

“ÍGY ÍRTOK TI”

SÉRÜLÉKENYSÉG VIZSGÁLATI
AJÁNLATKÉRÉSEK TAPASZTALATAI

PÁNCZÉL ZOLTÁN,

CISSP, OSCP, OSCE, OSWP, GPEN, GWAPT

SENIOR IT BIZTONSÁGI MANAGER, PARTNER

Tartalomjegyzék

- Ügyfél visszajelzések
- Mi így látjuk!
- Valós példák :)
- Szerintünk mi a “jó” kiírás
 - Általános elvek
 - Pontozás, súlyozás
 - Megfelelő kiírás alapjai
 - Összegzés

Ügyfél visszajelzések

- Több száz, ezer oldalas automatizált eszközöktől származó riport
- Nem megfelelő a kiírás, nem lehet számon kérni az eredmény terméket
- Nincs teljesskörűség
- 8-10(!) meghívott cég, amelynek 80-90%(!) már az első rostán kiesik.
- Minden rendben vs. több kritikus hiba

Mi így látjuk!

Az ügyfél sokszor nem tudja meghatározni,
mit is szeretne igazából (mindent :))



Mi így látjuk!

Nem a megfelelő ember viszi a projektet.



Mi így látjuk!

Egy kiírásra több különböző ajánlat érkezik.

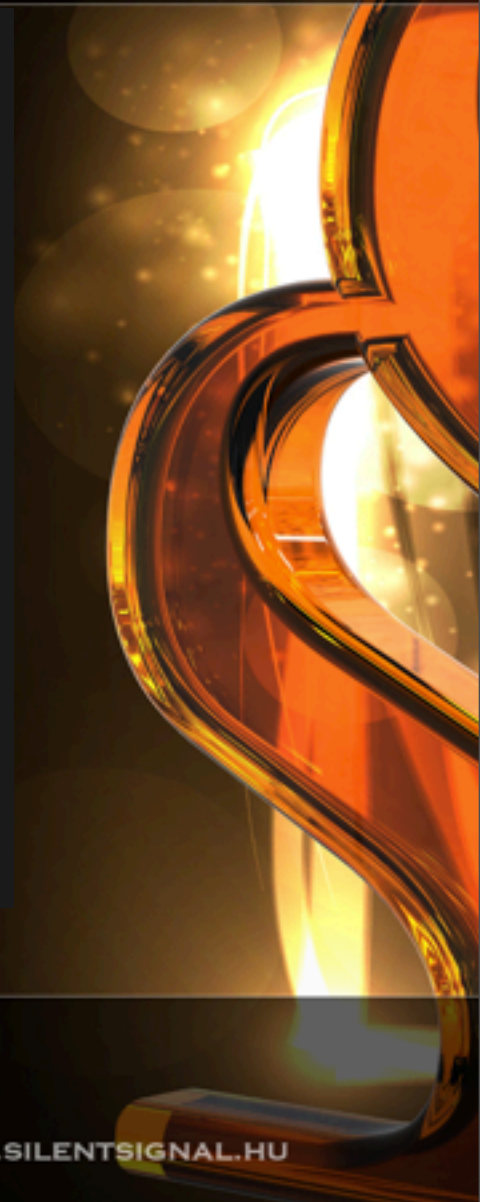


Mi így látjuk!

Dobozos termékként kezelik a megrendeléseket.



Mi így látjuk!



Valós ajánlati kiírás I.

Ajánlati kérés sérülékenység vizsgálatra és behatolás tesztelésre

Tisztelt Cím!

Ezúton kérünk ajánlatot a [REDACTED] rendszereinek biztonsági vizsgálatára.

A vizsgálat tartalma:

1. Blackbox vizsgálat

Internet felőli külső sérülékenységek vizsgálata

Vezeték nélküli hálózatok sérülékenység vizsgálata

2. Graybox vizsgálat

Belső sérülékenységek vizsgálata normál jogosultsággal

Webes alkalmazások sérülékenység vizsgálata

Kliens oldali biztonsági teszt

3. Social Engineering

4. Kockázatok elemzése, javaslatok a megszüntetésre

A vizsgálat terjedelme:

A vizsgálatokat egy telephelyre kérjük. Az alkalmazottak száma [REDACTED]

Szerverek száma: kb [REDACTED]

Munkaadások száma: kb [REDACTED]

Hordozható számítógépek száma: kb [REDACTED]

1. Internet felőli vizsgálatok

Blackbox

Greybox

Hostok/IP címek számát a megbeszélésen tisztázzuk

VPN kapcsolatok vizsgálata

2. Webes alkalmazás sérülékenység vizsgálat

Kb [REDACTED] db alkalmazás

A kritikus alkalmazások 24/7-ben futnak

Egyedi alkalmazás vizsgálatot (kód audit) nem kérünk

3. Belső hálózat felőli sérülékenységek vizsgálata

Blackbox

Greybox

Hostok/IP címek száma kb [REDACTED]

4. Vezeték nélküli hálózatok vizsgálata

Access point-ok száma [REDACTED], egy telephelyen

Valós ajánlati kiírás II.

Tisztelt Címzett!

Sérülékenységi vizsgálattal kapcsolatban szeretnénk árajánlatot kérni Önöktől, a honlapjukon olvastam, hogy foglalkoznak a témával.

80 munkaállomásra (windows) és 10 szerverre (3linux, amúgy windows) szeretnénk kérni.

Ajánlatukat kérem még a héten küldje meg számunkra.

Előre is köszönöm!

Tisztelettel,

Az alábbiakban részletezett munkára kérem szíves ajánlatukat.

Projekt célja a Sérülékenység Vizsgálat elvégzése a [REDACTED] cégcsoporton.

Projekt időbeosztás

- Október [REDACTED] - Kiírás
- Október [REDACTED] - Ajánlat leadása
- November [REDACTED] - Kiválasztás eredményének kihirdetése

Kitételek

- Ajánlat legyen moduláris felépítésű. Modulok:
 1. Külső hálózat felőli sérülékenység vizsgálat és WIFI vizsgálat
 2. Belső hálózaton sérülékenység vizsgálat
 3. Social engineering
 4. Szolgáltatásmegtagadással járó sérülékenységek vizsgálata

Valós ajánlati kiírás III.

- 5 különböző vizsgálati terület
- Óradíjas elszámolás (órakeret :))
- 70% ár, 15% műszaki tartalom, 15% referenciák (kvázi bemondásra)
- Határidő <> Elszámolás

Valós ajánlati kiírás IV.

- Decemberben ébredünk!
- Teszt csak munkaidő után, hétvégén ;)
- Segítsünk a kiírásban, majd pályázhatunk a munkára a többi meghívottal :D
- Szakmai keverések (black, grey, white)
- Inf.bizt. szakértők a túloldalon

Valós ajánlati kiírás V.

- Külföldi versenyző ;)
- Részletes leírása a teszelendő rendszereknek (rendszerterv, nem kezdemény!)
- 15 oldal a feladat műszaki leírása
- Szakmaiság, majd utána az ár!
- Megfelelő határidők
- Villámgyors szerződéskötés

Szerintünk mi a megfelelő?

- Kiírásban a legtöbb konkrétum szerepeljen a vizsgált rendszerekkel, komponensekkel kapcsolatban
- Ajánlattevő nem az ajánlatkérő alkalmazottja, a rövidítések, rendszer funkciók kifejtése
- Kérdésekre vagy konzultációra lehetőség biztosítása
- Normális, betartható határidő

Szerintünk mi a megfelelő?

- Személyes konzultáció
- Értékelés max. 10% súlyozással



SUIT UP

because it's going to be legendary

Szerintünk mi a megfelelő?

- Referenciák
- Értékelés kb. 10% súlyozással



Szerintünk mi a megfelelő?

- Szakmai csapat
- Értékelés kb. 20% súlyozással



Szerintünk mi a megfelelő?

- Minősítések
- Értékelés kb. 10% súlyozással



Szerintünk mi a megfelelő?

- Műszaki ajánlat
- Értékelés kb. 30% súlyozással

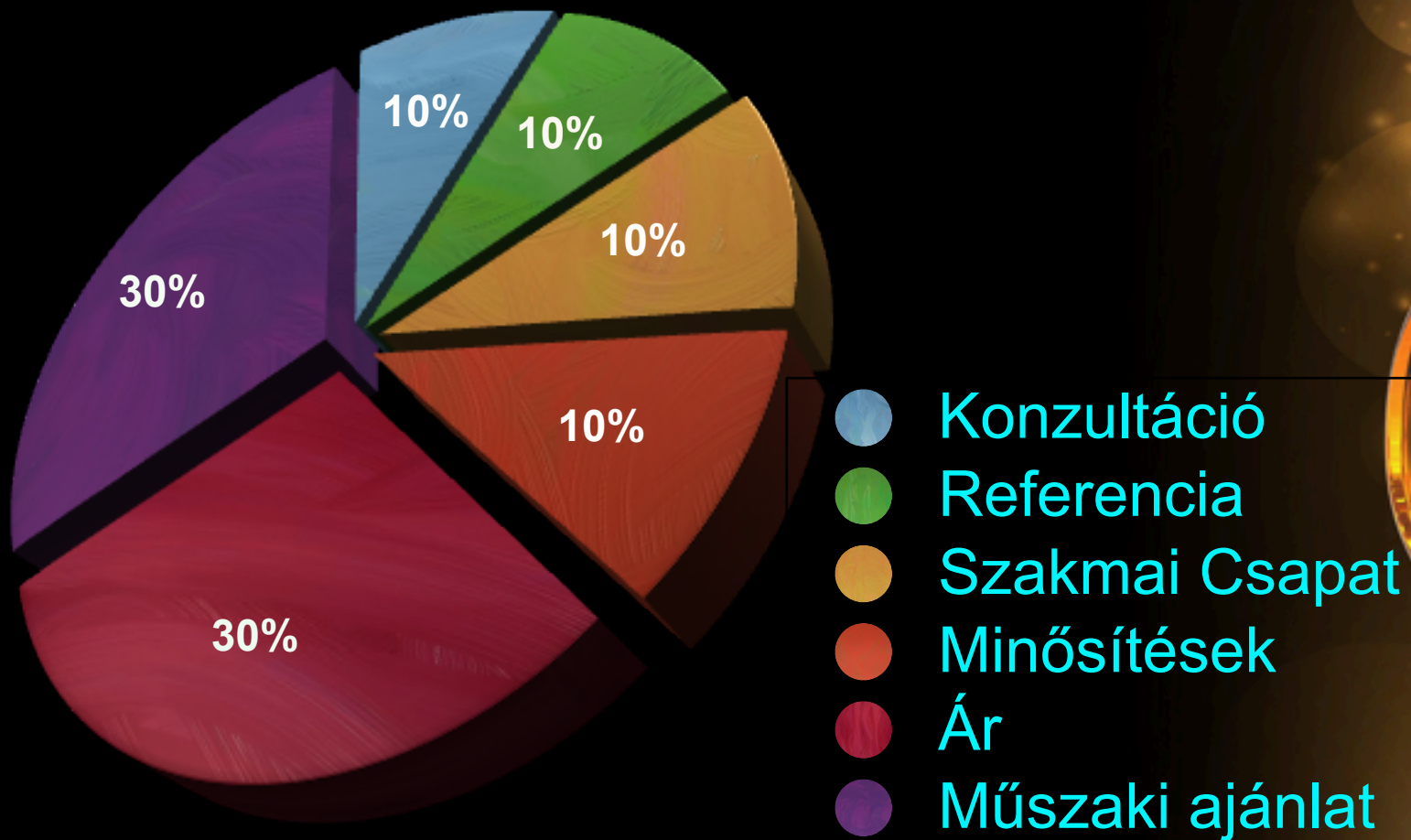


Szerintünk mi a megfelelő?

- Ár
- Értékelés kb. 30% súlyozással



Összegzés



KÖSZÖNÖM A FIGYELMET!

PÁNCZÉL ZOLTÁN

CISSP, OSCP, OSCE, OSWP, GPEN, GWAPT

Facebook

PANCZEL.ZOLTAN@SILENTSIGNAL.HU

web

e-mail