

LOGGING, SIEM INTEGRATION & EVIDENCE

Logging & Traceability Review

Trace important access and actions from end to end.

An event occurs - can you establish who did what and when? For an agreed service, I review which events are recorded, how they are brought together and who analyses them.

CONSULTING EFFORT

After scoping

PLANNING WINDOW

Schedule agreed individually

Preparation and follow-up are included in planning. Effort and scheduling depend on the systems in scope, available documentation, authorised access and stakeholder availability.

Your deliverables

- A log source and event matrix for the agreed service and events reviewed.
- Traceably documented gaps in data coverage, correlation and responsibilities.
- Prioritised requirements and actions for logging, SIEM integration and analysis.

Who is it for?

For IT, information security, platform operations and SIEM owners, and teams with technical traceability requirements.

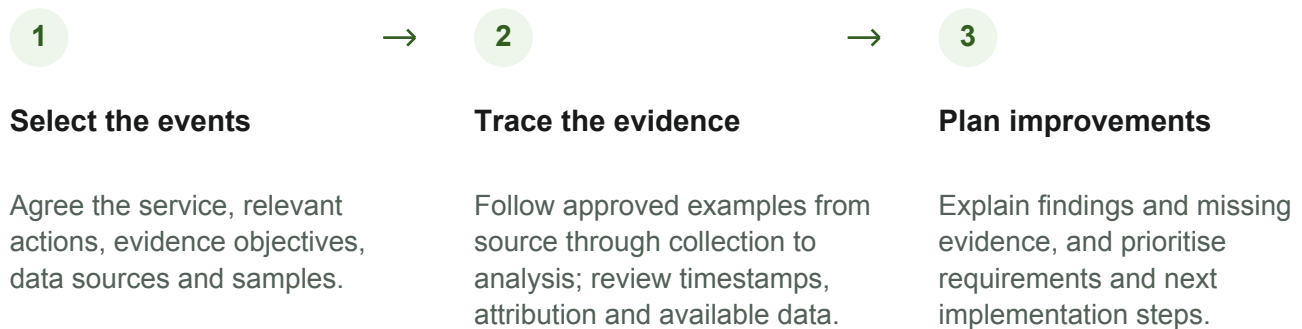
Price on request

You will receive a binding proposal after we agree the scope. Services, deliverables, fees and dates are agreed before the engagement begins.

SCOPE AND COLLABORATION

A clearly agreed scope

One service and an agreed selection of relevant events. Log sources, samples and business evidence requirements are defined in advance. Existing traceability is assessed using approved documentation and examples; complete coverage of all events is not promised.



What you provide

Service and logging architecture, a list of log sources, existing analysis use cases and named owners. Provide approved log examples in anonymised or pseudonymised form where possible; exclude sensitive content and credentials.

Location and arrangements

On site in Germany, Austria, Switzerland and the Netherlands. Remote work and travel and accommodation costs are agreed in the individual proposal.

A separate engagement

A separate engagement, not included in existing workshop or check fixed prices. Additional systems, samples or implementation services are agreed separately.

What is not included

No SOC or 24/7 operation, guaranteed attack detection or forensic investigation. No production changes or automatic legal assessment of retention periods. Technical implementation and further effectiveness testing are agreed separately.

Discuss scope and timing

Cedric Bergermann-Bißlich
Enterprise Architect | Security & Regulation

info@bergermann-consulting.de
+49 176 22636371