IAM Meets CTI: Make Identity and Access Management ready for Cyber Threat Intelligence*

Alexander Puchta[1], Thomas Baumer[1], Mathis Müller[2], and Günther Pernul[2]

[1] Nexis GmbH, Rudolf-Vogt-Straße 6, Regensburg 93053, Germany
{firstname}.{lastname}@nexis-secure.com
https://nexis-secure.com/en/
[2] University of Regensburg, Universitätsstraße 31, Regensburg 93053, Germany
{firstname}.{lastname}@informatik.uni-regensburg.de
https://www.uni-regensburg.de/informatik-data-science/wi-pernul/startseite/index.html

Abstract. Enterprises rely on Identity and Access Management (IAM) systems as their primary solution for digital identity management and access control. While regulatory compliance is often a driving factor for such systems, they also serve as an essential security gate fortifying the defense against cyber attacks. However, when analyzing suspected or actual attacks, Security Information and Event Management (SIEM) systems and Cyber Threat Intelligence (CTI) are commonly employed but under-utilize valuable IAM data. IAM analysts can overcome such challenges by designing and implementing suitable mechanisms for a swift, easy-to-use, and faultless data transfer from IAM to SIEM. We contribute with a survey to identify ten central IAM findings relevant to CTI. We also evaluate their real-world feasibility by applying them within an anonymized data set of *TrustCorp* and make our tools open-source.

Keywords: IAM, CTI, SIEM, IDS

1 Introduction

The 2021 OWASP Top Ten lists *Broken Access Control* as first place, indicating its severity for 94% of the tested applications. Regulative authorities acknowledge this risk and demand effective IAM controls. Notable regulations include the GDPR, Basel III, or SOX. Such IAM systems allow observing access control data: For example, a critical permission assignment to a recently created identity can indicate malicious actions. IAM can capture these patterns and can communicate them via CTI to SIEM systems [35]. However it remains unclear which IAM findings are relevant to CTI and SIEM. Thus, this paper provides the following central contributions:

* The research leading to these results was supported by the German Federal Ministry of Education and Research as part of the DEVISE project (https://devise.ur.de).

- We synthesize ten distinct IAM findings from theory and practice.
- We show real-world practicability by a case study for the role model of an anonymized enterprise *TrustCorp* (maintaining ca. 5.5k digital identities).
- We make our tools open-source to ease a vendor-independent impact.

To realize these contributions, the remainder of this work is outlined as follows: Section 2 covers related work and Section 3 details our method. In Section 4, we review various sources to synthesize a set of ten relevant IAM findings. Afterward, in Section 5, we show the feasibility by evaluating a selection of the IAM findings within a case study for the anonymized enterprise *TrustCorp*. Section 6 concludes our work and highlights future research.

2 Related Work

Research on CTI or SIEM has recently received much interest, with many published overviews and frameworks (e.g., [47,40]). However, integrating IAM data to leverage insights for improved detection of cyber attacks has yet to be noticed. On the contrary, there is already work published to identify individual anomalies or findings within access control or IAM (e.g., [37,7,28] to name only a few).

When looking into practice, one can find various frameworks like the Lockheed Martin Cyber Kill Chain [20] or the MITRE ATT&CK framework [44]. However, we have consulted more than 70 enterprises regarding IAM, and less than five of them integrate IAM information into their CTI processes.

Summarizing the research and practice experience above, we observe a research gap for applying IAM or access control data to CTI. An important enabler for this is also an overview of proposed detectable IAM anomalies. To the best of our knowledge, there is no comprehensive work considering IAM to include within CTI to enhance analytical results. Therefore, we close this research gap by defining IAM findings relevant to CTI.

3 Method

We research literature and and practitioner's sources to identify our IAM findings on a comprehensive basis. In Section 4, we summarize these IAM findings. While we are aware that there are more findings within an IAM landscape, we chose the most relevant ones for this work. For these findings, we show their applicability for the real-world data set of *TrustCorp*. We thus develop and apply scripts to transform the IAM data into CTI-readable information.

Literature survey. We employ a structured approach by defining suitable keywords to identify relevant IAM literature based on Levy and Ellis [26]. After defining suitable search terms[3][4], we apply them to academic databases (ACM, IEEE XPlore, DBLP, Google Scholar) and integrate research from the related

[3] identity and access management
[4] identity|access management analysis|anomaly|signature|pattern

topic "*access control*". Applying our search terms yields a feasible number of relevant results. We decreased the amount by manually filtering the results based on title, abstract, and content. This results in 23 relevant scientific entries (c.f. Table 1) mentioning or defining relevant IAM findings. We group the results, which leads to ten IAM findings (see Section 4).

Practitioners' view. Using the initial IAM findings as input, we further improve the results. We incorporate various sources for our business analysis by relying, among others, on analysts having specific expertise in IAM like KuppingerCole[5]. They have built up profound IAM knowledge and serve as a further source of information. Additionally, more general analysts like Gartner[6] and Forrester[7] also highlight IAM topics relevant to our work. We also include information security or IAM standards as they often have specific regulations (e.g., ISO/IEC 27001, SOX, BASEL). Violations of such lead to IAM findings. Hence, these sources offer further results for our analysis.

4 IAM Findings

Table 1 provides an overview of IAM findings based on theory and practice. We exclude valid findings which are only of small value for CTI processes as they do not pose any threat. Next, we detail each finding. We resort to some elements from Structured Threat Information eXpression (STIX) to provide additional, structured information, namely *Vulnerability* and *Course of Action* [45].

Table 1. IAM findings.

Name	Literature	Practitioner
F1 - Orphan accounts	[6]	[30]
F2 - Excessive permission assignments	[38,10]	[21,44,29,30]
F3 - Assignment rule errors	[15,23,46]	
F4 - Attribute data quality	[25,24,4,3,5,13]	[36,42]
F5 - Privacy leak of identity data	[34,33,41,1]	[8,27,44,29]
F6 - Process errors	[18]	[21]
F7 - Policy violations	[17,15,16,32,19]	[43,2,21]
F8 - Dead access control policies	[10,32]	[30]
F9 - Liveness	[41,32,44]	[30]
F10 - Missing recertification	[12]	[21,36]

F1 - Orphan accounts. An orphan account is an account without a connection to a valid identity [11,34,9,6]. An orphan account may prove a higher threat than others because nobody is responsible. A *vulnerability* arises as an orphan

[5] `https://www.kuppingercole.com/`
[6] `https://www.gartner.com`
[7] `https://www.forrester.com`

account is still usable and has irregularly examined permissions. Especially having administrative permissions assigned can lead to a privilege escalation attack. Suitable *courses of action* within IAM would be regular recertifications of all account types and the definition of sufficient identity life cycle processes [36].

F2 - Excessive permission assignments. Excessive permissions are a basic reason for IAM. Identities have unnecessary permissions directly assigned or inherited via roles, leading to *vulnerabilities*. Identification methods rely on visualization, access reviews, or automated algorithms for analysis [7,28]. Regarding *courses of actions*, automated account cleansing or automation of role assignments, or attribute-based access control are suitable options [39,15].

F3 - Assignment rule errors. Assignment rules typically encompass a condition set. All identities fulfilling the condition are automatically assigned to permissions (e.g., all internal identities get permission to the intranet). Errors (like a specific attribute is incorrectly set within the IAM) can lead to a wrong membership calculation, thus resulting in the *vulnerability* since identities get assigned the wrong permissions. Processes for assignment rule changes or automated validity checks before error occurrence are suitable *courses of action*.

F4 - Attribute data quality. Data quality is extensively covered by various authors with quality metrics and frameworks [13,3]. Lacking attribute data quality can impair the reasoning of permission assignment because of missing descriptions. Other data quality errors are missing ownership or criticality flags. Such cases lead to the *vulnerability* that poor data quality enables attackers to obtain permissions because of a poor criticality assessment. Organizations can employ *courses of action* like the regularly checked attribute quality rules.

F5 - Privacy leak of identity data. IAM systems typically cache privacy-related information (e.g., name, address, contact information) due to their connection to HR systems [6]. An information leakage bears the *vulnerability* that attackers may use privacy-related information retrieved from IAM systems (e.g., spear phishing) [14]. A suitable *course of action* is the encryption or anonymization of privacy-related information within IAM systems and processes [35].

F6 - Process errors. Organizations may lack automation, especially regarding leaver or mover processes [25]. Attackers may want to bypass defined processes to gain elevated permissions, resulting in a *vulnerability*. A suitable *course of action* is the automation of processes and integration into IAM tools.

F7 - Policy violations. Organizations often constrain their access control with policies like Separation of Duty (SoD). *Vulnerabilities* arise when attackers can directly exploit toxic permission combinations. As *course of action*, organizations can use automated SoD checks and regular maintenance of SoD rules.

F8 - Dead access control policies. Dead Access Control Policies (ACPs) refer to unused permissions or roles [32]. As a *vulnerability*, attackers might assign dead ACP to themselves by circumventing processes without further approval. Fortunately, *courses of action* are easy to deploy [22]. Organizations can automatically check for dead ACPs and process permanent deletion or reassignment.

F9 - Liveness. Liveness comprises ACPs assigned to exactly one identity. Liveness indicates that only a single person conducts a specific task. A *vul-*

nerability is that these ACPs become dead ACPs when this person leaves the organization or has the assignment removed. To avoid such cases, organizations can include such ACPs in a comprehensive role model as a *course of action* [39].

F10 - Missing recertification. A recertification (or access review) is a regular inspection of identities, accounts, permissions, or roles to maintain an organization's ACPs [31]. Uncertified identities are a *vulnerability* as these might have excessive permissions. Therefore, attackers might misuse these identities to gain access. A *course of action* is an automated reporting of uncertified entities.

5 Evaluation

This Section evaluates the practical feasibility of our IAM findings. Hence, we showcase generating a CTI threat report using an anonymized data set of the real-world enterprise *TrustCorp* (pseudonym). We make our implementations open-source: `https://github.com/IAMmeetsCTI/IAM-meets-CTI`

TrustCorp is a German enterprise in the finance and insurance sector. The enterprise has an IAM system with eight connected applications based on Role-Based Access Control (RBAC) [39]. We extracted several of our previously defined IAM findings during the analysis and integrated them in CTI.

TrustCrop also narrowed down the goals and wished an exclusive analysis of the existing role model and selected IAM findings, including *F3*, *F8*, *F9*, and *F10*. With this generously provided *TrustCorp* data and scope, we generated a threat report with our scripts by querying the dataset for our IAM findings.

Table 2 summarizes the analysis results. We apply further filter criteria only to include the most critical findings if analyzing and discussing the resulting number of defect roles with *TrustCorp* would become too cumbersome. Thus, our analysis covers 221 findings, comprising 3 of the 4 investigated IAM findings.

Table 2. Analysis results of TrustCorp.

Analyzed finding	**#Results**	**Filter criteria**
F3 - Assignment rule errors	0	No filter applied
F8 - Dead access control polices	49 roles	Criticality = 'high'
F9 - Liveness	162 roles	Criticality = 'high'
F10 - Missing recertification	10 roles	No filter applied

TrustCorp returned positive feedback. The swift and easy-to-use scripts allowed quick integration within their IAM system without tedious change requests. The reports contain interactive visualizations[8] and ease the awareness of solvable findings. *TrustCorp* further discussed a deeper integration to their SIEM infrastructure and also reporting the other IAM findings periodically.

[8] https://oasis-open.github.io/cti-stix-visualization/?url=https://raw.githubusercontent.com/IAMmeetsCTI/IAM-meets-CTI/main/example-trustcorp.json

6 Conclusion

We derived ten IAM findings (non-exhaustive) that would enhance the SIEM effectiveness from theory and practice. We focused on the most essential IAM findings relevant to CTI, which we verified throughout the practice-oriented analysis. Due to the scoping of our work, we excluded the authentication side of IAM (e.g., multiple login errors of the same identity at a suspicious time). IAM solutions predominantly focus on authorization, as having critical permissions assigned without suitable justification is often an immediate compliance violation and of particular interest for the domain of CTI. Moreover, we showed practical feasibility with our *TrustCorp* use case by successfully structuring and representing IAM data with STIX. We aim to empower others to leverage IAM data in their CTI efforts by sharing our open-source repository. As future work, we want to research the authentication side of IAM and its implications for CTI.

References

1. Asghar, M.R., Backes, M., Simeonovski, M.: Prima: Privacy-preserving identity and access management at internet-scale. In: 2018 IEEE International Conference on Communications (ICC). pp. 1–6. IEEE, Kansas City, MO, USA (May 2018)
2. Basel Comittee on Banking Supervisions: Basel III: International framework for liquidity risk measurement, standards and monitoring (2010)
3. Batini, C., Cappiello, C., Francalanci, C., Maurino, A.: Methodologies for data quality assessment and improvement. ACM computing surveys **41**(3), 1–16 (2009)
4. Batini, C., Scannapieco, M.: Data quality: Concepts, Methodologies and Techniques. Springer, New York, USA (2006)
5. Batini, C., Scannapieco, M.: Data and Information Quality: Dimensions, Principles and Techniques. Springer Publishing Company, Incorporated, International, 1st edn. (2016)
6. Baumer, T., Müller, M., Pernul, G.: System for cross-domain identity management (scim): Survey and enhancement with rbac. IEEE Access **11**, 86872–86894 (2023)
7. Colantonio, A., Di Pietro, R., Ocello, A., Verde, N.: Visual role mining: A picture is worth a thousand roles. IEEE Transactions on Knowledge and Data Engineering **24**(6), 1120–1133 (2012)
8. Diodati, M., Ruddy, M., Rabinovich, P., Mezzera, P.: Gartner - 2020 planning guide for identity and access management (2019)
9. Everett, C.: Identity and access management: The second wave. Computer Fraud & Security **2011**(5), 11–13 (2011)
10. Fuchs, L., Kunz, M., Pernul, G.: Role model optimization for secure role-based identity management. In: European Conference on Information Systems (ECIS). pp. 1–15. AIS, Tel Aviv, Israel (Juni 2014)
11. Fuchs, L., Pernul, G.: Supporting compliant and secure user handling - a structured approach for in-house identity management. In: The Second International Conference on Availability, Reliability and Security (ARES'07). pp. 374–384. IEEE, Vienna, Austria (2007). https://doi.org/10.1109/ARES.2007.145
12. Groll, S., Kern, S., Fuchs, L., Pernul, G.: Monitoring access reviews by crowd labelling. In: Fischer-Hübner, S., Lambrinoudakis, C., Kotsis, G., Tjoa, A.M., Khalil, I. (eds.) Trust, Privacy and Security in Digital Business. pp. 3–17. Springer International Publishing, Cham (2021)

13. Heinrich, B., Kaiser, M., Klier, M.: How to measure data quality? a metric-based approach. In: Rivard, S., Webster, J. (eds.) Proceedings of the 28th International Conference on Information Systems (ICIS). Montreal, Queen's University. pp. 1–15. AISeL, Montreal (2007), https://epub.uni-regensburg.de/23633/
14. Ho, G., Sharma, A., Javed, M., Paxson, V., Wagner, D.: Detecting credential spearphishing attacks in enterprise settings. In: Proceedings of the 26th USENIX Conference on Security Symposium. p. 469–485. SEC'17, USENIX Association, USA (2017)
15. Hu, V., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K.: Guide to attribute based access control (ABAC) definition and considerations. Tech. rep., NIST (2014)
16. Hu, V., Ferraiolo, D.F., Kuhn, D.R., Kacker, R.N., Lei, Y.: Implementing and managing policy rules in attribute based access control. In: 2015 IEEE International Conference on Information Reuse and Integration. pp. 518–525. IEEE, San Francisco, CA, USA (Aug 2015). https://doi.org/10.1109/IRI.2015.98
17. Hu, V., Scarfone, K.: Guidelines for access control system evaluation metrics. Tech. rep., NIST (2012)
18. Hummer, M., Groll, S., Kunz, M., Fuchs, L., Pernul, G.: Measuring identity and access management performance - an expert survey on possible performance indicators. In: Proceedings of the 4th International Conference on Information Systems Security and Privacy. pp. 233–240. SCITEPRESS - Science and Technology Publications, Funchal, Madeira, Portugal (2018)
19. Hummer, M., Kunz, M., Netter, M., Fuchs, L., Pernul, G.: Adaptive identity and access management—contextual data based policies. Journal on Information Security **2016**(1), 19 (2016)
20. Hutchins, E., Cloppert, M., Amin, R.: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Tech. rep., Lockheed Martin (2011)
21. ISO 27001: Information technology — Security techniques — Information security management systems — Requirements. Standard, International Organization for Standardization (Oct 2013)
22. Kern, S., Baumer, T., Fuchs, L., Pernul, G.: Maintain high-quality access control policies: An academic and practice-driven approach. In: Atluri, V., Ferrara, A.L. (eds.) Data and Applications Security and Privacy XXXVII. pp. 223–242. Springer Nature Switzerland, Cham (2023)
23. Kern, S., Baumer, T., Groll, S., Fuchs, L., Pernul, G.: Optimization of access control policies. Journal of Information Security and Applications **70**, 103301 (2022)
24. Kunz, M., Fuchs, L., Hummer, M., Pernul, G.: Introducing dynamic identity and access management in organizations. In: Jajoda, S., Mazumdar, C. (eds.) Information Systems Security. pp. 139–158. Springer International Publishing, Cham (2015)
25. Kunz, M., Puchta, A., Groll, S., Fuchs, L., Pernul, G.: Attribute quality management for dynamic identity and access management. Journal of Information Security and Applications **44**, 64–79 (2019)
26. Levy, Y., Ellis, T.: A systems approach to conduct an effective literature review in support of information systems research. International Journal of an Emerging Transdiscipline **9** (01 2006)
27. Maxim, M., Cser, A.: Forrester - Top trends shaping IAM in 2022 (2022)
28. Meier, S., Fuchs, L., Pernul, G.: Managing the access grid - A process view to minimize insider misuse risks. In: 11. Internationale Tagung Wirtschaftsinformatik,

Leipzig, Germany, February 27 – March 1, 2013. p. 66. AIS, Leipzig, Germany (2013), http://aisel.aisnet.org/wi2013/66
29. MITRE: CAPEC common attack pattern enumeration and classification. https://capec.mitre.org/index.html (2023), accessed: 2023-05-22
30. MITRE: CWE common weakness enumeration. https://cwe.mitre.org/index.html (2023), accessed: 2023-05-22
31. Osmanoglu, E.: Identity and Access Management: Business Performance Through Connected Intelligence. Newnes, Waltham (2013)
32. Parkinson, S., Khan, S.: A survey on empirical security analysis of access-control systems: A real-world perspective. ACM Computing Surveys **55**(6), 1–28 (2022)
33. Pfitzmann, A., Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management (2010)
34. Puchta, A., Böhm, F., Pernul, G.: Contributing to current challenges in identity and access management with visual analytics. In: Foley, S.N. (ed.) Data and Applications Security and Privacy XXXIII. pp. 221–239. Springer International Publishing, Cham (2019)
35. Puchta, A., Groll, S., Pernul., G.: Leveraging dynamic information for identity and access management: An extension of current enterprise iam architecture. In: Proceedings of the 7th International Conference on Information Systems Security and Privacy - ICISSP. pp. 611–618. INSTICC, SciTePress, Online Streaming (2021)
36. Reinwarth, M.: Access reviews done right. Tech. rep., Kuppingercole Analysts, https://www.kuppingercole.com/report/lb80195 (aug 2019)
37. Samarati, P., de Vimercati, S.C.: Access control: Policies, models, and mechanisms. In: International School on Foundations of Security Analysis and Design. pp. 137–196. Springer (2000)
38. Sandhu, R.: The authorization leap from rights to attributes: Maturation or chaos? In: Proceedings of the 17th ACM Symposium on Access Control Models and Technologies. p. 69–70. SACMAT '12, Association for Computing Machinery, New York, NY, USA (2012)
39. Sandhu, R., Coyne, E., Feinstein, H., Youman, C.: Role-based access control models. Computer **29**(2), 38–47 (1996)
40. Schlette, D., Caselli, M., Pernul, G.: A comparative study on cyber threat intelligence: The security incident response perspective. IEEE Communications Surveys & Tutorials **23**(4), 2525–2556 (2021)
41. Servos, D., Osborn, S.: Current research and open problems in attribute-based access control. ACM Computing Surveys **49**(4), 1–65 (2017)
42. Small, M.: Kuppingercole report - advisory note - big data security, governance, stewardship (2018)
43. SOX: Sarbanes-Oxley Act of 2002, pl 107-204, 116 stat 745 (2002)
44. Strom, B., Applebaum, A., Miller, D., Pennington, A., Thomas, C.: MITRE ATT&CK: Design and Philosophy. Framework, The MITRE Corporation, McLean, USA (Mar 2020)
45. Struse, R., Darley, T.: STIX Version 2.1. OASIS Standard, OASIS (June 2021)
46. Vijayalakshmi, K., Jayalakshmi, V.: Identifying considerable anomalies and conflicts in abac security policies. In: 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS). pp. 1273–1280. IEEE, Madurai, India (May 2021)
47. Wagner, T., Mahbub, K., Palomar, E., Abdallah, A.: Cyber threat intelligence sharing: Survey and research directions. Computers & Security **87**, 101589 (2019)