Így írtok ti ITBN Edition

Sérülékenységi vizsgálatok tapasztalatai

Varga-Perke Bálint - OSCP, GWAPT

ITBN Az Év Útmutató Szakembere 2012

Megrendelői visszajelzések

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

Mi a probléma?

Az ügyfél sokszor nem tudja meghatározni mit is szeretne igazából

- "Mindent"
- Sokszor megfelelő leltár nélkül…

Mi a probléma?

Az ügyfél sokszor nem tudja meghatározni mit is szeretne igazából

- Semmit
- "Csak a bejelentkező képernyő"

Mi a probléma?

Sokszor nem a megfelelő ember viszi a projektet

Mi a probléma?

A rossz kiírásokra lényegesen különböző ajánlatok érkeznek

Mi a probléma?

Dobozos termékként kezelik a megrendeléseket

Valós ajánlati kiírás I.

Ajánlat 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]

Munkaállomások 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 felöli 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)

Valós ajánlati kiírás IV.

- Decemberben ébredünk!
- Teszt csak munkaidő után, hétvégén ;)
- Segítsünk a kiírásban majd pályázhatunk a munkára a többi meghívottal…
- Szakmai keverések

Jó kiírás?

Valós ajánlati kiírás VI.

- Külföldi versenyző ;)
- Részletes leírása a tesztelendő rendszereknek
  - Kész rendszerterv, nem kezdemény!
- Szakmaiság majd utána az ár
- Megfelelő határidők
- Villámgyors szerződés kötés

Mi lehetne a megfelelő?

Reális scoping

- Létező szolgáltatás leltár ill. rendszerterv alapján
  - Létező célpontokra…
- Vizsgálat céljának meghatározása
  - Pl. Konkurencia, rosszindulatú felhasználók, PCI Council stb.
- Priorizálás

Mi lehetne a megfelelő?

Kiírás

- A lehető legtöbb konkrétum szerepeljen a vizsgált rendszerekkel, komponensekkel kapcsolatban
- Az ajánlattevő nem az ajánlatkérő alkalmazottja: a rövidítések, rendszer funkciók kifejtése
- Kérdésekre vagy konzultációra lehetőség biztosítása
- Normális, betartható határidő

Mi lehetne a megfelelő?

Személyes konzultáció

- Az érintett területek egy szakértője legyen jelen
- Pontozás előre felállított szabályrendszer szerint
  - Bemutatkozás
  - Projekt ismertetés
  - Szakmai kérdések
- Értékelés max. 10% súlyozással

Mi lehetne a megfelelő?

Szakmai csapat

- Szakmai önéletrajzok, minősítések
- Alvállalkozó bevonásának egyértelmű feltüntetése
- Saját és "bérelt" erőforrás feltüntetése
  - Partneri alvállalkozói viszony, összerántott projekt csapat
    - Bizalmasság?
- Értékelés max. 20% súlyozással

Mi lehetne a megfelelő?

Referenciák

- Publikus referenciák kérése
  - Kontakt személy
- 4-5 kontakt ellenőrzése, szondázás
- A “szakma” véleménye
- Értékelés max. 10% súlyozással

Mi lehetne a megfelelő?

Minősítések

- Súlyozott pontozás a relevancia szerint
  - Papíros vs. gyakorlati vizsgák
  - SANS-GIAC, Offensive Security, gyártói minősítések, stb.
- Értékelés max. 10% súlyozással

Mi lehetne a megfelelő?

Műszaki ajánlat

- A vizsgálatok részletes leírása
- Használt eszközök listája
- Dokumentáció tartalmának ismertetése
- Értékelés max. 30% súlyozással

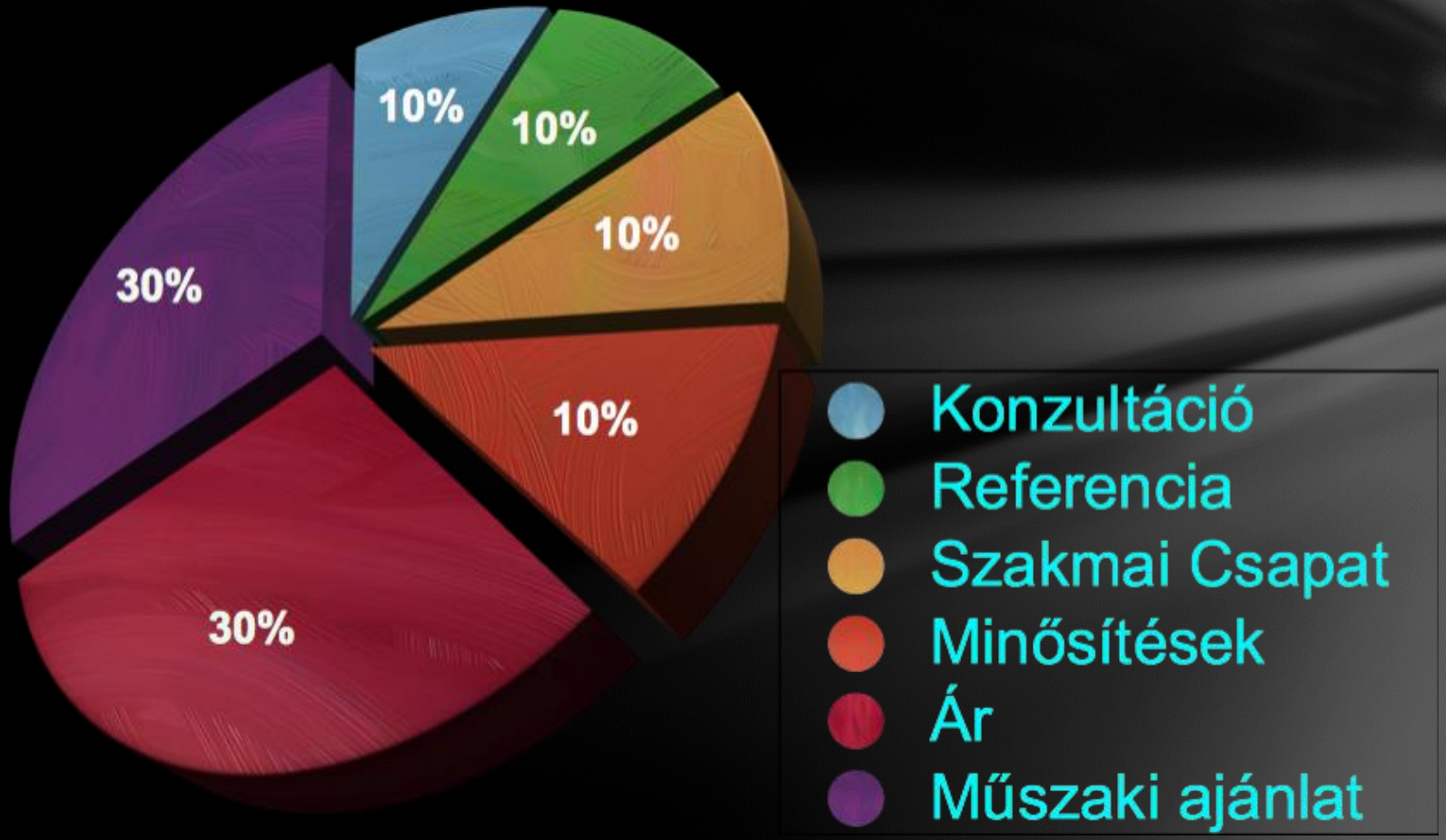
Kompetencia és
számon kérhetőség!

Mi lehetne a megfelelő?

Ár

- Szakértői tevékenység
- Professzionális tudás
  - Néhány cégnél világviszonylatban is mérvadó szakértők!
- Az üzemeltetési, adatgazdai szinten is legyen igényesség!
- Vezetői elkötelezettség

Összegzés


10%
10%
10%
10%
30%
30%
Konzultáció
Referencia
Szakmai Csapat
Minősítések
Ár
Műszaki ajánlat

Köszönöm a figyelmet!

buherator@gmail.com
http://buhera.blog.hu