Rapport titel: VGR Konsultförfrågningar Details
Run Date and Time: 2025-03-04 16:45:54 Central European Time
Run by: Maria Perlerot
Tabellnamn: u_vgr_consultant_function

VGR Konsultförfrågningar

Avropsnummer:	CONS0005970	Avropsnamn:	5970 Penetrationstestare för
Ramavtal:	RS 202306258 - IT-konsulttjänster 2021	ADDA	Millennium

Anteckningar:

Sista dag för frågor och svar: 2025-03-19
Sista dag för anbud: 2025-03-24
Anbudets giltighetstid: 2025-04-07

Uppdraget är inte bemannat idag

Vi förbehåller oss rätten att intervjua de tre bäst lämpade kandidaterna.

Option på förlängning:

VGR har ensidig rätt att förlänga hela eller delar av avtalet vid ett eller flera tillfällen i ytterligare sammanlagt 24 månader, varefter det upphör utan föregående uppsägning.

När möjligheten till förlängning av avtalet utnyttjas ska VGR lämna meddelande senast en månad innan gällande avrop löper ut. Förlängning sker till oförändrade avtalsvillkor

Uppdragsbeskrivning

Kompetensnivå:	Level 5	Startdatum:	2025-04-07
Roll:	Teknisk specialist	Slutdatum:	2026-01-31
Placeringsort:	Mölndal	Option på förlängning längst tom:	2028-01-31
		Omfattning av tid:	100%

Uppdragsbeskrivning Konsult

Uppdrag:

Syftet med detta uppdrag är att genomföra en omfattande penetrationstestning av de interna infrastrukturtjänster som tillhandahålls inom Västra Götalandsregionen.
Målet är att identifiera och utvärdera potentiella säkerhetssårbarheter som kan utnyttjas av illasinnade aktörer, bedöma den övergripande säkerhetsnivån för tjänsterna samt ge handlingsbara rekommendationer för att minska identifierade risker. Säkerhetsklassning kan förekomma.

Bakgrund:

Då det är av yttersta vikt att säkerställa att tjänster uppfyller högsta möjliga säkerhetsstandarder så behöver vi penetrationstesta delar av VGR:s miljö.

Kompetensprofil konsult:

Teknisk Kompetens
- Djupa kunskaper i nätverk och säkerhetsprotokoll: Förståelse för TCP/IP, DNS, VPN, brandväggar, IDS/IPS-system och andra nätverksrelaterade teknologier.
- Erfarenhet av operativsystem: God kunskap om Windows, Linux och andra operativsystem. Förmåga att arbeta med kommandoradsgränssnitt och skriptning (t.ex. Bash, PowerShell).
- Programmerings- och skriptkunskaper: Erfarenhet med språk som Python, Ruby, Perl, eller liknande för att skriva anpassade verktyg och automatisera uppgifter.
- Förståelse för webbapplikationer: Erfarenhet av webbteknologier (HTML, JavaScript, SQL) och sårbarheter som är vanliga i webbapplikationer, som SQL-injektion, cross-site scripting (XSS), och cross-site request forgery (CSRF).
- Kännedom om penetrationstestningsverktyg: Erfarenhet med verktyg som Nmap, Metasploit, Burp Suite, Wireshark, Nessus, OWASP ZAP, och andra verktyg som används för att identifiera och utnyttja sårbarheter.

Analytisk och Problemlösande Förmåga
- Analytisk förmåga: Förmåga att analysera komplexa system och identifiera potentiella svagheter. Detta inkluderar både tekniska detaljer och hur olika komponenter samverkar.
- Kreativt tänkande: Förmåga att tänka som en angripare och hitta okonventionella vägar för att penetrera systemet. Detta kräver ett kreativt sinne och en stark förståelse för hur system kan missbrukas.
- Noggrannhet: Förmåga att genomföra noggranna analyser och dokumentera resultat på ett tydligt och strukturerat sätt.

Erfarenhet och Utbildning
- Formell utbildning: En kandidatexamen i datavetenskap, informationsteknologi eller ett relaterat område kan vara fördelaktigt, även om det inte alltid är ett krav. Relevant erfarenhet kan ofta väga tyngre än formell utbildning.
- Certifieringar: Certifieringar som CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), CISSP (Certified Information Systems Security Professional), eller GPEN (GIAC Penetration Tester) är ofta högt värderade och visar på en djup förståelse för området.
- Praktisk erfarenhet:Tidigare erfarenhet av att genomföra penetrationstestningar eller arbete inom IT-säkerhet är mycket värdefullt. Erfarenhet av att ha arbetat med olika typer av miljöer, såsom molnbaserade system eller industriella kontrollsystem (ICS), kan också vara fördelaktigt beroende på organisationens behov.

Kommunikationsförmåga
- Rapportskrivning: Förmåga att skriva tydliga, koncisa och handlingsbara rapporter som beskriver sårbarheter, potentiell påverkan, och rekommenderade åtgärder.
- Muntlig kommunikation: Förmåga att presentera tekniska resultat och koncept för olika intressenter, inklusive de som inte har en teknisk bakgrund. Detta är särskilt viktigt när man diskuterar säkerhetsrisker och rekommendationer med ledningen eller kunder.

Etiska Riktlinjer och Integritet
- Etisk medvetenhet: En penetrationstestare måste följa strikta etiska riktlinjer och alltid arbeta i enlighet med de lagar och regler som gäller. De måste också ha ett starkt fokus på konfidentialitet, särskilt när de hanterar känslig information.
- Integritet: Hög personlig integritet och trovärdighet är avgörande, eftersom penetrationstestare ofta har tillgång till kritiska system och känsliga data.

Kontinuerlig Inlärning och Anpassningsförmåga**
- Håll dig uppdaterad:** Säkerhetslandskapet förändras ständigt, och en bra penetrationstestare måste vara proaktiv i att lära sig om nya sårbarheter, verktyg och tekniker.
- Anpassningsförmåga:** Förmåga att snabbt anpassa sig till nya teknologier, miljöer och hotbilder.

Obligatoriska krav (ska):

Erfarenhet
- Minst 3-5 års erfarenhet av penetrationstestning: Kandidaten ska ha dokumenterad erfarenhet av att genomföra penetrationstester, inklusive både externa och interna tester, webbapplikationstester och nätverkssäkerhet.
- att arbeta i olika miljöer: Erfarenhet av att testa säkerheten i både on-premises och molnbaserade infrastrukturer (t.ex. AWS, Azure) samt olika typer av applikationer och nätverk.

Teknisk Kompetens
- Kunskap i penetrationstestningsverktyg: Kandidaten måste ha omfattande erfarenhet av verktyg som Nmap, Metasploit, Burp Suite, Wireshark, Nessus, och andra relevanta verktyg som används i penetrationstestning.
- Programmerings- och skriptspråk: Erfarenhet av att skriva och använda skript i språk som Python, Bash, PowerShell, och eventuellt även lågnivåspråk som C för att utveckla anpassade verktyg eller exploateringskoder.
- Förståelse för nätverksprotokoll och säkerhetsprotokoll: Djup kunskap om TCP/IP, DNS, VPN, krypteringsprotokoll och andra relevanta teknologier och protokoll.

Certifieringar
- Certifieringar som CEH, OSCP eller motsvarande: Minst en erkänd certifiering inom penetrationstestning eller informationssäkerhet, som CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), eller liknande.

Rapportering och Dokumentation
- Förmåga att skriva detaljerade och tydliga rapporter: Kandidaten måste kunna dokumentera sina fynd och resultat på ett sätt som är lättförståeligt för både tekniska och icke-tekniska intressenter. Detta inkluderar både tekniska detaljer och sammanfattningar för ledningen.
- Erfarenhet av att ge rekommendationer: Kandidaten bör kunna ge praktiska och genomförbara rekommendationer för att åtgärda identifierade sårbarheter.

Etisk och Professionell Hållning
- Starkt etiskt förhållningssätt: Kandidaten måste arbeta inom lagens och organisationens ramar och upprätthålla högsta möjliga integritet. Konfidentialitet är kritiskt i denna roll.
- Referenser eller verifierad bakgrund: Det är viktigt att kandidaten kan tillhandahålla referenser eller verifiering av tidigare arbeten och projekt.

Kommunikationsförmåga
- Förmåga att kommunicera komplexa säkerhetskoncept: Kandidaten måste kunna förklara tekniska säkerhetskoncept för icke-tekniska teammedlemmar och beslutsfattare, både skriftligt och muntligt.
- Erfarenhet av att hålla presentationer: Förmåga att presentera sina fynd och rekommendationer för olika typer av publik, inklusive ledningsgrupper och tekniska team.

Arbetsmetodik och Verktyg
- Följande av erkända standarder: Erfarenhet av att arbeta enligt erkända säkerhetsramverk och standarder som OWASP Top Ten, NIST, eller ISO 27001.
- Användning av versionskontrollsystem: Erfarenhet av att använda verktyg som Git för att hantera kod och dokumentation är ett plus.

Anpassningsförmåga och Problemlösning
- Förmåga att arbeta i dynamiska miljöer: Kandidaten bör vara bekväm med att snabbt anpassa sig till nya teknologier och snabbt hitta lösningar på uppkomna problem.
- Bevis på tidigare framgångar i liknande roller: Exempel på tidigare uppdrag där kandidaten framgångsrikt har identifierat och åtgärdat kritiska säkerhetssårbarheter.

Tillgänglighet och Flexibilitet
- Möjlighet att arbeta på plats vid behov: Kandidaten bör kunna arbeta på plats i den fysiska miljön om det krävs av uppdraget, samt vara flexibel med arbetstider för att möta projektets behov.

Språkkunskaper
- Flytande svenska i tal och skrift.

Utvärderingskrav (bör):

Meriterande

Språkkunskaper:
Goda kunskaper i engelska i både tal och skrift.