

Specialist/Sektori i Hetimit 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 Hetimit 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:

- Ekzaminon incidentet e ndodhura në Infrastrukturat Kritike dhe të Rëndësishme duke përdorur mjete të autorizuara për Malware Analysis, Reverse Engineering dhe Digital Forensics;
- Kryen analizë statike, dinamike dhe sjellore të mostrave malware, binarëve, skripteve, dokumenteve dhe artefakteve të dyshimta;
- Kryen reverse engineering për identifikimin e funksionalitetit, komunikimeve C2, persistencës, evazionit dhe teknikave të përdorura nga aktorët keqdashës;
- Mbledh, ruan dhe analizon prova digjitale, përfshirë imazhe forensike, memorie, log-e, endpoint-e dhe file systems, duke ruajtur chain of custody kur është e aplikueshme;
- Përcakton vijën kohore të incidentit, vektorët e komprometimit, lëvizjen laterale dhe aktivitetet e dyshimta;
- Nxjerr dhe analizon IOC, TTP dhe, sipas rastit, përgatit rregulla YARA/Sigma dhe rekomandime për detektim, izolim dhe mitigim;
- Përgatit raporte teknike post-analizë, konkluzione, rekomandime, masa dhe kundërmasa për incidentet e trajtuara;
- Mbështet procesin e reagimit dhe rikuperimit me evidenca dhe gjetje teknike;
- Bashkëpunon me sektorët e tjerë për korelimin e gjetjeve dhe trajtimin e incidenteve komplekse;
- Kontribuon në përgatitjen dhe përmirësimin e metodologjive të brendshme për malware analysis, reverse engineering dhe digital forensics.

KËRKESA TË PËRGJITHSHME PËR KANDIDATËT

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

Përvoja: Të ketë të paktën 2 vjet përvojë pune në profesion, nga të cilat jo më pak se 1 vit përvojë në fusha që lidhen me trajtimin, analizën ose menaxhimin e incidenteve kibernetike.

FUSHA E NJOHURIVE

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

- Parimet dhe proceset e menaxhimit dhe hetimit të incidenteve kibernetike;
- Malware Analysis: analizë statike, dinamike dhe sjellore;
- Reverse Engineering dhe përdorimi i debugger, disassembler/decompiler dhe sandbox-eve të autorizuar;
- Digital Forensics: disk imaging, memory acquisition, analizë log-esh, file systems, timeline dhe chain of custody;
- IOC, TTP, MITRE ATT&CK dhe teknikat e komprometimit si persistence, credential access, lateral movement, C2, defense evasion dhe data exfiltration;
- Rregulla dhe mekanizma detektimi si YARA/Sigma, sipas rastit;
- Hetimi i incidenteve në mjedise cloud, tradicionale, hibride dhe njohuri bazë mbi OT/ICS;
- Raportimi teknik, dokumentimi i evidencave dhe përgatitja e rekomandimeve për mitigim dhe rikuperim.

AFTËSI PËR TË:

- Analizuar evidenca digjitale dhe artefakte të dyshimta dhe për të nxjerrë konkluzione teknike të argumentuara;
- Identifikuar vektorë komprometimi, teknika sulmi dhe indikatorë të komprometimit;
- Punuar në mënyrë të strukturuar në situata kritike dhe me incidente me prioritet të lartë;
- Dokumentuar metodologjinë, gjetjet dhe rekomandimet në raporte teknike të qarta;
- Komunikuar dhe bashkëpunuar me ekipet teknike dhe strukturat e tjera të përfshira në trajtimin e incidenteve;
- Përdorur mirë gjuhën angleze në literaturë, dokumentacion dhe komunikim profesional.

Certifikime/Trajnime që përbëjnë avantazh:

- Digital Forensics, Malware Analysis, Reverse Engineering dhe Incident Response;
- GCIH, GCFA, GREM, Security+ ose certifikime të tjera të ngjashme;
- Trajnime në MITRE ATT&CK, Cyber Range, Cyber Drill dhe ushtrime të reagimit ndaj incidenteve.

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.