SECURITY CONSULTANT

BEZPEČNOSTNÍ KONZULTANT / ETICKÝ HACKER / PENETRATION TESTER

Petr

Jak to vidím

- řeším otázky zabezpečení dat firem před jejich krádeží a zneužitím
- mám na starost ochranu systémů před kybernetickými útoky, naplnění legislativních požadavků...

Nejvíce mě z práce baví

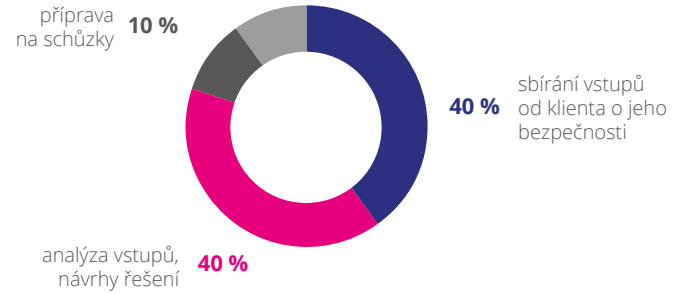
1. práce v oblasti, která má pro klienta důležitost a dopad napříč organizací
2. pestrost projektů, kde se mohu stále učit a získávat nové kontakty
3. práce v rychle se rozvíjejícím oboru

Moc mě z pracovních činností nebaví

1. vytváření status reportů pro management
2. meetingy bez jasného cíle
3. administrativa, papírování

POPIS POZICE

Rozdělení mého pracovního času



návrhy bezpečnostního řešení
schůzky s klientem
cestování
projektové řízení
analýza zadání
koordinace týmů

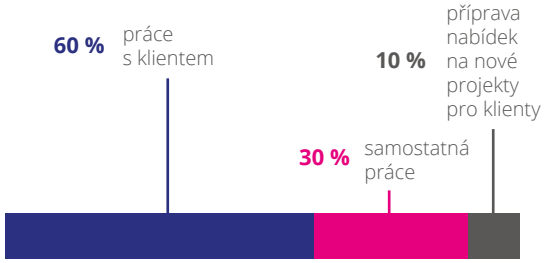
Můj typický pracovní den

- denně sbírám vstupy od klienta (např. k bezpečnosti přístupů do účtů zaměstnanců, k zabezpečení aplikací firmy, k práci s citlivými údaji)
- průběžně s klientem diskutuji jeho potřeby a návrhy řešení a posuzujeme společně stav jeho IT bezpečnosti
- analyzujeme oblast, kterou chce klient zlepšit (např. identity management, kybernetickou bezpečnost, bezpečnost zavádění nové aplikace)
- pak pracuji sám či v týmu (např. na analýze požadavků a rizik, na návrhu či implementaci řešení, na návrhu bezpečnostní architektury, na konkrétním bezpečnostním opatření)

Můj typický pracovní týden

- v týdenním cyklu je navíc zpravidla týdenní reporting dosažených dílčích výsledků pro management
- většinu týdne trávím přímo u klienta a časové i týmové uspořádání práce ovlivňuje velikost projektu a složení projektového týmu
- vedle denní agendy zahrnuje moje práce také zpracovávání nabídek pro potenciální klienty, návrhy řešení, odhady pracnosti, projektové řízení, sebevzdělávání, sdílení znalostí v rámci týmu

Samostatnost vs. týmovost práce



Nejčastěji komunikuji s

- s projektovým manažerem klienta
- s bezpečnostními specialisty klienta
- s 3. stranami = dodavatelé bezpečnostního řešení klienta
- s projektovým manažerem našeho týmu

JAK ZÍSKAT POZICI

Ideální člověk na tuto pozici je

1. komunikativní, asertivní, schopný získat důvěru
2. schopný se rychle a sám učit, pochopit problém
3. schopný se adaptovat a být odolný vůči stresu

+

Hard skills

1. principy řízení rizik
2. IT bezpečnost: autentizace, řízení přístupů, kryptografie, typické zranitelnosti, hrozby a útoky, standardy a legislativa,...
3. obecný IT přehled: architektura, infrastruktura, OS, síťové technologie a protokoly, web technologie, programování, ...

+

Soft skills

1. proklientská orientace – pochopení potřeb klienta
2. řešení problémů (s cílem: balanc mezi funkčností a potřebami klienta)
3. efektivní komunikace (schopnost se dobře ptát a umět přesvědčit)

Mezioborová inspirace

Z jakého oboru
- » IT: programování, správa systémů, sítí, ...
- » právo aplikované v ICT (compliance)
- » kybernetická kriminalita
- » forensics science

Jaká dovednost/znalost
- » aplikace právních norem do technického fungování firem
- » dovednost sběru stop z hacknutého systému za účelem dopadení pachatele a použití důkazů u soudu

Práci mi pomohlo získat

Během přípravy na pohovor
- » samostudium tématiky informační bezpečnosti

Během pohovoru
- » pomohlo, že bylo vidět, že mám zájem o obor a motivaci v něm pracovat a vzdělávat se

Doporučení těm, kdo mají o tuto pozici zájem

- » zlepšuj si stále hard skills a sledujte vývoj v informační bezpečnosti
- » piluj průběžně i soft skills: komunikační, prezentační dovednosti

Studuj, uč se
- » online IT kurzy pro širší rozhled

Zkoušej v praxi
- » absolvuj online challenges (hackme, crackme)
- » vytvoř si vlastní prostředí (web server a databázi) např. v AWS Free Tier a zkus si ho zabezpečit
- » dělej IT security pro bono, např. pro neziskovky
- » najdi si práci v příbuzném IT oboru či začni na vstupní pozici v oblasti bezpečnosti (např. jako SOC analytik = security operation center analytik, pen(etration) tester, admin přístupových práv)

Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

czechitas accenture

Kariérní web je realizován díky projektu: „Ženy do IT“ (reg.č. CZ.03.1.51/0.0/0.0/16_061/0003268), který je financován z prostředků Evropského sociálního fondu prostřednictvím Operačního programu Zaměstnanost.

itpozice.czechitas.cz

SECURITY CONSULTANT

ROZDÍL ÚROVNĚ

Junior

- » i junior musí mít poměrně dobrý přehled o většině informační bezpečnosti
- » složitější schůzky a úkoly dělá se seniorem a sám vede ty jednodušší
- » konsoliduje informace, rozpracovává návrhy řešení pod vedením seniorů
- » nejde o vstupní pozici – i na juniorní pozici je nutný dobrý základ IT
- » očekává se, že se sám iniciativně dále vzdělává

Senior

- » má výborný přehled o všech oblastech informační bezpečnosti
- » je často expertem na některou z dílčích oblastí
- » vidí „big picture“ projektu, umí ho naplánovat a řídit dodání
- » komunikuje s vedoucími pracovníky klienta a pracuje s jejich očekáváními
- » definuje klientovi strategii IT bezpečnosti, navrhuje komplexní řešení
- » rozumí potřebám klienta, umí je řešit a rozvíjet obchodní vztah

Průměrný posun z juniora na seniora
- » 5 let

BUDOUCNOST

Vývoj pozice za 3–5 let

- » poptávka po naší práci poroste mj. také kvůli rozšiřování IoT, cloud služeb, robotizaci, důrazu na ochranu osobních dat atd.
- » více budeme zapojováni do vývoje produktů od počátku a i další role (např. vývojáři) budou muset mít alespoň základní povědomí o IT bezpečnosti

Doporučené vzdělávání pro budoucnost
- » tech oblast: např. cloudové technologie, IoT (= Internet of Things), blockchain
- » legislativa a standardy, např. Zákon o kybernetické bezpečnosti, GDPR
- » vedení projektů a týmů