

Specialist/Sektori i Mbrojtjes, Menaxhimit dhe Reagimit të Incidenteve Kibernetike, Drejtoria e Analizës së Sigurisë Kibernetike, në Autoritetin Kombëtar për Sigurinë Kibernetike.

Në zbatim të ligjit nr. 25/2024 “Për Sigurinë Kibernetike”, ligjit nr. 7961, datë 12.07.1995 “Kodi i Punës i Republikës së Shqipërisë”, i ndryshuar, vendimit të Këshillit të Ministrave nr. 783 datë 18.12.2024 “Për organizimin dhe funksionimin e Autoritetit Kombëtar për Sigurinë Kibernetike”, vendimit të Këshillit të Ministrave nr. 325, datë 31.05.2023 “Për miratimin e strukturës së pagave, niveleve të pagave dhe shtesave të tjera mbi pagë të zëvendësministrit, funksionarëve të kabineteve, prefektit, nënprefektit, nëpunësve civilë dhe punonjësve në disa institucione të administratës publike”, i ndryshuar, vendimit të Këshillit të Ministrave nr. 482, datë 24.07.2024 “Për përcaktimin e masës së shtesës për natyrë të veçantë pune për drejtorin e përgjithshëm dhe nëpunësit në njësitë teknike të përmbajtjes së Autoritetit Kombëtar për Sigurinë Kibernetike, urdhrit të Kryeministrit nr. 154, datë 15.09.2026 “Për miratimin e strukturës dhe të organikës së Autoritetit Kombëtar për Sigurinë Kibernetike”, Autoriteti Kombëtar për Sigurinë Kibernetike shpall konkurrimin për 1 (një) vend të lirë pune në pozicionin:

- **Specialist/Sektori i Mbrojtjes, Menaxhimit dhe Reagimit të Incidenteve Kibernetike, Drejtoria e Analizës së Sigurisë Kibernetike, në Autoritetin Kombëtar për Sigurinë Kibernetike.**

DETYRAT DHE PËRGJEGJËSITË E POZICIONIT PËRMBAJNË POR NUK KUFIZOHEN NË:

- Mbledh dhe analizon informacion nga Infrastrukturat Kritike dhe të Rëndësishme, sistemet SOC/SIEM, platformat Threat Intelligence dhe partnerët e autorizuar rreth kërcënimeve active;
- Harton dhe zbaton plane për menaxhimin dhe reagimin ndaj incidenteve kibernetike, përfshirë zbulimin, klasifikimin, prioritarizimin, eskalimin, izolimin, eliminimin, rikuperimin dhe analizën pas incidentit;
- Analizon log-et e marra nga sistemet SIEM/EDR bazuar në evidenca dhe, kur është e nevojshme, kryen analiza më të thelluara për identifikimin e aktiviteteve të dyshimta;
- Përmbledh, monitoron dhe investigon informacion nga burime dark web, forume, markete, kanale dhe platforma të specializuara për zbulimin e rrjedhjeve të të dhënave, kredencialeve të komprometuar, tregtimit të aksesit dhe aktiviteteve të aktorëve keqdashës;
- Identifikon dhe analizon metoda, teknika dhe taktika të reja sulmi të evidentuara në dark web dhe burime Threat Intelligence;
- Kryen dhe mbështet Threat Hunting, duke hartuar hipoteza bazuar në TTP, IOC dhe inteligjencë kibernetike dhe duke analizuar log-e, endpoint-e, rrjete, identitete dhe cloud;
- Identifikon, analizon, korelon dhe priorizon Indikatorët e Komprometimit të filtruar nga SOC dhe burime të tjera, me qëllim uljen e rrezikut të sulmeve;
- Analizon trafikun rrjetor dhe vlerëson konfigurime firewall, IDS/IPS, VPN, NAC, proxy, DNS, routing/switching dhe segmentim, duke hartuar rekomandime për dobësitë e evidentuara;
- Mbështet mbrojtjen, monitorimin dhe reagimin ndaj incidenteve në mjedise OT/ICS, sipas nevojës.
- Ndjek dhe përditëson Procedurën e Incidenteve, playbook-et, use-case-et dhe rregullat e detektimit dhe koordinon zbatimin e tyre gjatë incidenteve;
- Bashkëpunon me Sektorin e Hetimit të Incidenteve Kibernetike, SOC, operatorët përgjegjës dhe partnerët e autorizuar për trajtimin e incidenteve dhe shkëmbimin e informacionit teknik.

KËRKESA TË PËRGJITHSHME PËR KANDIDATËT

Arsimi: Niveli minimal i diplomës “Master Profesional”, në Teknologji Informacioni/Inxhinieri Kompjuterike/Inxhinieri Informatike/Inxhinieri Telekomunikacioni/Inxhinieri Elektronike/Inxhinieri Elektrike/Shkenca Kompjuterike/Informatikë Ekonomike.

Përvoja: Të paktën 1 vit përvojë pune në fusha që lidhen me sigurinë kibernetike, teknologjinë e informacionit, monitorimin ose menaxhimin e incidenteve.

FUSHA E NJOHURIVE:

Kandidatët do të intervistohen mbi fushën e njohurive si më poshtë:

- Njohuri në fushën e sigurisë kibernetike dhe menaxhimit të incidenteve kibernetike;
- Kategoritë dhe procedurat e incidenteve kibernetike, cikli i reagimit dhe playbook-et;
- Analizë log-esh dhe telemetrie në SIEM/EDR; njohuri mbi KQL, SPL ose gjuhë të ngjashme;
- Threat Intelligence, investigim në dark web dhe identifikim i rrjedhjeve të të dhënave, kredencialeve të komprometuara dhe aktiviteteve të aktorëve keqdashës;
- Threat Hunting, IOC/TTP dhe MITRE ATT&CK;
- Mjetet që përdoren gjatë analizimit të një incidenti dhe reagimit ndaj tij;
- Siguria e rrjeteve: TCP/IP, DNS, firewall, IDS/IPS, VPN, NAC, proxy dhe segmentim;
- Njohuri bazë mbi sigurinë OT/ICS dhe mjediset industriale.

Aftësi për të:

- Realizuar objektivat teknike, evidentuar sulmet dhe analizuar log-et, telemetrinë, risqet dhe masat/kundërmasat për mbrojtjen;
- Menaxhuar dhe koordinuar incidentet kibernetike nga identifikimi deri në rikuperim dhe mbyllje;
- Kryer investigim dhe analizë të informacionit Threat Intelligence dhe dark web;
- Identifikuar, analizuar dhe priorizuar IOC/TTP dhe kryer aktivitete Threat Hunting;
- Komunikuar në grup dhe përballuar situata kritike, duke shkëmbyer dhe argumentuar ide e mendime teknike;
- Organizuar, komunikuar, prezantuar dhe dokumentuar qartë rezultatet teknike;
- Të njohë mirë gjuhën angleze.
- Të disponojë certifikime/trajnime në fushën e sigurisë kibernetike lidhur me Incident Response, Threat Hunting, Threat Intelligence, Dark Web Analysis, MITRE ATT&CK dhe sigurinë e rrjeteve;
- Përbën avantazh pajisja me certifikime profesionale si Security+, CySA+, GCIH, GCIA ose certifikime të tjera të ngjashme, si dhe pjesëmarrja në Cyber Ranges dhe Cyber Drills;
- Njohuri në vlerësimet e rrezikut të sigurisë së informacionit.

Çdo kandidat jo-kualifikues pas procesit të intervistës, ka të drejtë për ankim jo më vonë se 2 (dy) ditë kalendarike pas marrjes së njoftimit.

PAGA PËR POZICIONIN ËSHTË NË KATEGORINË (IV-1)

PARAQITJA E DOKUMENTEVE:

Kandidati duhet të dërgojë brenda datës 08.10.2026, në Autoritetin Kombëtar për Sigurinë Kibernetike, në adresën: Bulevardi “Bajram Curri”, nr. 3, Tiranë ose në adresën e emailit: burimet.njerezore@aksk.gov.al, këto dokumente:

- Kërkesë për aplikim;
- CV (sipas formatit europass në gjuhën shqipe);
- Fotokopje të diplomave që disponon dhe listës së notave;
- Diplomat e përfunduara jashtë vendit duhet të shoqërohen edhe me dokumentin e njohjes nga institucionet përkatëse, sipas legjislacionit të arsimit të lartë;
- Fotokopje të librezës së punës (të gjitha faqet që vërtetojnë eksperiencën në punë);
- Fotokopje të certifikatave të kualifikimit (nëse ka);
- Fotokopje të dëshmive të gjuhëve të huaja;
- Vërtetimin e gjendjes gjyqësore;
- Të paktën një letër rekomandimi.

Mosparaqitja e plotë dhe brenda afatit e dokumenteve sjell skualifikim të kandidatit.