

KEEN

KEY EVIDENCE ENGINE

Evidence first. Assurance connected.



Turn the work your organisation already does into evidence you can map, measure and audit.

COLLECT

MAP

AUDIT

IMPROVE

KEY EVIDENCE ENGINE

Your assurance workspace

Review what your evidence supports, decide what needs attention, and explore the connections.

ISO/IEC 27001:2022

Change framework using the navigation menu.

LATEST EVIDENCE · INSTALLATION-WIDE ed :: [mig5 supplier news] DumpTales gets a C heart: a conversational tour of nati

Find evidence

Search events...



Search the evidence available in this framework view.

Control evidence coverage

33%

31 of 93 in-scope controls have evidence

Framework clauses

41

Explore the clause hierarchy

Events mapped

77

Attributed to this framework

Events awaiting mapping

37

Not mapped to this framework

What would you like to do?

- Review evidence →
- Create an evidence mapping →
- Plan or run an audit →
- Review the risk register →
- Record an effectiveness measurement →

Needs attention

Refresh

62 control gaps 0 overdue audits 3 measures outside threshold 0 API collectors with failures · all frameworks

37 events awaiting mapping

Review events and create rules for the evidence you need.

A.5.1 Policies for information security

In-scope control without evidence

A.5.10 Acceptable use of information and other associated assets

In-scope control without evidence

One workspace for evidence, framework coverage, risks and the next action.

Explore KEEN / keen.cloud

01 / COLLECT

Bring your evidence together.

Connect the systems where work happens, then collect the records that demonstrate it.

Ready-made ingesters

Loki • Amazon CloudWatch Logs
GitHub • GitLab • Forgejo • Gitea
Jenkins • Redmine • Taiga
BookStack • Google Workspace • RSS

Build your own API ingester

Configure supported HTTP APIs in the web UI: endpoints, authentication, paths, query parameters, payloads, pagination and event fields. Preview responses and schedule collection.

KEEN Agent + webhooks

Ship server logs directly with the OTLP-based KEEN Agent: journald/syslog, nginx, PHP, package-manager and auditd evidence. Receive events and measurements through inbound webhooks. Add diary evidence for work recorded by people.

Events

Search and slice evidence by source, clause, actor/system — then jump to sampling.

Events

Visualisations

Filters

Expand

Results

1–50 of 114

Export

50

Prev

Next

Time	Source	Identifier	Summary	Mapped controls	Links	Artifacts
2026-10-07 04:06:35	Demo seed		Demo Fictional demo dataset			0
2026-10-06 19:50:00	Forgejo	git.mig5.net/mig5/keen-demo	Demo Forgejo KEEN demo release published with ISMS seed data	A.8.25 A.8.31 A.8.32	🔗	0
2026-10-06 17:02:00	Github	demo-org/keen-demo	Demo GitHub release published for KEEN demo version 1.2.0	A.8.25 A.8.31 A.8.32		0
2026-10-06 10:00:00	Demo	fictional.example.invalid	Demo Asset register reconciliation	A.5.9		0
2026-10-06 10:00:00	Demo	fictional.example.invalid	Demo Firewall rule review	A.8.9		0
2026-10-06 10:00:00	Demo	fictional.example.invalid	Demo Access review exception			0

Events bring records from different tools into a common, searchable evidence view.

Collect with care. Redact recognised secret values and configured sensitive keys; optionally mask email and IP addresses. Agent redaction patterns let you remove organisation-specific strings before delivery.

Make each event meaningful.

Build rules that connect operational activity to the controls and clauses it supports.

Start with a real event

Choose “Create mapping from this event” to prefill observed values. Match source, action, outcome and structured fields such as host, package, HTTP status, path or IP address.

Preview before applying

Name what the evidence demonstrates, explore suggested controls and check matching examples. Reuse rules for incoming events and apply them to relevant historical evidence.

Create an evidence definition

Back to definitions

Step 2 of 3 · Name and choose controls

Mapping name — what does this evidence demonstrate?

Supplier security updates and service notices

Use a meaningful name. Control suggestions use this text; change it and request suggestions again to explore other matches.

2. Select framework controls or clauses

The selected control is included when you click Next. To map to several controls or frameworks, click Add for each extra target. Every matching event maps to all selected targets.

Framework

Control or clause

ISO/IEC 27001:2022

A.5.1 — Policies for information security

Add

Suggest relevant controls

A.5.21 · Managing information security in the ICT supply chain

Matched: chain, security, supply. Click to add; review suitability before publishing.

A.5.19 · Information security in supplier relationships

Matched: security, supplier. Click to add; review suitability before publishing.

A.5.20 · Addressing information security within supplier agreements

Matched: security, supplier. Click to add; review suitability before publishing.

4.4 · Information Security Management System

Name the evidence and choose its target controls in the same guided workflow.

Multiple frameworks. Shared evidence.

Use ISO/IEC 27001:2022, Cyber Essentials, the KEEN Assurance Framework or the UK Digital Verification Services Trust Framework. Create and edit your own frameworks. Map one rule to several frameworks, and approve cross-framework control links to reuse evidence where requirements overlap.

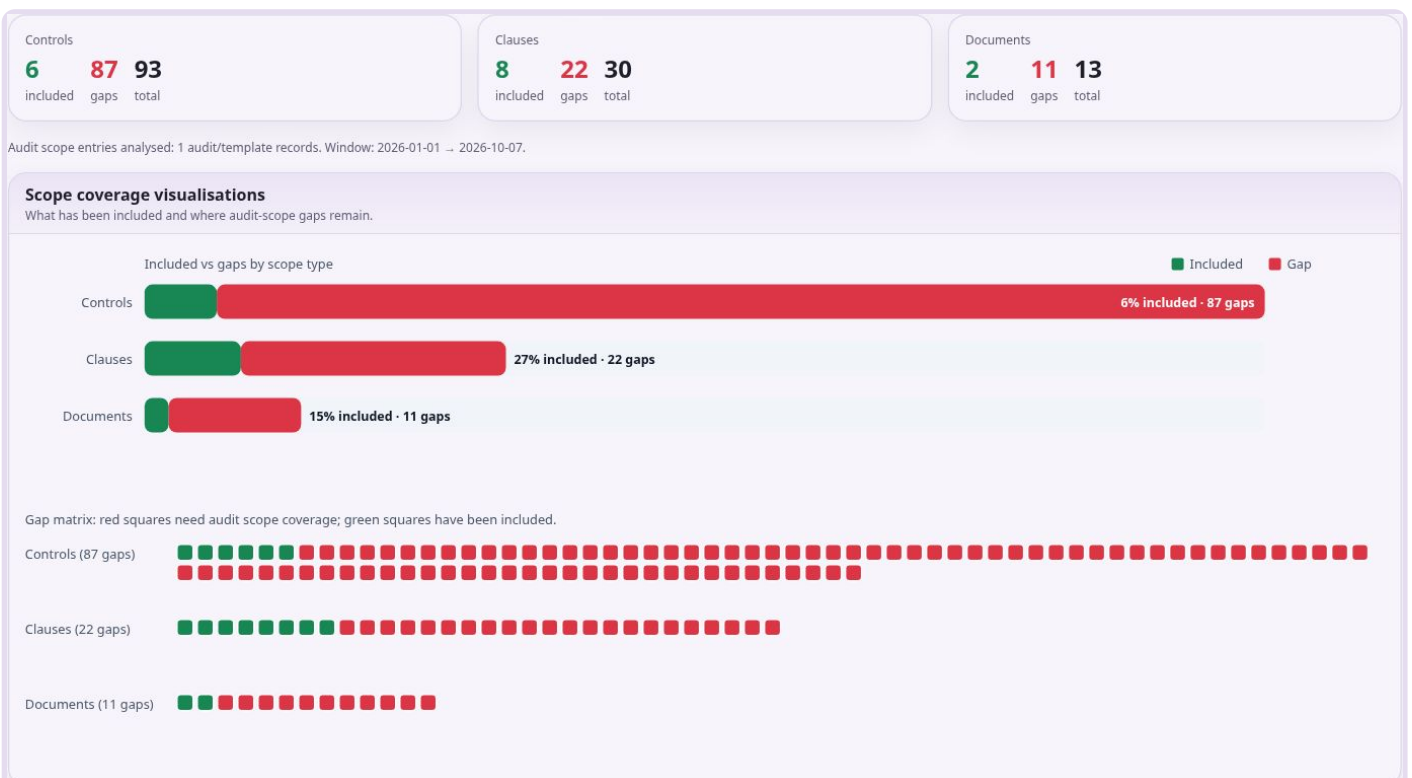
03 / AUDIT

From record to review.

Plan recurring audits or start one on demand. Keep scope, people, evidence and findings together.

Audit register									
Audits are shared between all auditors; the original author is retained.									
Filter by title...									
All statuses ▼ Reload									
Audit	Framework	Type	Dates	Author	Evidence	Scope	Findings	Status	Actions
Demo ISO27001:2022 Quarterly access review review Updated 2026-10-07 04:06:37	ISO27001:2022	Internal	2026-10-07 → 2026-10-14	workspace-owner	1	1 0 documents, 0 clauses, 1 controls	0	Open	Open Delete
Demo ISO27001:2022 Asset register reconciliation review Updated 2026-10-07 04:06:37	ISO27001:2022	Internal	2026-10-07 → 2026-10-14	workspace-owner	1	1 0 documents, 0 clauses, 1 controls	0	Open	Open Delete
Demo ISO27001:2022 Measured assurance review Updated 2026-10-07 04:06:37	ISO27001:2022	Internal	2026-10-07 → 2026-10-14	workspace-owner	11	3 0 documents, 0 clauses, 3 controls	0	In progress	Open Delete
Demo Incident Preparedness and Continuity Audit Updated 2026-10-07 04:06:36	ISO27001:2022	Internal	2026-08-23 → 2026-09-07	workspace-owner	4	13 2 documents, 5 clauses, 6 controls	0	Completed	Open Delete
Demo Supplier and Interested Parties Assurance Audit Updated 2026-10-07 04:06:36	ISO27001:2022	External	2026-10-22 → 2026-11-06	workspace-owner	3	11 2 documents, 4 clauses, 5 controls	0	Open	Open Delete
Demo Access Control and Operations Internal Audit Updated 2026-10-07 04:06:36	ISO27001:2022	Internal	2026-10-02 → 2026-10-17	workspace-owner	4	12 2 documents, 5 clauses, 5 controls	0	In progress	Open Delete

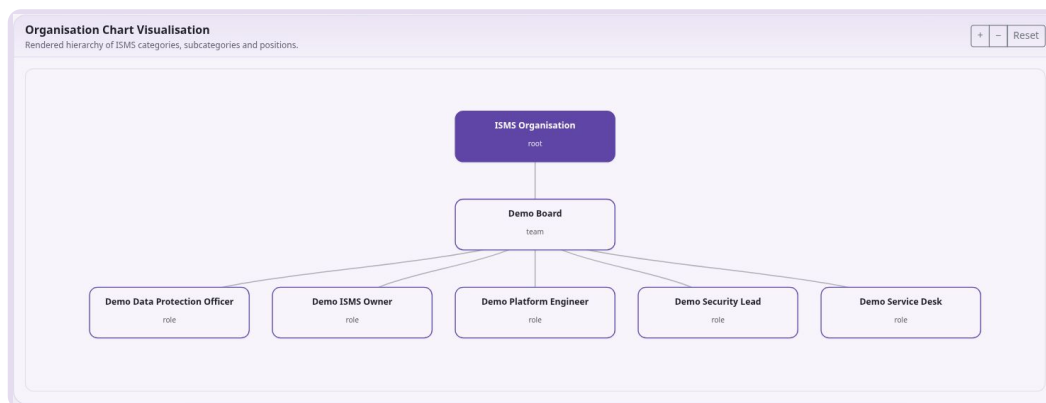
Audit register: track dates, scope, sampled evidence, findings and status.



Scope Coverage highlights included controls, clauses and documents, plus gaps to address.

Your ISMS, in one place.

Connect the people, assets, policies and decisions behind your information security management system.



Organisation charts make responsibility visible across the ISMS.

Access Control Matrix
Task/action and service access cross-referenced to managed hosting accounts, approval state, approver and organisation roles.

4 + Add new access row Manage hosting accounts

Service	Task/Action	Managed Hosting Accounts	Status	Approved by	Demo Data Protection Officer	Demo ISMS Owner	Demo Platform Engineer	Demo Security Lead	Demo Service Desk	Notes	Actions
Demo Customer Data Store	Demo Rotate backup restore credentials	Demo Backup Host...	Pending Approval	—			✓				
Demo KEEN Demo Web App	Demo Deploy application release to staging	Demo Staging Host...	Approved	workspace-o...			✓	✓			
Demo Production Platform	Demo Approve production administrator access	Demo Production H...	Approved	workspace-o...			✓	✓			
Demo Service Desk Team	Demo Triage customer security request	Demo Production H... Demo Staging Host...	Approved	workspace-o...	✓				✓		

Access Control Matrix: connect services and tasks with roles, approval state and approvers.

Assets and ownership

Maintain an asset matrix, categories, owners, licensing and CIA risk associations. Connect assets with applicable controls and clauses.

Access and accountability

Record service access, tasks, roles, approval state and approvers. Maintain people and supplier assurance records.

Policies and documents

Write in KEEN, upload files or link to external content. Organise policies and processes, including BookStack content when its ingester is enabled.

Objectives and decisions

Manage objectives, meeting agendas and minutes, attendees and supporting records. Link governance activity to framework requirements.

05 / ASSESS

Turn risk into action.

Describe the scenario, understand the impact and identify the controls that can help.

Risk register

One set of risks, rated by inherent and residual likelihood × impact, with CIA associations and framework controls.

Risk register & heatmap

Reusable risk library

5×5 heatmap

Cells show the number of rated risks at each likelihood and impact. Choose inherent or residual scores. Thresholds apply to the entire register.

☒ Inherent
 ☐ Residual

Likelihood \ Impact	1	2	3	4	5
5	0	0	0	0	0
4	0	0	0	4	1
3	0	0	1	5	1
2	0	0	0	0	0
1	0	0	0	0	0

Impact increases left to right; likelihood increases bottom to top.

Low through

Moderate through

High through

4

9

16

Save thresholds

Scores above the high threshold are critical.

Risk and treatment register

Filter scenario or asset

Asset	Scenario / CIA	Owner	Inherent	Residual	Treatment	Controls
Demo Production Platform	Demo UK-DVSTF:1.0 Recovery objectives review gap confidentiality / integrity / availability	workspace-owner	16 - High	6 - Moderate	mitigate open - due 2026-10-21	0 Rate / treat
Demo Production Platform	Demo UK-DVSTF:1.0 Information classification review gap confidentiality / integrity / availability	workspace-owner	12 - High	6 - Moderate	mitigate open - due 2026-10-21	0 Rate / treat
Demo Production Platform	Demo CYBER-ESSENTIALS:2026 Unused software removal gap confidentiality / integrity / availability	workspace-owner	16 - High	6 - Moderate	mitigate open - due 2026-10-21	0 Rate / treat
Demo Production Platform	Demo CYBER-ESSENTIALS:2026 Firewall rule review gap confidentiality / integrity / availability	workspace-owner	12 - High	6 - Moderate	mitigate open - due 2026-10-21	0 Rate / treat

Compare inherent and residual likelihood × impact in the 5×5 heatmap and treatment register.

A practical risk register

Record owners, treatment plans and control associations. Assess Confidentiality, Integrity and Availability, and start from reusable risk-library entries.

Meet the KEEN Mitigator

Describe a concern in natural language. The wizard suggests risk and control associations using CIA, PESTLE(E) and interested-party signals. In KEEN Assurance Framework scope, it also draws on the reusable risk library.



See the wider context. PESTLE(E) captures political, economic, social, technological, legal and environmental factors, with an ethical lens. Review suggestions and decide what applies to your organisation.

06 / MEASURE

See what is working. See what needs attention.

Compare recorded performance with clear targets, backed by a history of measurements.

ISMS Effectiveness Measures							
Effectiveness measures with latest and historic metric entries.							
7 + Add new effectiveness measure							
Summary / description	Effectiveness measure	Metric	Latest value	Target	Owner	Controls	Actions
Demo Verified restore time against recovery objective Fictional worked example: measured performance, source evidence and follow-up. These targets are example organisational objectives, not prescribed certification thresholds. DEMO-SLA-IS027001:2022-recovery	One scheduled synthetic restore test per month. Elapsed minutes from test declaration to restored-service validation, including checksum and application checks. Target ≤60 minutes.	Verified restore time against recovery objective	39 minutes Meets target 2026-09-01 - 2026-09-30 · Demo Synthetic monthly measurement report · e2aab91b-96e3-45c4-a28b-4bdfecd54642 6 metric entries in metric history	≤ 60 minutes	workspace-owner	A.8.13	    
Demo Critical updates installed within 14 days Fictional worked example: measured performance, source evidence and follow-up. These targets are example organisational objectives, not prescribed certification thresholds. DEMO-SLA-IS027001:2022-patch_sla	100 synthetic critical-update obligations due each month. Count those installed within 14 days of release, divided by all obligations due, × 100. No exceptions excluded.	Critical updates installed within 14 days	97 % Meets target 2026-09-01 - 2026-09-30 · Demo Synthetic monthly measurement report · d57d428f-f74f-4c00-8c0f-45c8e86d343f 6 metric entries in metric history	≥ 95 %	workspace-owner	A.8.8	    
Demo Service availability SLA Fictional worked example: measured performance, source evidence and follow-up. These targets are example organisational objectives, not prescribed certification thresholds. DEMO-SLA-IS027001:2022-availability	Calendar-month availability = 100 × (eligible minutes – unavailable minutes) / eligible minutes. All minutes included; no maintenance exclusions. Synthetic monitor coverage is 100%.	Service availability SLA	99.99 % Meets target 2026-09-01 - 2026-09-30 · Demo Synthetic monthly measurement report · 7b8577d4-3d8b-4995-8936-46eaf7a2a171 6 metric entries in metric history	≥ 99.9 %	workspace-owner	A.8.14	    
Demo Backup restore validation result Qualitative pass/fail status from scheduled restore testing. DEMO-METRIC-restore_validation	Restore tests are performed and reviewed by the platform team.	Restore test result	Pass 2026-08-01 - 2026-08-31 · Demo Backup restore validation result sample metric 3 metric entries in metric history	—	workspace-owner	A.5.30 A.8.13 A.8.14	    
Demo Incident tabletop actions closed Percentage of tabletop exercise actions closed by agreed date. DEMO-METRIC-tabletop_actions	Tabletop actions are tracked after each exercise.	Exercise actions closed (%)	75 % Outside target 2026-08-01 - 2026-08-31 · Demo Incident tabletop actions closed sample metric 3 metric entries in metric history	≥ 100 %	workspace-owner	A.5.24 A.5.27 A.5.30	    
Demo Critical patch remediation within SLA Percentage of critical patches remediated inside the approved SLA. DEMO-METRIC-patch_sla	Patch reports are reviewed monthly and exceptions are tracked.	Critical patches remediated within SLA (%)	88 % Outside target 2026-08-01 - 2026-08-31 · Demo Critical patch remediation within SLA sample metric 3 metric entries in metric history	≥ 90 %	workspace-owner	A.8.8 A.8.19 A.8.32	    
Demo Access reviews completed on time Percentage of scheduled access reviews completed by the due date. DEMO-METRIC-access_reviews	Review completion is tracked monthly by the ISMS owner.	Access reviews completed on time (%)	90 % Outside target 2026-08-01 - 2026-08-31 · Demo Access reviews completed on time sample metric 3 metric entries in metric history	≥ 95 %	workspace-owner	A.5.16 A.5.18 A.8.2	    

Effectiveness Measures: green badges show targets met; red badges highlight results needing attention.

Measurements with evidence

Define effectiveness measures and thresholds. Record values manually or POST SLA metrics to inbound webhooks. Copy Python or curl examples to connect your reporting tools.

Bring results into the audit

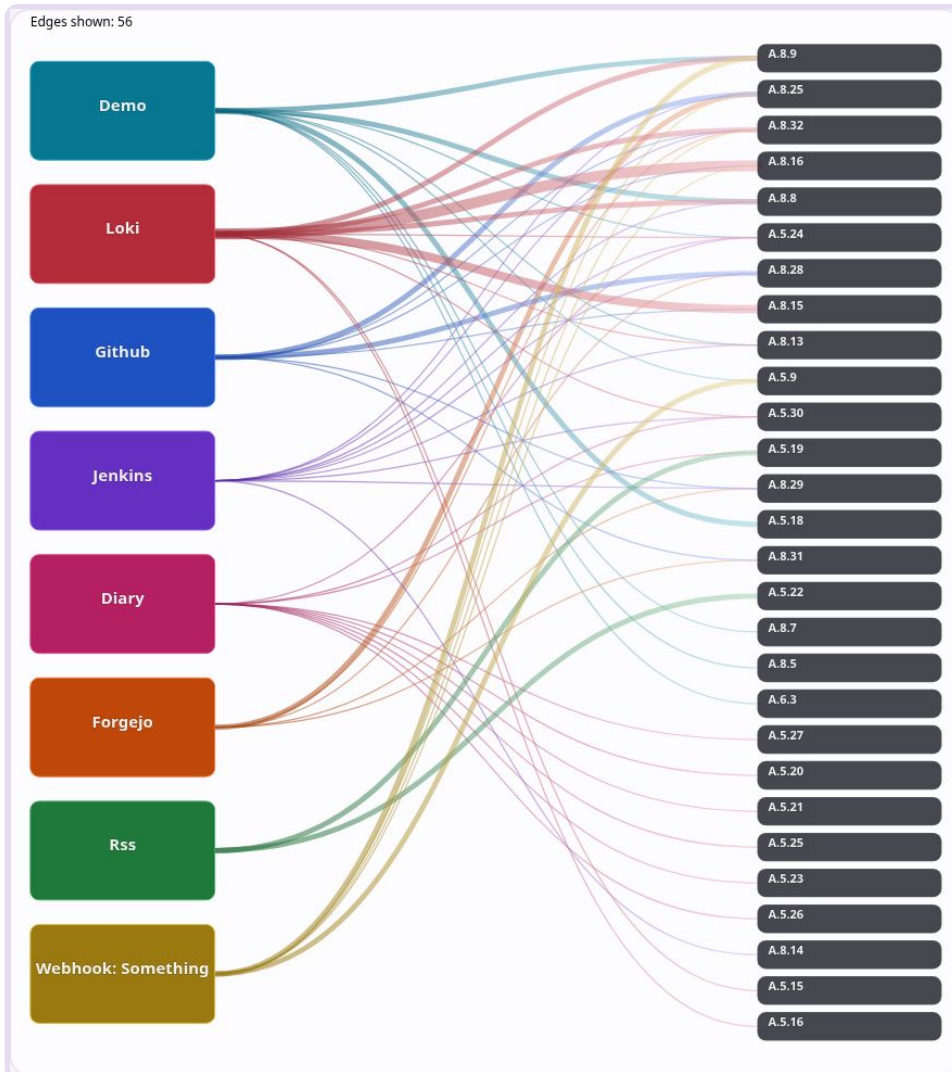
Review metric history and its supporting records. Sample measurements into active audits to demonstrate performance and the regular measurement of it.

Make follow-up visible. Use measured results to guide review, ask questions and prioritise improvement.

07 / EXPLORE

Follow the connections.

Explore how sources contribute evidence to controls, then drill into the records behind each relationship.



Each connection represents mapped events between an evidence source and a framework control.

Source ↔ control

The D3 relationship graph makes shared evidence visible. Follow a source to its detail page, or choose a control to explore its evidence.

Zoom into the detail

Explore charts, histograms, heatmaps and framework relationships. Move between controls, sources and events as you investigate coverage.

Find the gaps. Plan the next review.

Surface unmapped events, controls without evidence and gaps in recent audit-scope coverage. Download evidence as PDF, sample it into an active audit with your rationale, or export an audit ZIP with its report and sampled-event attachments.

Keep the conversation with the evidence.

Ask, annotate and investigate

Add review notes and rationale, ask questions about individual events and retain responses alongside the evidence. Declare incidents from relevant events and follow up with the people involved.

Control access to KEEN

Role-based access control and groups govern permissions. Local accounts support TOTP and WebAuthn security keys with one-time recovery codes. Use single sign-on with your identity provider.

Demo Jenkins restore smoke test build 22 succeeded
jenkins • 2026-10-06 06:30:00

Create mapping from this eventSample into auditSample as PDF evidence

Evidence snapshot
This view is designed to be printed or captured as a screenshot for auditors.

Open in sourceMore from this source

Source: jenkins
Timestamp: 2026-10-06 06:30:00
System: continuity
Actor: jenkins
Action: resilience-test
Outcome: success
Severity: 3

Mapped controls

A.5.30

ICT readiness for business continuity

A.8.13

Information backup

A.8.14

Redundancy of information processing facilities

Rationale

- Seeded jenkins demonstration event mapped to A.5.30
- Seeded jenkins demonstration event mapped to A.8.13
- Seeded jenkins demonstration event mapped to A.8.14

Artifacts

none

Questions

Auditor questions and responses associated with this evidence.

Ask a question about this event

none

A captured event links its source, mapped controls, rationale and auditor questions.

SEE YOUR EVIDENCE CONNECT.

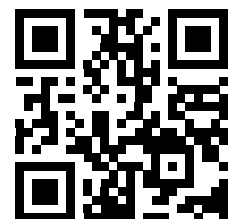
Free and open source software. Run on-premises or in the cloud.

Try KEEN free for 30 days.

keen.cloud

mig5: KEEN author and consultant

Explore a populated workspace. Use fictional data in the demo.



SCAN TO TRY KEEN