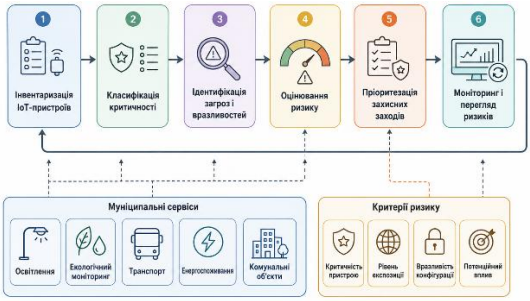

Рис.1. Ризик-орієнтований підхід до захисту IoT-пристроїв у муніципальних системах

З урахуванням сучасного ландшафту загроз особливої уваги потребують атаки на доступність, експлуатація відомих вразливостей, компрометація облікових даних і підміна даних. Можемо визначити загрози даним, атаки на доступність, соціальну інженерію та експлуатацію вразливостей серед провідних напрямів кіберзагроз Отже, ризик-орієнтований підхід дає змогу перейти від фрагментарного технічного захисту до системного управління безпекою муніципальних IoT-сервісів, раціонально розподіляти ресурси громади та підвищувати стійкість міської цифрової інфраструктури. Подальші дослідження доцільно спрямувати на кількісну модель оцінювання ризиків, автоматизацію інвентаризації активів та інтеграцію цього підходу з платформами моніторингу кібербезпеки [3,4].

1. Alavi A.H. et al. Internet of Things-enabled smart cities: State-of-the-art and future trends. Measurement. 2018. Vol. 129. P. 589-606.
2. Elmaghraby A.S., Losavio M.M. Cyber security challenges in smart cities: Safety, security and privacy. Journal of Advanced Research. 2014. Vol. 5(4). P. 491-497.
3. Tok Y.C., Chattopadhyay S. Identifying threats, cybercrime and digital forensic opportunities in smart city infrastructure via threat modeling. Forensic Science International: Digital Investigation. 2023. Vol. 45. Article 301540.
4. Kumar V. et al. Challenges in the design and implementation of IoT testbeds in smart-cities: A systematic review. arXiv:2302.11009. 2023.

Development of an artificial intelligence-driven managed detection and response framework for proactive enterprise cyber defense

UDK 004.056.53(043.2)

Kyrylo Kurchak

National University of Water and Environmental Engineering,
kurchak_ak21@nuwm.edu.ua

The continuous evolution of enterprise computing paradigms, characterized by the widespread adoption of hybrid cloud architectures, distributed microservices, and extensive remote-work infrastructures, has radically expanded the corporate attack

surface. Modern corporate networks generate an unprecedented volume of multi-layered telemetry streams originating from endpoints, cloud logging facilities, database management systems, and network perimeter devices [1, 5]. Security Operations Centers (SOCs) tasked with monitoring these vast data landscapes are increasingly overwhelmed by the sheer scale, velocity, and complexity of incoming alerts, a phenomenon that introduces critical operational risks [2]. Traditional security monitoring infrastructures rely heavily on static, rule-based signature detection mechanisms that evaluate events in isolation, failing to correlate disparate activities across different environment layers [3]. Consequently, human security analysts are subjected to pervasive alert fatigue, wherein thousands of low-fidelity warnings obscure the subtle, highly distributed indicators of compromise characteristic of advanced persistent threats (APTs) and sophisticated multi-stage cyber campaigns [3, 5].

This operational bottleneck is further exacerbated by the severe global shortage of specialized cybersecurity personnel capable of conducting deep forensic investigations under tight time constraints. When security analysts are forced to manually investigate, parse, and triage millions of continuous data events every day, the time elapsed between an initial perimeter breach and its subsequent identification — commonly referred to as threat dwell time — extends to unacceptable levels [1, 3]. Sophisticated adversarial groups exploit this visibility gap by deploying stealthy, living-off-the-land techniques, utilizing legitimate system administration tools to execute malicious actions that easily evade isolated endpoint detection rules. The fundamental challenge within modern enterprise cyber defense lies in the inability of conventional security frameworks to rapidly distinguish high-fidelity threat indicators from intense background operational noise, thereby preventing proactive containment and leaving corporate digital assets highly vulnerable to devastating operational disruptions, data exfiltration, and ransomware deployment.

The objective of the work is to design and evaluate an artificial intelligence-driven Managed Detection and Response (MDR) framework that automates high-volume telemetry correlation, accelerates threat containment, and optimizes analyst operational workflow. To achieve this objective, the system utilizes continuous behavioral modeling and cross-layer event correlation to minimize threat dwell time. The realization of this goal requires the systematic execution of several interconnected technical tasks, beginning with the establishment of a highly scalable, multi-layered telemetry ingestion architecture capable of normalizing heterogeneous log schemas into a unified data structure. Following this, automated behavioral analysis models must be developed to leverage machine learning algorithms for establishing dynamic operational baselines for all network entities and user accounts. Additionally, the framework incorporates an intelligent cross-environment orchestration layer designed to correlate separate localized anomalies into a single, comprehensive incident timeline. Finally, the operational performance of the proposed architecture must be validated through rigorous experimental testing against real-world attack vectors to measure improvements in critical security metrics, specifically focusing on the reduction of mean time to detect (MTTD) and mean time to respond (MTTR).

The relevance of this study is underscored by the rapidly escalating frequency, speed, and sophistication of automated cyber threats targeting critical corporate and

state infrastructures. In an era where adversarial actors routinely utilize automated exploit kits, artificial intelligence-driven scanning tools, and rapidly mutating malware variants, the traditional model of episodic or business-hours security monitoring is entirely obsolete [2]. Proactive, uninterrupted 24/7 defensive vigilance is a mandatory operational requirement to safeguard corporate data integrity, preserve financial stability, and maintain compliance with increasingly stringent global regulatory mandates [1, 2]. Organizations that fail to maintain continuous visibility over their digital assets face catastrophic financial liabilities, legal repercussions, and permanent reputational damage following a successful breach.

Managed Detection and Response services have emerged as a critical architectural solution for organizations seeking to achieve robust security coverage without incurring the prohibitive capital and operational expenses associated with building and maintaining a sophisticated, internal 24/7 SOC [3, 5]. However, as corporate networks scale exponentially with the integration of IoT devices and multi-cloud environments, human-centric MDR service designs encounter definitive physical limitations [2, 4]. The incorporation of advanced artificial intelligence models into the core of MDR platforms is highly relevant and urgent, as it provides the only viable computational mechanism to scale threat detection capabilities alongside expanding enterprise data volumes, ensuring that security analysts are empowered with pre-filtered, context-rich intelligence rather than being buried under unmanageable alert volumes [4].

The scientific novelty of this research consists in the development of a unified multi-environment telemetry correlation engine based on the CORTAI platform architecture [4]. Unlike conventional security frameworks that analyze endpoint events, cloud access logs, and network netflow data in isolated, parallel silos, the proposed model mathematically projects multi-layer telemetry into a single, cohesive investigation timeline. This approach advances the state of the art by replacing rigid, retrospective correlation rules with dynamic, context-aware risk scoring that continuously adapts to evolving adversarial techniques based entirely on live behavioral deviations.

Furthermore, the scientific innovation lies in the design of a temporal behavioral modeling approach within the CORTAI architecture that explicitly evaluates the structural and temporal links between independent, seemingly low-severity anomalies occurring across disparate enterprise sectors [4]. By mapping these distributed anomalies into a unified threat progression graph, the system is capable of detecting stealthy, slow-rate attack campaigns that purposefully operate below the detection thresholds of isolated security controls. This formulation successfully shifts the defensive paradigm from historical signature-matching to predictive intent modeling, enabling the early identification of multi-stage adversarial pathways before the final payload execution or data exfiltration phase can occur.

The proposed solution implements a comprehensive, multi-layered Managed Detection and Response architecture natively integrated with the CORTAI security intelligence platform [4]. Telemetry collection is executed via widespread deployment of lightweight endpoint detection and response (EDR) agents, cloud-native API logging facilities, and continuous network flow collectors, ensuring complete visibility across the hybrid corporate infrastructure [1, 2, 3]. These distributed data

sources feed raw log entries into localized ingestion nodes, which apply structural normalization and statistical parsing to transform heterogeneous data formats into a standardized, unified schema. As iThe core analytical engine of the CORTAI platform processes the normalized telemetry streams by applying unsupervised machine learning algorithms to establish dynamic, historical baseline behaviors for every user account, host device, and network interface within the organization [4].

Fig.1. Operational flow of the AI-augmented CORTAI platform from raw telemetry ingestion to predictive visibility

As illustrated in Fig. 1, the CORTAI engine performs automated event correlation by programmatically linking distributed anomalies across the network into pre-assembled investigation dossiers [4]. When a series of localized anomalies collectively exceeds the cumulative security threat score threshold, the platform automatically triggers localized containment playbooks designed to neutralize the threat instantly without requiring manual analyst intervention [5]. These playbooks include executing automated actions such as isolating compromised host devices from the network, revoking compromised user credentials, and modifying perimeter firewall rules [3, 5]. Concurrently, the system delivers a comprehensive, pre-filtered, and highly context-rich evidence dossier directly to senior security analysts for formal validation, preserving valuable human cognitive resources and maintaining an efficient human-in-the-loop oversight model for high-impact mitigation decisions [2].

The design and implementation of the artificial intelligence-driven Managed Detection and Response framework significantly enhances enterprise cybersecurity posture by systematically optimizing operational defensive metrics. By deploying the CORTAI platform as the central analytical engine, the framework achieves a drastic reduction in both the mean time to detect (MTTD) and the mean time to respond (MTTR) when faced with sophisticated, multi-vector adversarial campaigns [4]. The automation of low-level alert triage and context enrichment successfully mitigates the pervasive issue of analyst alert fatigue, allowing human security experts to allocate their specialized cognitive resources exclusively toward proactive threat hunting, deep forensic investigations, and strategic incident response planning [2, 4]. Experimental validation confirms that the proposed multi-layered correlation architecture effectively minimizes false-positive rates, maximizes threat detection coverage across highly complex hybrid infrastructures, and maintains continuous, robust 24/7 enterprise defense capabilities.

1. Hautala T. New Managed Detection and Response System to Lower the Likelihood of Malicious Activities in IP Network. Master's Thesis, Metropolia University of Applied Sciences, Helsinki, 2022. 46 p.
2. Rajgopal P.R., Karanam L. MDR Service Design: Building Profitable 24/7 Threat Coverage for SMBs. International Journal of Applied Mathematics. – 2025. – V. 38, № 2s.
3. Fortinet. What Is Managed Detection and Response (MDR)? URL: https://www.fortinet.com/uk/resources/cyberglossary/managed-detection-and-response (application date: 30.04.2026).
4. MCK. The Role of AI in Managed Detection: How Artificial Intelligence Strengthens MDR Security. URL: https://www.mck.com/blog/role-of-ai-in-managed-detection (application date: 30.04.2026).
5. Rapid7. What Is MDR? Managed Detection and Response Security. URL: https://www.rapid7.com/fundamentals/what-is-managed-detection-and-response-mdr/ (application date: 30.04.2026).

Модель оцінювання кіберризиків IoT-інфраструктури розумного міста

УДК 004.056:004.738.5:004.77

Віталій Левицький[1], Олег Тотоськo[2]
Олександр Добруцький[3]

Тернопільський національний технічний університет імені Івана Пулюя,
[1]levytskyylv@gmail.com, [2]totosko@gmail.com, [3]oleksandrdobruckij@gmail.com

Цифровізація міської інфраструктури передбачає впровадження IoT-пристроїв, сенсорних мереж, edge-вузлів, хмарних платформ і диспетчерських систем для моніторингу довкілля, транспорту, енергоресурсів, відеоспостереження та аварійного реагування. Зростання кількості підключених компонентів формує кіберфізичне середовище, у якому порушення безпеки даних має інформаційні, організаційні й технологічні наслідки. Традиційні підходи до управління ризиками орієнтовані переважно на корпоративні мережі й серверну інфраструктуру [1], тоді як міські IoT-системи мають малопотужні пристрої, неоднорідні протоколи, бездротові канали та залежність від хмарних сервісів. За NIST CSF 2.0 управління кіберризиками має охоплювати виявлення активів, захист, моніторинг, реагування й відновлення [2]. Метою роботи є розроблення моделі оцінювання кіберризиків IoT-інфраструктури розумного міста для пріоритезації захисту компонентів з урахуванням критичності, експозиції, вразливостей і зрілості захисних заходів. Новизна полягає в поєднанні логіки «загроза — вразливість — наслідок» із параметрами IoT-середовища: відкритістю, залежностями, сегментацією та рівнем захисту. Модель передбачає інвентаризацію активів, профіль загроз, оцінювання вразливостей, визначення впливу на сервіси, розрахунок інтегрального ризику та пріоритезацію заходів. До активів належать сенсори, виконавчі пристрої, шлюзи, edge-вузли, мережеве обладнання, API, бази даних, хмарні сервіси та операторські панелі.