SZIRÉNEK HÁLÓJÁBAN

AVAGY A SZERVEZETÜNKET ÉRINTŐ INFORMÁCIÓBIZTONSÁGI KOCKÁZATOK TELJESKÖRŰ FELTÉRKÉPEZÉSÉNEK FONTOSSÁGA

- OROSZI ESZTER DIÁNA
- CISA, CISM, CRISC, ISO 27001 LA
- INFORMÁCIÓBIZTONSÁGI TANÁCSADÁS ÜZLETÁGVEZETŐ

SIREN

silent signal

BEMUTATKOZÁS

OROSZI ESZTER DIÁNA, CISA, CISM, CRISC, ISO 27001 L

- 14 év szakmai tapasztalat – tanácsadói és ügyfél oldalon egyaránt
- Silent Signal Kft., információbiztonsági tanácsadás üzletágvezető
- Nemzeti Közszolgálati Egyetem, PhD hallgató
- Kutatási terület: Social Engineering, biztonságtudatosság mérése és fejlesztése, gamifikációs lehetőségek
- Biztonságtudatossági szabadulószoba
- Biztonságtudatossági társasjáték fejlesztés
- SIREN kockázat- és üzletfolytonosság menedzsment támogató rendszer fejlesztés

MIRŐL LESZ SZÓ?

KOCKÁZATELEMZÉST MINDENKI KÉSZÍT...

DE MIRE ÉS HOGYAN?

Social Engineering

Adatok

IT biztonság

Üzletfolytonosság

Sérülékenységek

Szolgáltatások

Humán biztonság

Külső megfelelés

Fizikai biztonság

Fejlesztések

Erőforrások

Folyamatok

HAGYOMÁNYOS

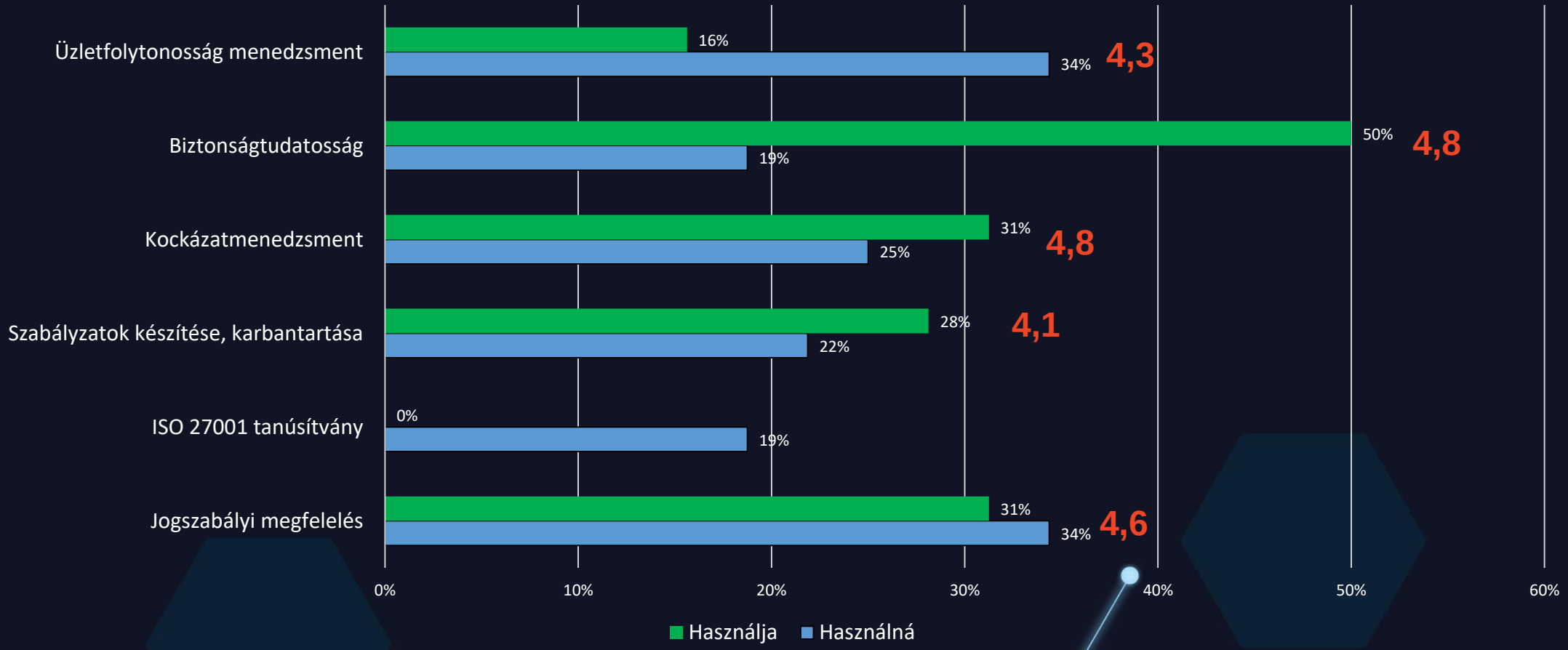
MÓDSZEREK

Szervezeti egység	Folyamat neve	Folyamatgazda	Folyamat rövid leírása	Kritikus dátum/időszak	Kritikus időszak
HR osztály (HRO)	Toborzás és kiválasztás	Horváth Renáta	Álláshirdetések kezelése, jelentkezőkkel való kapcsolattartás, interjú szervezés.	Nem került azonosításra.	-
HR osztály (HRO)	Új munkavállaló beléptetése	Horváth Renáta	Új munkavállaló belépésével kapcsolatos feladatok, belépési dokumentumok kezelése, igénylések.	Nem került azonosításra.	
HR osztály (HRO)	Munkavállaló kiléptetése	Horváth Renáta	Munkavállaló kilépésével kapcsolatos feladatok, kilépési dokumentumok kezelése.	Rendkívüli felmondás	
HR osztály (HRO)	Bérszámfejtés	Horváth Renáta	Bérszámfejtési tevékenység ellátása, munkabérek, pótlékok számfejtése, túlórák elszámolása.	Mind	
IT osztály (ITO)	IT eszköz nyilvántartás	Irinyi Tamás	Beszerzett IT eszközök nyilvántartásba vétele, eszköz kiadás és visszavétel dokumentálása, selejtezési jegyzőkönyvezése.		
IT osztály (ITO)	Jogosultságkezelés	Irinyi Tamás	Igényelt jogosultságok beállítása, visszavonása, jogosultság-felülvizsgálat támogatása.		
IT osztály (ITO)	Webshop üzemeltetés	Irinyi Tamás	Webshop infrastruktúra és alkalmazás üzemeltetése, karbantartási feladatok ellátása.		
Gazdasági igazgatóság (GIG)	Pénzügyi tranzakciók	Gazdag Ilona	Utalások és kifizetések (munkabér, költségtérítések, stb.) végrehajtása.		
Gazdasági igazgatóság (GIG)	Beszerzési tevékenység	Gazdag Ilona	Alapanyagok és szolgáltatások újraiati felhívásra		
Gazdasági igazgatóság (GIG)	Szerződéskötési folyamatok	Gazdag Ilona	Szerződések jogi és gazdasági		
Gazdasági igazgatóság (GIG)	Számviteli feladatok	Gazdag Ilona	Könyvelési		
Szállítás és logisztika (SZLO)	Szállítás	Szabó			
Szállítás és logisztika (SZLO)	Megrendelt termékek csomagolása				
Szállítás és logisztika (SZLO)	Hulladékszállítási tevékenység				
Szállítás és logisztika (SZLO)	Visszáru kezelés				
Biztonsági osztály (BO)	Ügyfélszolgálat, panaszkezelés				
Biztonsági osztály (BO)	Incidensmenedzsment				
Biztonsági osztály (BO)					

Erőforrás	Kockázatleírása	Gyakoriság	Hatás	Kockázati é	Javasolt védelmi intézkedés	Becsült ráfordítás (Ft vagy ember-nap)	Maradványkockázat gyakoriság	Maradványkockázat hatás	Maradványkockázat	Döntés
	KOCKÁZAT SZÁMÍTÁS				VÉDELMI INTÉZKEDÉS		MARADVÁNYKOCKÁZAT SZÁMÍTÁS			
IBUCSoft	A rendszer belső hálózaton kívülről kétfaktoros authentikáció alkalmazása nélkül elérhető, jogosulatlan hozzáférés esetén munkavállalói személyes adatokhoz való hozzáférés lehetséges.	Gyakori	Kritikus	16	MFA bevezetése.	2.000.000 Ft	Ritka	Kritikus	8	Kockázatcsökkentő intézkedés
IBUCSoft	A rendszer belső hálózaton kívülről kétfaktoros authentikáció alkalmazása nélkül elérhető, jogosulatlan hozzáférés esetén munkavállalói személyes adatokhoz való hozzáférés lehetséges.	Gyakori	Kritikus	16	A rendszer hálózaton belülről történő elérésének biztosítása.	4.000.000 Ft	Nagyon ritka	Kritikus	4	Alternatív intézkedés kerül
IBUCSoft	A IBUCSoft-ot fejlesztő és üzemeltető céggel nincsen információbiztonsági követelményrendszer érvényesítve, az adminisztrátori jogosultságok nem kontrolláltak.	Ritka	Kritikus	8	Információbiztonsági követelmények érvényesítése a szerződésben.	2 embernap	Nagyon ritka	Magas	3	Kockázatcsökkentő intézk
Alap informatikai eszközök	A végpontvédelmi szoftver licencei lejártak, a frissítések nem kerülnek telepítésre, így fennáll a kártékony kód rendszerbe jutásának kockázata.	Gyakori	Magas	12	Licenc frissítése vagy új végpontvédelmi szoftver beszerzése	1.200.000 Ft	Ritka	Közepes	4	Kockázatcsökkentő intézk
Alap informatikai eszközök	A munkavállalók nem zárják el a laptopokat, azok az irodában felügyelet nélkül hagyva eltulajdoníthatók.	Ritka	Magas	6	Kensington zár beszerzés.	500.000 Ft	Nagyon ritka	Magas	3	Kockázat felvállalása
Alap informatikai eszközök	A munkavállalók nem zárják el a laptopokat, azok az irodában felügyelet nélkül hagyva eltulajdoníthatók.	Ritka	Magas	6	Biztonságtudatossági oktatás.	250.000 Ft	Nagyon ritka	Magas	3	Kockázat felvállalása
Alap informatikai eszközök	A munkavállalók lokálisan tárolnak érzékeny munkaanyagokat, és a laptopokon teljes merevlemez titkosítás nincsen, elvesztés esetén jogosulatlan hozzáférés lehetséges szenzitív adatokhoz.	Ritka	Kritikus	8	Teljes merevlemez titkosítás bevezetése.	1.800.000 Ft	Nagyon ritka	Közepes	2	Alternatív intézkedés
Alap informatikai eszközök	A munkavállalók lokálisan tárolnak érzékeny munkaanyagokat, és a laptopokon teljes merevlemez titkosítás nincsen, elvesztés esetén jogosulatlan hozzáférés lehetséges szenzitív adatokhoz.	Ritka	Kritikus	8	Biztonságtudatossági oktatás.	250.000 Ft	Ritka	Magas	6	Kockázatcsökkentő in
Fájlszerver T meghajtó	A fájlszerver T meghajtón tárolt adatokról biztonsági mentés nem készül,	Ritka	Kritikus	8	Biztonsági mentés készítésének bevezetése, biztosítás.	5.800.000 Ft	Nagyon ritka	Kritikus	4	

TÁMOGATÓ
MEGOLDÁSOK

SZOFTVERES TÁMOGATÁS



Forrás: Saját felmérés, 2021

TENGERNYI KOCKÁZAT...

DE VAJON HOL JELENNEK MEG?

Kockázataink „tengere”

MI KÖZE A SZIRÉNEKNEK

AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZATOKHOZ?

SZIRÉNEK

Mitológiai lények, akik csodás hangú, de gyilkos természetű tengeri nimfák, akik a Sirenum scopuli elnevezésű kis szigetcsoporton laktak. Bűvös hangú, asszonyfejű, de madárszárnyakkal és karmokkal rendelkező szörnyek. Varázslatos hangjukkal és bölcs mindentudással elcsábítják a tengerészeket, majd megölik őket.

Forrás: Wikipedia

HÁLÓZZUK BE MI IS

AZ INFORMÁCIÓBIZTONSÁGI KOCKÁZATOKAT!

(ÉS KEZELJÜK ŐKET...)

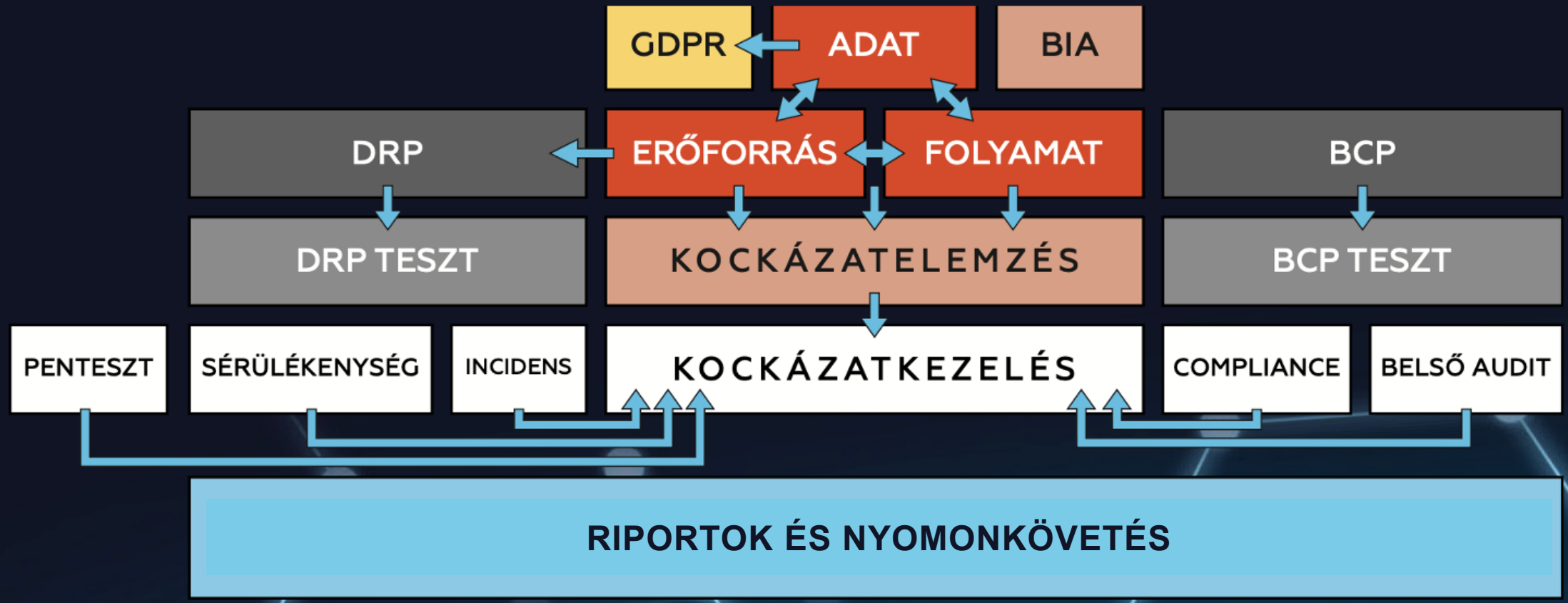
SECURITY
INVENTORY AND
RISK
EVALUATION
NETWORK

MIRE VÁGYUNK

A KOCKÁZATMENEDZSMENTBEN?


HATÉKONYSÁG-
NÖVELÉS
EGYSZERŰ
HASZNÁLAT
KOMPLEX
MEGOLDÁS
ÁTLÁTHATÓ
RIPORTOK
SZERVEZETRE
SZABÁS
EGYSÉGES
KEZELÉS

MÓDSZERTANUNK



EZZEL A SZEMLÉLETTEL

VALÓS KOCKÁZATOKAT LÁTUNK

TÁMOGATJUK AZ INTÉZKEDÉSEKET

SEGÍTJÜK A DÖNTÉSHOZATALT

MEGFELELŐEN DOKUMENTÁLJUK AZ EREDMÉNYEKET

BIZTOSÍTJUK A RENDSZERES FELÜLVIZSGÁLATOT

ÖSSZEFOGLALÁS

- VIASZ A FÜLÜNKBE? NEM MEGOLDÁS!
- A SZIGETSZERŰ MEGKÖZELÍTÉST A KOCKÁZATOK TERÉN IS ÉRDEMES FELSZÁMOLNI...
- ... ÉS A SZERVEZETNEK MEGFELELŐ KOCKÁZATMENEDZSMENT FOLYAMATOKAT KIALAKÍTANI

KÖSZÖNÖM A FIGYELM

KÉRDÉSEK?