic rules become Continuous Monitoring evidence in Kyūdō, mapped to logging-and-monitoring control families (SOC 2 CC7, ISO 27001 A.12, NIST CSF DE.AE, CMMC AU). The SOC lead's involvement in this integration is essential — they own the Sentinel workspace and the analytic rules that drive evidence.

What this integration provides

- Analytic rules inventory: every rule configured in your Sentinel workspace, its enablement state, its tactic and technique mapping (MITRE ATT&CK).
- Incident posture: open incidents, closed incidents with classification, mean time to acknowledge and resolve.
- Data connector inventory: which Microsoft and third-party sources are forwarding logs to your Sentinel workspace, connector health, last-ingested timestamps.
- Workbook and hunting query inventory: investigation capability, threat-hunting maturity signals, custom rule logic for the framework controls that require it.

Required Azure RBAC roles (assigned to the Kyūdō service principal at workspace scope)

Role	Required	Purpose
Microsoft Sentinel Reader	Yes	Read incidents, analytic rules, workbooks, and hunting queries
Log Analytics Reader	Yes	Read the underlying Log Analytics workspace data
Reader (subscription scope)	Yes	Enumerate Sentinel resource and parent subscription metadata

Step by step

26. Coordinate with your SOC lead before starting. Sentinel is the SOC lead's workspace; integration walkthrough should include them.

27. In Kyūdō, open Settings > Integrations. Select Microsoft Sentinel. Click Set Up.

28. Choose authentication pattern: Service Principal is recommended for Sentinel because the workspace scope is bounded and least-privilege role assignment is preferred.

29. Enter Tenant ID, Client ID, Client Secret. Confirm the service principal has Microsoft Sentinel Reader, Log Analytics Reader, and Reader at the workspace scope.

30. Stage 3: Select the Sentinel workspace(s) in scope. Most organizations have a single production workspace; mid-market organizations with multi-region deployments may have two or three.
31. Stage 4: Initial pull runs. The pull retrieves analytic rule definitions, recent incidents (typically last 30 days), and connector inventory. Long-history pulls (full 90 days of incidents) take 30–45 minutes.
32. Review AI mappings. Common Sentinel signals map to: detection coverage → SCF LM-1 (logging); incident response signals → SCF IRO-1, IRO-3; analytic rule operation → SCF MON-1.
33. Stage 5: Sync frequency 1 hour is recommended. Sentinel is the most velocity-sensitive integration; faster sync produces more current evidence.

You will know it worked when...

The Controls Hub > Logging & Monitoring assurance type shows completeness scores derived from Sentinel analytic rule coverage. Open any framework with a logging-and-monitoring control family — SOC 2 CC7.2, ISO 27001 A.12.4, NIST CSF DE.AE — and the controls show evidence-backed status with citations to specific Sentinel rules.

The Risk Management module shows incident-trend data: open incidents, mean time to detection, mean time to resolution. These are the metrics the board will ask about; they now appear with audit-defensible source lineage.

Failure modes

Symptom	Likely cause + remediation
"Workspace not found" error	The service principal does not have Reader on the resource group containing the Sentinel workspace. Add Reader at resource group scope and retry.
Analytic rules sync but no incidents appear	The integration only retrieves incidents from when it was connected forward. Historical backfill of incidents is configured separately; coordinate with your SOC lead and KMicro Customer Success if you require historical-incident backfill.
Connector inventory looks incomplete	Some Sentinel data connectors authenticate at the connector level (per-connector service principal); their inventory may not surface unless the corresponding integration scope includes them. Re-check the in-scope source systems.

Data governance. Two parts. Day 4.

Microsoft Purview spans two product areas with separate APIs: Compliance Manager (assessments, regulatory templates, improvement actions) and Data Governance (classifications, lineage, sensitivity labels). Connect both. Compliance Manager uses Microsoft Graph; Data Governance uses Azure RBAC.

Part A — Purview Compliance Manager

What this integration provides

- Compliance Manager assessment templates: SOC 2, ISO 27001, NIST, GDPR, HIPAA, CMMC, PCI DSS, and 250+ other regulatory frameworks.
- Improvement action recommendations and current state per assessment.
- Compliance score (the aggregate measure across active assessments).
- Mappings between Microsoft's regulatory control catalog and your internal control inventory.
- Policy state for retention labels, DLP rules, sensitivity labels, and information barrier policies.

Microsoft Graph application permissions (read-only)

Permission	Purpose
Compliance.Read.All	Read assessments, improvement actions, regulatory templates
ComplianceManagement.Read.All	Read compliance settings, DLP policies, retention labels
Policy.Read.All	Read M365 compliance and retention policies
DataPolicy.Read.All	Read sensitivity-label policies
Directory.Read.All	Correlate assessments with tenant-level metadata
SecurityEvents.Read.All (optional)	Compliance and identity-related security events
IdentityRiskEvent.Read.All (optional)	Insider-risk and compliance-risk signals

Step by step

34. In Kyūdō, open Settings > Integrations. Select Microsoft Purview — Compliance Manager. Click Set Up.

35. Click Sign in with Microsoft. Authenticate as a Compliance Administrator with admin consent capability.
36. Grant consent for the requested scopes.
37. Stage 3: Select which assessments to monitor. Most organizations select all assessments aligned with their active frameworks; some scope to specific assessments to reduce noise.
38. Stage 4: Initial pull runs. Compliance Manager is data-light; sync typically completes in 5–10 minutes. AI maps Microsoft's regulatory templates to your Kyūdō Controls Hub via SCF crosswalk.
39. Stage 5: Sync frequency daily is typical. Compliance Manager assessments do not change minute by minute.

Part B — Purview Data Governance

What this integration provides

- Data classifications across the organization: which data is classified, sensitivity propagation paths, glossary terms applied.
- Data lineage: source-to-target data flow across registered data assets.
- Scan results from registered data sources, schema changes, classification policy outcomes.

Required Purview RBAC roles

Role	Required	Purpose
Purview Reader	Yes	View data catalog, glossary, classifications
Purview Data Curator	Recommended	View lineage and advanced classifications
Purview Data Source Administrator	Optional	View scans and schema changes (read-only)

Required OAuth scopes

Scope	Purpose
https://purview.azure.net/.default	Access Purview Data Map and Catalog APIs
https://management.azure.com/.default	Inspect scanning and resource-level metadata

Step by step

40. In Kyūdō, open Settings > Integrations. Select Microsoft Purview — Data Governance. Click Set Up.

41. Choose authentication pattern. OAuth admin consent is the simpler path; Service Principal with Purview RBAC roles is the strict-scope path.

42. Confirm the principal has Purview Reader (and recommended: Purview Data Curator).

43. Stage 3: Select Purview accounts and data sources in scope. Multi-tenant organizations typically have multiple Purview accounts; one per business unit is common.

44. Stage 4: Initial pull runs. Data Governance pulls can be larger than other integrations because of asset-level metadata volume; allow 30–60 minutes for tenants with 10,000+ data assets.

45. Review AI mappings. Common Data Governance findings map to: data classification → SCF DP-1, DP-3; lineage and provenance → SCF DP-9; sensitivity-label policies → SCF DP-4.

46. Stage 5: Sync frequency 4 hours to daily.

You will know both Purview integrations worked when...

The Controls Hub > Data Protection assurance type shows completeness scores derived from both Compliance Manager assessment state and Data Governance classification state. Open any framework with a data-protection control family (SOC 2 CC6.7, ISO 27001 A.8, HIPAA §164.312(c), GDPR Articles 5 and 32) — the controls show evidence-backed status with citations to both Microsoft Compliance Manager assessment results and Purview data-classification records.

Configuration control. Service Principal. Day 5.

Azure Policy and Azure Resource Graph are the configuration-control evidence sources. Where Defender for Cloud surfaces posture findings (‘what is misconfigured’), Azure Policy surfaces enforcement state (‘what does the policy say should be true’), and Resource Graph surfaces asset truth (‘what is actually deployed’). All three together close the configuration-management evidence loop.

What this integration provides

- Azure Policy compliance summary: which policy assignments are evaluating, which resources are compliant, which are non-compliant, the cause of non-compliance per resource.
- Per-resource policy failures with full lineage to the policy definition that flagged them.
- Azure Resource Graph asset enumeration: every resource in the in-scope subscriptions with metadata sufficient for control mapping.
- Tag inventory and policy-driven tag enforcement state.

Authentication pattern

Service principal only. OAuth admin consent is not the right pattern for Resource Graph because the scope is per-subscription, not tenant-wide; Service Principal allows precise scoping.

Required Azure RBAC roles (assigned to the Kyūdō service principal)

Role	Scope	Purpose
Reader	Subscription	Enumerate resources, read policy state
Resource Graph Contributor	Subscription	Run Resource Graph queries
Security Reader	Subscription	Optional: cross-reference with Defender findings

Step by step

47. Confirm the service principal exists in your tenant and has the required role assignments at each subscription scope. (Service principal creation is documented in the prerequisites section.)

48. In Kyūdō, open Settings > Integrations. Select Azure Policy + Resource Graph. Click Set Up.

49. Stage 2: Enter Tenant ID, Client ID, Client Secret (or upload certificate). Click Validate.
50. Kyūdō validates by querying the first subscription for metadata. Successful validation produces a green Connected indicator; failure produces a specific error code with remediation suggestion.
51. Stage 3: Select subscriptions in scope. Most organizations select all production subscriptions; non-production environments are typically connected later.
52. Stage 4: Initial pull runs. Resource Graph queries for asset enumeration are fast (typically 5–10 minutes); Azure Policy compliance state runs in parallel.
53. Review AI mappings. Common Azure Policy findings map to: encryption at rest → SCF DP-5; logging enabled → SCF LM-2; configuration baseline drift → SCF CFG-2.
54. Stage 5: Sync frequency 4 hours to daily. Azure Policy state changes are slower than Defender XDR signals; faster sync is not required.

You will know it worked when...

The Controls Hub > Cloud Posture and Configuration Management assurance types populate with completeness scores. Open any framework with a configuration-management control family (NIST CSF PR.IP, CMMC CM-2, ISO 27001 A.8.9) — the controls show evidence-backed status with citations to specific Azure Policy assignments and per-resource compliance state.

Failure modes

Symptom	Likely cause + remediation
"Tenant ID does not match" error during validation	The service principal is in a different tenant than the one signed into Kyūdō. Confirm the Tenant ID matches the customer’s Entra tenant.
Validation succeeds but no policy data after sync	Service principal has Reader but not Resource Graph Contributor; pure Reader is insufficient for Resource Graph queries. Add Resource Graph Contributor at subscription scope.
Some subscriptions show data, others do not	Role assignment is at resource group scope rather than subscription scope. Azure Policy queries require subscription-scope role for full visibility.

10 · MICROSOFT GRAPH API FOR M365

Microsoft 365 governance. Day 5.

Microsoft Graph API for M365 closes the gap that the security-focused integrations leave. Where Defender, Sentinel, and Purview surface security and compliance posture, Microsoft Graph for M365 surfaces M365 governance posture: Unified Audit Log entries, mailbox configurations, SharePoint and OneDrive sharing, Teams policies, retention rules, DLP policies, and sensitivity-label deployment.

What this integration provides

- Unified Audit Log: every governance-relevant action across M365 (admin role changes, mailbox configurations, file sharing, policy modifications).
- Mailbox policies: retention, DLP, encryption, mailbox auditing state across all mailboxes in the tenant.
- SharePoint and OneDrive sharing settings: external sharing posture, anonymous link policies, retention configurations per site.
- Teams policies: external access, federation, recording, transcription, retention per channel.
- DLP rules and sensitivity label policy deployment state.

OAuth scopes requested (read-only)

Scope	Purpose
Directory.Read.All	Read users, groups, directory objects (correlation with Entra ID integration)
User.Read.All	Read user details and role assignments
Group.Read.All	Map business unit → group → control relationships
Sites.Read.All	Read SharePoint and OneDrive site-level metadata
Files.Read.All (optional)	Read file metadata for evidence-based classification
Policy.Read.All	Read M365 compliance and retention policies
DataPolicy.Read.All	Read sensitivity-label policies
AuditLog.Read.All	Read Unified Audit Log events
Reports.Read.All (optional)	Read sign-in anomalies and risk events

Step by step

55. In Kyūdō, open Settings > Integrations. Select Microsoft Graph API — M365. Click Set Up.
56. Click Sign in with Microsoft. Authenticate as a Global Administrator with admin consent capability.
57. Grant consent for the requested scopes. The consent screen will display a longer scope list than the single-purpose integrations because Microsoft Graph for M365 covers multiple workloads.
58. Stage 3: Select scope by workload (Exchange Online, SharePoint, OneDrive, Teams) or by business-unit / site collection. Most organizations select all workloads tenant-wide for the initial integration.
59. Stage 4: Initial pull runs. M365 governance data is voluminous; tenants with 10,000+ users and large SharePoint estates can take 60–120 minutes for the first ingestion. Subsequent syncs are incremental.
60. Review AI mappings. Common M365 governance signals map to: external sharing → SCF DP-4; retention → SCF OP-1; DLP → SCF DP-5; mailbox auditing → SCF LM-1.
61. Stage 5: Sync frequency 4 hours is typical baseline; Unified Audit Log can justify hourly sync if your organization has high-velocity governance events.

You will know it worked when...

The Controls Hub > Data Protection and Operations Continuity assurance types populate with completeness scores derived from M365 policy and audit-log state. Open any framework with retention, DLP, or external-sharing controls (HIPAA §164.312, ISO 27001 A.8, SOC 2 CC6.7) — the controls show evidence-backed status with citations to specific M365 policies and Unified Audit Log entries.

After integration: the rhythm of operation.

Once all seven integrations are connected and validated, integration management becomes a low-effort operational rhythm. The mechanisms below cover the daily, weekly, and exception-based work.

The integrations dashboard

Settings > Integrations is the operational hub. The dashboard shows every integration with: connection status (Connected / Pending Authorization / Error / Token Expired), last successful sync timestamp, number of resources imported in the last sync, number of controls mapped, and any active alerts (token expiring within 7–14 days, sync failures, mapping discrepancies).

Daily — 5-minute integration health check

Open the Integrations dashboard. Confirm all seven integrations show Connected (green status badge). Investigate any that show yellow or red. Most issues self-resolve within an hour; persistent issues route through the troubleshooting in the next section.

Weekly — 30-minute review

- Open each integration’s detail page. Verify the resource counts and control-mapping counts are stable and aligned with your environment’s expected scale.
- Review the AI-mapping change log. New SCF mappings created during the week; any overrides made by the Compliance Officer or AI re-classifications. Confirm or override per your judgment.
- Spot-check the Evidence Hub for one or two recently-collected artifacts per integration. Confirm the source signal is what you expect; confirm the lineage chain is intact; confirm the confidence score is acceptable.

Test Connection and Sync Now

Every integration detail page has Test Connection and Sync Now buttons. Test Connection issues a probe call to the source API and verifies the credentials are still valid; useful when a sync has not run in longer than expected. Sync Now triggers an immediate sync run rather than waiting for the next scheduled cycle; useful after a major configuration change in the source environment that you want reflected in Kyūdō immediately.

Token refresh and re-consent

OAuth tokens refresh automatically. The Kyūdō platform manages the refresh cycle; admin re-consent is required only in two scenarios: (1) the requested scopes change in a Kyūdō platform

update (notified via the Kyūdō Update Channel and the Tenant Admin email); (2) the Microsoft Entra ID administrator revokes the consent in the Microsoft Entra admin center.

Service Principal credentials require manual rotation per your organization’s secrets management standard. Kyūdō notifies the Tenant Admin 14 days before a configured expiration; rotate the secret in your Entra ID, update the new value in the Kyūdō Integration detail page, and Test Connection.

Quarterly access review

Once per quarter, review every integration’s consented scope and role assignment. Confirm the principle of least privilege is still satisfied: no integration has scopes broader than required for its evidence-collection function. The Microsoft Entra admin center > Enterprise applications view shows the Kyūdō consent record; the Azure RBAC view shows the service principal role assignments.

The most common issues. Triaged.

The patterns below cover the issues you will encounter most. For anything beyond these, escalate via Test Connection failure log to KMicro Customer Success.

OAuth and consent issues

Symptom	Triage
Consent screen shows scopes you did not expect	Stop. Do not click Accept. Cancel the flow. Contact KMicro Customer Success and review the Kyūdō application registration in your Microsoft Entra admin center > Enterprise applications.
"Need admin approval" after Sign in	Signed-in user lacks Global Administrator or App Administrator role. Elevate via PIM or have a user with the role complete the consent.
Consent succeeds but integration shows Pending Authorization	Token exchange failed in Stage 2. Open the integration detail page; click Test Connection. If failure persists, redo Stage 2 with a fresh consent flow.
Integration shows Token Expired	Refresh-token chain is broken (most common: a Conditional Access policy change). Click Reconnect on the integration detail page; complete the consent flow again.

Service principal issues

Symptom	Triage
"Tenant ID does not match" during validation	The service principal is in a different tenant from the customer Entra tenant. Confirm Tenant IDs match.
Validation succeeds but no data after sync	Service principal has Reader but not the additional roles (Security Reader, Resource Graph Contributor, Sentinel Reader) per the integration documentation. Add the missing roles at the correct scope.
Sync was working, now fails	Client secret expired or was rotated. Update the secret in the Integration detail page; Test Connection.

Sync and ingestion issues

Symptom	Triage
Initial sync runs forever	Tenant scale is large. Defender for Cloud + 50+ subscriptions, or Microsoft Graph M365 + 10,000+ users, can take 60–120 minutes for first ingestion. Wait for completion before declaring failure.
Sync runs but resource count is lower than expected	Scope is narrower than expected. Open Stage 3 of the integration detail page; verify all intended subscriptions, workspaces, or workloads are selected.
Sync throttling alerts in the integration detail log	Microsoft API throttling. Kyūdō backs off automatically and retries; sync run will complete, just slower. If throttling persists for hours, contact Customer Success.

Mapping and evidence issues

Symptom	Triage
AI mapping suggestion looks wrong	Override the suggestion. Open the unmapped or mismapped control; manually map to the correct SCF control. The AI learns from overrides.
Control completeness score does not move after sync	Evidence is being collected but is mapped to controls outside the framework you are inspecting. Switch the framework filter; confirm the evidence appears under the correct framework view.
Confidence score below 0.7 on most evidence	Source signal is weak or ambiguous. The HITL threshold flag is the platform behaving correctly; review the flagged items and confirm or override per your judgment.

When to escalate

Most issues self-triage with the patterns above. Escalate to KMicro Customer Success when: (a) the integration shows persistent Token Expired even after reconnect; (b) sync errors include API status codes outside 401/403/429; (c) AI mappings are systematically wrong (not just occasionally); (d) the integration is connected and syncing but no evidence appears in Controls Hub for more than 24 hours. Provide the integration name, the error message text, and a screenshot of the integration detail page when escalating.

APPENDIX A · UNIFIED PERMISSIONS MATRIX

All seven integrations. One reference table.

This matrix consolidates the permissions and RBAC roles required for each integration. Use it as the procurement-and-IT-approval document when planning the integration sequence.

Integration	Auth pattern	Required permissions / RBAC
Microsoft Entra ID	OAuth	Directory.Read.All, AuditLog.Read.All, Reports.Read.All, Policy.Read.All. Consent role: Global Administrator.
Defender for Cloud	OAuth or SP	Reader + Security Reader at subscription. Optional: Resource Graph Contributor. SecurityRecommendation.Read.All, SecurityConfiguration.Read.All.
Defender XDR	OAuth	Alerts.Read.All, Machine.Read.All, Software.Read.All, Vulnerability.Read.All. Consent role: Security Administrator.
Microsoft Sentinel	Service Principal	Microsoft Sentinel Reader + Log Analytics Reader + Reader at workspace and subscription scope.
Purview Compliance Manager	OAuth	Compliance.Read.All, ComplianceManagement.Read.All, Policy.Read.All, DataPolicy.Read.All, Directory.Read.All. Consent role: Compliance Administrator.
Purview Data Governance	OAuth or SP	Purview Reader (recommended: Purview Data Curator). Scope: https://purview.azure.net/.default and https://management.azure.com/.default.
Azure Policy + Resource Graph	Service Principal	Reader + Resource Graph Contributor at subscription scope. Optional: Security Reader for Defender cross-reference.
Microsoft Graph API (M365)	OAuth	Directory.Read.All, User.Read.All, Group.Read.All, Sites.Read.All, Policy.Read.All, DataPolicy.Read.All, AuditLog.Read.All. Consent role: Global Administrator.

APPENDIX B · SCF CONTROL MAPPING EXAMPLES

From signal to control to framework crosswalk.

The examples below illustrate how Microsoft Security signals become evidence in the Kyūdō Knowledge Graph, mapped via STRM to SCF controls, and then crosswalked to multiple framework controls simultaneously. Each row is a real example from production deployments.

Microsoft signal	SCF control	NIST CSF	ISO 27001	SOC 2
Entra ID: MFA enabled on Global Admin	AC-3	PR.AC-1	A.5.17	CC6.1
Entra ID: Conditional Access policy on admin roles	AC-5	PR.AC-4	A.5.18	CC6.3
Defender for Cloud: Storage encryption	DP-5	PR.DS-1	A.8.24	CC6.7
Defender for Cloud: Network exposure check	NS-1, NS-2	PR.AC-5	A.8.20	CC6.6
Defender XDR: Endpoint compliance	END-1	PR.IP-1	A.8.9	CC7.1
Defender XDR: Vulnerability finding	TVM-1, VPM-3	ID.RA-1	A.8.8	CC7.2
Sentinel: Analytic rule operational	LM-1	DE.AE-3	A.8.16	CC7.2
Sentinel: Incident response time	IRO-1	RS.AN-1	A.5.24	CC7.3
Purview Compliance Manager: Assessment score	GOV-2	ID.GV-3	A.5.31	CC1.4
Purview Data Governance: Sensitivity label applied	DP-4	PR.DS-5	A.5.13	CC6.7
Microsoft Graph: External sharing restricted	DP-4	PR.DS-5	A.5.13	CC6.7

Source — Kyūdō STRM crosswalk per NIST IR 8477. Mappings reflect April 2026 SCF v2025.1 baseline. This is a sample; the full STRM crosswalk for Microsoft signals against the 1,470+ SCF controls and the 80+ frameworks Kyūdō supports is in the Reference Runbook and queryable in the Kyūdō Knowledge Graph.

APPENDIX C · GLOSSARY

Terms used in this playbook.

Term	Definition
Admin consent	Microsoft Entra ID flow where a Global Administrator grants OAuth scope consent on behalf of the entire tenant. Required for tenant-wide application registrations such as Kyūdō.
Application registration	The Microsoft Entra ID object representing Kyūdō in the customer's tenant. Visible in Microsoft Entra admin center > Enterprise applications.
Assurance Control Type	Kyūdō's normalized categorization of evidence: Identity & Authentication, Endpoint Hardening, Logging & Monitoring, Data Protection, Cloud Posture, Threat & Vulnerability Management, Configuration Management, Operations Continuity.
CMCAE	Continuous Multi-Framework Control Assessment Engine. The Kyūdō engine that recalculates control completeness, capability maturity levels, and residual risk on every signal change.
Conditional Access	Microsoft Entra ID policy framework that governs sign-in conditions (device compliance, MFA method, geographic restrictions, sign-in risk, user risk).
Confidence score	AI-computed score on every Kyūdō output. Below the human-in-the-loop threshold of 0.7, outputs are flagged for human review before propagating.
Connector	Microsoft Sentinel mechanism for ingesting log data from a source system. Different connectors authenticate differently; some use service principals, others use API keys.
CSPM	Cloud Security Posture Management. The Defender for Cloud capability that surfaces misconfigurations, exposed assets, and posture-improvement recommendations.
HITL threshold	Human-in-the-Loop. The confidence threshold (0.7 default) below which AI-produced outputs are flagged for human review.
MCSB	Microsoft Cloud Security Benchmark. Microsoft's built-in regulatory compliance assessment in Defender for Cloud, mapping Azure resource state to NIST SP 800-53, NIST SP 800-171, ISO 27001, and CIS Microsoft Azure Foundations.

Term	Definition
MDE	Microsoft Defender for Endpoint. The endpoint protection component within Defender XDR.
MFA	Multi-factor authentication.
NIST IR 8477	Mapping Relationships Between Documentary Standards, Regulations, Frameworks, and Guidelines. The NIST Internal Report formalizing Set Theory Relationship Mapping (STRM).
OAuth admin consent	The OAuth 2.0 flow used by Kyūdō for Microsoft Graph and Defender API authentication. Tenant-wide consent granted by a Global Administrator.
PIM	Privileged Identity Management. Microsoft Entra ID feature replacing standing privileged access with eligible-and-activate; activation is logged and time-bound.
RBAC	Role-Based Access Control. The Azure and Kyūdō permission model. Maps Entra ID security groups to Azure roles or Kyūdō roles.
SCF	Secure Controls Framework. The meta-framework substrate that anchors the Kyūdō Knowledge Graph; over 1,470 controls across 80+ frameworks.
Scope Selection Group	Reusable Kyūdō configuration of resources monitored under a specific framework or assessment. Subscriptions, workspaces, Entra groups, M365 workloads can all be members of a Scope Selection Group.
Service principal	Microsoft Entra ID object representing a non-human application identity. Used for the Azure Resource Graph and Sentinel integrations.
STRM	Set Theory Relationship Mapping (per NIST IR 8477). The mathematical substrate that makes one Kyūdō control set satisfy 70+ frameworks simultaneously.
Sync frequency	How often Kyūdō pulls fresh data from a source integration. Configurable per integration: 1 hour, 4 hours, daily, weekly.
Token	OAuth bearer token used for API authentication. Refreshed automatically by Kyūdō; admin re-consent required only when scopes change or consent is revoked.
Unified Audit Log	Microsoft 365 service that captures every governance-relevant action across Exchange Online, SharePoint, OneDrive, Teams, and Microsoft Entra ID.