eivok

INCIDENSKEZELÉS

EGY RENDSZERINTEGRÁTORNÁL

Bódis Péter

ISACA
Budapest Chapter

Fogalmak
Szabályozói környezet
Követelmények
Feltételek
Folyamat
Eredmények
Tervek

INCIDENSKEZELÉS

Az **INCIDENS** olyan nem kívánt / nem várt egyedi / sorozatos információbiztonsági **ESEMÉNY**/ek együttese, amely/ek nagy valószínűséggel veszélyeztetik az **üzleti tevékenység**et és fenyegetik az elektronikus információs rendszereken (EIR) tárolt, továbbított vagy kezelt adatok, vagy az e rendszerek által **nyújtott szolgáltatás**ok bizalmasságát, sértetlenségét vagy rendelkezésre állását.

Fogalmak

Szabályozói környezet

Követelmények

Feltételek

Folyamat

Eredmények

Tervek

INCIDENSKEZELÉS

+ JELENTŐS INCIDENS, amelynél a hatásküszöbök (érintett felhasználók száma, földrajzi kiterjedés, szolgáltatáskiesés mértéke stb.) meghaladják az előírt értékeket,

IKT-INCIDENS (információs és kommunikációs technológiai) incidens,

+ JELENTŐS IKT-INCIDENS

69/2024. (LXIX.) Kiberbiztonsági tv., ISO27001, NIS-2 irányelv (EU 2022/2555), DORA EU 2022/2554) rendelet…

Fogalmak
Szabályozói környezet
Követelmények
Feltételek
Folyamat
Eredmények
Tervek

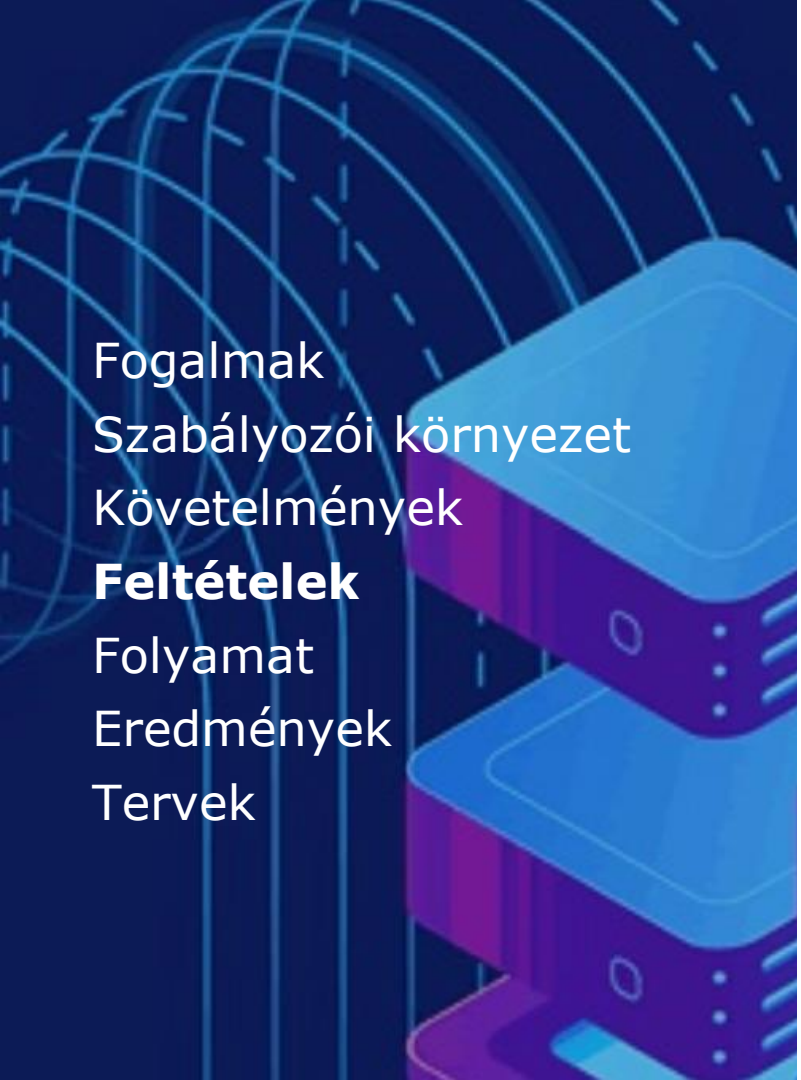
INCIDENSKEZELÉS

ISO 27001, 27017, 27018: **22+ kontroll**
NIS-2: **10+ kontroll**
DORA: **5+ kontroll**
+ ENISA ajánlások

Fogalmak
Szabályozói környezet
Követelmények
Feltételek
Folyamat
Eredmények
Tervek

INCIDENSKEZELÉS

Felelősségi körök / **szerepkörök**
Incidensek **azonosítása** és bejelentése
Incidensek osztályozása és **priorizálása**
Reakció- és **válaszidő**
Kommunikáció az érintettekkel
Incidens – **életút dokumentálás**
Tudásbázis
Tesztelés és **gyakorlat**



Fogalmak
Szabályozói környezet
Követelmények
Feltételek
Folyamat
Eredmények
Tervek

INCIDENSKEZELÉS

Strukturált folyamat
Szabályzat
Kommunikációs csatornák
Tudatosság - Képzés
Ticketing rendszer
SOCaaS
Incidenskezelő csapat
Gyakorlat
Riport

Fogalmak
Szabályozói környezet
Követelmények
Feltételek
Folyamat
Eredmények
Tervek

INCIDENSKEZELÉS

Felkészülés

Tervezés, Csapat, Folyamat, Eszközök, Képzés

Észlelés és elemzés

Monitorozás, Riasztás-fogadás, Azonosítás, Jelentés

Elhárítás

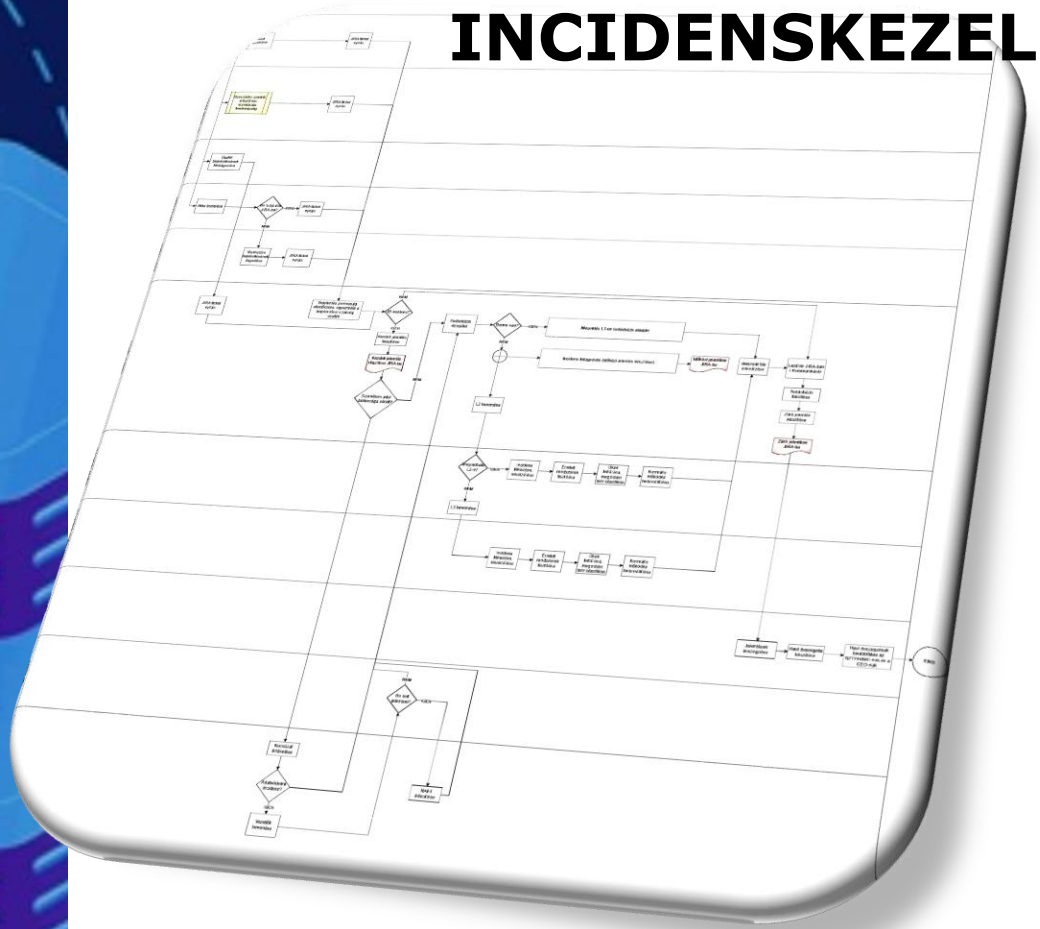
Incidens megfékezés, OK feltárása, Helyreállítás

Utó-tevékenységek

Elemzés, Jelentés, Fejlesztési, Tudásbázis

INCIDENSKEZELÉS

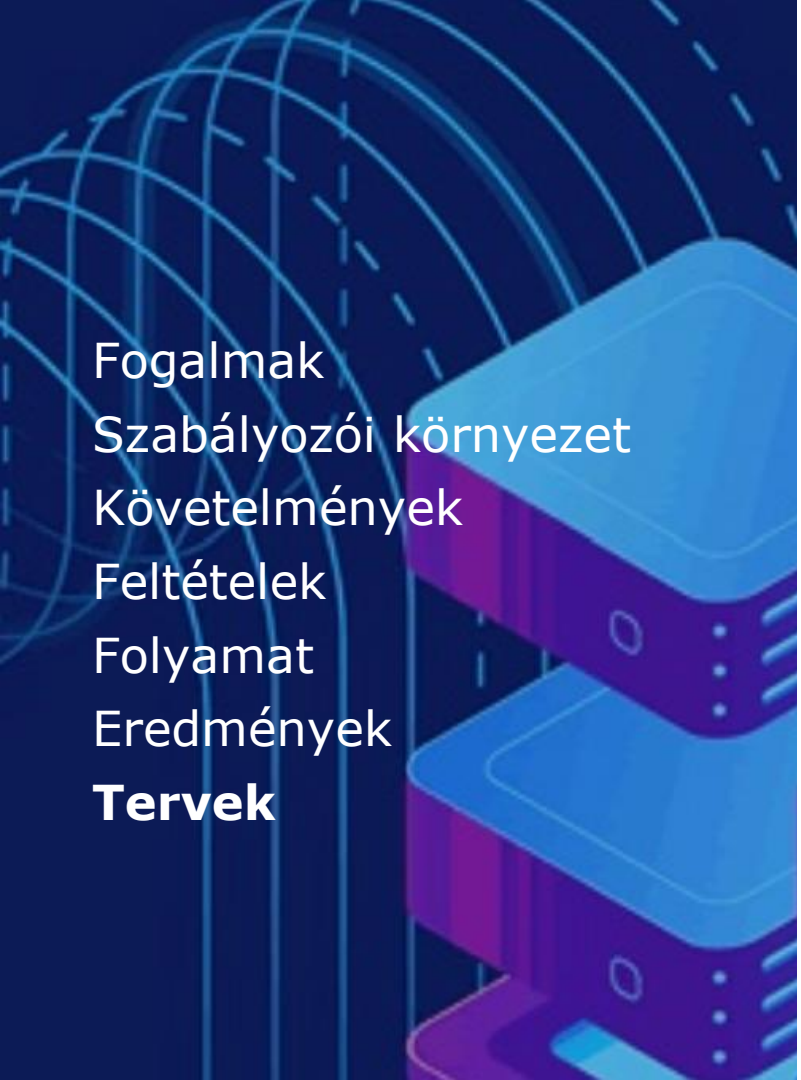
Fogalmak
Szabályozói környezet
Követelmények
Feltételek
Folyamat
Eredmények
Tervek



Fogalmak
Szabályozói környezet
Követelmények
Feltételek
Folyamat
Eredmények
Tervek

INCIDENSKEZELÉS

Tudatos felhasználók
AI alapú képzés
AI alapú bejelentés-támogatás
Monitorozás – Kritikus rendszerek
SIEM jelzések
SOC - automatizmusok
Ticketing rendszer
Incidenskezelő csapat
Jelentések – Ügyfél / Partner / Hatóság
Tudásbázis – Tapasztalat és Megosztás



Fogalmak
Szabályozói környezet
Követelmények
Feltételek
Folyamat
Eredmények
Tervek

INCIDENSKEZELÉS

Vezetői helyzetgyakorlatok
Válságkommunikáció
AI alapú támadás-tesztek
AI alapú bejelentés automatizáltan