Coa.nl | Cybersecurity Engineer

Ben jij een ervaren Security Engineer met een sterke achtergrond in Red Teaming, pentesten, en het implementeren van securityoplossingen? Heb jij diepgaande kennis van netwerk- en serverbeveiliging, geavanceerde authenticatieprotocollen, en automatisering? Wil je een actieve rol spelen in het versterken van de digitale weerbaarheid van een toonaangevende organisatie? Sluit je dan aan bij ons d**ynamische Team Cyberweerbaarheid, waar i**edere dag anders is!

Taakomschrijving

Als **Security Engineer** binnen Team Cyberweerbaarheid ben je verantwoordelijk voor het ontwerpen, implementeren en onderhouden van securityoplossingen. Ons team kenmerkt zich door een dynamische werkomgeving met wisselende prioriteiten. Dit vereist flexibiliteit in aanpak: de ene uitdaging vraagt om diepgaande analyse, terwijl een andere situatie vraagt om implementeren, doorontwikkelen, consulteren, afstemmen of het snel regelen van praktische oplossingen.

Je voert Red Teaming-oefeningen en penetratietesten uit en implementeert geavanceerde oplossingen zoals PAM- en IAM-systemen. Je ontwikkelt hardeningmaatregelen voor Linux- en Windows-servers, versterkt netwerkbeveiliging en optimaliseert securityprocessen met behulp van automatisering.

Samen met jouw team bouw je aan een robuuste beveiligingsarchitectuur en zorg je ervoor dat de organisatie voorbereid is op complexe dreigingen.

Verantwoordelijkheden

- **Red Teamingen assessments**: Uitvoeren van Red Teaming-oefeningen, penetratietesten en risico-assessments.
- **Securityoplossingen implementeren**: Ontwerpen, implementeren en beheren van oplossingen zoals PAM (bijv. CyberArk), IAM (bijv. One Identity), en SIEM-systemen (zoalsSplunk, Sentinel).
- **Hardening en optimalisatie**: Ontwikkelen van hardeningmaatregelen voor Linux- en Windows-servers.
- **Netwerk- en serverbeveiliging**: Optimaliseren van netwerkarchitecturen, firewallbeheer en endpointbeveiliging.
- **Beheer van Entra ID**:Configureren en beherenvan Microsoft Entra ID (AzureAD) en integratie met IAM- en PAM-oplossingen.
- **Processen en protocollen**: Implementeren en naleven van beveiligingsstandaarden zoals SAML, OAuth, OIDC en SCIM.
- **Automatisering en scripting**: Automatiseren van beveiligingsprocessen met PowerShell, Python of vergelijkbare talen.
- **Incidentresponse**: Analyseren van beveiligingsincidenten en ontwikkelen van responsstrategieën.
- **Dynamisch werken**: Afstemmen met stakeholders, consulteren bij implementatievraagstukken, en het pragmatisch oplossenvan urgente uitdagingen.
- **Rapportages**: Opstellen van gedetailleerde rapportages over incidenten, kwetsbaarheden en securitymaatregelen.

Profielomschrijving

- Ervaring:Minimaal 5 jaar ervaring als Security Engineerof vergelijkbare rol in cybersecurity.Aantoonbare ervaring met Red Teaming,pentesten, en incident response.Ervaring met implementatie en beheer van securityoplossingen zoals PAM, IAM, SI EM en endpointbeveiliging.

- Technische kennis:Diepgaande kennis van Linux- en Windows-serverbeveiliging.Expertise in netwerkbeveiliging, firewallbeheer en SIEM-tools (zoals Splunk, Sentinel).Bekendheid met EntraID, Azure Cloud, en identitygovernance-oplossingen.

- Automatiseringen
  scripting:Ervaring met PowerShell, Python of andereprogrammeertalen om processen te automatiseren.

- Beveiligingsprotocollen:Kennis van SAML, OIDC, OAuth, SCIM en andere relevantebeveiligin gsstandaarden.

- Certificeringen:Bij voorkeur gecertificeerd in SC-900, AZ-900,CEH, CISSP, of vergelijkbare certificeringen.

- Soft skills:Flexibel en in staat om snel te schakelen tussen verschillende werkstijlen en prioriteiten.Sterke analytische vaardigheden, communicatief vaardig en in staat complexe concepten begrijpelijk te maken.Proactieve werkhouding en teamspeler in een dynamische omgeving.

Functie-eisen

- **Opleiding**: HBO/WO-diploma in IT, Cybersecurity, of een gerelateerd vakgebied; praktijkervaring wordt zeer gewaardeerd.
- **Locatie**: Den Haag, met mogelijkheid tot hybride werken.Vaste dagen op kantoor: dinsdagen woensdag.
- **Flexibiliteit**: Bereidheid om buitenkantooruren te werkenindien nodig.
- **Persoonlijkheid**: Gedreven, analytisch, oplossingsgericht en een teamspeler.

Wat bieden wij jou?

- Een uitdagende functie binnen een toonaangevend Team Cyberweerbaarheid.
- De kans om impactte maken en een leidenderol te spelen in Red Teaming en pentesten.
- Flexibele werkuren en de mogelijkheid tot hybride werken.
- Uitstekende arbeidsvoorwaarden en een marktconform salaris.
- Een dynamische werkomgeving waar innovatie en samenwerking centraal staan.

Het COA hecht sterk waarde aan integriteit en betrouwbaarheid. Zodra wij jou een aanbod doen voor indiensttreding voeren we een pre-employment screening uit. De screening bestaat uit ten minste de volgende onderdelen: aanvraag Verklaring Omtrent Gedrag (VOG), Diploma- en certificaten controle, Identiteitscontrole.
Geïnteresseerd?
Sluit je aan bij Team Cyberweerbaarheid en werk mee aan een veilige en innovatieve digitale toekomst! Heb je vragen over de rol? Voel je vrij om Matthijs van der Velde (Recruitment Adviseur) te bellen op 0631329061. Acquisitie naar aanleiding van deze vacature wordt niet op prijs gesteld. Ben jij ZZP’er, houdt er dan rekening mee dat wij onze nieuwe collega’s alleen een loondienstverband aanbieden.