Comparative analysis of Shodan and Censys platforms for assessing IoT exposure

Mari-Anais Sachian,
Beia Consult International, Bucharest, Romania
anais.sachian@beia.ro

Maria Niculae,
Beia Consult International, Bucharest, Romania
maria.niculae@beia.ro

George Suciu,
Beia Consult International, Bucharest, Romania
george@beia.ro

Vlad-Andrei Ionescu,
Beia Consult International, Bucharest, Romania
ionescuvlad31@gmail.com

Mihai-Sorin Lazăr,
Beia Consult International, Bucharest, Romania
mihailazar6@gmail.com

Abstract
The exponential growth of Internet of Things (IoT) infrastructures has introduced new cybersecurity challenges, often poorly managed or overlooked. This study aims to compare two major Open Source Intelligence (OSINT) platforms, Shodan and Censys, in order to evaluate their effectiveness in mapping exposed infrastructures and identifying potential vulnerabilities. Previous research has shown the importance of OSINT tools for network reconnaissance and threat intelligence, yet few studies have directly compared their practical accuracy and data coverage. Building on existing analyses of IoT security assessment frameworks, this paper focuses on the empirical differences between two widely used scanning platforms. The research involved extracting 561 IP addresses from the BitTorrent network and querying both Shodan and Censys using their free access interfaces. The analysis assessed detection rates, metadata richness (open ports, protocols, TLS certificates), and capabilities in identifying insecure configurations and outdated software components. The results reveal notable differences between the platforms in detection accuracy, data freshness, and the identification of standard services (HTTP/HTTPS, SSH, FTP, Telnet) as well as IoT-specific protocols (MQTT, CoAP, Modbus). These differences highlight the distinct scanning methodologies and indexing strategies used by each tool. The findings offer practical guidance for researchers and cybersecurity practitioners in selecting appropriate OSINT instruments for large-scale exposure analysis. The paper contributes a structured comparative framework for evaluating OSINT-based network intelligence platforms, enhancing understanding of their limitations and potential applications in securing IoT ecosystems.

Keywords: network reconnaissance, exposure analysis, threat intelligence, data collection methodologies, digital forensics.

1. Introduction

The rapid proliferation of Internet-connected devices, under the umbrella of the Internet of Things (IoT), has transformed both consumer and industrial landscapes, enabling new services and capabilities for smart homes, manufacturing, utilities, and urban infrastructure. However, this growth also brings a surge of cyber-security challenges: many IoT devices

are deployed with minimal or no hardening, leaving services exposed on the public Internet. Misconfigured devices, outdated software, default credentials, or missing encryption can all result in critical vulnerabilities. Indeed, public-facing IoT devices have been repeatedly implicated in large-scale attacks and privacy breaches [1, 2].

To identify and assess such exposure, security practitioners and researchers increasingly rely on open-source intelligence (OSINT) tools. Among them, Shodan and Censys are two of the most widely used Internet-wide scanning platforms. Shodan specializes in discovering devices via banner and port scans [3]. Censys, on the other hand, emphasizes deep metadata collection, including TLS certificates, protocol details, and continuous scanning [4].

Despite their extensive use, few studies provide a direct, empirical comparison of these two platforms in the context of IoT exposure assessment. This gap limits our understanding of their respective strengths and weaknesses, particularly when used for large-scale scanning of devices originating from complex, decentralized networks.

In this work, we perform a comparative analysis of Shodan and Censys with the goal of evaluating their effectiveness in mapping exposed infrastructures and identifying potential vulnerabilities. We draw on a dataset of IP addresses extracted from a peer-to-peer network, query both platforms using their free access interfaces, and systematically compare detection coverage, metadata richness, data freshness, and capability to identify both standard and IoT-specific protocols. Our findings reveal substantial differences between the two tools in terms of detection accuracy, data completeness, and suitability for exposure analysis. The results inform practical guidelines for researchers and practitioners on which OSINT platform, or combination thereof, is better suited for large-scale IoT security assessments.

In doing so, we contribute a structured comparative framework for OSINT-based network intelligence platforms, thereby filling a notable gap in the literature and advancing understanding of their limitations and potential applications in securing IoT ecosystems.

2. State of the art

The security risks associated with the ever-increasing number of Internet-connected devices have motivated a growing body of recent research on IoT exposure, vulnerabilities, and large-scale scanning. Several works emphasize that many IoT deployments remain poorly secured, often exposing services with default credentials, weak or no TLS, or outdated software components. For example, Securing IoT Devices Against Emerging Security Threats (2023) provides a comprehensive overview of common security threats affecting IoT devices, including weak authentication, misconfiguration, and insecure transport, highlighting the difficulty in applying traditional security practices in heterogeneous and resource-constrained IoT environments [5].

Another significant contribution is A Large-scale Empirical Study on the Vulnerability of Deployed IoT Devices (2024), which evaluated over 1.3 million IoT devices. The authors found that around 28.3% of devices suffered from at least one known (“N-days”)

vulnerability; they also highlighted major inconsistencies among different IoT-search engines (including Shodan and Censys), suggesting that no single tool provides a complete picture [6].

Using OSINT tools for security assessment, especially search engines like Shodan, has been validated as an effective approach in specialized domains. For instance, Detection of Vulnerabilities in Smart Buildings Using the Shodan Tool (2023) applied Shodan to identify misconfigured devices in building-automation systems, showing how open Internet exposure can compromise availability, confidentiality, and occupant safety [7].

More broadly, concerns have been raised about the operational practices of device-search engines themselves. The recent study Revealing the Black Box of Device Search Engine: Scanning Assets, Strategies, and Ethical Consideration (2024) analyzed the internal scanning behavior of major "search-engine for devices" platforms (including Shodan and Censys), and demonstrated that these engines often scan without transparency, use a broad set of scanner IP addresses, and may collect more data than what is publicly disclosed, raising ethical, privacy, and reliability questions [8].

In parallel, recent work has explored the security posture of IoT-specific protocols. The study Large-Scale Security Analysis of Real-World Backend Deployments Speaking IoT-Focused Protocols (RAID 2024) examined hundreds of thousands of back-end services using IoT-oriented protocols (e.g. MQTT, CoAP, XMPP), revealing that the vast majority use insecure transport (only 0.16% adopt TLS), and many expose sensitive information or are vulnerable to denial-of-service attacks [9].

Complementary research presented in the Smart Cities International Conference (SCIC) proceedings further illustrates how IoT technologies are integrated into critical smart-city applications and why their secure deployment is essential. For example, Danila et al. propose an IoT-based platform for real-time environmental monitoring in museums to protect cultural heritage assets, relying on cloud-connected sensors and continuous data collection [10]. For example, a SCIC study presents a city-scale IoT-based water-incident monitoring system, illustrating how widespread deployment of sensor networks in urban infrastructure can significantly broaden the attack surface of smart-city services [11]. [11]. From a defensive perspective, Waizel introduces a modern honeypot model tailored to smart cities, designed to detect ransomware and advanced persistent threats targeting heterogeneous IoT-rich environments, and highlights the role of deception and early-warning mechanisms in cyber resilience [12].

Collectively, these recent contributions underscore several key insights relevant to exposure analysis:

- Many IoT devices remain vulnerable long after deployment, due to weak default settings, lack of updates, or insecure protocols.
- OSINT search engines like Shodan (and by extension, Censys) are widely used and effective in mapping the Internet exposure of such devices, but data coverage and completeness can vary substantially across engines.

- The metadata retrieved via Internet-wide scanning (open ports, banners, TLS certificates, protocol support) is instrumental in assessing risk, but the internal scanning strategies and ethical implications of these tools warrant careful scrutiny.
- Combining scan-based data with protocol-specific analysis (e.g. for MQTT, CoAP) and insights from real-world smart-city deployments [10–12] can reveal deeper systemic weaknesses in IoT ecosystems.

Despite these advances, there remains a gap in the literature: few studies offer a head-to-head, empirical, large-scale comparison between major OSINT platforms (especially Shodan vs. Censys), specifically in the context of IoT exposure detection, particularly with regard to detection coverage, metadata richness, freshness, and ability to identify IoT-specific protocols. This is the gap the present work aims to fill.

3. Methodology

The methodological approach adopted in this study is designed to systematically evaluate and compare the capabilities of two major OSINT platforms, Shodan and Censys, in identifying exposed infrastructures and IoT-related vulnerabilities. The process integrates structured data collection, rigorous preprocessing, and a unified risk-assessment framework to ensure comparability across platforms.

3.1. Data Collection

The dataset used in this study originates from publicly reachable IP addresses collected from a peer-to-peer environment, chosen for its heterogeneity and relevance for real-world exposure analysis. After initial parsing and filtering, the resulting set of 561 unique IP addresses was used as input for the scanning phase.

Both Shodan and Censys were queried using their publicly available search interfaces. Due to inherent API limitations, including rate throttling, query size restrictions, and daily usage caps, the dataset was processed in smaller sub-batches to ensure complete coverage. The queries targeted each IP individually or in small groups, requesting comprehensive metadata such as:

- open ports and exposed services
- protocol banners
- TLS configuration details
- certificate attributes
- identified software products and versions
- HTTP headers and authentication requirements

Data from each platform was retrieved in JSON or structured output format and stored for subsequent processing.

3.2. Data Processing Workflow

The collected data was preprocessed and normalized to enable direct comparison between Shodan and Censys results. This step addressed the heterogeneity of metadata formats, variable naming conventions, and inconsistent completeness of fields across platforms.

The workflow consisted of the following steps:

1. Parsing and normalization:
- extraction of IP-level metadata from JSON responses
- unification of service descriptors and port mappings
- normalization of protocol, software, and TLS fields
2. Service and port enumeration:
- identification of the total number of detected services
- counting of open ports based on validated port ranges
- classification of service types (e.g., HTTP, SSH, FTP, Telnet)
3. Protocol security assessment:
- detection of insecure or IoT-specific protocols (e.g., MQTT, CoAP, SSDP, mDNS)
- identification of deprecated TLS versions
4. TLS and certificate analysis:
- evaluation of the presence or absence of TLS
- extraction of certificate properties (expiration, issuer type, key length)
5. Software fingerprinting:
- extraction of software products and versions reported by banners
- categorization of outdated or unsupported components
6. HTTP security evaluation:
- detection of missing security headers (HSTS, X-Frame-Options, CSP, X-Content-Type-Options)
- identification of services that fail to require authentication
7. De-duplication and correlation:
- merging platform outputs
- resolving conflicting metadata
- assembling unified records for each IP

The resulting dataset provides a consolidated representation of exposure indicators, enabling both cross-platform comparison and risk scoring.

3.3. Exposure and Risk Assessment Framework

To assess the security posture of the scanned IP addresses, a unified risk-evaluation framework was developed. The framework integrates multiple categories of indicators extracted from both platforms:

- Exposure breadth: number of services and open ports
- Protocol security: presence of insecure or IoT-specific protocols, usage of deprecated TLS versions
- Cryptographic robustness: absence of TLS, expired or self-signed certificates, weak cryptographic parameters
- Software hygiene: detection of exposed software components, presence of known outdated versions
- Access control and HTTP hardening: failure to require authentication, missing critical HTTP security headers

Each indicator category contributes to an aggregated exposure profile. Although no sensitive weighting scheme is disclosed, the assessment prioritizes misconfigurations that

directly increase the accessibility of a device to unauthorized entities, consistent with principles commonly applied in vulnerability assessment research.

This framework enables a consistent evaluation of IPs regardless of the differences in metadata detail between Shodan and Censys. It also facilitates the identification of systemic vulnerability patterns within the dataset.

4. Comparative Analysis of Shodan and Censys

This section presents a structured comparison between Shodan and Censys based on the empirical results obtained from querying both platforms for the same set of IP addresses. The analysis focuses on four key dimensions: detection coverage, metadata completeness, data freshness, and capability to identify IoT-specific protocols. Together, these dimensions offer a comprehensive view of how the platforms perform as OSINT tools for exposure analysis.

4.1. Detection Coverage

Detection coverage refers to the ability of each platform to successfully identify an IP address as active and to enumerate its associated services. Although both platforms use large-scale scanning infrastructures, they differ in methodology and scanning frequency.

Shodan tends to provide broader initial coverage for responsive hosts. Its scanning strategy is optimized for banner grabbing and quick service identification across a wide range of ports. As a result, Shodan frequently detects a higher number of IPs as active, especially when dealing with hosts that expose commonly scanned ports (e.g., HTTP, SSH, Telnet, FTP).

Censys, on the other hand, adopts a more targeted approach, focusing on fewer ports but performing deeper protocol-level inspection. Its certificate-based scans, for instance, allow detection of hosts that expose TLS-enabled services even when banner information is limited. However, this deeper but narrower scanning strategy can result in a smaller number of IPs being classified as active compared to Shodan.

Across the dataset, Shodan generally identified a greater proportion of the IPs as responsive, while Censys provided richer detail for those it did detect. This divergence highlights the complementary nature of the two tools: Shodan excels in breadth, while Censys excels in depth.

4.2. Metadata Completeness

Metadata completeness captures the richness and granularity of information retrieved for each IP. This includes port-level details, service banners, TLS configurations, certificate attributes, software fingerprints, and HTTP header information.

Censys consistently offers more complete metadata, especially related to encryption and protocol configuration. Its scanning architecture allows extraction of:

- certificate chains and issuers
- key lengths and cryptographic parameters

- TLS versions and cipher suites
- protocol-specific fields
- detailed service fingerprints

Censys' dataset is structured with a strong emphasis on security posture, making it particularly useful for vulnerability assessments centered on cryptography and protocol correctness.

Shodan's metadata, although broad, is generally more variable in detail. It reliably captures service banners and open ports, offering a practical overview of exposed services. However, advanced fields, such as full certificate chain analysis, security header evaluation, or extended protocol metadata, are sometimes missing or incomplete unless the service explicitly returns this information in its banner.

Overall, Censys outperforms Shodan in metadata richness, while Shodan provides broader but less granular coverage.

4.3. Accuracy and Freshness of Scan Data

The accuracy and freshness of scan data depend on how frequently each platform updates its index of the Internet.

Censys performs continuous scanning, particularly for TLS-enabled services. This enables it to maintain relatively fresh datasets for protocols such as HTTPS, SMTPS, and other encrypted services. When evaluating cryptographic posture, Censys' results tend to more accurately reflect the current configuration of a host.

Shodan's scanning schedule is periodic, with the frequency depending on port importance and historical responsiveness. Popular ports (e.g., 80, 443, 22) are scanned more frequently, while less common ports may exhibit longer update intervals. This variability can occasionally lead to detection of services that have since been modified or removed.

In practice:

- Censys showed fewer stale entries, especially for certificate data.
- Shodan occasionally reported older service configurations but provided broader detection.

Thus, Censys demonstrates better freshness for critical security attributes, whereas Shodan provides more extensive but sometimes less up-to-date service inventories.

4.4. Identification of IoT-Specific Protocols

IoT ecosystems rely heavily on specialized protocols such as MQTT, CoAP, SSDP, mDNS, and Modbus. Identifying these protocols is crucial for exposure analysis since they often lack strong authentication or encryption mechanisms.

Shodan has stronger detection capabilities for banner-based IoT protocols, particularly:

- MQTT

- CoAP
- Modbus
- Telnet–based embedded interfaces
- proprietary vendor services

Its broad port scanning strategy increases the likelihood of detecting such services, especially when devices expose readable banners that identify themselves.

Censys, while highly effective in analyzing TLS-enabled services, is more limited in detecting lightweight or UDP-based IoT protocols. Many IoT protocols operate over unencrypted channels or nonstandard ports that fall outside Censys' regular scanning range. As a result:

- Censys is strong in detecting secure IoT services (e.g., MQTT over TLS),
- but weaker in detecting unsecured or UDP-based IoT protocols.

When comparing both platforms across the dataset:

- Shodan identified a wider range of IoT-specific protocols.
- Censys provided deeper details for the subset of devices using encrypted or standards-compliant configurations.

Overall, Shodan is better suited for wide discovery of IoT-protocol exposure, while Censys is more informative when analyzing encrypted IoT deployments.

5. Results

This section presents the empirical results obtained from querying Shodan and Censys for the selected dataset. The analysis focuses on exposure statistics, comparative performance between the two OSINT platforms, and observed vulnerability patterns derived from unified data processing.

5.1. Exposure Statistics

The exposure statistics summarize the security-relevant attributes identified across the scanned IP addresses. These values reflect the aggregated indicators extracted during the analysis phase.

Service and Port Exposure: A considerable portion of the scanned infrastructure was found to expose multiple services simultaneously:

- 30 IPs were identified as exposing more than 10 services, indicating a wide attack surface.
- 29 IPs showed more than 10 open ports, reinforcing the trend of broad exposure and potential misconfiguration.

Such levels of exposure increase the likelihood of attack vectors linked to lateral movement, enumeration, or unauthorized access.

Insecure Protocols: The dataset revealed widespread usage of insecure or plaintext protocols:

- 178 IPs were found using at least one insecure protocol.
- The most frequently identified insecure protocols were: CoAP, DNS, and TLSv1.0 (deprecated).

These protocols lack adequate encryption or authentication mechanisms, making them vulnerable to interception or spoofing.

TLS and Certificate Issues: Transport security analysis identified several shortcomings:
- 89 IPs did not support TLS at all, exposing services in unencrypted form.
- 62 IPs presented expired or self-signed certificates, reducing trust and enabling man-in-the-middle attacks.

Software Exposure: Software fingerprinting highlighted:
- 95 IPs running publicly exposed software components.
- 55 IPs using outdated software, which increases susceptibility to known vulnerabilities.

Authentication and HTTP Security Headers: Access control analysis showed:
- 155 IPs did not require authentication for at least one exposed service.
- 65 IPs lacked essential HTTP security headers, such as HSTS, CSP, or X-Frame-Options, weakening web-service hardening.

Overall, the exposure statistics illustrate a high prevalence of insecure configurations, consistent with trends reported in recent IoT security literature.

5.2. Comparative Performance

This subsection analyzes how Shodan and Censys performed relative to each other along key dimensions.

Detection Breadth: Shodan identified a larger number of active IPs and exposed services, largely due to its broader port-scanning strategy. This makes Shodan more effective for initial discovery and enumeration.

Metadata Depth: Censys demonstrated superior detail in specific areas:
- TLS versions
- certificate chains
- cryptographic key properties
- enriched HTTP and service metadata when available

This makes Censys more suitable for in-depth vulnerability assessment.

Consistency Across Scans: Shodan showed occasional inconsistencies, such as outdated banners for services that had since been modified. Censys provided more stable results for encrypted services but missed some non-TLS or UDP-based protocols that Shodan captured.

IoT-Protocol Visibility: Shodan outperformed Censys in detecting IoT-specific protocols (MQTT, CoAP, Modbus), largely because many of these protocols lack TLS and produce identifiable plaintext banners.

In summary, Shodan excels in breadth and IoT-specific visibility, while Censys excels in depth and cryptographic accuracy.

The platforms behave not as substitutes but as complementary tools for comprehensive exposure analysis.

5.3. Observed Vulnerability Patterns

Correlating all extracted attributes revealed several recurring patterns that characterize the security posture of the analyzed infrastructure.

1. ***Prevalence of Weak or Missing Encryption***

A significant fraction of devices used deprecated TLS versions or lacked TLS entirely. This indicates outdated firmware, weak configuration practices, or resource-constrained IoT devices incapable of supporting modern encryption.

2. ***Use of Insecure or Legacy IoT Protocols***

Protocols such as CoAP, mDNS, SSDP, and MQTT were frequently exposed. These protocols are widely used in IoT deployments but often lack native security features, making them attractive entry points for attackers.

3. ***High Rate of Missing Authentication***

Many services responded without requiring authentication, particularly admin interfaces or embedded web portals. This reflects common misconfigurations in IoT environments, where usability often takes precedence over hardening.

4. ***Outdated Software and Components***

Numerous services reported outdated versions of software stacks, operating systems, or server applications. These outdated versions are likely to contain known vulnerabilities that can be exploited using publicly available tools.

5. ***Deficient Web-Service Hardening***

The absence of key HTTP security headers indicates insufficient hardening of web interfaces. This increases exposure to clickjacking, MIME-type confusion, or downgrade attacks.

6. ***Fragmented Exposure Across Platforms***

Some vulnerabilities were detected by only one platform:

- Shodan identified more insecure IoT protocols.
- Censys identified more certificate-related weaknesses.

This fragmentation reinforces the necessity of multi-platform OSINT strategies.

6. Conclusions

This study provided a systematic comparative analysis of two widely used OSINT platforms, Shodan and Censys, focusing on their effectiveness in identifying exposed infrastructures and assessing IoT-related vulnerabilities. Using a dataset of 561 publicly reachable IP addresses, we examined four key dimensions of platform performance: detection coverage, metadata completeness, data freshness, and capability to identify IoT-specific protocols.

The results demonstrate that Shodan and Censys exhibit complementary strengths.

Shodan excels in broad detection, identifying a larger number of active hosts and capturing a diverse set of exposed services, including lightweight and banner-based IoT protocols such as MQTT, CoAP, and Modbus. Its wide port-scanning strategy makes it particularly effective for initial reconnaissance and exposure mapping.

Conversely, Censys provides greater metadata depth and more accurate insights into cryptographic posture. Its continuous scanning of TLS-enabled services allows for detailed evaluation of certificates, key parameters, and encryption configurations. This level of granularity is essential for analyzing transport-layer security and identifying weaknesses in encrypted IoT deployments.

The unified exposure analysis revealed significant security issues across the scanned infrastructure, including widespread use of insecure protocols, outdated software, missing authentication, deprecated TLS versions, and insufficient web-service hardening. These findings align with recent research indicating that many IoT devices remain vulnerable long after deployment due to weak configuration practices and limited update mechanisms.

Importantly, several vulnerabilities were detected by only one of the two platforms, highlighting the fragmented visibility inherent to OSINT tools. This observation reinforces a key implication of our work: using a single Internet-wide scanner provides an incomplete view of IoT exposure, whereas combining Shodan and Censys yields a significantly more accurate and comprehensive assessment.

Overall, the study contributes a structured comparison of Shodan and Censys and offers practical guidance for researchers, security analysts, and organizations seeking to evaluate large-scale IoT exposure. Future work may extend this research by integrating machine learning techniques for automated risk scoring, exploring additional OSINT sources, and conducting longitudinal analyses to observe how exposure patterns evolve over time.

Acknowledgements

This study was supported by UEFISCDI through the project CIRANET, Contract no. 8 dated 23/10/2024, Project Code: EUROSTARS-3-E!6335-CIRANET-1.

References

[1] Rytel, Marcin, Anna Felkner, and Marek Janiszewski. "Towards a safer internet of things—a survey of iot vulnerability data sources." *Sensors* 20.21 (2020): 5969.

[2] Rajasekar, V. R., and S. Rajkumar. "A study on Internet of Things devices vulnerabilities using Shodan." *International Journal of Computing* 22.2 (2023): 149-158.

[3] Mulero-Palencia, Sofía, and Victor Monzon Baeza. "Detection of vulnerabilities in smart buildings using the Shodan tool." *Electronics* 12.23 (2023): 4815.

[4] Durumeric, Zakir, et al. "Censys: A Map of Internet Hosts and Services." *Proceedings of the ACM SIGCOMM 2025 Conference*. 2025.

[5] Aziz Al Kabir, Mohammed, Wael Elmedany, and Mhd Saeed Sharif. "Securing IOT devices against emerging security threats: Challenges and mitigation techniques." *Journal of Cyber Security Technology* 7.4 (2023): 199-223.

[6] Zhao, Binbin, et al. "A large-scale empirical study on the vulnerability of deployed IoT devices." *IEEE Transactions on Dependable and Secure Computing* 19.3 (2020): 1826-1840.

[7] Mulero-Palencia, Sofía, and Victor Monzon Baeza. "Detection of vulnerabilities in smart buildings using the Shodan tool." *Electronics* 12.23 (2023): 4815.

[8] Wu, Mengying, et al. "Revealing the Black Box of Device Search Engine: Scanning Assets, Strategies, and Ethical Consideration." *arXiv preprint arXiv:2412.15696* (2024).

[9] Tagliaro, Carlotta, et al. "Large-scale security analysis of real-world backend deployments speaking IoT-focused protocols." *Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses*. 2024.

[10] DANILA, Andrei, et al. “IoT Systems for Efficient Preservation of Cultural Heritage”. *Smart Cities International Conference (SCIC) Proceedings*, vol. 11, June 2024, pp. 515-26, https://www.scrd.eu/index.php/scic/article/view/515.

[11] VOICU, Ioan Florin, and Daniel Constantin DIACONU. “Monitoring City Water Incidents via an Internet of Things-Based Sensor Network”. *Smart Cities International Conference (SCIC) Proceedings*, vol. 10, Oct. 2023, pp. 207-14, https://scrd.eu/index.php/scic/article/view/436.

[12] WAIZEL, Guy. “Using a Modern Honeypot Model to Defend Smart Cities and Provide Early Detection to APT and Ransomware Attacks”. *Smart Cities International Conference (SCIC) Proceedings*, vol. 10, Oct. 2023, pp. 33-46, https://scrd.eu/index.php/scic/article/view/423.