DLP Training

What is DLP?

Data Loss Prevention (**DLP**) refers to a set of technologies and strategies aimed at preventing sensitive data from leaving an organization. This involves identifying, monitoring, and protecting data across various states: in motion, at rest, and in use.

There's a focus on compliance and protecting intellectual property, DLP systems have evolved to address a broader range of threats including insider threats, data breaches, and regulatory requirements.

Data Classification

Data classification is the categorization of data based on its sensitivity, importance, and confidentiality to ensure appropriate protection measures are applied. This process assigns labels or tags to data sets, defining how they should be handled, accessed, and protected throughout their lifecycle. Typically, data is classified into categories such as public, internal use, confidential, and restricted, each with varying levels of access control and security requirements. Effective data classification enables organizations to prioritize resources and implement tailored security controls.

Domains

DLP solutions are typically categorized into several domains or types, each focusing on protecting data at different points within an organization's IT infrastructure. At a high level they can be categorized as follows:

Email DLP

DLP for email systems helps prevent sensitive data from being lost, leaked, misused, or accessed by unauthorized individuals. Email DLP solutions monitor inbound and outbound messages, scanning for sensitive content and attachments. Upon detecting potential data

leaks, these solutions flag, block, or delete the messages based on security policies. Data leaks through email can occur in several ways:

- **Inadvertent Leaks:** Sending the wrong attachment, misaddressing recipients (See Data Disclosures Procedure), forgetting to encrypt, or forwarding emails with sensitive content.
- **Insider Threats:** Actions by employees or privileged users intentionally sending sensitive data out of the organization. Employees on the verge of resigning might send business plans or customer data (Potential PII) to their personal email for future use. Some may leak sensitive information to the media or sell it on the dark web. Others may send work files to personal accounts to work from home, unknowingly compromising data security.
- **Cybercriminals:** Using compromised credentials to access email accounts and steal data.

Prevention Methods

Tools to prevent Email DLP typically works by inspecting all messages and attachments to look for content that may represent a potential data leak. There are several types of techniques we employ here that are common across organizations: **Rule-based searches** spot patterns like PII or confidential data using specific rules**. Exact matches** search for specific confidential documents. **Pre-built categories** rely on compliance standards to identify regulated information. **AI and machine learning** analyze data statistically to detect sensitive content.

Network DLP

Network DLP refers to a set of tools and processes designed to monitor, detect, and prevent unauthorized data transfers or leaks that occur over the network. This encompasses data moving across internal and external networks, including web traffic, file transfers, and other network communications.
Email DLP would be a subset of Network.

Prevention Methods

Monitoring and inspecting network traffic to prevent unauthorized data transfers, using **predefined policies** based on regulatory requirements and corporate standards. These

policies dictate what constitutes sensitive data and how it should be handled. Network DLP systems **enforce** these policies **in real-time**, blocking or alerting administrators to violations, such as blocking unauthorized file uploads.

These events are managed through network security monitoring tools or DLP-specific consoles, providing details like source and destination IP addresses, transferred data types, and actions taken (e.g., block, allow with encryption).

Endpoint DLP

Endpoint DLP focuses on securing data at the point where it is created, stored, or accessed on individual devices such as laptops, desktops, and mobile devices. Leaks from an endpoint can occur when users upload materials to USB drives or external drives, or when malware infects endpoints and exfiltrates data without authorization (often the starting point of another type of DLP like Network or Email).

Prevention Methods

Many solutions include scanning endpoints for sensitive data stored locally or accessed from external sources. It controls how and where sensitive data can be copied or moved and whether the user attempting the action has the necessary privileges or policy exceptions in place. Endpoint DLP monitors endpoint activities for policy violations, generates alerts, and provides visibility into incidents. Events are managed through endpoint security management consoles or integrated with broader security information and event management (SIEM) systems, detailing user actions (e.g., file transfer, printing), detected sensitive data, and enforcement actions (e.g., block, encrypt).

DFIR Analyst DLP Responsibilities

When investigating DLP incidents the role of an analyst is to conduct the following:

1. Review the alert triggered by the DLP system.
2. Check the user's permissions or confirm if they received explicit permission from their leadership for the action.
3. Contact the user's leadership to confirm whether the activity was previously authorized; if authorized, log the justification.
4. If not authorized, contact the user to delete or otherwise remove sensitive materials.
5. Escalate the incident to the appropriate teams or stakeholders, especially when the leaked data involves Personally Identifiable Information (PII), Business-to-Business

(B2B) information, or other highly confidential data. Ensure that all necessary parties are informed and involved in managing the incident according to organizational protocols and compliance requirements.

Sometimes a DLP tool may have it wrong, or a user has a specific business need being blocked by a solution. One way or another a user may get in touch with cyber asking for an action to be allowed. Our typical action would be to:

1. Upon receiving a DLP unblock request, acknowledge receipt to the requester.

2. Verify the requester's permissions and access rights related to the data or action in question.

3. Evaluate the business justification provided for the requested action. Determine if the request aligns with organizational policies and security protocols.

4. Assess the potential risk associated with granting the unblock request, considering factors such as data sensitivity, regulatory compliance, and security implications. Consult the Corporate Information Security Policy (CISP).

5. Based on the investigation and assessment:

- If the request is justifiable and aligns with policies, proceed to whitelist domains, add user exceptions, or otherwise allow the action as per established procedures.
- If the request lacks sufficient justification or poses security risks, reject the activity and communicate the decision clearly to the requester.

6. Document the decision, rationale, and any actions taken in response to the request. Maintain a record for auditing and compliance purposes.

7. Notify the requester of the decision promptly, providing reasons for approval or rejection and any additional steps or instructions if applicable.

[Links for DLP Tools]

References:

Mwila, K. A., & Phiri, J. (2019). Data Loss Prevention. Unpublished manuscript, University of Zambia, Lusaka, Zambia.