iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IX **Month of publication:** September 2020

DOI: https://doi.org/10.22214/ijraset.2020.31527

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IX Sep 2020- Available at www.ijraset.com

RECONYMOUS - An Open Source User Activity Monitoring/Timeline Solution

Shyamsundar P G[1], Ravi D N[2], Dhruv Kalaan[3]
[1, 2, 3]*REVA Academy for Corporate Excellence, REVA University, Bangalore, India*

Abstract: Reconymous concentrates on endpoint detection and analysis based on the user activities and available log data from the corresponding windows machine(s). Reconymous is a file forensic tool which enables the analyst/user to get a visualized approach to monitor any access/modification/deletion of any user files and/or system files.
The biggest question in today's day and age of a cybersecurity analyst is when did a system get compromised or which file/files were modified, by whom, by which process and when. Manually capturing this data requires hours of manual effort and sometimes the trail is lost. Although custom EDRs monitor this but have a significant cost attached to it making the solution out of reach for MSME's or SMME's. Current solutions also require a system endpoint which the user can easily remove, or a malicious program can easily corrupt/disable. Since we rely on basic logs of the operating system to receive this information we are applying an approach where system generated logs are utilized and forensics data is available on a complete open source solution for review/audit or investigation purposes
Keywords: Reconymous, ELK, SIEM, EDR, forensic, file access auditing.

I. INTRODUCTION

Windows Event viewer is a feature available with Microsoft Windows OS that can be used for viewing the logs of any local or remote machines. Every activity being done on a windows machine is registered as a log in the event viewer and any centralized log monitoring platform can import these logs to understand the events that had took place in the hosts.

There are three main categories of events based on which they are destined as:

A. System logs, consists of the events related to system and activities carried out.
B. Security logs have the events related to audit, security, logon/logoff attempts, file/folder access, modification, deletion, encryption etc, that can be used for analysis.
C. Application logs, consists of events related to applications that are being installed in the windows system.

This paper concentrates more on a file forensic approach that enables the user to get a proper visualization that serves the purpose of monitoring any security audit related events related to any user/system files. File auditing in windows allows monitoring of events related to users accessing, modifying, and deleting the files and folders that an analyst wants to monitor.
Insider threat is one of the biggest security risks to an organization despite having state of art security features and it originates within the targeted organization. It basically involves the user associated with the business or a user having access to sensitive data with administrative privilege. Traditional security measures are fixed to focus on external threats, and they do not seem to be capable enough to identify an internal threat in an organization. Although there are monitoring capabilities available within the organization, a very common question that occurs within today's cyber security analysts is that when was the incident occurred or which file/folder was modified, when and by whom. File Integrity Monitoring (FIM) is an important security compliance that is covered under PCI-DSS regulations. The FIM solution monitors the integrity of every file with the help of an agent installed and the same is being monitored by the analysts by alerting and analysis methods.

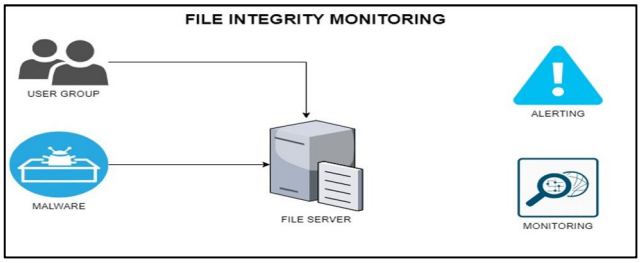


Figure 1: File Integrity Monitoring

Centralized security monitoring involves collecting and analyzing event logs to detect suspicious behavior or any unauthorized changes in system. Among this huge amount of data being collected by these monitoring tools, capturing a specific data related to user activity on file/folder requires hours of manual effort which can also lead to an event getting missed. Compared to many conventional EDR solutions with significant cost that concentrate on such activities, Reconymous is completely built with opensource technology, hence reducing the cost and making it affordable for medium and small-scale organizations.

II. PROBLEM STATEMENT

Forensic investigation is a time-consuming manual process and there is also a dependency on the impacted system's availability. This creates various challenges in visualizing as the data is vast in quantity and is not well organized for the investigation purpose hence making it difficult to give proper understanding on the visual aids. When it comes to the analyst point of view, it becomes hard to find the answers for questions related to who accessed the file, did what to it, by which process, when and how. Critical data functions such as deletion or encryption of files are to be manually searched for in between the huge chunk of data only if there is a suspicion of any such incident.

Current generation security solutions are capable enough to track such user activities but when it comes to cost, these solutions are out of reach to small and medium scale organizations whereas the threat to these organizations remains to be the same. Hence these organizations invest more on securing their outer ring compared to their internal security posture.

There are solutions that are used to manage centralized log collection which are mostly dependent on agents that needs to be deployed at the log sources. These agents can be disabled or deleted at any point of time by a user or any program that tends to be malicious. Hence the dependency towards these collection agents are more in these log collection tools.

Usually when there is an attack, the attacker plans to wipe out the traces by removing the logs from the target machine hence making it difficult to trace the malicious activity during a forensic investigation. In general infections happen and cover tracks as in delete logs etc. which are not recoverable at a later stage.

Organization's major threat comes into picture through an insider attack i.e. a company's own employee or a user associated with the critical data of the organization tend to access, modify or delete some important files/folders that brings the organization into a great trouble on a real time basis. Though the affected files can be retrieved post incident, the job becomes time consuming and the analyst may tend to miss out the user/insider who is behind this attack as this is not being captured and isolated on a real time basis.

We have state of art technologies like SIEMs, EDRs available at the market to perform a continuous monitoring of every devices and endpoints respectively and provide threat intel feeds to serve the purpose. But these solutions are bought by larger organizations to collect many logs since it is a centralized monitoring solution. Here these solutions do not tend to isolate a user related activity that is happening on a file server hence reducing the chance to detect the real time incident with a time series-based analysis. Moreover, these solutions cannot be affordable to a small and medium organization that is looking out for a file integrity monitoring or an end point monitoring at a smaller scale.

III. OBJECTIVE

The objective of this initiative is to provide a solution for tracking user activity related to object access with minimal resource and open source solution. Reconymous will completely use the inbuilt windows architecture to solve its purpose of tracking down user activity and the data that is being collected from the audit logs especially will work around the windows event ids to track down the activities of any user.

This paper considers small and medium scale industry to provide an affordable low budget solution to do a File Integrity monitoring on real time and post incident basis. The main advantage of this solution is that if in case the incident is missed in real time we can still track down the activity and do a timeline analysis without extracting the forensic image of the compromised system as we already have the data in log form and the same can be made as log to timeline analysis.

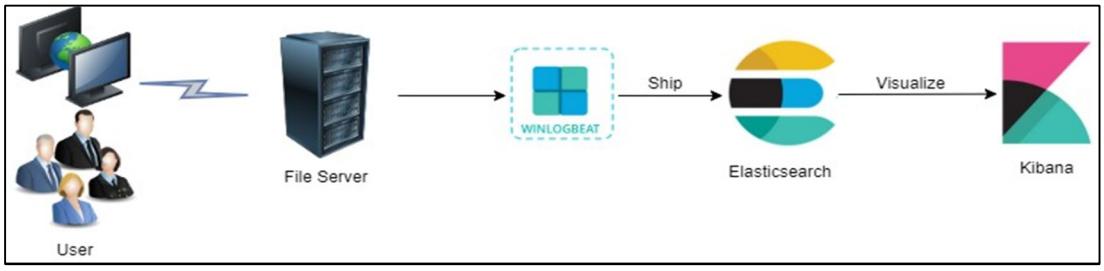


Figure 2: Workflow – simplified

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IX Sep 2020- Available at www.ijraset.com

IV. METHODOLOGY

The solution mainly consists of the following steps as a part of implementation and setup:

A. Windows 10 / any windows server
B. File auditing enabling
C. ELK stack setup in windows
D. Winlobeat setup

Windows system being the host is the log source that provides events for the user activity monitoring. The critical files/folders will be set to audit the access data and the same will be shipped to the monitoring destination.
ELK stack is the log collection center and monitoring platform that will be used by the analyst panel to monitor the user related activities on the file server. Winlogbeat (used only for windows) is the data shipper that is configured and installed in log source to push the event logs to ELK stack.

V. SOFTWARE DESIGN

Reconymous is a solution that combines Microsoft's inbuilt audit logging and open source technology to perform user activity monitoring related to file/folder access, modification and deletion effectively. Below mentioned flowchart explains the high-level data flow of Reconymous in detail.

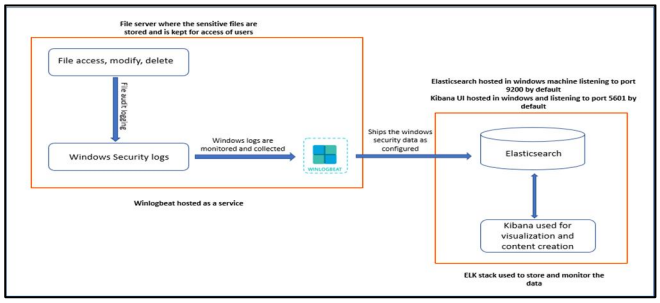


Figure 3: High level data flow

VI. RESOURCE SPECIFICATION

Reconymous has a simple infrastructure as it involves the very few components to achieve the requirement of user activity capturing. Below mentioned is the basic Data Flow Diagram (DFD) that shows the basic flow of logs from the file server to the ELK platform.

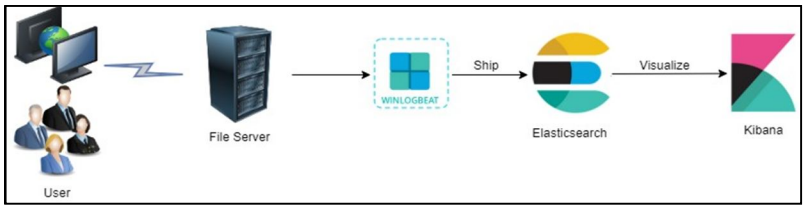


Figure 4: Data Flow Diagram

The major components of Reconymous includes:

1) *Winlogbeat:* Data shipper that will be placed at the file server to ship the windows event logs to ELK.
2) *Elastic Search*: A no-SQL database that will be storing the event log data that are being collected from the file server and all other servers with critical confidential data. The Elasticsearch engine will be installed in a separate windows/linux server.
3) *Kibana:* Visualization engine that will be used by the analyst panel to view the logs from Elasticsearch and monitor the user activities on the file access.

The main resource that needs to be considered for this project is for ELK stack which can be installed in Windows/Linux platforms. We will be using Windows platform in our Lab environment with a single node cluster design. Below table will give a brief detail on the system requirements for a lab environment with one log source. Production deployment will have a slight change in the requirements based on the log reception and number of hosts to be monitored.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IX Sep 2020- Available at www.ijraset.com

VII. TESTING AND VALIDATION

The whole set up has been implemented in a lab environment with a windows host sending the file audit logs to ELK and as a part of content development, there are Dashboards designed especially to provide an easier way of analysis with respect to user activity monitoring for file access, modification, deletion.

This solution is intended to provide internal security with respect to user activity monitoring corresponding to file/folder access, modification and deletion at a low cost that can be adopted by any small and medium scale industries who are looking for a similar functionality of a commercial EDR solution.

Using the event IDs 4663, 4656, 4660, and corelating them gives us the actual findings of any incident related to file access, deletion and modification.

Further to this, there is a timeline chart available that gives the details of timestamp of an event which can serve the incident response.

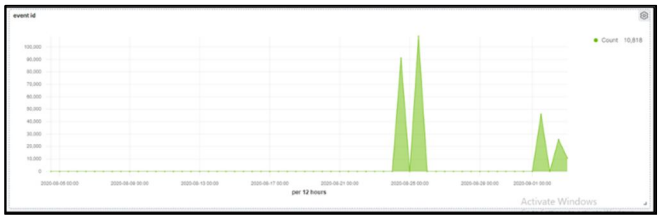


Figure 5: Time-series chart

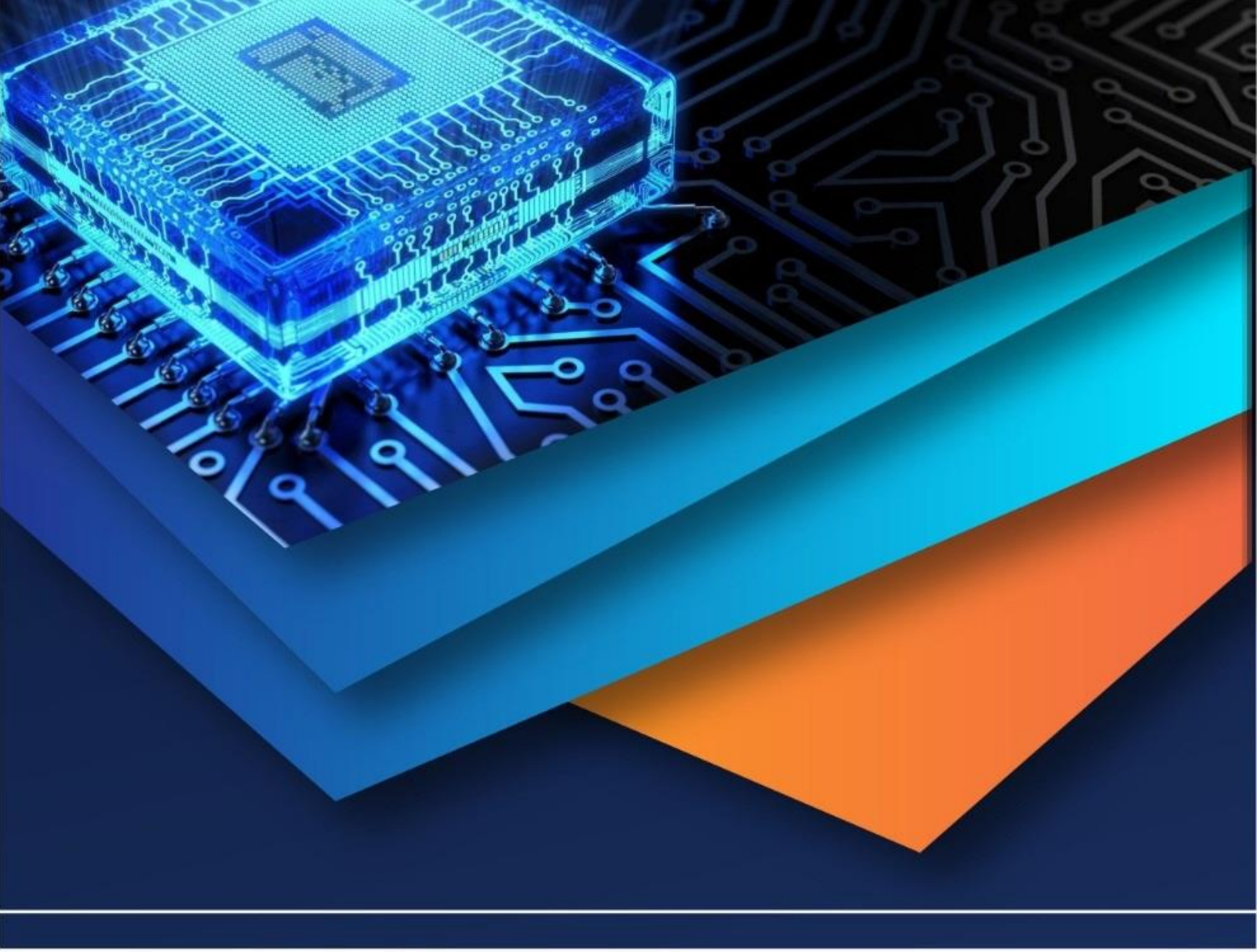
VIII.CONCLUSION

Reconymous meets the requirement and solves the important problem statement of identifying user activities on real time basis with time stamp capturing. This solution can be easily understood by any technical team who has a better knowledge on windows events and can implement the same to solve the purpose of object access monitoring on real time and on a timely fashion.

IX. RECOMMENDATIONS FOR FUTURE WORK

Reconymous can be made more efficient by automating the file access auditing process. A proper research study on the Batch scripting can help this solution to perform the basic windows task automatically. PowerShell script can be supplied with which admins can setup the windows settings automatically. Further to this, since the visualization platform is Kibana, analyst can further add/modify dashboards and widgets to further fine tune the process of identifying the object access activities even at a faster rate and this would further reduce the mean time to detect the incident.

Future recommendations can also have Linux/mac servers to supply logs via syslog and other FIM tools to Reconymous to monitor. Additionally, single install docker file can be created to reduce the overhead of setup.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY