International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 5, Sep-Oct 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

# Intrusion Lens: Real-Time Shellbag, Jumplist, and Recent Docs Analysis for Insider Threat Detection

Shloka Shah[1], Keshvi Mistry[2], Aditya More[3], Dr. Kapil Kumar[4]

1,2- Student, Integrated M.Sc. Cyber Security and Forensics
3- Teaching and Research Associate, Cyber Security and Forensics
4- Associate Professor and Co-ordinator

1,2,3,4- Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, INDIA

----------**********----------

## Abstract:

With the increasing frequency of insider threats in today's cybersecurity landscape, there is a need for better, more proactive monitoring tools to enhance visibility to user behavior as well as privacy violations required by law. Conventional solutions are designed with a network point of view; therefore, they fail to see suspicious activity at the endpoint, especially by people who have legitimate access. This research proposes Intrusion Lens - a real-time monitoring tool that examines Windows forensic artifacts, Shellbags, Jumplists, and RecentDocs, to see user interactions with files and directories and identifies anomalous file access behavior for potential insider threats. Intrusion Lens expands the current forensic state of the art to include continuous monitoring, access to behavioral patterns, and automated email alerts to suspicious/abnormal access to private data. Intrusion Lens works right at the endpoint to view local-level actions otherwise potentially missed. By identifying local-level access activity, it supports shorter response times, reduces potential data breaches, and generally improves an organization's overall security posture. In addition, the study examines the effectiveness and responsiveness of real-time alerts on incident response efficiency (moving from reactively responding to proactive forensic intentions). This dissertation outlines the design, development, and testing of Intrusion Lens to address current deficiencies in real-time insider threat detection, stressing the real-world utility of enhancing digital forensics. The study offers efficiency and scale to modern enterprise needs while stressing data privacy and providing rapid threat mitigation, ultimately situating the study within the wider area of cybersecurity.

*Keywords* **— Insider Threats, Digital Forensic, Shellbags Analysis, Jumplist Monitoring, Real-Time Detection, Intrusion Lens, Cybersecurity.**

----------**********----------

## I. INTRODUCTION

In the dynamic cybersecurity landscape we navigate, organizations are increasingly focused on protecting their digital assets from threats—both internal and external. Insider threats can be driven by malicious intent, human error—or negligence, or compromised user credentials; all competitive risks to organizational security, typically ending with data breaches, theft of intellectual property, and significant financial and reputational damage. Insider threats are difficult to detect because insiders have legitimate access to systems, files, and networks, allowing them to evade perimeter-based defences.

While modern security solutions are increasingly sophisticated, they have yet to fully consider the nuances of user behaviour at the endpoint level. Intrusion detection systems (IDS), Security Information and Event Management (SIEM) solutions, and network log analysis continue to dominate many organizations' defences. These

  

security solutions are good at identifying network anomalies, brute-force attempts, or external attacks, but they often leave organizations blind to behavioural patterns that hint at insider misuse. These blind spots leave organizations vulnerable, especially in cases where indicators of compromise did not generate noticeable traffic or events at the network level.

Through our research and field observations, we determined three major gaps in the existing monitoring and forensic systems that delay recognition and response to insider threats:

1. Over-reliance on network data: Most systems rely on network logs and access control events, but these are usually prefaced with some endpoint behaviours like local file browsing or document interactions that play an essential role in discerning user intent.
2. Lack of proactive automation: Investigative processes lack proactive automation and tend to be post-mortem—the reliance is on after-the-fact log analyses or memory dumps—meaning we're only able to discover potential threats once the offense has already taken place.
3. No real-time alerts or artifact-level forensic visibility: Existing tooling tends to lack the scope or timing to correctly capture artifacts like Shellbags, Jumplists, or RecentDocs. The amount of time it takes to discover recent artifacts has a negative impact on incident response speed and contextual intelligence.

The context of these issues means there is a clear need to reconsider how this endpoint activity is monitored and analyzed. There's a balance between monitor system logs produced by firewalls, access locks, or compiled logs through SIEMs and transitioning to continuously monitoring and processing user behavior with the operating system. For example, forensic artifacts like Shellbags, which provide information about accessed and created folders; Jumplists which notes used applications and accessed files; or RecentDocs, which lists documents accessed recently provide rich insight into the user's behavior and intent. However, traditionally, the use of these artifacts is fixed to static digital forensics investigations off-line and not utilized, in real time, for future or live detection of real threats.

To tackle these challenges, we propose Intrusion Lens+, a light-weight, real-time forensic monitoring system to identify suspicious activities at the system level. Our tool continuously collects and analyses user activities with a focus on key forensic artifacts and logs them into a unified repository in real time. Intrusion Lens is based on the premise that, in the subtle footprint of daily activity by a user, there exist indications of meaningful insider misuse—footprints we can acquire and analyse for anomalies long before critical damage take place. By targeting artifacts, we can monitor access to things such as confidential folders, abnormal frequency of interactions with files, unusual working hour behaviours, or a combination of different situations—many of which are missed by existing monitoring products.

The research taken in this study represents a shift from traditional digital forensics in which endpoint artifacts are used as mainly post-incident value, to real-time digital artifacts in the form of security intelligence. De-constructing the process of artifact collection, correlation, and alert generation through automation, Intrusion Lens+ represents a move from audit-based investigation to proactive threat detection and forensics. In addition, it presents a new phased discovery for insider threats in which user intent and behavior and forensic tracer are addressed together in sufficient levels of detail to develop a resilient and secure operating environment.

## II. METHODOLOGY

This study aimed to resolve the issue of undetected insider threats, while improving real-time digital forensic analysis. The study had a structured approach based on endpoint monitoring from Windows artifact logs. The study had four phases of work: data collection, event detection, alert implementation, and real-time monitoring. Each phase was designed to offer a low impact and practical alternative to traditional network-based intrusion detection systems, focusing instead on the real-time visibility of user actions that could

  

indicate unauthorized access to data for privacy violations.

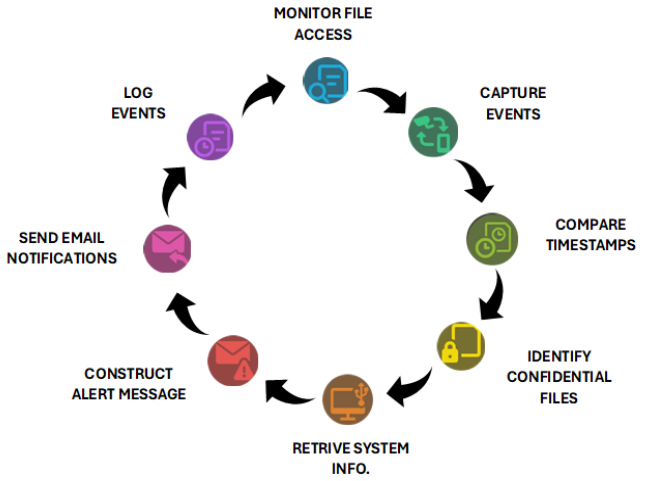


**Figure 1- Real-Time Detection Cycle of the proposed framework**

With its focus on an OS-level, resource-optimized solution and generation of real-time alerts, Intrusion Lens+ departs from the high resource investments and lengthy setups required by traditional ML-based systems or fully integrated cloud monitoring suites. Intrusion Lens+ closes the gap between detection and action through the capability of generating alerts in real-time, intelligently capturing essential system identifiers (hostname, IP address, etc.) and automatically sending structured and timestamped reports to evaluators through automated channels (email by secure OAuth-authenticated APIs).

### A. Data Collection

For data collection we used Python scripts on each endpoint, set to pull specific forensic artifacts from the operating system, including Shellbags, Jumplists, and RecentDocs. These artifacts provide specific insight into user's navigation history, recently opened files, and folders interacted with. By being able to collect periodically and compare a snapshot of these logs, we were able to build a baseline of normal user behavior and identify any deviation from "normal," which may indicate suspicious activity.

### B. Event Detection

Instead of relying on complex machine learning models, this system utilized rules-based logic and heuristics to alert on events of interest. Flags were raised when activities were consistent with white-listed suspicious behavior that concerned the user accessing files out of the ordinary (e.g., late at night), unauthorized access of protected or confidential files, or a frequent number of touches on certain documents. Although simple, these rules were very effective and represented the types of behavior anomalies experienced in insider threat cases

### C. Alert Mechanism

When an anomaly is detected, the system captures important identifying system information such as the hostname and IP address of the workstation. The system created a structured set of alert logs, including the filename accessed, event type detected, and accurate timestamp. This structured summary was sent (as alerts) by email using the Gmail API with OAuth 2.0 authentication, which provides automated secure communication with the security team or administrator for alerts, in near real-time.

### D. Continuous Monitoring

The system was built to run in a loop, allowing for continuous observation in real-time through monitoring. Running in a loop also minimized deleterious overhead of system resources for review. Any and all events that were observed, no matter their categorization of threat, were recorded with timestamps in a central log file stored as monitor.log. This created a monitoring system that allowed immediate reaction through alerting, and also allows forensic audit review at a much later time if necessary. The continuous logs, alongside their alert reports, provided a foundation for prolonged and sustained monitoring, forensic audibility, and incident response.

## III. RESULTS

### A. Overview of Real-Time monitoring of Shellbag, Jumplist and RecentDocs

As business environments become larger and users continue to engage with sensitive digital resources, the demand for intelligent behavior-based security controls is critical. This research shows that real-time forensic artifact monitoring could be a viable predictive technique of insider threat detection. Particularly our solution, Intrusion Lens, that actively monitors three forensic artifacts,

  

Shellbags, Jumplists, and RecentDocs to detect and respond to unauthorized or anomalous actions occurring on the host system.

To make this operational, we created and deployed a lightweight Python agent that runs in the background and watches the host system for artifact changes, recording user activity and identifying anomalous behaviors on the host system. The system's goal was to find suspicious behaviors (for instance, file access out of hours, overstepping privilege level, or accessing potentially sensitive folders without a valid reason).

The areas of monitoring are:

1. Shellbags: Identify user's history as they navigate various directory trees, including folders that generally do get accessed during a normal workflow. These can indicate intent or reconnaissance by an insider.
2. Jumplists: Record files or applications that have been opened and identify how often or how much the application or document has been used.
3. RecentDocs: Record documents that have been opened recently, generally useful for identifying access to confidential or evaluated materials.

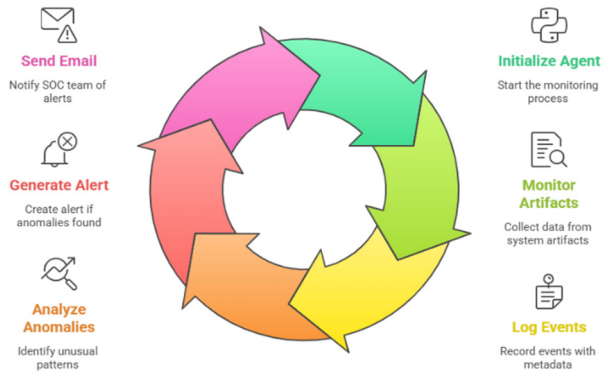


**Figure 2- Real-Time monitoring of Shellbag, Jumplist and RecentDocs**

| Artifact | Description | Use Case |
|---|---|---|
| **Shellbags** | Tracks user's folder navigation history. | Identify reconnaissance behavior. |
| **Jumplists** | Records usage patterns of applications and files. | Detect suspicious usage frequency. |
| **RecentDocs** | Logs recently accessed documents. | Flag sensitive document interactions. |

**Table 1- Important Windows Artifacts**

The system sends real time alerts by email identifying anomalous patterns and can immediately inform security staff before any potential damage is incurred.

### B. Analysis of Monitoring Results

The use of Intrusion Lens in a controlled environment generated several interesting findings that support the hypothesis that real-time artifact monitoring can be an important factor in identifying insider threats. In this section, we provide our analysis:

i) Access Logs of Suspicious Files

The monitoring system included a log file (monitor.log) that actively recorded each event related to users' file access patterns, which allowed us to clearly see the activities pertaining to files and systems. After we performed a review of the log file, we noted findings such as the following:

1. Multiple instances of unauthorized or atypical access attempts, such as opening protected files by users who did not appear to have security clearance for access.
2. High access rates within sensitive directories for certain users during hours the organization was assumed to be closed, suggesting intentional or negligent misuse of access privileges.
3. Access attempts outside the scope of normal business operations revealed access attempts that highlighted potential data reconnaissance or security policy violations.

  

| Pattern | Example | Potential Risk |
|---|---|---|
| Off-hours access | 21:00-06:00 | Unauthorized after-hours behavior |
| High frequency access | Same file opened 10+ times in 1 hr | Data collection or staging |
| Privilege oversteps | File accessed by intern | Insider reconnaissance |

**Table 2- Potential Suspicious Patterns**

We can verify that all the log entries contained structured mandatory metadata, including things such as event timestamps, file name, access action type (open/create/modify), username, and system hostname, which demonstrates very good chain of custody when investigated as part of unauthorized event actions.



**Figure 4- The log entries contained structured mandatory metadata saved as monitor.log**

ii) Email Alert Mechanism

A key aspect of Intrusion Lens is its automated email alerting capabilities. The system was designed to provide life-cycle alerts to the security operations team when a possible breach or anomalous activity was discovered. Each alert email contained the:

- File Name and Event Type (e.g., "Attempted access to HR_Salaries_2023.xlsx - Unauthorized Access")
- Timestamp of Event
- System Name
- Host IP Address

The alerting process would then ensure that any suspicious activity would trigger an immediate response, which followed the principle that the less time between discovery and action would minimize the remain time. In addition, all alert emails were retained as part of the forensic audit trail to allow a review of the incident and methods taken, and the ability to identify repeat threat actors or similar behaviour patterns.

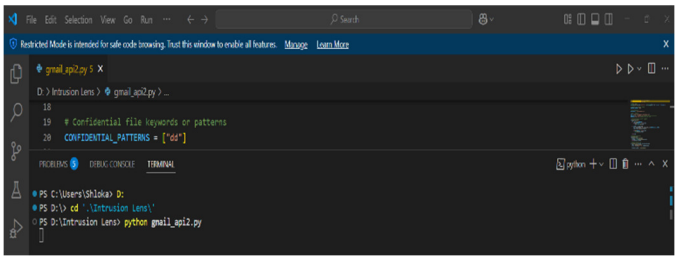


**Figure 5- Intrusion Detection and Response & Confidential Patterns Set**

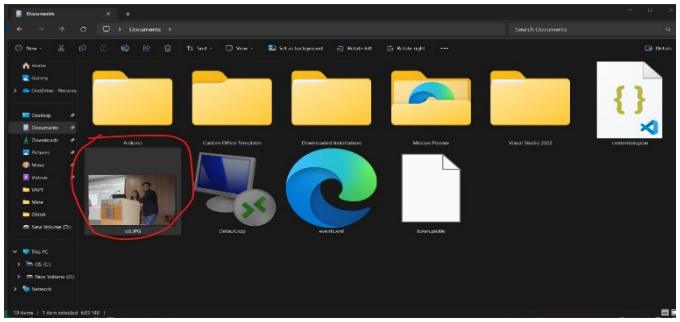

**Figure 6- Confidential File has been accessed**

  

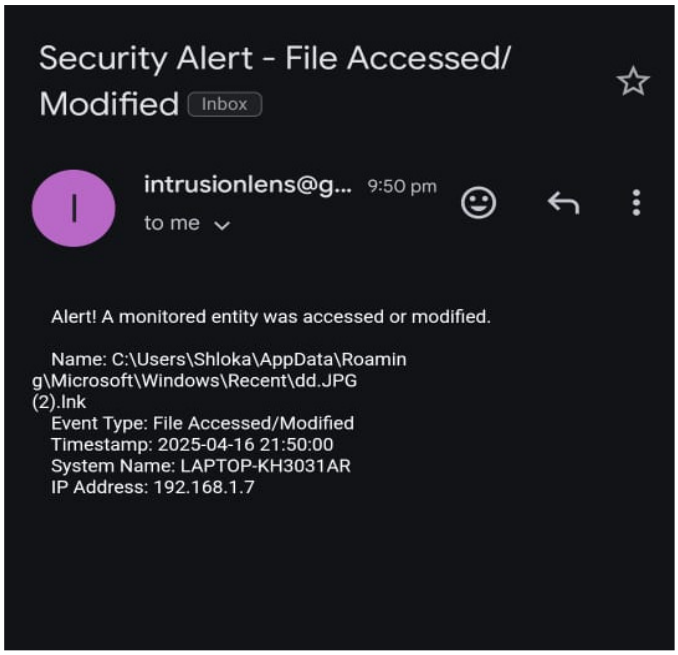


**Figure 7- The email alert is received.**

iii) User Behaviour Analysis

With the continuous monitoring and attentive observation, Intrusion Lens provided useful information about user interaction and often establishes behavioral baselines. Through correlation and pattern recognition, we identified cases of unexpected activity, including the following:

- Abnormal use of sensitive documents through multiple accesses, without business justification or authorization.
- Deviations from normal work patterns, such as nighttime document access by employees whose work hours were fixed.
- Unusual file action; multiple file access; suspected bulk copy; and unexplained file deletions or file renaming events.
- Users attempting to change or circumvent permissions set on files. Similar attempts would indicate an escalation of privilege or an initial stage of preparation for exfiltration.

When a forensic monitoring system incorporates behavioural analytics, Intrusion Lens was able to identify legitimate workflows as separate and distinct from suspicious activity. Instead, the behavioural analytics served as an enhancement to, and part of, an overall threat detection process and audit function.

## IV. DISCUSSION

The development and evaluation of Intrusion Lens demonstrate the idea of leveraging real-time forensic artifact watching as an additional layer of insider threat detection. The system facilitated not only the traditional collection of digital evidence but also converted those artifacts into active signals of risk, that could initiate alerts and drive response.

Key outcomes of this research include:

- Increased visibility of endpoint-level activities, well beyond the limitations of current network monitoring tools.
- Timely alerts that led to intervention in advance of data exfiltration or compromise.
- Structured logs used as credible forensic evidence, providing everything from intent, a sequence of activity, and attribution.

| Category | Insight |
|---|---|
| **Visibility** | Endpoint-level behaviors captured accurately. |
| **Alerts** | Near-instant delivery with actionable data. |
| **Forensics** | Log and alert audit trail for post-incident analysis. |
| **Behavioral Patterns** | Legitimate vs. suspicious workflows established. |

**Table 3- Results of the tool summarized**

This approach, in conjunction with an existing SIEM or EDR, can dramatically reduce response times, improve threat intelligence, and show how to improve policies with respect to user access and data protection.

  

The Intrusion Lens framework is beneficial to any industry that possesses data whose integrity, confidentiality, and availability is critical. Given the ability Intrusion Lens brings to monitoring file and folder access at the systems-level in real-time, users' activities can be observed in a manner that shows greater visibility into user behaviors than traditional cybersecurity solutions. Automated alerts and real-time detections add value to the intrusion lens, as well as traceability and forensic insights. These applications are just a few examples of real-world uses for the system:

1. Healthcare Sector:
   Keeps track of authorized access to patient records and provides alerts for access during off hours or by unauthorized personnel to maintain compliance to HIPAA regulations.
2. Financial Institutions:
   Detects access to sensitive financial documents during off-hours by unauthorized employees.
3. Government and Law Enforcement:
   Flags access to classified files and supports evidence that cannot be tampered with for any internal investigations.
4. Educational Institutions:
   Tracks unauthorized access attempts to grades, research, and exam content.
5. Corporate Enterprises:
   Detects suspicious access with IP, such as source code and legal documents.
6. Critical Infrastructure and Energy:
   Detects insider access to engineering or operational files that could be used to execute sabotage.

## V. CONCLUSION

The main goal of this study was to create a real-time forensic monitoring system to detect unauthorized access to files using forensic artifacts on Windows operating systems. The study successfully demonstrated that monitoring based on artifacts could enhance digital forensics and cybersecurity in significant ways by providing real-time visibility into a user's activities and access patterns.

The Intrusion Lens system proved to be a reliable and efficient tool for identifying unauthorized access and preventing insider threats. By facilitating real-time detection, structured forensic logging, and automated alerts, this tool complements contemporary security frameworks whereby incidents can be addressed in real-time rather than post-breach.

While this research has made significant advancements, it could have addressed future work, which could include:

- Integration with SIEM platforms to provide centralized threat intelligence, and broader visibility of security incidents.
- Enhancing adaptive anomaly detection algorithms, reducing false positives, and improving threat detection accuracy of intrusive events using machine learning.
- Adding monitoring of network-based file access, USB device usage and activity, and tracking potentially malicious activity in cloud storage to provide a more holistic security model.
- Development of forensic reporting modules that produce detailed, legally admissible reports that can foster compliance and legal proceedings.
- Expanding support of Intrusion Lens to monitor Linux and macOS forensics.

## REFERENCES

[1] Amoruso, Edward L., "Privacy and Security of the Windows Registry" (2024). Graduate Thesis and Dissertation 2023-2024. 118.

[2] G. Gonzalez-Granadillo, S. Gonzalez-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," Multidisciplinary Digital Publishing Institute, [Online]. Available: https://doi.org/10.3390/s21144759

  

[3] X. Cai et al., "LAN: Learning Adaptive Neighbors for Real-Time Insider Threat Detection," arXiv.org, vol. abs/2403.09209, Mar. 2024, doi: 10.48550/arxiv.2403.09209.

[4] Amoruso, Edward L., et al. "Seeshells: An optimized solution for utilizing Shellbags in a digital forensic investigation." 2022 IEEE International Conference on Cyber Security and Resilience (CSR), 27 July 2022, pp. 143–148, https://doi.org/10.1109/csr54599.2022.9850296.

[5] Mize, R. (2018). BEHAVIOR OF SHELLBAGS IN WINDOWS 10 [ProQuest]. https://www.proquest.com/openview/490b1eb9d179216a3ba5281a5204e3f1/1?cbl=18750&pq-origsite=gscholar

[6] L. Jones, "Windows 10 Jump List and Link File Artifacts - Saved, Copied and Moved," 2020. [Online]. Available: https://doi.org/10.21428/b0ac9c28.92ca3973

[7] [1] Y. Zhu, P. Gladyshev, and J. James, "Using shellbag information to reconstruct user activities," Digital Investigation, vol. 6. Elsevier BV, pp. S69–S77, Sep. 2009. doi: 10.1016/j.diin.2009.06.009.

[8] A. Đuranec, D. Topolčić, K. Hausknecht and D. Delija, "Investigating file use and knowledge with Windows 10 artifacts," 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2019, pp. 1213-1218, doi: 10.23919/MIPRO.2019.8756877.

[9] "A Visualization Jump Lists tool for Digital Forensics of Windows," KSII Transactions on Internet and Information Systems, vol. 14, no. 1. Korean Society for Internet Information (KSII), Jan. 31, 2020. doi: 10.3837/tiis.2020.01.013.

[10] A. A. Adesina, A. A. Adebiyi, and C. K. Ayo, "Identification of forensic artifacts from the registry of windows 10 device in relation to idrive cloud storage usage," Bulletin of Electrical Engineering and Informatics, vol. 11, no. 1. Institute of Advanced Engineering and Science, pp. 521–529, Feb. 01, 2022. doi: 10.11591/eei.v11i1.3489.

[11] T. Arjunan, "Detecting Anomalies and Intrusions in Unstructured Cybersecurity Data Using Natural Language Processing," International Journal for Research in Applied Science and Engineering Technology, vol. 12, no. 2. International Journal for Research in Applied Science and Engineering Technology (IJRASET), pp. 1023–1029, Feb. 29, 2024. doi: 10.22214/ijraset.2024.58497.

[12] Bhanage, D., Pawar, A., Joshi, A., & Pawar, R. G. (2024). An Efficient Failure Predictive and Remediation System for Windows Infrastructure with Analysis of Log-Event Records. International Journal of Computing and Digital Systems, 16(1), 1713–1723. https://doi.org/10.12785/ijcds/1601127

[13] S. S. ANJUM and V. S. KARWANDE, INTRUSION DETECTION SYSTEM (IDS) BASED ON INTERNET, 1st ed., vol. 6. 2021.

[14] Nguyễn, T. H. (2022). Cybersecurity Logging & Monitoring Security Program [Unpublished manuscript]. School of Computer Science & Engineering, Sacred Heart University.

[15] Bhanage, D., Pawar, A., Joshi, A., & Pawar, R. G. (2024). An Efficient Failure Predictive and Remediation System for Windows Infrastructure with Analysis of Log-Event Records. *International Journal of Computing and Digital Systems*, *16*(1), 1713–1723. https://doi.org/10.12785/ijcds/1601127

  