VSTOPI V DIGITALNI SVET PRILOŽNOSTI.
PRIDRUŽI SE NAM KOT

TelekomSlovenije

ANALITIK KIBERNETSKE VARNOSTI (CSOC ANALYST) (M/Ž)

V Telekomu Slovenije, vodilnem slovenskem ponudniku najsodobnejših komunikacijskih rešitev, iščemo strokovnjake, ki jih prihodnost navdušuje, ob tem pa želijo s svojim znanjem in izkušnjami prispevati k nadaljnji krepitvi področja zagotavljanja kibernetske varnosti.
Vas zanima digitalno forenzično raziskovanje, etično hekanje ali iskanje ranljivosti v sistemu? Želite spremljati razvoj komunikacij, testirati najsodobnejšo opremo ter se nenehno učiti in izpopolnjevati svoje znanje?
Potem smo se našli, zato se nam pridružite.

VSEBINA DELA

- stalni nadzor nad sistemi za zagotavljanje kibernetsko-informacijske varnosti,
- preventivno in proaktivno raziskovanje dogodkov, groženj,
- spremljanje in analiziranje omrežnega prometa,
- pregledovanje in ustrezno odzivanje na varnostne dogodke v orodju SIEM,
- skeniranje podatkovnih baz, zbiranje, analiziranje in korelacija dogodkov,
- izvajanje postopkov za analizo in zamejitev zlonamernih dejavnosti,
- takojšnji odziv na zaznane napade, ranljivosti,
- prijave dogodkov v TTS sistem (prioritizacija, kategorizacija, kritičnost),
- dokumentiranje vseh aktivnosti med trajanjem incidenta, zavarovanje dokazov in obveščanje,
- priprava nujnih obvestil, opozoril in izdelava poročil,
- izdelava zahtevkov za izboljšave in popravke.

OSEBNOSTNE LASTNOSTI, KI NAS NAVDUŠIJO

- natančnost,
- odgovornost,
- proaktivnost,
- želja po znanju, raziskovanju,
- samoiniciativnost,
- sposobnost dela v kritičnih situacijah / stres,
- timsko delo.

POGOJI ZA OPRAVLJANJE DELA

- najmanj VI. stopnja izobrazbe,
- izkušnje na področju informacijske in kibernetske varnosti,
- znanje angleškega jezika,
- obvladovanje windows in unix okolja (server in workstation),
- pripravljenost na triizmensko delo,
- vozniški izpit B-kategorije.

ŽELENA ZNANJA IN CERTIFIKATI

- poznavanje in uporaba orodij za zaznavo in preprečevanje vdorov,
- poznavanje in uporaba orodij za zajem in analizo mrežnega prometa,
- A/V orodja (poznavanje protivirusne rešitve, obvladovanje izbruhov virusov in na podlagi vzorcev razlikovanje dejavnosti virusov od usmerjenih napadov),
- poznavanje tehnologij in sistemov za DDOS zaščito,
- poznavanje osnov algoritmov kriptiranja podatkov (3DES, AES, RSA, MD5, SHA, SSL/TLS, DH ipd.),
- izkušnje s produkti varnostnih orodij: SIEM, IDS/IPS, NetFlow in orodij, kot so Snort, Argus, tcpdump, Wireshark, MS ATA, SCCM,
- poznavanje Checkpointa, Cisco stikal, Juniper,
- poznavanje telekomunikacijskih omrežji (TKO),
- napredna računalniška znanja (LAN, WAN, VPN), JavaScrip, Python, Perl ali PHP programiranje,
- poznavanje metodologije taktik, tehnik in postopkov za varnost omrežij.

POLNI CERTIFIKAT Družini prijazno podjetje

Zaposlujemo po načelu raznolikosti in enakih možnosti.

Delo se bo opravljalo v Ljubljani. Delovno razmerje bomo sklenili z več kandidati, sklenjeno pa bo po dogovoru. Prošnjo z življenjepisom pošljite na **zaposlitve@telekom.si**, in sicer najkasneje **do vključno 1. 9. 2018**.