DOI: https://doi.org/10.53486/sstc2026.v1.105

CZU: 004.056.53:004.8(478)

SECURIZAREA FLUXURILOR DE DATE PRIN PLATFORMA MCONNECT UTILIZÂND TEHNOLOGII DE DETECȚIE A AMENINȚĂRILOR BAZATE PE INTELIGENȚĂ ARTIFICIALĂ

SECURING DATA FLOWS THROUGH THE MCONNECT PLATFORM USING AI-BASED THREAT DETECTION TECHNOLOGIES

LESNIC Andrei, student, specialitatea: Cibernetică și Informatică Economică
Academia de Studii Economice din Moldova,
str. Bănulescu-Bodoni 61, Chișinău, Republica Moldova,
Telefon: +373 78 597 665
e-mail autor: andrei.lesnic.zfdi@ase.md

Abstract: *This paper explores the integration of Artificial Intelligence (AI) for securing data flows within the Republic of Moldova's Interoperability Platform, MConnect. In the context of the Digital Transformation Strategy 2023–2030 and the rising threats of hybrid warfare, the study analyzes the shift from traditional rule-based security to AI-driven anomaly detection. The research methodology combines a comparative analysis of the Zero Trust Architecture (ZTA) and the technical evolution of the MConnect Events infrastructure. The results highlight that using machine learning models to establish "normative boundaries" for institutional data exchange significantly enhances threat detection accuracy (exceeding 91%) and enables real-time automated response. The study concludes that AI-powered security is essential for achieving cyber resilience and aligning with European Union standards like NIS2 and the AI Act.*
Key words: *MConnect, Artificial Intelligence, Zero Trust Architecture, Cyber Security, Interoperability, Anomaly Detection, Digital Public Infrastructure.*
JEL CLASSIFICATION: O33, K24, H11

INTRODUCERE

Republica Moldova se află într-un moment de cotitură tehnologică, digitalizarea serviciilor publice devenind pilonul central al agendei de modernizare a statului. Această transformare, accelerată de criza COVID-19, a dus la o creștere exponențială a volumului de date schimbate între instituții, dar și a vulnerabilităților în fața războiului hibrid. Platforma MConnect, care procesează circa 2,5 milioane de mesaje zilnic, reprezintă infrastructura critică ce necesită mecanisme avansate de protecție. Obiectivul acestei cercetări este de a demonstra cum integrarea Inteligenței Artificiale (IA) poate asigura securizarea acestor fluxuri prin trecerea de la modelele de securitate perimetrală la arhitecturi de tip Zero Trust, capabile de detecție proactivă a amenințărilor.

CONȚINUTUL DE BAZĂ

Analiză succintă a surselor bibliografice în domeniul problemei cercetate Literatura de specialitate subliniază că modelele de securitate tradiționale au devenit ineficiente în fața atacurilor complexe și automatizate. Cercetările recente ale lui Mangla (2023) propun utilizarea IA pentru a extinde capacitățile de detecție în infrastructuri cloud și IoT, eliminând „încrederea implicită”. La nivel național, „Strategia de transformare digitală 2023-2030” și „Programul Național de Securitate Cibernetică 2026-2030” stabilesc cadrul strategic pentru implementarea „Cyber Shield”, o rețea de centre de securitate dotate cu IA. Studiile realizate în cadrul institutului Cybercor accentuează rolul factorului uman și necesitatea utilizării învățării automate pentru a prezice comportamentele de risc în nodurile umane ale rețelei.

Descrierea metodelor de cercetare utilizate Cercetarea utilizează o abordare mixtă, combinând modelarea conceptuală a arhitecturii Zero Trust cu analiza tehnică a componentelor platformei MConnect. S-a analizat evoluția platformei de la utilizarea middleware-ului WSO2 către

arhitectura modernă bazată pe evenimente (MConnect Events), care utilizează Apache Kafka pentru procesarea datelor în timp real. Metodologia de detecție a anomaliilor a fost evaluată prin compararea modelelor de învățare supervizată (Random Forest, XGBoost) și nesupervizată (Isolation Forest), necesare pentru definirea barierelor normative de schimb de date între ministere.

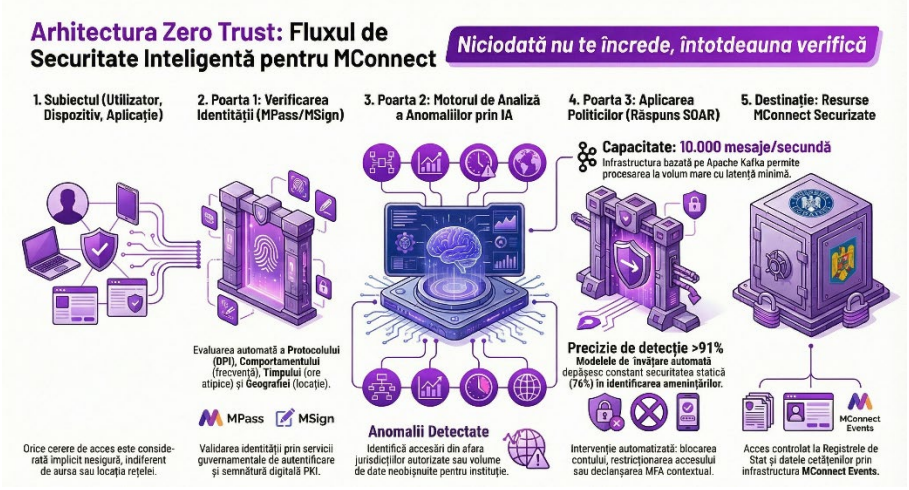


Figura 1. Arhitectura de Securitate Zero Trust (ZTA)
Sursa: NIST SP 800-207, Mangla(2023)

Rezultatele obţinute Rezultatele analizei indică faptul că integrarea IA în ecosistemul MConnect oferă o precizie de detecție a amenințărilor de peste 91%, depășind constant modelele statice care ating doar 76%. Utilizarea „MConnect Events" permite sincronizarea datelor în câteva secunde, oferind granularitatea necesară pentru antrenarea modelelor de IA pe date de tip serie temporală. S-au identificat patru categorii principale de anomalii detectabile prin IA în fluxurile MConnect:

Tabelul 1. Clasificarea anomaliilor detectabile prin IA în fluxurile MConnect

Categoria Anomaliei	**Descriere Tehnică**	**Metodă de Detecție/Impact**
Protocol	Detecția pachetelor neconforme prin inspecție profundă (**Deep Packet Inspection**)	Identificarea atacurilor la nivel de rețea și a datelor corupte
Comportamentală	Cereri de date neobișnuite ca **volum sau frecvență** pentru o instituție	Detectarea exfiltrării masive de date sau a accesului abuziv
Temporală	Accesări la **ore atipice**, nespecifice regimului administrativ standard	Semnalarea utilizării neautorizate a acreditărilor în afara programului
Geografică	Tentative de autentificare din **afara jurisdicțiilor autorizate**	Blocarea accesului de la adrese IP externe sau regiuni suspecte

Sursa: Mangla(2023)

Sistemele de tip SOAR (Security Orchestration, Automation, and Response) pot iniția intervenții rapide, cum ar fi suspendarea automată a acreditărilor MPass în cazul detectării unui atac de tip „credential-stuffing".

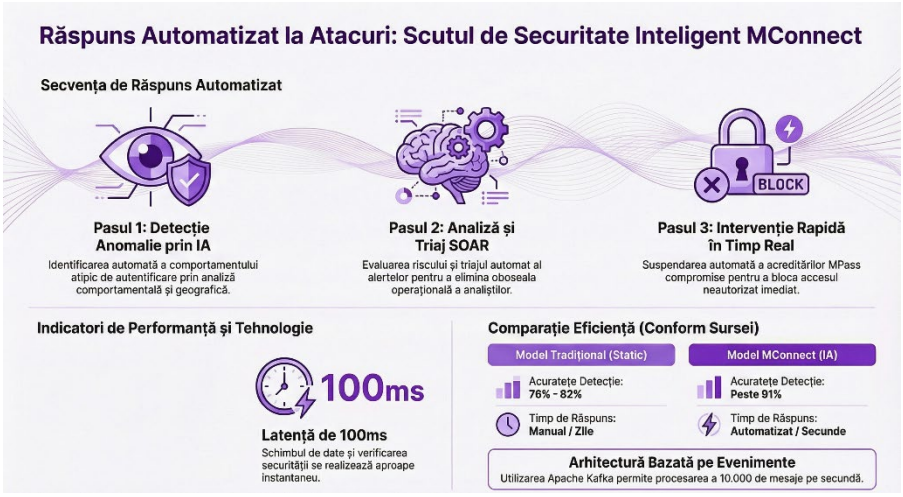


Figura 2. Răspunsul SOAR la atacuri de tip „credential-stuffing”
Sursa: Cloud Security Alliance Romania

CONCLUZIE

Cercetarea demonstrează că securizarea fluxurilor de date prin MConnect utilizând IA nu este doar o opțiune tehnologică, ci o necesitate pentru reziliența statului digital. Se recomandă operaționalizarea completă a Agenției pentru Securitate Cibernetică și interconectarea platformei naționale cu „Cyber Shield”-ul european. Moldova trebuie să continue investițiile în capitalul uman prin Cybercor pentru a gestiona complexitatea sistemelor de risc ridicat conform AI Act. Implementarea principiului „securizat prin proiectare” și adoptarea standardelor globale de hardware și software vor asigura o integrare sigură în Piața Unică Digitală a UE.

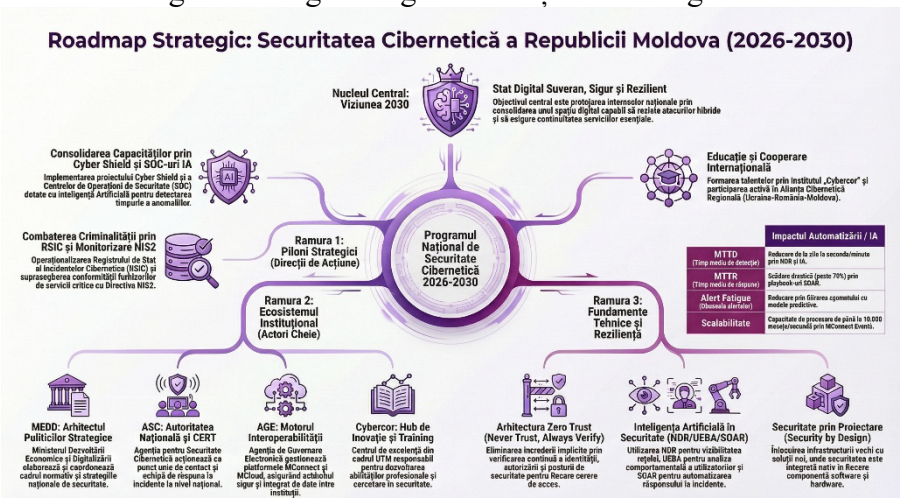


Figura 3. Roadmap Strategic al Securității Cibernetice (2026-2030)
Sursa: Programului Național de Securitate Cibernetică 2026-2030

REFERINȚE:

1. Agenția de Guvernare Electronică. (2025). *MConnect Events: The Intelligent Infrastructure Revolutionizing Real-Time Data Exchange*. [Online]. Disponibil la: https://egov.md/en/node/40817. Accesat la 24 martie 2026.
2. Guvernul Republicii Moldova. (2023). *Hotărâre Nr. HG650/2023 din 06.09.2023 cu privire la aprobarea Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030*. Monitorul Oficial nr. 383-386.
3. Mangla, M. (2023). AI-Driven Zero Trust Architecture: A Scalable Framework for Threat Detection and Adaptive Access Control. *International Journal Science and Technology, 2*(3), 117-124. https://doi.org/10.56127/ijst.v2i3.2274.
4. Ministerul Dezvoltării Economice și Digitalizării. (2025). *Programul Național de Securitate Cibernetică 2026–2030*. Aprobat prin Hotărârea Guvernului nr. 821/2025.
5. Parlamentul Republicii Moldova. (2023). *Legea nr. 48 din 16.03.2023 privind securitatea cibernetică*. Monitorul Oficial nr. 124-127.

6. Țurcanu, D., Peca, L., Prisacaru, A., & Țurcanu, T. (2025). Cyber Security Professional Development within Cybercor. *Journal of Engineering Science, 32*(2), 87-98. https://doi.org/10.52326/jes.utm.2025.32(2).08.
7. Cloud Security Alliance Romania. (2026, 4 februarie). *AI-driven Security Operations (SecOps) Across Multi-Framework Environments to Empower Organizations – Webinar*. [Online]. Disponibil la: https://cloudsecurityalliance.ro/event/ai-driven-security-operations/.
8. Ministerul Dezvoltării Economice și Digitalizării. (2025). *Programul Național de Securitate Cibernetică 2026–2030*. Aprobat prin Hotărârea Guvernului nr. 821/2025.
9. National Institute of Standards and Technology. (2020). *NIST Special Publication 800-207: Zero Trust Architecture*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207.

Coordonator științific: ȚURCAN Aurelia, conf. univ., dr.
Academia de Studii Economice din Moldova, str. Bănulescu-Bodoni 61,
Chișinău, Republica Moldova
Telefon: +373 69 255 595
e-mail: turcan.aurelia.4u8h@ase.md