CHECKLISTE

Wer war auf meinem Server? Anmeldungen und Änderungen mit Alloy, Prometheus und Grafana überwachen

Aus dem Beitrag vom 6. November 2026 · klein-it.solutions/blog/linux-server-anmeldungen-und-aenderungen-ueberwachen

- [ ] auditd läuft und überwacht SSH-Konfiguration, authorized_keys, Benutzer, sudoers, systemd-Units und seine eigene Konfiguration.
- [ ] Jede erfolgreiche SSH-Anmeldung löst einen Alarm aus, mit Benutzer, Quell-IP und Fingerprint des Schlüssels.
- [ ] Schreibzugriffe auf überwachte Dateien lösen einen Alarm aus, auch beim allerersten Mal.
- [ ] Logs landen außerhalb des Servers, damit ein Angreifer sie nicht einfach löschen kann.
- [ ] Es gibt einen Alarm, wenn der Server keine Daten mehr liefert, denn ein gestoppter Wächter ist selbst ein Warnsignal.
- [ ] Die Mitarbeiter wissen, dass Befehle auf den Servern protokolliert werden.

Wenn du an einem der Punkte hängen bleibst: ein Anruf oder eine kurze E-Mail genügt. Die Kontaktdaten stehen unten.

Klein IT Solutions
An der Zickelburg 9
53604 Bad Honnef

+49 170 8843097

info@klein-it.solutions

Inhaber
Henning Klein