

OFERTA TEHNICĂ

ACHIZIȚIONAREA ȘI IMPLEMENTAREA PLATFORMEI
INTEGRATE DE MONITORIZARE A TRAFICULUI RUTIER ȘI
SUPRAVEGHERE VIDEO

Oferta Tehnică

MELITAX-GRUP | STR. VASILE ALECSANDRI, 143, CHIȘINĂU, MD2005

Table of Contents

1.	Introducere	2
1.1	Obiectivele Proiectului și Scopul Achiziției	2
1.2	Informații generale cu privire la soluția de platformă.....	2
2.	Configurația Ofertată	7
2.1.	Descrierea Soluției de Platformă.....	8
2.2.	Alte funcționalități cheie	13
3.	Lista materialelor anexate	17
4.	Complianța cu cerințele Caietului de sarcini	17
4.1	Cerințe față de platforma unificată de securitate.....	17
4.1.1	- Interfața unificată de management și control	18
4.1.2	- Cerințe față de interoperabilitate și integrare	20
4.1.3	- Monitorizarea și raportarea în timp real	22
4.2	Cerințe față de arhitectura	24
4.2.1	Arhitectura deschisă și modulară	25
4.2.2	Implementare distribuită	25
4.2.3	Cerințe de securitate.....	27
4.2.4	Suport pentru extensii și inovație.....	29
4.3	Evaluarea Performanței și Scalabilității	31
4.3.1	Scalabilitatea Sistemului	31
4.3.2	Performanța Sistemului	32
4.3.3	Redundanță și recuperare în caz de dezastru.....	32
5.	Cerințe funcționale ale platformei	33
5.1	Componenta de analiză a traficului rutier	33
5.2	Componenta de management video (VMS).....	36
5.3	Analiză video avansată	38
5.4	Interfața programatică de aplicație (API)	43
5.5	Monitorizarea și gestionarea incidentelor.....	43
6.	Suport tehnic și mentenanță.....	45

1. Introducere

1.1 Obiectivele Proiectului și Scopul Achiziției

Înțelegem că obiectivul acestei achiziții este de a implementa o platformă integrată de monitorizare a traficului rutier și supraveghere video, care să sprijine eforturile naționale de a asigura siguranța publică și fluidizarea traficului. Pe măsură ce densitatea traficului crește și mediul urban evoluează, Republica Moldova, asemenea multor alte țări europene, se confruntă cu provocări semnificative în gestionarea securității rutiere și a ordinii publice. Prin această achiziție, autoritatea contractantă urmărește să adopte o soluție modernă, aliniată standardelor internaționale, capabilă să îmbunătățească monitorizarea în timp real și să faciliteze un răspuns rapid și coordonat în caz de incidente.

Oferta noastră reflectă angajamentul de a sprijini aceste obiective printr-o soluție tehnică de ultimă generație, care integrează capabilități de analiză video, recunoaștere automată a numerelor de înmatriculare (ANPR) și monitorizare inteligentă. Soluția noastră este gândită să ofere o interfață unificată și intuitivă pentru gestionarea centralizată a tuturor componentelor de securitate și supraveghere, asigurând în același timp flexibilitate și scalabilitate pentru viitoarele extinderi sau modificări ale infrastructurii de monitorizare.

Cunoaștem că, din perspectivă globală și europeană, tendințele actuale în domeniul monitorizării traficului pun accentul pe utilizarea tehnologiilor inteligente pentru optimizarea fluxului de trafic și creșterea siguranței publice. Tehnologii precum IoT, analiza video avansată și integrarea cu sisteme de inteligență sunt acum indispensabile pentru un management eficient și un mediu sigur. Prin această propunere, ne angajăm să furnizăm o soluție de platformă, specializată, de ultimă generație, care să răspundă la cerințele operaționale aliniate la nevoile și viziunile naționale în materie de siguranță.

Scopul ofertei noastre este de a contribui la dezvoltarea unei infrastructuri robuste și interconectate, capabile să susțină cerințele specifice de securitate, să faciliteze monitorizarea traficului într-o manieră eficientă și modernă, dar și să ofere perspective fiabile și sustenabile de extindere a aplicabilității. Soluția propusă este concepută astfel încât să permită o expansiune facilă a capacităților și o integrare rapidă a modulelor funcționale și tehnologiilor noi, în funcție de necesitățile operaționale și provocărilor întâmpinate.

Prin această ofertă, dorim să demonstrăm că suntem un partener de încredere, cu o înțelegere profundă a provocărilor specifice ale acestui proiect și a contextului național și internațional în care se înscrie. Ne propunem să contribuim la realizarea unui sistem de monitorizare care să fie nu doar eficient, dar și adaptabil, capabil să răspundă la cerințele în continuă schimbare.

1.2 Informații generale cu privire la soluția de platformă

Soluția tehnică propusă reprezintă o platformă integrată de monitorizare și securitate, construită pe baza produselor și tehnologiilor avansate **Genetec, BriefCam și Vaxtor**. Această combinație puternică de sisteme reprezintă o soluție unificată, flexibilă și scalabilă, creată special pentru a răspunde cerințelor funcționale și nevoile operaționale ale autorității contractante și pentru a depăși așteptările în ceea ce privește performanța și adaptabilitatea la noile provocări din domeniul siguranței publice și monitorizării traficului.



GENETEC este un lider recunoscut în domeniul platformelor unificate de securitate, oferind soluții complexe care îmbină sisteme, sub-sisteme și instrumente specializate de securitate, inclusiv gestionarea video, controlul accesului și recunoașterea automată a numerelor de înmatriculare într-o singură interfață. Platforma Genetec Security

Center este folosită la scară globală și este apreciată pentru flexibilitatea, capacitățile de integrare și scalabilitatea sa. Prin integrarea diverselor module și tehnologii, Genetec facilitează o viziune unificată asupra securității și oferă operatorilor instrumente puternice pentru monitorizare și control. Compania a primit numeroase premii și distincții în cadrul unor competiții prestigioase din industrie.

OUR BUSINESS AND CULTURE

Awards and recognition



Department of
Homeland Security
(DHS) Compliance–
Security Center



Omdia recognizes Genetec
as the world leader in VMS,
and the fastest-growing
access control software
provider in the world



Genetec was selected as
the Best Security
Manufacturer at the 2022
US OSPA Awards



Genetec authorized by the
Common Vulnerabilities
and Exposures (CVE)
Program as a CVE
Numbering Authority (CNA)

Acste mențiuni atestă angajamentul Genetec față de dezvoltarea și implementarea unor soluții sigure, fiabile și inovatoare, recunoscute la nivel global pentru performanță și tehnologie de vârf.

În aceeași ordine de idei angajamentul companiei față de securitate, conformitate și protecția datelor, asigurând clienților soluții de încredere, conforme cu cele mai stricte standarde internaționale sunt susținute de certificările deținute. De la certificări pentru soluții on-premise și cloud, până la acreditări pentru protecția datelor personale și analitica, aceste recunoașteri demonstrează performanța și calitatea înaltă a platformelor Genetec în sectoarele guvernamentale, private și industriale. În imagine sunt prezentate principalele certificări, precum ISO 27001, SOC 2, DHS approval, și aprobări de la organizații de top precum FBI CJIS, CPNI, și EuroPriSe, garantând conformitatea în materie de securitate fizică, cloud și confidențialitatea datelor.

CERTIFICATIONS

Our certifications

On
premise



UL 2900-2-3
SC Omnicast



CSPN ANSSI
Synergis Cloud Link



DHS approved
Security Center

Cloud
solutions



ISO 27001
ISMS



FBI CJIS
Cloud archives



SOC 2
Cloud Products



ISO 27017
CSM

Privacy &
analytics



EuroPriSe certified
Privacy Protector



CPNI approved
Intrusion Detector

Portofoliul de aplicații software Genetec include soluții inovatoare și integrate pentru securitate, operațiuni și inteligență. Aceste aplicații utilizează tehnologii avansate pentru a facilita gestionarea incidentelor, analiza datelor și colaborarea între echipe.

SOLUTIONS OVERVIEW

Our software applications portfolio

Intelligence

Understand the everyday



**Genetec
Citigraf.**
Comprehensive response
coordination



**Genetec
Clearance.**
Digital evidence
management



**Genetec
Valcri.**
Investigative analysis system

Operations

Improve the everyday



**Genetec
Mission Control.**
Collaborative decision
management



**Genetec
ClearID.**
Physical identity and
access management

Security

Protect the everyday

PHYSICAL SECURITY SOLUTIONS



**Genetec
Security Center.**
Comprehensive unified security



**Security Center
Omnicast.**
Scalable video management



**Security Center
AutoVu.**
Automatic license plate recognition



**Security Center
Synergis.**
Complete access control



**Security Center
Sipelia.**
Communications management system



**Genetec
Stratocast.**
Cloud-based video monitoring

APPLIANCES



Streamvault
Turnkey security infrastructure solutions

Structura Portofoliului de Soluții Software Genetec

Portofoliul de soluții software Genetec este conceput cu o arhitectură modulară, care permite integrarea fluidă și interoperabilitatea între diverse aplicații, oferind utilizatorilor o soluție coerentă și eficientă pentru gestionarea securității și operațiunilor. La baza acestei structuri se află **Genetec Security Center**, platforma centralizată care reunește toate componentele necesare pentru o securitate completă și integrată.

Genetec Security Center este compus din module specializate, fiecare având roluri bine definite:

- **Omnicast** este dedicat gestionării video, permițând utilizatorilor să integreze și să controleze camere de supraveghere din diverse surse. Acest modul asigură un flux constant de date video, facilitând monitorizarea în timp real a situațiilor critice.

- **Synergis** oferă soluții avansate pentru controlul accesului, gestionând identificarea și autorizarea utilizatorilor în locațiile fizice.

- **AutoVu** se concentrează pe recunoașterea automată a numerelor de înmatriculare, având capacitatea de a monitoriza vehiculele în diverse contexte. Acest modul este esențial pentru gestionarea traficului rutier.

- **Sipelia** integrează comunicațiile, facilitând gestionarea eficientă a interacțiunilor între părțile implicate. Această interfață permite o comunicare rapidă și eficientă, esențială în situații de interes.

Pe lângă aceste module dedicate securității, portofoliul include soluții axate pe operațiuni:

- **Mission Control** este structurat pentru a gestiona incidentele, oferind fluxuri de lucru predefinite și personalizabile care ghidează operatorii în gestionarea eficientă a situațiilor critice. Acest modul permite implementarea unor proceduri standardizate, asigurând o reacție organizată și rapidă la evenimentele care necesită intervenție.

- **Clear ID** se concentrează pe managementul identității fizice și accesului, aducând un plus de organizare în procesele de autorizare.

În plus, Genetec îmbogățește portofoliul cu aplicații de inteligență care sprijină soluțiile de securitate și operațiuni:

- **Citigraf** este dedicat gestionării coordonării răspunsurilor în situații de urgență, facilitând integrarea informațiilor din diferite surse pentru a oferi o imagine completă asupra incidentelor.

- **Clearance** se ocupă de gestionarea probelor digitale, permițând integrarea eficientă a datelor relevante în procesul de investigație.

- **Valcri** se concentrează pe analiza investigativă, completând astfel capabilitățile analitice ale platformei și oferind instrumente esențiale pentru investigarea incidentelor.

Această structură modulară și interconectată a portofoliului de soluții Genetec permite organizațiilor să își adapteze sistemele de securitate și operațiuni în funcție de cerințele specifice, asigurându-se că fiecare componentă funcționează armonios într-un ecosistem integrat. Astfel, utilizatorii beneficiază de o soluție adaptabilă, capabilă să răspundă provocărilor variate întâmpinate în gestionarea securității și operațiunilor.



BriefCam este o companie de top în domeniul analizei video, specializată în dezvoltarea de soluții care transformă conținutul video din sisteme de supraveghere în informații acționabile și utile pentru o gamă largă de aplicații. Fondată în 2008, BriefCam este cunoscută pentru inovațiile sale în tehnologia de analiză video, utilizată de organizații din întreaga lume pentru a spori siguranța publică, a optimiza operațiunile și a susține luarea deciziilor strategice. Compania oferă o platformă cuprinzătoare de *Video Content Analytics*.

Detalii:

<https://www.briefcam.com/>

VAXTOR companie recunoscută pentru tehnologiile sale avansate de recunoaștere a numerelor de înmatriculare și clasificare a vehiculelor, oferă soluții de înaltă precizie care pot funcționa în condiții variate de trafic și la viteze ridicate. Soluțiile Vaxtor sunt integrate cu platformele de management video de top și sunt folosite pentru supravegherea și controlul traficului în numeroase țări, aducând valoare adăugată prin capacitățile extinse de recunoaștere și raportare.

Detalii:

<https://www.vaxtor.com/>

2. Configurația Ofertată

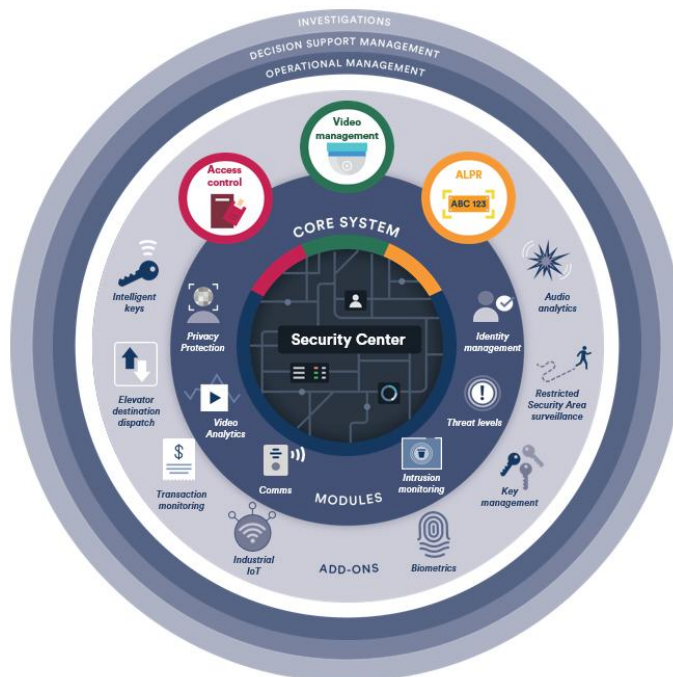
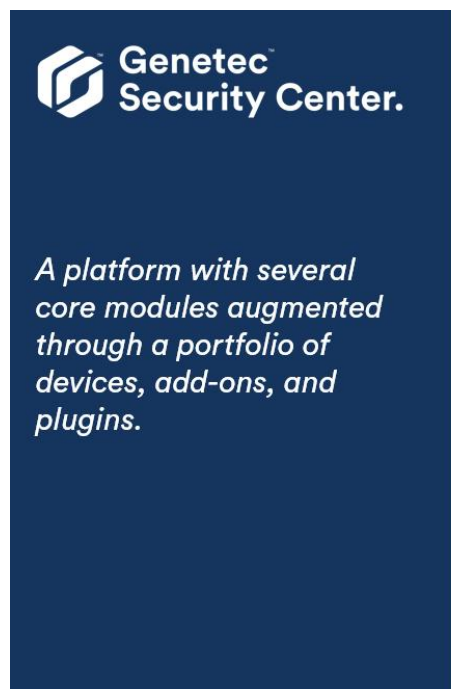
#	Denumire	Cant	Configurație Soluție Ofertată
1.	Platforma Unificată de Securitate	1	Platforma Unificata de Securitate Soluția de platformă oferită se bazează pe o serie de componente și module funcționale cheie, specializate, integrate într-o platformă unificată. menite să asigure toate cerințele funcționale și operaționale ale beneficiarului. Configurația Soluției: Genetec Security Center 5.12 Genetec Security Center (GSC) Base Enterprise Package; BriefCam – soluție avansată de analiză video Including Review, Research, Respond, Face Recognition, Multi-camera Search, Investigation; VaxALPR - ANPR server based analytical solution. Licențe incluse: - Dispozitive ANPR – 100; - Dispozitive ANPR server-based processing (4k) – 25; - Dispozitive analiză video avansată în timp real (server-based) – 20; - Analiză video avansată în regim de investigare (server-based) – 100 (dispozitive); - Utilizatori concomitenți pe platformă unificată – 10 - Utilizatori concomitenți pentru componenta de analiză video avansată – 5 utilizatori; - Utilizatori concomitenți pentru componenta de gestionare a incidentelor – 10 utilizatori; - Conexiuni concurente pentru componenta API – 10.
2.	Suport tehnic și garanție		Garanție și suport tehnic pentru o perioadă de 5 ani pentru toate componentele furnizate

2.1. Descrierea Soluției de Platformă



Genetec Security Center reprezintă nucleul soluției propuse - o platformă unificată de monitorizare și securitate, concepută pentru a oferi un management centralizat și integrat al mediului de securitate. Platforma

Genetec Security Center reunește **toate** componentele necesare pentru a crea o soluție completă, capabilă să integreze și să gestioneze diverse funcționalități printr-o interfață unificată.



Securitate unificată prin integrarea mai multor module Genetec Security Center. Este o platformă modulară care permite integrarea soluțiilor de supraveghere video (Omnicast), control al accesului (Synergis) și recunoașterea automată a numerelor de înmatriculare (AutoVu). Această unificare oferă o viziune completă și coordonată asupra activităților de securitate dintr-o organizație, asigurând controlul tuturor componentelor de securitate într-o singură platformă.

Interfață intuitivă și unică de utilizare. Platforma este construită pentru a oferi o experiență de utilizare simplificată printr-o interfață unică. Toate funcțiile și modulele sunt accesibile printr-un singur „panou de control,” facilitând gestionarea și monitorizarea integrată a securității. Operatorii au acces la toate funcționalitățile dintr-o singură interfață, reducând complexitatea și crescând eficiența.

Suport pentru diverse dispozitive și infrastructuri. Genetec Security Center este compatibil cu o gamă largă de echipamente și sisteme terțe, permițând beneficiarilor să aleagă hardware-ul care se potrivește cel mai bine nevoilor lor. Această compatibilitate extinsă oferă flexibilitate în implementare și permite o adaptare ușoară la infrastructuri complexe și diverse.

Scalabilitate ridicată. Platforma este extrem de scalabilă, fiind capabilă să susțină organizații de toate dimensiunile – de la ecosisteme mici, până la rețele globale extinse. Genetec Security Center poate crește odată cu organizația, adaptându-se ușor la noi cerințe și la extinderea infrastructurii de securitate.

Monitorizare în timp real și gestionarea incidentelor. Platforma include funcționalități de monitorizare în timp real și gestionare a incidentelor, oferind alerte și notificări instantanee pentru a sprijini răspunsul rapid la incidente de securitate. Genetec Mission Control™, un modul integrat de management al incidentelor, ghidează operatorii printr-un flux de lucru structurat pentru o intervenție eficientă și coordonată.

Rapoarte și analize detaliate. Genetec Security Center oferă instrumente avansate de raportare și analiză, permițând organizațiilor să acceseze informații istorice, să identifice tipare și să ia decizii informate pe baza datelor colectate. Aceste rapoarte sunt esențiale pentru audit, conformitate și optimizarea operațiunilor de securitate.

Genetec Security Center Federation. Funcționalitatea permite integrarea și gestionarea centralizată a mai multor sisteme Genetec Security Center distribuite geografic într-o singură infrastructură de securitate unificată. Această funcționalitate este ideală pentru organizațiile mari sau pentru cele cu locații multiple, oferind o viziune de ansamblu și un control unificat asupra securității, fără a compromite autonomia fiecărui sistem local.

- **Vizibilitate și control centralizat.** Prin Federalizare, administratorii pot monitoriza și gestiona toate locațiile dintr-o interfață centralizată, obținând o imagine completă a activităților și incidentelor din fiecare site. Aceasta permite o gestionare eficientă a incidentelor și a operațiunilor, indiferent de locația fizică a fiecărui sistem de securitate.
- **Autonomie locală și administrare centralizată.** Fiecare site sau locație poate funcționa autonom, având propriile setări și reguli de securitate, dar poate raporta și partaja informații cu sediul central. Acest lucru permite fiecărei locații să își mențină funcționalitățile și independența operațională, în timp ce managementul centralizat beneficiază de o viziune unificată.
- **Partajarea informațiilor și a resurselor.** Federalizarea permite partajarea de fluxuri video, date de acces și evenimente între site-uri, permițând operatorilor din locații diferite să colaboreze și să răspundă coordonat la incidente. De asemenea, permite accesul la resursele critice și la datele altor site-uri atunci când este necesar, îmbunătățind reacția și colaborarea la nivel organizațional.
- **Scalabilitate ridicată.** Funcționalitatea de Federalizare este extrem de scalabilă, permițând integrarea și adăugarea de noi site-uri sau locații pe măsură ce organizația se extinde. Aceasta face din Genetec Security Center o soluție ideală pentru organizațiile în creștere, care au nevoie de o platformă flexibilă și capabilă să gestioneze o rețea de securitate de mari dimensiuni.
- **Eficiență în gestionarea resurselor.** Cu Federalizarea, resursele de securitate pot fi gestionate mai eficient, eliminând redundanța și asigurând un control uniform asupra procedurilor de securitate în toate locațiile. De exemplu, administratorii pot aplica politici de securitate uniforme sau pot urmări KPI-urile de securitate într-un mod coordonat și unitar.
- **Securitate și redundanță.** Federalizarea Genetec Security Center este proiectată cu mecanisme de securitate robuste și redundanță, asigurând continuitatea operațională și securitatea datelor partajate între site-uri. Fiecare site poate funcționa independent, astfel încât o întrerupere într-o locație să nu afecteze întreaga infrastructură.



Pachetul de bază **Genetec Security Center (GSC) Base Enterprise** oferă funcționalități esențiale. În centrul acestei soluții se află **Video Management System - Omnicast**, care permite o monitorizare video

continuă și detaliată prin intermediul unui sistem unificat de gestionare a camerelor. Acest modul asigură captarea, stocarea și accesarea rapidă a fluxurilor video de la sute și mii de camere, facilitând o vizualizare clară a evenimentelor și suport pentru arhivare și transfer de date video. Fiecare incident poate fi urmărit și documentat cu ușurință, iar operatorilor li se oferă la dispoziție o interfață intuitivă pentru a controla toate echipamentele de supraveghere dintr-o singură platformă.



Suport pentru o gamă largă de camere și echipamente video. Omnicast este compatibil cu o varietate extinsă de camere de supraveghere și echipamente de margine de la diferiți producători, asigurând o integrare flexibilă. Acesta permite organizarea unui sistem de supraveghere unitar, indiferent de furnizorii echipamentelor video.

Monitorizare video în timp real și acces la înregistrări. Operatorii pot monitoriza fluxurile video live și pot accesa înregistrările video din arhivă în orice moment. Această capacitate de acces instant la înregistrări este esențială pentru evaluarea rapidă a incidentelor și pentru luarea de decizii informate în timp real.

Arhivare avansată și redundanță. Omnicast oferă opțiuni avansate de stocare și arhivare a datelor video, inclusiv redundanță pentru a asigura integritatea și continuitatea datelor chiar și în cazul defecțiunilor hardware. Acest lucru garantează că toate datele importante sunt protejate și accesibile în orice moment.

Gestionarea și controlul camerelor. Modulul Omnicast permite operatorilor să controleze și să gestioneze camerele de supraveghere, inclusiv funcții precum pan, tilt și zoom (PTZ). Aceasta oferă flexibilitate și posibilitatea de a ajusta rapid punctele de vedere pentru a răspunde eficient la incidente.

Alertare și notificare automată. Omnicast poate genera alerte automate și notificări pe baza unor reguli și evenimente predefinite, cum ar fi detectarea mișcării sau încălcările zonelor de acces. Aceasta

permite echipelor de securitate să fie informate imediat despre activități neobișnuite și să intervină prompt.

Analize și rapoarte video. Modulul oferă funcționalități de analiză video care permit organizațiilor să obțină informații detaliate despre activitatea monitorizată. Rapoartele video pot fi generate pentru a identifica tipare și pentru a sprijini deciziile.



Genetec Security Center AutoVu este un modul de recunoaștere automată a numerelor de înmatriculare (ANPR) integrat în platforma Genetec Security Center. AutoVu este proiectat pentru a facilita

monitorizarea și gestionarea traficului și pentru a sprijini siguranța publică, oferind capacități avansate de identificare și înregistrare automată a vehiculelor. Această soluție este ideală pentru aplicații precum monitorizarea parcarilor, supravegherea zonelor de acces restricționat și gestionarea traficului urban. Funcționalități principale ale AutoVu:

Recunoașterea automată a numerelor de înmatriculare (ANPR). AutoVu poate detecta și identifica rapid numerele de înmatriculare ale vehiculelor în mișcare sau staționare. Sistemul capturează plăcuțele de înmatriculare și le compară cu baze de date predefinite, alertând în cazul vehiculelor marcate ca fiind suspecte sau neautorizate.

Integrarea cu baze de date și liste de supraveghere. AutoVu se poate conecta la diverse liste de supraveghere și baze de date, permițând identificarea instantanee a vehiculelor care îndeplinesc anumite criterii (de exemplu, vehicule furate, vehicule neautorizate). Aceste liste pot fi actualizate în timp real, oferind informații precise și relevante pentru operatori.

Monitorizarea parcarilor și a zonelor de acces restricționat. Modulul AutoVu este util în gestionarea spațiilor de parcare prin identificarea vehiculelor care au permise valide sau care încalcă regulile de parcare. Aceasta permite o mai bună administrare a parcarilor publice sau private, reducând abuzurile și îmbunătățind experiența utilizatorilor legitimi.

Analiză de trafic și rapoarte statistice. AutoVu poate colecta și analiza date despre traficul rutier, oferind autorităților informații utile despre volumul și tiparele de trafic din anumite zone. Aceste informații pot fi folosite pentru a lua decizii informate privind infrastructura și planificarea traficului.

Suport pentru camere fixe și mobile. AutoVu este compatibil atât cu camerele fixe instalate în locații strategice, cât și cu camerele mobile montate pe vehicule de patrulare. Acest lucru extinde raza de acțiune a sistemului, permițând monitorizarea vehiculelor într-un mod flexibil și eficient.

Red Light Violation Detection aduce un plus de valoare în detectarea automată a încălcărilor de trafic. Integrând recunoașterea automată a numerelor de înmatriculare direct în platforma unificată Genetec, aceste module nu doar simplifică identificarea rapidă a vehiculelor în situații de interes, ci și contribuie la monitorizarea continuă a respectării regulilor de circulație.



Genetec Security Center Synergis este modulul de control al accesului fizic din cadrul platformei Genetec Security Center, cunoscut sub denumirea de Synergis

Enterprise Package. Synergis este proiectat pentru a oferi o soluție de control al accesului scalabilă și integrată, care permite organizațiilor să își securizeze eficient spațiile și să gestioneze accesul în timp real. Acest pachet avansat de control al accesului asigură o integrare nativă cu celelalte module Genetec, cum ar fi Omnicast pentru gestionarea video, AutoVu pentru recunoașterea automată a numerelor de înmatriculare (ANPR), Mission Control pentru managementul incidentelor, și altele, oferind astfel o soluție unificată de securitate.

Control în timp real al accesului. Synergis permite monitorizarea și gestionarea accesului în timp real, oferind operatorilor capacitatea de a vizualiza instantaneu evenimentele de acces și de a interveni rapid în situații de securitate. Controlul în timp real permite un răspuns prompt la orice tentativă de acces neautorizat.

Compatibilitate deschisă cu o gamă largă de echipamente. Synergis suportă o varietate de controlere și cititoare de acces de la diverși producători, ceea ce oferă organizațiilor flexibilitate în alegerea echipamentelor. Această compatibilitate extinsă facilitează integrarea într-o infrastructură existentă sau extinderea cu noi dispozitive fără a depinde de un singur furnizor.

Administrarea centralizată a drepturilor de acces. Prin Synergis, operatorii pot administra și configura centralizat permisiunile de acces, definind reguli și drepturi de acces pe baza rolurilor și necesităților fiecărui angajat. Aceasta asigură o gestionare granulară și eficientă a accesului, reducând riscurile și facilitând controlul.

Rapoarte și auditare detaliată. Modulul permite generarea de rapoarte detaliate și istorice de acces, oferind vizibilitate completă asupra activităților de acces și a evenimentelor din fiecare locație. Aceste rapoarte sunt utile pentru audituri interne și pentru a asigura conformitatea cu reglementările de securitate și protecția datelor.

Notificări și alerte de securitate. Synergis poate declanșa alerte automate atunci când sunt detectate încercări de acces neautorizat sau alte incidente critice, informând echipa de securitate în timp real. Aceasta asigură un răspuns rapid și o intervenție eficientă în caz de necesitate.

Integrare perfectă cu Omnicast și AutoVu. Prin integrarea cu Omnicast (gestionarea video) și AutoVu (recunoașterea automată a numerelor de înmatriculare), Synergis oferă o soluție completă de securitate fizică, permițând monitorizarea video sincronizată cu evenimentele de acces și detectarea vehiculelor în zonele de monitorizare.



Genetec Mission Control™ este un modul avansat de management al incidentelor și suport decizional, integrat în platforma Genetec Security Center.

Conceput pentru a ajuta organizațiile să gestioneze eficient situațiile de securitate și de interes, Mission Control permite o coordonare în timp real a resurselor, un răspuns structurat și o monitorizare atentă a evenimentelor de securitate, de la declanșare până la finalizarea și auditarea lor. Funcționalități cheie:

Management complet al incidentelor. Genetec Mission Control gestionează întregul ciclu al unui incident, de la momentul în care este declanșat până la auditul final. Aceasta permite o urmărire detaliată a fiecărui pas, asigurând o abordare coerentă și documentată pentru fiecare situație de securitate.

Proceduri de operare standard dinamice (SOP). Modulele de proceduri standard de operare ghidează operatorii prin pași clari și predefiniți pentru a asigura un răspuns rapid și consecvent la incidente. SOP-urile dinamice sunt adaptate contextului fiecărui incident, asigurând conformitatea cu protocoalele de securitate și sporind eficiența în gestionarea situațiilor critice.

Automatizarea fluxurilor de lucru. Mission Control automatizează procesele operaționale prin fluxuri de lucru personalizabile, care simplifică sarcinile de rutină și reduc volumul de muncă al operatorilor. Această automatizare asigură o intervenție rapidă și consistentă și permite echipelor să se concentreze pe sarcini cu prioritate ridicată.

Reguli inteligente de calificare a incidentelor. Motorul de reguli din Mission Control permite reducerea alarmelor false și a alarmelor neimportante, printr-o evaluare automată a incidentelor. Astfel, doar alertele relevante sunt transmise operatorilor, îmbunătățind concentrarea și eficiența.

Rapoarte detaliate și audit. Genetec Mission Control oferă capacități avansate de raportare și auditare, monitorizând performanța operatorilor, indicatorii de performanță (KPI) și lecțiile învățate din experiențele anterioare. Aceasta permite o îmbunătățire continuă a proceselor de securitate și o învățare sistematică pentru o adaptare eficientă la situațiile viitoare.

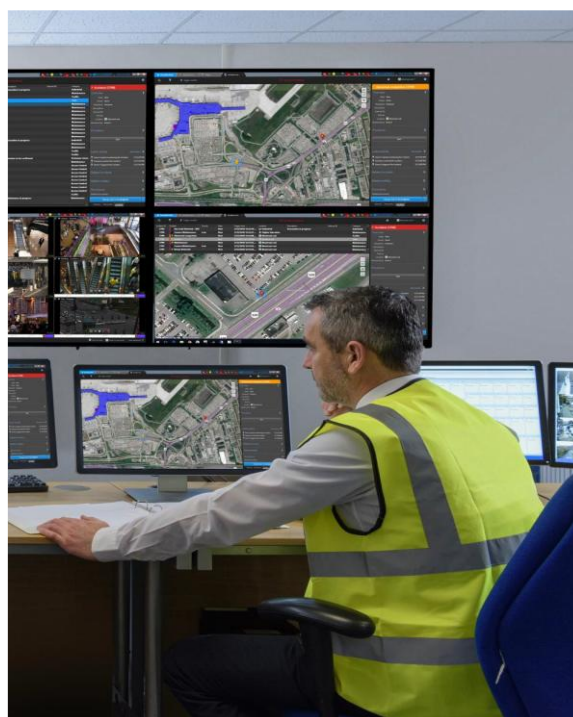
Vizualizare intuitivă și conștientizare situațională. Platforma oferă operatorilor o vizualizare clară și intuitivă a incidentelor și a locațiilor monitorizate, ajutându-i să înțeleagă mai bine contextul și să ia decizii rapide și informate.

MISSION CONTROL

Managementul complet al incidentelor, de la declanșare pînă la audit

Înțelegere clară și vizuală a evenimentelor și locațiilor monitorizate.

Planifică proactiv, ghidează și îmbunătățește activitatea operatorilor



Mission Control oferă un cadru structurat, automatizat și scalabil pentru a răspunde eficient la orice provocare de securitate.

2.2. Alte funcționalități cheie

Modulul Threat Level. Acest modul permite utilizatorilor să gestioneze diferite niveluri de amenințare prin ajustarea automată a comportamentului și setărilor sistemului în funcție de nivelul de risc.

Operatorii pot activa sau dezactiva rapid seturi prestabilite de măsuri de securitate (de exemplu, restricționarea accesului în anumite zone, activarea alertelor automate sau modificarea comportamentului camerelor) în funcție de nivelul de amenințare declarat. Aceasta adaugă flexibilitate și eficiență în situații critice, ajutând organizațiile să își adapteze răspunsul la amenințări în timp real.

Plan Manager Advanced pentru servere de hărți GIS. Plan Manager Advanced oferă capacități avansate de integrare GIS (Sisteme Informaționale Geografice), permițând vizualizarea și gestionarea entităților de securitate direct pe hărți interactive. Acesta suportă un număr nelimitat de entități, precum camere, puncte de acces, și zone de securitate, facilitând localizarea rapidă și monitorizarea într-un context geografic. Acest instrument este extrem de util pentru organizațiile cu infrastructuri complexe, oferind o vizualizare clară și contextualizată a tuturor resurselor și elementelor de infrastructură.

Integrarea cu Active Directory (AD). Integrarea cu Active Directory permite gestionarea centralizată a utilizatorilor și autentificarea bazată pe roluri, folosind informațiile de utilizator și structura organizațională existente în AD. Acest lucru facilitează adăugarea și gestionarea rapidă a utilizatorilor în sistemul de securitate și permite configurarea permisiunilor în funcție de rolul fiecărui utilizator în cadrul organizației.

Active Directory Federation Services connection (ADFS). Această funcționalitate oferă opțiuni de autentificare avansate, permițând utilizatorilor să se autentifice în sistemul Genetec folosind credențialele ADFS. Conexiunea cu ADFS permite autentificarea securizată și accesul unificat între diferite aplicații și servicii, îmbunătățind securitatea și simplificând accesul pentru utilizatorii care fac parte din aceeași rețea federată.

Failover Directory Role. Failover Directory Role asigură redundanță și continuitate operațională în cazul în care serverul principal de director se confruntă cu o defecțiune. Aceasta înseamnă că, dacă serverul primar devine inaccesibil, un server de rezervă preia automat funcțiile, asigurând disponibilitatea continuă a sistemului și prevenind întreruperile în monitorizarea și gestionarea securității.

Genetec™ Advantage. Genetec Advantage este un pachet de suport și mentenanță care oferă acces la actualizări regulate de software, suport tehnic și noi funcționalități. Acesta este un serviciu esențial pentru menținerea performanței și securității platformei pe termen lung, asigurând că sistemul este la zi cu cele mai recente inovații și îmbunătățiri de securitate.



BriefCam reprezintă un element esențial al soluției oferite pentru Platforma Unificată de Securitate, contribuind cu o suită de funcționalități avansate de analiză video care completează platforma Genetec Security Center. Soluția integrată oferă o perspectivă unificatoare asupra tuturor datelor colectate, permițând utilizatorilor să maximizeze valoarea investiției în

supraveghere video printr-o într-un mod extrem de eficient.

BriefCam este o platformă inovatoare de analiză a conținutului video, capabilă să transforme ore întregi de înregistrări în minute, oferind astfel o modalitate rapidă de a căuta, de a extrage informații utile și de a reacționa în fața schimbărilor situaționale critice. Platforma dispune de trei module integrate – REVIEW, RESPOND și RESEARCH – care contribuie fiecare la o gamă largă de funcționalități utile pentru utilizatorii din diferite domenii.

Modulul REVIEW este destinat accelerării investigațiilor și permite utilizatorilor să identifice rapid obiectele și evenimentele de interes, facilitând gestionarea cazurilor prin organizarea înregistrărilor video, marcarea obiectelor de interes și exportarea rapoartelor. Astfel, timpul necesar pentru investigații se reduce semnificativ, iar utilizatorii beneficiază de o vedere de ansamblu asupra incidentelor.

Modulul RESPOND asigură alertare în timp real și contribuie la creșterea gradului de conștientizare situațională. Utilizatorii pot configura reguli complexe de alertare bazate pe clasificarea obiectelor și pot primi notificări în timp real pentru a reacționa prompt la evenimente. Această funcționalitate este integrată cu platforma Genetec Security Center, permițând astfel o colaborare eficientă între toate modulele sistemului de securitate și oferind operatorilor o interfață unificată pentru controlul accesului, supraveghere video și interfoane.

Modulul RESEARCH oferă capabilități de analiză operațională și de business intelligence, generând tablouri de bord personalizabile ce permit identificarea tendințelor de comportament,

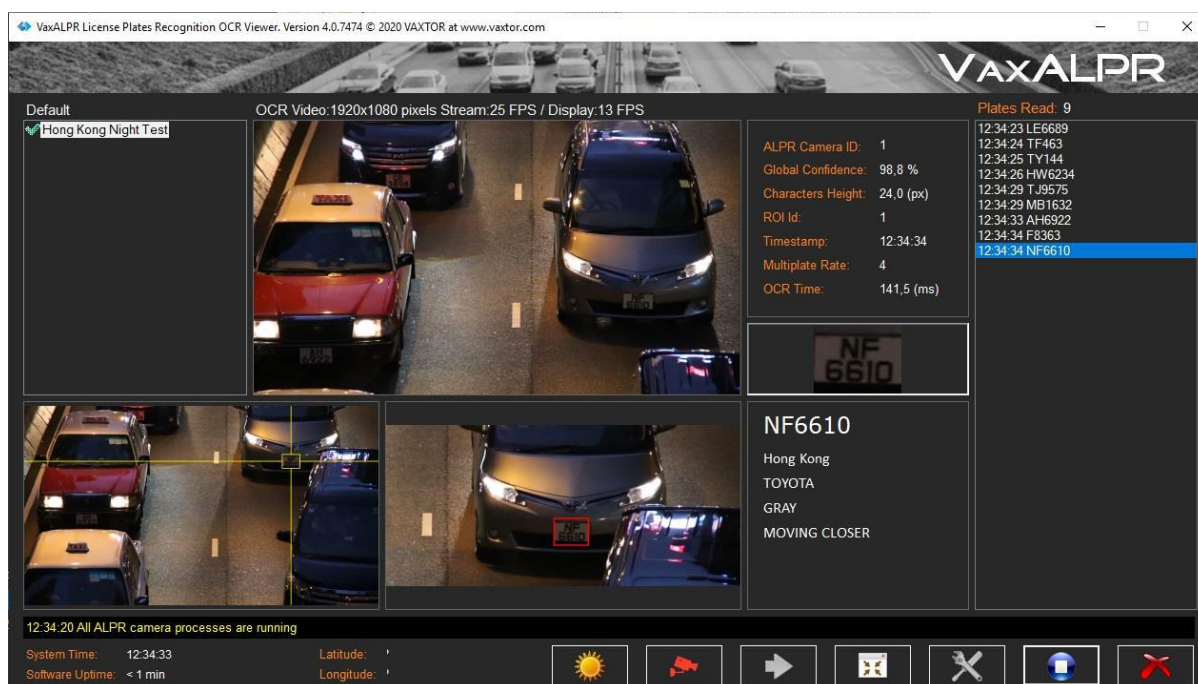
BriefCam se integrează nativ cu Genetec Security Center, asigurând o interoperabilitate perfectă între toate componentele sistemului. Integrarea cu modulul de supraveghere video permite ca alertele generate de BriefCam să fie vizibile în Genetec Security Center, în timp ce datele extrase prin modulele REVIEW și RESEARCH sunt disponibile pentru o vizualizare avansată direct în tablourile de bord din Genetec. Astfel, platforma oferă utilizatorilor o experiență unitară, reducând semnificativ complexitatea operării mai multor sisteme distincte.



Vaxtor reprezintă o soluție avansată de recunoaștere automată a plăcuțelor de înmatriculare (ALPR - Automatic License Plate Recognition), concepută pentru a funcționa într-o gamă largă de scenarii, inclusiv monitorizarea traficului pe autostrăzi, controlul accesului și alte aplicații de securitate critice. Utilizând un motor OCR puternic, Vaxtor poate identifica rapid și precis plăcuțele vehiculelor, indiferent de condițiile de mediu sau viteza acestora.

Vaxtor se integrează perfect cu soluții VMS precum Genetec Security Center, dar și altele, ceea ce permite o interoperabilitate excelentă și utilizarea eficientă a infrastructurilor existente. Soluția permite gestionarea simultană a mai multor fluxuri video și transmite rezultatele în timp real prin diverse protocoale, facilitând astfel integrarea cu alte sisteme de securitate.

Configurarea Vaxtor include module de configurare și suport la distanță, precum și un pachet anual de suport profesional, care asigură acces la suport tehnic dedicat și o platformă de asistență. Prin flexibilitatea operațională și capacitatea de a gestiona multiple fluxuri video simultan, Vaxtor oferă o soluție completă pentru securizarea traficului și a punctelor de acces, răspunzând cerințelor ridicate ale aplicațiilor de securitate moderne.



3. Lista materialelor anexate

În această secțiune, prezentăm lista materialelor anexate care susțin oferta noastră tehnică. Aceste documente includ broșuri și fișe tehnice relevante pentru componentele soluției propuse, precum Genetec Security Center, BriefCam și Vaxtor. Informațiile furnizate vor oferi detalii suplimentare despre capacitățile, integrarea și funcționalitățile fiecărei componente, contribuind astfel la o înțelegere mai profundă a soluției oferite. De asemenea, suntem pregătiți să prezentăm la solicitare și alte materiale care pot clarifica și detalia oferta noastră, asigurând astfel transparență și înțelegere completă a propunerii.

01. Genetec-security-center Brochure	Genetec Datasheets & Brochures
02. EN-Genetec-integration-vs-true-unification	
03. EN-security-center-omnicast-technical-brochure	
04. Synergis-product-technical-brochure	
05. Genetec-mission-control	
06. EN-Genetec-Federation	
07. Red-light-violation-detection	
08. BriefCam Platform Datasheet	BriefCam
09. VALPR-PC-Brochure	VAXTOR
10. Genetec-autovu-license-plate-recognition	Genetec

4. Complanța cu cerințele Caietului de sarcini

Această ofertă tehnică detaliază propunerea noastră pentru implementarea unei platforme unificate de securitate, concepută să susțină modernizarea sistemului de control al traficului rutier. Soluția propusă integrează o gamă completă de funcționalități esențiale pentru monitorizarea și gestionarea eficientă a traficului, având ca prioritate compatibilitatea cu echipamentele și sistemele existente în infrastructura actuală.

Platforma va asigura un nivel înalt de securitate cibernetică, protejând astfel datele și informațiile critice de amenințări externe. Prin utilizarea celor mai recente tehnologii și standarde de securitate, ne propunem să creăm un mediu operativ sigur și fiabil, capabil să răspundă provocărilor contemporane în gestionarea traficului.

Această ofertă evidențiază angajamentul nostru de a oferi o soluție robustă, adaptabilă și de înaltă calitate, care să satisfacă cerințele specificate în caietul de sarcini și să contribuie la îmbunătățirea continuă a gestionării traficului rutier.

4.1 Cerințe față de platforma unificată de securitate

Platforma unificată de securitate propusă este proiectată să servească drept componentă centrală a soluției de modernizare, având responsabilitatea de a agrega, monitoriza și controla toate componentele și modulele funcționale. Aceasta va permite o gestionare centralizată și eficientă a tuturor datelor și evenimentelor colectate din sistem, facilitând astfel o reacție rapidă și coordonată la incidente. Arhitectura modulară a platformei asigură interoperabilitatea cu echipamentele existente, garantând o integrare fluidă și o utilizare optimă a resurselor disponibile.

4.1.1 - Interfața unificată de management și control

Interfața unificată de management și control este un element esențial al platformei integrate, fiind proiectată pentru a asigura gestionarea eficientă a tuturor componentelor sistemului, inclusiv camerele de supraveghere, modulele de analiză și soluțiile de stocare a datelor. Această interfață oferă operatorilor un acces rapid și intuitiv la funcționalitățile critice, permițând monitorizarea în timp real, precum și administrarea și configurarea tuturor resurselor disponibile.

Prin integrarea tuturor elementelor platformei într-un singur panou de control, interfața asigură o experiență de utilizare simplificată, indiferent de complexitatea sau distribuția geografică a sistemului. Aceasta facilitează gestionarea eficientă a evenimentelor, incidentelor și alarmelor generate, oferind operatorilor vizualizări clare și detaliate ale fluxurilor video și rapoartelor generate. Astfel, interfața unificată contribuie la optimizarea procesului de răspuns și la îmbunătățirea coordonării în gestionarea situațiilor critice.

#	Cerință	Obligator	Declarație Ofertant
1.	Platforma Unificată de Securitate (soluția de platformă) trebuie să fie o soluție integrată care să combine într-un singur sistem toate componentele esențiale de securitate. Soluția trebuie să poată asigura centralizarea datelor și a proceselor de securitate relevante.	Da	Conform. Soluția oferată integrează toate componentele esențiale de securitate și asigură centralizarea datelor într-un singur sistem.
2.	Soluția de platformă trebuie să fie <i>Enterprise/Industrial grade</i> , concepută pentru a răspunde nevoilor complexe și variate de securitate, incluzând monitorizarea traficului, siguranța publică și alte domenii conexe.	Da	Conform. Soluția oferată este o platformă Enterprise/Industrial grade, care nu doar asigură funcționalități pentru monitorizarea traficului și siguranța publică, ci și pentru domenii conexe, cum ar fi gestionarea infrastructurii critice, protecția perimetrală, securitatea clădirilor și a campusurilor, transportul public și gestionarea evenimentelor.
3.	Soluția de platformă trebuie să fie scalabilă și flexibilă, permițând adaptarea treptată la cerințele și nevoile specifice, asigurând capacități de integrare eficiente și gestionare centralizată a informațiilor	Da	Conform.
4.	Platforma trebuie să ofere o interfață unificată de gestionare și control care să permită administrarea centralizată a cel puțin următoarelor module funcționale/subsisteme: modulul de gestionare a evenimentelor traficului rutier în baza numerelor de înmatriculare, modulul de gestionare video (VMS), modul de gestionare situațiilor de interes, modul de analiza inteligentă a fluxurilor video.	Da	Conform. Interfața unificată de gestionare și control din Genetec Security Center permite administrarea centralizată a modulelor specificate, dar și a altor sisteme/subsisteme de securitate, cum ar fi controlul accesului, gestionarea alarmelor și protecția perimetrală.
5.	Platforma trebuie să ofere o interfață unificată de gestionare și control care să permită administrarea centralizată suplimentară a cel puțin următoarelor module funcționale/subsisteme: modul de gestionare a dispozitivelor IoT, Controlul Accesului, Controlul Perimetral.	Nu (30 puncte)	Conform. Interfața unificată din Genetec Security Center permite nu doar administrarea centralizată a modulelor de gestionare a dispozitivelor IIoT, control acces și protecție perimetrală, ci și integrarea altor subsisteme de securitate, precum sisteme de intruziune, detecția incendiului, și altele, asigurând o viziune completă și extinsă asupra tuturor componentelor monitorizate.
6.	Platforma trebuie să permită monitorizarea în timp real a tuturor fluxurilor video și datelor capturate, oferind acces rapid și securizat la toate informațiile esențiale într-un singur tablou de bord.	Da	Conform. Platforma Genetec Security Center permite monitorizarea în timp real printr-un tablou de bord centralizat, unde toate fluxurile video și datele capturate sunt integrate și accesibile

			instantaneu. Accesul securizat și rapid este asigurat prin funcții avansate de administrare a utilizatorilor și prin criptarea datelor.
7.	Platforma trebuie să permită utilizatorilor să personalizeze tablourile de bord, permițând configurarea vizualizării datelor în funcție de preferințele și nevoile specifice ale fiecărui operator.	Da	Conform. Genetec Security Center permite utilizatorilor să își personalizeze tablourile de bord, configurând afișarea datelor în funcție de preferințele și cerințele lor specifice, prin funcții de drag-and-drop și widget-uri configurabile.
8.	Platforma trebuie să asigure accesibilitatea tuturor componentelor și modulelor funcționale integrate prin intermediul unei interfețe unificate, oferind operatorilor o vizualizare coerentă și eficientă a datelor și evenimentelor în timp real.	Da	Conform.
9.	Platforma trebuie să includă un sistem de notificări personalizabile, care să alerteze operatorii în caz de incidente critice sau situații de interes	Da	Conform. Genetec Security Center include un sistem de notificări personalizabile, care permite configurarea alertelor pentru incidente critice și situații de interes
10.	Platforma trebuie să permită controlul și dirijarea dispozitivelor de monitorizare video direct din interfața de management, permițând operatorilor să ajusteze unghiul de vizualizare, zoom-ul și focalizarea camerelor în timp real.	Da	Conform. Controlul și dirijarea camerelor sunt realizate prin modulul de gestionare video (VMS) din Genetec Security Center, care permite operatorilor să ajusteze în timp real unghiul de vizualizare, zoom-ul și focalizarea camerelor direct din interfața de management,
11.	Platforma trebuie să ofere suport pentru mai multe limbi, inclusiv Română și Engleză, asigurând astfel accesibilitate pentru toți utilizatorii.	Da	Conform.
12.	Platforma trebuie să includă funcționalități de audit și logare a activităților utilizatorilor, pentru a monitoriza și verifica accesul și acțiunile efectuate în sistem.	Da	Conform.
13.	Platforma trebuie să includă funcționalități de gestionare a alarmelor și incidentelor, permițând monitorizarea, clasificarea și raportarea acestora în timp real, cu opțiunea de escaladare automată către autoritățile competente.	Da	Conform. Genetec Security Center include funcționalități de gestionare a alarmelor și incidentelor prin modulul Security Desk, care permite monitorizarea, clasificarea și raportarea acestora în timp real, cu opțiuni de escaladare automată
14.	Platforma trebuie să permită gestionarea și actualizarea dinamică a drepturilor de acces și a privilegiilor utilizatorilor, cu posibilitatea de a defini roluri specifice în funcție de responsabilitățile fiecărui operator.	Da	Conform. Genetec Security Center permite gestionarea și actualizarea dinamică a drepturilor de acces prin modulul de administrare a utilizatorilor, care oferă posibilitatea de a crea și personaliza roluri specifice
15.	Platforma trebuie să fie compatibilă cu dispozitive mobile, oferind acces securizat la funcționalitățile critice și din afara locațiilor fixe de lucru.	Da	Conform.
16.	Platforma trebuie să permită vizualizarea și gestionarea hărților interactive, oferind localizarea geografică a dispozitivelor, afișarea incidentelor și monitorizarea activităților în funcție de locație.	Da	Conform. Genetec Security Center oferă funcționalități de hărți interactive prin modulul Plan Manager, permițând localizarea dispozitivelor, afișarea în timp real a incidentelor și monitorizarea activităților pe baza locației geografice.
17.	Platforma trebuie să permită actualizarea centralizată a firmware-ului și software-ului pentru dispozitivele conectate.	Da	Conform.

18.	Platforma trebuie să permită configurarea fluxurilor de lucru automatizate, bazate pe scenarii specifice (ex: detectarea vehiculelor de interes sau declanșarea alarmelor de securitate), care să declanșeze acțiuni automate sau notificări.	Da	Conform. Genetec Security Center permite configurarea fluxurilor de lucru automatizate prin modulul de reguli și alerte, declanșând acțiuni automate și notificări în funcție de scenarii specifice
-----	---	----	---

4.1.2 - Cerințe față de interoperabilitate și integrare

#	Cerință	Obligator	
19.	Platforma trebuie să aibă o arhitectură deschisă, care să permită integrarea ușoară cu echipamente și sisteme furnizate de terți (3rd party), inclusiv camere de supraveghere; sisteme de video management; sisteme de control al accesului; soluții de analiză video; sisteme anti-incendiu; alte sisteme/sub-sisteme de securitate și/sau management fluxuri operaționale.	Da	Conform. Genetec Security Center are o arhitectură deschisă, permițând integrarea facilă cu echipamente și sisteme de la terți, inclusiv camere, VMS, soluții de analiză video, sisteme de control acces, anti-incendiu și alte subsisteme de securitate și management operațional.
20.	Platforma trebuie să permită integrarea cu sisteme de supraveghere video existente, inclusiv suport pentru camere IP de la diferiți producători, asigurând compatibilitatea cu echipamentele deja instalate.	Da	Conform. Genetec Security Center permite integrarea cu sisteme de supraveghere video existente, oferind suport extensiv pentru camere IP de la multiple branduri și producători. Platforma este compatibilă cu standardele ONVIF și include drivere pentru o gamă variată de echipamente video
21.	Platforma trebuie să integreze și să gestioneze următoarele echipamente existente, asigurând compatibilitate și operare centralizată: 1. Camere PTZ - DS-2DE4425IW-DET5 - 5 unități; 2. Camere iDS-TCV907-BIR/C – min 25 dispozitive; 3. Camere PTZ - DS-2SE7C432MWG-EB/26(F0) - 15 unități 4. Camere PTZ - DS-2DE7232IW-AE - 13 unități	Da	Conform.
22.	Platforma trebuie să fie compatibilă cu camerele ANPR produse de producători renumiți din industrie, asigurând interoperabilitatea completă și integrarea fără probleme. Aceasta trebuie să includă, dar nu se limitează la, următorii producători: • Axis Communications • Bosch Security Systems • Hanwha Techwin • Motorola Solutions • Sony • Panasonic • Vivotek • Pelco Compatibilitatea trebuie să permită utilizarea tuturor funcționalităților avansate oferite de aceste camere, precum recunoașterea automată a numerelor de înmatriculare, integrarea cu fluxurile video și raportarea incidentelor.	Da	Conform. https://www.genetec.com/supported-device-list
23.	Platforma trebuie să permită integrarea cu sisteme de video management terțe (VMS), control acces și alte soluții de securitate, utilizând protocoale standardizate precum ONVIF, PSIA, RTSP, SIP, HTTPS, TLS, și API-uri REST pentru a asigura	Da	Conform.

	interoperabilitatea și schimbul de date fără întreruperi.		
24.	Platforma trebuie să ofere suport pentru integrarea soluțiilor de recunoaștere facială, ANPR și alte tehnologii avansate de identificare, altele decât cele solicitate, permițând extinderea capacităților de monitorizare și analiză a traficului și securității publice.	Da	Conform. Genetec Security Center permite integrarea soluțiilor de recunoaștere facială și ANPR, inclusiv soluții de la terți, prin modulul AutoVu și API-urile deschise ale platformei, extinzând capacitățile de monitorizare și analiză a traficului și securității publice.
25.	Platforma trebuie să asigure compatibilitatea cu soluțiile de analiză video și management al incidentelor, permițând corelarea datelor din multiple surse și facilitând generarea automată de rapoarte și analize pentru decizii operaționale rapide.	Da	Conform.
26.	Platforma trebuie să suporte integrarea cu sisteme de gestionare a traficului și infrastructurii rutiere, permițând controlul și monitorizarea în timp real a fluxurilor de vehicule, semafoarelor, bariere automate și altor dispozitive de gestionare a traficului.	Da	Conform.
27.	Platforma trebuie să permită integrarea cu soluții de stocare și arhivare terțe, permițând stocarea în siguranță a datelor video și ANPR pe termen lung, cu suport pentru sisteme locale și de tip cloud.	Da	Conform.
28.	Platforma trebuie să suporte integrarea cu sisteme IoT (Internet of Things) pentru a extinde funcționalitățile de monitorizare și control la nivelul dispozitivelor conectate din rețea.	Da	Conform.
29.	Platforma trebuie să suporte integrarea cu protocoale standard de comunicare, cum ar fi Modbus, BACnet, MQTT, OPC și SNMP, pentru a asigura conectivitatea și interoperabilitatea între diverse sisteme.	Da	Conform. Genetec Security Center suportă integrarea prin protocoale standard, inclusiv MQTT, Modbus, BACnet, PC, SNMP, RTSP, HTTPS, TLS și ONVIF, asigurând conectivitate și interoperabilitate între sisteme diverse. Aceste protocoale permit schimbul de date securizat și în timp real, facilitând integrarea eficientă cu echipamentele și sistemele terțe.
30.	Platforma trebuie să suporte integrarea cu soluții de comunicații securizate, inclusiv VoIP, permițând coordonarea rapidă și eficientă a echipelor de intervenție și schimbul de informații în timp real între operatori și autorități.	Da	Conform. Genetec Security Center realizează integrarea cu soluțiile de comunicații securizate, inclusiv VoIP, prin modulul <i>Sipelia™ Communications Management</i> . Acest modul permite gestionarea comunicațiilor VoIP în cadrul platformei,
31.	Platforma trebuie să suporte adăugarea și gestionarea de conectori pentru integrarea soluțiilor terțe, permițând extinderea capacităților sistemului fără modificări majore în infrastructură, asigurând astfel flexibilitate și scalabilitate.	Da	Conform. Genetec Security Center suportă adăugarea și gestionarea de conectori pentru soluții terțe prin <i>Genetec Integration SDK</i> și arhitectura sa modulară, care permit integrarea rapidă și flexibilă a unor noi soluții fără modificări majore în infrastructură.
32.	Platforma trebuie să suporte integrarea cu soluții terțe de reprezentare geografică (GIS MAP), cel puțin cu ArcGIS, Google, BING, OpenStreetMap.	Nu (15 puncte)	Conform. Soluția oferită suportă integrarea cu soluții terțe de reprezentare geografică (GIS), inclusiv ArcGIS, Google Maps, Bing Maps și OpenStreetMap, prin modulul <i>Plan Manager</i> . Acesta permite utilizatorilor să acceseze și să gestioneze hărți interactive din diverse surse GIS.
33.	Platforma trebuie să suporte importul și exportul de date între sisteme terțe, asigurând	Da	Conform.

	interoperabilitatea și sincronizarea continuă a datelor critice pentru monitorizare și analiză.		
34.	Platforma trebuie să suporte integrarea cu soluții de automatizare și machine learning pentru analiza predictivă, permițând dezvoltarea de soluții personalizate și extinderea funcționalităților în funcție de nevoile organizației.	Da	Conform.
35.	Platforma trebuie să permită implementarea și gestionarea mecanismelor de autentificare puternică, compatibile cu standardele OpenID Connect și SAML 2.0, asigurând că toate comunicările între utilizatori și sistem sunt autentificate și protejate corespunzător.	Da	Conform.
36.	Platforma trebuie să sprijine utilizarea discurilor NAS, PC-uri și alte echipamente de stocare din rețele LAN/WAN, oferind suport pentru arhivarea flexibilă a fluxurilor video și datelor colectate într-un mediu distribuit, fără dependențe de soluții proprietare.	Da	Conform.
37.	Platforma trebuie să fie compatibilă cu standardele de criptare și protecție a datelor, asigurând confidențialitatea și integritatea datelor transmise și stocate, folosind metode de criptare de nivel înalt, cum ar fi AES-256 pentru datele stocate și TLS pentru datele transmise	Da	Conform.
38.	Platforma trebuie să sprijine utilizarea de echipamente și infrastructuri de rețea non-propietare, oferind suport pentru switch-uri, servere și alte componente de la diferiți furnizori, asigurând o soluție scalabilă și flexibilă, fără constrângeri legate de furnizorii de echipamente.	Da	Conform. Soluția oferată realizează integrarea cu echipamente și infrastructuri de rețea non-propietare prin utilizarea protocoalelor standardizate de comunicație
39.	Platforma trebuie să permită actualizarea și extinderea facilă a funcționalităților și componentelor, permițând adaptarea la nevoile viitoare ale infrastructurii de securitate, fără a fi necesare modificări semnificative ale arhitecturii sau echipamentelor existente.	Da	Conform. Soluția oferată permite actualizarea și extinderea funcționalităților printr-o arhitectură modulară, care facilitează integrarea de noi module și aplicații.
40.	Platforma trebuie să sprijine utilizarea de servere și stații de lucru conforme cu specificațiile de securitate impuse de standardele internaționale, asigurând că toate componentele hardware respectă cerințele de protecție și integritate impuse de normele de securitate cibernetică.	Da	Conform.

4.1.3 - Monitorizarea și raportarea în timp real

#	Cerință	Obligator	
41.	Platforma trebuie să permită monitorizarea și raportarea în timp real a datelor și evenimentelor colectate de la dispozitivele de monitorizare video, senzori de notificare/alarmare; precum și de la alte echipamente integrate.	Da	Conform. Soluția oferată permite centralizarea informațiilor colectate de la dispozitivele de monitorizare video și senzori de notificare/alarmare, asigurând vizualizarea instantanee a evenimentelor și generarea de rapoarte detaliate pentru o reacție rapidă și informată
42.	Platforma trebuie să includă funcționalități de raportare în timp real a evenimentelor critice, permițând operatorilor să seteze niveluri de prioritate pentru notificări și	Da	Conform. Soluția oferată facilitează raportarea în timp real a evenimentelor critice prin intermediul modului <i>Event Management</i> , care permite operatorilor să definească parametrii de

	alerte, astfel încât incidentele importante să fie gestionate eficient.		alertare personalizabili. Acest modul oferă opțiuni pentru setarea nivelurilor de prioritate pentru notificări, astfel încât alertele pentru incidentele importante să fie accentuate și gestionate eficient.
43.	Platforma trebuie să includă funcționalități de diagnosticare a stării de sănătate a sistemului, oferind informații detaliate despre funcționarea optimă a tuturor componentelor.	Da	Conform.
44.	Platforma trebuie să permită generarea de rapoarte personalizabile, care să includă grafice, diagrame și statistici privind activitatea din trafic și starea sistemului.	Da	Conform.
45.	Platforma trebuie să permită vizualizarea în timp real a fluxurilor video multiple pe ecrane dedicate, oferind operatorilor capacitatea de a monitoriza simultan mai multe locații, cu posibilitatea de a comuta între fluxuri video și de a ajusta setările de afișare	Da	Conform. Soluția oferată permite vizualizarea în timp real a fluxurilor video multiple prin intermediul modulului <i>Omnicast</i> . Acest modul oferă operatorilor capacitatea de a monitoriza simultan mai multe locații pe ecrane dedicate, permițând comutarea rapidă între diferitele fluxuri video. Operatorii pot ajusta setările de afișare, cum ar fi dimensiunea și aranjamentul ferestrelor video, pentru a personaliza experiența de monitorizare în funcție de nevoile operaționale specifice
46.	Platforma trebuie să includă funcționalități de căutare avansată în arhivele video, permițând identificarea rapidă a incidentelor pe baza unor criterii predefinite (de ex., ora, locația, tipul incidentului).	Da	Conform. Soluția oferată include funcționalități de căutare avansată în arhivele video prin intermediul modulului <i>Video Analytics</i> . Acest modul permite operatorilor să identifice rapid incidentele pe baza unor criterii predefinite, precum ora, locația și tipul incidentului.
47.	Platforma trebuie să permită operatorilor să configureze și să monitorizeze simultan multiple fluxuri video pe ecrane dedicate, asigurând astfel o supraveghere eficientă și continuă.	Da	Conform. <i>Omnicast</i> asigură afișarea fluxurilor video pe ecrane dedicate, oferind flexibilitate în gestionarea aranjamentului ecranelor și a setărilor de afișare
48.	Platforma trebuie să suporte crearea și gestionarea incidentelor în timp real, permițând înregistrarea și urmărirea fiecărui incident până la rezolvarea acestuia.	Da	Conform. Soluția oferată permite crearea și gestionarea incidentelor în timp real prin intermediul modulului <i>Incident Management</i> . Acest modul permite operatorilor să înregistreze, să clasifice și să urmărească fiecare incident până la rezolvarea sa
49.	Platforma trebuie să permită partajarea rapidă a informațiilor și a înregistrărilor video cu alte agenții sau autorități relevante, asigurând astfel o coordonare eficientă în caz de incidente majore.	Da	Conform. Soluția oferată permite partajarea rapidă a informațiilor și a înregistrărilor video cu alte agenții sau autorități relevante prin intermediul modulului <i>Secure Sharing</i> . Acest modul asigură un transfer securizat și eficient al datelor
50.	Platforma trebuie să permită funcționalități de export și distribuire a rapoartelor și datelor critice, permițând generarea rapidă a dosarelor de incident și transmiterea acestora în formate standardizate (PDF, CSV) pentru analiză ulterioară.	Da	Conform. Modulul Reporting and Analytics din Genetec Security Center, facilitează generarea rapidă a dosarelor de incident. Acesta oferă opțiuni pentru a exporta informațiile în formate standardizate, cum ar fi PDF și CSV
51.	Platforma trebuie să includă capacități de vizualizare a datelor în format geografic, permițând supravegherea vizuală a incidentelor și activităților pe hărți	Da	Conform. <i>Plan Manager</i> din Genetec Security Center include capacități de vizualizare a datelor în format geografic, permițând supravegherea

	interactive, cu opțiuni de filtrare pe baza locației sau a altor parametri specifici.		vizuală a incidentelor și activităților pe hărți interactive.
52.	Platforma poate să includă funcționalități de monitorizare stare entități (camere video, camere ANPR fixe și mobile, dispozitive IoT, etc.) pe hartă și să permită personalizarea acestora.	Nu (20 puncte)	Conform. Soluția oferată realizează monitorizarea stării entităților prin integrarea modulului <i>Plan Manager</i> , care permite afișarea pe hărți interactive a camerelor video, camerelor ANPR și dispozitivelor IoT. Aceasta se bazează pe fluxuri de date în timp real de la aceste dispozitive, care sunt colectate și procesate pentru a reflecta starea lor curentă pe hartă. Utilizatorii pot personaliza vizualizarea acestor entități prin setarea simbolurilor, culorilor și informațiilor afișate, ceea ce ajută la gestionarea eficientă a resurselor și la identificarea rapidă a eventualelor probleme de operare.
53.	Platforma poate să includă funcționalități de accesare fluxurilor video direct din interfața de reprezentare geografică.	Nu (10 puncte)	Conform. Soluția oferată include funcționalități de accesare a fluxurilor video direct din interfața de reprezentare geografică. Aceasta permite operatorilor să vizualizeze în timp real fluxurile video asociate entităților de pe hartă. Funcționalitățile de accesare a fluxurilor video direct din interfața de reprezentare geografică sunt realizate prin integrarea modulelor de gestionare video cu un sistem de informații geospațiale (GIS). În această configurație, Genetec Security Center servește drept platformă centralizată, care permite operatorilor să vizualizeze și să gestioneze camerele de supraveghere pe o hartă interactivă. Prin utilizarea modulului Omnicast pentru managementul video, operatorii pot accesa fluxurile video asociate fiecărei locații geografice specificate pe hartă. Interfața geografică oferă un mod intuitiv de a localiza rapid camerele și de a vizualiza fluxurile video corespunzătoare, facilitând astfel reacția rapidă în situații de urgență.
54.	Platforma trebuie să permită integrarea cu soluții de raportare și analiză predictivă, permițând generarea de analize detaliate care să identifice tipare și să ofere predicții despre tendințele traficului și incidentele viitoare.	Da	Conform.
55.	Platforma trebuie să permită personalizarea rapoartelor și a notificărilor în funcție de utilizator sau rol, asigurând că operatorii primesc doar informațiile relevante pentru activitatea lor, evitând astfel supraîncărcarea cu date neesențiale.	Da	Conform. Soluția oferată permite personalizarea rapoartelor și a notificărilor în funcție de utilizator sau rol prin intermediul modulului <i>User Management</i> . Acesta permite administratorilor să configureze setările de notificare și să personalizeze formatele rapoartelor

4.2 Cerințe față de arhitectura

Arhitectura platformei este concepută pentru a permite integrarea eficientă cu sisteme și soluții existente sau viitoare, asigurând compatibilitate între diverse tehnologii. Aceasta se bazează pe un model modular care facilitează adăugarea rapidă a componentelor noi, fără a afecta funcționalitatea sistemului existent.

Platforma va avea capacitatea de a scala în funcție de cerințele operaționale, permițând extinderea resurselor hardware și software în mod dinamic. De asemenea, va utiliza standarde deschise și API-uri pentru a facilita integrarea cu aplicații externe și pentru a permite interoperabilitatea între diferite soluții.

Funcționalitățile arhitecturale vor include gestionarea centralizată a datelor și a proceselor, asigurând astfel acces rapid la informații și facilitând analiza acestora în timp real. De asemenea, platforma va integra protocoale de securitate avansate, inclusiv criptarea datelor și autentificarea utilizatorilor, pentru a proteja informațiile sensibile și a asigura o operare sigură.

4.2.1 Arhitectura deschisă și modulară

#	Cerință	Obligator	
56.	Platforma trebuie să fie construită pe o arhitectură deschisă și modulară, care să permită adăugarea și eliminarea de componente fără a afecta funcționarea generală a sistemului.	Da	Conform.
57.	Platforma trebuie să fie posibil de instalat local (on-premises) pe infrastructura de procesare asigurată de beneficiar, fie că aceasta constă în servere fizice sau mașini virtuale.	Da	Conform. Soluția oferată poate fi instalată local (on-premises) pe infrastructura de procesare asigurată de beneficiar, fie că aceasta constă în servere fizice sau mașini virtuale.
58.	Platforma trebuie să permită integrarea cu diverse tipuri de servere, soluții de stocare și echipamente de rețea, fără a necesita hardware proprietar, asigurând astfel flexibilitate în implementare și costuri reduse.	Da	Conform.
59.	Platforma trebuie să fie compatibilă cu soluțiile de virtualizare (ex. VMware, Hyper-V) și să permită rularea eficientă a componentelor sale în medii virtualizate sau cloud.	Da	Conform.
60.	Platforma trebuie să sprijine o arhitectură de tip microservicii, permițând distribuirea sarcinilor de procesare și reducerea dependențelor între diferitele module.	Da	Conform.
61.	Platforma trebuie să permită integrarea de noi funcționalități și module software prin intermediul API-urilor deschise și standardizate, asigurând astfel extinderea capacităților fără întreruperi.	Da	Conform.
62.	Platforma trebuie să ofere interfața de comunicare standardizată (ex. RESTful API) pentru a facilita integrarea cu diverse sisteme terțe și pentru a permite interoperabilitatea între soluții diferite.	Da	Conform.
63.	Platforma trebuie să permită configurarea și gestionarea centralizată a tuturor componentelor sale, printr-o interfață unică de administrare, care să ofere acces la toate funcționalitățile necesare pentru operare și mentenanță.	Da	Conform. Soluția oferată permite configurarea și gestionarea centralizată a tuturor componentelor prin intermediul unei interfețe unice de administrare, numită <i>Security Center Unified Interface</i> .

4.2.2 Implementare distribuită

#	Cerință	Obligator	
64.	Platforma trebuie să sprijine o arhitectură distribuită, în care componentele software și	Da	Conform.

	hardware pot fi amplasate în locații geografice diferite, asigurând o operare eficientă și sincronizată în timp real, indiferent de distanțe.		
65.	Platforma trebuie să sprijine distribuirea sarcinilor de procesare și stocare între site-uri diferite, asigurând echilibrul sarcinilor și evitarea suprasolicitării unor locații specifice.	Da	Conform.
66.	Platforma trebuie să permită gestionarea centralizată a tuturor componentelor distribuite, oferind o interfață unică pentru administrarea și monitorizarea întregii rețele.	Da	Conform. Soluția oferată sprijină gestionarea centralizată a tuturor componentelor distribuite prin intermediul caracteristicii <i>Security Center Federation™</i> . Aceasta permite administrarea și monitorizarea în timp real a site-urilor multiple într-o singură interfață unificată, asigurând o vizualizare globală a evenimentelor și alarmei, indiferent de locația fizică a componentelor distribuite
67.	Platforma trebuie să permită sincronizarea automată a datelor și evenimentelor între toate locațiile, asigurând că informațiile sunt actualizate și accesibile în timp real în orice locație conectată.	Da	Conform.
68.	Platforma trebuie să asigure continuitatea operațională în toate locațiile prin implementarea de mecanisme de failover distribuite, care să permită preluarea automată a sarcinilor în cazul unei defecțiuni locale.	Da	Conform. Soluția oferată asigură sincronizarea automată a datelor și evenimentelor între locații prin intermediul funcției <i>Federation™</i> din Genetec Security Center, care permite monitorizarea și gestionarea centralizată a mai multor site-uri în timp real.
69.	Platforma trebuie să ofere suport pentru configurarea unui sistem de disponibilitate ridicată (HA), asigurând că serviciile critice sunt replicate și disponibile fără întreruperi în caz de defecțiuni hardware sau software.	Da	Conform.
70.	Platforma trebuie să permită extinderea facilă a infrastructurii distribuite prin adăugarea de cel puțin 10 site-uri noi (locații) și resurse, fără a afecta performanța globală a sistemului.	Da	Conform.
71.	Platforma trebuie să suporte extinderea facilă a infrastructurii distribuite prin adăugarea de cel puțin 20 site-uri noi (locații) și resurse, fără a afecta performanța globală a sistemului.	Nu (10 puncte)	Conform. Soluția oferată permite extinderea facilă a infrastructurii distribuite prin adăugarea de cel puțin 20 de site-uri noi, fără limită superioară, folosind arhitectura modulară și funcționalitatea <i>Federation</i> din Genetec Security Center.
72.	Platforma trebuie să ofere mecanisme de unificare a datelor și evenimentelor, permițând agregarea acestora din multiple locații într-o platformă unificată de management.	Da	Conform.
73.	Platforma trebuie să asigure un model de operare distribuit, în care fiecare site poate funcționa independent, dar toate datele și evenimentele să fie centralizate și disponibile pentru vizualizare și analiză în timp real.	Da	Conform. Soluția oferată asigură un model de operare distribuit prin funcționalitatea <i>Federation™</i> , care permite fiecărui site să funcționeze independent, menținând în același timp centralizarea datelor și evenimentelor.
74.	Platforma trebuie să permită configurarea de politici de acces diferențiate pentru fiecare locație, asigurând un control granular al permisiunilor și accesului la datele distribuite.	Da	Conform. Soluția oferată permite configurarea de politici de acces diferențiate pentru fiecare locație prin modulul de <i>User Management</i> din Genetec Security Center.

75.	Platforma trebuie să permită administrarea descentralizată a site-urilor, oferind posibilitatea configurării și gestionării locale a componentelor, dar cu raportarea și agregarea datelor la nivel central.	Da	Conform.
76.	Platforma trebuie să sprijine monitorizarea centralizată a performanței și securității tuturor locațiilor distribuite, cu generarea de rapoarte unificate care să includă date din toate site-urile conectate.	Da	Conform.
77.	Platforma trebuie să asigure un flux de date sigur și optimizat între toate locațiile, minimizând latențele și asigurând integritatea și confidențialitatea informațiilor transmise.	Da	Conform.
78.	Platforma trebuie să sprijine configurarea dinamică a resurselor, permițând ajustarea automată a alocării resurselor în funcție de nevoile fiecărei locații și de volumul de date procesat.	Da	Conform.
79.	Platforma trebuie să asigure compatibilitatea cu diverse topologii de rețea și configurații de conectivitate, permițând implementarea sa în medii variate, de la centre urbane la locații izolate.	Da	Conform.

4.2.3 Cerințe de securitate

#	Cerință	Obligator	
80.	Platforma trebuie să asigure criptarea tuturor comunicațiilor între componentele sistemului, utilizând protocoale de securitate avansate (ex. TLS) pentru a preveni interceptarea datelor.	Da	Conform. Soluția oferată asigură criptarea tuturor comunicațiilor între componentele sistemului folosind protocoale de securitate avansate, inclusiv TLS și SRTP.
81.	Platforma trebuie să sprijine autentificarea utilizatorilor și dispozitivelor conectate prin metode sigure, cum ar fi autentificarea multi-factor (MFA) și certificarea digitală.	Da	Conform.
82.	Platforma trebuie să includă un mecanism centralizat de jurnalizare, care să înregistreze toate acțiunile utilizatorilor și evenimentele critice, incluzând accesările, modificările de configurare, incidentele de securitate și alertele generate. Platforma trebuie să permită generarea de jurnale detaliate pentru fiecare subsistem integrat, oferind informații despre momentul, utilizatorul, acțiunea și rezultatul fiecărui eveniment. Platforma trebuie să includă un mecanism de audit automat, care să monitorizeze activitățile administratorilor și utilizatorilor cu privilegii ridicate, pentru a detecta orice tentativă de acces neautorizat sau abuz. Platforma trebuie să permită exportul și stocarea jurnale de audit și activitate într-un format standardizat (de exemplu, JSON, XML, CSV) pentru analiză externă și raportare. Platforma trebuie să permită integrarea cu soluții externe de jurnalizare și audit, inclusiv cu platforma guvernamentală de jurnalizare MLog, asigurând conformitatea cu cadrul normativ.	Da	Conform. Soluția oferată include un mecanism centralizat de jurnalizare și auditare, care înregistrează toate acțiunile utilizatorilor și evenimentele critice prin funcția <i>Audit trails</i> din Genetec Security Center. Acest mecanism permite înregistrarea detaliată a accesărilor, modificărilor de configurare și incidentelor de securitate, cu opțiuni de export în formate standardizate (JSON, XML, CSV) pentru analiză externă. De asemenea, platforma suportă integrarea cu soluții externe de jurnalizare, inclusiv soluții SIEM, și oferă capacități de alertare automată pentru detectarea activităților anormale

	Platforma trebuie să ofere un sistem de alertare automată bazat pe reguli personalizabile, care să notifice administratorii în cazul detectării unor activități anormale sau încercări de acces neautorizat în jurnalele de audit. Platforma trebuie să ofere suport pentru jurnalizarea externă către soluții SIEM (Security Information and Event Management) prin protocoale standard, pentru corelarea și analizarea evenimentelor de securitate la nivel enterprise.		
83.	Platforma trebuie să permită configurarea de politici de acces diferențiate, oferind control granular asupra permisiunilor și privilegiilor utilizatorilor în funcție de rolurile acestora.	Da	Conform.
84.	Platforma trebuie să asigure protecția împotriva atacurilor cibernetice în scop de detectare și prevenire a intruziunilor.	Da	Conform.
85.	Platforma trebuie să sprijine segmentarea rețelei și izolarea componentelor critice, minimizând riscul de propagare a amenințărilor în cazul unei breșe de securitate.	Da	Conform.
86.	Platforma trebuie să asigure compatibilitatea cu standardele internaționale de securitate cibernetică (ex. ISO/IEC 27001, NIS) și să permită integrarea cu soluții de management al conformității.	Da	Conform. Soluția oferită este compatibilă cu standardele ISO/IEC 27001, NIS, GDPR, SOC 2 și CJIS.
87.	Platforma trebuie să permită criptarea automată a fluxurilor media (video, audio, metadata) atât în tranzit, cât și în repaus, asigurând protecția datelor sensibile împotriva accesului neautorizat, fără a compromite performanța sistemului.	Da	Conform.
88.	Platforma trebuie să sprijine setarea criptării la nivel de cameră, permițând operatorilor să configureze criptarea individuală pentru fiecare dispozitiv, asigurând astfel o protecție suplimentară pentru fluxurile video și alte date transmise de camerele de supraveghere.	Da	Conform. Genetec Security Center permite setarea criptării la nivel de cameră prin modulul Omnicast, oferind opțiuni de configurare individuală a criptării pentru fiecare dispozitiv conectat. Operatorii pot activa criptarea direct din interfața de administrare Omnicast, asigurând astfel protecția fluxurilor video și a datelor transmise de camere, fără a compromite performanța sistemului.
89.	Platforma trebuie să utilizeze chei de criptare generate aleatoriu, care să fie rotite periodic pentru a preveni atacurile de tip replay și pentru a asigura protecția pe termen lung a datelor.	Da	Conform. Genetec Security Center utilizează chei de criptare generate aleatoriu, cu funcționalități de rotire periodică, gestionate prin modulul de securitate a datelor. Acest proces asigură protecția pe termen lung a datelor și previne atacurile de tip replay,
90.	Platforma trebuie să permită managementul centralizat al cheilor de criptare, oferind administratorilor control complet asupra generării, distribuției și rotației cheilor, pentru a gestiona eficient securitatea criptografică a platformei.	Da	Conform. Genetec Security Center permite managementul centralizat al cheilor de criptare prin modulul său de administrare a securității, oferind control complet asupra generării, distribuției și rotației cheilor.
91.	Platforma trebuie să dețină certificări recunoscute internațional, cum ar fi certificarea CSPN de la ANSSI și certificarea DHS Safety Act, pentru a demonstra robustețea și rezistența la atacuri cibernetice, sau analogice.	Da	Conform. Genetec Security Center este certificat CSPN de către ANSSI și deține certificarea DHS Safety Act, demonstrând conformitatea cu standardele de securitate recunoscute internațional. În plus, platforma beneficiază de certificări precum FIPS 140-2 pentru criptografie și ISO/IEC 27001 pentru

			managementul securității informațiilor, oferind un nivel ridicat de robustețe și rezistență la atacuri cibernetice și amenințări fizice.
92.	Platforma trebuie să fie conformă cu legislațiile naționale și internaționale privind protecția datelor, asigurând respectarea reglementărilor aplicabile, cum ar fi GDPR.	Da	Conform. Genetec Security Center respectă reglementările naționale și internaționale privind protecția datelor, inclusiv conformitatea cu GDPR.
93.	Platforma trebuie să includă un modul de conformitate integrat, care să monitorizeze continuu starea sistemului și să genereze alerte în cazul unor neconformități detectate.	Da	Conform. Soluția oferită include un modul de conformitate integrat, denumit System Health Monitoring, care monitorizează continuu starea sistemului și emite alerte automate în caz de neconformități.
94.	Platforma trebuie să suporte mecanisme de audit și raportare, care să permită verificarea conformității cu standardele și reglementările de securitate aplicabile.	Da	Conform. Soluția oferită suportă mecanisme de audit și raportare prin module dedicate, care permit verificarea conformității cu standardele și reglementările de securitate aplicabile.
95.	Platforma trebuie să permită autentificarea utilizând protocoale moderne, inclusiv să fie integrată cu MPASS, asigurând un acces sigur și controlat la sistem.	Da	Conform.
96.	Platforma trebuie să permită definirea drepturilor și privilegiilor utilizatorilor, oferind un control detaliat asupra accesului la funcționalitățile platformei.	Da	Conform.
97.	Platforma trebuie să integreze soluții de management al identității și accesului (IAM), oferind o experiență de utilizare sigură și eficientă.	Da	Conform. Soluția oferită integrează soluții de management al identității și accesului (IAM) prin modulul de administrare a utilizatorilor, care permite autentificarea securizată și alocarea rolurilor personalizate. Platforma oferă opțiuni de autentificare multifactor și suport pentru integrarea cu sisteme IAM externe,
98.	Platforma trebuie să permită gestionarea centralizată a drepturilor și privilegiilor, oferind administratorilor capacitatea de a defini și revizui periodic accesul utilizatorilor.	Da	Conform.
99.	Platforma trebuie să includă funcționalități de audit și raportare a autentificărilor și activităților utilizatorilor, pentru a monitoriza și documenta accesul în sistem.	Da	Conform.
100.	Platforma trebuie să fie capabilă să detecteze și să prevină tentativele de acces neautorizat, declanșând alerte și blocând automat accesul în cazul unor activități suspecte.	Da	Conform.

4.2.4 Suport pentru extensii și inovație

#	Cerință	Obligator	
101.	Platforma trebuie să fie proiectată pe o arhitectură modulară, permițând adăugarea sau eliminarea de funcționalități și module fără a afecta stabilitatea și performanța sistemului.	Da	Conform. Soluția oferită este construită pe o arhitectură modulară, care permite ca fiecare componentă să fie gestionată independent prin module funcționale autonome. Această structură modulară asigură că adăugarea sau eliminarea de funcționalități și module nu afectează stabilitatea sistemului, datorită designului său de tip „plug-and-play” și mecanismelor integrate de gestionare a resurselor.

102.	Platforma trebuie să suporte dezvoltarea și integrarea rapidă a modulelor suplimentare, permițând extinderea capacităților sale în funcție de cerințele operaționale și tehnologice emergente.	Da	Conform. Soluția oferată suportă dezvoltarea și integrarea rapidă a modulelor suplimentare printr-o arhitectură deschisă și utilizarea SDK-urilor și API-urilor standardizate.
103.	Platforma trebuie să suporte implementarea de soluții personalizate pentru diferite scenarii de utilizare, asigurând flexibilitatea necesară pentru a răspunde cerințelor specifice ale fiecărei locații sau operațiuni.	Da	Conform.
104.	Platforma trebuie să ofere suport pentru API-uri deschise și standardizate, facilitând integrarea cu alte soluții software și hardware, precum și cu platforme terțe de securitate și monitorizare.	Da	Conform.
105.	Platforma trebuie să sprijine actualizările continue ale modulelor existente, asigurând compatibilitatea retroactivă și minimizând impactul asupra serviciilor în timpul procesului de upgrade.	Da	Conform.
106.	Platforma trebuie să fie compatibilă cu cele mai recente tehnologii de inteligență artificială (AI) și machine learning (ML), permițând implementarea de soluții avansate de analiză și predicție.	Da	Conform. Soluția oferată este compatibilă cu tehnologiile avansate de inteligență artificială (AI) și machine learning (ML), permițând implementarea de soluții avansate de analiză și predicție.
107.	Platforma trebuie să ofere suport pentru dezvoltarea și integrarea de soluții de automatizare a proceselor, reducând nevoia de intervenție manuală și îmbunătățind eficiența operațională.	Da	Conform.
108.	Platforma trebuie să sprijine integrarea de tehnologii emergente, cum ar fi realitatea augmentată (AR) și realitatea virtuală (VR), pentru a extinde capacitățile de vizualizare și monitorizare în timp real.	Nu (20 puncte)	Conform. Soluția oferată permite integrarea cu tehnologii emergente, inclusiv AR și VR, folosind API-uri și SDK-uri deschise pe care soluția le oferă. De exemplu, integrarea Genetec Security Center cu soluții VR precum Headwall's Granite Security Ops Center oferă un mediu virtual pentru vizualizarea și controlul sistemului de securitate
109.	Platforma trebuie să suporte dezvoltarea și implementarea de algoritmi personalizați pentru analiza datelor, oferind posibilitatea de a optimiza soluțiile de securitate și monitorizare în funcție de nevoile lor specifice.	Da	Conform.
110.	Platforma trebuie să sprijine inovarea continuă prin integrarea facilă a noilor tehnologii și soluții, asigurând astfel că beneficiarul rămâne la curent cu cele mai recente dezvoltări din domeniul securității și monitorizării.	Da	Conform.
111.	Platforma trebuie să suporte integrarea cu platforme cloud și de edge computing, oferind flexibilitate în gestionarea resurselor și scalarea capacităților în funcție de cerințele operaționale.	Da	Conform. Soluția oferată suportă integrarea cu platforme cloud și de edge computing, permițând flexibilitate în gestionarea resurselor și scalarea capacităților în funcție de cerințele operaționale. Genetec Security Center este compatibil cu furnizori de cloud public și privat
112.	Platforma trebuie să suporte integrarea cu soluții de Internet of Things (IoT).	Da	Conform. Soluția oferată suportă integrarea cu soluții de Internet of Things (IoT)
113.	Platforma trebuie să permită gestionarea flexibilă a ciclului de viață al modulelor și	Da	Conform.

	funcționalităților, permițând upgrade-uri și actualizări iterative în funcție de cerințele operaționale și de securitate.		
--	---	--	--

4.3 Evaluarea Performanței și Scalabilității

Această platformă de securitate este proiectată pentru a oferi performanțe constante în gestionarea volumului crescând de date și a cerințelor operaționale. Arhitectura sa modulară permite scalarea ușoară a resurselor hardware și software, asigurându-se că sistemul poate răspunde eficient la creșterea numărului de utilizatori și la variațiile în fluxurile de date.

Platforma va implementa tehnici avansate de optimizare a performanței, inclusiv caching, load balancing și procese de indexare eficientă, pentru a asigura acces rapid la datele critice și pentru a minimiza timpii de răspuns în timpul operațiunilor. De asemenea, va fi capabilă să gestioneze simultan un număr mare de fluxuri video și evenimente, fără a compromite calitatea serviciilor oferite.

Prin aceste caracteristici tehnice, platforma se va adapta dinamic la cerințele operaționale în continuă schimbare, asigurându-se că poate susține o expansiune viitoare fără pierderi de performanță.

4.3.1 Scalabilitatea Sistemului

#	Cerință	Obligator	
114.	Platforma trebuie să permită extinderea de la 500 la cel puțin 5000 de camere prin adăugarea de resurse de procesare și licențe, fără necesitatea înlocuirii infrastructurii hardware existente.	Da	Conform. Soluția oferată, prin Genetec Security Center Base Enterprise Package, permite extinderea numărului de camere de la 500 până la 5000 prin adăugarea de licențe suplimentare și resurse de procesare.
115.	Platforma trebuie să permită extinderea de la 500 la cel puțin 20 000 de camere prin adăugarea de resurse de procesare și licențe, fără necesitatea înlocuirii infrastructurii hardware existente.	Nu (10 puncte)	Conform. Genetec oferă scalabilitate nelimitată pentru numărul de camere având referințe din diferite verticale de activitate, precum retail, în care numărul de dispozitive conectate depășește 200.000. (Lanțul de magazine Target)
116.	Platforma trebuie să fie proiectată pentru a fi non-hardware dependentă, permițând integrarea și operarea eficientă pe diverse tipuri de servere, dispozitive de stocare și echipamente de rețea, inclusiv cele existente.	Da	Conform. Genetec Security Center suportă operarea pe platforme hardware variate și virtualizare
117.	Platforma trebuie să sprijine extinderea prin adăugarea de noi locații și echipamente într-un mod modular, permițând implementarea progresivă și fără întreruperi a noilor resurse.	Da	Conform. Genetec Security Center sprijină o arhitectură modulară, care permite adăugarea de noi locații și echipamente în mod progresiv
118.	Platforma trebuie să permită gestionarea centralizată a tuturor site-urilor și camerelor conectate printr-o singură interfață de management, asigurând o vizualizare unificată și coerentă a întregului sistem.	Da	Conform.
119.	Platforma trebuie să sprijine un model de implementare multi-site, permițând agregarea datelor și evenimentelor din multiple locații într-o platformă unificată, similar conceptului de federalizare.	Da	Conform.
120.	Platforma trebuie să permită distribuirea sarcinilor de procesare între multiple servere și locații, asigurând o performanță optimă și un timp de răspuns minim, indiferent de numărul de camere conectate.	Da	Conform.

121.	Platforma trebuie să sprijine integrarea cu sisteme terțe și tehnologii emergente, permițând extinderea capabilităților și funcționalităților fără constrângeri de compatibilitate.	Da	Conform.
122.	Platforma trebuie să permită adăugarea de noi funcționalități și module prin intermediul licențelor software suplimentare, fără necesitatea de a modifica infrastructura fizică existentă.	Da	Conform.
123.	Platforma trebuie să includă funcționalități avansate de balansare a încărcării și redundanță, pentru a asigura continuitatea operațională și prevenirea suprasolicitării resurselor.	Da	Conform.

4.3.2 Performanța Sistemului

#	Cerință	Obligator	
124.	Platforma trebuie să suporte procesarea a cel puțin 500 de fluxuri video simultane, fără a impacta calitatea imaginii sau viteza de procesare, cu posibilitatea de extindere la minim 5000 de fluxuri prin adăugarea de resurse de procesare și licențe suplimentare.	Da	Conform. Genetec Security Center Base Enterprise Package este proiectat pentru a gestiona un număr mare de fluxuri video simultane prin distribuirea sarcinilor pe mai multe servere și utilizarea resurselor de procesare adiționale. Arhitectura modulară permite extinderea de la 500 până la 5000 de fluxuri prin adăugarea de licențe și resurse de procesare, fără a compromite calitatea imaginii sau viteza de procesare.
125.	Platforma trebuie să includă funcționalități de auto-optimizare, ajustând performanța în funcție de condițiile de operare și volumul de date procesat, pentru a menține un nivel constant de performanță.	Da	Conform. Soluția oferită include funcționalități de auto-optimizare care ajustează dinamic utilizarea resurselor pe baza volumului de date procesat. Aceasta se realizează prin monitorizarea continuă a performanței și reglarea automată a alocării resurselor pentru a asigura performanță constantă, indiferent de condițiile de operare.
126.	Platforma trebuie să permită monitorizarea continuă a performanței sistemului, cu generarea de rapoarte detaliate privind utilizarea resurselor, latențele și starea componentelor critice.	Da	Conform.
127.	Platforma trebuie să fie capabilă să gestioneze traficul de date între multiple locații, asigurând un flux de date sigur și rapid între site-uri și centrul de management.	Da	Conform.

4.3.3 Redundanță și recuperare în caz de dezastru

#	Cerință	Obligator	
128.	Platforma trebuie să ofere mecanisme native de asigurarea redundanței la toate nivelurile critice ale sistemului (procesare, stocare, rețea), asigurând continuitatea operațiunilor chiar și în cazul unei defecțiuni majore.	Da	Conform. Genetec Security Center asigură redundanța la nivel de procesare, stocare și rețea prin funcționalitățile de failover și clustering. Failover-ul pentru camere și arhive, împreună cu clustering-ul serverelor, permit platformei să continue operațiunile fără întreruperi chiar și în caz de defecțiuni majore.
129.	Platforma trebuie să sprijine replicarea datelor între multiple locații, permițând	Da	Conform.

	restaurarea rapidă a datelor în caz de dezastru și minimizând pierderile de informații.		
130.	Platforma trebuie să permită configurarea automată a mecanismelor de failover, astfel încât, în cazul unei defecțiuni, sarcinile să fie preluate instantaneu de resursele de rezervă.	Da	Conform.
131.	Platforma trebuie să asigure compatibilitatea cu soluțiile de backup și recuperare în cloud, permițând protejarea și accesul la datele critice din orice locație.	Da	Conform.
132.	Platforma trebuie să includă funcționalități de monitorizare și raportare a stării sistemului de redundanță și backup, cu notificări automate în cazul detectării unor probleme.	Da	Conform. Genetec Security Center dispune de funcționalități de monitorizare a stării sistemului de redundanță și backup, cu notificări automate pentru detectarea rapidă a problemelor.
133.	Platforma trebuie să sprijine planuri de recuperare în caz de dezastru testabile și documentate, permițând validarea periodică a capacității de restaurare a sistemului.	Da	Conform.
134.	Platforma trebuie să permită configurarea de proceduri automate pentru migrarea sarcinilor și datelor către alte locații în caz de necesitate, asigurând continuitatea operațională fără întreruperi.	Da	Conform.

5. Cerințe funcționale ale platformei

5.1 Componenta de analiză a traficului rutier

Pe aspect de analiză a traficului rutier Platforma de monitorizare propusă include funcționalități esențiale pentru colectarea, procesarea și gestionarea datelor referitoare la vehicule și comportamentele de trafic. Aceasta permite înregistrarea în timp real a vehiculelor, detecția automată a comportamentelor și identificarea încălcărilor, contribuind astfel la o gestionare eficientă.

Soluția tehnologică include capabilități avansate de înregistrare automată, precum și detecție și clasificare automată a vehiculelor și obiectelor. Funcționalitatea de analiză comportamentală permite monitorizarea activităților de trafic, generând alerte automate în cazul incidentelor sau comportamentelor anormale.

Platforma integrează procesarea video în timp real, asigurându-se că informațiile sunt disponibile instantaneu pentru utilizatori. De asemenea, oferă suport pentru analiza detaliată a datelor video offline, facilitând investigațiile ulterioare.

Flexibilitatea platformei permite integrarea cu alte sisteme existente, cum ar fi gestionarea amenzilor și sancțiunilor, asigurând astfel o utilizare eficientă a resurselor. Funcționalitățile avansate de raportare și analiza vizuală a datelor permit utilizatorilor să obțină perspective detaliate asupra traficului și incidentelor.

Un aspect critic al soluției este capacitatea de a detecta și semnaliza vehiculele de interes, sincronizându-se cu baze de date relevante pentru a oferi monitorizare în timp real și notificări imediate autorităților competente. Aceste cerințe sunt fundamentale pentru a asigura o gestionare eficientă a traficului și aplicarea legii în mod proactiv.

#	Cerință	Obligator	Declarație Ofertant
135.	Platforma trebuie să asigure înregistrarea automată a tuturor vehiculelor care traversează puncte de monitorizare, utilizând resurse de tip edge-computing și/sau server-based. Datele colectate trebuie să includă imagini, data, ora și locația trecerii vehiculelor.	Da	Conform. Soluția oferată asigură înregistrarea automată a vehiculelor prin integrarea soluțiilor Genetec Security Center și VaxALPR, utilizând resurse de edge-computing și server-based. Datele colectate includ imagini, data, ora și locația trecerii vehiculelor, fiind salvate într-o bază de date centralizată pentru acces rapid și eficient.
136.	Platforma trebuie să permită identificarea vehiculelor prin numărul de înmatriculare, cel puțin pentru vehicule din spațiul UE.	Da	Conform.
137.	Platforma trebuie să permită vizualizarea și revizuirea în timp real a fluxului de vehicule, oferind operatorilor acces instantaneu la imagini și date colectate.	Da	Conform. Soluția oferată facilitează vizualizarea și revizuirea în timp real a fluxului de vehicule prin integrarea interfeței de utilizator a Genetec Security Center
138.	Platforma trebuie să fie capabilă să detecteze automat vehicule, persoane și alte obiecte, utilizând algoritmi avansați de procesare a imaginilor. Obiectele trebuie clasificate cel puțin în funcție de dimensiune, formă, culoare, direcția de deplasare sau tipul vehiculului.	Da	Conform. Soluția oferată utilizează algoritmi avansați de procesare a imaginilor pentru a detecta automat vehicule, persoane și alte obiecte, integrând tehnologia din Genetec Security Center, BriefCam și VaxALPR. BriefCam contribuie cu capacități de analiză video avansată, permițând clasificarea obiectelor în funcție de dimensiune, formă, culoare, direcția de deplasare și tipul vehiculului. Această integrare permite o gestionare eficientă a fluxului de date și o reacție rapidă la situații de interes, asigurând o monitorizare completă și precisă a zonei, contribuind astfel la îmbunătățirea securității publice.
139.	Detectația și clasificarea automată trebuie să funcționeze în toate condițiile de iluminare (zi/noapte) și în condiții meteorologice variate, asigurând o acuratețe ridicată.	Da	Conform.
140.	Platforma trebuie să fie capabilă să genereze alerte automate în timp real atunci când sunt detectate evenimente de interes.	Da	Conform.
141.	Platforma trebuie să permită definirea și ajustarea regulilor pentru declanșarea alertelor, pe baza scenariilor de securitate sau monitorizare.	Da	Conform.
142.	Platforma trebuie să includă capabilități de analiză comportamentală pentru a detecta automat activități sau comportamente neobișnuite în zona monitorizată (ex. staționarea nejustificată, vehiculele care se deplasează în sens opus).	Da	Conform. Soluția oferată include capabilități avansate de analiză comportamentală prin integrarea tehnologiilor din Genetec Security Center și BriefCam. Aceste tehnologii utilizează algoritmi sofisticati pentru a detecta automat activități sau comportamente neobișnuite în zona monitorizată, cum ar fi staționarea nejustificată a vehiculelor sau deplasarea acestora în sens opus. BriefCam analizează fluxurile video și generează alerte în timp real, permițând operatorilor să reacționeze rapid la situațiile potențial problematice, contribuind astfel la îmbunătățirea siguranței publice și a eficienței operațiunilor de monitorizare.
143.	Sistemul trebuie să permită definirea și ajustarea regulilor comportamentale, permițând utilizatorilor să creeze scenarii personalizate de monitorizare și detectare.	Da	Conform.
144.	Sistemul trebuie să includă un modul avansat de raportare, care să permită	Da	Conform.

	generarea de rapoarte detaliate cu privire la evenimente, vehicule și comportamente detectate.		
145.	Platforma trebuie să ofere capabilități de vizualizare grafică și interactivă a datelor, permițând generarea de diagrame și alte reprezentări vizuale pentru analiza.	Da	Conform. Soluția oferită oferă capabilități de vizualizare grafică și interactivă a datelor prin integrarea modulelor din Genetec Security Center și BriefCam. Aceste module permit generarea de diagrame și alte reprezentări vizuale care facilitează analiza datelor colectate.
146.	Platforma trebuie să fie capabilă să detecteze automat încălcările regulilor de circulație cel puțin trecerea la culoarea roșie a semnalului semaforului, parcare în zonă interzisă, deplasarea pe benzi specializate (cum ar fi banda destinată transportului public)	Da	Conform.
147.	Sistemul trebuie să ofere funcționalități de capturare a imaginilor și înregistrărilor video relevante pentru fiecare încălcare, alături de datele de identificare ale vehiculului (număr de înmatriculare, viteză, data, ora, locația)	Da	Conform.
148.	Sistemul trebuie să ofere alerte automate în caz de încălcări, notificând operatorii pentru a lua măsuri imediate.	Da	Conform.
149.	Platforma trebuie să ofere rapoarte statistice și analize asupra încălcărilor, cu opțiunea de a integra aceste date cu sistemele de gestionare a amenziilor.	Da	Conform.
150.	Platforma trebuie să fie capabilă să detecteze automat vehiculele suspecte sau care se află pe liste de interes (ex. vehicule furate) și să semnaleze acest lucru către operatori pentru investigare.	Da	Conform.
151.	Platforma trebuie să ofere suport pentru detectarea obiectelor sau vehiculelor staționare pentru perioade lungi de timp, alertând operatorii în caz de comportamente suspecte.	Da	Conform.
152.	Platforma trebuie să asigure actualizarea automată și manuală a listei de interes, cu posibilitatea de a adăuga sau elimina vehicule pe baza informațiilor furnizate de autorități.	Da	Conform. Soluția oferită oferă suport pentru detectarea obiectelor sau vehiculelor staționare pentru perioade lungi de timp prin utilizarea tehnologiilor avansate de analiză video din Genetec Security Center și BriefCam. Aceste tehnologii monitorizează continuu zonele specifice și utilizează algoritmi de învățare automată pentru a identifica vehiculele care rămân staționate pentru perioade neobișnuit de lungi.
153.	Platforma trebuie să permită integrarea cu bazele de date naționale și internaționale pentru a sincroniza și actualiza lista de interes în timp real.	Da	Conform.
154.	Platforma trebuie să permită urmărirea vehiculelor de interes în timp real, permițând vizualizarea traseului și a punctelor de trecere înregistrate.	Da	Conform.
155.	Sistemul trebuie să fie capabil să genereze alerte instantanee atunci când vehiculele de interes sunt detectate, notificând imediat autoritățile competente sau operatorii responsabili.	Da	Conform.

156.	Sistemul trebuie să ofere opțiuni de integrare cu sistemele de gestionare a contravențiilor.	Da	Conform.
------	--	----	-----------------

5.2 Componenta de management video (VMS)

În cadrul ofertei noastre, componenta de Management Video (VMS) joacă un rol esențial în monitorizarea, înregistrarea și gestionarea fluxurilor video provenite de la camerele de supraveghere. Această soluție include funcționalități cheie care asigură o monitorizare video eficientă și sigură.

VMS-ul nostru dispune de capacități avansate de înregistrare, permițând stocarea continuă a fluxurilor video pentru revizuire ulterioară. Operatorii beneficiază de vizualizare în timp real, facilitând monitorizarea activităților din zonele de interes și reacția rapidă la evenimentele detectate.

Interfața utilizatorului este concepută pentru a fi intuitivă, oferind funcții de gestionare ușoară a fluxurilor video. Utilizatorii pot căuta și filtra înregistrările pe baza criteriilor specifice, cum ar fi data, ora și tipul de eveniment, asigurându-se astfel acces rapid la informațiile necesare.

De asemenea, soluția noastră integrează analize video avansate, care permit detecția automată a comportamentelor suspecte și generarea de alerte, contribuind astfel la o monitorizare proactivă.

În ceea ce privește securitatea, datele video sunt protejate prin măsuri de criptare și control al accesului, asigurând integritatea și confidențialitatea informațiilor. Această arhitectură robustă permite o gestionare eficientă a resurselor video, sprijinind astfel aplicarea corectă a legii și îmbunătățind managementul traficului rutier.

#	Cerință	Obligator	
157.	Platforma trebuie să permită agregarea fluxurilor video de la toate camerele de supraveghere conectate, oferind o vizualizare centralizată a acestora într-o interfață unificată.	Da	Conform. Soluția oferată permite agregarea fluxurilor video de la toate camerele de supraveghere conectate prin intermediul modulului Omnicast, oferind o vizualizare centralizată într-o interfață unificată. Aceasta facilitează gestionarea eficientă a tuturor camerelor dintr-o singură platformă, asigurând o experiență de utilizare intuitivă
158.	Platforma trebuie să suporte fluxuri video de la camere de diferite rezoluții și tipuri (ex. camere IP, PTZ, termice), asigurând compatibilitatea și interoperabilitatea între echipamente.	Da	Conform. Soluția oferată suportă fluxuri video de la camere de diferite rezoluții și tipuri, inclusiv camere IP, PTZ și termice, asigurând compatibilitatea și interoperabilitatea între echipamente. Modulul Omnicast integrează o varietate de dispozitive, permițând utilizatorilor să beneficieze de soluții personalizate în funcție de necesități
159.	Platforma trebuie să permită configurarea fluxurilor video în funcție de nevoile operaționale, inclusiv setarea calității video, a cadrelor pe secundă și a modului de înregistrare (continuu, la detecție de mișcare, manual).	Da	Conform. Soluția oferată permite configurarea fluxurilor video în funcție de nevoile operaționale, inclusiv setarea calității video, a cadrelor pe secundă și a modului de înregistrare (continuu, la detecție de mișcare, manual). Utilizatorii pot crea profiluri de înregistrare personalizate pentru diferite scenarii
160.	Platforma trebuie să permită redarea în timp real și înregistrarea simultană a fluxurilor video, oferind opțiuni de control asupra parametrilor video (zoom, panoramare, înclinare) pentru camerele PTZ.	Da	Conform. Redarea simultană și înregistrarea fluxurilor video sunt realizate fără întreruperi, permițând utilizatorilor să controleze parametrii video, cum ar fi zoom-ul și unghiurile de vizionare,

			în cazul camerelor PTZ. Aceasta asigură o reacție rapidă și un control eficient în scenarii de monitorizare activă.
161.	Platforma trebuie să asigure sincronizarea automată a fluxurilor video cu datele de la alte sisteme (ex. ANPR, gestionarea incidentelor), pentru a permite corelarea informațiilor și o analiză eficientă.	Da	Conform.
162.	Platforma trebuie să permită crearea și gestionarea de grupuri de camere, oferind posibilitatea monitorizării simultane a mai multor fluxuri video într-o singură fereastră de vizualizare.	Da	Conform. Soluția oferită asigură managementul grupurilor de camere și permite operatorilor să monitorizeze simultan mai multe fluxuri video într-o fereastră unificată, sporind eficiența supravegherii. Aceasta oferă o vizualizare integrată a mai multor locații, optimizând procesul decizional în timp real.
163.	Platforma trebuie să includă funcționalități de ajustare automată a parametrilor video în funcție de condițiile de iluminare și meteo, asigurând calitatea optimă a imaginilor înregistrate.	Da	Conform. Soluția oferită include ajustarea automată a parametrilor video în funcție de condițiile de iluminare și meteorologice, asigurând calitatea optimă a imaginilor. Aceasta poate include și opțiuni de configurare manuală pentru utilizatori
164.	Platforma trebuie să permită configurarea și gestionarea alarmei video, care să fie declanșată în funcție de detectarea unor evenimente specifice (ex. mișcare în zone restricționate).	Da	Conform. Soluția oferită permite configurarea alarmelor video, care pot fi activate în funcție de detectarea anumitor evenimente, cum ar fi intrarea în zone restricționate. Aceste alerte pot fi integrate cu altele pentru o reacție coordonată
165.	Platforma trebuie să permită arhivarea automată a fluxurilor video înregistrate, cu opțiuni de stocare pe termen scurt și lung, în funcție de necesitățile operaționale.	Da	Conform. Soluția oferită asigură arhivarea automată a fluxurilor video, cu opțiuni de stocare pe termen scurt și lung, în funcție de necesitățile operaționale. Utilizatorii pot defini politici de stocare pentru a optimiza utilizarea resurselor.
166.	Platforma trebuie să permită accesul rapid la arhivele video, cu funcționalități avansate de căutare pe baza criteriilor de timp, locație și tip de eveniment.	Da	Conform. Soluția oferită asigură acces rapid la arhivele video, beneficiind de funcționalități avansate de căutare
167.	Platforma trebuie să includă funcționalități de gestionare a spațiului de stocare, permițând administratorilor să aloce și să monitorizeze utilizarea capacității de stocare pentru fiecare cameră sau grup de camere.	Da	Conform.
168.	Platforma trebuie să permită setarea unor politici automate de curățare a arhivelor vechi, cu opțiuni de păstrare a înregistrărilor critice pentru perioade extinse de timp.	Da	Conform.
169.	Platforma trebuie să asigure criptarea înregistrărilor video stocate, pentru a proteja datele împotriva accesului neautorizat și a asigura conformitatea cu reglementările de securitate.	Da	Conform.
170.	Platforma trebuie să permită exportul înregistrărilor video în formate standardizate (ex. MP4, AVI) pentru utilizarea în investigații sau proceduri judiciare.	Da	Conform.
171.	Platforma trebuie să ofere funcționalități de redare a înregistrărilor video la diferite viteze, inclusiv redare cadru cu cadru și redare accelerată, pentru o analiză detaliată.	Da	Conform.
172.	Platforma trebuie să permită configurarea de alerte pentru administratorii de sistem în cazul în care spațiul de stocare atinge	Da	Conform.

	capacitatea maximă, pentru a preveni pierderea datelor.		
173.	Platforma trebuie să permită arhivarea automată a fluxurilor video înregistrate, cu opțiuni de stocare pe termen scurt și lung, în funcție de necesitățile operaționale.	Da	Conform.
174.	Platforma trebuie să includă suport complet pentru camerele PTZ, permițând operatorilor să controleze mișcările camerelor (panoramare, înclinare, zoom) în timp real.	Da	Conform.
175.	Platforma trebuie să permită definirea unor tururi automate pentru camerele PTZ, permițând monitorizarea automată a zonelor critice conform unor trasee predefinite.	Da	Conform.
176.	Platforma trebuie să ofere funcționalități de detecție automată a mișcării și urmărirea automată a obiectelor în mișcare, utilizând camerele PTZ pentru a menține ținta în cadru.	Da	Conform. Funcționalitățile de detecție a mișcării și urmărirea obiectelor sunt disponibile prin camerele PTZ, menținând țintele în cadru pentru o supraveghere dinamică.
177.	Platforma trebuie să permită configurarea de scenarii automate, unde camerele PTZ să reacționeze la evenimente detectate de alte sisteme (ex. detectarea unui vehicul pe lista de interes).	Da	Conform. Soluția oferită permite camerele PTZ să reacționeze la evenimentele detectate de alte sisteme, asigurând o reacție rapidă.
178.	Platforma trebuie să asigure compatibilitatea cu camere PTZ de la diferiți producători, permițând integrarea ușoară a noilor echipamente în infrastructura existentă.	Da	Conform.
179.	Platforma trebuie să ofere opțiuni de configurare a parametrilor PTZ direct din interfața de utilizator, inclusiv setarea zonelor de interes și a limitelor de mișcare.	Da	Conform.
180.	Platforma trebuie să permită configurarea de zone de protecție, în care mișcarea detectată de camerele PTZ să declanșeze automat alarme sau notificări.	Da	Conform.
181.	Platforma trebuie să includă funcționalități de diagnosticare și întreținere pentru camerele, oferind informații despre starea și funcționarea echipamentelor.	Da	Conform.
182.	Platforma trebuie să permită detectarea automată a mișcării și clasificarea obiectelor pe baza dimensiunii, vitezei și comportamentului acestora, oferind alerte în timp real pentru activitățile suspecte.	Da	Conform.
183.	Platforma trebuie să fie capabilă să analizeze activitatea pietonală și rutieră, generând rapoarte și statistici cu privire la fluxurile de persoane și vehicule, în scopul optimizării securității și gestionării traficului.	Da	Conform.

5.3 Analiză video avansată

Analiza video avansată constituie un element cheie al soluțiilor moderne de securitate și monitorizare, având capacități extinse de colectare, procesare și interpretare a datelor vizuale. Platforma propusă oferă capacități avansate de identificare și clasificare automată a evenimentelor complexe din fluxurile video, ceea ce contribuie la creșterea eficienței în detectarea și investigarea incidentelor.

Utilizând algoritmi avansați și specializați, analiza video avansată îmbunătățește semnificativ procesul de recunoaștere a obiectelor, detectarea anomaliilor și comportamentelor suspecte, precum și corelarea datelor din multiple surse de monitorizare. Platforma permite integrarea și utilizarea modulelor

specializate, cum ar fi BriefCam pentru analiza video și Vaxtor pentru recunoașterea automată a numerelor de înmatriculare (ANPR), facilitând astfel identificarea vehiculelor și gestionarea incidentelor.

Funcționalitățile incluse în platformă sunt variate și includ detectarea automată a mișcării, analiza comportamentală a obiectelor și identificarea tipurilor de vehicule. Generarea de alerte în timp real permite operatorilor să reacționeze prompt la evenimentele detectate.

Prin combinarea acestor capabilități, analiza video avansată oferă un suport esențial pentru activitățile de securitate și investigare. Sistemul este scalabil și adaptabil, având capacitatea de a gestiona un volum mare de date video, asigurând astfel eficiența în investigarea incidentelor și prevenirea riscurilor.

#	Cerință	Obligator	
184.	Platforma trebuie să includă capabilități de analiză video avansată, utilizând tehnologii emergente pentru detectarea comportamentului suspect și recunoașterea automată a obiectelor, cu specializări dedicate pentru: - Analiza vehiculelor în trafic (ANPR) – recunoașterea automată a numerelor de înmatriculare, clasificarea vehiculelor, detectarea încălcărilor rutiere și generarea de alerte în timp real. Sistemul trebuie să permită monitorizarea mai multor benzi de circulație simultan. - Analiză Public-Safety (Investigație) – detectarea și investigarea comportamentelor suspecte și anomaliilor în spații publice, incluzând analiza obiectelor și persoanelor, identificarea riscurilor potențiale și generarea de rapoarte detaliate pentru investigații ulterioare. Ambele specializări trebuie să fie integrate într-o interfață unificată, oferind monitorizare în timp real și suport pentru investigarea și raportarea evenimentelor.	Da	Conform. Soluția oferată include capabilități avansate de analiză video prin integrarea modulelor Vaxtor și BriefCam în Genetec Security Center. În ceea ce privește analiza vehiculelor în trafic, Vaxtor oferă recunoașterea automată a numerelor de înmatriculare, asigurând o acuratețe foarte înaltă. Acesta permite și clasificarea vehiculelor în funcție de tip, facilitând astfel monitorizarea traficului. De asemenea, Vaxtor detectează încălcările rutiere, generând alerte în timp real și monitorizând simultan mai multe benzi de circulație. Pe de altă parte, analiza Public-Safety este gestionată prin BriefCam, care detectează comportamente suspecte și anomalii în spații publice. Acesta oferă capabilități de investigare detaliată, permițând căutarea în arhivele video pentru a identifica riscurile potențiale. BriefCam produce, de asemenea, rapoarte detaliate ce includ informații despre incidente, imagini și videoclipuri asociate. Ambele specializări sunt integrate într-o interfață unificată oferită de Genetec Security Center, permițând operatorilor să monitorizeze în timp real toate fluxurile video și să acceseze rapid informațiile necesare pentru investigarea și raportarea evenimentelor.
185.	Platforma trebuie să permită configurarea de reguli personalizate de analiză, permițând identificarea unor scenarii specifice de risc (ex. părăsirea unui obiect într-o zonă publică).	Da	Conform. Soluția oferată permite configurarea de reguli personalizate de analiză prin intermediul modului BriefCam. Aceasta facilitează identificarea scenariilor specifice de risc, cum ar fi părăsirea unui obiect într-o zonă publică. Utilizatorii pot defini aceste reguli în funcție de nevoile lor operaționale,
186.	Platforma trebuie să sprijine analiza video retrospectivă, oferind funcționalități de căutare în arhivele video pe baza tiparelor sau comportamentelor definite de utilizatori.	Da	Conform. Analiza video retrospectivă este susținută de Genetec Security Center, care oferă funcționalități avansate de căutare în arhivele video. Utilizatorii pot căuta pe baza tiparelor sau comportamentelor definite anterior, facilitând identificarea rapidă a incidentelor anterioare și investigarea lor detaliată.
187.	Platforma trebuie să integreze algoritmi de recunoaștere facială, permițând identificarea	Da	Conform. Integrarea algoritmilor de recunoaștere facială este realizată prin BriefCam, care permite

	automată a persoanelor de interes în fluxurile video în timp real sau înregistrate.		identificarea automată a persoanelor de interes în fluxurile video, fie în timp real, fie înregistrate.
188.	Platforma trebuie să permită detectarea și urmărirea automată a vehiculelor în mișcare, utilizând capacități de recunoaștere a numerelor de înmatriculare și a caracteristicilor vehiculului.	Da	Conform. Detectarea și urmărirea automată a vehiculelor în mișcare sunt gestionate de Vaxtor, care utilizează capacități avansate de recunoaștere a numerelor de înmatriculare și a caracteristicilor vehiculului.
189.	Platforma trebuie să sprijine integrarea cu soluții terțe de analiză video, permițând extinderea capacităților de detectare și recunoaștere în funcție de cerințele operaționale.	Da	Conform.
190.	Platforma trebuie să includă funcționalități de vizualizare și raportare a rezultatelor analizei video, oferind operatorilor informații detaliate și ușor de interpretat.	Da	Conform.
191.	Platforma trebuie să ofere suport pentru actualizarea continuă a algoritmilor de analiză, asigurând adaptarea la noi tipuri de amenințări sau comportamente suspecte.	Da	Conform.
192.	Platforma trebuie să permită analiza comportamentului persoanelor și obiectelor în spații publice, cu alertare automată pentru riscuri detectate.	Da	Conform. Analiza comportamentului persoanelor și obiectelor în spații publice se realizează prin tehnologiile din BriefCam, care includ capacități de alertare automată pentru riscurile detectate,
193.	Platforma trebuie să fie capabilă să coreleze evenimente multiple, identificând modele de comportament periculos și incidente asociate.	Da	Conform.
194.	Platforma trebuie să fie capabilă să genereze alerte vizuale și sonore pentru orice comportament deviant detectat, inclusiv pentru obiecte abandonate.	Da	Conform.
195.	Platforma trebuie să permită integrarea cu alte sisteme de securitate și supraveghere, inclusiv senzori audio pentru corelarea incidentelor cu alte surse de date.	Da	Conform. Integrarea cu alte sisteme de securitate și supraveghere, inclusiv senzori audio, este posibilă prin modulul de integrare din Genetec Security Center. Aceasta permite corelarea incidentelor cu datele provenite din diverse surse
196.	Platforma trebuie să permită analiza video avansată în timp real, procesând cel puțin 20 de fluxuri video simultan, fără a afecta performanța generală.	Da	Conform. Soluția oferită include BriefCam care permite analiza video avansată în timp real. Aceasta este realizată prin modulul de analiză video al BriefCam, care poate procesa simultan cel puțin 20 de fluxuri video.
197.	Platforma trebuie să permită analiza video avansată în regim de investigație, procesând cel puțin 100 de fluxuri video simultan, fără a afecta performanța generală.	Da	Conform. În modul de investigație, BriefCam permite analiza video avansată procesând simultan cel puțin 100 de fluxuri video. Aceasta se bazează pe funcționalitatea de investigație din BriefCam
198.	Platforma trebuie să fie capabilă să detecteze mișcarea și să identifice obiecte de interes (vehicule, persoane, obiecte abandonate) cu o acuratețe de cel puțin 95%.	Da	Conform. Soluția oferită include BriefCam, care este capabil să detecteze mișcarea și să identifice obiecte de interes, cum ar fi vehicule, persoane și obiecte abandonate, cu o acuratețe de cel puțin 95%. Aceasta se realizează prin modulul de detecție a mișcării din BriefCam, care utilizează algoritmi avansați de procesare a imaginii pentru a asigura precizia detecției

199.	Platforma trebuie să asigure analiza comportamentală automată, identificând anomalii, comportamente suspecte și încălcări de reguli, generând alerte instantanee.	Da	Conform. Analiza comportamentală automată este gestionată de modulul de analiză comportamentală din BriefCam, care identifică anomalii, comportamente suspecte și încălcări de reguli.
200.	Platforma trebuie să detecteze automat comportamente suspecte, precum aglomerații neobișnuite, obiecte abandonate sau mișcări anormale.	Da	Conform. Detectarea automată a comportamentelor suspecte, inclusiv aglomerațiile neobișnuite și obiectele abandonate, este realizată prin funcționalitatea de analiză comportamentală din BriefCam.
201.	Platforma trebuie să genereze rapoarte detaliate privind incidentele detectate, inclusiv imagini și videoclipuri asociate, marcate temporal pentru o investigație ușoară.	Da	Conform. Soluția oferată generează rapoarte detaliate privind incidentele detectate prin modulul de raportare din BriefCam. Acesta include imagini și videoclipuri asociate incidentelor, toate marcate temporal
202.	Platforma trebuie să permită operatorilor să vizualizeze simultan fluxuri video în timp real și arhive video pentru investigarea incidentelor, fără întreruperea funcționalității de monitorizare live.	Da	Conform. Operatorii pot vizualiza simultan fluxuri video în timp real și arhive video datorită funcționalității oferite de modulul Omnicast din Genetec Security Center. Aceasta asigură acces continuu la informații
203.	Platforma trebuie să permită căutarea avansată în arhivele video pe baza unor criterii precum: număr de înmatriculare, tipul vehiculului, comportament suspect, data și ora, obiect, îmbrăcăminte, etc.	Da	Conform.
204.	Platforma trebuie să permită configurarea și definirea zonelor de interes pentru fiecare flux video, permițând filtrarea mișcărilor și evenimentelor în aceste zone.	Da	Conform.
205.	Platforma trebuie să permită exportul de înregistrări video, în formate standardizate, pentru a fi utilizate în alte sisteme sau pentru investigare.	Da	Conform.
206.	Platforma trebuie să dispună de capabilități de redare accelerată (video synopsis), afișând simultan activități din aceeași perioadă de timp pentru o revizuire eficientă.	Da	Conform. Soluția oferată include capabilități de redare accelerată. Această funcționalitate BriefCam permite afișarea simultană a activităților din aceeași perioadă de timp.
207.	Sistemul trebuie să permită reconstrucția secvențelor video pentru a investiga în detaliu incidentele și a înțelege pe deplin evenimentele.	Da	Conform. Soluția oferată permite reconstrucția secvențelor video pentru a investiga în detaliu incidentele prin intermediul modulului de analiză din BriefCam. Această funcționalitate utilizează tehnici avansate de procesare a imaginilor și algoritmi de analiză comportamentală pentru a extrage și organiza informațiile relevante din fluxurile video.
208.	Sistemul trebuie să includă funcționalități avansate de filtrare și revizuire a evenimentelor video, permițând operatorilor să se concentreze doar pe evenimentele de interes (ex. comportamente suspecte, opriri neautorizate).	Da	Conform. Soluția oferată include funcționalități avansate de filtrare și revizuire a evenimentelor video prin intermediul modulului de analiză din BriefCam. Aceste funcționalități permit operatorilor să se concentreze exclusiv pe evenimentele de interes. BriefCam oferă opțiuni de filtrare detaliate care permit utilizatorilor să definească criteriile specifice pentru tipurile de evenimente pe care doresc să le monitorizeze.

			Aceasta include selectarea anumitor comportamente sau activități anormale.
209.	Platforma trebuie să asigure compresie video H.264, H265, MPEG-4, MPEG-2, MJPEG, MxPEG pentru fluxurile video și MJPEG pentru capturile statice, optimizând stocarea și transmitia datelor.	Da	Conform.
210.	Platforma trebuie să permită detectarea automată a vehiculelor, inclusiv clasificarea acestora în funcție de tip autoturism, camion, motocicletă.	Da	Conform. Soluția oferată permite detectarea automată a vehiculelor și clasificarea acestora în funcție de tip (autoturism, camion, motocicletă) prin modulul ANPR din Vaxtor. Aceasta se realizează prin algoritmi avansați de procesare a imaginii care analizează fluxurile video în timp real.
211.	Platforma trebuie să fie capabilă să recunoască comportamente neobișnuite sau activități suspecte, cum ar fi opriri neautorizate, schimbări bruște de direcție sau vehicule staționate în zone interzise.	Da	Conform.
212.	Platforma trebuie să asigure integrarea funcționalităților de recunoaștere a numerelor de înmatriculare (ANPR), cu o rată de acuratețe de cel puțin 98% în condiții normale de trafic și lumină, pentru cel puțin 25 fluxuri video simultan, într-o rezoluție minimă de 4k, fără a se limita la numărul de benzi sau direcția de deplasare.	Da	Conform. Conform. Funcționalitățile ANPR din Vaxtor permit, de asemenea, recunoașterea numerelor de înmatriculare cu o rată de acuratețe de cel puțin 98% pentru cel puțin 100 de fluxuri video simultan, la o rezoluție minimă de 4K, asigurând monitorizarea eficientă a traficului pe multiple benzi.
213.	Platforma trebuie să asigure integrarea funcționalităților de recunoaștere a numerelor de înmatriculare (ANPR), cu o rată de acuratețe de cel puțin 98% în condiții normale de trafic și lumină, pentru cel puțin 50 fluxuri video simultan, într-o rezoluție minimă de 4k, fără a se limita la numărul de benzi sau direcția de deplasare.	Nu (15 puncte)	Conform. Conform. Funcționalitățile ANPR din Vaxtor permit, de asemenea, recunoașterea numerelor de înmatriculare cu o rată de acuratețe de cel puțin 98% pentru cel puțin 100 de fluxuri video simultan, la o rezoluție minimă de 4K, asigurând monitorizarea eficientă a traficului pe multiple benzi.
214.	Platforma trebuie să asigure integrarea funcționalităților de recunoaștere a numerelor de înmatriculare (ANPR), cu o rată de acuratețe de cel puțin 98% în condiții normale de trafic și lumină, pentru cel puțin 100 fluxuri video simultan, într-o rezoluție minimă de 4k, fără a se limita la numărul de benzi sau direcția de deplasare.	Nu (30 puncte)	Conform. Conform. Funcționalitățile ANPR din Vaxtor permit, de asemenea, recunoașterea numerelor de înmatriculare cu o rată de acuratețe de cel puțin 98% pentru cel puțin 100 de fluxuri video simultan, la o rezoluție minimă de 4K, asigurând monitorizarea eficientă a traficului pe multiple benzi.
215.	Platforma trebuie să permită căutări avansate pe baza meta-datelor aferente vehiculului, locației și timpului, facilitând investigarea incidentelor.	Da	Conform.
216.	Platforma trebuie să fie capabilă să detecteze și să recunoască automat marca și modelul vehiculului (ex: BMW, Audi, Toyota), utilizând algoritmi avansați de clasificare vizuală.	Nu (30 puncte)	Conform. Soluția oferată permite detectarea și recunoașterea automată a mărcii și modelului vehiculului prin modulul ANPR din Vaxtor. Acest modul utilizează algoritmi avansați de clasificare vizuală pentru a analiza caracteristicile specifice ale vehiculelor
217.	Platforma trebuie să includă funcționalități de înregistrare a vehiculelor identificate în componenta de analiză a traficului rutier.	Da	Conform.
218.	Platforma trebuie să permită indexarea automată a fluxurilor video înregistrate, organizând toate datele pe baza caracteristicilor detectate (ex. vehicule, obiecte, activități).	Da	Conform.

219.	Sistemul trebuie să ofere funcționalități avansate de căutare în înregistrările video, permițând filtrarea evenimentelor pe criterii multiple (ex. culoare, dimensiune, tip de vehicul, direcție de deplasare).	Da	Conform.
220.	Platforma trebuie să ofere opțiuni de export al datelor și înregistrărilor video pentru investigarea suplimentară sau utilizarea în alte sisteme de analiză și raportare.	Da	Conform.
221.	Platforma trebuie să fie capabilă să recunoască automat fețele persoanelor, inclusiv să ofere opțiuni de comparare cu liste de persoane cunoscute sau suspecte.	Da	Conform.

5.4 Interfața programatică de aplicație (API)

#	Cerință	Obligator	
222.	Platforma trebuie să ofere un API robust care să permită accesul programatic la datele și funcționalitățile platformei, facilitând integrarea cu alte sisteme și aplicații.	Da	Conform. Soluția propusă oferă un API robust care facilitează accesul programatic la datele și funcționalitățile sale. Acest API permite integrarea cu diverse sisteme și aplicații terțe.
223.	Platforma trebuie să asigure autentificarea și autorizarea utilizatorilor care accesează API-ul.	Da	Conform. Soluția asigură mecanism de autentificare și autorizare pentru acces la API
224.	Platforma trebuie să permită accesul la API prin metode standard, cum ar fi RESTful services, pentru a asigura interoperabilitatea și ușurința în utilizare.	Da	Conform. API-ul suportă metode standard, în special servicii RESTful
225.	Platforma trebuie să ofere documentație completă și actualizată pentru API, incluzând exemple de utilizare, descrierea endpoint-urilor și specificațiile tehnice.	Da	Conform.
226.	Platforma trebuie să permită monitorizarea și auditarea accesului la API, oferind administratorilor un control complet asupra activităților programatice efectuate prin intermediul acestuia.	Da	Conform. Platforma include funcționalități pentru monitorizarea și auditarea accesului API
227.	Platforma trebuie să asigure securitatea datelor transmise prin API, implementând criptarea datelor în tranzit și protecția împotriva atacurilor de tip injection sau man-in-the-middle.	Da	Conform. Securitatea datelor este asigurată în designul API-ului, cu criptare implementată pentru datele în tranzit.

5.5 Monitorizarea și gestionarea incidentelor

#	Cerință	Obligator	
228.	Platforma trebuie să permită monitorizarea în timp real a incidentelor detectate de camerele de supraveghere, oferind o interfață dedicată pentru gestionarea și documentarea acestora.	Da	Conform. Soluția ofertată include Genetec Mission Control ce permite vizualizarea incidentelor detectate de camerele de supraveghere, oferind o interfață dedicată care facilitează gestionarea și documentarea acestora. Utilizatorii pot observa pe hartă locația incidentelor, detalii generale și statusul fiecărui incident.
229.	Platforma trebuie să detecteze automat incidentele pe baza unor reguli și scenarii predefinite, generând alerte în timp real la declanșarea evenimentelor critice.	Da	Conform. Sistemul utilizează un motor de reguli care analizează datele colectate și, pe baza unor reguli și scenarii predefinite, poate genera alerte în timp real pentru evenimentele de interes.

230.	Platforma trebuie să permită clasificarea automată a incidentelor în funcție de tip, severitate și locație, pentru a asigura prioritizarea corectă a intervențiilor.	Da	Conform.
231.	Platforma trebuie să includă fluxuri de lucru predefinite și personalizabile, care să ghideze operatorii prin pașii necesari pentru gestionarea fiecărui incident într-un mod eficient.	Da	Conform. Soluția oferită include fluxuri de lucru predefinite și personalizabile prin modulul Mission Control. Funcționalitatea include interfețe vizuale intuitive care facilitează configurarea acestor fluxuri,
232.	Platforma trebuie să permită configurarea de fluxuri de lucru personalizate pentru gestionarea incidentelor, adaptate nevoilor specifice ale fiecărui departament sau organizație.	Da	Conform. Platforma permite configurarea de fluxuri de lucru personalizate pentru gestionarea incidentelor, utilizând o arhitectură flexibilă care permite integrarea de pași specifici. Operatorii pot crea și modifica aceste fluxuri direct din interfața de utilizator, cu opțiuni de drag-and-drop
233.	Platforma trebuie să permită alocarea automată și manuală a resurselor necesare, cum ar fi personalul de patrulare/securitate și echipamentele, pentru a gestiona fiecare incident corespunzător.	Da	Conform. Mission Control permite alocarea automată și manuală a resurselor necesare, cum ar fi personalul de patrulare și echipamentele, prin funcționalități de management al resurselor.
234.	Platforma trebuie să ofere o interfață unificată pentru vizualizarea, monitorizarea și gestionarea în timp real a tuturor incidentelor, facilitând coordonarea centralizată.	Da	Conform. Aceasta se realizează prin integrarea datelor din diverse surse, inclusiv camerele de supraveghere și senzori, într-un tablou de bord centralizat. Operatorii pot accesa informații despre incidentele active, istoricul acestora și pot gestiona resursele
235.	Platforma trebuie să permită documentarea completă a fiecărui incident, incluzând momentul, locația, acțiunile întreprinse și resursele alocate pentru gestionare.	Da	Conform. Soluția oferită permite documentarea completă a fiecărui incident prin modulul Mission Control. Acesta colectează informații esențiale precum momentul, locația, acțiunile întreprinse și resursele alocate, asigurând astfel o bază de date detaliată pentru fiecare caz gestionat.
236.	Platforma trebuie să genereze rapoarte detaliate post-incident, incluzând date despre cauze, intervenții și rezultate pentru fiecare incident gestionat.	Da	Conform. Platforma generează rapoarte detaliate post-incident care includ date despre cauzele incidentelor, intervențiile realizate și rezultatele obținute.
237.	Platforma trebuie să fie capabilă să integreze date din multiple surse (camere video, senzori, alarme), corelând aceste informații pentru a oferi o imagine completă a incidentului.	Da	Conform. Integrarea datelor din multiple surse, cum ar fi camere video, senzori și alarme, este facilitată de modulul de corelare a datelor din Genetec Security Center. Această funcționalitate corelează informațiile din diverse surse pentru a oferi o imagine completă și detaliată a incidentului.
238.	Platforma trebuie să permită escaladarea automată a incidentelor nerezolvate, alertând echipele de management sau autoritățile competente dacă timpul de răspuns depășește un anumit prag.	Da	Conform.
239.	Platforma trebuie să sprijine colaborarea între echipe și agenții de securitate, permițând partajarea informațiilor și resurselor între organizații în timpul gestionării incidentelor majore.	Da	Conform. Soluția sprijină colaborarea între echipe și agenții de securitate, permițând partajarea informațiilor și resurselor în timpul gestionării incidentelor majore. Aceasta facilitează un flux de informații eficient între diferite organizații.
240.	Platforma trebuie să permită revizuirea și validarea manuală a incidentelor, oferind	Da	Conform.

	operatorilor posibilitatea de a adăuga note și comentarii la fiecare caz documentat.		
241.	Platforma trebuie să ofere funcționalități de auditare a gestionării incidentelor, înregistrând toate acțiunile întreprinse de operatori în timpul monitorizării și investigării cazurilor.	Da	Conform. Funcționalitățile de auditare a gestionării incidentelor sunt integrate în platformă, înregistrând toate acțiunile întreprinse de operatori în timpul monitorizării și investigării cazurilor. Aceasta permite o trasabilitate completă și un control al calității asupra procesului de gestionare a incidentelor.

6. Suport tehnic și mentenanță

Pentru a asigura continuitatea și performanța optimă a soluției implementate, oferta noastră include servicii complete de suport tehnic, garanție și mentenanță pe o perioadă de 5 ani. Această perioadă extinsă include asigurarea funcționării corecte a soluției, și la necesitate intervenții corective și preventive, precum și actualizări periodice de software și firmware.

Furnizorul nostru garantează opțiuni flexibile de extindere a serviciilor, asigurând astfel adaptabilitate la nevoile organizației. Suportul tehnic live și accesul la resurse de auto-servire sunt disponibile, iar intervențiile rapide pentru probleme critice minimizează impactul defecțiunilor asupra funcționării sistemului.

#	Cerință	Obligator	
242.	Furnizorul soluției va asigura servicii de suport tehnic, mentenanță și garanție de producător pentru soluția livrată pe o perioadă de minim 3 ani.	Da	Conform.
243.	Furnizorul soluției va asigura servicii de suport tehnic, mentenanță și garanție de producător pentru soluția livrată pe o perioadă de minim 5 ani.	Nu (30 puncte)	Conform. Soluția oferită include un pachet de suport pentru o perioada de 5 ani.
244.	Serviciile și angajamentele de mentenanță trebuie să includă toate activitățile necesare pentru a asigura funcționarea corectă a soluției, cum ar fi intervențiile corective, preventive și predictive, precum și asistența tehnică la distanță sau la fața locului, atunci când este necesar.	Da	Conform.
245.	Furnizorul trebuie să asigure actualizări periodice ale software-ului și firmware-ului pe întreaga perioadă de garanție, mentenanță și suport, pentru a asigura îmbunătățirea performanțelor soluției și remedierea eventualelor vulnerabilități de securitate.	Da	Conform.
246.	Furnizorul trebuie să garanteze disponibilitatea pieselor de schimb pentru echipamentele livrate, după caz, pe toată durata perioadei de mentenanță, astfel încât orice defect să fie remediat rapid, fără întreruperea funcționării sistemului.	Da	Conform.
247.	Timpul maxim de intervenție pentru remedierea unei defecțiuni critice nu trebuie să depășească 24 de ore de la raportarea incidentului, iar pentru problemele minore intervenția trebuie efectuată în termen de 48 de ore.	Da	Conform.
248.	Soluția trebuie să permită monitorizarea proactivă, astfel încât potențialele probleme	Da	Conform.

	să fie detectate și raportate înainte ca acestea să devină critice, minimizând astfel riscurile de întrerupere a serviciilor.		
249.	Pe întreaga durată a contractului de mentenanță și suport, furnizorul trebuie să asigure accesul extins la suport tehnic, incluzând o linie directă și un portal online pentru gestionarea rapidă a solicitărilor.	Da	Conform.
250.	Soluția trebuie să includă mentenanță preventivă programată pentru a asigura funcționarea optimă a sistemului și pentru a reduce riscurile de defecțiuni sau întreruperi neașteptate.	Da	Conform.
251.	Furnizorul la solicitare poate să efectueze evaluări anuale ale sistemului, analizând toate componentele, setările de configurare și starea generală a sistemului, pentru a se asigura că respectă cele mai bune practici și standarde de securitate.	Da	Conform.
252.	Furnizorul trebuie să furnizeze documentație detaliată de mentenanță și ghiduri pentru întreținerea regulată a sistemului, inclusiv intervalele și procedurile recomandate de mentenanță	Da	Conform.
253.	Soluția trebuie să includă suport telefonic și prin chat live în timpul programului de lucru pentru asistență la depanare, consultanță tehnică și ghidare în configurare. Suportul trebuie să fie disponibil prin telefon, portal online sau chat live.	Da	Conform.
254.	Suportul trebuie să includă diagnostic colaborativ, oferind echipei tehnice acces de la distanță (cu autorizare) pentru diagnosticare, replicare a problemelor și soluționare.	Da	Conform.
255.	Furnizorul trebuie să clasifice incidentele pe niveluri de severitate (Critic, Ridicat, Mediu, Scăzut) și să ofere timpi de răspuns corespunzători.	Da	Conform.
256.	Furnizorul trebuie să asigure acces la un portal de suport online pentru gestionarea cazurilor, urmărirea incidentelor, accesul la articole din baza de cunoștințe și alte resurse de auto-servire.	Da	Conform.
257.	Furnizorul trebuie să asigure acces la toate actualizările software (majore, minore și patch-uri) și la remediile urgente pentru probleme critice.	Da	Conform.
258.	Furnizorul trebuie să ofere suport tehnic de instalare și configurare a soluției livrate.	Da	Conform.