DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

FIȘA DE POST

Direcția Generală Operațiuni Tehnice

Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911

Expert preluare, analiză primară și răspuns la incidente securitate cibernetică
#789

1 Identificarea postului

1.1 Numele si prenumele titularului

- NUME + PRENUME

1.2 Denumirea postului

- **Expert preluare, analiză primară și răspuns la incidente securitate cibernetică**
- *Notă: În cazul în care denumirea postului din Directoratul Național de Securitate Cibernetică (DNSC) nu se regăsește în COR, se va trece denumirea din COR cea mai apropiată din punct de vedere al sarcinilor și responsabilităților.*

1.3 Gradul profesional / treapta profesională

- **Superior**

1.4 Poziția în COR (Clasificarea Ocupațiilor din Romania)

- **Cod COR: Expert în securitate cibernetică 252904**
- *Notă: În cazul în care poziția postului din DNSC nu se regăsește în COR, se va trece codul din COR pentru denumirea cea mai apropiata din punct de vedere al sarcinilor și responsabilităților.*

1.5 Compartimentul funcțional și locația

- Direcția Generală Operațiuni Tehnice - Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911
- Sediul DNSC / telemuncă
- **Poziția #789 în statul de funcții al DNSC**

1.6 Nivelul postului

- Execuție

1.7 Sfera relațională internă și externă

1.7.1 Ierarhice

- Se subordonează pe următoarea linie ierarhică următoarelor funcții de conducere:
    - **Coordonator securitate cibernetică** - Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911
    - **Manager securitate cibernetică** - Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911
    - **Manager superior securitate cibernetică** - Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911
    - **Manager superior securitate cibernetică** - Direcția Generală Operațiuni Tehnice; Conducere - Direcția Generală Operațiuni Tehnice, care coordonează Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911
    - **Adjunctul Directorului DNSC** care coordonează Direcția Generală Operațiuni Tehnice
    - **Directorul DNSC**
- Are în subordine: nu are în subordine alte posturi.

1.7.2 Funcționale

- Colaborează și cooperează cu toate funcțiile de conducere sau de execuție din:
    - Direcția Generală Operațiuni Tehnice (toate compartimentele)
    - Direcția Generală Strategie

        - Conducere Direcția Generală Strategie
        - Direcția Studii, Cercetare și Analiză Aprofundată
        - Direcția Prognoză, Raportare și Indicatori Cibernetici
        - Direcția Management al Riscurilor Cibernetice
        - Direcția Comunicare, Media și Marketing
        - Serviciul Protecție Reputație și Marcă în Spațiul Cibernetic
    - Direcția Generală Parteneriate Instituționale (toate compartimentele)
    - Direcția Generală Internă
        - Conducere Direcția Generală Internă
        - Direcția Juridică
        - Direcția Protecția Datelor Personale, Etică și Securitate Internă
- Colaborează și cooperează cu Directorul DNSC și cu membrii cabinetului acestuia.
- Colaborează și cooperează cu Adjuncții Directorului DNSC și cu membrii cabinetelor acestora.
- Colaborează și cooperează cu managerii de proiect și cu membrii echipelor de proiect în care participă, inclusiv cu beneficiarii, partenerii instituționali, contractorii, subcontractorii și consultanții implicați în aceste proiecte.

1.7.3 Reprezentare

- **Reprezintă DNSC și interesele DNSC** în raport cu părțile interne și externe implicate în activitățile specifice de preluare, analiză primară și răspuns la incidente de securitate cibernetică, în contextul funcției de Security Operating Center (SOC) național 24/7 și de punct național de contact prin sistemul 1911 a DNSC.
- **Reprezintă DNSC și interesele DNSC** în raport cu experți individuali și organizații profesionale sau non-guvernamentale implicate în activități profesionale, de conștientizare și educație privind echipe de tipul:
    - Computer Security Incident Response Team (CSIRT)
    - Computer Emergency Response Team (CERT)
    - Computer Incident Response Center (CIRC)
    - Cyber Security Incident Response Center (CSIRC)
    - Security Operations Center (SOC)
    - IT / Information Security Helpdesk
    - Crisis Management Team.

1.7.4 Control

- Nu are.

2 Descrierea postului

2.1 Scopul principal al postului

- Efectuează activități specifice de preluare, analiză primară și aprofundată și răspuns la incidente de securitate cibernetică, în contextul funcției DNSC de Security Operating Center (SOC) național 24/7 și de punct național de contact prin sistemul 1911.
- Participă la asigurarea de către DNSC a funcției de Security Operating Center (SOC) național 24/7 și de punct național de contact prin sistemul 1911, în colaborare și coordonare cu instituțiile statului care au competențe și atribuții în domeniu și cu autoritățile de reglementare din sectoarele implicate.

2.2 Descrierea sarcinilor / atribuțiilor / activităților postului

- Preia/răspunde la, procesează și documentează corespunzător apelurile telefonice venite pe numărul unic național 1911.
- Contribuie activ la menținerea și operarea/ utilizarea instrumentelor și tehnologiilor de securitate utilizate în **Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**, inclusiv sisteme de detectare și prevenire a intruziunilor, SIEM, firewall-uri și instrumente de protecție a stațiilor de lucru.
- Abordează în mod activ, spre rezolvare, incidentele reale/confirmate de securitate cibernetică detectate sau raportate la nivelul **Direcției Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**.
- Evaluează incidentele identificate și utilizează informații privind amenințările cibernetice, precum reguli și indicatori de compromis (IOCs) pentru a identifica sistemele afectate și amploarea atacului.
- Evaluează, analizează și documentează riscurile, impactul potențial și cauza aparentă a incidentelor de securitate cibernetică pe care le investighează și a fișierelor malițioase (malware) implicate.
- Identifică vulnerabilitățile ce au fost utilizate de atacatori, legate de incidentele de securitate cibernetică pe care le investighează.
- Participă în mod activ la activitățile de restabilire a confidențialității, integrității și disponibilității datelor și/sau infrastructurilor impactate datorită incidentului.
- Colectează și documentează date și informații suplimentare, atât din surse deschise, sau prin cooperare cu alte compartimente funcționale ale DNSC ori cu partenerii instituționali.
- Analizează procesele și configurațiile care rulează pe sistemele afectate de incidentele cibernetice. Efectuează analize aprofundate ale informațiilor privind amenințările pentru a identifica date privind autorul atacului, tipul de atac și datele sau sistemele afectate. Creează și implementează strategie de izolare a incidentelor și de recuperare a datelor și infrastructurilor impactate.
- Răspunde de identificarea amenințărilor cibernetice pentru infrastructurile pe care le monitorizează Aceasta include menținerea la curent cu atacurile și tendințele cibernetice noi și asigurarea faptului că sistemele de securitate au un set actualizat de reguli pentru a ajuta la detectarea unor astfel de atacuri.
- Furnizează expertiză și sprijin pentru identificarea, aplicarea și testarea corecțiilor (patch-uri) pentru infrastructurile, sistemele și software-ul vulnerabile.
- Pentru incidentele de securitate cibernetică pentru procesarea cărora este responsabil(ă) sau în rezolvarea cărora este implicat(ă) ca parte a activității derulate în **Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**:
    - Asigură înregistrarea incidentului, pregătește și transmite răspunsul preliminar al DNSC la incidentele de securitate cibernetică notificate către DNSC.
    - Analizează, înțelege și categorizează incidentul de securitate cibernetică.
    - Evaluează, analizează și documentează impactul potențial și cauza aparentă a incidentului.
    - Colectează și documentează date și informații suplimentare privind incidentul, atât din surse deschise, prin cooperare cu alte compartimente funcționale ale DNSC sau prin cooperare cu partenerii instituționali cu care **Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911** este în contact.
    - Identifică vulnerabilitățile ce au fost utilizate de atacatori, legate de incidente.
    - Participă în mod activ la activitățile de restabilire a confidențialității, integrității și disponibilității datelor impactate datorită incidentului.
    - Analizează preliminar artefactele tehnice corespunzând incidentului.
    - Efectuează clasificarea preliminară a tacticilor și tehnicilor folosite de atacatorii cibernetici, pe baza datelor disponibile.
    - Întocmește analiza de risc privind incidentele de securitate cibernetică.

- Întocmește, la cerere sau din proprie inițiativă, în limbile Română sau Engleză rapoarte privind incidentele de securitate cibernetică, ce conțin minimum următoarele secțiuni:
  - Rezumat - Executive summary
  - Descrierea incidentului - Description of the incident
  - Descrierea vulnerabilităților exploatate de atacatori precum și a tacticilor și tehnicilor utilizate de aceștia - Description of exploited vulnerabilities and of the adversary tactics and techniques
  - Concluzii - Conclusions
  - Recomandări - Recommendations
- Întocmește, la cerere sau din proprie inițiativă, statistici privind incidentele de securitate cibernetică.
- Pregătește, la cerere sau din proprie inițiativă, anunțuri sau comunicări în vederea publicării și diseminării de informații relevante privind categoriile de incidente procesate, sau privind incidente specifice.

- Răspunde de confidențialitatea datelor privind incidentele de securitate cibernetică notificate către DNSC sau procesate și analizate la nivelul **Direcției Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**, în conformitate cu prevederile legale, regulamentele interne ale DNSC și cu instrucțiunile primite.
- Participă, după caz, în echipele de implementare a proiectelor finanțate prin programe, instrumente, mecanisme, fonduri naționale, europene sau internaționale, precum și a celor finanțate prin Planul Național de Redresare și Reziliență (PNRR) al României ocupând în cadrul proiectelor o funcție / rol corespunzător experienței, aptitudinilor și cunoștințelor tehnice și non-tehnice. Participarea în proiect a titularului postului se face prin numire astfel:
  - Prin decizie a **Directorului DNSC;** sau
  - Prin decizie a **Adjunctului Directorului DNSC** care coordonează Direcția Generală Operațiuni Tehnice (DGOT).
- Elaborează, documentează și folosește în activitatea curentă proceduri (inclusiv incident response playbooks), metode, standarde, tehnici și instrumente privind atacurile și incidentele de securitate cibernetică notificate către DNSC sau monitorizate, procesate și analizate la nivelul **Direcției Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**.
- Participă la sesiunile de pregătire profesională **organizate trimestrial la nivelul Direcției Monitorizare Alerte Cibernetice, SOC 24/7 și 1911,** pentru a asigura menținerea și îmbunătățirea cunoștințelor profesionale proprii.
- Asigură o comunicare adecvată, prin metode de comunicare scrisă, discuții și feedback la nivelul **Direcției Monitorizare Alerte Cibernetice, SOC 24/7 și 1911** precum și între această direcție și alte compartimente din cadrul DNSC, constituenți și/sau partenerii instituționali.
- Răspunde pentru corectitudinea de fond și de formă a tuturor lucrărilor întocmite și/sau semnate.
- Lucrează atât individual cât și în echipă, și facilitează cooperarea și lucrul în echipă la nivelul **Direcției Monitorizare Alerte Cibernetice, SOC 24/7 și 1911** prin comunicare verbală și scrisă cu personalul direcției, diseminarea permanentă a tuturor informațiilor relevante către personalul direcției.
- Face propuneri concrete de îmbunătățire a mijloacelor și metodelor de lucru la nivelul **Direcției Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**, pentru a maximiza utilizarea eficientă a timpului de lucru și a resurselor avute la dispoziție, în scopul atingerii obiectivelor instituționale.
- **Asigură identificarea și rezolvarea cu celeritate** a problemelor apărute în derularea activităților curente în care este implicat(ă) și informează la timp superiorii ierarhici despre problemele apărute pe care nu le poate rezolva la nivelul său.

- Pregătește datele și informațiile necesare și întocmește raportarea periodică, pentru următorii **indicatori de performanță (KPIs - Key Performance Indicators)** ai activităților proprii:
    - Numărul total și numărul mediu de incidente gestionate într-o anumită perioadă de timp (lunar, trimestrial, anual) pe nivele de prioritate și pe sectoare / sub-sectoare.
    - Procentul (%) de incidente gestionate într-o anumită perioadă de timp (lunar, trimestrial, anual) pe nivele de prioritate, din totalul incidentelor gestionate la nivelul **Direcției Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**.
    - Nivelul mediu de satisfacție din partea raportorilor de incidente în urma feedback-ului primit (**CSAT - Customer Satisfaction Score**) pentru incidentele de securitate cibernetică pentru a căror preluare, analiză primară și răspuns este responsabil(ă).
    - Durata medie de timp necesară pentru a răspunde sau rezolva un incident (**MTTR - Mean Time to Resolution**) pentru rezolvarea căruia este responsabil(ă), pe baza datelor și informațiilor aferente tichetelor procesate la nivelul **Direcției Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**.
    - Rata cu care incidentele sunt rezolvate în timpul primei apariții, fără alerte repetate.
- Acționează cu bună-credință și amabilitate în exercitarea sarcinilor profesionale, prezentând o atitudine civilizată și un comportament bazat pe respect, corectitudine, integritate morală și profesională.
- Respectă dispozițiile Regulamentului European nr. 679/2016 și a Legii nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.

2.3 Delegarea de atribuții și competență

- În situația și pe perioada în care titularul postului se află în imposibilitatea de a-și îndeplini atribuțiile de serviciu (spre exemplu: concediu de odihnă, concediu pentru incapacitate de muncă, delegații, concediu fără plată, suspendare, detașare etc.), o parte din atribuțiile sale menționate în secțiunea anterioară vor fi preluate prin delegare de către una sau mai multe din următoarele funcții din **Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**:
    - Coordonator securitate cibernetică - Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911
    - Expert preluare, analiză primară și răspuns la incidente securitate cibernetică - Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911
    - Asistent preluare, analiză primară și răspuns la incidente securitate cibernetică - Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911

  iar preluarea de atribuții se face prin desemnare de către **Managerul superior securitate cibernetică, din Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911.**

3 Condiții specifice de ocupare a postului

3.1 Studii de specialitate

- Studii universitare de licență absolvite cu diplomă, respectiv studii superioare de lungă durată, absolvite cu diplomă de licență sau echivalentă.

3.2 Experiență profesională, competențe și aptitudini necesare

- **Experiență dovedită de minimum un (1) an în echipe de tipul următor (sau echivalent), acumulată în ultimii cinci (5) ani:**
    - Computer Security Incident Response Team (CSIRT)
    - Computer Emergency Response Team (CERT)
    - Computer Incident Response Center (CIRC)

- Cyber Security Incident Response Center (CSIRC)
- Security Operations Center (SOC)
- IT / Information Security Helpdesk
- Crisis Management Center
- IT Audit, IT Security Audit, Audit, Internal Audit
- Digital Forensics and Investigation (DFIR)
- Echipe de analiză și / sau investigare a incidentelor sau infracțiunilor digitale
- Echipe sau laboratoare de analiză și / sau testare a tehnologiilor digitale

- Cunoașterea prevederilor din:
  - OUG 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică;
  - Legea 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative;
  - Legea 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, Secțiunea a 3-a Managementul incidentelor Art. 27, 28, 29;
  - Hotărârea 1.321 din 30 decembrie 2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027;
  - Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS 2);
  - Standardul Ocupațional din Romania pentru: Codul Nomenclator / COR al calificării / ocupației: **Expert în securitate cibernetică 252904**.
- Cunoașterea **la un nivel general** a principiilor și conceptelor de bază privind securitatea informației / securitatea cibernetică: confidențialitate, disponibilitate, autentificare, integritate, control al accesului, non-repudiere, privacy (protecția datelor personale).
- Abilitatea de a procesa și analiza date și informații în scopul pregătirii de **rapoarte și rezumate de un nivel calitativ foarte ridicat**, ce includ utilizarea de tabele, imagini ilustrative sau grafice pentru sublinierea de concluzii și inter-relaționare a datelor și informațiilor analizate.
- Gândire critică și centrată pe rezolvarea problemelor profesionale din domeniul propriu.
- Abilitatea de a procesa, analiza și gestiona informații contextuale și volume mari de date.
- Abilitatea de a acționa într-o manieră logică și investigativă și cu atenție sporită la detalii.
- Aptitudini excelente de prezentare, comunicare, relaționare și interpersonale.
- Aptitudini de planificare, organizare și control a activității proprii.
- Aptitudini de luare a deciziilor, inițiativă și autonomie în acțiune.
- **Cunoștințe, competențe și abilitați (KSAs - knowledge, skills, and abilities) specifice efectuării de activități în cadrul unui CSIRT**, așa cum acestea sunt definite de National Institute of Standards and Technologies (NIST) National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity Education **(i.e. NICE Framework):**
  - Cunoștințe, competențe și abilități **profesionale**:
    - **Gândire critică - Critical Thinking (C011)** - are aptitudini privind analiza obiectivă a faptelor pentru a forma o judecată profesională.
    - **Comunicare orală/verbală - Oral Communication (C036)** - are aptitudini privind exprimarea informațiilor sau a ideilor prin viu grai.
    - **Comunicare scrisă - Written Communication (C060)** - are aptitudini privind formularea și comunicarea oricărui tip de mesaj care utilizează cuvântul scris.

- Cunoștințe, competențe și abilități **tehnice**:
  - **Rezolvarea de probleme - Problem Solving (C040)** - are aptitudini privind determinarea exactității și relevanței informațiilor și utilizarea unei judecăți profesionale solide pentru a evalua alternative; luarea unor decizii bine informate, obiective, care să ia în considerare faptele, obiectivele, constrângerile și riscurile, percepând în același timp impactul și implicațiile deciziilor proprii.
  - **Protejarea rețelelor - Computer Network Defense (C007)** - are aptitudini privind măsuri defensive pentru a detecta incidente, a răspunde și a proteja informațiile, sistemele informatice și rețelele împotriva amenințărilor cibernetice.
  - **Managementul incidentelor - Incident Management (C021)** - are aptitudini privind tactici, tehnologii, principii și procese pentru a analiza, prioritiza și gestiona incidentele cibernetice.
  - **Sisteme informatice / securitatea retelelor - Information Systems/Network Security (C024)** - are aptitudini privind metode, instrumente și proceduri, inclusiv elaborarea de planuri de securitate a informațiilor pentru a preveni vulnerabilitățile sistemelor informatice și pentru a menține sau a restabili securitatea sistemelor informatice și a serviciilor de rețea.
  - **Analiza de informații - Intelligence Analysis (C027)** - are aptitudini privind procesul prin care informațiile colectate despre un adversar sunt folosite pentru a răspunde la întrebări tactice despre operațiunile curente sau pentru a prezice comportamentul viitor al adversarilor cibernetici.
  - **Analiza amenințărilor - Threat Analysis (C055)** - are aptitudini privind procesul în care cunoașterea vulnerabilităților interne și externe relevante pentru o anumită organizație este corelată cu atacurile cibernetice din lumea reală.
  - **Evaluarea vulnerabilităților - Vulnerabilities Assessment (C057)** - are aptitudini privind principiile, metodele și instrumentele de evaluare a vulnerabilităților (e.g. în infrastructuri, rețele și sisteme informatice) precum și elaborarea sau recomandarea unor contramăsuri adecvate.
- Cunoștințe, competențe și abilități **operaționale**:
  - **Confidențialitatea și protecția datelor - Data Privacy and Protection (C014)** - are aptitudini privind relația dintre colectarea, stocarea și difuzarea datelor, protejând în același timp viața privată a persoanelor fizice.
  - **Juridic, Guvernanță și Jurisprudență - Legal, Government, and Jurisprudence (C030)** - are aptitudini privind legi, reglementări, politici și etică, care pot avea un impact asupra activităților organizaționale.
  - **Cunoașterea/conștientizarea situației externe - External Awareness (C019) - este de dorit -** are aptitudini privind identificarea și înțelegerea modului în care problemele interne și externe influențează activitatea unei organizații.

3.3 Instrumente și tehnologii de lucru

- Are experiență anterioară și poate să utilizeze **la un nivel avansat** aplicații de tip Office din lista de mai jos sau echivalent:
  - Microsoft Word, Excel, Powerpoint, Outlook, Teams, etc.
  - Google Docs, Sheets, Slides, Calendar, Sites etc.
  - Libre Office Writer, Calc, Impress, Draw, Math, Base etc.
- Are experiență anterioară practică cu, sau poate să utilizeze **la un nivel avansat** cel puțin una din platformele următoare (sau echivalent) de tip Security Information and Event Management (SIEM), SOC sau Incident Response:
  - Request Tracker for Incident Response (RTIR)

- Malware Information Sharing Platform (MISP)
- ArcSight Enterprise Security Manager (ESM)
- AlienVault OSSIM
- CrowdStrike Falcon Insight
- Cynet 360
- Exabeam
- Heimdal Security XDR
- IBM QRadar
- IBM X-Force Incident Response and Intelligence Services (IRIS)
- IntelMQ
- LogRhythm SIEM
- LogRhythm XDR Stack
- SolarWinds Security Event Manager
- Splunk Security Orchestration and Automation (Splunk SOAR) / Splunk Phantom
- TheHive
- Trellix
- TrendMicro XDR
- Mandiant Advantage Automated Defense, etc.

3.4 Certificări sau cursuri de specializare

- **Trebuie să posede cel puțin una (1)** din următoarele certificări sau cursuri de specializare (sau echivalent):
  - CISM (Certified Information Security Manager)
  - CISA (Certified Information Systems Auditor)
  - CISSP (Certified Information Systems Security Professional)
  - CRISC (Certified in Risk and Information Systems Control)
  - IACIS Certified Forensic Computer Examiner (CFCE)
  - CompTIA Security+
  - CompTIA Cybersecurity Analyst (CySA+)
  - EC-Council Certified Incident Handler (E|CIH)
  - EC-Council Certified SOC Analyst (CSA)
  - EC-Council Computer Hacking Forensic Investigator (CHFI)
  - EnCase Certified Examiner (EnCe)
  - GIAC Advanced Smartphone Forensics (GASF)
  - GIAC Certified Forensic Analyst (GCFA)
  - GIAC Certified Forensic Examiner (GCFE)
  - GIAC Certified Incident Handler (GCIH)
  - GIAC Cloud Forensics Responder (GCFR)
  - GIAC Cyber Threat Intelligence (GCTI)
  - GIAC Network Forensic Analyst (GNFA)

- GIAC Reverse Engineering Malware (GREM)
- GIAC Response and Industrial Defense (GRID)
- GIAC Security Operations Certified (GSOC)
- ISO/IEC 27001 Lead Auditor
- ISO/IEC 27001 Lead Implementer
- MITRE ATT&CK Fundamentals
- MITRE ATT&CK Defender
- OSWP (Offensive Security Wireless Professional)

- **Are obligația ca în termen de maximum un (1) an de la data preluării postului, să obțină cel puțin una (1) din următoarele certificări** (sau echivalent) - costurile aferente fiind suportate de către DNSC:
  - CISM (Certified Information Security Manager)
  - CISA (Certified Information Systems Auditor)
  - CISSP (Certified Information Systems Security Professional)
  - CRISC (Certified in Risk and Information Systems Control)
  - IACIS Certified Forensic Computer Examiner (CFCE)
  - CompTIA Security+
  - CompTIA Cybersecurity Analyst (CySA+)
  - EC-Council Certified Incident Handler (E|CIH)
  - EC-Council Certified SOC Analyst (CSA)
  - EC-Council Computer Hacking Forensic Investigator (CHFI)
  - EnCase Certified Examiner (EnCe)
  - GIAC Advanced Smartphone Forensics (GASF)
  - GIAC Certified Forensic Analyst (GCFA)
  - GIAC Certified Forensic Examiner (GCFE)
  - GIAC Certified Incident Handler (GCIH)
  - GIAC Cloud Forensics Responder (GCFR)
  - GIAC Cyber Threat Intelligence (GCTI)
  - GIAC Network Forensic Analyst (GNFA)
  - GIAC Reverse Engineering Malware (GREM)
  - GIAC Response and Industrial Defense (GRID)
  - GIAC Security Operations Certified (GSOC)
  - ISO/IEC 27001 Lead Auditor
  - ISO/IEC 27001 Lead Implementer
  - MITRE ATT&CK Fundamentals
  - MITRE ATT&CK Defender
  - OSWP (Offensive Security Wireless Professional)

3.5 Metodologii cunoscute

- Trebuie să cunoască **la un nivel general** metodologiile sau cadrele tehnice (frameworks) din lista de mai jos sau echivalent:

- FIRST - Computer Security Incident Response Team (CSIRT) Services Roles and Competencies
- FIRST - Computer Security Incident Response Team (CSIRT) Services Framework
- MITRE ATT&CK
- NIST - Computer Security Incident Handling Guide, Special Publication 800-61
- NIST - Guide to Malware Incident Prevention and Handling, Special Publication 800-83

3.6 Cunoștințe de limba română și de limbi străine

- Cunoașterea limbii române ca limbă maternă sau limbă română de **minimum nivel C1** conform Common European Framework of Reference for Languages CEFR
- Cunoașterea limbii engleze de **minimum nivel B2** conform Common European Framework of Reference for Languages CEFR. Titularul postului are obligația ca în termen de maximum trei (3) luni de la data angajării să prezinte dovada îndeplinirii cerinței obligatorii de limbă engleză de minimum nivel B2 conform Common European Framework of Reference for Languages CEFR.
- Cunoașterea unei a doua limbi străine europene (franceza, germana, italiana, spaniola, olandeza, maghiara, greaca, etc.) este de dorit.

3.7 Cerințe privind cetățenia

- Cetățenie română, a unui alt stat membru al Uniunii Europene ori al Spațiului Economic European, ori cetățenia Confederației Elvețiene.
- *Notă: Persoanele care au cetățenia unui alt stat membru al Uniunii Europene ori al Spațiului Economic European ori cetățenia Confederației Elvețiene pot fi încadrate în muncă pe teritoriul României în baza unui contract individual de munca în aceleași condiții în care pot fi angajați și cetățenii români.*

3.8 Autorizații speciale pentru exercitarea atribuțiilor

- Nu este cazul.

4 Indicatori de performanță

- **Numărul total și numărul mediu de incidente gestionate** într-o anumită perioadă de timp (lunar, trimestrial, anual) pe nivele de prioritate.
- **Procentul (%) de incidente gestionate** într-o anumită perioadă de timp (lunar, trimestrial, anual) pe nivele de prioritate, din totalul incidentelor gestionate la nivelul **Direcției Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**.
- **Nivelul mediu de satisfacție din partea raportorilor de incidente** în urma feedback-ului primit (CSAT - Customer Satisfaction Score) pentru incidentele de securitate cibernetică pentru a căror preluare, analiză primară și răspuns este responsabil(ă).
- **Durata medie de timp necesară pentru a răspunde sau rezolva un incident** (MTTR - Mean Time to Resolution) pentru rezolvarea căruia este responsabil(ă), pe baza datelor și informațiilor aferente tichetelor procesate la nivelul **Direcției Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**.
- Rata cu care incidentele sunt rezolvate în timpul primei apariții, fără alerte repetate.
- Efectuarea anuală a unui **număr minimal de șaisprezece (16) ore de cursuri online de pregătire profesională în domenii relevante pentru Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**, dovedită cu certificat de participare/absolvire/diplomă sau similar. În cazul în care sunt costuri implicate de efectuarea cursurilor, acestea vor fi suportate de către DNSC, cu aprobarea superiorilor ierarhici.
- Lipsa absențelor nemotivate pentru participarea la sesiunile de pregătire profesională **organizate trimestrial la nivelul Direcției Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**, ce au ca obiectiv asigurarea menținerii și îmbunătățirii cunoștințelor profesionale proprii.

- **Concluzii pozitive la evaluarea independentă bi-anuală (la 6 luni)** a performanței în acest post, cu accent pe îndeplinirea sarcinilor, atribuțiilor și activităților postului.
- **Lipsa unor plângeri sau reclamații fundamentate** venite din partea constituenților implicați cu privire la incidentele de securitate cibernetică pentru procesarea cărora este responsabil(ă) sau în rezolvarea cărora este implicat(ă) ca parte a activității derulate în **Direcția Monitorizare Alerte Cibernetice, SOC 24/7 și 1911**.

Directoratul Național de Securitate Cibernetică	Angajat/Salariat
Nume + Prenume	**Nume + Prenume**
Data _____	Data _____
Nume + Prenume	
Data _____	
Nume + Prenume	
Data _____	