A09:2021 - Security Logging and Monitoring

- **Deskripsi**

Security Logging and Monitoring Failures terjadi ketika sistem tidak mampu mencatat (logging) dan memantau (monitoring) aktivitas keamanan dengan efektif

Dampak

- Kegagalan login dan transaksi dengan nilai yang tinggi tidak di catat.
- Peringatan dan Error tidak menghasilkan pencatatan yang memadai atau catatan pesan yang tidak jelas.
- Log dari aplikasi dan API tidak di monitor untuk aktifitas mencurigakan.
- Log hanya disimpan secara lokal.
- Threshold peringatan yang sesuai dan proses dari respon eskalasi tidak efektif
- Sistem tidak dapat melacak, menganalisis, dan merespons ancaman keamanan dengan cepat dan akurat.

Mitigasi

- Memastikan semua kesalahan login, kontrol akses dan validasi input dari server-side dapat di catat dan disimpan dengan waktu yang cukup untuk analisis forensik.
- Memastikan semua catatan dihasilkan dalam format dimana solusi pengelola catatan dapat dengan mudah digunakan.
- Memastikan data catatan telah di encode dengan benar untuk mencegah injeksi atau serangan pada pencatatan atau sistem monitor.
- Memastikan transaksi dengan nilai yang tinggi memiliki jejak audit dengan kontrol integritas untuk mencegah gangguan dan penghapusan, seperti hanya dapat ditambahkan ke database atau yang mirip seperti itu.
- Melakukan monitoring secara efektif dan memberikan peringatan terhadap aktifitas mencurigakan yang terdeteksi dan merespon secara cepat.
- Membuat atau adopsi sebuah respon insiden dan rencana pemulihan

Revision #2
Created 4 September 2024 04:22:07 by Tim Persandian
Updated 4 September 2024 04:31:07 by Tim Persandian