КІБЕРБЕЗПЕКА: освіта, наука, техніка № 3 (31), 2025
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE ISSN 2663 - 4023

DOI 10.28925/2663-4023.2025.31.1066
UDC 004.056

Pavlo Chernikov
Specialist in Law, Master of Public Service,
Head of the Specialized Municipal Enterprise “Kyivteleservis” (2021–2024)
ORCID: 0009-0006-7390-9698
pavlo.chernikov@gmail.com

CYBER DEFENSE OF URBAN DIGITAL SYSTEMS: SCALING SIEM CORRELATION TO REDUCE INCIDENTS IN A WARTIME CITY

Abstract. Modern megacities are increasingly dependent on the resilience of digital platforms and converged networks that sustain critical urban life support systems. In the context of a full-scale war, where cyberattacks are strictly synchronized with the physical destruction of energy and communication infrastructure, ensuring the continuity of municipal services requires a fundamental shift from fragmented monitoring to centralized, intelligent incident management. This article systematizes the practical experience of designing, building, and operating a city-scale Security Operations Centre (SOC) based on the Specialized Municipal Enterprise “Kyivteleservis” during the period of 2021–2024. The object of the study is the complex protection processes of the Corporate Multiservice Network (CMN) of Kyiv, which connects over 1,800 municipal institutions, spans 1,500 km of fiber-optic communication lines, and supports the “Safe City” video surveillance system (comprising over 8,000 cameras) alongside the Internet of Things (LoRaWAN) sensor network. The author provides a detailed analysis of the operational challenges resulting from the sharp increase in cyber incidents and the shifting threat landscape: from massive DDoS attacks on “Kyiv Digital” ecosystem services to sophisticated attempts at exploiting vulnerabilities in telecommunications equipment during emergency power blackouts. The primary focus of the work is on the development and implementation of a methodology for scaling correlation rules within a SIEM system. The article proposes a transition from standard signature-based detection to behavioral analysis, structured according to the five core functions of the NIST Cybersecurity Framework 2.0 (Identify – Protect – Detect – Respond – Recover). A specific mechanism for the “Contextual Enrichment” of security events is described, which involves automatically appending metadata regarding asset criticality, physical location, and responsible administrator to raw logs. This approach effectively addressed the issue of “alert fatigue,” filtering out up to 90% of false positives caused by legitimate remote user activity via VPN gateways during air raid alerts. The research results are substantiated by quantitative performance metrics of the SOC: the Mean Time to Respond (MTTR) for high-severity incidents was reduced by 30% (decreasing from 45 to 30 minutes on average), and the availability of key administrative services for citizens was maintained at a level of 99.9% even during peak load periods and kinetic attacks. The conclusions formulate practical recommendations for city digital transformation leaders regarding the prioritization of monitoring tools and the construction of a fault-tolerant cyber defense architecture under conditions of limited human and financial resources. This article will be useful for critical infrastructure cybersecurity specialists, system architects, and local government officials facing similar threats.

Keywords: urban cyber security; SIEM; SOC; incident correlation; MTTD; MTTR; municipal digital services; cyber resilience.

INTRODUCTION

Cities that actively digitalised their services during the last decade entered the period of full-scale war with a difficult paradox. On the one hand, municipal authorities rely on online platforms for transport, utilities, social support, and education. On the other hand, these platforms—along with critical infrastructure like the "Safe City" video surveillance system and LoRaWAN sensor networks—became attractive targets for hostile cyber activity [3].

In this context, a city-scale Security Operations Centre (SOC) is no longer an optional project but a daily necessity. As the head of the Specialized Municipal Enterprise "Kyivteleservis" from 2021 to 2024, I witnessed firsthand how cyber defense directly influences whether residents receive critical services. Our team managed the IT infrastructure for the Kyiv City Council and State Administration, protecting data across a fiber-optic network spanning over 1,500 km and connecting thousands of municipal institutions.

Table 1.

Scope of the Kyiv municipal digital infrastructure (2021–2024).

Component	Scale / Notes
Connected municipal institutions	>1,800
Fiber-optic backbone	~1,500 km
Video surveillance ("Safe City")	>8,000 cameras
IoT sensor network	LoRaWAN gateways + utility/municipal sensors
Operating constraints	Wartime conditions; periodic power outages; staffing shifts incl. remote work

This article summarizes our experience in evolving an urban SOC and SIEM platform under extreme pressure. The focus is practical: how to scale correlation, structure incident handling, and reduce the number of impactful incidents, ensuring that city services remain available 99.9% of the time despite missile attacks and coordinated cyber campaigns.

PROBLEM STATEMENT

At the starting point (early 2021), the city had various security controls: firewalls, antivirus solutions, and fragmented monitoring for video surveillance. However, these did not form a cohesive picture. The main operational problems were:

- **High volume of raw noise:** A single misconfigured switch or a legitimate high-load backup process could generate hundreds of alerts, masking real threats like brute-force attacks on administrative portals.
- **Fragmented visibility:** The team managing the Wi-Fi network for schools often saw different logs than the team protecting the City Hall's data center.
- **Slow response times:** Without a unified view, the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) for cross-system incidents were unacceptably long.

The challenge was to build a realistic SOC and SIEM approach that fits limited staff resources but supports 24/7 operations, even during air raids and power outages.

ANALYSIS OF RECENT RESEARCH AND PUBLICATIONS

Research on critical infrastructure protection emphasizes treating security as a continuous cycle. The NIST Cybersecurity Framework (CSF) 2.0 identifies five key functions: Identify, Protect, Detect, Respond, and Recover [1], [2]. This cycle is crucial for urban resilience, as highlighted in systematic reviews of critical infrastructure protection [3], [4].

Technical implementation often relies on SIEM systems to correlate events. Modern best practices suggest moving away from simple signature matching to behavioral analysis and context-aware correlation rules [5], [6]. Specific models for situational centers and their cyber protection have been proposed by Ukrainian researchers. For instance, Grechaninov, Skladannyi, and colleagues describe the dependability models for information systems in situational centers, which closely matches our municipal context [12]. Others emphasize the need for proactive SIEM models specifically for critical infrastructure [8], [9]. However, few studies address the practical "war stories" of implementing these models in a city under active military aggression, where physical kinetic threats (missile strikes on energy grids) directly impact cyber defense capabilities [10], [11].

PURPOSE OF THE ARTICLE

The purpose of this article is to present a practical methodology for scaling SIEM correlation rules in an urban SOC, demonstrating how aligning technical rules with the NIST functional cycle and enriching data with local context can significantly reduce incident response times and prevent service disruptions.

THEORETICAL BACKGROUND

Our approach relies on three pillars:

1. **The NIST Functional Cycle:** Using the Identify-Protect-Detect-Respond-Recover model to categorize every correlation rule [2].
2. **Contextual Correlation:** The idea that an alert's severity depends not just on the technical event (e.g., "failed login") but on the asset's context (e.g., "is this the Mayor's workstation or a public kiosk?") [7].
3. **Cyber Resilience:** Shifting the goal from "zero incidents" to "zero critical disruptions," ensuring essential services like the 1551 contact center or air raid alert systems continue functioning even if minor peripheral components are compromised [3].

RESEARCH METHODOLOGY

The methodology combines qualitative process analysis with quantitative metrics tracked at "Kyivteleservis" between 2021 and 2024.

- **Qualitative:** Analysis of SOC playbooks, incident post-mortems, and workflow changes during the migration to a private cloud infrastructure.
- **Quantitative:** Tracking MTTD and MTTR for high-severity incidents, the ratio of false positives (noise) to actionable alerts, and the availability of critical services (e.g., "Kyiv Digital" backend services).
-

RESEARCH RESULTS

1. **Structuring SIEM by Cyber Security Functions** Initially, our SIEM had hundreds of default rules enabled. We audited and disabled 60% of them, keeping only those relevant to our specific environment (Cisco network gear, specific server OS versions, virtualization platforms). We then mapped the remaining rules to the NIST functions. For example, "Detect" rules were tuned to catch anomalous traffic patterns on the LoRaWAN gateway, which collects data from utility sensors.

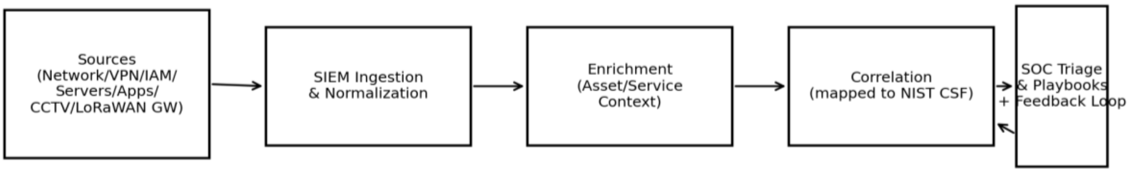
Sources (Network/VPN/IAM/ Servers/Apps/ CCTV/LoRaWAN GW)
SIEM Ingestion & Normalization
Enrichment (Asset/Service Context)
Correlation (mapped to NIST CSF)
SOC Triage & Playbooks + Feedback Loop

Figure 1. High-level data flow for municipal SOC/SIEM correlation.

2. Contextual Enrichment A raw log entry saying "High CPU usage on Server-101" is useless. We implemented a lookup mechanism that enriched logs with asset data. The alert became: "High CPU on Server-101 (Role: e-Ticket Database, Zone: Critical, Owner: Transport Dept)." This allowed L1 analysts to prioritize immediately. This aligns with the "Situational Center" model described by Skladannyi et al., where dependability attributes are key [12].

3. Operational Impact The results of these changes were measurable:

Table 2.

Operational effect after SIEM correlation redesign (selected KPIs).

Metric	Baseline	After tuning	Notes
Disabled default SIEM rules	0%	~60% disabled	Removed irrelevant/default noise rules
Noise / false-positive alerts	100% (index)	~10% (index)	~90% reduction via correlation + context
MTTR for high-severity incidents	~45 min	~30 min	~30% improvement for known patterns
Remote workforce share (context factor)	—	~80%	Increased VPN/remote-related noise

- **Noise Reduction:** By correlating firewall logs with identity management logs, we eliminated 90% of alerts caused by authorized remote workers connecting via VPN, which was critical when 80% of our staff worked remotely.
- **Improved MTTR:** The average time to respond to critical incidents decreased by approximately **30%** (from ~45 minutes to ~30 minutes) for known attack patterns.

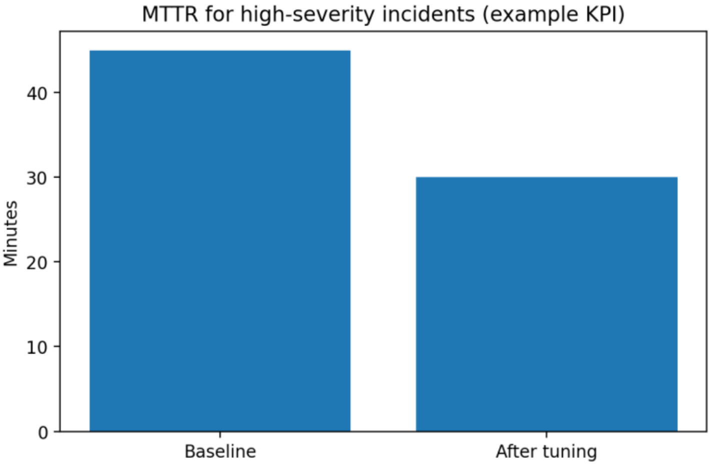

Figure 2. MTTR improvement after correlation and playbook redesign (example KPI).

• **Resilience:** During the massive kinetic and cyber attacks in late 2022 and 2023, the unified SOC allowed us to quickly identify which network segments went dark due to power cuts versus those under cyberattack, preventing wasted dispatch efforts.

Limitations. This case study reflects an applied SOC/SIEM program in a single large municipality under wartime constraints. The metrics reported are operational indicators collected for incident handling rather than results of a controlled experiment. Changes in the threat landscape, staffing availability, and power-outage patterns may act as confounders. Therefore, the reported improvements should be interpreted as evidence of practical feasibility and operational value, not as universally guaranteed performance.

Replication checklist for other cities:

- Inventory critical services and service owners (including dependencies).
- Audit and disable irrelevant default SIEM rules; keep only rules tied to services and threats.
- Implement enrichment (service, criticality tier, location/zone, and asset ownership).
- Map correlation rules to an operational model (e.g., NIST CSF) and align alerts to playbooks.
- Route alerts to responsible teams and establish feedback loops from post-mortems to rule tuning.
- Track operational KPIs (e.g., noise ratio, MTTD, MTTR) and review them on a fixed cadence.

CONCLUSIONS

The experience of "Kyivteleservis" proves that effective urban cyber defense does not require unlimited budgets. It requires a disciplined approach to SIEM configuration. By structuring correlation rules around the NIST framework [1] and enriching events with local context, a municipal SOC can filter out noise and focus on protecting what matters—the digital services that citizens rely on. For other cities, we recommend starting not with buying more tools, but with building a clear inventory of assets and defining what "critical impact" means for their specific community.

REFERENCES

1. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
2. Mahn, A. (2018, April 16). *Identify, Protect, Detect, Respond, and Recover: The NIST Cybersecurity Framework*. NIST Taking Measure Blog. https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework
3. Naserinia, V., Ekstedt, M., & Asplund, M. (2021). *Cyber Resilience for Critical Infrastructure: A Systematic Literature Review*. KTH Royal Institute of Technology. https://www.diva-portal.org/smash/get/diva2:1576950/FULLTEXT03.pdf
4. Bellini, E., Marrone, S., & Di Mauro, N. (2025). Situation awareness for cyber resilience: A review. *International Journal of Critical Infrastructure Protection, 48,* Article 100720. https://doi.org/10.1016/j.ijcip.2025.100755
5. Cybersecurity Ventures. (2024). *SIEM Implementation: Strategies and Best Practices*. Cybersecurity Ventures. https://cybersecurityventures.com/siem-implementation-strategies-and-best-practices/
6. Cymulate. (2025). *SIEM Correlation Rules: Fine-Tune Detection Logic at Scale*. Cymulate Glossary. https://cymulate.com/cybersecurity-glossary/siem-correlation-rules/
7. Redborder. (2024, September 10). *How SIEM correlation rules work*. Redborder Blog. https://redborder.com/how-siem-correlation-rules-work/

8. Subach, I. Yu., Fesokha, V. V., & Fesokha, N. O. (2019). Model proaktyvnoi intelektualnoi SIEM-systemy dlia kiberzahystu obiektiv krytychnoi infrastruktury [Model of proactive intellectual SIEM-system for cyber protection of critical infrastructure objects]. *Information Technology and Security, 7*(2), 209–216. https://doi.org/10.20535/2411-1031.2019.7.2.190570

9. Hnatiuk, S. O. (2023). Systema koreliuvannia podii ta upravlinnia intsydentamy kiberbezpeky na obiektakh krytychnoi infrastruktury [Event correlation and cyber security incident management system at critical infrastructure objects]. *Cybersecurity: Education, Science, Technique, 19*, 161–174. https://doi.org/10.28925/2663-4023.2023.19.176196

10. Piadyshev, V. H. (2022). Kiberbezpeka krytychnykh infrastruktur: zakordonnyi dosvid ta ukrainski realii [Cybersecurity of critical infrastructures: foreign experience and Ukrainian realities]. *South Ukrainian Law Journal*, *4*(3), 229–234. https://doi.org/10.32850/sulj.2022.4.3.38

11. Zubok, V. Yu., Davydiuk, A. V., & Klymenko, T. M. (2023). Cybersecurity of critical infrastructure in Ukrainian legislation and in Directive (EU) 2022/2555. *Electronic Modeling*, *45*(5), 54–66. https://doi.org/10.15407/emodel.45.05.054

12. Grechaninov, V., Hulak, H., Sokolov, V., Skladannyi, P., & Korshun, N. (2022). Formation of dependability and cyber protection model in information systems of situational center. In *Proceedings of the 1st International Workshop on Control, Optimisation and Analytical Processing of Social Networks (COAPSN-2022)* (pp. 107–117). CEUR Workshop Proceedings, Vol-3149. https://ceur-ws.org/Vol-3149/paper11.pdf

Черніков Павло Олександрович
магістр державної служби, спеціаліст права,
керівник Спеціалізованого комунального підприємства «Київтелесервіс» (2021–2024)
ORCID: 0009-0006-7390-9698
pavlo.chernikov@gmail.com

КІБЕРЗАХИСТ МІСЬКИХ ЦИФРОВИХ СИСТЕМ: МАСШТАБУВАННЯ КОРЕЛЯЦІЇ ПОДІЙ У SIEM ДЛЯ ЗМЕНШЕННЯ ІНЦИДЕНТІВ В УМОВАХ ВОЄННОГО ЧАСУ

Анотація. Сучасні мегаполіси дедалі більше залежать від стійкості цифрових платформ та конвергентних мереж, які забезпечують життєдіяльність міста. В умовах повномасштабної війни, коли кібератаки синхронізуються з фізичним руйнуванням інфраструктури, забезпечення безперервності надання муніципальних послуг вимагає переходу від фрагментарного моніторингу до централізованого, інтелектуального управління інцидентами. У статті систематизовано практичний досвід побудови та експлуатації міського центру кіберзахисту (SOC) на базі Спеціалізованого комунального підприємства «Київтелесервіс» у період 2021–2024 років. Об'єктом дослідження є процеси захисту корпоративної мультисервісної мережі (КММ) міста Києва, яка об'єднує понад 1800 муніципальних установ, 1500 км волоконно-оптичних ліній зв'язку, систему міського відеоспостереження «Безпечне місто» (понад 8000 камер) та мережу датчиків інтернету речей (LoRaWAN). Автором детально проаналізовано операційні виклики, що виникли внаслідок різкого зростання кількості кіберінцидентів та зміни ландшафту загроз: від масованих DDoS-атак на сервіси «Київ Цифровий» до спроб експлуатації вразливостей у телекомунікаційному обладнанні під час блекаутів. Основну увагу в роботі приділено розробці та впровадженню методики масштабування правил кореляції в SIEM-системі. Запропоновано перехід від використання стандартних сигнатур до поведінкового аналізу, структурованого відповідно до функцій рамкової моделі NIST Cybersecurity Framework 2.0 (Identify – Protect – Detect – Respond – Recover). Описано механізм «контекстного збагачення» подій безпеки (Contextual Enrichment), який передбачає автоматичне додавання до сирих логів метаданих про критичність активу, його фізичне розташування та відповідального адміністратора. Це дозволило вирішити проблему «втоми від сповіщень» (alert fatigue), відсіявши до 90% помилкових спрацювань, спричинених легітимною активністю віддалених користувачів через VPN-шлюзи. Результати дослідження підтверджено кількісними показниками ефективності роботи SOC: середній час реагування (MTTR) на інциденти високої критичності вдалося скоротити на 30% (з 45 до 30 хвилин), а доступність ключових адміністративних послуг для громадян було збережено на рівні 99,9% навіть у періоди пікових навантажень. У висновках сформульовано практичні рекомендації для керівників цифрової трансформації міст щодо пріоритезації засобів моніторингу та побудови відмовостійкої архітектури кіберзахисту в умовах обмежених кадрових та фінансових ресурсів. Стаття може бути корисною для фахівців із кібербезпеки критичної інфраструктури, системних архітекторів та посадових осіб органів місцевого самоврядування.

Ключові слова: кіберзахист міських систем; SIEM; центр кіберзахисту; кореляція інцидентів; MTTD; MTTR; цифрові міські сервіси; кіберстійкість; критична інфраструктура.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
2. Mahn, A. (2018, April 16). *Identify, Protect, Detect, Respond, and Recover: The NIST Cybersecurity Framework*. NIST Taking Measure Blog. https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework

3. Naserinia, V., Ekstedt, M., & Asplund, M. (2021). *Cyber Resilience for Critical Infrastructure: A Systematic Literature Review*. KTH Royal Institute of Technology. https://www.diva-portal.org/smash/get/diva2:1576950/FULLTEXT03.pdf
4. Bellini, E., Marrone, S., & Di Mauro, N. (2025). Situation awareness for cyber resilience: A review. *International Journal of Critical Infrastructure Protection, 48,* Article 100720. https://doi.org/10.1016/j.ijcip.2025.100755
5. Cybersecurity Ventures. (2024). *SIEM Implementation: Strategies and Best Practices*. Cybersecurity Ventures. https://cybersecurityventures.com/siem-implementation-strategies-and-best-practices/
6. Cymulate. (2025). *SIEM Correlation Rules: Fine-Tune Detection Logic at Scale*. Cymulate Glossary. https://cymulate.com/cybersecurity-glossary/siem-correlation-rules/
7. Redborder. (2024, September 10). *How SIEM correlation rules work*. Redborder Blog. https://redborder.com/how-siem-correlation-rules-work/
8. Subach, I. Yu., Fesokha, V. V., & Fesokha, N. O. (2019). Model proaktyvnoi intelektualnoi SIEM-systemy dlia kiberzahystu obiektiv krytychnoi infrastruktury [Model of proactive intellectual SIEM-system for cyber protection of critical infrastructure objects]. *Information Technology and Security, 7*(2), 209–216. https://doi.org/10.20535/2411-1031.2019.7.2.190570
9. Hnatiuk, S. O. (2023). Systema koreliuvannia podii ta upravlinnia intsydentamy kiberbezpeky na obiektakh krytychnoi infrastruktury [Event correlation and cyber security incident management system at critical infrastructure objects]. *Cybersecurity: Education, Science, Technique, 19*, 161–174. https://doi.org/10.28925/2663-4023.2023.19.176196
10. Piadyshev, V. H. (2022). Kiberbezpeka krytychnykh infrastruktur: zakordonnyi dosvid ta ukrainski realii [Cybersecurity of critical infrastructures: foreign experience and Ukrainian realities]. *South Ukrainian Law Journal, 4*(3), 229–234. https://doi.org/10.32850/sulj.2022.4.3.38
11. Zubok, V. Yu., Davydiuk, A. V., & Klymenko, T. M. (2023). Cybersecurity of critical infrastructure in Ukrainian legislation and in Directive (EU) 2022/2555. *Electronic Modeling, 45*(5), 54–66. https://doi.org/10.15407/emodel.45.05.054
12. Grechaninov, V., Hulak, H., Sokolov, V., Skladannyi, P., & Korshun, N. (2022). Formation of dependability and cyber protection model in information systems of situational center. In *Proceedings of the 1st International Workshop on Control, Optimisation and Analytical Processing of Social Networks (COAPSN-2022)* (pp. 107–117). CEUR Workshop Proceedings, Vol-3149. https://ceur-ws.org/Vol-3149/paper11.pdf