MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software şi Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.

„___" _____ 2026

ANALIZA PROCESELOR TEHNICE ÎN CADRUL MANAGEMENTULUI IDENTITĂȚII ȘI ACCESULUI

Proiect de master

Student: _____ **Parşov Nadejda, TIA-241M**

Coordonator: _____ **Ludmila Peca, conf. univ.,dr**

Consultant: _____ **Cojocaru Svetlana, asist.univ.**

Chişinău, 2026

REZUMAT

Teza de master „Analiza proceselor tehnice în cadrul managementului identității şi accesului”, autor Parşov Nadejda, specialitatea Tehnologia informaţiei pentru afaceri, Chişinău, 2026

Structura lucrării: Introducere, 3 capitole, Concluzii, Bibliografie din 71 surse, 3 anexe, 69 pagini de text de bază.

Cuvinte cheie: IAM, identitate digitală, Active Directory, SIEM, securitate informațională.

Scopul şi obiectivele tezei: Scopul lucrării constă în analiza proceselor tehnice specifice managementului identităților și accesului, precum și în evaluarea modului în care integrarea serviciilor de directoare cu sisteme de tip SIEM contribuie la monitorizarea și analiza evenimentelor de securitate în mediile organizaționale. În vederea realizării acestui scop, au fost stabilite următoarele obiective: analiza conceptelor fundamentale IAM și a componentelor arhitecturale acestuia; examinarea soluțiilor de tip serviciu de directoare, cu accent pe Active Directory; analiza arhitecturii și funcționalitățile sistemului SIEM Splunk; investigarea rolului tehnologiilor de inteligență artificială și machine learning în procesele de securitate; implementarea și configurarea unei soluții integrate bazate pe Active Directory și SIEM; interpretarea rezultatelor obținute în urma integrării acestor tehnologii.

Metodologia cercetării: Cercetarea se bazează pe o abordare metodologică mixtă, care combină analiza teoretică a literaturii de specialitate, a standardelor și a bunelor practici internaționale, cu o componentă aplicativă realizată prin metoda studiului de caz. În cadrul lucrării au fost utilizate metode precum analiza, sinteza, comparația și modelarea arhitecturală, precum și configurarea și integrarea unor sisteme informatice într-un mediu controlat, în vederea simulării unui scenariu organizațional real.

Importanţa teoretică şi practică a lucrării: Importanța teoretică a lucrării constă în sistematizarea conceptelor, principiilor și cadrului normativ aferent managementului identității și accesului, precum și în evidențierea rolului acestuia în securitatea informațională. Din punct de vedere practic, lucrarea contribuie prin realizarea unei implementări simulate a unei soluții integrate bazate pe Active Directory și SIEM, demonstrând modul în care aceste tehnologii pot fi utilizate pentru monitorizarea activităților utilizatorilor, detectarea comportamentelor anormale și susținerea proceselor de audit și securitate. Rezultatele obținute pot constitui un suport relevant pentru proiectarea și implementarea unor soluții IAM adaptate cerințelor mediului organizațional contemporan.

ABSTRACT

Master's Thesis "Analysis of Technical Processes within Identity and Access Management", author Parşov Nadejda, specialization Information Technologies for Business, Chişinău, 2026

Thesis's structure: Introduction, three chapters, Conclusions, Bibliography (71 sources), 3 annexes, 69 pages of main text.

Key words: IAM, digital identity, Active Directory, SIEM, information security.

The thesis's aim and targets: The aim of the thesis is to analyze the technical processes specific to identity and access management, as well as to evaluate how the integration of directory services with SIEM systems contributes to the monitoring and analysis of security events in organizational environments. In order to achieve this purpose, the following objectives have been established: the analysis of fundamental IAM concepts and its architectural components; the examination of directory service solutions, with a focus on Active Directory; the analysis of the architecture and functionalities of Splunk SIEM system; the investigation of the role of artificial intelligence and machine learning technologies in security processes; the implementation and configuration of an integrated solution based on Active Directory and SIEM; as well as the evaluation of the results obtained from the integration of these technologies.

Research Methodology: The research is based on a mixed methodological approach that combines theoretical analysis of specialized literature, standards, and international best practices with an applied component developed through the case study method. The study employs methods such as analysis, synthesis, comparison, and architectural modeling, as well as the configuration and integration of information systems within a controlled environment in order to simulate a real organizational scenario.

Theoretical and practical importance of the study: The theoretical significance of the thesis lies in the systematization of concepts, principles, and the regulatory framework related to Identity and Access Management, as well as in highlighting its role in information security. From a practical perspective, the thesis contributes through the simulated implementation of an integrated solution based on Active Directory and SIEM, demonstrating how these technologies can be used to monitor user activities, detect abnormal behavior, and support audit and security processes. The obtained results may serve as a relevant reference for the design and implementation of IAM solutions adapted to the requirements of modern organizational environments.

CUPRINS

ABREVIERI ŞI DEFINIȚII

IAM (Identity and Access Management)- Managementul Identităților și Accesului

AD -Active Directory- Serviciu de director Active Directory

SIEM (Security Information and Event Management)- Sistem de management al informațiilor și evenimentelor de securitate

IT- Tehnologia informației

Guest- vizitator, oaspete

MAC (Media Access Control)- un identificator unic alocat fiecărui dispozitiv de rețea, fie ca este vorba de un calculator, un smartphone, o imprimanta sau orice alt dispozitiv care utilizează o interfață de rețea.

PC- computer personal

ID- șir unic de caractere, cifre sau document utilizat pentru a identifica în mod unic o persoană, un dispozitiv, un cont sau un obiect într-un sistem

IP (Internet Protocol)- cod numeric unic care identifică un dispozitiv (computer, telefon, router) într-o rețea locală sau pe internet, facilitând comunicarea.

GPS- Sistemul de poziționare global

AI- Inteligență Artificială

ML (Machine Learning)- Învățare automată

MFA- Autentificare multifactor

RBAC (Role-Based Access Control)- Control al accesului bazat pe roluri

ABAC (Attribute-Based Access Control)- Control al accesului bazat pe atribute

ISO/IEC 27001- Standard internațional pentru Sistemul de Management al Securității Informației

ISO/IEC 27002- Standard complementar ISO/IEC 27001 care oferă ghiduri de implementare pentru controalele de securitate informațională.

NIST SP 800-63- ghid NIST pentru gestionarea identității digitale, autentificare și niveluri de asigurare a identității.

NIST SP 800-53- Ghid NIST privind controalele de securitate pentru sistemele informatice și organizaționale.

CIA- Triada CIA – Confidențialitate, Integritate, Disponibilitate

InfoSec (Information Security)- Securitatea informațională

Zero Trust- Model de securitate „zero încredere”

VPN (Virtual Private Network)- Rețea virtuală privată

PII (Personally Identifiable Information)- Informații de identificare personală

IoT (Internet of Things)- Internetul lucrurilor

DoS (Denial of Service)- Atac de tip refuz de serviciu

RFID- Identificarea prin frecvență radio, tehnologie fără fir care utilizează unde radio pentru a identifica, urmări și gestiona obiecte sau persoane, constând dintr-o etichetă (cip și antenă) și un cititor.

Token- element de securitate digitală, o reprezentare virtuală a unui activ sau un obiect fizic (dispozitiv) folosit pentru autentificare, autorizare și securizare

Firewall- sistem de securitate (software sau hardware) care monitorizează și controlează traficul de rețea, blocând accesul neautorizat și protejând datele sensibile

AAA- Autentificare, Autorizare, Audit

IDC-Corporația Internațională de Date- organizație globală de cercetare de piață, analiză și consultanță în domeniul tehnologiilor informaționale, telecomunicațiilor și electronicii de consum. Aceasta furnizează studii, prognoze și analize privind tendințele tehnologice.

DNS (Domain Name System)- sistem utilizat pentru traducerea numelor de domenii în adrese IP, facilitând astfel localizarea resurselor în rețea.

LDAP- Lightweight Directory Access Protocol (Protocol Ușor de Acces la Directoare) un protocol standard utilizat pentru accesarea și administrarea serviciilor de directoare distribuite, fiind frecvent utilizat pentru autentificare și gestionarea utilizatorilor în rețele.

Single Sign-On-Autentificare unică- mecanism de autentificare care permite unui utilizator să acceseze mai multe aplicații sau sisteme informatice utilizând un singur set de credențiale.

AD DS -Active Directory Domain Services- omponenta principală a serviciilor Active Directory, responsabilă pentru stocarea și gestionarea informațiilor despre resursele din rețea și pentru autentificarea și autorizarea utilizatorilor.

AD LDS -Active Directory Lightweight Directory Services- Constituie o versiune flexibilă a serviciilor de directoare, care nu necesită implementarea unui domeniu Active Directory complet, fiind utilizată pentru aplicații specifice.

AD CS -Active Directory Certificate Services- infrastructura de gestionare a certificatelor digitale, utilizată pentru implementarea criptografiei cu cheie publică și pentru securizarea comunicațiilor.

AD FS -Active Directory Federation Services- serviciu care permite autentificarea federată, oferind utilizatorilor posibilitatea de a accesa resurse externe pe baza identității interne.

AD RMS - Active Directory Rights Management Services- serviciu destinat protecției informațiilor prin controlul accesului și al utilizării documentelor digitale, inclusiv prevenirea copierii sau distribuirii neautorizate.

OU- **Organizational Units-** Unitățile organizaționale

Multimaster- model de replicare în care mai multe controlere de domeniu pot efectua modificări asupra datelor, acestea fiind ulterior sincronizate între toate nodurile.

GPO-Group Policy Objects- Obiecte de Politică de Grup- mecanisme utilizate pentru configurarea și controlul mediului de lucru al utilizatorilor și calculatoarelor dintr-un domeniu, prin aplicarea de politici centralizate.

RPC- Remote Procedure Call- Apel de Procedură la Distanță-protocol care permite unui program să execute proceduri pe un alt sistem din rețea, fără a gestiona explicit detaliile comunicării.

Dashboard- interfață grafică ce prezintă informații sintetizate și indicatori relevanți, facilitând monitorizarea și analiza sistemelor sau proceselor.

UEBA- User and Entity Behavior Analytics - analiza comportamentală a utilizatorilor.

IBM- International Business Machines- corporație multinațională din domeniul tehnologiei informației, cunoscută pentru dezvoltarea de hardware, software și servicii IT, inclusiv soluții de inteligență artificială și cloud computing.

Proxmox Virtual Environment (Proxmox VE)- – platformă de virtualizare open-source utilizată pentru crearea și administrarea mașinilor virtuale și a containerelor într-un mediu centralizat.

Domain Controller (DC)- server responsabil pentru gestionarea autentificării utilizatorilor, aplicarea politicilor de securitate și administrarea resurselor într-un domeniu Active Directory.

RAM- memorie volatilă utilizată pentru stocarea temporară a datelor și a instrucțiunilor necesare procesării în timp real.

CPU- unitatea centrală de procesare responsabilă pentru executarea instrucțiunilor și controlul operațiilor sistemului.

Brute-force- tip de atac cibernetic care presupune încercarea repetată a diferitelor combinații de parole sau credențiale în scopul obținerii accesului neautorizat.

Dashboard- interfață vizuală utilizată pentru reprezentarea grafică a datelor și monitorizarea în timp real a evenimentelor sau indicatorilor de performanță.

Forwardere- componentă software utilizată pentru colectarea și transmiterea datelor (logurilor) de la sistemele sursă către un server central, în cadrul unei platforme SIEM.

Index- structură logică utilizată pentru stocarea și organizarea datelor colectate, facilitând căutarea și analiza acestora în cadrul platformei SIEM.

Remote Desktop (RDP)- protocol de comunicație utilizat pentru accesul la distanță la un sistem informatic prin intermediul unei interfețe grafice.

Remote- termen utilizat pentru a descrie accesul sau operarea unui sistem de la distanță, fără prezență fizică directă asupra acestuia.

INTRODUCERE

Actualitatea temei investigate. Transformarea digitală accelerată a mediului de afaceri și a instituțiilor publice a condus la o creștere semnificativă a volumului de date gestionate, precum și a numărului de utilizatori și sisteme care accesează resurse informatice. În acest context, identitățile digitale și conturile de utilizator au devenit elemente centrale în asigurarea securității informaționale, reprezentând principalul mecanism de control al accesului la date, aplicații și servicii. Odată cu digitalizarea proceselor de business, datele au devenit unul dintre cele mai valoroase active ale organizațiilor, iar compromiterea acestora poate genera pierderi financiare semnificative, afectarea reputației și consecințe juridice sau de conformitate.

Într-o lume interconectată, domeniul IAM a devenit o componentă esențială a securității cibernetice, reflectând nevoia tot mai mare de protejare a ecosistemelor digitale și a informațiilor sensibile. Pe măsură ce organizațiile se bazează tot mai mult pe transformarea digitală, soluțiile IAM nu mai pot fi considerate opționale, dar au devenit vitale pentru protejarea datelor, asigurarea conformității și menținerea integrității operaționale. Iar integrarea soluțiilor de tip Active Directory cu sisteme avansate SIEM, dotate cu tehnologii de inteligență artificială și învățare automată, oferă premise reale pentru creșterea capacității organizațiilor de a detecta, preveni și răspunde eficient la incidente de securitate. Astfel, tema investigată se înscrie în preocupările actuale ale domeniului securității informație și răspunde unor nevoi concrete ale mediului de afaceri modern.

Scopul şi obiectivele cercetării. Scopul prezentei lucrări constă în analiza și implementarea proceselor tehnice specifice managementului identităților și accesului, prin integrarea serviciilor de directoare cu un sistem de tip SIEM în vederea îmbunătățirii securității informaționale în mediile organizaționale.

În vederea atingerii acestui scop, au fost stabilite următoarele **obiective**:

- analiza conceptelor fundamentale privind managementul identităților și accesului, inclusiv componentele arhitecturale și rolul acestora în securitatea informațională;
- studierea soluțiilor de tip serviciu de directoare, cu accent pe rolul și funcționalitățile platformei Active Directory în administrarea utilizatorilor și a resurselor;
- analiza arhitecturii și funcționalitățile sistemului SIEM Splunk în procesul de colectare, corelare și analiza evenimentelor de securitate;
- cercetarea rolului tehnologiilor de inteligență artificială și machine learning în procesul de monitorizare și detecție a incidentelor;
- proiectarea și implementarea unei soluții integrate AD–SIEM pentru gestionarea și monitorizarea conturilor de utilizator.

Suportul metodologic şi teoretico-ştiinţific al lucrării. Cercetarea se bazează pe o abordare mixtă, care îmbină analiza literaturii de specialitate cu aplicarea practică a conceptelor studiate într-un scenariu de

implementare. Baza metodologică include analiza critică a bibliografiei de specialitate, studiilor de cercetare, surselor electronice, publicațiilor statistice, articolelor științifice, etc. în domeniul subiectului studiat. În cadrul lucrării au fost utilizate în primul rînd, metodele general-științifice și principiile acesteia: analiza, observația, sinteza, inducția, deducția, cât și metodele științifice de cercetare empirică: observația, descrierea, explicarea, studiul comparat, care au contribuit la o mai bună conceptualizare a subiectului cercetat.

Suportul teoretico-științific este asigurat prin raportarea la literatura de specialitate, standarde și cadre de referință recunoscute la nivel internațional, precum și la modele moderne de arhitectură de securitate, precum Zero Trust. Componenta practică este realizată prin metoda studiului de caz, având ca obiect implementarea și evaluarea unui sistem de management al identităților și al accesului într-un mediu organizațional. De asemenea, sunt utilizate metode comparative pentru evaluarea diferitelor soluții tehnice având în vedere criterii precum arhitectura sistemelor, funcționalitățile oferite, nivelul de securitate asigurat, gradul de integrare cu infrastructurile existente și impactul asupra proceselor operaționale.

Noutatea științifică a lucrării. Noutatea lucrării constă în abordarea integrată a managementului conturilor de utilizator prin corelarea dintre mecanismele IAM, platforma Active Directory și un sistem SIEM avansat, extins cu funcționalități bazate pe inteligență artificială și machine learning. Prin analiza modului în care evenimentele generate de infrastructura IAM pot fi corelate și interpretate inteligent în cadrul unui sistem SIEM, lucrarea propune o perspectivă practică asupra îmbunătățirii capacității de detecție a comportamentelor anormale și a tentativelor de acces neautorizat. Această integrare depășește abordările tradiționale, orientate preponderent pe administrarea izolată a identităților, și evidențiază rolul analitic avansat al SIEM-urilor moderne în consolidarea securității identităților digitale.

Importanța teoretică și practică a lucrării. Din punct de vedere teoretic, lucrarea contribuie la sistematizarea și aprofundarea conceptelor de management al identităților digitale, conturilor de utilizator și control al accesului, prin integrarea acestora într-un cadru unitar care corelează securitatea informațională cu arhitecturile moderne IAM. Analiza comparativă a standardelor și bunelor practici oferă un suport conceptual util pentru cercetători și practicieni interesați de proiectarea soluțiilor IAM.

Din perspectivă practică, rezultatele obținute pot fi utilizate ca model de referință pentru implementarea unor soluții integrate AD–SIEM în organizații reale, contribuind la îmbunătățirea securității operaționale, la reducerea riscurilor asociate gestionării necorespunzătoare a conturilor de utilizator și la creșterea capacității de detecție și răspuns la incidente de securitate. Lucrarea oferă, totodată, recomandări aplicabile pentru îmbunătățirea proceselor de administrare a identităților și pentru consolidarea mecanismelor de control al accesului în mediile IT moderne.

BIBLIOGRAFIE

1. Silverfort: *User Account Explained* [accesat 04.02.2026] Disponibil: https://www.silverfort.com/glossary/user-account/#:~:text=There%20are%20several%20types%20of,Standard%20user%20accounts
2. GAREY, Lorna. *What Is Digital Identity?*, 19 septembrie 2024 [accesat 04.02.2026] Disponibil: https://www.oracle.com/asean/security/identity-management/digital-identity/
3. Silverfort: *Identity and Access Management (IAM)* [accesat 06.02.2026] Disponibil: https://www.silverfort.com/glossary/identity-and-access-management-iam/
4. KISSEL, Richard. *Glossary of Key Information Security Terms*, 3 iulie 2019 [accesat 08.02.2026] Disponibil: https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf
5. MASIUTIN, Maxim. *Lecture 1: Core Concepts and Terminology in Information Security* [Suport de curs]. [accesat 14.02.2026] Disponibil: https://else.fcim.utm.md/pluginfile.php/184160/mod_resource/content/1/Lecture_01_Core_Concepts_EN.pdf
6. CISCO: *What is cybersecurity?* [accesat 08.02.2026] Disponibil: https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html
7. Dot Security: *Identity and Access Management (IAM) Standards,* 7 octombire 2024 [accesat 08.02.2026] Disponibil: https://dotsecurity.com/insights/blog-identity-access-management-standards
8. Identity Management Institute Blog: *AAA Identity and Access Management Framework Model* [accesat 09.02.2026] Disponibil: https://identitymanagementinstitute.org/identity-and-access-management-model/
9. IBM: *What is information security (InfoSec)?* [accesat 14.02.2026] Disponibil: https://www.ibm.com/think/topics/information-security#:~:text=Information%20security%20is%20an%20umbrella,and%20organizational%20policies%20and%20procedures.
10. Fortinet: *What Is the CIA Triad?*, 2025 [accesat 14.02.2026] Disponibil: https://www.fortinet.com/resources/cyberglossary/cia-triad?
11. National Institute of Standards and Technology. (2020). *An Introduction to Information Security (SP 800-12 Rev.1)*. [accesat 14.02.2026] Disponibil: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf
12. GeeksforGeeks: *What is Information Security?* [accesat 14.02.2026] Disponibil: https://www.geeksforgeeks.org/computer-networks/what-is-information-security/

13. International Standard ISO/IEC 27001 *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* [accesat 14.02.2026] Disponibil: https://km.thainsw.net/kmdcs/images/File/ISO%2027001-2022%20rm.pdf
14. International Standard ISO/IEC 27002 *Information technology — Security techniques — Code of practice for information security management* [accesat 14.02.2026] Disponibil: https://portalcip.org/wp-content/uploads/2019/07/ISO27001.pdf
15. CISCO: *What Is Zero-Trust Networking?* [accesat 15.02.2026] Disponibil: https://www.cisco.com/site/us/en/learn/topics/networking/what-is-zero-trust-networking.html
16. NIST SP 800-63 *Digital Identity Guidelines-SP 800-63B-4 Authentication & Authenticator Management* [accesat 15.02.2026] Disponibil: https://pages.nist.gov/800-63-4/sp800-63b.html#abstract
17. NIST SP 800-53: *Security and Privacy Controls for Information Systems and Organizations* [accesat 15.02.2026] Disponibil: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
18. Fortinet: *IT Security Policy: An Overview* [accesat 16.02.2026] Disponibil: https://www.fortinet.com/resources/cyberglossary/it-security-policy#:~:text=An%20Information%20Technology%20(IT)%20security,than%20a%20set%20of%20strategies.
19. LockBaud: *IT Policies and Procedures: Your Comprehensive Guide* [accesat 16.02.2026] Disponibil: https://lockbaud.com/it-policies-and-procedures/
20. IDMWORKS: *13 Latest Trends in Identity and Access Management,* 25 august 2025 [accesat 07.04.2026]. Disponibil: https://www.idmworks.com/insight/latest-trends-in-identity-and-access-management/#:~:text=IAM%20as%20a%20Managed%20Service,with%20best%20practices%20and%20compliance.
21. RADOVAN, Semančík. Evolveum, *Practical Identity Management With MidPoint* [accesat 24.02.2026]
Disponibil: https://docs.evolveum.com/book/practical-identity-management-with-midpoint.pdf
22. Cotocus: *Top 10 Directory Services (LDAP/AD): Features, Pros, Cons & Comparison* [accesat 24.02.2026]
Disponibil: https://www.cotocus.com/blog/top-10-directory-services-ldap-ad-features-pros-cons-comparison/
23. StatCounter Global Stats: *Desktop Operating System Market Share Worldwide*, February 2026 [accesat 02.03.2026]
Disponibil: https://gs.statcounter.com/os-market-share/desktop/worldwide/

24. WASEEM, Umar. Fortray: *Why Microsoft Active Directory is the Foundation of Secure & Scalable IT Infrastructures?* [accesat 24.02.2026] Disponibil: https://www.fortray.com/blog/it-services-solutions-articles/why-microsoft-active-directory-is-important-for-it-infrastructure/
25. Picus Security: *The Complete Active Directory Security Handbook Exploitation, Detection, and Mitigation Strategies* [accesat 03.03.2026] Disponibil: https://ciso2ciso.com/wp-content/uploads/2023/06/The-Complete-Active-Directory-Security-Handbook.pdf
26. BHARGAV, Jyotsna J. ManageEngine: *A practical approach to Active Directory Domain Services, Part 1: A beginner's guide to Active Directory* [accesat 03.03.2026] Disponibil: https://www.manageengine.com/blog/index.php/active-directory/2022/03/15/a-practical-approach-to-active-directory-domain-services-part-1-a-beginners-guide-to-active-directory.html
27. Fortinet: *Active Directory - Complete Guide for IT Security* [accesat 04.03.2026] Disponibil: https://www.fortinet.com/uk/resources/cyberglossary/active-directory#:~:text=What%20is%20Active%20Directory?,manages%20two%20fundamental%20security%20functions
28. Quest: *What is Active Directory and how does it work?* [accesat 04.03.2026] Disponibil: https://www.quest.com/solutions/active-directory/what-is-active-directory.aspx
29. RAAFAY, Muhammad Abdur. *Active Directory: Architecture, Components, and Importance*, 2 Mai 2025 [accesat 04.03.2026] Disponibil: https://medium.com/@abdurraafay/what-is-active-directory-its-architecture-components-and-importance-1de3d982c9fc
30. Cayosoft: *What is an Active Directory Forest?* [accesat 04.03.2026] Disponibil: https://www.cayosoft.com/what-is-an-active-directory-forest/
31. NAVARRO, Daniel Garcia. ISDecisions: *How authentication works in Active Directory* [accesat 06.03.2026] Disponibil: https://www.isdecisions.com/en/blog/mfa/how-authentication-works-in-active-directory
32. KIDD, Chrissy. Splunk Blogs: *SIEM: Security Information & Event Management Explained* [accesat 11.03.2026] Disponibil: https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html
33. Exabeam: *What Is SIEM? 7 Pillars and 13 Core Features [2025 Guide]* [accesat 11.03.2026] Disponibil: https://www.exabeam.com/explainers/siem/what-is-siem/#:~:text=4.,traditional%20signature%2Dbased%20detection%20methods.
34. Fortinet: *SIEM for Enhanced Security: How It Detects & Manages Threats* [accesat 11.03.2026] Disponibil:https://www.fortinet.com/resources/cyberglossary/what-is-siem#:~:text=Security

%20information%20and%20event%20management%20(SIEM)%20is,*%20**Insider%20threat%20detection**%20*%20**Phishing%20detection**

35. SentinelOne: *What is SIEM Architecture? Components & Best Practices,* 11 august 2025 [accesat 13.03.2026]
    Disponibil: https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-architecture/#what-are-the-components-of-siem-architecture
36. COONEY Chris. Snowbit: *SIEM Architecture: 10 Key Components and Best Practices* [accesat 11.03.2026]
    Disponibil: https://snowbit.io/guide/observability-vs-monitoring-5-key-differences/
37. Mordor Intelligence: *Security information and event management (siem) market size & share analysis - growth trends and forecast (2026 - 2031)* [accesat 15.03.2026] Disponibil: https://www.mordorintelligence.com/industry-reports/global-security-information-and-event-management
38. ABRAHAM, Michelle. *IDC MARKET SHARE. Worldwide Security Information and Event Management Market Shares, 2024* [accesat 15.03.2026] Disponibil: https://idcdocserv.com/US53330426e_Cisco
39. Splunk: *Splunk, a Cisco company, Named No. 1 SIEM Provider by IDC for the fifth Year in a Row* [accesat 15.03.2026] Disponibil: https://www.splunk.com/en_us/form/idc-siem-market-share-report.html
40. DevopsByoli: *Splunk Enterprise: 7.0.0* [accesat 20.03.2026] Disponibil: https://devopsbyoli.wordpress.com/2018/03/07/splunk-enterprise-7-0-0/
41. Coursera: *What Is Splunk?* [accesat 20.03.2026] Disponibil: https://www.coursera.org/articles/what-is-splunk
42. Fortinet: *What Is Splunk?* [accesat 20.03.2026] Disponibil: https://www.fortinet.com/resources/cyberglossary/what-is-splunk
43. McKinsey Company: *The state of AI in 2025: Agents, innovation, and transformation, November 5, 2025* | Survey_____[accesat 21.03.2026] Disponibil: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai
44. COJOCARU, S., PECA, L. Challenges and solutions on the use of Artificial Intelligence in internet of things network security. In: Electronics, Communications and Computing (IC ECCO-2024): The conference program and abstract book: 13th intern. conf., Chişinău, 17-18 Oct. 2024. Technical University of Moldova. Chişinău: Tehnica-UTM, 2024, pp. 120-121. ISBN 978-9975-64-480-8 (PDF)
45. MajorKey: *The Impact of Artificial Intelligence and Machine Learning on IAM* [accesat 21.03.2026] Disponibil: https://www.majorkeytech.com/blogs/impact-of-ai-machine-learning-on-iam

46. Identity Management Institute: *Artificial Intelligence and Machine Learning are Transforming IAM, Blog* [accesat 21.03.2026] Disponibil: https://identitymanagementinstitute.org/artificial-intelligence-and-machine-learning-are-transforming-iam/
47. IBM: *Reinventing IAM: AI in Identity Verification and Access Management* [accesat 21.03.2026] Disponibil: https://community.ibm.com/community/user/blogs/andre-smith1/2024/12/06/reinventing-iam-ai-in-identity-verification-and-ac
48. PECA, L., ŢURCANU, D. Reducing cyber risk through a human–centred approach. In: *Journal of Engineering Science.* Vol. XXXII, no. 1, 2025, pp. 18 – 31 ISSN 2587-3474 https://doi.org/10.52326/jes.utm.2025.32(1).02
49. CyberSec: *AI Revolution in Identity and Access Management (IAM) [accesat 22.03.2026]* Disponibil: https://cybersecit.net/cybersec-blogs/ai-revolution-in-identity-and-access-management
50. Grand View Research: *Identity And Access Management Market (2023 - 2030)* [accesat 22.03.2026] Disponibil: https://www.grandviewresearch.com/industry-analysis/identity-and-access-management-iam
51. Trio: *Best Directory as a Service: Top 8 Platforms Compared*, [accesat 21.03.2026] Disponibil: https://www.trio.so/blog/best-directory-as-a-service
52. BestDevops: *Top 10 Directory Services (LDAP/AD): Features, Pros, Cons & Comparison* [accesat 21.03.2026]. Disponibil: https://www.bestdevops.com/top-10-directory-services-ldap-ad-features-pros-cons-comparison/
53. DevopsSchool: *Top 10 Directory Services (LDAP/AD): Features, Pros, Cons & Comparison* [accesat 21.03.2026]. Disponibil: https://www.devopsschool.com/blog/top-10-directory-services-ldap-ad-features-pros-cons-comparison/
54. Exabeam: *Best SIEM Solutions: Top 10 SIEM systems and How to Choose 2025* [accesat 22.03.2026] Disponibil: https://www.exabeam.com/explainers/siem-tools/siem-solutions/
55. DELGADO, Daute. Unihackers: *Splunk vs QRadar vs Sentinel: SIEM Comparison for SOC* [accesat 22.03.2026] Disponibil: https://unihackers.com/blog/siem-comparison-splunk-qradar-sentinel
56. EShield IT Services: *Most Popular SIEM Tools 2025 – Best Security Solutions* [accesat 22.03.2026] Disponibil: https://eshielditservices.com/most-popular-siem-tools/
57. ManageEngine: *Understanding SIEM tools: Selecting the best SIEM solution for your enterprise* [accesat 22.03.2026] Disponibil: https://www.manageengine.com/log-management/top-siem-tools.html
58. Stellar Cyber: *Best SIEM Tools and Solutions for 2026* [accesat 22.03.2026] Disponibil: https://stellarcyber.ai/learn/top-siem-solutions/
59. Exabeam: *Top 5 Free Open Source SIEM Tools* [Updated 2025] [accesat 22.03.2026] Disponibil: https://www.exabeam.com/explainers/siem-tools/7-open-source-siems/

60. SANCHEZ, Angel. *Creating an Active Directory Home Lab with Proxmox* , 20 decembrie 2022, [accesat 26.03.2026], Disponibil: https://medium.com/@happy_shimmer_hyena_411/creating-an-active-directory-home-lab-with-proxmox-ba3c94120b2e
61. AdminDroid Blog: *How to Add Domain Controller to Existing Domain in Active Directory*, [accesat 02.04.2026]. Disponibil: https://blog.admindroid.com/how-to-install-new-domain-controller-to-existing-active-directory-domain/
62. Microsoft: *Manage user accounts in Active Directory Users and Computers* , [accesat 02.04.2026]. Disponibil: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage-user-accounts-in-windows-server
63. Microsoft: *Active Directory security groups,* [accesat 04.04.2026]. Disponibil: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups
64. Microsoft: *Group Policy Management* , [accesat 04.04.2026]. Disponibil: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview
65. ADAudit Plus: *Configuring audit policies - Manual configuration,* [accesat 04.04.2026]. Disponibil: https://www.manageengine.com/products/active-directory-audit/help/data-source/ad-audit-configure-audit-policies-manually.html
66. Medium: *SOC Automation with Splunk, Active Directory & SOAR,* [accesat 07.04.2026]. Disponibil: https://medium.com/@stevenrim/soc-automation-with-splunk-active-directory-soar-b121465b08b9
67. Splunk: *Configure the universal forwarder using configuration files,* [accesat 07.04.2026]. Disponibil: https://help.splunk.com/en/splunk-cloud-platform/forward-and-process-data/universal-forwarder-manual/9.4/configure-the-universal-forwarder/configure-the-universal-forwarder-using-configuration-files
68. Splunk: *Monitor Active Directory,* [accesat 07.04.2026]. Disponibil: https://help.splunk.com/en/splunk-enterprise/get-started/get-data-in/10.2/get-windows-data/monitor-active-directory#the-ad-monitor-does-not-chase-ldap-referrals-0
69. Splunk: *How to Create Custom Dashboards and Alerts to Achieve the Best Mean Time to Detection,* [accesat 02.04.2026]. Disponibil: https://www.splunk.com/en_us/resources/videos/how-to-create-custom-dashboards-and-alerts-to-achieve-the-best-mean-time-to-detection.html
70. AMINE, Nina. *How To Monitor Windows Active Directory with Splunk* , 24 aprilie 2024, [accesat 02.04.2026]. Disponibil: https://www.youtube.com/watch?v=AgFwOg5l9Fs
71. AMINE, Nina. *How To Detect Active Directory Threats Using Splunk* , 29 aprilie 2024, [accesat 02.04.2026]. Disponibil: https://www.youtube.com/watch?v=XP9qI_1mKpM