

PROTOKOLLIERUNG, SIEM-ANBINDUNG & NACHWEISE

Logging- und Nachvollziehbarkeitscheck

Wichtige Zugriffe und Aktionen durchgängig nachvollziehen.

Ein Ereignis tritt auf - lässt sich nachvollziehen, wer was wann getan hat? Ich prüfe für einen vereinbarten Service, welche Ereignisse erfasst werden, wie sie zusammengeführt werden und wer sie auswertet.

BERATUNGSAUFWAND

Nach Umfangsklärung

ZEITLICHER RAHMEN

Termine individuell vereinbart

Vor- und Nachbereitung werden berücksichtigt. Aufwand und Ablauf hängen von den betrachteten Systemen, vorhandenen Unterlagen, freigegebenen Zugängen und verfügbaren Ansprechpartnern ab.

Ihre Ergebnisse

- Logquellen- und Ereignismatrix für den vereinbarten Service und die betrachteten Ereignisse.
- Nachvollziehbar dokumentierte Lücken in Datenabdeckung, Korrelation und Zuständigkeiten.
- Priorisierte Anforderungen und Maßnahmen für Logging, SIEM-Anbindung und Auswertung.

Für wen?

Für Verantwortliche aus IT, Informationssicherheit, Plattformbetrieb und SIEM sowie Teams mit Anforderungen an technische Nachvollziehbarkeit.

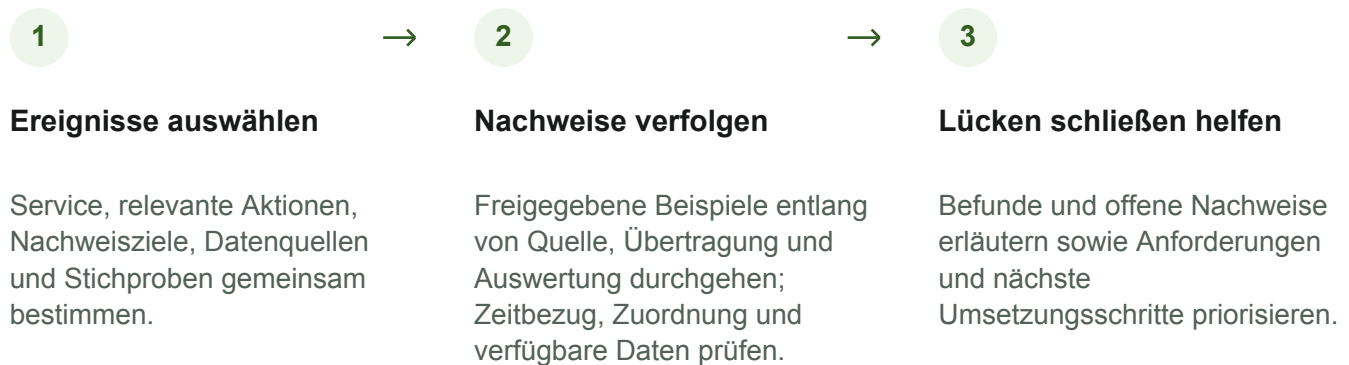
Preis auf Anfrage

Ein verbindliches Angebot erhalten Sie nach gemeinsamer Umfangsklärung. Leistungsumfang, Ergebnisse, Honorar und Termine werden vor der Beauftragung vereinbart.

LEISTUNGSUMFANG UND ZUSAMMENARBEIT

Ein klar vereinbarter Rahmen

Ein Service und eine vereinbarte Auswahl relevanter Ereignisse. Logquellen, Stichproben und fachliche Nachweisanforderungen werden vorab festgelegt. Bewertet wird die vorhandene Nachvollziehbarkeit anhand freigegebener Unterlagen und Beispiele; eine vollständige Erfassung aller Ereignisse wird nicht zugesagt.



Das bringen Sie mit

Service- und Logging-Architektur, Übersicht der Logquellen, vorhandene Auswertungsfälle und benannte Verantwortliche. Freigegebene Protokollbeispiele möglichst anonymisiert oder pseudonymisiert bereitstellen; sensible Inhalte und Zugangsdaten ausschließen.

Ort und Organisation

Vor Ort in Deutschland, Österreich, der Schweiz und den Niederlanden. Remote-Anteile sowie Reise- und Übernachtungskosten werden im individuellen Angebot geregelt.

Eigenständige Leistung

Eigenständige Leistung, nicht in bestehenden Workshop- oder Check-Festpreisen enthalten. Weitere Systeme, Stichproben oder Umsetzungsleistungen werden separat vereinbart.

Was nicht enthalten ist

Kein SOC- oder 24/7-Betrieb, keine garantierte Angriffserkennung und keine forensische Untersuchung. Keine produktiven Änderungen oder automatische rechtliche Bewertung von Aufbewahrungsfristen. Technische Umsetzung und weitergehende Wirksamkeitstests werden separat vereinbart.

Umfang und Termin besprechen

Cedric Bergermann-Bißlich
Enterprise Architect | Security & Regulation

info@bergermann-consulting.de
+49 176 22636371