

Conceptual approach to the interaction of zero trust and SOC in cybersecurity system of enterprises

Zarina Poberezhna^{1,*}

¹Transport Academy of Ukraine, Omelyanovich-Pavlenko Str., 1, Kyiv, 02000, Ukraine

Abstract

The paper presents the theoretical foundations of the integration of the Zero Trust Architecture (ZTA) with the Security Operation Center (SOC) to form a conceptual approach to increasing the cyber resilience of enterprises. The problems of the functioning of perimeter Zero Trust protection models with the analytical capabilities of the SOC are analyzed, which allows minimizing the risks of internal and external threats. The key components of the integrated ZTA+SOC model are considered, which use identity and access management mechanisms (IAM), authentication and authorization, as well as threat detection and incident response systems of the SIEM, SOAR and XDR class. The basic principles of the Zero Trust architecture are formed, which are consistent with the principles of NIST SP 800-207 and SOC when exposed to hybrid threats. The basis for quantitative risk assessment is a mathematical model that takes into account both the probability of the threat and the effectiveness of protection measures. A mathematical model for assessing trust for the decision-making point is developed and an algorithm for automated SOC response in ZTA conditions is proposed. The proposed algorithm allows to reduce the response time to incidents and blocks the movement of the threat, and also allows the SOC analytics department of the enterprise to reduce the number of routine tasks, leaving the response time for more complex ones. A comparative analysis of the effectiveness of the classic SOC and ZTA-integrated SOC by key cyber defense metrics was conducted.

Keywords

Zero Trust Architecture, ZTA, Security Operation Center, SOC, trust level, cyber resilience, micro-segmentation, IAM, SIEM, SOAR, enterprise cybersecurity, threats

1. Introduction

In modern conditions, enterprises operate in complex dynamic conditions, characterized by a high degree of digitalization, integrated systems, digital technologies and services. The development of digitalization, the implementation of the Industry 4.0 concept creates new opportunities for enterprises, but exposes them to greater influence of possible cyberattacks. Traditional protection methods that use static rules, antiviruses and firewalls are no longer effective in overcoming new types of threats and targeted attacks, because they operate on the principle of protecting a clearly defined perimeter.

Therefore, when forming a cybersecurity system, enterprises need to use modern methods and tools in infrastructure protection, which are focused on the ability to predict, resist, recover and adapt to cyberattacks without stopping the main processes of the enterprise.

The basis for forming the concept of enterprise cyber resilience is the integration of the Zero Trust architecture (ZTA) and Security Operations Center (SOC), which allows to localize threats, minimize the blast radius through verification of each request based on contextual data [1]. SOC provides the enterprise with constant monitoring, log consolidation, early detection of anomalies and orchestration of incident response processes, which significantly reduces the likelihood of disruptions and downtime in the functioning of enterprises.

Despite the significant advantages of these two concepts, they usually operate autonomously from each other, however, for the formation of a high level of enterprise cybersecurity, their interaction is critically important, which will allow creating an adaptive cyber defense system, where SOC acts as an analytical center, and Zero Trust is an executive mechanism that instantly isolates compromised nodes.

WCH'26: Fifth International Workshop on Cyber Hygiene, June 25–26, 2026, Krakow, Poland

*Corresponding author.

✉ zarina_www@ukr.net (Z. Poberezhna)

ORCID 0000-0001-6245-038X (Z. Poberezhna)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

The autonomous operation of Zero Trust and SOC limits the overall potential of the cybersecurity system, because without dynamic data analytics, the SOC concept of ZTA does not take into account the real context of threats, and vice versa, SOC without integration with ZTA loses the speed of incident response due to the lack of telemetric data on access rights and behavior of subjects [2].

Therefore, the development of conceptual principles of such interaction for modern enterprises that seek to ensure continuity of operation in the face of hybrid threats and changing cyberspace is becoming increasingly relevant.

2. Literature review

The development and formation of an enterprise cybersecurity system, ensuring its cyber resilience have been studied by many domestic and foreign scientists. Issues of the theory and practice of Zero Trust were considered in paper [3], which systematized the principles of ZTA in the context of cloud and IoT environments. However, the features of adapting this concept to outdated operational technologies that operate in real time and do not support modern authentication protocols remained unstudied.

In paper [4] the Zero Trust architectural model and its basic principles in a corporate environment were studied, but the specifics of transferring this model to modern enterprises need to be studied, since most of them have certain technological limitations.

In paper [5] a scientific approach to implementing Zero Trust in hybrid enterprise security architectures using the MITRE ATT&CK + FAIR risk assessment methodology was developed. However, the developed methodology is focused mainly on threats of the corporate IT segment and does not take into account the specifics of the MITRE ATT&CK for Industrial Control Systems (ICS) matrices.

In order to identify anomalies and automatically change the access policy (Session Revocation), the authors of paper [6] proposed to use machine learning (ML) methods, which allows to detect “Man-in-the-Middle” attacks in technological networks. However, the proposed methods do not connect the security system with the Zero Trust architecture, no algorithm was proposed that would transform the detected anomaly through the PEP broker without the risk of an emergency shutdown of the system.

In paper [7], the ZTA architecture is systematized through key components: the decision point (PDP) and the policy execution point (PEP), but the strict requirements for data request delays inherent in OT systems (levels 0–2 according to the Purdue model) are not taken into account.

The need for convergence of monitoring processes and the creation of unified security centers (I-SOC) for correlating logs from the corporate and technological segments of the enterprise is considered in paper [8], but the authors do not take into account attacks aimed at hiding traces within the industrial protocols themselves. As already noted, most scientific papers focus on network isolation and passive anomaly analysis. In particular, the issues of designing a Zero Trust architecture related to identity management (IAM) and network microsegmentation were considered in paper [9].

In paper [10], the issues of technological optimization of SOC, implementation of SIEM/XDR systems and automated response (SOAR) were considered, however, methodological approaches to the interaction between ZTA and analytical cycles of SOC in order to increase the cyber resilience of enterprises remain unexplored.

The purpose of the study is to develop a conceptual approach to the interaction of the Zero Trust Architecture architectural model with the SOC functioning system, as a single mechanism of functioning in the formation of an enterprise cybersecurity system aimed at increasing its cyber resilience and ensuring the continuity of critical processes of the enterprise.

3. Materials and methods

3.1. Architecture of the ZTA+SOC integrated system

Zero Trust architecture is focused on protecting the network perimeter, services, and data; all data sources and computing services are considered resources, trust is never implicitly granted by design,

but is constantly asserted, and access is granted to the minimum necessary extent in accordance with the principle of least privilege [11].

The NIST SP 800-207 standards provide seven core principles of Zero Trust architecture, each of which directly defines the detection and response processes in a SOC [12]. All data sources are considered resources regardless of their location, and include SOC sensors that should provide visibility both inside and outside the perimeter. All communication is protected regardless of network location, with internal traffic between segments subject to the same analysis as external traffic. Access is granted on a per-session basis with a continuous trust assessment based on the request, while the SOC receives a continuous stream of signals about the status of each request and each session.

Failures in technical equipment, inconsistencies in technological procedures, and inefficient operation reduce the level of resilience of cyber-physical systems [13, 14].

A number of ZTA principles are distinguished in accordance with the SOC operational processes, which are regulated according to the NIST SP 800-207 standards:

- all resources are subject to protection regardless of location (extended visibility of cloud, OT, and mobile environments);
- all communication is protected regardless of network location (encrypted traffic analysis and SSL inspection);
- access is granted possessively with trust assessment (automated triage of access requests via PDP);
- access is determined by rules and policies (continuous process of updating rules and playbooks);
- data integrity monitoring process (incident sensitivity management and control);
- authentication and protection of personal data through authorization (detection of event anomalies);
- analysis and collection of information about the state of objects (construction of behavior during threat exposure and correlation of telemetry).

Each of the above ZTA principles is directly reflected in SOC processes, and there is a close relationship between the trust model and operational data. When integrating ZTA+SOC, an enterprise can monitor data in real time, maintain asset integrity using SIEM and XDR platforms that integrate with decision-making processes (Policy Decision Point, PDP) to automatically block compromised assets.

The above principles change the functionality of the SOC, transforming it from a network perimeter monitoring center to a proactive system that includes device identity control, data, and telemetry.

The proposed architecture of the integrated ZTA+SOC system in the context of forming the enterprise cybersecurity system is built on the principle of data distribution and management, where each component performs a clearly defined role in the overall chain (Fig. 1).

The SOC in this system functions as an analytical and operational center covering both planes. The SIEM platform aggregates telemetry from PEP, IAM, EDR, network sensors and cloud environments. The SOAR system receives alerts from the SIEM and automatically executes playbook scenarios, including isolating a compromised node, resetting the session, increasing the TS_{min} threshold for a specific resource, or transferring the incident to an analyst for manual investigation [15].

One of the important elements of the architecture is a closed feedback loop, in which the results of incident response are returned to adjust the weights, as well as to Threat Intelligence systems to update compromise indicators.

The problem of analyzing the efficiency of enterprise operational processes, which are implemented using statistical data processing algorithms aimed at reducing average operating costs, contributes to increasing the level of enterprise security [16, 17].

In this context, the stability of information support is determined by the reliability and efficiency of operational processes [18].

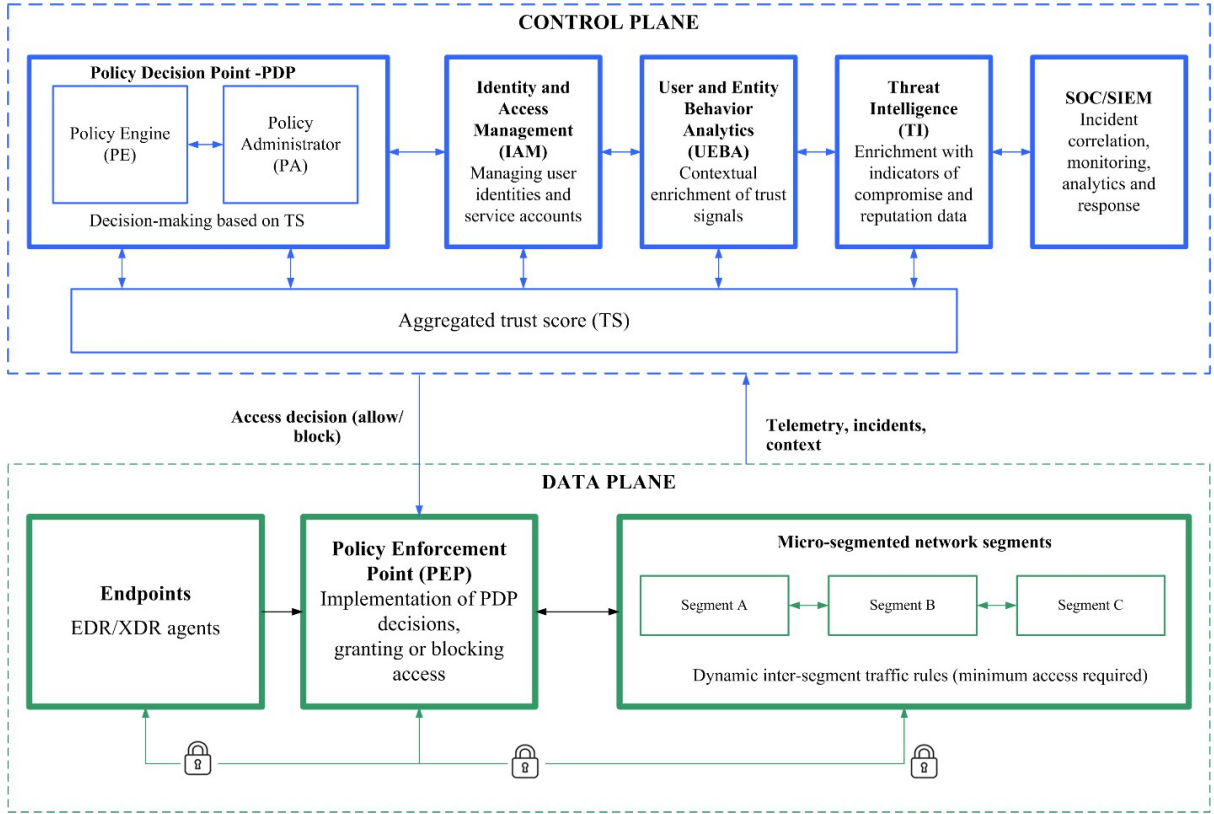


Figure 1: Architecture of the integrated ZTA+SOC system in the formation of enterprise cyber resilience.

Improving the cybersecurity of enterprises should be based on the development of a comprehensive dynamic protection strategy that combines automation, identity management and adaptive response processes. In the conditions of modern Zero Trust architecture, it is necessary to develop an automated response algorithm adapted to the operating conditions of a ZTA-integrated SOC, using the SOAR and XDR platforms [19]. The main goal of which is instant response to incidents and threats, assessment of the level of risk and adaptability, as well as the status of security. The author proposed an automated response algorithm built in accordance with the best practices of NIST SP 800-61 Rev. 3 and the MITRE ATT&CK framework model (Fig. 2).

In the first stage, the algorithm captures the access request and transmits it to the PDP along with the contextual attributes of the subject, device, and environment. The PDP calculates an aggregated trust rating TS using the formula and compares it to the threshold TS_{min} . If $TS \geq TS_{min}$, access is secure and the incident is logged in the SIEM journal. If $TS < TS_{min}$, then the PDP system rejects the request or requires additional verification; repeated MFA is performed, confirmation is performed via an out-of-band channel. SIEM telemetry analysis and correlation of all system components are also performed, and static methods and models are used to check for anomalies. The results of the check are documented and returned to the feedback loop to improve the trust model.

Implementation of such an algorithm allows to reduce incident response time and block the movement of the threat, and also allows the enterprise SOC analytics department to reduce the number of routine tasks, leaving the response time for more complex ones. Automation of incident response processes allows to increase the level of cybersecurity of the system, while reducing the negative impact of cyberattacks on the main processes of the enterprise. It is worth noting that increasing the level of cybersecurity of the enterprise also requires the development of encryption algorithms based on fixed lookup tables with extended data depth and key-dependent lookup tables [20, 21].

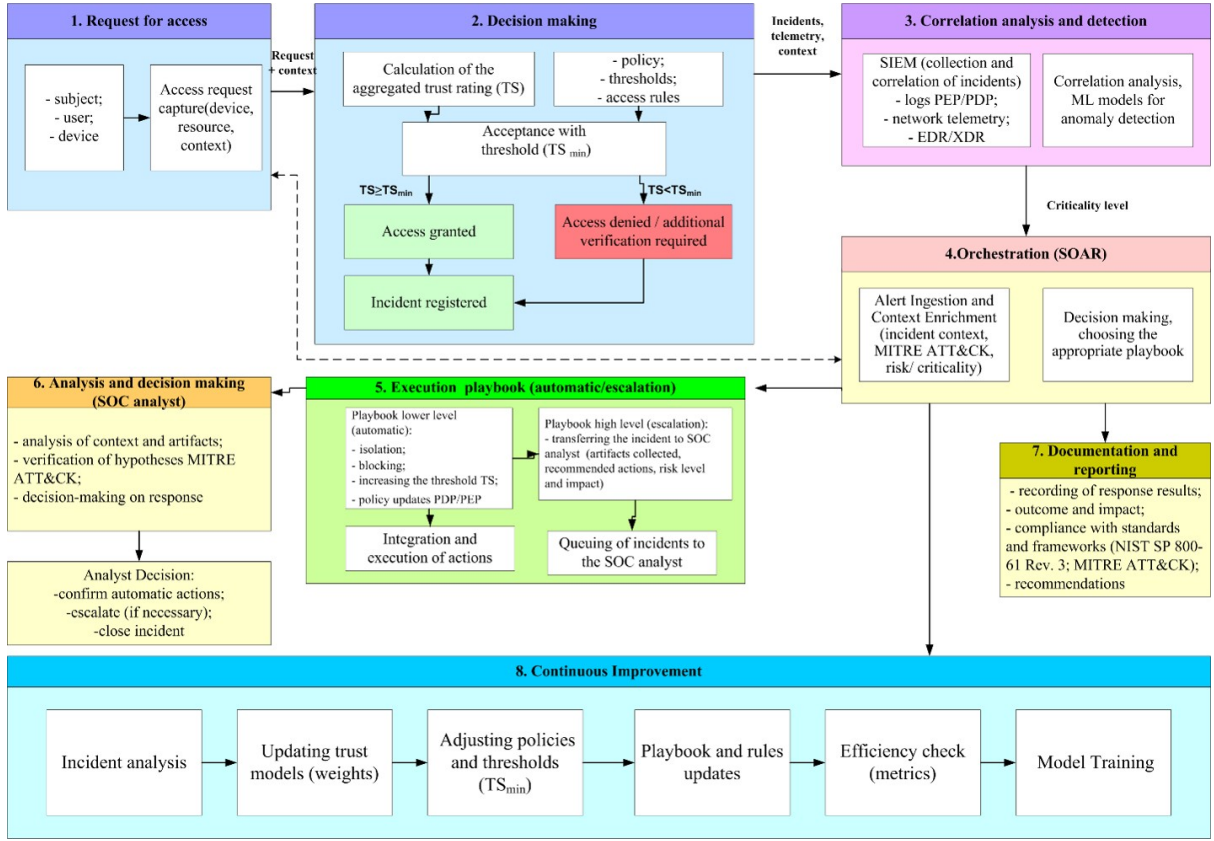


Figure 2: Automated SOC response algorithm in ZTA conditions.

3.2. Trust score model for PDP and trust score mechanism

The main analytical element of ZTA is the Policy Decision Point (PDP) and the Trust Score mechanism for each resource access request. Unlike static rules of perimeter models, trust score in ZTA is multifactorial, context-dependent, and time-sensitive, which is consistent with weighted-additive models.

The basis of quantitative risk assessment is a mathematical model that takes into account both the probability of a threat and the effectiveness of protection measures.

To substantiate the integrated ZTA+SOC system, a mathematical model for calculating the Cyber-Physical Trust Score (TS) has been developed. The integral trust score $TS_i(t) \in [0, 1]$ is calculated as the weighted sum of three main components:

$$TS_i(t) = \omega_1 \cdot TS_{rr}(i, t) + \omega_2 \cdot TS_{Net}(i, t) + \omega_3 \cdot TS_{Phys}(i, t) \quad (1)$$

where $TS_{rr}(i, t)$ is the context coefficient (authentication, access rights); $TS_{Net}(i, t)$ is the network behavior coefficient (protocol compliance, request frequency); $TS_{Phys}(i, t)$ is the coefficient of the physical context of the technological process; $\omega_1, \omega_2, \omega_3$ are weight coefficients determined by expert means, under the condition $\sum_{j=1}^3 \omega_j = 1$.

To determine network behavior and detect anomalies, it is necessary to determine the network trust component $TS_{Net}(i, t)$, which is calculated based on the detected SOC anomalies and the corresponding actions on the attacker's tactics:

$$TS_{Net}(i, t) = \exp \left(-\lambda \sum_{k=1}^M \alpha_k \cdot Score_{MITRE}(k) \right) \quad (2)$$

where λ is the system sensitivity coefficient to anomalies ($\lambda > 0$); $Score_{MITRE}(k)$ is the basic level of danger of the k -th device according to the MITRE ATT&CK for ICS classification; $\alpha_k \in [0, 1]$ is the probability of implementing the k -th attack, determined by the SOC module at a certain time t .

The principle of continuous verification determines that trust is not constant during a session, so the trust level decays over time:

$$TS(t) = TS(t_0) \times \exp(-\lambda \cdot (t - t_0)) \quad (3)$$

where λ is the decay constant. If TS_t falls below the threshold values, forced re-authentication or session termination is initiated.

The behavior of the model depends on the basic thresholds of the resource classes (θ_j), the weight profile (W_i), and (C_i) the trust level:

$$TS(q, t) = \left(\sum_{i=1}^n W_i C_i(q) \right) \cdot \prod_{j \in M} \mathbf{1}[C_j(q) \geq \theta_j] \cdot e^{-\lambda(t-t_0)} \quad (4)$$

In the matrix-vector form, trust aggregation (TS) is performed by combining the current trust score (C_i) and weight normalization (W_i) into a single dynamic system:

$$\begin{aligned} \mathbf{C} &= (C_1, \dots, C_n)^T, \quad \mathbf{W} = (W_1, \dots, W_n)^T, \quad g_j = \mathbf{1}[C_j \geq \theta_j], \quad \sum_{i=1}^n W_i = 1, \\ TS &= [W_1 g_1 \quad \dots \quad W_n g_n] \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} e^{-\lambda(t-t_0)} W^{(k+1)} = \Pi_{\Delta} \left(W^{(k)} + \mu \nabla_W J(W^{(k)}) \right), \quad (5) \\ \Delta &= \{W \in \mathbb{R}^n : W_i \geq 0, \sum_i W_i = 1\} \end{aligned}$$

The decision rule (PDP) in a dynamic SOC continuously compares the integral indicator TS_i^t with the adaptive safety threshold τ , the sensitivity coefficient $\eta \in [0; 1]$, and the resource threshold r :

$$Policy(i, t) = \begin{cases} \text{ALLOW,} & TS_i(t) \geq TS_{min}^0(r) + (1 - TS_{min}^0(r)) \eta \tau \\ \text{STEP-UP,} & TS_{Net} \leq TS(q, t) < TS_{min}(r, \tau) \\ \text{DENY,} & TS_i(t) < TS_{Net} \text{ or } \exists j \in M : C_j < \theta_j \end{cases} \quad (6)$$

Recommended threshold values by resource class are given in Table 1. As (τ) increases, the threshold asymptotically approaches unity (Fig. 3).

Table 1
Basic Trust Thresholds by Resource Class

Resource class	TS_{min}^0	Examples of resources	A feature of the policy
Public	0,40	Public portals, marketing	Minimum requirements
Internal	0,65	Internal applications, e-mail	Standard profile
Confidential	0,80	Financial systems, customer databases	Enhanced verification
Critical	0,85	Management systems, privileged access	Maximum requirements, frequent reassessments

The developed mathematical model of trust assessment, formulas (1)–(6), sets a multifactor rating for determining the level of trust and attenuation, defines the logic of the PDP decision policy, and matrix-vector calculation of weights in the feedback loop with the SOC. This allows to automate the process of managing security policies in real time, minimize human influence, and develop mechanisms for responding to new types of cyber threats.

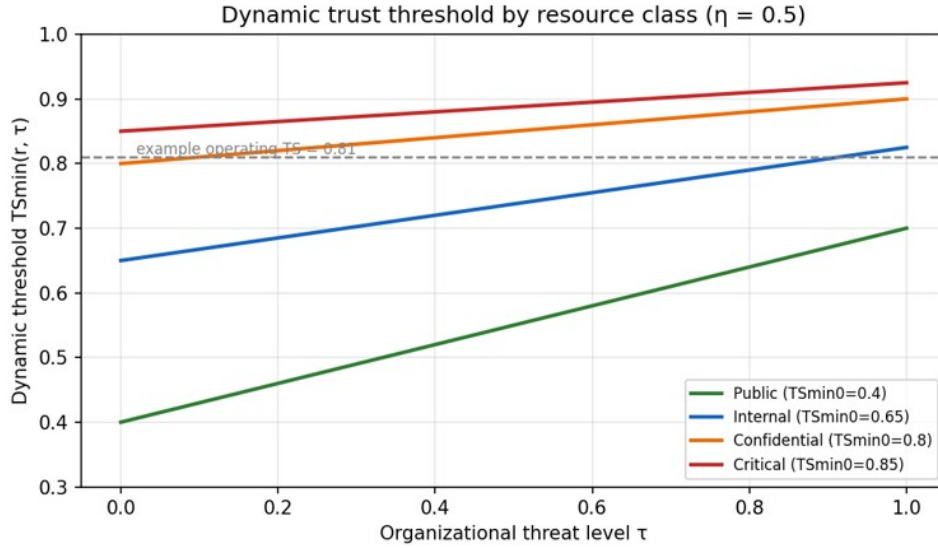


Figure 3: Dynamic threshold $TS_{min}^0(r, \tau)$ by resource classes.

4. Results of empirical testing of ZTA+SOC in the aviation domain

The European Air Traffic Management (ATM) system is an example of a critical infrastructure with possible threats to the functioning of the system, making it a target for attack. ATM coordinates air traffic in 41 states within the Single European Sky concept, integrating corporate IT systems, operational traffic control (OT) systems, satellite navigation (GNSS), data channels and landing services. The scale of the system directly determines the amount of potential damage, which makes it an attractive target and at the same time vulnerable due to the high interdependence of digital processes.

Cyber threats to the aviation domain cover several levels, which well illustrate the limits of the perimeter logic of protection. At the corporate IT level, one of the most common is a DDoS attack, which can disrupt the availability of web services, but traffic control security systems are not damaged due to their isolation (air-gap). However, isolation itself is a classic manifestation of perimeter trust, which is becoming less and less suitable in the context of digitalization and IT/OT convergence. If we consider the operational (navigation) airspace level, it systematically encounters jamming and spoofing of GNSS signals. A comparison of threat levels with the corresponding ZTA+SOC controls is given in Table 2.

In order to connect SOC cybermetrics (MTTD, MTTR, level of automation) with practically real consequences for critical infrastructures, it is advisable to consider an example of operational indicators of a highly loaded node.

To test the proposed methodology, formulas (1)–(6), EUROCONTROL data were used on the example of the Amsterdam Schiphol (EHAM) hub airport for 2021–2025 [22, 23]. The main calculation data are IFR traffic volumes, as well as additional Taxi-out (a proxy for the average departure queue time during busy periods), and additional arrival time (additional ASMA, the average arrival queue time). The initial data for the calculation are given in Table 3.

The above indicators confirm that for highly loaded systems such as the aviation domain, even a slight degradation of digital processes (access, routing, accounting, planning) can correlate with measurable losses of time and airport capacity, since the system operates close to its capacity limit. The growth of traffic from 280 thousand movements in 2021 to about 493 thousand in 2025 is accompanied by an increase in additional departure time. Therefore, in the aviation domain, the effect of ZTA-integrated SOC should be assessed not only through MTTD/MTTR, but also through the stability of service KPIs as the “operational equivalent” of the stability of the digital circuit. Calculations of the volume of IFR traffic and additional service time at EHAM airport for 2021–2025, with the integration of the ZTA+SOC

Table 2

Comparison of Aviation Domain Threat Levels to ZTA+SOC Controls

Level/vector	Threat Example	Why Perimeter is Insufficient	ZTA+SOC Controls
Corporate IT	DDoS on web services	Isolation/perimeter trust; web loop open	IT Micro-Segmentation, Continuous Trust Assessment, SOAR Blocking
Accounting / Application	Credential compromise and remote access	Implicit trust after login	Least Privilege, MFA, UEBA Behavioral Analysis
OT / Navigation (GNSS)	GNSS jamming and spoofing	Threat bypasses network perimeter completely	Treat-as-Compromised, RFI Monitoring as SOC Telemetry, Position Cross-Validation
Regulatory / Process	EASA Part-IS, NIS2 requirements	Requires system-wide, not point-based protection	ISMS, Risk Management and Incident Reporting as SOC Functions

Table 3

IFR Traffic and Additional Time Indicators for Airport EHAM (Amsterdam Schiphol) for 2021–2025.

Year	IFR arrivals	IFR departures	IFR total	Add. Taxi-out, min/Dep.	Add. ASMA, min/Arr.
2021	139 892	139 982	279 784	2.99	2.55
2022	207 875	207 938	415 813	3.17	2.61
2023	229 088	229 095	458 183	3.19	2.56
2024	244 509	244 562	489 071	3.41	2.67
2025	246 511	246 531	493 042	3.25	2.59

concepts, are presented in Fig. 4.

The presented results confirm that the symbiosis of ZTA and SOC for critical infrastructure is of great importance. Firstly, micro-segmentation between corporate IT and ATM operating systems localizes the effects of attacks, and complicates lateral movement according to formula (4), the probability of detection threats with the number of requests. Secondly, continuous trust assessment makes it impossible to abuse compromised remote access credentials for a long time. ATM operating systems belong to the class of critical resources with a high baseline threshold TS_{min}^0 , and during periods of active countermeasures to incidents, the organizational threat level τ increases, so the dynamic threshold $TS_{min}(r, \tau)$ according to formula (6) automatically increases the trust requirements.

Thirdly, integration with SOC provides end-to-end visibility of IT and OT environments; in particular, RFI data telemetry can be considered as an additional source of signals for assessing the contextual trust factor in the Zero Trust concept, as well as for correlation in SIEM. The processes of risk management, incident response, and reporting methodologically correspond to the functions of the SOC, and are consistent with the principle of Zero Trust. Thus, the analysis of the aviation domain demonstrates that the proposed trust assessment model and the architecture of the ZTA-integrated SOC are applicable to critical infrastructure not only in the IT dimension, but also at the level of operational resilience of services.

The proposed trust assessment model for the decision point (PDP) allows for dynamic adjustment of access rights based on the current level of cyber threats recorded by the SOC. The SOC security loop transmits anomalies to the analytics in real time, and the trust assessment mechanism instantly calculates the weight coefficients for the PDP, which allows isolating the threat before the system is completely compromised.

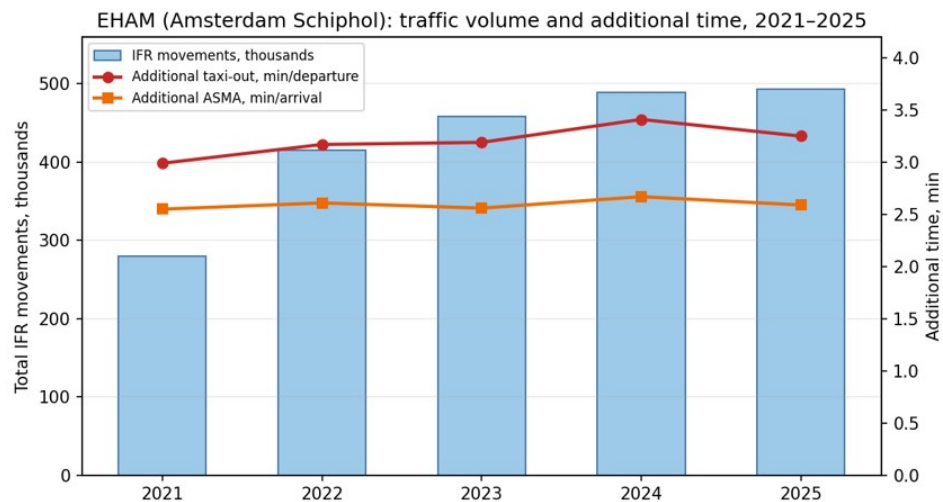


Figure 4: IFR traffic volume and additional service time at EHAM airport in 2021–2025.

5. Conclusions

The conceptual approach of integrating Zero Trust Architecture and SOC allows to increase the level of cybersecurity through the symbiosis of these two strategies, which form a new level of cyber resilience of the enterprise. Traditional approaches to using SOC operate within the perimeter model, forced to compensate for the architectural vulnerability of the perimeter with reactive monitoring; however, a ZTA-integrated SOC allows to conduct control of each transaction, using dynamic trust assessment as the main tool for incident prevention. This allows to increase the level of the enterprise cybersecurity system, and to assess the level of trust (TS) in the decision-making process, connecting ZTA control with the level of residual risk. The proposed model for assessing the level of system trust provides measurable, protection-based indicators that meet modern regulatory requirements and the provisions of the NIST SP 800-207 standards. The principle of continuous assurance and micro-segmentation have been found to be effective countermeasures against various types of threats associated with the physical capture of IT assets and secondary compromise of the central infrastructure.

Declaration on Generative AI

The author have not employed any Generative AI tools.

References

- [1] S. Kumar, Cyber resilience through zero-trust architectures: A paradigm shift, *International Journal of Emerging Research in Engineering and Technology* 1 (2020) 10–18. doi:10.63282/3050-922X.IJERET-V1I3P102.
- [2] S. Duchek, Organizational resilience: a capability-based conceptualization, *Business Research* 13 (2020) 215–246. doi:10.1007/s40685-019-0085-7.
- [3] H. Kang, G. Liu, Q. Wang, L. Meng, J. Liu, Theory and application of zero trust security: A brief survey, *Entropy* 25 (2023) 1595. doi:10.3390/e25121595.
- [4] O. Prydybaylo, I. Sribna, R. Prydybaylo, Zero trust architecture: Basic principles of organization, *Svyazok* 5 (2022) 16–20. doi:10.31673/2412-9070.2022.051620.
- [5] O. Horodytsky, I. Opirsky, Step-by-step approach to implementing zero trust in hybrid corporate security architectures, *Cybersecurity: Education, Science, Technology* 3 (2025) 346–366. doi:10.28925/2663-4023.2025.31.1029.

- [6] C. Konstantinou, M. Maniatakos, F. Saqib, S. Hu, J. Plusquellic, Y. Jin, Cyber-physical systems: A security perspective, in: *Proceedings of the 20th IEEE European Test Symposium (ETS)*, Cluj-Napoca, Romania, 2015, pp. 1–8. doi:10.1109/ETS.2015.7138763.
- [7] H. Joshi, Emerging technologies driving zero trust maturity across industries, *IEEE Open Journal of the Computer Society* 6 (2025) 25–36. doi:10.1109/OJCS.2024.3505056.
- [8] V. Gnanasekaran, T. Nilsen, P. Heegaard, A comparative study of security operations center models for operational technology, *Norsk IKT-Konferanse for Forskning Og Utdanning* 37 (2025) 1–16. doi:10.5324/yd7t8t20.
- [9] A. Al-Khouri, Optimizing identity and access management (IAM) frameworks, *International Journal of Engineering Research and Applications* 1 (2011) 461–477.
- [10] S. Millionis, G. Karetsos, An open-source SIEM and XDR monitoring framework towards holistic IoT security, in: *Proceedings of the 2025 IEEE Middle East Conference on Communications and Networking (MECOM)*, Cairo, Egypt, 2025, pp. 1–6. doi:10.1109/MECOM67453.2025.11439492.
- [11] K. Govindan, P. Mohapatra, Trust computations and trust dynamics in mobile adhoc networks: A survey, *IEEE Communications Surveys & Tutorials* 14 (2011) 279–298. doi:10.1109/SURV.2011.042711.00083.
- [12] S. Rose, O. Borchert, S. Mitchell, S. Connelly, Zero Trust Architecture NIST SP 800-207, Technical Report, National Institute of Standards and Technology, Gaithersburg, 2020. doi:10.6028/NIST.SP.800-207.
- [13] J. Al-Azzeh, et al., A method of accuracy increment using segmented regression, *Algorithms* 15 (2022) 378. doi:10.3390/a15100378.
- [14] V. Ivannikova, M. Zaliskyi, O. Solomentsev, I. Ostroumov, N. Kuzmenko, Statistical data processing technologies for sustainable aviation: A case study of Ukraine, *Sustainability* 17 (2025) 5781. doi:10.3390/su17135781.
- [15] J. Kindervag, No more chewy centers: Introducing the zero trust model of information security, Forrester Research, 2010.
- [16] O. Solomentsev, M. Zaliskyi, Z. Poberezhna, O. Zuiev, Predictive analytics of decision-making for aviation operation enterprise, in: I. Ostroumov, K. Marais, M. Zaliskyi (Eds.), *Advances in Civil Aviation Systems Development (ACASD)*, volume 1418 of *Lecture Notes in Networks and Systems*, Springer, Cham, 2025, pp. 348–363. doi:10.1007/978-3-031-91992-3_23.
- [17] A. Dziubynskyi, et al., Management of transport and logistics systems: Problems under conditions of military operations, in: B. Alareeni, A. Hamdan (Eds.), *Navigating the Technological Tide: The Evolution and Challenges of Business Model Innovation*, volume 1080 of *Lecture Notes in Networks and Systems*, Springer, Cham, 2024, pp. 363–373. doi:10.1007/978-3-031-67444-0_35.
- [18] M. Zaliskyi, O. Solomentsev, Z. Poberezhna, O. C. Okoro, B. Chumachenko, S. Chumachenko, Information technologies of data processing for linear deterioration process during aviation equipment operation, *CEUR Workshop Proceedings* 3732 (2024) 32–44. URL: <https://ceur-ws.org/Vol-3732/paper03.pdf>.
- [19] D. Prokopovych-Tkachenko, V. Zvieriev, I. Kozachenko, Integration of security operations centers (SOC) into Ukraine's national security system, *State Security* 1 (2025) 106–114. doi:10.33405/2786-8613/2025/1/5/336736.
- [20] M. Iavich, S. Gnatyuk, E. Jintcharadze, Y. Polishchuk, R. Odarchenko, Hybrid encryption model of AES and ElGamal cryptosystems for flight control systems, in: *Proceedings of the 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC)*, Kiev, Ukraine, 2018, pp. 229–233. doi:10.1109/MSNMC.2018.8576289.
- [21] S. Gnatyuk, V. Kinzeryavyy, M. Iavich, D. Prysiaznyi, K. Yubuzova, High-performance reliable block encryption algorithms secured against linear and differential cryptanalytic attacks, *CEUR Workshop Proceedings* 2104 (2018) 657–668. URL: https://ceur-ws.org/Vol-2104/paper_220.pdf.
- [22] EUROCONTROL Performance Review Unit, Datasets, 2025. URL: <https://ansperformance.eu/data/>.
- [23] EUROCONTROL Network Manager, Operational data (IFR traffic), amsterdam schiphol (EHAM), 2021–2025, 2025. URL: <https://www.eurocontrol.int/publication/annual-network-operations-report-2025>.