Pașaportul Sistemului de Monitorizare Proactivă de Securitate

1. *Informații generale despre sistem*

1.1. Denumirea sistemului: Sistem de Monitorizare Proactivă de Securitate.

1.2. Scopul: Asigurarea securității obiectivelor infrastructurii, prevenirea accesului neautorizat, identificarea potențialelor amenințări, prevenirea incidentelor și reacția operativă la acestea.

1.3. Obiective monitorizate: Obiective de infrastructură, incluzând perimetrul și clădirile administrative și gospodărești situate în interiorul acestuia.

2. *Componența sistemului*

Sistemul de Monitorizare Proactivă de Securitate este compus dintr-un ansamblu de mijloace tehnice și software care asigură controlul continuu și neîntrerupt al obiectivelor monitorizate, cu posibilitatea de reacție întârziată și intervenție în caz de alertă, precum și cu posibilitatea notificării rapide a utilizatorilor responsabili.

Acest sistem permite integrarea sistemului de securitate existent la obiectiv cu sistemul de monitorizare prin protocoale specializate ale sistemului inteligent de supraveghere video Dahua și sistemului de securitate Ajax

2.1. Echipamente:

- Camere de supraveghere video: Camere inteligente cu funcții de configurare a zonelor de alarmă, detectare a mișcării și transmitere a datelor prin protocolul TCP/IP.
- Senzori de securitate: Senzori de mișcare, de spargere a geamurilor și alte tipuri de senzori instalați în interior pentru detectarea accesului neautorizat.
- Dispozitive de descurajare activă: Lămpi stroboscopice, sirene și difuzoare instalate pe perimetru pentru a speria intrușii și a atrage atenția asupra incidentului.
- Hub-ul sistemului Ajax: Nod central pentru procesarea semnalelor de la senzori și transmiterea informațiilor către operator.
- Infrastructură de rețea: Routere pentru transmiterea rapidă și sigură a datelor (cu utilizarea criptării conform standardelor de securitate), servere pentru stocarea informațiilor.
- Elemente de alimentare de rezervă: Acumulatori și UPS instalate atât la obiectivele monitorizate, cât și la centrul de monitorizare, pentru asigurarea funcționării continue în caz de pierdere a alimentării (durata de funcționare de până la 12 ore).

2.2. Software:

- Dahua DSS Pro: Platformă specializată pentru gestionarea supravegherii video, analiza evenimentelor, stocarea datelor și afișarea informațiilor pentru operator.
- Ajax Security System: Software pentru armarea sistemului, configurarea programului de armare, recepționarea alarmelor, analiza stării obiectivului și a echipamentelor, și monitorizarea zonelor de securitate.

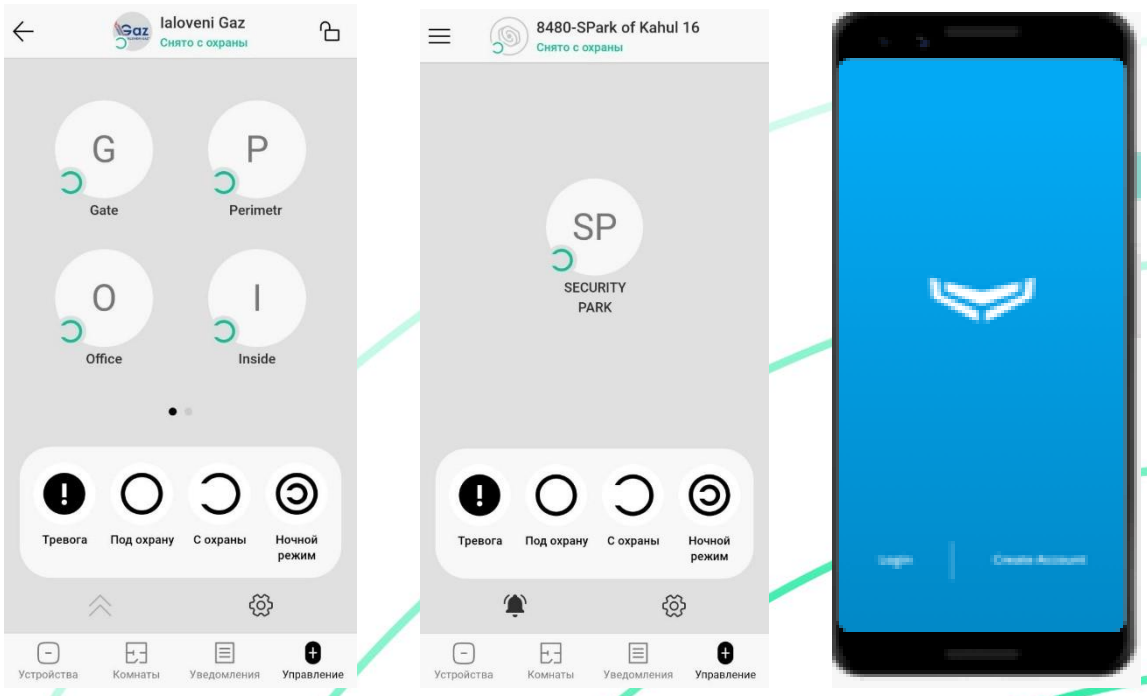
www.securitypark.md
info@securitypark.md
+373 22 106 105

- Looker Studio: Studio de date pentru afișarea și analiza evenimentelor (contul personal al utilizatorului).
- Telegram: Utilizat pentru notificări imediate și planificate despre evenimentele de alarmă.
- Intelligent Flex Management Plug-in: Funcționalitate specializată pentru gestionarea flexibilă a tuturor elementelor sistemului de securitate.

3. *Funcționalitatea sistemului*

3.1. Armarea sistemului de securitate.

- Armare automata: Sistemul este armat automat în intervalul de timp specificat, fie în totalitate, fie pe zone, conform programului și cerințelor clientului. Numărul de zone de securitate pe obiectiv nu depășește 25. Sistemul permite configurarea flexibilă a zonelor și susține combinarea zonelor de alarmă pe camerele inteligente cu senzorii de securitate.
- Armare manuală: Utilizatorul poate arma sistemul în mod flexibil, fie în totalitate, fie pe zone specifice, utilizând aplicația mobilă Ajax Security System sau software-ul specializat API. Armarea poate fi realizată de la distanță, fără prezența fizică la obiectiv.



Interfața aplicației mobile a sistemului de securitate Ajax, utilizată pentru gestionarea de la distanță a alarmei de securitate, inclusiv funcțiile de armare/dezarmare, activarea alarmei si controlul modurilor de securitate

De asemenea, (în cazuri excepționale) există posibilitatea armării întregului obiectiv folosind telecomanda, aflându-se la fața locului.

Tastatura tactilă Ajax KeyPad pentru gestionarea sistemului de securitate, care permite activarea și dezactivarea alarmei folosind un cod sau comenzi speciale

Acest sistem (flexibil) de armare oferă posibilitatea de a activa sau dezactiva securitatea într-un mod extrem de convenabil pentru utilizator - în orice moment, din orice locație, în funcție de cerințele și situațiile apărute.

Combinația între armarea automată și cea manuală permite implementarea diferitelor scenarii de gestionare a sistemului, în funcție de condițiile și procesele specifice care au loc la obiectivele monitorizate.

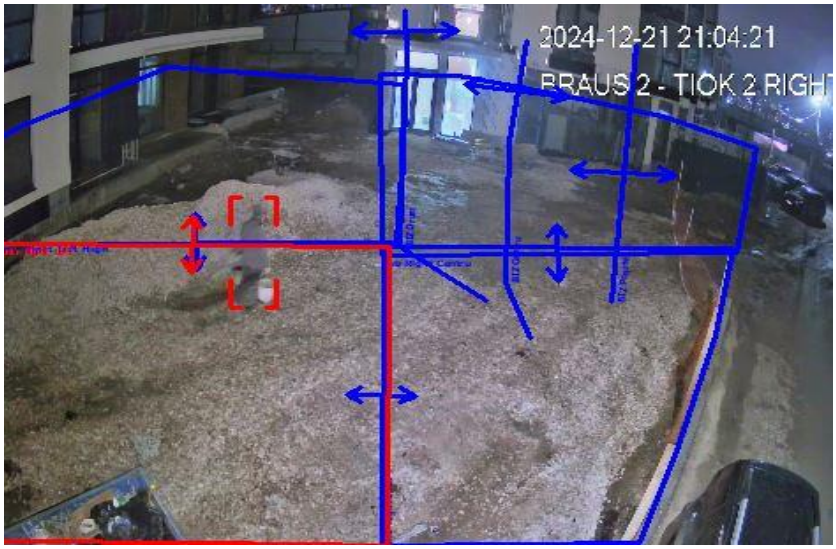
3.2. Detectarea și înregistrarea amenințărilor:

- Configurarea zonelor de alarmă în camerele de supraveghere video, cu notificări în cazul traversării acestora.
- Alarmare prin protocolul TCP/IP și prin închiderea contactului uscat pentru transmiterea semnalelor de alarmă către Hub-ul Ajax.
- Configurarea senzorilor din interiorul spațiilor pentru detectarea și înregistrarea alarmelor.

3.3. Reacția la alarme:

- Notificare automată imediată a operatorului prin funcționalitățile specializate DSS Pro și Ajax în cazul declanșării unei alarme.

În cazul declanșării unei zone de alarmă, camera trimite un semnal către server prin protocolul de schimb de date TCP/IP. Simultan, contactele uscate se închid, trimițând un semnal analogic către Hub-ul Ajax. Astfel, semnalele de alarmă sunt dublate din două surse, asigurând un nivel ridicat de protecție.

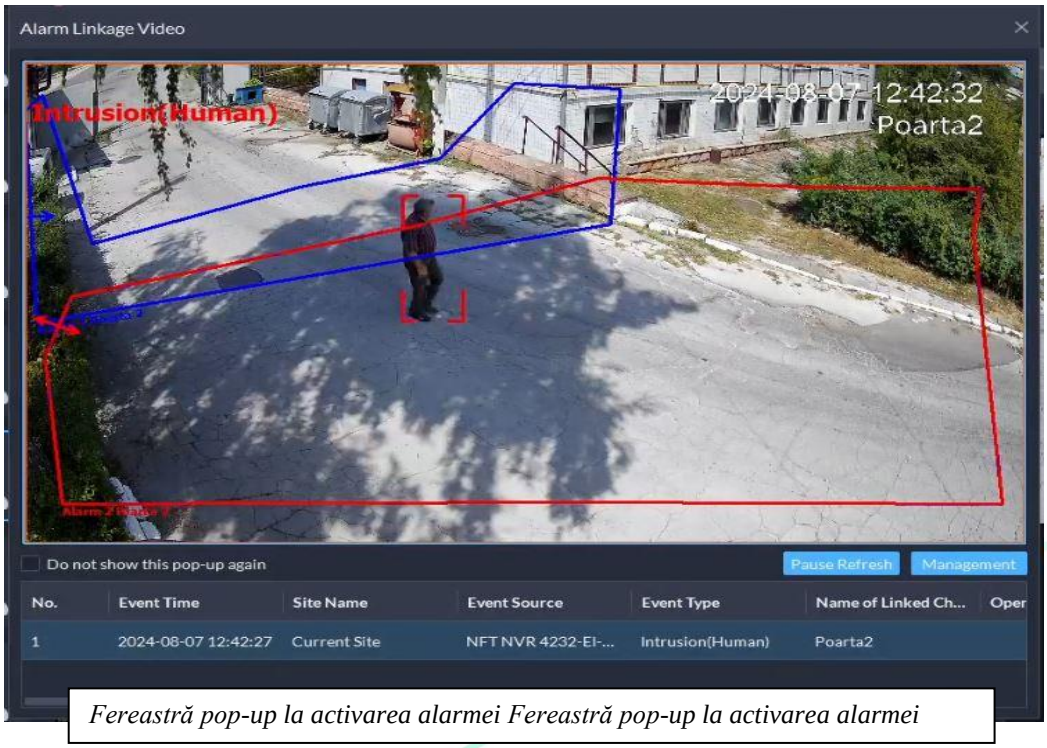


Traversarea zonei de securitate de către un potențial intrus

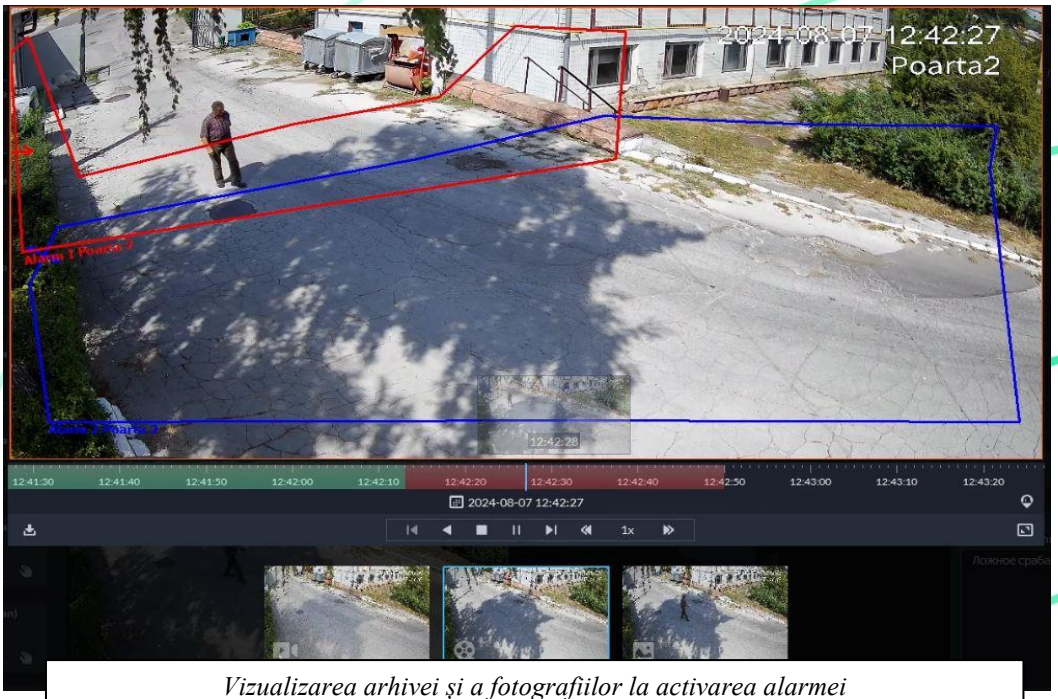
Furnizarea operatorului de fotografii și videoclipuri de la locul incidentului cu 30 de secunde înainte de producerea evenimentului pentru analiza situației.

www.securitypark.md
info@securitypark.md
+373 22 106 105

- Pe ecranul monitorului operatorului apare o fereastră pop-up cu informații detaliate de la locul evenimentului - fotografie de la locul incidentului, arhivă video cu segmentul marcat pe linia de timp, videoclipuri de la camerele adiacente conectate la acest loc, ceea ce permite vizualizarea și evaluarea rapidă a situației.



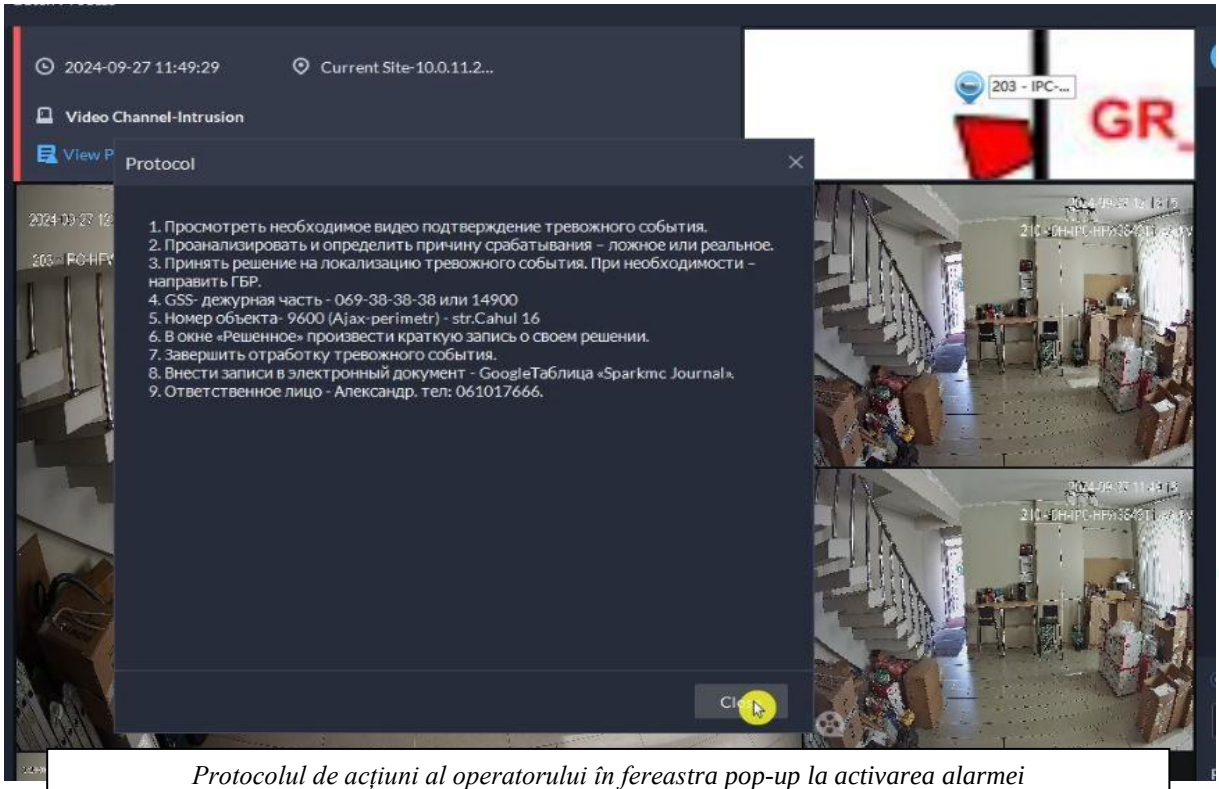
Fereastră pop-up la activarea alarmei Fereastră pop-up la activarea alarmei



Vizualizarea arhivei și a fotografiilor la activarea alarmei

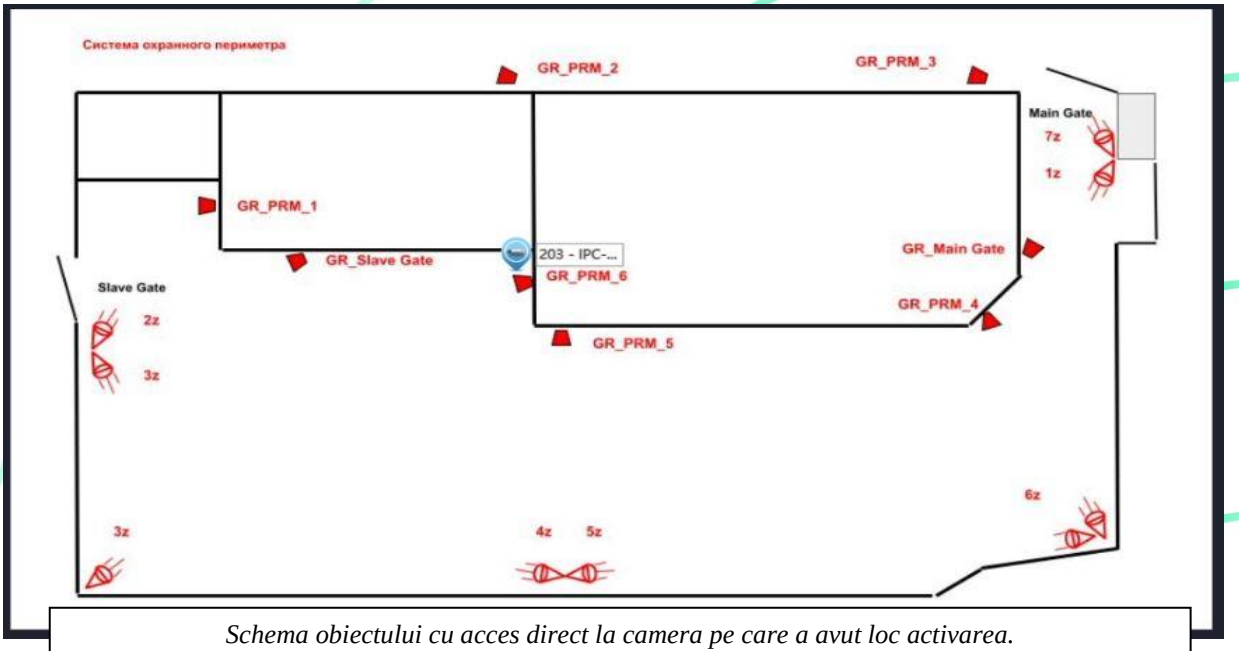
www.securitypark.md
info@securitypark.md
+373 22 106 105

- De asemenea, operatorului îi este disponibil, într-un acces rapid, în aceeași fereastră, protocolul de intervenție în caz de alarmă, cu indicarea acțiunilor necesare, numerelor de telefon de urgență și contactelor persoanelor responsabile.



Protocolul de acțiuni al operatorului în fereastra pop-up la activarea alarmei

- Tot acolo este disponibilă o hartă/schemă a obiectivului, cu zonele de securitate desenate, cu camerele amplasate pe aceasta și cu acces direct la videoclipurile de pe aceste camere.



Schema obiectului cu acces direct la camera pe care a avut loc activarea.

www.securitypark.md
info@securitypark.md
+373 22 106 105

- Analiza situației de către operator în vederea detectării unei alarme false și luarea unei decizii privind acțiunile ulterioare.

  Pe baza datelor obținute de la locul incidentului, operatorul ia o decizie rapidă (în maxim 30 de secunde) privind validitatea alarmei (de exemplu, din cauza intrării animalelor, obiectelor străine sau a altor entități în zona camerei), sau dacă situația este serioasă și necesită intervenție imediată.

  - În caz de amenințare reală: operatorul trimite o echipă de reacție rapidă (ER) la locație cu instrucțiuni detaliate despre locul și natura incidentului. Până la sosirea echipei, se menține înregistrarea video continuă și controlul situației la fața locului.

    În același timp, se activează semnalizarea luminoasă și sonoră pentru a avertiza încălcătorul că a pătruns într-o zonă interzisă și că încalcă codul penal, printr-un fișier audio sau prin contact vocal direct cu acesta.

    În cazul unor obiective mari, operatorul indică în detaliu echipei de reacție rapidă unde și în ce zonă a teritoriului protejat trebuie să ajungă pentru a reține infractorul.

  - În caz de alarmă falsă: evenimentul este procesat corespunzător în DSS și Ajax și datele sunt înregistrate în jurnal.

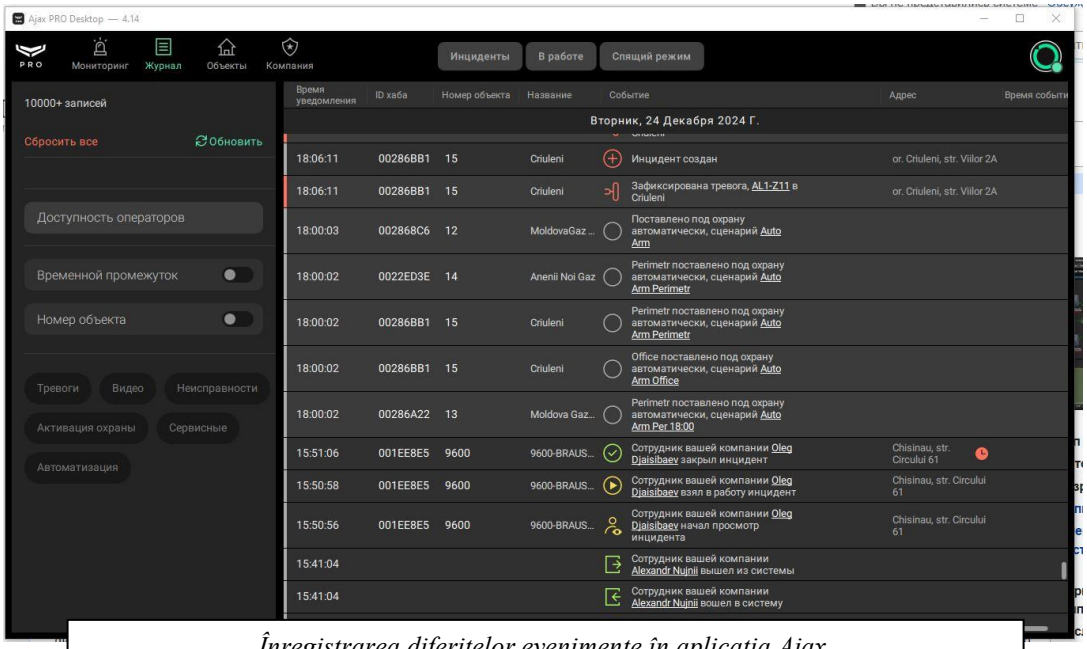
4. Informații pentru client

Notificarea și informarea clientului despre toate evenimentele care au loc la obiectiv se realizează în două moduri:

4.1. În mod normal (de lucru).

• În aplicația Ajax:

- Se înregistrează toate evenimentele legate de armarea/dezarmarea obiectivului și cine dintre utilizatori a efectuat această operațiune, dacă a avut loc în modul manual.
- Evenimente legate de defecțiuni ale echipamentului sau depanarea alimentării cu energie sau rețelei.
- Evenimente legate de încălcarea perimetrului, dar care nu sunt legate de o situație de alarmă (așa-numitele alarme false - animale, obiecte străine, condiții meteorologice nefavorabile).

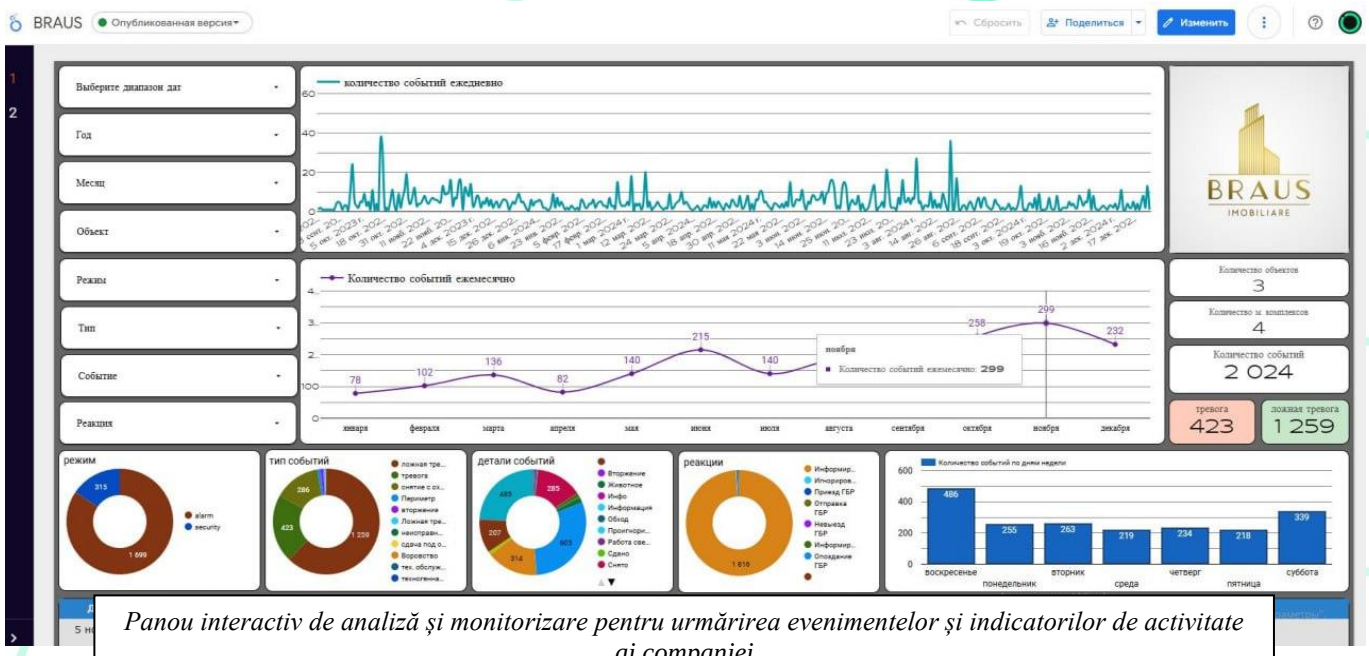


Înregistrarea diferitelor evenimente în aplicația Ajax.

- În Google Cabinet

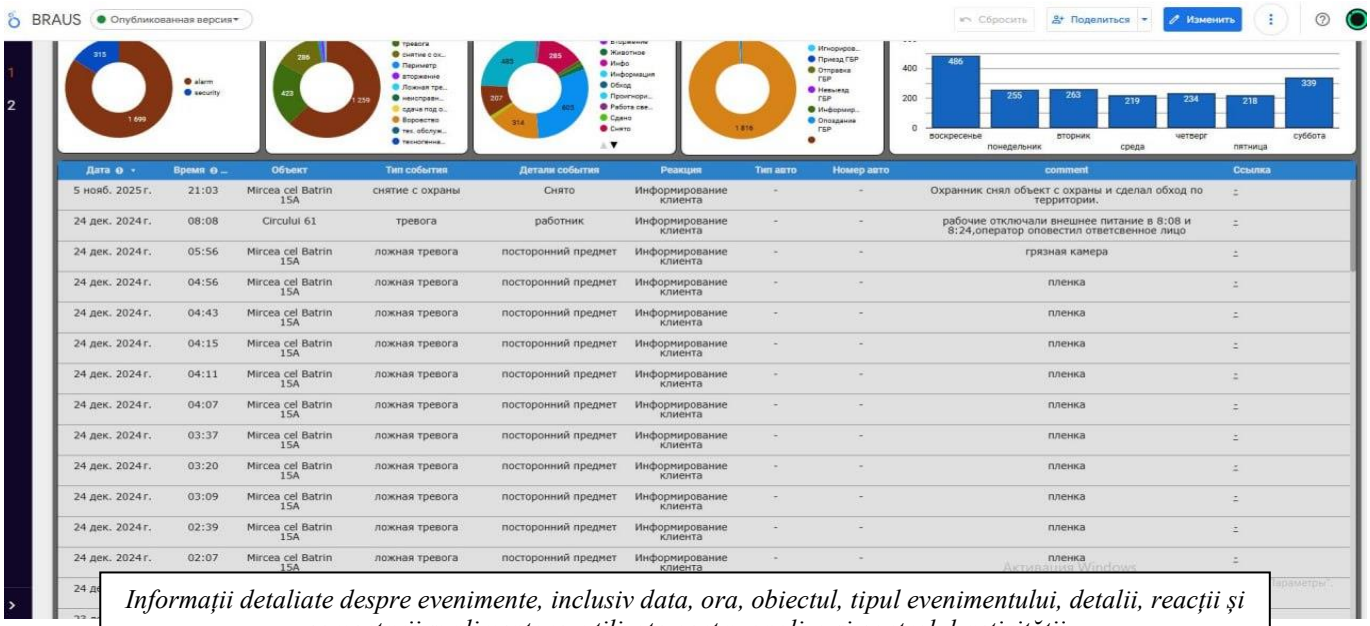
Clientului i se oferă acces permanent la aplicația Looker Studio, care conține:

- Descriere mai detaliată a evenimentelor
- Fotografii și videoclipuri de la locul evenimentelor
- Descrierea reacției operatorului la fiecare eveniment
- Analiza tipurilor de evenimente, a orei, datelor și a modurilor de reacție.



Panou interactiv de analiză și monitorizare pentru urmărirea evenimentelor și indicatorilor de activitate ai companiei

www.securitypark.md
info@securitypark.md
+373 22 106 105

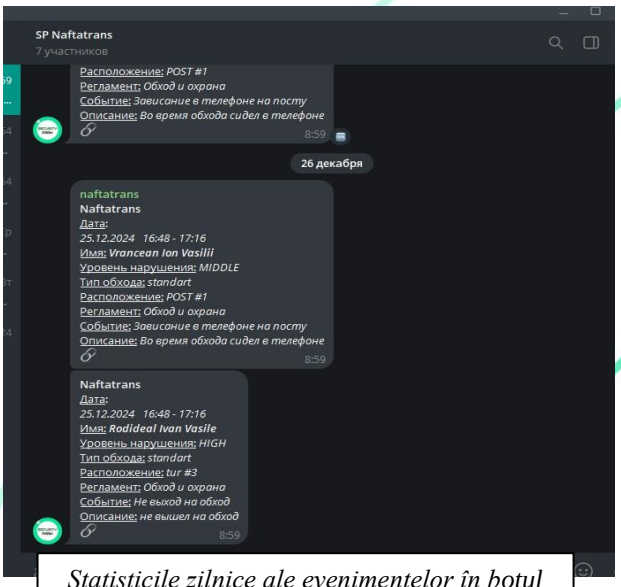


Дата	Время	Объект	Тип события	Детали события	Реакция	Тип авто	Номер авто	comment	Ссылка
5 нояб. 2025 г.	21:03	Mircea cel Batrin 15A	снятие с охраны	Снято	Информирование клиента	-	-	Охранник снял объект с охраны и сделал обход по территории.	
24 дек. 2024 г.	08:08	Circului 61	тревога	работник	Информирование клиента	-	-	рабочие отключали внешнее питание в 8:08 и 8:24,оператор оповестил ответственное лицо	
24 дек. 2024 г.	05:56	Mircea cel Batrin 15A	ложная тревога	посторонний предмет	Информирование клиента	-	-	грязная камера	
24 дек. 2024 г.	04:56	Mircea cel Batrin 15A	ложная тревога	посторонний предмет	Информирование клиента	-	-	пленка	
24 дек. 2024 г.	04:43	Mircea cel Batrin 15A	ложная тревога	посторонний предмет	Информирование клиента	-	-	пленка	
24 дек. 2024 г.	04:15	Mircea cel Batrin 15A	ложная тревога	посторонний предмет	Информирование клиента	-	-	пленка	
24 дек. 2024 г.	04:11	Mircea cel Batrin 15A	ложная тревога	посторонний предмет	Информирование клиента	-	-	пленка	
24 дек. 2024 г.	04:07	Mircea cel Batrin 15A	ложная тревога	посторонний предмет	Информирование клиента	-	-	пленка	
24 дек. 2024 г.	03:37	Mircea cel Batrin 15A	ложная тревога	посторонний предмет	Информирование клиента	-	-	пленка	
24 дек. 2024 г.	03:20	Mircea cel Batrin 15A	ложная тревога	посторонний предмет	Информирование клиента	-	-	пленка	
24 дек. 2024 г.	03:09	Mircea cel Batrin 15A	ложная тревога	посторонний предмет	Информирование клиента	-	-	пленка	
24 дек. 2024 г.	02:39	Mircea cel Batrin 15A	ложная тревога	посторонний предмет	Информирование клиента	-	-	пленка	
24 дек. 2024 г.	02:07	Mircea cel Batrin 15A	ложная тревога	посторонний предмет	Информирование клиента	-	-	пленка	

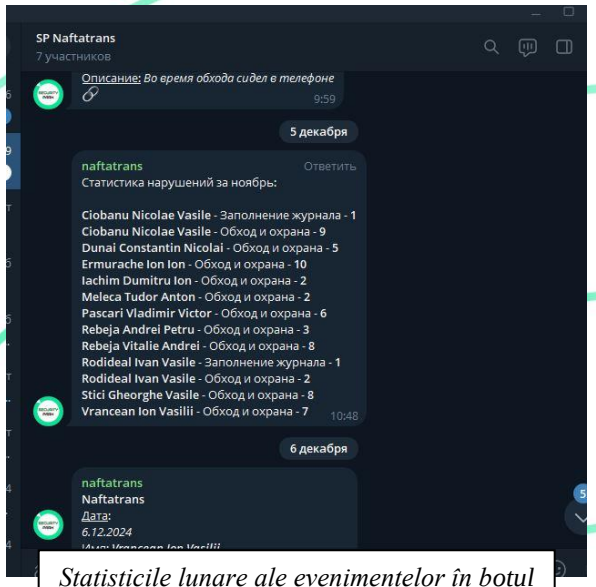
Informații detaliate despre evenimente, inclusiv data, ora, obiectul, tipul evenimentului, detalii, reacții și comentarii suplimentare, utilizate pentru analiza și controlul activității

Acest instrument asigură acces rapid și convenabil la arhiva evenimentelor de alarmă, precum și permite utilizatorului să analizeze eficiența sistemului, să identifice vulnerabilitățile și să optimizeze măsurile de securitate.

- În canalul Telegram
  - În fiecare zi, la o oră prestabilită, se trimite statistica tuturor evenimentelor de alarmă și non-alarmă sub formă de mesaje.
  - Statistica lunară pe tipuri de evenimente (dacă este necesar).



Statisticile zilnice ale evenimentelor în botul Telegram al utilizatorului



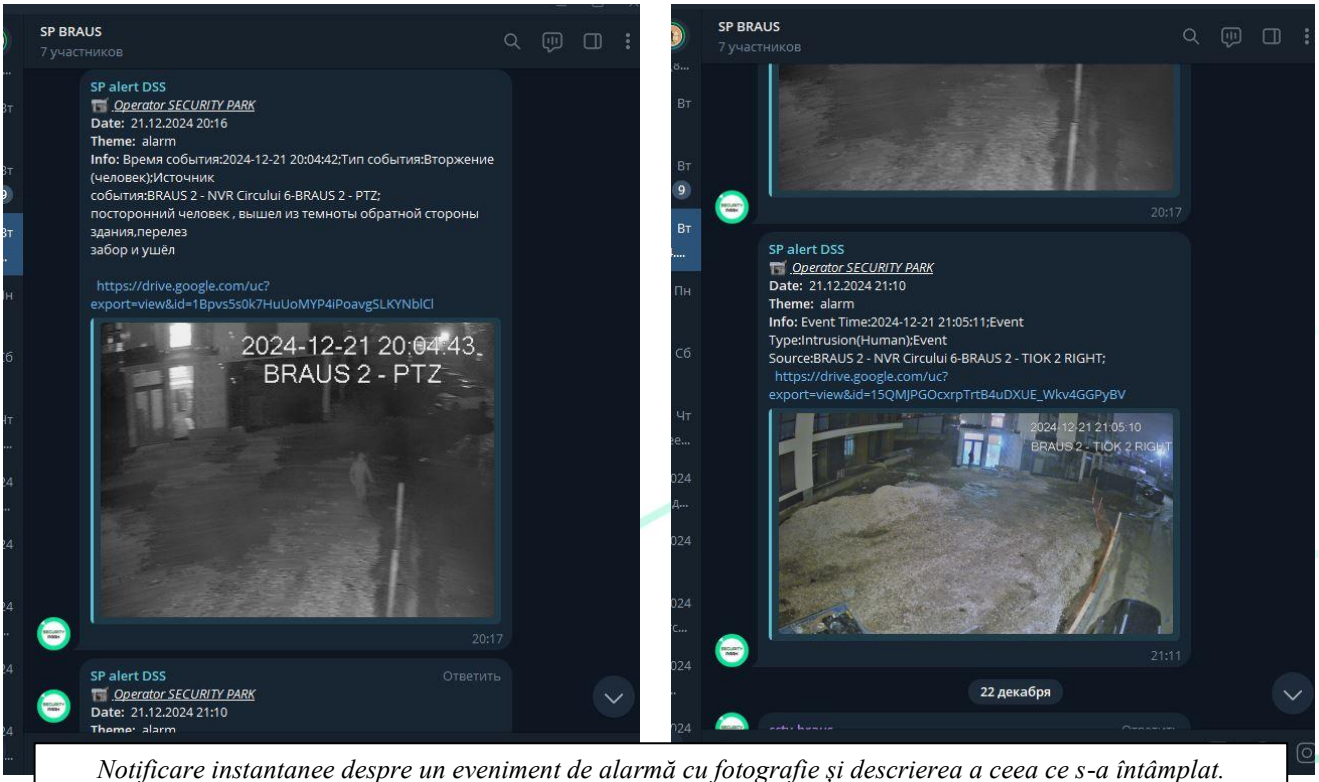
Statisticile lunare ale evenimentelor în botul Telegram al utilizatorului

www.securitypark.md
info@securitypark.md
+373 22 106 105

4.2 În regim de urgență.

În cazul unui eveniment real (de alarmă), utilizatorul primește o notificare în termen de 60 de secunde, care include o fotografie de la locul evenimentului și o descriere a ceea ce s-a întâmplat:

- În canalul Telegram
- Pe email (dacă este necesar)



Notificare instantanee despre un eveniment de alarmă cu fotografie și descrierea a ceea ce s-a întâmplat.

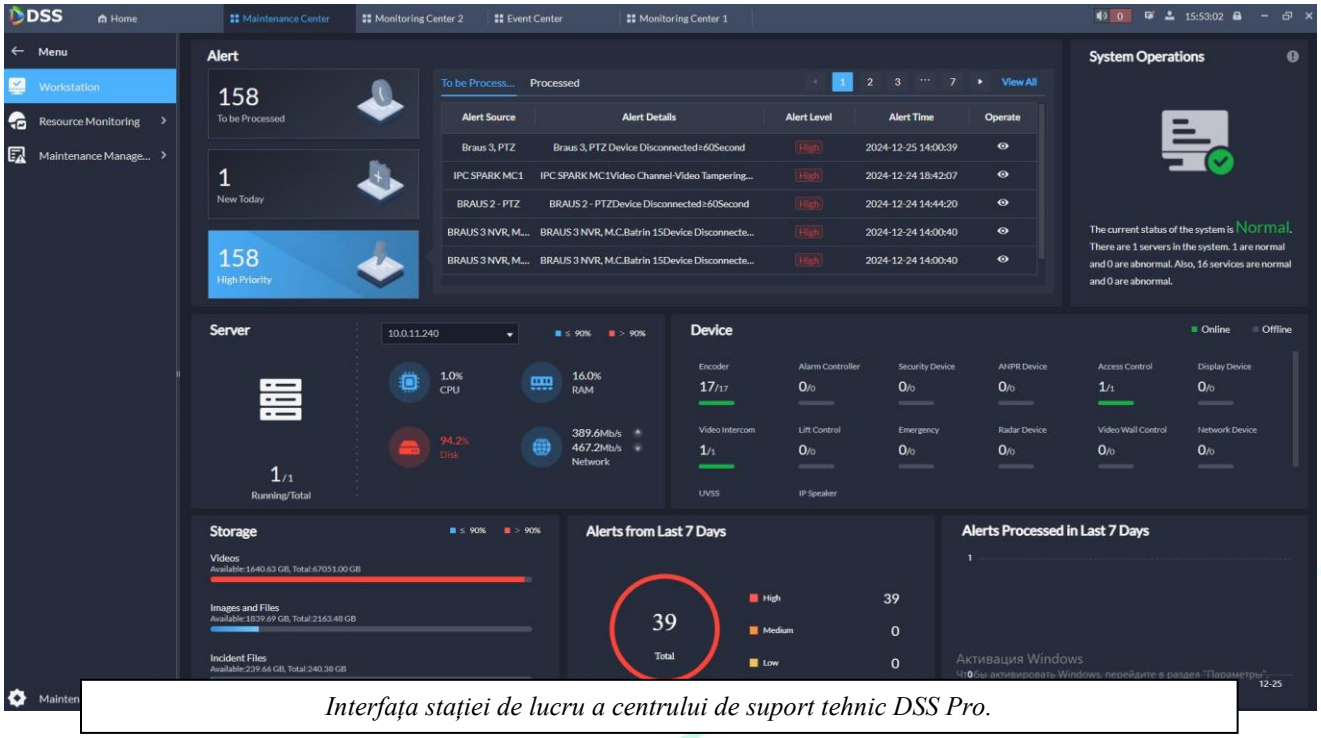
Astfel, se realizează informarea imediată a utilizatorului despre evenimentul de alarmă care a avut loc la obiectiv.

5. Monitorizarea stării tehnice și întreținerea sistemului

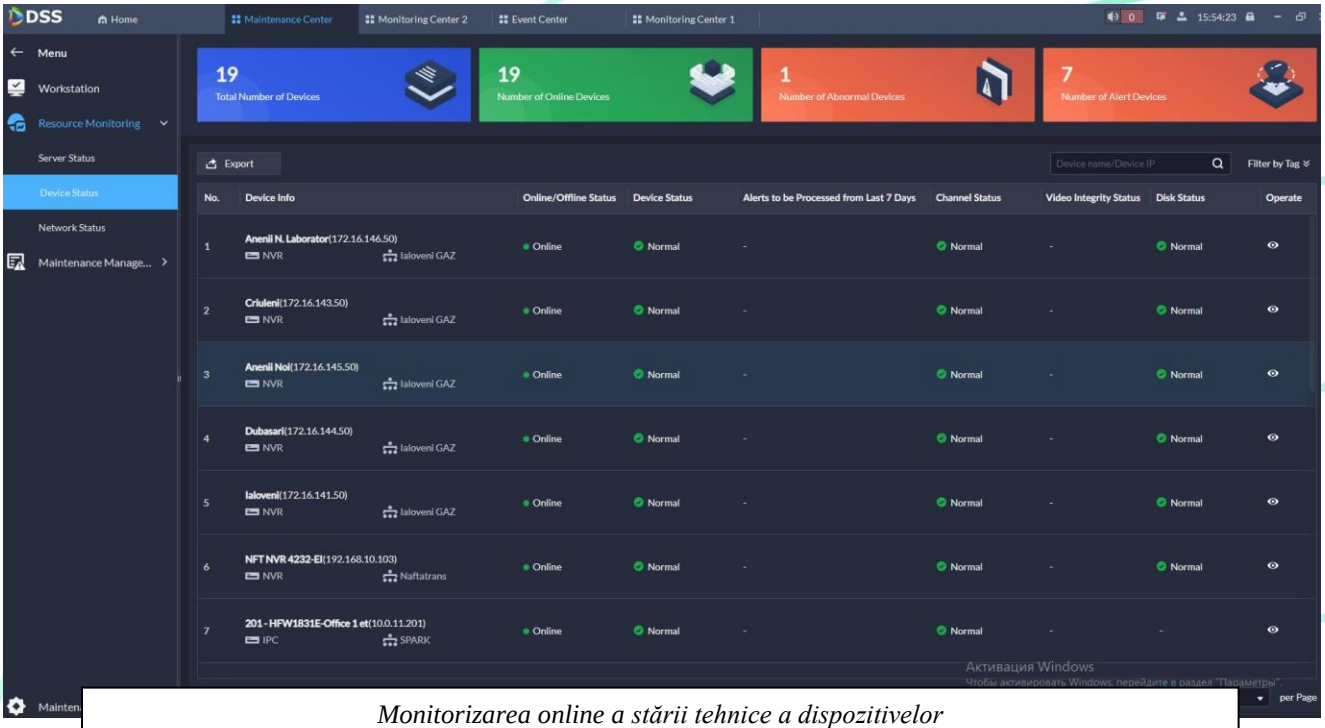
5.1. Funcționalitatea de monitorizare

Pentru monitorizarea stării tehnice a sistemului se utilizează software specializat DSS Pro, care include funcționalitatea Maintenance Center. Acest instrument asigură:

- Monitorizarea elementelor cheie ale sistemului (înregistratoare, camere, routere) în regim 24/7.
- Generarea de evenimente (events) în cazul unor defecțiuni, cum ar fi schimbarea unghiului, deplasarea, întunecarea, oprirea alimentării, pierderea rețelei etc.

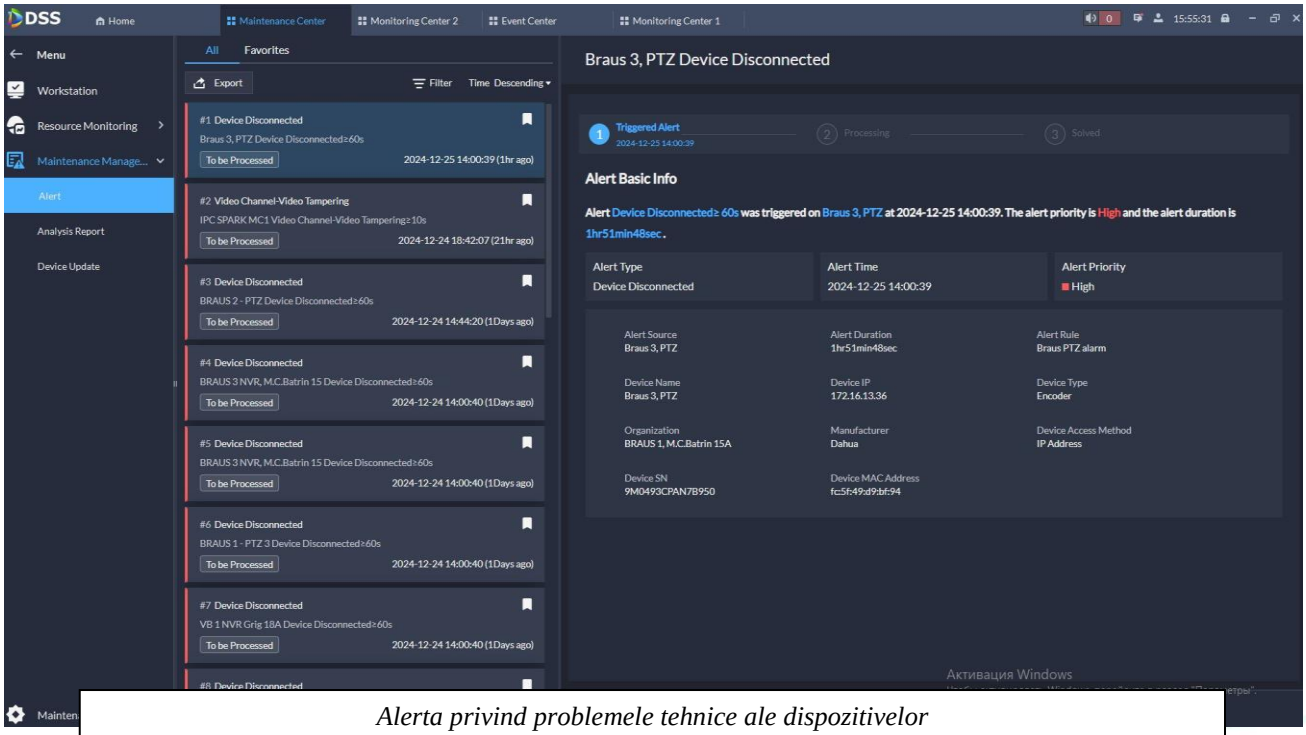


Interfața stației de lucru a centrului de suport tehnic DSS Pro.



Monitorizarea online a stării tehnice a dispozitivelor

www.securitypark.md
info@securitypark.md
+373 22 106 105

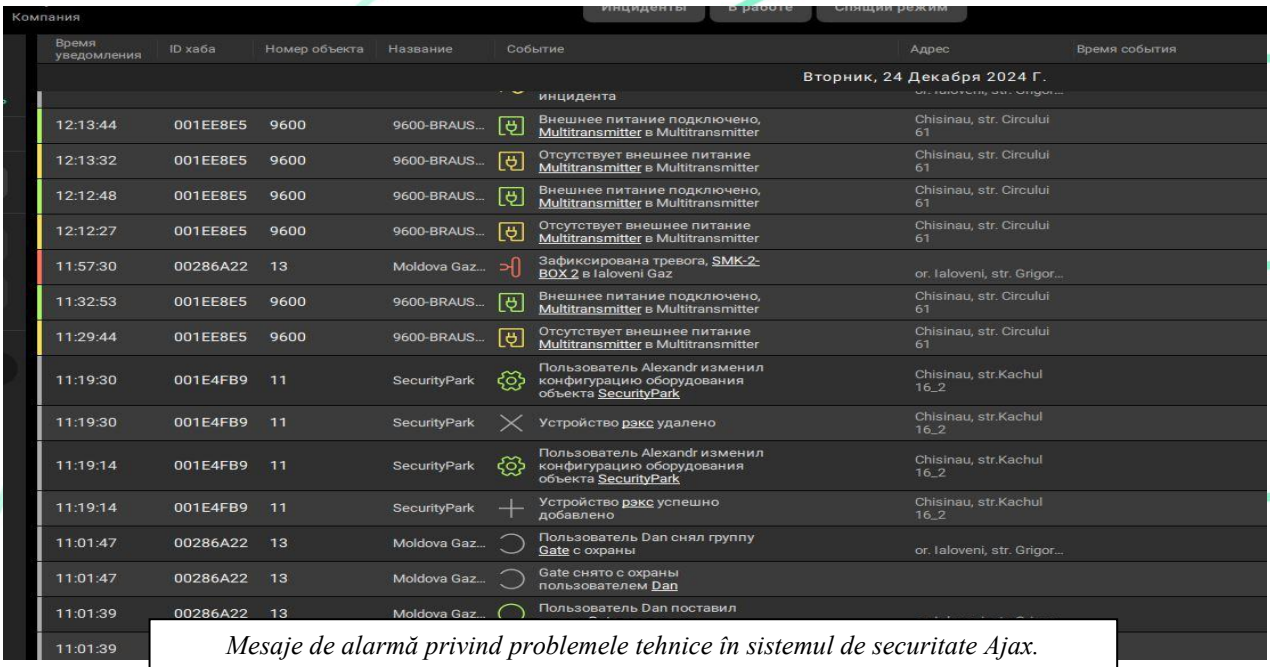


Alerta privind problemele tehnice ale dispozitivelor

De asemenea, în DSS Pro și Ajax este implementată funcționalitatea de generare a alarmelor în cazul unor defecțiuni critice, cum ar fi:

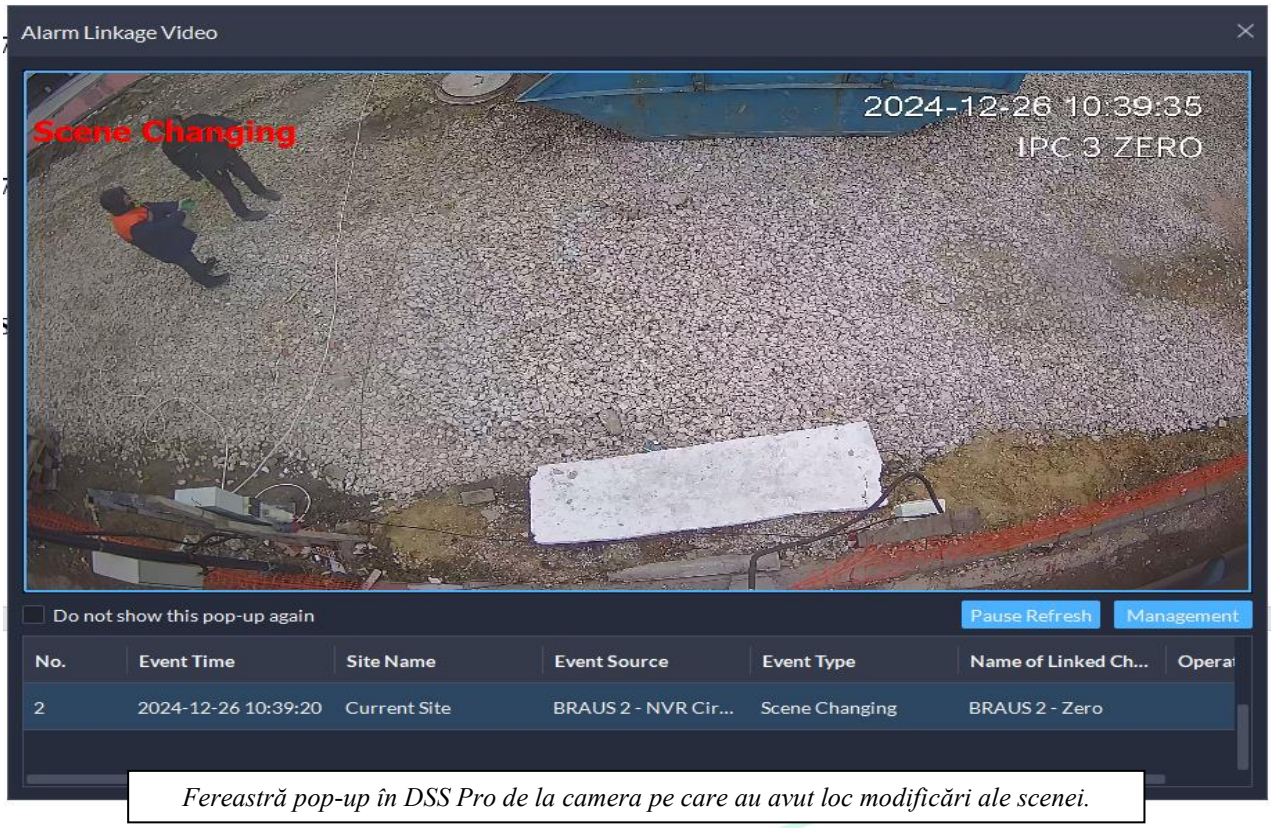
- Oprirea alimentării multitransmitterului.
- Pierderea semnalului de la cameră pe termen lung.

Mesajele despre probleme sunt trimise operatorului prin notificări de alarmă în Ajax și prin ferorțele pop-up în DSS Pro.

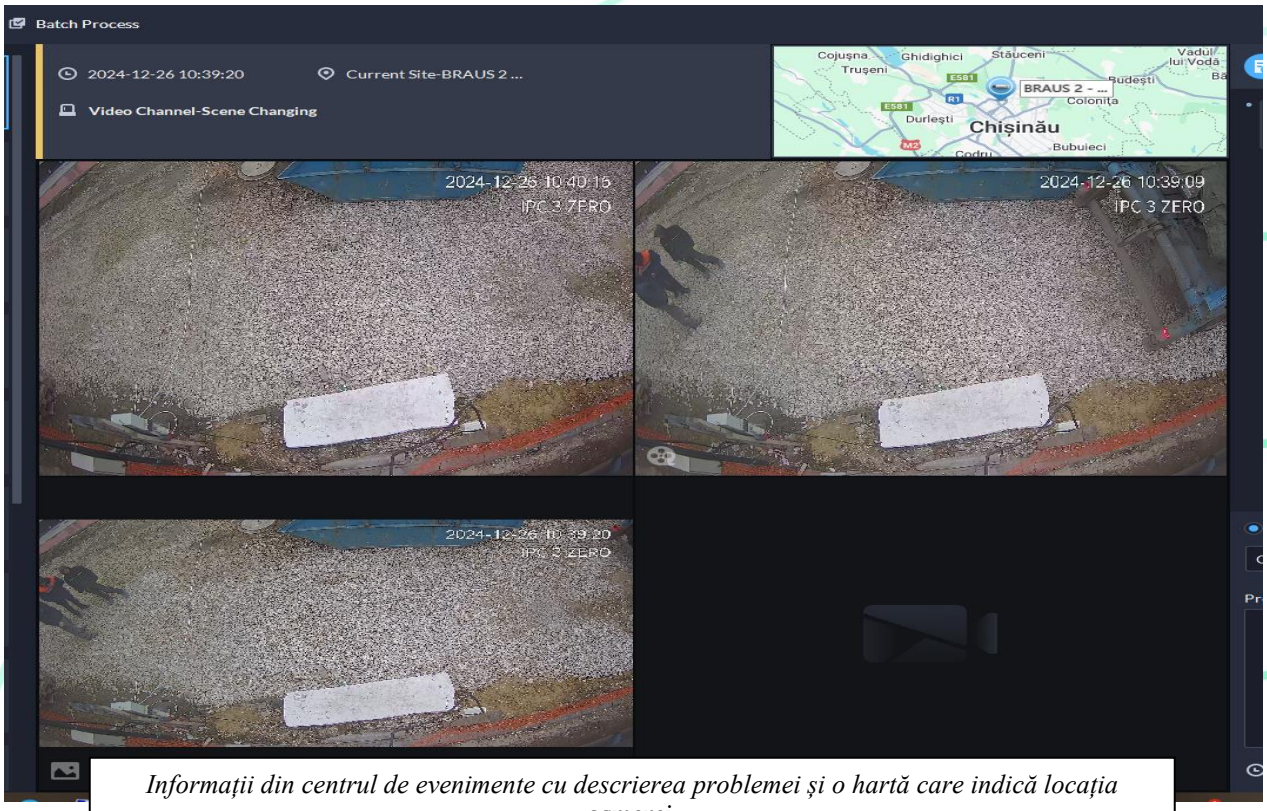


Mesaje de alarmă privind problemele tehnice în sistemul de securitate Ajax.

www.securitypark.md
info@securitypark.md
+373 22 106 105



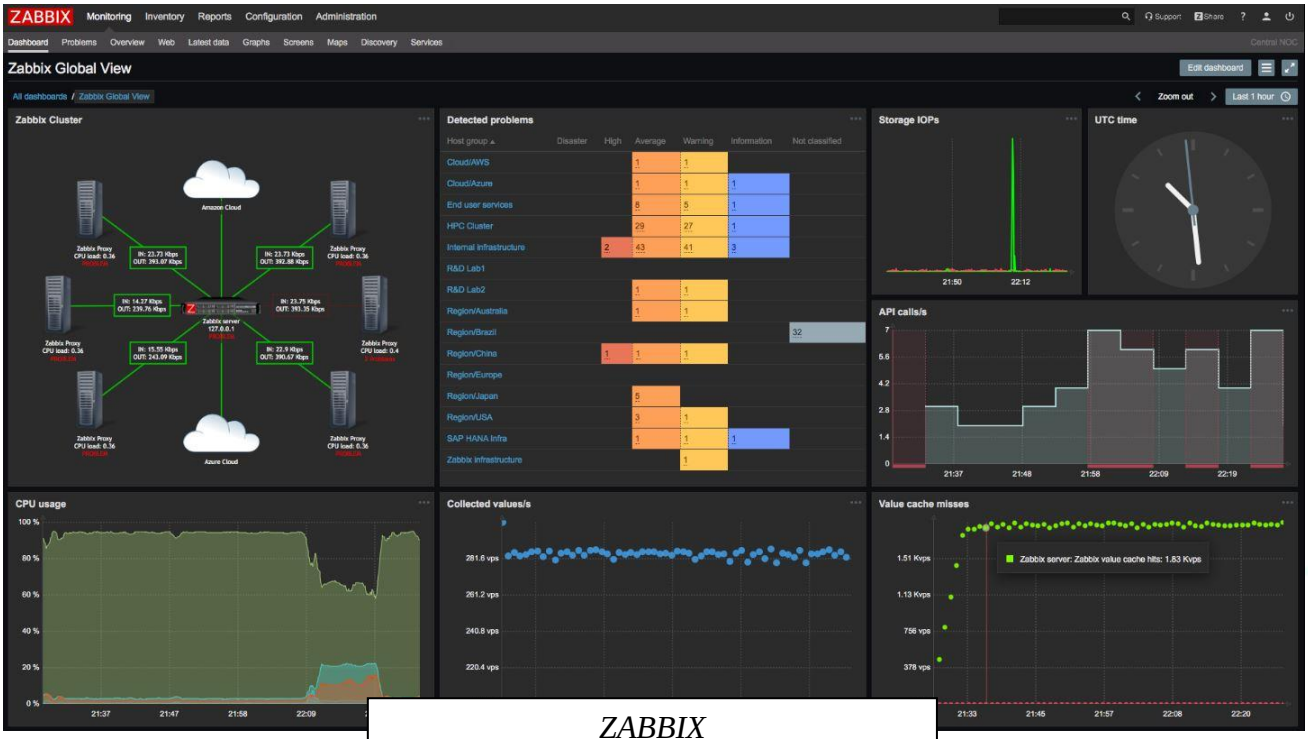
Fereastră pop-up în DSS Pro de la camera pe care au avut loc modificări ale scenei.



Informații din centrul de evenimente cu descrierea problemei și o hartă care indică locația camerei.

www.securitypark.md
info@securitypark.md
+373 22 106 105

Pentru duplicare se utilizează Zabbix – un sistem liber de monitorizare a statusurilor diverselor servicii de rețea, servere și echipamente de rețea, care notifică administratorii despre problemele apărute la echipamentele monitorizate.



ZABBIX

5.2. Acțiunile operatorului în caz de evenimente

1. **Analiza evenimentului:**
   - La primirea unui eveniment (event), operatorul trebuie să verifice situația dispozitivului în timp real.
   - Se examinează arhiva cu un minut înainte de eveniment pentru a clarifica circumstanțele.
2. **Reacția la amenințări:**
   - În cazul unei amenințări la echipament cauzate de un infractor, operatorul:
     - Acționează conform protocolului de pătrundere.
     - Trimite echipa de reacție rapidă (ER).
     - Notifică persoanele responsabile.
3. **Reacția la defecțiuni tehnice:**
   - În cazul defecțiunilor tehnice minore, operatorul notifică serviciul de suport tehnic prin chat în Telegram în termen de 30 de minute de la descoperirea acestora.
   - În caz de defecțiuni la echipamente critice (hub, switch, router principal, blocuri de alimentare):
     - Operatorul trebuie să notifice serviciul de suport tehnic prin apel telefonic.
     - Se realizează monitorizarea directă a obiectivului utilizând echipamentele disponibile până la sosirea echipei tehnice.
4. **Termenele de remediere a defecțiunilor:**
   - Serviciul de suport tehnic asigură remedierea defecțiunilor în termen de 24 de ore.

- În cazul în care repararea nu este posibilă din motive obiective, înlocuirea echipamentului se face în termen de 72 de ore.

5.3. Reacția la situații de urgență

1. **Deconectarea prelungită a alimentării electrice la obiectiv:**
   - Se notifică serviciul de suport tehnic și reprezentantul utilizatorului prin apel telefonic și mesaj în Telegram.
   - Ulterior, conform acordului prealabil, care nu face parte din obligațiile și funcționarea sistemului de monitorizare, utilizatorul asigură fie conectarea unui generator de rezervă, fie un post de pază fizică la obiectiv.
2. **Pierderea rețelei:**
   - Se activează canalul de rezervă pe baza transmisiei de date prin rețele mobile 4G, cu limitarea traficului la 500 GB, minimizându-se traficul.
   - În cazul unei întreruperi prelungite a canalului principal, se va extinde pachetul de rezervă conform acordului prealabil cu utilizatorul.

5.4. Măsuri suplimentare

- Testarea periodică a tuturor elementelor sistemului pentru a confirma funcționarea corectă a acestora.
- Actualizarea reglementărilor și a instrucțiunilor, ținând cont de noi situații de urgență posibile.

6. Securitatea datelor

- Conformitatea cu cerințele legale privind protecția datelor personale.
- Criptarea datelor de supraveghere video este asigurată de MikroTik utilizând VPN WireGuard pe protocoale proprietare.
- Jurnalele de evenimente sunt asigurate printr-un set de măsuri specializate, conform protocoalelor interne (autentificare cu doi factori).
- Realizarea de backup regulat al înregistrărilor pe dispozitive independente.
- Perioada de păstrare a arhivelor: minimum 180 de zile.

7. Asigurarea rezilienței sistemului

7.1. Alimentare de rezervă:

- Utilizarea surselor de alimentare neîntreruptibile (UPS) pentru toate componentele critice ale sistemului pentru cel puțin 12 ore și a unui generator pentru cel puțin 3 zile.

7.2. Dublarea canalelor de comunicare:

- Disponibilitatea unei conexiuni internet de rezervă pentru transmiterea datelor.

- Utilizarea mai multor protocoale de comunicare independente (TCP/IP, comunicații radio).

7.3. Echipamente de rezervă:

- Disponibilitatea camerelor, senzorilor și altor componente de rezervă pentru înlocuirea rapidă a elementelor defecte.

8. Scalabilitatea sistemului

- Posibilitatea de a adăuga noi zone de supraveghere și de a integra echipamente suplimentare, după necesități, este asigurată prin funcționalitatea standard a DSS Pro, Ajax și Intelligent Flex Management Plug-in.
- Flexibilitate în configurarea sistemului pentru a se adapta la particularitățile fiecărui obiectiv.

9. Integrarea cu alte sisteme de securitate

9.1. Compatibilitatea echipamentului: Sistemul de monitorizare proactivă a securității suportă integrarea cu majoritatea sistemelor moderne de securitate, inclusiv:

- **Sisteme de control al accesului (SCA):** posibilitatea de a gestiona accesul la obiectiv în mod automat și manual.
- **Sisteme de securitate la incendiu:** sincronizarea semnalelor de incendiu și posibilitățile de notificare a operatorilor și utilizatorilor.
- **Sisteme de alarmă:** centralizarea semnalelor de alarmă pentru gestionare centralizată.
- **Sisteme inteligente de gestionare a clădirilor (BMS):** configurarea scenariilor automate (de exemplu, oprirea aparatelor de aer condiționat sau a lifturilor în caz de evenimente de alarmă).

9.2. Protocole de integrare:

- Se utilizează protocoale API standard pentru conectarea dispozitivelor suplimentare și asigurarea funcționării diferitelor sisteme într-un mediu unificat.
- Suport pentru protocoale proprietare ale producătorilor de echipamente.

10. Interfața utilizatorului

10.1. Platforma web:

- Acces convenabil prin browser pentru gestionarea sistemului, vizualizarea înregistrărilor și configurarea setărilor.
- Interfață intuitivă cu panou de control pentru reacție operativă.

10.2. Aplicația mobilă:

- Suport pentru platformele iOS și Android pentru a primi notificări și a gestiona sistemul din orice locație.

- Posibilitatea de a pune/înlătura zone de la securitate, vizualizarea evenimentelor de alarmă și obținerea analizei.

10.3. Cabinete personale:

- Pentru administratorii sistemului: acces la setări, analize și protocoale de evenimente.
- Pentru utilizatori: acces la rapoarte, notificări și funcții de bază pentru gestionarea obiectivelor.

11. Instruire și suport pentru utilizatori

11.1. Instruirea operatorilor:

- Organizarea unui curs introductiv pentru operarea sistemului pentru operatorii centrului de monitorizare.
- Instruire periodică pentru îmbunătățirea calificării, ținând cont de noile funcționalități ale sistemului.

11.2. Instruirea utilizatorilor finali:

- Organizarea de sesiuni introductive pentru utilizatorii sistemului.
- Furnizarea de materiale educaționale (tutoriale video, ghiduri, manuale).

11.3. Suport tehnic:

- Suport 24/7 prin chat, telefon sau email.
- Timp de răspuns la solicitări: maximum 30 de minute în timpul orelor de lucru.
- Actualizări regulate ale software-ului și testarea sistemului.

12. Concluzie

Sistemul de monitorizare proactivă a securității reprezintă o soluție modernă pentru asigurarea securității obiectivelor de infrastructură. Flexibilitatea, fiabilitatea și capacitatea sa de a se adapta nevoilor utilizatorilor îl fac un instrument eficient pentru prevenirea incidentelor și reacționarea rapidă la amenințări.

Digitally signed by Nicora Alexandru
Date: 2024.12.26 19:27:59 EET
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ