VIŠE O DPMETALS BH

Cijenimo raznoliku i motiviranu radnu snagu koja napreduje u traženju odgovornosti za izvrsnost.

DMP Metals je posvećen izgradnji sigurnog, poštenog i raznolikog radnog okruženja i kulture koja njeguje liderstvo i omogućava svakoj osobi da doprinese i ostvari svoj potencijal. Zdrave prakse zapošljavanja ključne su za razvoj radne snage sa potrebnim vještinama i kvalitetima za podršku uspješnom, etičkom i odgovornom poslovanju. Različitost se slavi i podstiče. Prednost će imati državljani i ljudi iz lokalnih zajednica.

Svi novi zaposleni će biti odabrani na osnovu kulture i usklađenosti vrijednosti.

ABOUT DPMETALS BH

We value a diverse and motivated workforce that thrives on seeking responsibility for excellence. DPMetals BH is committed to building a working environment that is secure, fair, and diverse and a culture that fosters leadership and allows every person to contribute and realize their potential. Sound employment practices are crucial to developing a workforce with the necessary skills and qualities to support a successful, ethical, and responsible business. Diversity is celebrated and encouraged.

Preference will be given to citizens and individuals from local communities. All new hires will be selected based on culture fit and alignment of values.

Pozicija: Inženjer za sajber sigurnost
Position: Cyber Security Engineer

Inženjer za sajber sigurnost odgovoran je za zaštitu informacionih sistema i operativne tehnologije organizacije kroz implementaciju, održavanje i stalno unapređenje sigurnosnih kontrola, alata i procesa. Ova pozicija osigurava povjerljivost, integritet i dostupnost korporativnih podataka i sistema putem proaktivnog nadzora prijetnji, detekcije i odgovora na incidente, upravljanja ranjivostima i zaštite krajnjih tačaka. Inženjer blisko sarađuje s IT, OT i timovima za usklađenost kako bi identifikovao rizike, otklonio ranjivosti i ojačao sveukupnu sigurnosnu poziciju organizacije u skladu s korporativnim standardima i regulatornim zahtjevima.

The Cyber Security Engineer is responsible for safeguarding the organization's information systems and operational technology by implementing, maintaining, and continuously improving cybersecurity controls, tools, and processes. This role ensures the confidentiality, integrity, and availability of corporate data and systems through proactive threat monitoring, incident detection and response, vulnerability management, and endpoint protection. The position collaborates closely with IT, OT, and compliance teams to identify risks, remediate vulnerabilities, and strengthen the overall security posture in alignment with corporate standards and regulatory requirements.

Glavne odgovornosti:

- Implementacija i održavanje sigurnosnih kontrola i alata u mrežnim, serverskim i endpoint okruženjima.
- Praćenje, analiza i reagovanje na sigurnosne alarme i incidente, uključujući slučajeve fišinga i malvera.
- Podrška aktivnostima upravljanja i otklanjanja ranjivosti u IT i OT sistemima.
- Učešće u procjeni rizika, zaštiti podataka i unapređenju procesa odgovora i oporavka od incidenata.
- Pravovremeno prijavljivanje otkrivenih ili potencijalnih sigurnosnih incidenata nadređenom ili vođi tima za odgovor na incidente.
- Osiguravanje da se DPM aktivnosti redovno izvještavaju direktoru operacija.
- Upravljanje i održavanje platformi za zaštitu krajnjih tačaka (antivirus, EDR, kontrola aplikacija).
- Osiguravanje da su svi endpoint uređaji ažurirani, nadgledani i usklađeni s korporativnim sigurnosnim standardima.
- Istraživanje sigurnosnih upozorenja na krajnjim tačkama i sprovođenje korektivnih mjera.
- Pružanje smjernica krajnjim korisnicima o sigurnosnim incidentima i najboljim praksama.
- Praćenje i analiza upozorenja iz SIEM, EDR i drugih sigurnosnih alata radi otkrivanja potencijalnih prijetnji.
- Odgovaranje na prijavljene fišing e-mailove i druge sigurnosne incidente.
- Dokumentovanje incidenata i izrada izvještaja s naučenim lekcijama radi kontinuiranog unapređenja.
- Saradnja s internim timovima na implementaciji korektivnih mjera i smanjenju rizika.
- Praćenje i procjena novootkrivenih ranjivosti relevantnih za IT i OT okruženja.
- Koordinacija planova za upravljanje zakrpama i otklanjanje ranjivosti sa vlasnicima sistema i aplikacija.
- Korištenje alata za skeniranje ranjivosti radi identifikacije slabosti i praćenja napretka u njihovom otklanjanju.
- Izvještavanje o trendovima ranjivosti i pokazateljima usklađenosti.
- Saradnja s različitim timovima radi jedinstvenog pristupa sajber sigurnosti.

- Učešće u inicijativama za edukaciju i podizanje svijesti o sajber sigurnosti.
- Predlaganje poboljšanja za unapređenje detekcije, prevencije i odgovora na incidente.
- Podrška internim i eksternim revizijama kroz obezbjeđivanje potrebne dokumentacije i dokaza.

Main Responsibilities:

- *Implement and maintain security controls and tools across network, server, and endpoint environments.*
- *Monitor, analyze, and respond to security alerts and incidents, including phishing and malware cases.*
- *Support vulnerability management and remediation activities across IT and OT systems.*
- *Assist in risk assessments, data protection, and improvement of incident response and recovery processes.*
- *Escalate detected or potential security incidents to the supervisor or incident response lead in a timely manner.*
- *Ensures that DPM activities are reported to the Operations Director.*
- *Manage and maintain endpoint security platforms (antivirus, EDR, application control).*
- *Ensure all endpoints are updated, monitored, and compliant with corporate security standards.*
- *Investigate endpoint alerts and perform remediation activities.*
- *Provide guidance to end users on endpoint security incidents and best practices.*
- *Monitor and analyze alerts from SIEM, EDR, and other security tools to detect potential threats.*
- *Respond to and investigate reported phishing emails and other security incidents.*
- *Document incidents and provide lessons learned for continuous improvement.*
- *Collaborate with internal teams to implement corrective measures and reduce future risk.*
- *Track and assess newly discovered vulnerabilities relevant to both IT and OT environments.*
- *Coordinate patch management and remediation plans with system and application owners.*
- *Use vulnerability scanning tools to identify weaknesses and verify remediation progress.*
- *Report on vulnerability trends and compliance metrics.*
- *Collaborate with different teams to ensure a unified approach to cybersecurity.*
- *Participate in cybersecurity awareness and training initiatives.*
- *Propose improvements to enhance detection, prevention, and incident response processes.*
- *Support internal and external audits, providing necessary documentation and evidence.*

Najuspješniji kandidati idealno će posjedovati slijedeće:

- ✓ Bachelor diploma iz oblasti računarstva, informacione sigurnosti, informacionih tehnologija ili srodnih oblasti.
- ✓ Relevantne certifikacije iz oblasti sigurnosti (npr. CompTIA Security+, CEH ili slične) predstavljaju prednost.
- ✓ Najmanje 2 godine radnog iskustva u oblasti sajber sigurnosti, administraciji mreža ili srodnim ulogama.
- ✓ Iskustvo u radu sa alatima za praćenje sigurnosti, EDR sistemima i upravljanjem ranjivostima.
- ✓ Iskustvo u radu sa SIEM platformama i analizom logova.
- ✓ Sposobnost istraživanja sigurnosnih incidenata i primjene korektivnih mjera.
- ✓ Znanje skriptovanja ili automatizacije u sigurnosnim operacijama (PowerShell, Python i sl.).
- ✓ Izražene analitičke sposobnosti i vještine rješavanja problema.
- ✓ Osnovno razumijevanje koncepata, standarda i okvira sajber sigurnosti.
- ✓ Dobro poznavanje mrežnih protokola, Windows/Linux sistema i sigurnosti Active Directory-a.
- ✓ Poznavanje zaštite krajnjih tačaka, vatrozida i alata za skeniranje ranjivosti.
- ✓ Razumijevanje principa IT/OT sigurnosti i najčešćih prijetnji.

ABOUT YOU

The most successful candidate will ideally possess the following:

- ✓ *Bachelor's degree in Computer Science, Information Security, Information Technology, or related field.*
- ✓ *Relevant security certifications (e.g., CompTIA Security+, CEH, or similar) are an advantage.*
- ✓ *Minimum of 2 years of experience in cybersecurity operations, network administration, or related role.*
- ✓ *Experience with security monitoring tools, EDR, and vulnerability management systems.*
- ✓ *Experience with SIEM platforms and log analysis.*
- ✓ *Ability to investigate security incidents and apply remediation measures.*
- ✓ *Knowledge of scripting or automation for security operations (PowerShell, Python, etc.).*
- ✓ *Strong analytical and problem-solving skills.*
- ✓ *Basic understanding of cybersecurity concepts, standards, and frameworks.*
- ✓ *Strong knowledge of network protocols, Windows/Linux systems, and Active Directory security.*
- ✓ *Familiarity with endpoint protection, firewalls, and vulnerability scanning tools.*

- ✓ *Understanding of IT/OT security principles and common threats.*

O PROCESU

U DPM Metals se predano angažiramo u zapošljavanju pojedinaca koji su u skladu s vrijednostima tvrtke i ispunjavaju zahtjeve uloge. Kao dio procesa zapošljavanja, provode se različite provjere radi utvrđivanja prikladnosti kandidata za određenu ulogu, uključujući provjere kriminalnog dosjea, medicinske provjere, provjere poslovnih partnera, provjere radnih dozvola, profesionalnu procjenu i/ili provjere referenci.

KAKO SE PRIJAVITI

Kako biste se prijavili za ovu priliku, prije isteka roka pošaljite kopiju svoje biografije sa jasnim naglaskom **za koji oglas i poziciju se prijavljujete** na e-mail **posao@dpmmetals.com.** Napominjemo da će samo kandidati koji uđu u uži izbor biti kontaktirani radi daljnjeg procesa. Još jednom zahvaljujemo na interesu za DPMetals BH. Radno mjesto je otvoreno dok ne nađemo najboljeg kandidata.

ABOUT OUR PROCESS

At DPMetals BH, we are committed to hiring individuals who align with the company's values and meet the requirements of the role. As part of the hiring process, there are various checks that can be conducted to establish the suitability of candidates for a role, including police/criminal checks, medical checks, business partner checks, right-to-work checks, occupational assessments, and/or reference checks.

HOW TO APPLY?

To apply for this role, please send a copy of your Resume clearly indicating the name of the role, to ***posao@dpmmetals.com***

Please note that only shortlisted candidates will be contacted for further consideration. Once again, thank you for your interest in DPMetals BH. The vacancy is open until we find our best match. We wish you the best of luck in your job search!