## Week 13 Assignment

Karim Ahmed

CIS433/533

Spring 2022

# Question1:

Research 3 different DLP solutions from 3 different vendors. Create a table that compares at least 4 different functions/options. Based on your research what solution is better and why? Write a short paragraph that summarize your research.

|  |  |
| --- | --- |
| **Function** | **Description** |
| Rule-based/Regular Expression (reg-ex) | An engine that validates patterns such as SSNs, Credit Card numbers, and any important data that needs to be validated before processing |
| Database Fingerprinting | A function that focuses on matching data with what is already persisted in the database. It is not very performant since it looks through a live database and/or database dump. |
| Statistical Analysis | Machine learning algorithm is used to look through all the data, policies, and perform an analysis. |
| Partial Document Matching | Looks for previous forms that were submitted to find matching information to validate data |

The vendors I looked at include *McAfee*, *Symantec*, and *Safetica ONE.* All of which offer the same functions mentioned above. In my opinion, all of the above functions are important for Data Loss Prevention in networks and servers. Arguably, Statistical Analysis could be the most important of them all since this seems to be the layer that validates data before it moves towards the database fingerprinting layer.

# Question 2:

Identify two organization that implements a DLP plan. Briefly introduce the organization and what they do. Then answer the following

**IT Services company SaaS (name not included)**

1. What was the need behind implementing a DLP policy/plan?
   1. The need to secure and protect data from loss and reduce human error.
2. What components were included in the Data Loss Prevention (DLP) plan?
   1. Protection of all major data, endpoints, network points, active and inactive files, mobile data, data in the cloud, on the web, and at rest.
3. What type of data was protected? Was there any distinction between data at rest, data at motion and data in processing?
   1. Data at rest, data in motion, and data in processing is all important to the company and are all covered in the protection plan
4. What were the benefits gained from Data Loss Prevention (DLP) plan?
   1. The company was able to take actions against malicious activity as they were notified about possible intrusions and attacks against customer and organizational data after using *Symantec*.

**Banking Industry (name not included)**

1. What was the need behind implementing a DLP policy/plan?
   1. The need to monitor data transmission to secure clients’ data across the network.
   2. The necessity to implement file upload protection
   3. Create internal/operational efficiencies.
2. What components were included in the Data Loss Prevention (DLP) plan?
   1. Data protection over the network
   2. File protection
   3. Network monitoring capability
   4. Intrusion detection and notification
   5. Data authentication and validation
3. What type of data was protected? Was there any distinction between data at rest, data at motion and data in processing?
   1. Files, client information, and organization information. Data at rest, data in motion, and data in processing is all important to the company and are all covered in the protection plan
4. What were the benefits gained from Data Loss Prevention (DLP) plan?
   1. All file uploads, client data, and organizational data are protected.

# Question 3

Examine the Department of Defense cyber-attack that originated from a USB drive. Summarize the case study.

<https://www.wearethemighty.com/mighty-history/worst-cyber-attack-usb/>

look at some of the policies that are implanted there.

<https://dpcld.defense.gov/Portals/49/Documents/Media/BestPractices%20(PDF).pdf>

After that attack, the DOD has banned all employees from connecting USB drives. This ban has been lifted recently. Would a one policy fit all (ban USB’s for all) work in such a case? Why or why not?

Summary:

* A USB was picked up by an officer in a parking lot that included a worm “*Agent.btz*” which made its way around the network of the Department of Defense. The worst part is that no one knows what information was leaked or who created the worm. The DoD was notified by the NSA that a worm was in their system, and it took 14 months to eradicate. During that time all their network communications were compromised.
* The policy was effective if you put it in the context of where and why it was used. However, it is not effective to prevent many other attacks that could potentially compromise their systems. Also, many agents probably had to use USBs daily, so this policy could have potentially delayed tasks during the implementation plan if they did not have an incident response plan that already existed.