Start with the cloud. Follow the access.

SkyKick detection and response: cross-platform field guide

A practical source-first workflow, complete query appendix, and matching embedded attachments for MSPs and security teams.

01 / AUTHENTICATION	02 / AUTHORITY	03 / RESOURCE ACTIVITY
Which identity tried to authenticate?	What credentials, roles, owners, or consent changed?	What happened after access was granted?

Investigation workflow, not a reconstruction of attacker actions. Disabling a vendor connection does not by itself settle what happened inside a customer tenant.

23 primary hunt blocks, 2 experimental Sigma rules, and 6 retained advanced normalized hunts. Read-only starters; no installed alerts or customer-tenant execution.

Historical scope: the October 19 advisory snapshot and October 13 investigation start are preserved. This refresh changes usability and source routes; it is not a new incident finding.

Choose the records that answer the question.

Microsoft: application sign-ins and directory changes

Start with the five KQL blocks over AADServicePrincipalSignInLogs and AuditLogs. Check the customer AADTenantId, retention, ingestion, and explicit UTC window. Run in Sentinel or Log Analytics.

Sophos: cloud records, workload audit, and local context

Fusion Advanced Search uses connected cloud sources. Data Lake SQL uses Microsoft 365 Management Activity. Windows endpoint SQL uses retained local journals. These are three different editors and sources. The Sophos appendix appears first in the Sophos-focused edition.

Splunk, LogScale, and Sumo: direct directoryAudit JSON

The six new searches parse Microsoft Graph v1.0 directoryAudit objects. They provide broad change review and listed-application actor review. They do not cover service-principal sign-ins. A real collected source is required; see the exact collection and ingestion steps below.

Sigma and advanced engineering

Two standard Azure auditlogs Sigma rules supplement the broad review. At the back, all original normalized queries, mapping, and portable logic remain available for teams that maintain that engineering contract.

First action

Open SOURCE-GUIDE.txt, confirm one known source record, and choose one block in its named editor. Establish source coverage before treating an empty result as evidence. For each match, preserve the original event, result, actor, targets, before/after properties, and customer scope.

Source setup and interpretation

Start here: identify your customer tenant, source, UTC start, recorded end, and retention. Verify one known service-principal sign-in and one directory change against the original source. Missing records are not a negative finding. These are read-only hunt starters; no tenant or vendor engine execution is claimed.

1. Microsoft Sentinel or Log Analytics: queries/skykick-hunt-starters.kql has five blocks: 01A, 01B, 02, 03, and 04. Requires AADServicePrincipalSignInLogs and AuditLogs ingested through configured Microsoft Entra diagnostic settings, the relevant categories, workspace access, and any applicable Entra/Azure licensing and ingestion charges. The workspace's TenantId is not the customer's AADTenantId. Set TenantFilter to the customer Entra tenant GUID; an empty filter searches every visible tenant. KQL here belongs in Sentinel/Log Analytics, not automatically Defender Advanced Hunting. Set the portal picker to include the full explicit query interval. Table existence is not proof of continuous collection.

2. Splunk, LogScale/Falcon Next-Gen SIEM, and Sumo Logic: the new graph-directoryaudit files parse Microsoft's documented Graph v1.0 directoryAudit JSON directly. They are audit-only routes. They do not supply or infer service-principal sign-ins. GS/GL/GU01 selects five broad directory categories; GS/GL/GU02 selects a listed application as the recorded initiating application. The actor route is not a target application search, self-assignment finding, or maliciousness verdict. Missing actor fields remain in the broad category route. User actors, empty target arrays, failed results, and unknown results are not filtered out by that broad route.

Use real retained Graph directoryAudit exports already collected, or configure an authorized Microsoft Graph collection workflow. GET https://graph.microsoft.com/v1.0/auditLogs/directoryAudits supports AuditLog.Read.All as the least privileged API permission; delegated access also needs a supported directory role. Follow @odata.nextLink until all pages are retrieved. Export the individual objects from value[] as UTF-8 JSON lines. Preserve every property, nested initiatedBy, targetResources, modifiedProperties, original event ID, collection time, and customer identity in protected collection metadata. Never save bearer tokens in event content. This package has no collector and does not create historical data.

Each SIEM event must be one original directoryAudit object, not a wrapper, value[] response, Event Hub envelope, Azure Monitor uppercase-schema row, or Microsoft 365 Management Activity record. If your integration supplies another event format, use its documented parser and corresponding query. Do not silently treat that envelope as Graph JSON. These searches parse real Microsoft keys; their few output aliases are direct query-local extractions, not a new event schema.

Splunk: ingest the JSON lines using your managed file/HEC route; configure event boundaries and _time from activityDateTime, retaining _raw. Replace both index and sourcetype with the verified, customer-scoped source. SPL spath explicitly extracts each key. Check extraction limits on long events,

field collisions with automatic extractions, and inspect the original record for every result. The shipped block is SPL, not SPL2.

LogScale: ingest the same JSON objects into an authorized repository or view with a JSON parser and @timestamp parsed from activityDateTime. Select that exact customer source in the UI before running GL01 or GL02. parseJson(field=@raw) extracts the original keys at query time; no dc_* normalization is used. Retain @raw and view complete events. These blocks deliberately omit select() so that a default projection does not hide nested evidence; verify result/export limits for a full timeline. A Falcon endpoint sensor alone does not collect this cloud feed.

Sumo: ingest those objects using an existing documented Local File or HTTP Logs and Metrics Source route. Replace _sourceCategory with the configured customer-scoped source category; this literal is a selector, not a built-in feed or table. Configure one JSON object per message and event time from activityDateTime. Explicit json ... nodrop extraction preserves missing keys. Inspect the Messages view and raw record, including all nested targets. The HTTP transport alone is not telemetry: Graph records must actually be collected, paginated, and delivered first. No custom Deception Check event producer is required or implied.

For all three Graph routes, verify customer attribution from the configured source and protected export manifest. directoryAudit does not provide a universal tenantId field. Never substitute a workspace, repository, or organization identifier for a source tenant. Select October 13, 2026 00:00 UTC to a recorded end for the historical indicator-led investigation; extend to October 1 only where retained history permits. When old exports are reingested, ensure event-time parsing is correct and widen the picker if ingest time and event time differ. Treat the seven IDs and three IPs as the October 19 advisory snapshot, not a refreshed current indicator list. Confirm current vendor guidance before action.

3. Sophos: queries/skykick-sophos-searches.json contains six query strings for Fusion Advanced Search (C00-C04, N01); it is not a policy import. Configure the Microsoft Entra Activity Reports integration with ServicePrincipalSignInLogs and AuditLogs when using Event Hubs. For Graph-based integration, verify service-principal login collection explicitly; interactive sign-ins and directory audits are defaults in the documented integration setup. Confirm current Sophos entitlement, integration health, customer scope, and source categories on a known event. auth/cloudaudit are documented Sophos logical schemas, not a package-defined feed. C00 counts alone do not prove the right auth source. C02-C04 inspect original text; GUID roles require manual confirmation. Sophos documents a 20-day raw access limit: older raw-dependent searches may be unavailable even when some normalized data remains. Use retained exports when needed.

Sophos Data Lake SQL: skykick-sophos-m365-datalake.sql has L00-L02 over the documented xdr_identity_o365 table from the Microsoft 365 Management Activity integration. This is a distinct audit feed, not dedicated service-principal sign-in history. Verify organization_id/customer scope and query_name partitions. Endpoint SQL: skykick-sophos-endpoint.sql has E01-E03 for authorized Windows Live Discover endpoints. Network/process journals provide supporting local history; sophos_pid is not the Windows numeric PID. Endpoint snapshots are not a tenant-wide cloud ledger.

Run the exact dialect in its named editor.

4. Sigma: two experimental Azure auditlogs rules keep standard source fields and Deception Check in author. Nested InitiatedBy.app field extraction needs a verified backend mapping. App-initiated does not mean self-assigned, successful, or unauthorized. Preserve outcomes. YAML parsing, source fixtures, and successful backend conversion are different checks; no backend or tenant execution is claimed for this refresh.

5. ADVANCED: retained October 19 dc_* mapping, normalized SPL/CQL, full portable pseudocode, and explanation. This is engineering reference for teams deliberately maintaining that mapping. It is not the primary customer route. Do not deploy these as stock vendor-field searches.

Interpret findings: keep listed app OR reported address paths independent; retain IPv6, failed, and unknown outcomes. Examine credential, owner, role, and consent changes across all applications. Follow verified identities and key IDs into available Microsoft Graph and Microsoft 365 resource records. Compare event time with the specific customer's containment time. A recorded attempt is not proof of success; a permission change is not proof of data access. No validated malicious file or memory sample supports a YARA signature here.

Primary query appendix

All blocks below are printed from the downloadable source files. Long lines wrap visually; use the exact embedded attachment for copying. Every block keeps its native editor and source prerequisites. The attachments are also supplied in the ZIP.

01A / Available service-principal records by tenant and UTC day.

Microsoft Sentinel / Log Analytics KQL. Requires the named Entra tables and customer AADTenantId. Blank TenantFilter searches all visible tenants. Include the explicit UTC query interval in the portal picker.

Source attachment: skykick-hunt-starters.kql

```
// Missing days do not appear as zero rows. Check ingestion and retention separately.
let StartTime = datetime(2026-10-13T00:00:00Z);
let EndTime = now();
let TenantFilter = "";
AADServicePrincipalSignInLogs
| where TimeGenerated >= StartTime and TimeGenerated < EndTime
| where isempty(TenantFilter) or AADTenantId =~ TenantFilter
| summarize Records=count(), FirstRecord=min(TimeGenerated), LastRecord=max(TimeGenerated)
    by AADTenantId, DayUTC=bin(TimeGenerated, 1d)
| order by AADTenantId asc, DayUTC asc
```

01B / Available directory audit records. Run separately from 01A.

Microsoft Sentinel / Log Analytics KQL. Requires the named Entra tables and customer AADTenantId. Blank TenantFilter searches all visible tenants. Include the explicit UTC query interval in the portal picker.

Source attachment: skykick-hunt-starters.kql

```
let StartTime = datetime(2026-10-13T00:00:00Z);
let EndTime = now();
let TenantFilter = "";
AuditLogs
| where TimeGenerated >= StartTime and TimeGenerated < EndTime
| where isempty(TenantFilter) or AADTenantId =~ TenantFilter
| summarize Records=count(), FirstRecord=min(TimeGenerated), LastRecord=max(TimeGenerated)
    by AADTenantId, DayUTC=bin(TimeGenerated, 1d)
| order by AADTenantId asc, DayUTC asc
```

02 / Listed applications OR reported source addresses. Preserve failures and IPv6.

Microsoft Sentinel / Log Analytics KQL. Requires the named Entra tables and customer AADTenantId. Blank TenantFilter searches all visible tenants. Include the explicit UTC query interval in the portal picker.

Source attachment: skykick-hunt-starters.kql

```
// Public response indicators below are from ConnectWise, reviewed October 19.
let StartTime = datetime(2026-10-13T00:00:00Z);
let EndTime = now();
let TenantFilter = "";
let AppIds = dynamic([
    "506e08f9-6e9a-4da4-942b-a099a03644ae",
    "2399d300-6fca-4e6a-a686-399fefe75b83",
    "24205314-2b89-4e07-a2a4-579e898a5640",
    "b78f6a77-d4e5-46fb-87e5-d1648bd02519",
    "0de14c77-b9b0-4137-9360-34878a929827",
    "412dcf96-176d-4b3a-a1b0-4981ad66971e",
    "b2b55f5b-7758-4719-8d8f-88ae172e6bdb"
]);
let ReportedIPs = dynamic(["144.172.64.128", "144.172.64.99", "144.172.64.60"]);
AADServicePrincipalSignInLogs
| where TimeGenerated >= StartTime and TimeGenerated < EndTime
| where isempty(TenantFilter) or AADTenantId =~ TenantFilter
| extend ListedApp = AppId in~ (AppIds), ReportedIP = IPAddress in (ReportedIPs)
| where ListedApp or ReportedIP
| extend MatchBasis=case(ListedApp and ReportedIP, "app and IP", ListedApp, "app", "IP")
// Preserve raw result fields. Verify your tenant's values before classifying them.
| project TimeGenerated, AADTenantId, AppId, ServicePrincipalId, ServicePrincipalName,
    ResourceDisplayName, IPAddress, MatchBasis, ResultType, ResultSignature,
    ResultDescription, ClientCredentialType, ServicePrincipalCredentialKeyId,
    ServicePrincipalCredentialThumbprint, UserAgent, CorrelationId, Id
| order by TimeGenerated asc
```

03 / Broad access-change review, all actors and target identities in scope.

Microsoft Sentinel / Log Analytics KQL. Requires the named Entra tables and customer AADTenantId. Blank TenantFilter searches all visible tenants. Include the explicit UTC query interval in the portal picker.

Source attachment: skykick-hunt-starters.kql

```
// Intentional review queue, NOT a high-confidence alert. Authorized changes match.
// Keep failed and unknown results. TargetResources contains per-target properties.
// Category fallback retains relevant changes even if an operation name changes.
let StartTime = datetime(2026-10-13T00:00:00Z);
let EndTime = now();
let TenantFilter = "";
AuditLogs
| where TimeGenerated >= StartTime and TimeGenerated < EndTime
| where isempty(TenantFilter) or AADTenantId =~ TenantFilter
| where Category in~ ("ApplicationManagement", "RoleManagement", "Policy",
"UserManagement", "Audit")
    or OperationName contains "credential"
    or OperationName contains "Certificates and secrets"
    or OperationName contains "consent"
    or OperationName contains "owner"
    or OperationName contains "member to role"
| extend ActorAppId=tostring(InitiatedBy.app.appId),
    ActorServicePrincipalId=tostring(InitiatedBy.app.servicePrincipalId),
    ActorAppName=tostring(InitiatedBy.app.displayName),
    ActorUserId=tostring(InitiatedBy.user.id),
    ActorUPN=tostring(InitiatedBy.user.userPrincipalName),
    ActorIP=coalesce(tostring(InitiatedBy.user.ipAddress),
tostring(InitiatedBy.app.ipAddress)),
    AllTargets=TargetResources
// Preserve the parent event when targets are absent or an empty array.
| extend TargetsForExpansion=iff(coalesce(array_length(TargetResources), 0) == 0,
    dynamic([{}]), TargetResources)
| mv-expand Target=TargetsForExpansion
| extend TargetObjectId=tostring(Target.id), TargetType=tostring(Target.type),
    TargetName=tostring(Target.displayName), ModifiedProperties=Target.modifiedProperties
| project TimeGenerated, AADTenantId, Id, CorrelationId, Category, OperationName,
    Result, ResultReason, ActorAppId, ActorServicePrincipalId, ActorAppName,
    ActorUserId, ActorUPN, ActorIP, TargetObjectId, TargetType, TargetName,
    ModifiedProperties, AllTargets
| order by TimeGenerated asc
```

04 / Credential-use pivot AFTER confirming the target identity and key metadata.

Microsoft Sentinel / Log Analytics KQL. Requires the named Entra tables and customer AADTenantId. Blank TenantFilter searches all visible tenants. Include the explicit UTC query interval in the portal picker.

Source attachment: skykick-hunt-starters.kql

```
// Replace all three REPLACE values. These are keys/IDs, never secret values.
// Query deliberately returns nothing with placeholders; that is NOT a negative hunt.
// Credential IDs may be absent. Tokens can be reused without a new sign-in.
// Failed attempts are retained. Check the recorded outcome before inferring use.
let StartTime = datetime(2026-10-13T00:00:00Z);
let EndTime = now();
let TargetTenantId = "REPLACE_WITH_ENTRA_TENANT_GUID";
let TargetAppId = "REPLACE_WITH_APPLICATION_CLIENT_ID";
let TargetKeyId = "REPLACE_WITH_CREDENTIAL_KEY_ID";
AADServicePrincipalSignInLogs
| where TimeGenerated >= StartTime and TimeGenerated < EndTime
| where AADTenantId =~ TargetTenantId and AppId =~ TargetAppId
| where ServicePrincipalCredentialKeyId =~ TargetKeyId
| project TimeGenerated, AADTenantId, AppId, ServicePrincipalId, IPAddress,
    ResourceDisplayName, ResultType, ResultDescription, ClientCredentialType,
    ServicePrincipalCredentialKeyId, ServicePrincipalCredentialThumbprint, CorrelationId,
Id
| order by TimeGenerated asc
```

GS01 / Splunk: broad directory changes

Microsoft Graph v1.0 directoryAudit JSON, one original object per event. Audit-only, all outcomes. Customer source and event-time setup are required. Broad category review is independent of the listed-actor path.

Source attachment: skykick-graph-directoryaudit.spl

```
index=REPLACE_WITH_CUSTOMER_INDEX sourcetype=REPLACE_WITH_GRAPH_DIRECTORYAUDIT_SOURCE
| spath input=_raw path=id output=id
| spath input=_raw path=activityDateTime output=activityDateTime
| spath input=_raw path=activityDisplayName output=activityDisplayName
| spath input=_raw path=category output=category
| spath input=_raw path=initiatedBy.app.appId output=actorAppId
| spath input=_raw path=result output=result
| where in(lower(category), "applicationmanagement", "rolemanagement", "policy",
"usermanagement", "audit")
| fields _time, id, activityDateTime, activityDisplayName, category, actorAppId, result,
_raw
```

Broad category queue: authorized activity and failed or unknown results can match. Empty targets and missing app actors are not excluded. Compare this queue with the full directory timeline; changes in other categories can still matter.

GS02 / Splunk: listed app is actor

Microsoft Graph v1.0 directoryAudit JSON, one original object per event. Audit-only, all outcomes. Customer source and event-time setup are required. Broad category review is independent of the listed-actor path.

Source attachment: skykick-graph-directoryaudit.spl

```
index=REPLACE_WITH_CUSTOMER_INDEX sourcetype=REPLACE_WITH_GRAPH_DIRECTORYAUDIT_SOURCE
| spath input=_raw path=id output=id
| spath input=_raw path=activityDateTime output=activityDateTime
| spath input=_raw path=activityDisplayName output=activityDisplayName
| spath input=_raw path=category output=category
| spath input=_raw path=initiatedBy.app.appId output=actorAppId
| spath input=_raw path=result output=result
| where in(lower(actorAppId),
    "506e08f9-6e9a-4da4-942b-a099a03644ae",
    "2399d300-6fca-4e6a-a686-399fefe75b83",
    "24205314-2b89-4e07-a2a4-579e898a5640",
    "b78f6a77-d4e5-46fb-87e5-d1648bd02519",
    "0de14c77-b9b0-4137-9360-34878a929827",
    "412dcf96-176d-4b3a-a1b0-4981ad66971e",
    "b2b55f5b-7758-4719-8d8f-88ae172e6bdb")
| fields _time, id, activityDateTime, activityDisplayName, category, actorAppId, result,
_raw
```

This is an exact initiating application client-ID path. It does not search target application identities or credential properties. A listed application can operate legitimately; inspect authorization and outcome.

GL01 / LogScale: broad directory changes

Microsoft Graph v1.0 directoryAudit JSON, one original object per event. Audit-only, all outcomes. Customer source and event-time setup are required. Broad category review is independent of the listed-actor path.

Source attachment: skykick-graph-directoryaudit.cql

```
parseJson(field=@raw)
| in(field=category, values=["ApplicationManagement", "RoleManagement", "Policy",
"UserManagement", "Audit"], ignoreCase=true)
```

Broad category queue: authorized activity and failed or unknown results can match. Empty targets and missing app actors are not excluded. Compare this queue with the full directory timeline; changes in other categories can still matter.

GL02 / LogScale: listed app is actor

Microsoft Graph v1.0 directoryAudit JSON, one original object per event. Audit-only, all outcomes. Customer source and event-time setup are required. Broad category review is independent of the listed-actor path.

Source attachment: skykick-graph-directoryaudit.cql

```
parseJson(field=@raw)
| in(field="initiatedBy.app.appId", values=[
    "506e08f9-6e9a-4da4-942b-a099a03644ae",
    "2399d300-6fca-4e6a-a686-399fefe75b83",
    "24205314-2b89-4e07-a2a4-579e898a5640",
    "b78f6a77-d4e5-46fb-87e5-d1648bd02519",
    "0de14c77-b9b0-4137-9360-34878a929827",
    "412dcf96-176d-4b3a-a1b0-4981ad66971e",
    "b2b55f5b-7758-4719-8d8f-88ae172e6bdb"], ignoreCase=true)
```

This is an exact initiating application client-ID path. It does not search target application identities or credential properties. A listed application can operate legitimately; inspect authorization and outcome.

GU01 / Sumo: broad directory changes

Microsoft Graph v1.0 directoryAudit JSON, one original object per event. Audit-only, all outcomes. Customer source and event-time setup are required. Broad category review is independent of the listed-actor path.

Source attachment: skykick-graph-directoryaudit.sumo

```
_sourceCategory="REPLACE_WITH_CUSTOMER_GRAPH_DIRECTORYAUDIT_SOURCE"
| json "id", "activityDateTime", "activityDisplayName", "category",
"initiatedBy.app.appId", "result"
  as eventId, activityDateTime, activityDisplayName, category, actorAppId, result nodrop
| where category in ("ApplicationManagement", "RoleManagement", "Policy", "UserManagement",
 "Audit")
```

Broad category queue: authorized activity and failed or unknown results can match. Empty targets and missing app actors are not excluded. Compare this queue with the full directory timeline; changes in other categories can still matter.

GU02 / Sumo: listed app is actor

Microsoft Graph v1.0 directoryAudit JSON, one original object per event. Audit-only, all outcomes. Customer source and event-time setup are required. Broad category review is independent of the listed-actor path.

Source attachment: skykick-graph-directoryaudit.sumo

```
_sourceCategory="REPLACE_WITH_CUSTOMER_GRAPH_DIRECTORYAUDIT_SOURCE"
| json "id", "activityDateTime", "activityDisplayName", "category",
"initiatedBy.app.appId", "result"
  as eventId, activityDateTime, activityDisplayName, category, actorAppId, result nodrop
| if(isNull(actorAppId), "", toLowerCase(actorAppId)) as actorAppId
| where actorAppId in (
    "506e08f9-6e9a-4da4-942b-a099a03644ae",
    "2399d300-6fca-4e6a-a686-399fefe75b83",
    "24205314-2b89-4e07-a2a4-579e898a5640",
    "b78f6a77-d4e5-46fb-87e5-d1648bd02519",
    "0de14c77-b9b0-4137-9360-34878a929827",
    "412dcf96-176d-4b3a-a1b0-4981ad66971e",
    "b2b55f5b-7758-4719-8d8f-88ae172e6bdb")
```

This is an exact initiating application client-ID path. It does not search target application identities or credential properties. A listed application can operate legitimately; inspect authorization and outcome.

C00 / Visible authentication and cloud-audit records

Sophos Fusion Advanced Search, not SQL. Select customer, integration, and explicit UTC range. C02-C04 require available raw records; a raw GUID match does not establish its identity role.

Source attachment: skykick-sophos-searches.json

```
FROM auth, cloudaudit | aggregate count BY 1d
```

Separate counts per schema, not a combined incident count or proof of Entra service-principal coverage. Confirm integration, customer tenant, event time, ingestion lag, and the selected categories. An unrelated auth source can produce a healthy-looking chart.

C01 / Reported source addresses in authentication and cloud audit

Sophos Fusion Advanced Search, not SQL. Select customer, integration, and explicit UTC range. C02-C04 require available raw records; a raw GUID match does not establish its identity role.

Source attachment: skykick-sophos-searches.json

```
FROM auth, cloudaudit WHERE source_address IN
('144.172.64.128','144.172.64.99','144.172.64.60')
```

Retains all outcomes. Inspect the source event, identity, resource, and original result. An IP match is a review lead, not proof of unauthorized access.

C02 / Seven listed application IDs in original event content

Sophos Fusion Advanced Search, not SQL. Select customer, integration, and explicit UTC range. C02-C04 require available raw records; a raw GUID match does not establish its identity role.

Source attachment: skykick-sophos-searches.json

```
FROM auth, cloudaudit WHERE @raw CONTAINS '506e08f9-6e9a-4da4-942b-a099a03644ae' OR @raw
CONTAINS '2399d300-6fca-4e6a-a686-399fefe75b83' OR @raw CONTAINS
'24205314-2b89-4e07-a2a4-579e898a5640' OR @raw CONTAINS
'b78f6a77-d4e5-46fb-87e5-d1648bd02519' OR @raw CONTAINS
'0de14c77-b9b0-4137-9360-34878a929827' OR @raw CONTAINS
'412dcf96-176d-4b3a-a1b0-4981ad66971e' OR @raw CONTAINS
'b2b55f5b-7758-4719-8d8f-88ae172e6bdb'
```

Independent of the IP search; keeps other addresses, including IPv6. Substring matches may identify an actor, target, resource, or old/new property. Inspect the original JSON before assigning a role. Not an exact AppId-field filter.

C03 / Access-change review across all applications

Sophos Fusion Advanced Search, not SQL. Select customer, integration, and explicit UTC range. C02-C04 require available raw records; a raw GUID match does not establish its identity role.

Source attachment: skykick-sophos-searches.json

```
FROM cloudaudit WHERE @raw CONTAINS 'credential' OR @raw CONTAINS 'passwordCredentials' OR
@raw CONTAINS 'keyCredentials' OR @raw CONTAINS 'Certificates and secrets' OR @raw CONTAINS
 'member to role' OR @raw CONTAINS 'consent' OR @raw CONTAINS 'Add owner to' OR @raw
CONTAINS 'Remove owner from' OR @raw CONTAINS 'Update application' OR @raw CONTAINS 'Update
 service principal'
```

Broad triage, including legitimate changes and failed attempts. Does not restrict actors or targets to SkyKick. Inspect action, result, target object, actor, and before/after properties. Wording or parser differences can miss events; reconcile with the wider directory audit timeline.

C04 / Pivot on an investigated identity or credential key ID

Sophos Fusion Advanced Search, not SQL. Select customer, integration, and explicit UTC range. C02-C04 require available raw records; a raw GUID match does not establish its identity role.

Source attachment: skykick-sophos-searches.json

```
FROM auth, cloudaudit WHERE @raw CONTAINS 'REPLACE_WITH_VERIFIED_NONEMPTY_ID'
```

Replace the placeholder with a verified, nonempty target object ID, application client ID, or credential key ID, one at a time. Never use a secret value. Search matches are not a join: compare tenant, identity type, credential field, time, and result. A missing key field or reused token can leave this empty.

N01 / Supporting network pivot on either side

Sophos Fusion Advanced Search, not SQL. Select customer, integration, and explicit UTC range. C02-C04 require available raw records; a raw GUID match does not establish its identity role.

Source attachment: skykick-sophos-searches.json

```
FROM netflow WHERE @ip IN ('144.172.64.128','144.172.64.99','144.172.64.60')
```

Requires an ingested network source, such as configured firewall or endpoint telemetry. Inspect direction, allow/drop outcome, NAT, ports, and device context. Does not see attacker-to-Microsoft traffic that never crosses your monitored network.

L00 / Inventory of visible workload partitions in the selected window.

Sophos Live Discover Data Lake SQL; requires Microsoft 365 Management Activity xdr_identity_o365. Verify customer organization_id and time selector. This feed is not dedicated application sign-in history.

Source attachment: skykick-sophos-m365-datalake.sql

```
-- Counts do not prove continuous collection or dedicated SP sign-in coverage.
SELECT query_name, count(*) AS records
FROM xdr_identity_o365
GROUP BY query_name
ORDER BY query_name;
```

L01 / Listed requesting application OR reported client/actor IP in directory audit.

Sophos Live Discover Data Lake SQL; requires Microsoft 365 Management Activity xdr_identity_o365. Verify customer organization_id and time selector. This feed is not dedicated application sign-in history.

Source attachment: skykick-sophos-m365-datalake.sql

```
-- All outcomes retained. Exact IP strings can miss IP:port or alternate representations.
-- SELECT * preserves available source and metadata fields; handle exports as sensitive.
SELECT *
FROM xdr_identity_o365
WHERE query_name = 'AzureActiveDirectory'
  AND (
    lower(application_id) IN (
      '506e08f9-6e9a-4da4-942b-a099a03644ae',
      '2399d300-6fca-4e6a-a686-399fefe75b83',
      '24205314-2b89-4e07-a2a4-579e898a5640',
      'b78f6a77-d4e5-46fb-87e5-d1648bd02519',
      '0de14c77-b9b0-4137-9360-34878a929827',
      '412dcf96-176d-4b3a-a1b0-4981ad66971e',
      'b2b55f5b-7758-4719-8d8f-88ae172e6bdb'
    )
    OR client_ip IN ('144.172.64.128','144.172.64.99','144.172.64.60')
    OR actor_ip_address IN ('144.172.64.128','144.172.64.99','144.172.64.60')
  );
```

L02 / Broad access-change queue, independent of the app/IP list.

Sophos Live Discover Data Lake SQL; requires Microsoft 365 Management Activity xdr_identity_o365. Verify customer organization_id and time selector. This feed is not dedicated application sign-in history.

Source attachment: skykick-sophos-m365-datalake.sql

```
-- Strings are not parsed JSON. Inspect actor, target, result_status, and properties.
-- This keyword subset is not exhaustive; compare the wider directory audit timeline.
SELECT *
FROM xdr_identity_o365
WHERE query_name = 'AzureActiveDirectory'
  AND (
    lower(coalesce(operation, '')) LIKE '%credential%'
    OR lower(coalesce(operation, '')) LIKE '%member to role%'
    OR lower(coalesce(operation, '')) LIKE '%consent%'
    OR lower(coalesce(operation, '')) LIKE '%owner%'
    OR lower(coalesce(operation, '')) LIKE '%update application%'
    OR lower(coalesce(operation, '')) LIKE '%update service principal%'
    OR lower(coalesce(modified_properties, '')) LIKE '%passwordcredentials%'
    OR lower(coalesce(modified_properties, '')) LIKE '%keycredentials%'
    OR lower(coalesce(modified_properties, '')) LIKE '%credential%'
  );
```

E01 / Available IP-journal records within the window, by UTC day.

Sophos Windows Live Discover endpoint SQL. Run on authorized devices, record device scope, and use the same endpoint for sophos_pid pivots. Local journals do not prove tenant-wide cloud activity.

Source attachment: skykick-sophos-endpoint.sql

```
-- Missing days are absent, not zero-filled. Coverage must be checked separately.
SELECT date(time, 'unixepoch') AS day_utc,
       count(*) AS records,
       datetime(min(time), 'unixepoch') AS first_record_utc,
       datetime(max(time), 'unixepoch') AS last_record_utc
FROM sophos_ip_journal
WHERE time >= CAST(strftime('%s', '2026-10-13T00:00:00Z') AS INTEGER)
  AND time < CAST(strftime('%s', 'now') AS INTEGER)
GROUP BY date(time, 'unixepoch')
ORDER BY day_utc;
```

E02 / Reported IP on either side of a recorded endpoint connection event.

Sophos Windows Live Discover endpoint SQL. Run on authorized devices, record device scope, and use the same endpoint for sophos_pid pivots. Local journals do not prove tenant-wide cloud activity.

Source attachment: skykick-sophos-endpoint.sql

```
-- No process JOIN: retain events whose process context is unavailable.
-- A journal row is not proof of successful application traffic or compromise.
SELECT datetime(time, 'unixepoch') AS event_utc, time,
       pid, sophos_pid, process_start_time,
       source, source_port, destination, destination_port, protocol,
       CASE
         WHEN source IN ('144.172.64.128','144.172.64.99','144.172.64.60')
          AND destination IN ('144.172.64.128','144.172.64.99','144.172.64.60') THEN 'both'
         WHEN source IN ('144.172.64.128','144.172.64.99','144.172.64.60') THEN 'source'
         ELSE 'destination'
       END AS indicator_side
FROM sophos_ip_journal
WHERE time >= CAST(strftime('%s', '2026-10-13T00:00:00Z') AS INTEGER)
  AND time < CAST(strftime('%s', 'now') AS INTEGER)
  AND (source IN ('144.172.64.128','144.172.64.99','144.172.64.60')
    OR destination IN ('144.172.64.128','144.172.64.99','144.172.64.60'))
ORDER BY time;
```

E03 / Process context for an E02 hit, on the SAME endpoint.

Sophos Windows Live Discover endpoint SQL. Run on authorized devices, record device scope, and use the same endpoint for sophos_pid pivots. Local journals do not prove tenant-wide cloud activity.

Source attachment: skykick-sophos-endpoint.sql

```
-- Replace REPLACE_WITH_SOPHOS_PID with a nonempty sophos_pid from E02.
-- This is not the numeric Windows PID. Preserve the device identifier alongside it.
-- Explicit time bounds avoid the journal's default recent-only search.
-- Search retained process history, including starts before the incident window.
-- Start and end events are separate rows; a missing start may have aged out.
SELECT datetime(time, 'unixepoch') AS journal_utc, time, event_type,
       pid, sophos_pid, parent_sophos_pid, process_start_time,
       path, process_name, cmd_line
FROM sophos_process_journal
WHERE time >= 0
  AND time < CAST(strftime('%s', 'now') AS INTEGER)
  AND sophos_pid = 'REPLACE_WITH_SOPHOS_PID'
ORDER BY time;
```

Experimental Azure Sigma

Standard product azure / service auditlogs. Backend extraction of nested InitiatedBy.app fields is required. No backend conversion or tenant execution is claimed for this refresh.

skykick-entra-app-credential-events.yml

```
title: Entra ID Credential Related Audit Event with Application Actor
id: c90ce13e-ae7b-463a-a89f-4054cf18bc70
status: experimental
description: >-
  Review lead for credential-related audit events with a nonempty app actor ID.
  Includes removal/rotation and all results; does not prove a credential was added
  or abuse occurred. Read skykick-base-logic.txt for mapping and coverage limits.
references:
  - https://sigmahq.io/sigma-specification/specification/sigma-appendix-taxonomy.html
  - https://learn.microsoft.com/en-us/azure/azure-monitor/reference/tables/auditlogs
author: Deception Check
date: '2026-10-19'
logsource:
    product: azure
    service: auditlogs
    definition: >-
      Microsoft AuditLogs spelling; conversion must extract nested InitiatedBy.app
      fields as strings. Dotted field names require a validated backend mapping.
detection:
    selection_operation:
        OperationName|contains:
            - 'Certificates and secrets'
            - 'service principal credentials'
    selection_actor:
        - InitiatedBy.app.appId: '?*'
        - InitiatedBy.app.servicePrincipalId: '?*'
    condition: selection_operation and selection_actor
fields: [TimeGenerated, AADTenantId, Id, CorrelationId, OperationName, Result,
    ResultReason, InitiatedBy, TargetResources]
falsepositives:
    - Approved application credential rotation by CI/CD or infrastructure automation
    - Authorized vendor onboarding, credential removal, or remediation
    - System-initiated activity represented by an application identity
level: medium
tags: [attack.persistence, attack.t1098.001]
```

Experimental Azure Sigma

Standard product azure / service auditlogs. Backend extraction of nested InitiatedBy.app fields is required. No backend conversion or tenant execution is claimed for this refresh.

skykick-entra-app-role-events.yml

```
title: Entra ID Role Addition Related Audit Event with Application Actor
id: 7d6f9b4e-4976-41d6-a12e-f1b7f90c4813
status: experimental
description: >-
  Review lead for role-addition-related audit events with a nonempty app actor ID.
  Includes requests, cancellations, and all results; does not prove self-assignment
  or compromise. Read skykick-base-logic.txt for mapping and coverage limits.
references:
  - https://sigmahq.io/sigma-specification/specification/sigma-appendix-taxonomy.html
  - https://learn.microsoft.com/en-us/azure/azure-monitor/reference/tables/auditlogs
author: Deception Check
date: '2026-10-19'
logsource:
    product: azure
    service: auditlogs
    definition: >-
      Microsoft AuditLogs spelling; conversion must extract nested InitiatedBy.app
      fields as strings. Dotted field names require a validated backend mapping.
detection:
    selection_operation:
        OperationName|contains: 'member to role'
    selection_actor:
        - InitiatedBy.app.appId: '?*'
        - InitiatedBy.app.servicePrincipalId: '?*'
    condition: selection_operation and selection_actor
fields: [TimeGenerated, AADTenantId, Id, CorrelationId, OperationName, Result,
    ResultReason, InitiatedBy, TargetResources]
falsepositives:
    - Authorized vendor onboarding and application automation that assigns roles
    - Legitimate PIM requests, eligibility changes, approvals, and cancellations
    - System-initiated activity represented by an application identity
level: medium
tags: [attack.persistence, attack.privilege_escalation, attack.t1098.003]
```

Validation and source references

The new JSON routes were checked against primary schema/parser documentation and safe synthetic fixtures that read the final query files. Fixtures cover broad categories, actor identity, missing fields, empty targets, and retained results. A Python model of predicates does not execute SPL, CQL, or Sumo. The customer TEST-RECORD.txt records exact checks and limits.

The original KQL, Sophos, and Sigma source bytes are retained. Current author reruns cover 35 KQL static/modeled checks, 39 endpoint/Fusion checks, 21 portable Microsoft 365 SQL checks, and 32 Sigma synthetic cases. Endpoint and portable SQL run on synthetic SQLite tables; other predicates are modeled. Exact Sigma selectors were extracted from source text, without a YAML-parser check. These tests do not execute Sophos providers, Trino, Kusto, or a Sigma backend. Historical parser checks remain provenance. Confirm known events in the target platform before operational use.

No passwords, tokens, private keys, or customer events are included. Public advisory identifiers are the historical snapshot. Protect exported findings and collection metadata. No validated file or memory sample supports a YARA rule here.

https://learn.microsoft.com/en-us/graph/api/resources/directoryaudit?view=graph-rest-1.0

https://learn.microsoft.com/en-us/graph/api/directoryaudit-list?view=graph-rest-1.0

https://learn.microsoft.com/en-us/azure/azure-monitor/reference/tables/aadserviceprincipalsigninlogs

https://learn.microsoft.com/en-us/azure/azure-monitor/reference/tables/auditlogs

https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-configure-diagnostic-settings

https://help.splunk.com/en/splunk-enterprise/spl-search-reference/9.4/search-commands/spath

https://library.humio.com/crowdstrike-query-language/functions-parsejson.html

https://library.humio.com/crowdstrike-query-language/functions-in.html

https://help.sumologic.com/docs/search/search-query-language/parse-operators/parse-json-formatted-logs/

https://help.sumologic.com/docs/send-data/installed-collectors/sources/local-file-source/

https://help.sumologic.com/docs/send-data/hosted-collectors/http-source/logs-metrics/

https://docs.sophos.com/fusion/customer/help/en-us/ManageYourProducts/XDRSecOps/Integrations/Products/MicrosoftEntra/ActivityReports/Setup/index.html

https://docs.sophos.com/fusion/customer/help/en-us/ManageYourProducts/XDRSecOps/Search/DataLakeSearch/QueryLanguage/index.html

https://docs.sophos.com/fusion/customer/help/en-us/ManageYourProducts/XDRSecOps/Integrations/Products/Microsoft365/ManagementAPI/index.html

https://docs.sophos.com/central/References/schemas/schemas/xdr_identity_o365_schema_docs.json

https://docs.sophos.com/central/References/schemas/schemas/endpoint_schema.json

https://www.connectwise.com/company/trust/advisories

Advanced engineering appendix

The following complete October 19 source documents preserve all specialty normalized queries and mapping. They require engineering work and verified source fields. The dc_* fields are package-defined, not stock vendor telemetry or existing Deception Check instrumentation. Use the primary native-source routes first.

Historical filenames and cross-references below describe that earlier edition. All exact documents are embedded under ADVANCED/ and supplied in the ZIP.

query-logic-map.txt

```
DECEPTION CHECK / SKYKICK / PORTABLE HUNT LOGIC / 2026-10-19

Purpose: carry the investigation intent into another SIEM or EDR without assuming
that field names, event categories, or query syntax transfer unchanged. The PDF
prints every supplied query. This file describes the base predicates and mappings.
These are hunt starters and proposed triage decisions, not installed alerts.

COMMON GATES
1. Confirm customer tenant/workspace/integration; endpoint queries also need device.
2. Confirm the necessary source and category with a known source event.
3. Select an explicit UTC window and record the end time and actual retention.
   Default incident start is 2026-10-13T00:00:00Z; broaden to October 1 if retained.
   KQL/endpoint code uses a half-open [start, end) range. Fusion/Data Lake use their
   UI selectors; verify actual selector behavior and boundaries on that platform.
   SPL supplies earliest/latest; record the exclusive end. CQL also needs the UI/API
   window and its lower bound. Verify record versus activity and ingestion times.
4. Retain source event ID, tenant, event time, ingest time, raw result, and provenance.
5. Preserve missing context. Do not convert unavailable telemetry into a clean hunt.

AVAILABILITY
KQL 01A/01B: for each tenant and UTC day, count sign-in/audit records and retain first
and last timestamps. They are separate queries, so an absent table is not hidden.
Fusion C00: counts per schema per selected day, not combined incident counts.
Data Lake L00: counts by query_name workload partition, not sign-in coverage.
Endpoint E01: counts by UTC day plus first/last IP-journal record on each endpoint.
None of these queries fills missing days with zero or proves uninterrupted collection.

AUTHENTICATION / INDICATOR PATHS
Let ListedApps be the seven public application client IDs printed in KQL 02 / L01.
Let ReportedIPs be the three public addresses printed in KQL 02 / L01.

KQL 02 base selection:
  in_scope(event)
  AND (case_insensitive_exact(event.AppId, ListedApps)
       OR exact(event.IPAddress, ReportedIPs))

Do not change OR to AND. Do not remove IPv6 or filter to successes prematurely.
Keep raw results; a success still does not prove data access or exfiltration.

SPL SP01 and CrowdStrike CQL CS01 implement the same app OR address intent over
the declared dc_* contract. Read skykick-cross-platform-mapping.txt and apply its
verified source mapping first. These are templates, not native connector fields.

Fusion C01: reported source_address within auth/cloudaudit sources.
Fusion C02: any listed GUID appears as a substring in original event content.
These are separate searches; C02 is not equivalent to an exact AppId-field match.
Resolve whether the matching GUID is actor, target, resource, or a property value.

Data Lake L01: query_name = AzureActiveDirectory AND (lower(application_id) in the
listed apps OR client_ip in ReportedIPs OR actor_ip_address in ReportedIPs).
This is Microsoft 365 directory audit, not the dedicated sign-in table. Exact IP
```

strings can miss IP:port or alternate forms. Do not silently strip data without documenting and testing the normalization.

ACCESS CHANGES
KQL 03: selected broad directory-audit categories OR credential/certificate/consent/owner/role operation-name fallbacks, across all apps and actors. Retain outcomes. Expand all target objects while preserving empty-target parent events. Keep nested modifiedProperties with the correct target. Expanded targets are not new incidents.

Fusion C03: raw-content keyword matches for credentials, roles, owners, consent, and app/service-principal changes. Data Lake L02: operation and modified_properties text keywords in AzureActiveDirectory audit. These two keyword implementations do not provide the same category coverage or structured parsing as KQL 03.

Sigma S01/S02: narrower application-actor event predicates, detailed in skykick-base-logic.txt. They supplement the broad queries; they are not conversions. SPL SP02 and CQL CS02 retain the broad category/operation selection across all applications and actors. Entire nested actor/target JSON remains on the parent row; unlike KQL 03, these adapters do not expand targets. Inspect every target explicitly.

VERIFIED CREDENTIAL / IDENTITY PIVOT
KQL 04: exact case-insensitive match of verified tenant ID, application client ID, and credential key ID in the sign-in table. Replace all three placeholders.
Fusion C04: substring match for one verified nonempty identity/key ID in raw events. Do not treat it as an automatic join; establish identity type, tenant, and field. Never use a secret value. Missing key metadata or token reuse can leave a pivot empty. Compare successful/failed outcomes and the tenant's recorded containment timestamp.
SPL SP03 and CQL CS03 use the verified tenant/app/key tuple in mapped sign-in records. Their named query files retain all outcomes and need no secret values. Check UI and export limits before treating a projected result table as the complete timeline.

NETWORK + PROCESS CONTEXT
Endpoint E02: source OR destination equals a reported IP in the IP journal window. No inner join to process data, so a missing process record does not erase a hit.
Endpoint E03: same endpoint AND verified sophos_pid, with explicit retained-history time bounds. This is not a numeric Windows PID. Narrow deliberately because the process identifier is not indexed; inspect execution errors and truncation.
Fusion N01: reported address in logical @ip within netflow, with parser-dependent source/destination/NAT mappings. Inspect direction and outcome on the original record. These paths cannot see traffic that never crossed a monitored device or network.

TRIAGE / PROPOSED DECISIONS, NOT EXECUTED CORRELATION RULES
A. Successful, unapproved authentication from a reported address merits escalation. Keep attempts separate. Review unlisted addresses for implicated identities too.
B. Successful, unapproved credential/role/owner/consent changes merit escalation. Check the target object and approval evidence; an app actor does not prove abuse.
C. Confirmed unauthorized credential use or related resource activity after that tenant's recorded containment time merits escalation. Distinguish event time from late ingestion. Successful authentication is not itself proof of resource access.

For recurring detection, implement tenant-scoped deduplication by source event ID, appropriate late-arrival handling, a tested result mapping, change context, and an assigned response owner. Validate against positive, negative, absent-field, and missing-source cases in the destination environment. The package does not implement these scheduling, correlation, or response controls.

Continue into collected Graph and Microsoft 365 resource records. The supplied queries do not cover every mailbox, file, token, or policy action. An EDR installation alone does not imply collection of cloud-identity and workload logs.

Public indicators: https://www.connectwise.com/company/trust/advisories
Source schemas, validation boundaries, and language-specific instructions are in the companion PDF. Do not contact indicator infrastructure during validation.

README.txt

ADVANCED / ENGINEERING REFERENCE
Original October 19 normalized SPL/CQL and complete mapping retained.
These dc_* fields are package-defined and must be mapped from real Entra events.
They are not built-in vendor telemetry, universal imports, or existing Deception Check instrumentation.
Use the native source routes in ../SOURCE-GUIDE.txt first. Historical filenames and internal cross-references in these retained references describe the October 19 edition.

skykick-base-logic.txt

```
DECEPTION CHECK / SKYKICK RESPONSE / BASE LOGIC AND STANDARD RULES / 2026-10-19

Purpose
Two experimental Sigma rules provide narrower event-match review leads for Entra
directory audit data. They supplement the broad access-change queues in KQL 03,
SPL SP02, CrowdStrike CQL CS02, and Sophos Data Lake L02. They are not conversions and do
not replace
service-principal sign-in review, credential inventory, or the full audit timeline.
Sigma is a rule format; it does not collect logs or guarantee backend compatibility.
Read these mapping and result limitations before converting or enabling a rule.

EXACT BASE PREDICATES
Within the verified tenant and selected UTC investigation window:

APP_ACTOR(e) :=
  a nonempty string at e.InitiatedBy.app.appId
  OR a nonempty string at e.InitiatedBy.app.servicePrincipalId

S01(e) := APP_ACTOR(e)
  AND case_insensitive_contains(e.OperationName, "member to role")

S02(e) := APP_ACTOR(e)
  AND (case_insensitive_contains(e.OperationName, "Certificates and secrets")
       OR case_insensitive_contains(e.OperationName, "service principal credentials"))

In Sigma, the list of actor maps means OR; the condition joins actor and operation
with AND. The '?*' wildcard requires at least one character. Missing, null, and empty
actor strings do not match. It is not a GUID validator; whitespace-only or malformed
nonempty strings can match, so validate source field quality. These rules do not
filter Result, compare actor and target IDs, limit to the incident app/IP list,
select only privileged roles, or correlate multiple events. Tenant and time scoping
belong to the verified backend query, not to these portable event predicates.

S01 matches an operation-name family, including eligible/scoped additions, requests,
completions, and cancellations when the phrase is present. It does not establish
that the change completed. Inspect the operation, result, role, principal, and
approval context. Other role operations whose names lack the phrase are excluded.

S02 selects credential-related operation names. Matching ignores case and does not
depend on the dash before 'Certificates and secrets'. It can match removal and
rotation, and does not prove that a credential was added. Generic 'Update application'
without a matching phrase is excluded even when its nested properties describe a
credential change. Review such events in the broader queue. Inspect all target
resources and their modifiedProperties, compare old/new credential metadata, and
verify the current application/service-principal object before drawing conclusions.

REQUIRED SOURCE FIELDS AND MAPPING
Rule input spelling is Microsoft's Azure Monitor AuditLogs schema:

  OperationName                       string; operation-name predicate
  InitiatedBy.app.appId                nested string; application/client ID
```

```
  InitiatedBy.app.servicePrincipalId   nested string; tenant service-principal ID
```

At least one of the two actor IDs must be available for an app-actor match. Preserve both when present. Preserve user initiator information too; an app identity recorded here does not by itself establish that authentication was app-only. Microsoft also represents some system initiators as apps. Events with only an app display name or with only user-actor data are outside this rule pair and remain in the broad hunt.

For investigation, retain TimeGenerated, AADTenantId, Id, CorrelationId, OperationName, Result, ResultReason, the complete InitiatedBy object, and every TargetResources entry, including modifiedProperties. Do not assume the first target is the principal or that a top-level ModifiedProperties column exists. Do not compare an application client ID directly to a service-principal object ID. Establish the object types and tenant before evaluating self-assignment or an actor/target difference.

The Sigma logsource is product: azure / service: auditlogs, from Sigma's taxonomy. The nested field spellings describe actual Microsoft source properties. They are not promises that every SIEM stores or resolves dotted fields in this form. A Log Analytics conversion must resolve, for example, InitiatedBy.app.appId from the dynamic InitiatedBy object as a string. A backend that quotes the whole dotted name as an unrelated flat column needs a mapping/extraction fix before use.

Raw Microsoft Graph directoryAudit JSON uses initiatedBy (lowercase i) and activityDisplayName. Map those source fields explicitly if that is your feed. Do not silently equate them to a different connector's normalized fields. Sophos xdr_identity_o365 uses its own Microsoft 365 Management Activity schema and is not the direct input to these rules. Confirm the actual source, tenant identifiers, field types, parser, and conversion pipeline against a known event.

TRUTH FIXTURES / EXPECTED EVENT MATCHES
These are synthetic predicate examples, not observed incident records.

Operation or condition	App identity	S01	S02
Add member to role	appId populated	Y	N
Add member to role completed.	SP ID only	Y	N
Add eligible member to role	appId populated	Y	N
Add member to role canceled (PIM activation)	appId populated	Y	N
Remove member from role	appId populated	N	N
Add member to role	user only	N	N
Add member to role	IDs null/empty	N	N
Update application - Certificates and secrets management	appId populated	N	Y
Same operation with an en dash before Certificates	appId populated	N	Y
Add service principal credentials	SP ID only	N	Y
Remove service principal credentials	appId populated	N	Y
Update application; keyCredentials in properties only	appId populated	N	N
Matching operation; result=failure or unknown	appId populated	same	
Matching operation; absent targets	appId populated	same	
Matching operation; actor and target equal/different	appId populated	same	

VALIDATION RECORD
PyYAML 6.0.3 and pySigma 1.5.1 parsed both rules. The author checked 38 synthetic records, yielding 76 predicate assertions against the parsed Sigma conditions; all passed. An independent reviewer checked 32 synthetic predicate scenarios; all passed, including a rerun against the compact rule files supplied here. These checks use declared nested-field mapping and test predicate behavior. They

are not backend conversion, target-SIEM execution, or customer-tenant validation. No alert rule was enabled or changed. Local mapping, telemetry, runtime, and approved alert tuning still require validation before operational deployment.

DEPLOYMENT AND INTERPRETATION

Validate conversion output, table selection, case handling, '?*' wildcard behavior, JSON extraction, null/empty handling, and tenant/time scope in the actual backend. Run positive, negative, and missing-field samples before production use. Establish coverage and retention separately; zero hits cannot clear a tenant. Tune approved automation with tenant, actor, operation, target, and change context; blanket vendor app allowlists can hide abuse of an otherwise legitimate identity. A match is a review lead. Human-initiated abuse, alternate operation names, missing audit data, and absent actor IDs can be missed. No customer-tenant or target-SIEM execution is represented by the supplied rule files. ATT&CK tags describe investigative relevance, not proof that a technique occurred.

YARA: NOT INCLUDED

The supplied package contains cloud-identity/API evidence and no recovered file or memory artifact with distinctive content from which to author a useful YARA rule. YARA can examine file or process-memory content, but it does not provide the Entra event, actor, target, and result semantics used here. A rule matching public app IDs, IP addresses, generic OAuth text, or library user-agent strings in arbitrary files would not establish this abuse. Reassess YARA if a relevant artifact is recovered. This assessment does not claim that no malware exists anywhere in the incident.

PRIMARY REFERENCES

Sigma specification, including list/map, wildcard, and condition semantics:
https://sigmahq.io/sigma-specification/specification/sigma-rules-specification.html
Sigma taxonomy (azure / auditlogs):
https://sigmahq.io/sigma-specification/specification/sigma-appendix-taxonomy.html
Microsoft AuditLogs:
https://learn.microsoft.com/en-us/azure/azure-monitor/reference/tables/auditlogs
Microsoft auditActivityInitiator:
https://learn.microsoft.com/en-us/graph/api/resources/auditactivityinitiator?view=graph-rest-1.0
Microsoft appIdentity:
https://learn.microsoft.com/en-us/graph/api/resources/appidentity?view=graph-rest-1.0
Microsoft directoryAudit:
https://learn.microsoft.com/en-us/graph/api/resources/directoryaudit?view=graph-rest-1.0
Microsoft audit activity names:
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities
Microsoft Sentinel credential analytic (operation examples and target-property logic):
https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Microsoft%20Entra%20ID/Analytic%20Rules/NewAppOrServicePrincipalCredential.yaml
YARA documentation:
https://yara.readthedocs.io/en/stable/commandline.html

skykick-cross-platform-mapping.txt

DECEPTION CHECK / SKYKICK / SPLUNK AND CROWDSTRIKE ADAPTER NOTES / 2026-10-19

START HERE
The SPL and CQL files contain three read-only hunts each: application/IP sign-ins, broad authority/credential changes across all apps, and a confirmed credential-key pivot. These are mapping-required templates, not native-schema detections. No Splunk, Falcon, or LogScale runtime or customer-tenant execution is represented.

The dc_* names are this companion's deliberately small normalization contract. They are not Splunk CIM, CrowdStrike CPS/ECS, or built-in connector field names. Have the SIEM owner map the source records before running the searches. A saved search or view name alone does not create these fields. Preserve the original raw event and record the parser version/source so an analyst can verify each mapping.

TELEMETRY REQUIRED
Ingest both Entra service-principal sign-ins and directory audits for each tenant. An endpoint sensor alone does not supply either cloud event stream. A connector being installed does not prove that these event types, dates, tenants, or credential fields are collected. Inspect a known event from each stream and verify retention, ingestion health, permissions, and first/last available times before hunting.

The exact source mapping below is for Azure Monitor table-shaped records from AADServicePrincipalSignInLogs and AuditLogs. A raw Event Hub export, Graph feed, Splunk add-on, or Falcon connector can use a different envelope or field spelling. Unwrap the actual source first. For example, published Falcon Entra examples use Vendor.properties.* fields; its Graph examples use Vendor.* for some properties. Those examples do not establish the full service-principal sign-in mapping here. Map a verified sample, including nested objects; never blindly substitute prefixes. Splunk's documented azure:monitor:aad example uses lowercase tenantId/time and a properties object, illustrating why table spellings cannot be assumed on ingest. Microsoft 365 Management Activity records are a separate schema.

NORMALIZATION CONTRACT
Each normalized row represents one source event. All dc_* fields below are scalar strings; *_json fields contain complete serialized JSON. Missing source values remain null/missing, not invented success values. GUID fields must be canonical lowercase, without braces/whitespace; keep the original source alongside them. Keep source IPv4 and IPv6 as strings. The three reported IPv4s use exact equality; alternative IP encodings require a verified mapping and the original address.

Common mapping (both source tables)
  dc_event_kind   constant from verified source: entra_sp_signin OR
                      entra_directory_audit; never infer from outcome or app ID
  dc_tenant_id   AADTenantId (Entra tenant, NOT workspace TenantId)
  dc_event_time   TimeGenerated, preserved UTC timestamp string
  dc_event_id   Id
  dc_correlation_id   CorrelationId
  Splunk _time   parse TimeGenerated as UTC epoch seconds at ingestion
  CQL @timestamp   parse TimeGenerated as UTC epoch milliseconds at ingestion

Service-principal sign-ins (AADServicePrincipalSignInLogs)

```
  dc_activity_time       CreatedDateTime
  dc_app_id              AppId
  dc_sp_id               ServicePrincipalId
  dc_sp_name             ServicePrincipalName
  dc_source_ip           IPAddress
  dc_result_type         ResultType
  dc_result_signature    ResultSignature
  dc_result_description  ResultDescription
  dc_resource_name       ResourceDisplayName
  dc_credential_type     ClientCredentialType
  dc_key_id              ServicePrincipalCredentialKeyId
  dc_thumbprint          ServicePrincipalCredentialThumbprint
  dc_user_agent          UserAgent

Directory audit (AuditLogs)
  dc_activity_time       ActivityDateTime
  dc_category            Category
  dc_operation           OperationName
  dc_result              Result
  dc_result_reason       ResultReason
  dc_initiated_by_json   entire InitiatedBy object serialized without loss
  dc_targets_json        entire TargetResources array, including every target's
                         modifiedProperties, serialized without loss

TimeGenerated is the investigation filter used by this companion; AuditLogs
documents it as record creation time. Keep the separate activity timestamp shown
above and the platform's ingestion timestamp. Do not silently replace one with
another. Validate timezone, seconds versus milliseconds, delays, and the earliest
and latest source events. Extend the window when source timing requires it.

IMPLEMENTATION AND COMPLETENESS
Splunk: supply real index/sourcetype selectors, then create and verify the dc_*
fields through your source-specific extraction/normalization. If a field contains
raw JSON, explicit spath input/path/output extraction can be used; first confirm
the exact path and that the complete payload is retained. Do not depend on an
unverified automatic extraction or on a universal sourcetype. The supplied files
are SPL, not SPL2. Their triple-backtick comments are SPL search comments.

Falcon Next-Gen SIEM / LogScale: choose the repository/view with the verified
Entra feeds and expose the contract through your parser or tested query adapter.
No #repo, #event_simpleName, or Vendor.* value is asserted by these templates.
Set the UI/API time range explicitly; a query's lower bound cannot recover events
excluded by the picker. Use the recorded exclusive end for every comparison.

Copy one numbered block. Replace every REPLACE value. Default start is October 13,
2026, 00:00 UTC. Extend to October 1 where history permits. SPL provides the start
and latest=now; record execution time or insert a fixed exclusive epoch end.
CQL also requires the selected UI/API UTC end and a picker spanning the start.

The queries preserve individual rows and do not prove export completeness. CQL
select() can display only the last 200 events in a standard query; its export path
is intended for matching event rows. Verify the actual export and service limits.
Splunk table can truncate results under limits.conf search settings as well.
For both platforms, compare pre-projection match counts with exported rows, inspect
warnings, and split large windows into adjacent non-overlapping intervals if needed.
```

Do not treat the visible table as the complete timeline. Keep tenant plus source event ID when reconciling duplicates; retain separate source streams.

HOW TO READ THE THREE HUNTS

01: A listed app OR a reported source address matches. Known apps on new addresses, IPv6 app matches, failures, unknown outcomes, and IP matches for other apps remain in scope. A listed vendor application can have legitimate activity. Confirm the outcome, resource, tenant, credential, and surrounding actions before concluding that access succeeded or was unauthorized. IDs/IPs are unchanged from KQL 02.

02: The category fallback plus operation phrases creates a broad review queue. It includes other applications, all actor types, and failed/unknown outcomes; there is no incident-app filter or success-only filter. Authorized changes match. Generic Update application events can enter through ApplicationManagement even when only their nested properties describe credential changes. Inspect every target and old/new credential metadata. Events without target entries remain one parent row. App display names and an app initiator do not establish app-only authentication; verify initiator IDs and actor context. Unexpected operation names/categories outside this predicate can be missed.

03: After confirming tenant, application/client ID, and key ID from the changed object, pivot on all three. Never substitute a service-principal object ID for an application/client ID, or paste secret values. A match can be a failed attempt; read the preserved result. Missing key IDs and reuse of an already-issued token can produce no new matching sign-in. A zero result is not clearance.

PRIMARY REFERENCES (opened 2026-10-19)

Microsoft source schema: service-principal sign-ins
https://learn.microsoft.com/en-us/azure/azure-monitor/reference/tables/aadserviceprincipalsigninlogs
Microsoft source schema: directory audit
https://learn.microsoft.com/en-us/azure/azure-monitor/reference/tables/auditlogs
Splunk SPL conditional predicates: in, if, coalesce, and like
https://help.splunk.com/en/splunk-enterprise/search/spl-search-reference/10.0/evaluation-functions/comparison-and-conditional-functions
Splunk lower() and text functions
https://help.splunk.com/en/splunk-enterprise/search/spl-search-reference/10.0/evaluation-functions/text-functions
Splunk table projection and truncation behavior
https://help.splunk.com/en/splunk-enterprise/search/spl-search-reference/10.0/search-commands/table
Splunk epoch/time modifiers
https://help.splunk.com/en/splunk-enterprise/search/spl-search-reference/10.0/time-format-variables-and-modifiers/time-modifiers
Splunk explicit JSON extraction
https://help.splunk.com/en/splunk-enterprise/search/spl-search-reference/9.0/search-commands/spath
Splunk Data Inputs source-type examples and Entra event envelope
https://help.splunk.com/en/splunk-cloud-platform/ingest-data-from-cloud-services/data-inputs-user-manual/1.17/getting-data-in-gdi/overview-of-source-types-for-data-inputs
Splunk search comment syntax
https://help.splunk.com/en/splunk-enterprise/search/search-manual/9.1/using-the-search-app/add-comments-to-searches
CrowdStrike CQL in(), including case-based OR and case-insensitive matching
https://library.humio.com/crowdstrike-query-language/functions-in.html

CrowdStrike CQL operators and regular-expression filtering
https://library.humio.com/crowdstrike-query-language/syntax-operators.html
CrowdStrike CQL select() and standard-query display/export distinction
https://library.humio.com/crowdstrike-query-language/functions-select.html
CrowdStrike Entra data connector availability, not a full field-map guarantee
https://marketplace.crowdstrike.com/listings/data-connector-built-for-microsoft-entra-id/
CrowdStrike examples distinguishing Entra and Graph parser envelopes
https://www.crowdstrike.com/en-us/blog/defending-against-scattered-spider-with-falcon-next-gen-siem/

skykick-crowdstrike.cql

```
// DECEPTION CHECK / SKYKICK / FALCON NEXT-GEN SIEM / LOGSCALE / 2026-10-19
// Run ONE numbered block at a time after reading skykick-cross-platform-mapping.txt.
// Mapping-required, read-only CQL hunt starters; not deployed detections.
// dc_* are OUR normalized fields, not native Falcon/CPS/ECS connector field names.
// Select the verified repository/view containing both required Entra event feeds.
// Replace tenant in every block; replace app/key in CS03 with confirmed IDs.
// Set the UI/API UTC range explicitly: October 13, 2026 00:00 inclusive to a
// recorded exclusive end. @timestamp lower bound below uses epoch milliseconds.
// To extend to October 1, change BOTH the picker and bound to 1790812800000.
// Verify @timestamp is TimeGenerated, not ingestion time, and record the window.
// select() preserves matching rows for export; the UI may show only 200 events.
// Check export counts and limits; see mapping notes. Native runtime not tested.

// CS01 / Listed applications OR reported source addresses.
dc_event_kind="entra_sp_signin" dc_tenant_id="REPLACE_WITH_ENTRA_TENANT_GUID"
| @timestamp >= 1791849600000
| case {
    in(dc_app_id, ignoreCase=true, values=[
        "506e08f9-6e9a-4da4-942b-a099a03644ae",
        "2399d300-6fca-4e6a-a686-399fefe75b83",
        "24205314-2b89-4e07-a2a4-579e898a5640",
        "b78f6a77-d4e5-46fb-87e5-d1648bd02519",
        "0de14c77-b9b0-4137-9360-34878a929827",
        "412dcf96-176d-4b3a-a1b0-4981ad66971e",
        "b2b55f5b-7758-4719-8d8f-88ae172e6bdb"]);
    in(dc_source_ip, values=[
        "144.172.64.128","144.172.64.99","144.172.64.60"]);
}
| select([@timestamp, dc_event_time, dc_activity_time, dc_tenant_id,
    dc_event_id, dc_correlation_id, dc_app_id, dc_sp_id, dc_sp_name,
    dc_source_ip, dc_result_type, dc_result_signature, dc_result_description,
    dc_resource_name, dc_credential_type, dc_key_id, dc_thumbprint,
    dc_user_agent])

// CS02 / Broad authority and credential review, including other apps.
dc_event_kind="entra_directory_audit" dc_tenant_id="REPLACE_WITH_ENTRA_TENANT_GUID"
| @timestamp >= 1791849600000
| case {
    in(dc_category, ignoreCase=true, values=["ApplicationManagement",
        "RoleManagement","Policy","UserManagement","Audit"]);
    dc_operation=/credential|Certificates and secrets|consent|owner|member to role/i;
}
| select([@timestamp, dc_event_time, dc_activity_time, dc_tenant_id,
    dc_event_id, dc_correlation_id, dc_category, dc_operation,
    dc_result, dc_result_reason, dc_initiated_by_json, dc_targets_json])

// CS03 / Confirmed application and credential key pivot.
dc_event_kind="entra_sp_signin" dc_tenant_id="REPLACE_WITH_ENTRA_TENANT_GUID"
| @timestamp >= 1791849600000
| in(dc_app_id, ignoreCase=true, values=["REPLACE_WITH_APPLICATION_CLIENT_ID"])
| in(dc_key_id, ignoreCase=true, values=["REPLACE_WITH_CREDENTIAL_KEY_ID"])
```

```
| select([@timestamp, dc_event_time, dc_activity_time, dc_tenant_id,
    dc_event_id, dc_correlation_id, dc_app_id, dc_sp_id, dc_source_ip,
    dc_result_type, dc_result_signature, dc_result_description,
    dc_resource_name, dc_credential_type, dc_key_id, dc_thumbprint])
```

skykick-splunk.spl

```
``` DECEPTION CHECK / SKYKICK / SPL (not SPL2) / 2026-10-19
Run ONE numbered block at a time after reading skykick-cross-platform-mapping.txt.
These are mapping-required, read-only hunt starters, not deployed detections.
dc_* are OUR normalized fields, not native Splunk CIM or connector field names.
Replace index, sourcetype, and Entra tenant placeholders in every block.
earliest=1791849600 is 2026-10-13T00:00:00Z; latest=now ends at execution time.
For repeatable results replace latest=now with a recorded exclusive epoch end.
Extend earliest to 1790812800 (October 1 UTC) where retention permits.
Verify _time comes from TimeGenerated, ingestion coverage, and export completeness.
Preserve outcomes. Zero matches do not clear a tenant. Native runtime not tested.
```

``` SP01 / Listed applications OR reported source addresses. ```
index=REPLACE_WITH_INDEX sourcetype=REPLACE_WITH_SOURCETYPE
earliest=1791849600 latest=now
dc_event_kind="entra_sp_signin" dc_tenant_id="REPLACE_WITH_ENTRA_TENANT_GUID"
| eval listed_app=if(in(lower(coalesce(dc_app_id,"")),
    "506e08f9-6e9a-4da4-942b-a099a03644ae",
    "2399d300-6fca-4e6a-a686-399fefe75b83",
    "24205314-2b89-4e07-a2a4-579e898a5640",
    "b78f6a77-d4e5-46fb-87e5-d1648bd02519",
    "0de14c77-b9b0-4137-9360-34878a929827",
    "412dcf96-176d-4b3a-a1b0-4981ad66971e",
    "b2b55f5b-7758-4719-8d8f-88ae172e6bdb"),1,0)
| eval reported_ip=if(in(coalesce(dc_source_ip,""),
    "144.172.64.128","144.172.64.99","144.172.64.60"),1,0)
| where listed_app=1 OR reported_ip=1
| table _time dc_event_time dc_activity_time dc_tenant_id dc_event_id
    dc_correlation_id dc_app_id dc_sp_id dc_sp_name dc_source_ip
    listed_app reported_ip dc_result_type dc_result_signature
    dc_result_description dc_resource_name dc_credential_type
    dc_key_id dc_thumbprint dc_user_agent

``` SP02 / Broad authority and credential review, including other apps. ```
index=REPLACE_WITH_INDEX sourcetype=REPLACE_WITH_SOURCETYPE
earliest=1791849600 latest=now
dc_event_kind="entra_directory_audit" dc_tenant_id="REPLACE_WITH_ENTRA_TENANT_GUID"
| eval category_lc=lower(coalesce(dc_category,"")),
    operation_lc=lower(coalesce(dc_operation,""))
| where in(category_lc,"applicationmanagement","rolemanagement",
    "policy","usermanagement","audit")
    OR like(operation_lc,"%credential%")
    OR like(operation_lc,"%certificates and secrets%")
    OR like(operation_lc,"%consent%") OR like(operation_lc,"%owner%")
    OR like(operation_lc,"%member to role%")
| table _time dc_event_time dc_activity_time dc_tenant_id dc_event_id
    dc_correlation_id dc_category dc_operation dc_result dc_result_reason
    dc_initiated_by_json dc_targets_json

``` SP03 / Confirmed application and credential key pivot. ```
index=REPLACE_WITH_INDEX sourcetype=REPLACE_WITH_SOURCETYPE
```
```

```
earliest=1791849600 latest=now
dc_event_kind="entra_sp_signin" dc_tenant_id="REPLACE_WITH_ENTRA_TENANT_GUID"
| where lower(dc_app_id)=lower("REPLACE_WITH_APPLICATION_CLIENT_ID")
    AND lower(dc_key_id)=lower("REPLACE_WITH_CREDENTIAL_KEY_ID")
| table _time dc_event_time dc_activity_time dc_tenant_id dc_event_id
    dc_correlation_id dc_app_id dc_sp_id dc_source_ip dc_result_type
    dc_result_signature dc_result_description dc_resource_name
    dc_credential_type dc_key_id dc_thumbprint
```