APAVIL S.A.

ISO 9001
ISO 14001
OHSAS 18001
BUREAU VERITAS Certification

Nr.Reg.Com. J 38/522/2004
C.U.I.: RO 16468149
Site: www.apavil.ro

Str. CAROL I, nr. 3-5, Rm. Vâlcea, jud. Vâlcea Fax: 0250/738903
Nr. 13711/14.07.2022 Tel: 0250/739580;0350/805461

ANUNȚ

privind scoaterea la concurs a unui post de inginer in cadrul Compartimentului IT

Pentru a participa la concurs, candidații trebuie să îndeplinească cumulativ următoarele condiții:

Condiții generale:

a) Să dețină cetățenia română, cetățenie a altor state membre ale Uniunii Europene sau a statelor aparținând Spațiului Economic European și domiciliul în România;
b) Să cunoască limba română, scris și vorbit;
c) Să îndeplinească vârsta minimă reglementată de prevederile legale;
d) Să aibă capacitate deplină de exercițiu;
e) Să dețină o stare de sănătate corespunzătoare postului pentru care candidează, atestată pe baza adeverinței medicale eliberate de medicul de familie sau de unitățile sanitare abilitate;
f) Să îndeplinească condițiile de studii și, după caz, de vechime sau alte condiții specifice potrivit cerințelor postului scos la concurs;
g) Să nu fie condamnat/ă definitiv pentru săvârșirea unei infracțiuni contra umanității, contra statului ori contra autorității, de serviciu sau în legătură cu serviciul, care împiedică înfăptuirea justiției, de fals ori a unor fapte de corupție sau a unei infracțiuni săvârșite cu intenție, care ar face-o incompatibilă cu exercitarea funcției, cu excepția situației în care a intervenit reabilitarea.

Condiții specifice:

- absolvent(a) învățământ superior: Facultatea de Electronică, Telecomunicații și Tehnologia Informației, Facultatea de Automatică și Calculatoare, Facultatea de Inginerie Electrică (Electrotehnica), Facultatea Ingineria Industriala și Robotică, Facultatea de Matematică și Informatică, Facultatea de Matematică, Facultatea de Cibernetică, Statistică și Informatică Economică sau absolvent al unor universități cu profil tehnic;
- cunoștințe avansate despre sisteme de operare MS Windows 98, 2000, XP, 7, 8, 10; MS Windows Server 2003, 2008, 2012; Linux CentOS 5, 6, 7; Linux Ubuntu Server 18, 20; Linux workstation (Debian, Ubuntu);
- cunoștințe privind sisteme de securitate cibernetică (SIEM, IDS/IPS, firewall, anti-virus/anti-malware, anti-spam, etc.);
- cunoștințe privind sisteme de managementul utilizatorilor;
- cunoștințe privind procesul de investigare a incidentelor de securitate cibernetică;
- cunoștințe privind evaluarea vulnerabilităţilor şi a amenințărilor de securitate;
- cunoștințe avansate despre securizarea datelor informatice și a rețelelor de calculatoare;
- administrarea rețelelor de calculatoare LAN/ WAN;
- cunoașterea la nivel avansat a principiilor, arhitecturilor şi tehnologiilor utilizate în rețele de calculatoare (LAN, WAN) tehnologiile: VLAN, routing, SSH, NFS, firewall, IPS, IDS, blocare atacuri cibernetice, VPN, SNMP, SMTP, IMAP, LDAP, pppoe, DNS, DHCP, FTP, web proxy (forward, reverse, load-balancing, fail-over);
- cunoașterea tehnologiilor pentru servicii tip server Web(Nginx, Apache), Email server(Postfix, Sendmail, Dovecot, iRedMail, Mailcow), virtualizare (KVM, Virtual Box), containerization platform(Docker, Kubernetes), Active Directory Domain Services, SAMBA;

- administrare baze de date MS SQL, PostgreSQL;
- cunoașterea unor limbaje scriptice: linux bash, command prompt;
- cunoștințe privind protocoalele de comunicații uzuale utilizate în rețele de tip SCADA;
- cunoștințe HTML, PHP;
- cunoștințe limbaje de programare: C/C++, Python.
- deținerea unor certificări tehnice valide în domeniul de specializare constituie un avantaj;
- abilitați de comunicare și lucru în echipă și în condiții de stres;

Principalele sarcini si responsabilitati:

- realizarea analizei riscurilor de securitate a rețelelor și sistemelor informatice;
- realizarea metodologiei de gestionare a riscurilor furnizării serviciilor esențiale;
- întreținerea registrului de risc organizațional;
- stabilește politica de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale;
- menține sistemul de management al securității informației;
- întocmește rapoarte privind implementarea politicii de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale și a documentelor de aplicare a acesteia;
- răspunde de acreditarea rețelele și sistemele informatice din cadrul Apavil SA;
- stabilește indicatorii de evaluarea și metodele de evaluarea a indicatorilor din punct de vedere al securității informatice;
- stabilește și actualizează periodic procedura privind evaluarea conformității NIS și efectuarea auditului de securitate a rețelelor și sistemelor informatice;
- contribuie la testarea și evaluarea rețelelor și sistemelor informatice efectuate pentru identificarea venerabilităților;
- întreprinde acțiuni în vederea conștientizării și instruirii utilizatorilor de resurse informatice, din cadrul Apavil SA, cu privire la tipurile de amenințări de securitate informatică și măsurile de protecție corespunzătoare;
- întreține un inventar actualizat al proceselor IT, sistemelor și elementelor componente ale rețelelor și sistemelor informatice din cadrul societății, precum și o procedura privind etichetarea și clasificarea datelor și informațiilor;
- întreține situația cartografică a ecosistemului și lista riscurilor potențiale identificate și evaluarea acestora în furnizarea serviciilor esențiale;
- menține o procedura de stabilire a relațiilor ecosistemului și o listă cu acorduri la nivel de serviciu și/sau mecanisme de audit a rețelelor și sistemelor informatice;
- menține o situație actualizata cu schemele arhitecturii rețelelor și sistemelor informatice din cadrul societății și analiza riscurilor de securitate a rețelelor și sistemelor informatice;
- menține registre de evidență a suporților de memorie externă și o procedură privind utilizarea suporților de memorie externă;
- se asigura ca în cadrul societății se respecta segregarea și segmentarea rețelelor și sistemelor informatice și menține o procedura în acest sens;
- se asigura ca în cadrul societății se aplica filtrarea traficului și menține o procedura în acest sens; face analize cu privire la riscurile de securitate a rețelelor și sistemelor informatice;
- menține o procedură pentru asigurarea protecției criptografice pentru informații și resurse și asigura managementul cheilor de criptare;
- menține o procedură pentru asigurarea protecției malware;
- menține lista conturilor de administrare într-o forma actualizata;
- se asigura ca este respectata politica de securitate a rețelelor și sistemelor informatice, ca exista jurnale de înregistrare și plicuri cu parole de administrare a rețelelor și sistemelor informatice, conform unei proceduri pe care o întreține;
- menține proceduri pentru lucrul la distanța și pentru asigurarea protecției criptografice pentru informații și resurse;
- se asigura ca exista o evidenta actualizata pentru utilizatori și pentru procesele automatizate și ca se folosește un mecanism de autentificare;
- se asigura ca exista o evidenta cu nivele de acces pentru utilizatori;
- întreține proceduri pentru menținerea securității rețelelor și sistemelor informatice, pentru reducerea riscurilor legate de utilizarea unei versiuni învechite, pentru asigurarea protecției criptografice pentru informații și resurse;

- urmărește riscurile de securitate și se asigura ca sunt implementate și respectate măsuri de securitate pentru sistemele de monitorizare și control industrial SCADA;
- menține o procedura privind accesul și securitatea resurselor și informațiilor și se asigura ca este respectata;
- menține o procedura pentru detectarea incidentelor de securitate care afectează rețelele și sistemele informatice; se asigura ca sistemul pentru înregistrarea evenimentelor la nivelul rețelelor și sistemelor informatice este funcțional;
- întreprinde acțiuni în vederea identificării, clasificării, remedierii și eliminării vulnerabilităților la nivelul rețelelor și sistemelor informatice;
- menține o procedura pentru gestionarea, răspunsul și analiza incidentelor care afectează funcționarea sau securitatea rețelelor și sistemelor informatice;
- menține o procedură pentru raportarea incidentelor de securitate;
- menține o procedură de interconectare la serviciul de alertare și cooperare al CERT-RO;
- menține o procedură pentru gestionarea informațiilor primite de la CERT-RO și a măsurilor de securitate adoptate pentru protejarea rețelelor și sistemelor informatice;
- menține o procedură privind managementul asigurării disponibilității serviciului esențial, în caz de incident de securitate cibernetică;
- menține o procedură privind managementul recuperării datelor în caz de dezastre, precum și în caz de incidente severe de securitate cibernetică;
- menține o procedură privind organizarea gestionării crizelor în caz de incidente de securitate cibernetică pentru asigurarea continuității activităților organizaționale;
- asigura comunicarea cu organe specializate în investigații, CERT-RO - DNSC, alte entități naționale/sectoriale în cazul confruntării cu incidente de securitate cibernetică;
- informează și consiliază conducerea societății cu privire la securitatea datelor informatice, conform cerințelor legii în vigoare;
- instruiește ceilalți administratori de resurse informatice din cadrul societății în vederea respectării masurilor de securitate a datelor;
- instalează, configurează și administrează sisteme informatice;

Dosarul de Concurs trebuie să conțină următoarele documente:

a) Cerere de înscriere în concurs adresată Directorului General;
b) Copia actului de identitate sau orice alt document care atestă identitatea, potrivit legii, după caz;
c) Copiile documentelor care atestă nivelul studiilor și ale altor acte care atestă efectuarea unor specializări, precum și copiile documentelor care atestă îndeplinirea condițiilor specifice ale postului;
d) Cazierul judiciar;
e) Adeverință medicală care să ateste starea de sănătate corespunzătoare eliberată cu cel mult 6 luni anterior derulării concursului de către medicul de familie al candidatului sau de unitățile sanitare abilitate. Adeverința trebuie să conțină, în clar, numărul, data, numele emitentului și calitatea acestuia, în formatul standard stabilit de Ministerul Sănătății;
f) Curriculum vitae, model european;

Tematica si Bibliografie

- Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice;
- Ordin nr. 1.323 din 9 noiembrie 2020 pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale;
- Hotărâre nr. 976 din 12 noiembrie 2020 privind aprobarea valorilor de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale;
- Hotărâre nr 963 din 5 noiembrie 2020 pentru aprobarea Listei serviciilor esențiale;
- ORDIN 599/2019 privind aprobarea Normelor metodologice de identificare a operatorilor de servicii esențiale și furnizorilor de servicii digitale;
- ORDIN 600/2019 privind aprobarea Normelor metodologice de organizare și funcționare a Registrului operatorilor de servicii esențiale;

- ORDIN 601/2019 pentru aprobarea Metodologiei de stabilire a efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale.
- administrare rețele de calculatoare LAN, VLAN, WAN, IPv4/v6, TCP/IP, subnets, switch, router, OSI layers - (Networking Essentials - Glenn Berg);
- administrare windows 10, windows server - (Windows 10 1909 GP OS Administrative Guide, Windows Server 2012 Study Guide, Windows Server 2016 Study Guide);
- administrare Linux - (UNIX and Linux System Administration Handbook, 5th edition);
- Ubuntu Server Guide (https://ubuntu.com/server/docs);
- Docker - (https://docs.docker.com/)
- Kubernetes - (https://kubernetes.io/docs/home/)
- tehnologii de detecție și prevenire a atacurilor sisteme de tip IPS/IDS, detectarea scanărilor de rețea, a pachetelor greșit formatate, a atacurilor tip DoS etc; reguli de bune practici în securitatea cibernetica; (Guide to Intrusion Detection and Prevention Systems -IDPS);

Concursul se va desfășura în trei etape succesive, după cum urmează:

- selecția dosarelor de înscriere va avea loc în 02.08.2022 ora 15^{00};
- proba scrisă va avea loc în data de 08.08.2022, ora 09^{00};
- interviul va avea loc în data de 12.08.2022 ora 09^{00};

Se pot prezenta la următoarea etapă numai candidații declarați admiși la etapa precedentă.
Data limită până la care candidații vor depune actele pentru dosarul de concurs este 01.08.2022 ora 15^{00}, la Registratura APAVIL SA, Rm.Vâlcea, str. Carol I, nr.3-5.
Concursul se va desfășura la sediul APAVIL din str.Carol I, nr.3-5.
Informații suplimentare: Serviciul Resurse Umane, Salarizare și Arhivă tel. 0250/739580, interior 22.
Program de lucru: luni-joi, între orele $07^{00} – 15^{30}$
vineri, între orele $07^{00} – 13^{00}$.

CALENDARUL CONCURSULUI

01.08.2022 ora 15^{00}	termenul limită pentru depunerea dosarelor de concurs de către candidați
02.08.2022 ora 15^{00}	selecția dosarelor de concurs și afișarea rezultatelor selecției dosarelor
03.08.2022 ora 15^{00}	termenul limită pentru depunerea contestațiilor privind selecția dosarelor
04.08.2022 ora 15^{00}	soluționarea contestațiilor și afișarea rezultatelor acestora
08.08.2022 ora 09^{00}	proba scrisă
09.08.2022 ora 15^{00}	afișarea rezultatelor probei scrise
10.08.2022 ora 15^{00}	termenul limită pentru depunerea contestațiilor la proba scrisă
11.08.2022 ora 15^{00}	soluționarea contestațiilor și afișarea rezultatelor acestora
12.08.2022 ora 09^{00}	proba interviu
16.08.2022 ora 15^{00}	afișarea rezultatelor probei interviu
17.08.2022 ora 15^{00}	termenul limită pentru depunerea contestațiilor la proba interviu
18.08.2022 ora 15^{00}	soluționarea contestațiilor și afișarea rezultatelor acestora
19.08.2022 ora 13^{00}	afișarea rezultatelor finale la sediul societății APAVIL și pe site-ul www.apavil.ro

Director General
ing. Florescu Ion

SOCIETATEA COMERCIALĂ APAVIL S.A. 2 RM. VÂLCEA JUD. VÂLCEA

Șef Serviciu R.U., Salarizare și Arhivă
ec. Voican Georgeta

Întocmit,
insp. RU Tănăsescu Elena