DLP QUICK WINS

TALES FROM A RECOVERING INFOSEC PRACTITIONER

Micah K Brown

- Twitter: @MicahKBrown
- Munich Re: IT Security Engineer II
- GitHub: https://github.com/micahkbrown
  - DLP Demystified (2018 talk)
  - Star Wars: How an ineffective Data Governance Program Destroyed the Galactic Empire (2019 talk)
  - How to cook a Five Star Meal from the Convenience of Your Hotel Room (Derby Con 2019)
  - Doing simple at scale (2020 talk)
- Vice President of Greater Cincinnati ISSA Chapter
- CISSP

- Served 45 pounds of free Pulled Pork to @DerbyCon 2019!
- Real Corp 2018 goal: "Learn to Cook Brisket Like a Texan."
- Real Corp 2019 goal: "Continue to Cook Brisket Like a Texan."
- On most Fridays, find me smoking both an old fashioned and pizza!

*Thoughts and view are my own and do not reflect that of my employer.

Greater Cincinnati IT Security groups

ISSA

http://www.cincy-issa.org/

SMBA

https://www.linkedin.com/company/cincinnati-smba

CiNPA
Cincinnati Networking Professionals Association
Security Special Interest Group
SECURITY SIG

https://www.meetup.com/TechLife-Cincinnati/events/241602925/

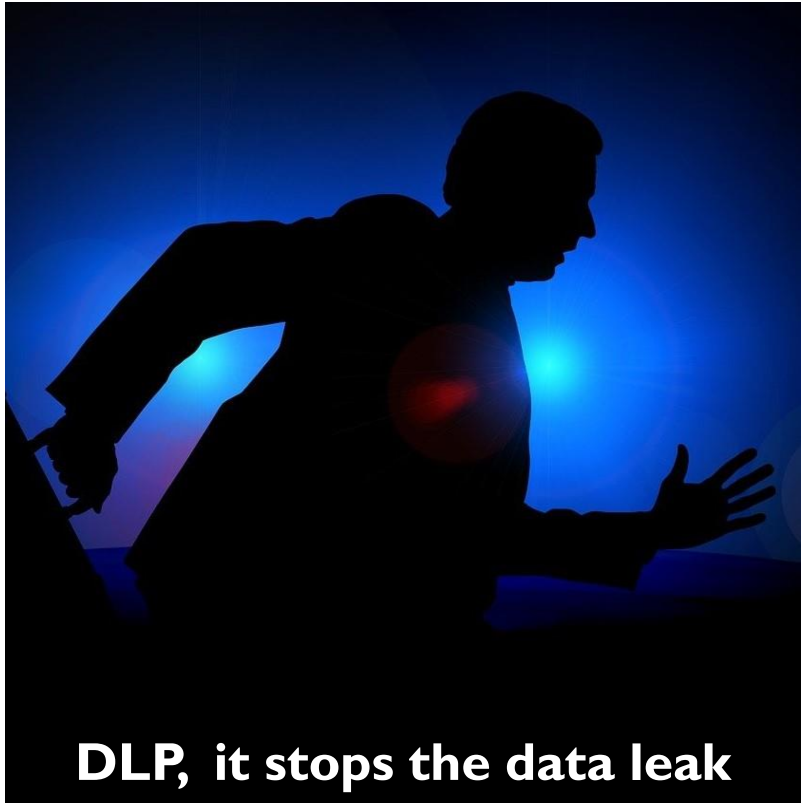
(ISC)²®

https://www.infoseccincy.org/

A Special Thank You to McAfee for this (and other) opportunities!

1,105,246
Ransomware damages today (USD)
112,652,719
Skype calls today
1,542,730
Smartphones sold today
1,613
New ransomware attacks today
Web
Unified Cloud Edge
Devices
SWG
CASB
Cloud
Amazon
Salesforce
Box
Office 365
G Suite
YouTube
Dropbox
MVISION
ePO
DLP
Data
Benefits
CENTRALIZED POLICY DEFINITION
For threat prevention and data protection
UNIFIED INCIDENT MANAGEMENT
ACCESS CONTROL
Over managed and unmanaged devices
CLOUD DATA AND PERMISSION CONTROLS
Via API integrations
ACCEPTABLE USE POLICY ENFORCEMENT
With advanced malware protection

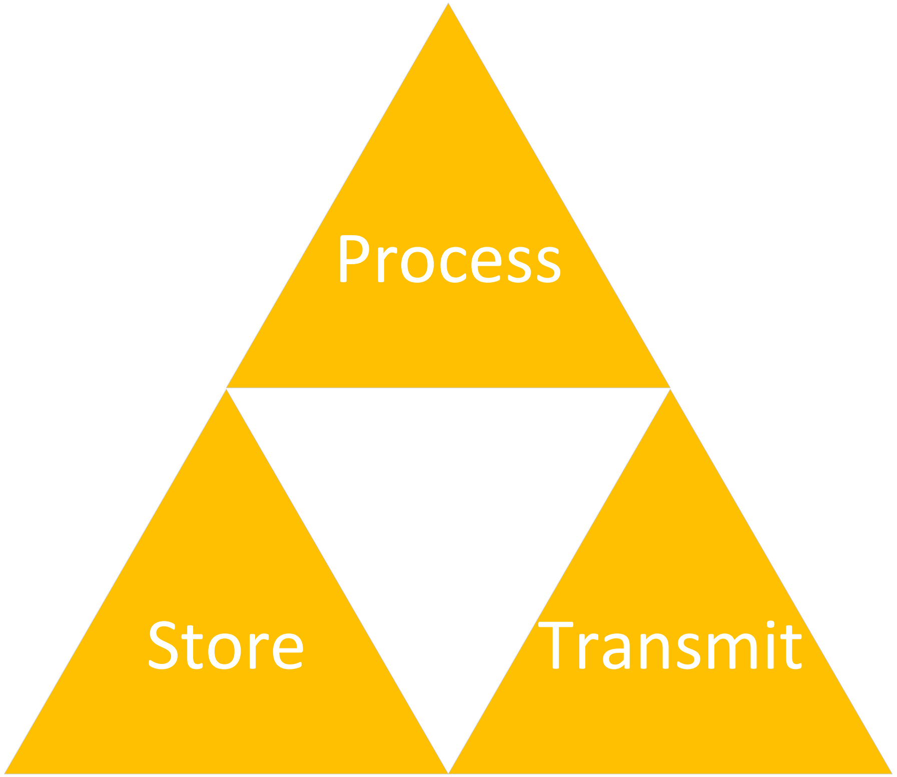
WHAT IS DLP?



- **DLP is NOT . . .** a 'monolithic' stack of technology by one single vendor
- **DLP is NOT . . .** designed to stop a sufficiently advanced advisory [internal | external] by itself
- **DLP is NOT . . .** 'Digital Rights Management'
- **DLP is NOT . . .** 'User Behavioral Analytics'
- **DLP is NOT . . .** a 'Silver Bullet'

- **DLP IS** becoming a 'feature' in many different tools
- **DLP IS** designed to help establish proper data ownership
- **DLP IS** more aligned with Business Risk Management than IT Security
- **DLP IS** a collection of tools that allows the business to define policies on how data is Stored, or Processed, the environment

https://pixabay.com/get/57e6d2464c5aa914f6da8c7dda353678153ad6e55154794b_1280.jpg



THE STATES OF DATA IN OUR ENVIRONMENT

DLP is made up of many different tools that work together. Each tool will inspect / interact with data in at least one or more of these states of data.

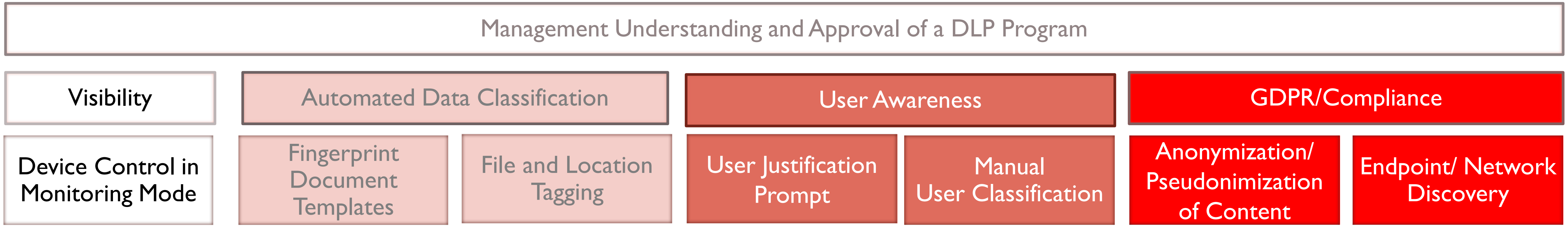
WE ARE GONNA NEED A BIGGER MEETING ROOM!!!

STILL ONLY 35¢
MARVEL® COMICS GROUP
181 MAR
02458
EARTH'S MIGHTIEST HEROES!
the AVENGERS®
©1978 MARVEL COMICS GROUP
We are setting up a global DLP program!

- IT Security (Build)
- IT Security (Run)
- Senior Management
- Line Management
- Data Governance
- Risk & Compliance
- Legal
- Human Resources
- ?Government / Workers Council?
- Other groups depending on your organizations!

- Who owns event investigation?
- Where can evidence be stored?
- Does evidence need to match rules, laws, regulations?

DLP QUICK WINS: VISIBILITY



Management Understanding and Approval of a DLP Program

Visibility

Automated Data Classification

User Awareness

GDPR/Compliance

Device Control in Monitoring Mode

Fingerprint Document Templates

File and Location Tagging

User Justification Prompt

Manual User Classification

Anonymization/ Pseudonimization of Content

Endpoint/ Network Discovery

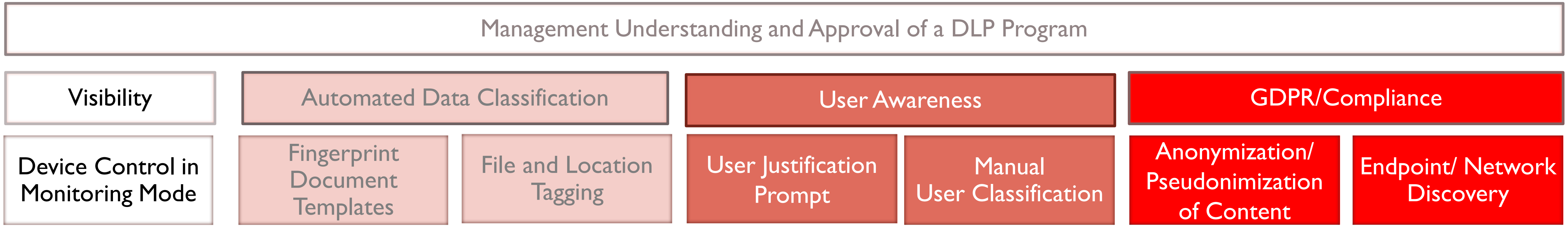
Outcome:
Visibility and Inventory of external devices

Prevent execution from a portable media

Prevent access to portable media

Understanding of management console

DLP QUICK WINS: AUTOMATED DATA CLASSIFICATION



Management Understanding and Approval of a DLP Program

Visibility

Device Control in Monitoring Mode

Automated Data Classification

Fingerprint Document Templates

File and Location Tagging

User Awareness

User Justification Prompt

Manual User Classification

GDPR/Compliance

Anonymization/ Pseudonimization of Content

Endpoint/ Network Discovery

Outcome:
Visibility and Inventory of external devices

Prevent execution from a portable media

Prevent access to portable media

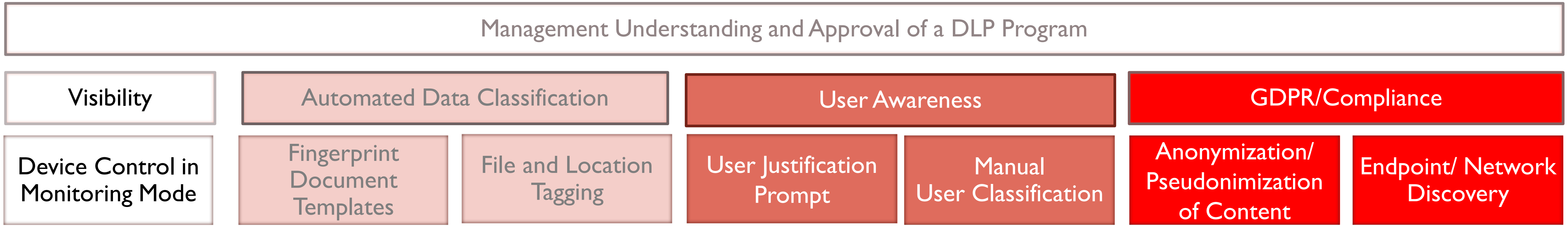
Understanding of management console

Outcome:
Fingerprint document templates and control each copy everywhere

Outcome:
Define file types or server locations for automated classification

\\server\HR
\\server\Project
*.CAD

DLP QUICK WINS: USER AWARENESS



Management Understanding and Approval of a DLP Program

Visibility

- Device Control in Monitoring Mode

Automated Data Classification

- Fingerprint Document Templates
- File and Location Tagging

User Awareness

- User Justification Prompt
- Manual User Classification

GDPR/Compliance

- Anonymization/ Pseudonimization of Content
- Endpoint/ Network Discovery

Outcome:
Visibility and Inventory of external devices

Prevent execution from a portable media

Prevent access to portable media

Understanding of management console

Outcome:
Fingerprint document templates and control each copy everywhere

Outcome:
Define file types or server locations for automated classification

\\server\HR
\\server\Project
*.CAD

Outcome:
Don’t block, but create awareness on data usage, let the user digitally sign for their action

Be open and honest. Win Trust!

Outcome:
User has the capability to protect their own content

This enriches many other tools outside of DLP and is a huge win!

DLP QUICK WINS: COMPLIANCE

Management Understanding and Approval of a DLP Program

Visibility	Automated Data Classification		User Awareness		GDPR/Compliance	
Device Control in Monitoring Mode	Fingerprint Document Templates	File and Location Tagging	User Justification Prompt	Manual User Classification	Anonymization/ Pseudonimization of Content	Endpoint/ Network Discovery
Outcome: Visibility and Inventory of external devices Prevent execution from a portable media Prevent access to portable media Understanding of management console	Outcome: Fingerprint document templates and control each copy everywhere	Outcome: Define file types or server locations for automated classification \\server\HR \\server\Project *.CAD	Outcome: Don’t block, but create awareness on data usage, let the user digitally sign for their action Be open and honest. Win Trust!	Outcome: User has the capability to protect their own content This enriches many other tools outside of DLP and is a huge win!	Outcome: Get visibility around data flows Network, email, web, and cloud oh my! Prepare your organization easily for the GDPR required 72-hour evidence proof	Outcome: Comply with GDPR the “right to forget,” and technically enable discovery of data records company wide Get creative and search repositories for ‘ransomwared’ files!

"That's all Folks!"™
A WARNER BROS. CARTOON
© WARNER BROS. INC 1989
Limited Film Art Originals Authenticated by WB Limited Edition Hand Painted

Imaged by Heritage Auctions, HA.com