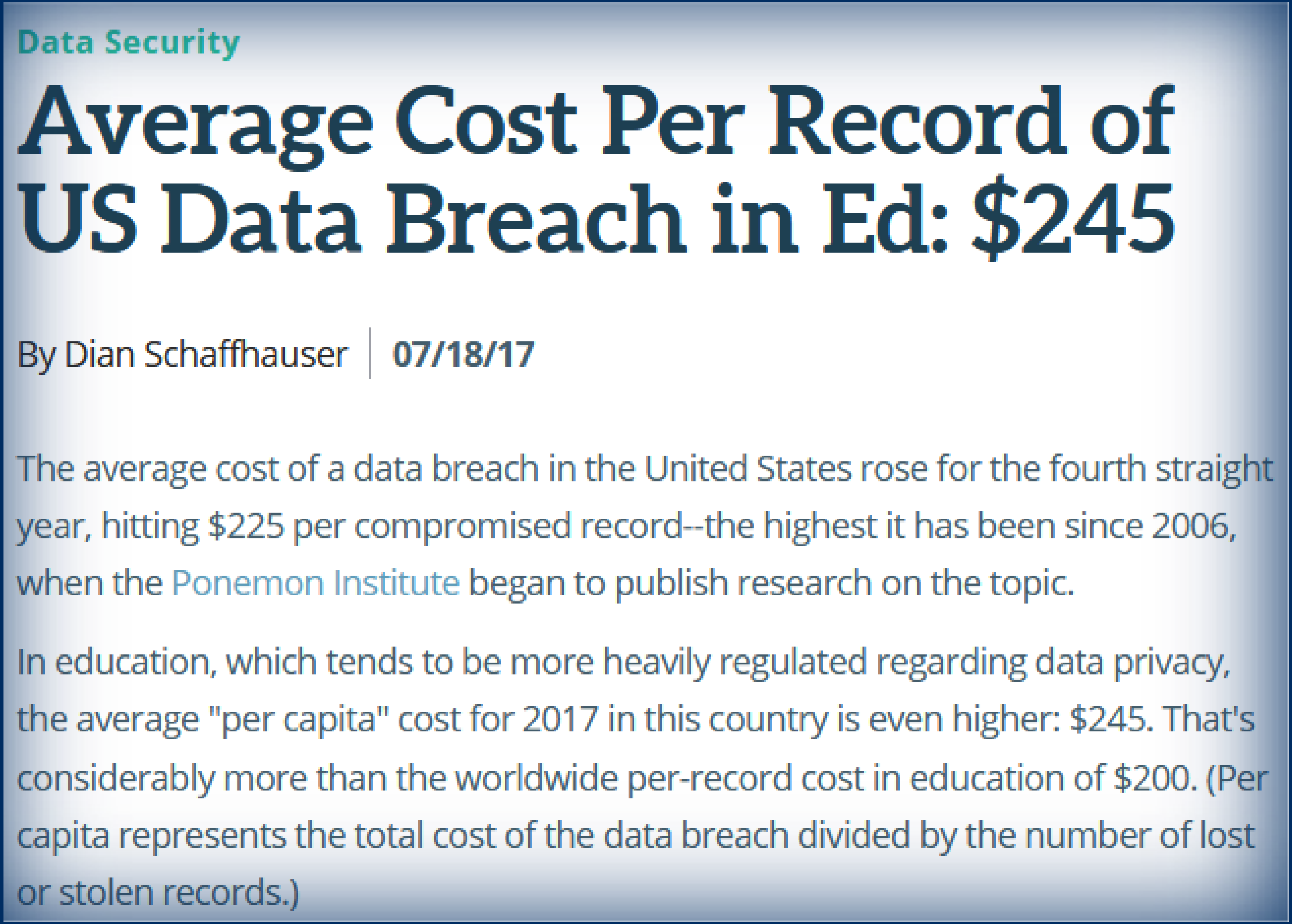
Data Loss Prevention @ Duquesne University

Brad Maloney | maloneyb@duq.edu
Manager, Secure Integrated Infrastructure

Michael Muto | mutom@duq.edu
Sr. Information Security Engineer

Reasons for DLP

- Assessing where your organization's confidential and sensitive data is being stored and who is accessing it
- Mitigating liability, negative exposure, fines and lost revenue
- Maintaining compliance with increasingly mobile workforce
- Cloud deployment sanitization
- Compliance: HIPAA, GLBA, FERPA, GDPR, PCI



Data Security

Average Cost Per Record of US Data Breach in Ed: $245

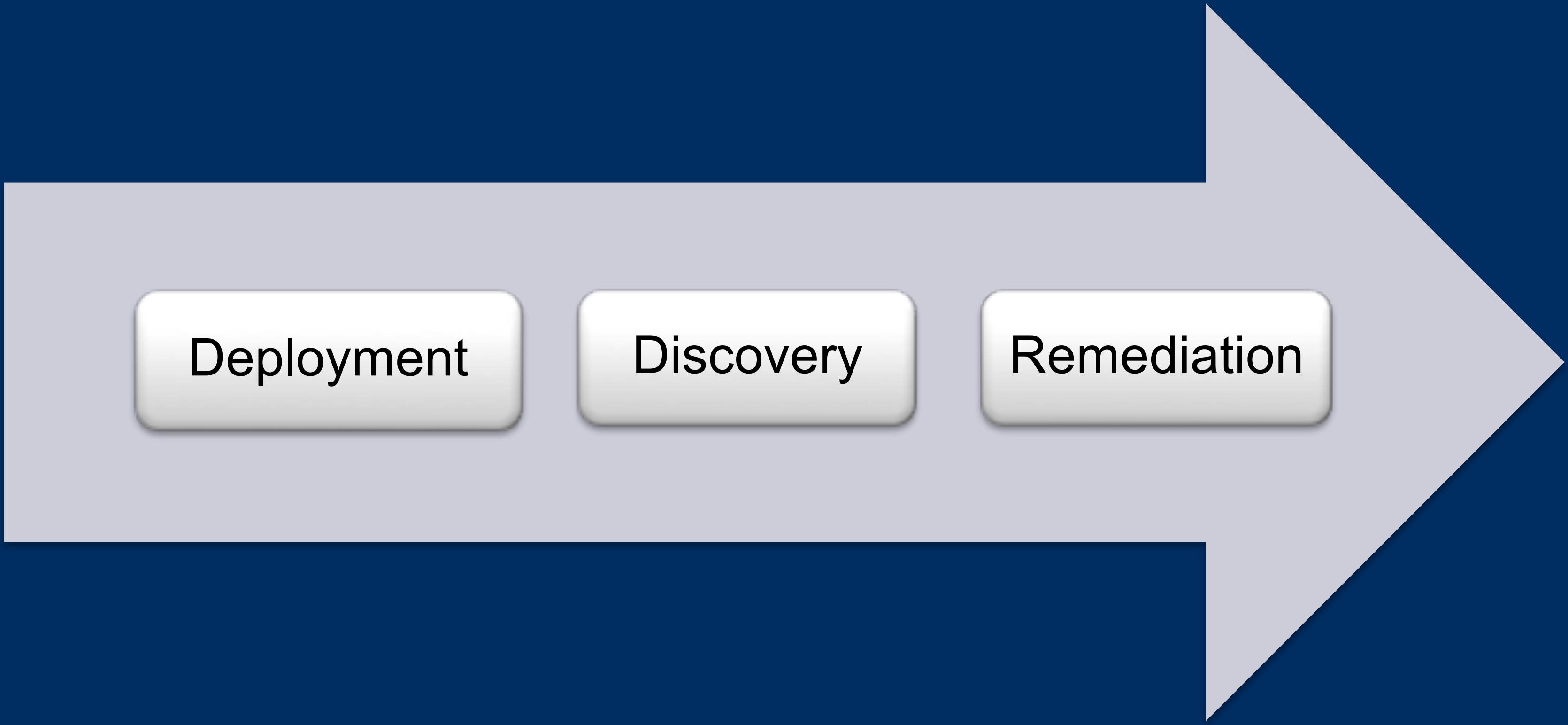
By Dian Schaffhauser | 07/18/17

The average cost of a data breach in the United States rose for the fourth straight year, hitting $225 per compromised record--the highest it has been since 2006, when the Ponemon Institute began to publish research on the topic.

In education, which tends to be more heavily regulated regarding data privacy, the average "per capita" cost for 2017 in this country is even higher: $245. That's considerably more than the worldwide per-record cost in education of $200. (Per capita represents the total cost of the data breach divided by the number of lost or stolen records.)

https://thejournal.com/articles/2017/07/18/average-cost-per-record-of-us-data-breach-in-ed-245.aspx

The DLP Workflow



Deployment

Discovery

Remediation

Deployment Strategy: Introducing Gradual Change

- Start with Help Desk / end-user support
- Create documentation, policies, videos, training
- Pilot key IT staff via opt-in
- Departmental rollout, starting with IT
- Deploy to smaller business units first
- Outreach / Q&A sessions with departments

Data Classification

Data Classification	Institutional Risk	Description	Examples
Level 1 – Restricted Data	High	Institutional data that could seriously or adversely impact Duquesne University and/or could have consequences on our responsibility for safety and education if accessed by unauthorized individuals. Institutional data is considered as high risk related to compliance, reputation, and/or confidentiality/privacy concerns. This data should have the highest level of security controls applied	-PII (Social Security Number-SSN, Driver's License Number) -Bank/Financial Account Information -Credit Card Information (PCI) -Student Protected Data (FERPA) -Health Protected Data (HIPPA)
Level 2 – Internal Data	Medium	Institutional data that should be protected from general access and/or restricted to protected groups or individuals. A reasonable level of security controls should be applied.	-Non-Banner Information stored in and/or accessed via DORI -Institutional data not publicly available and not classified as restricted.
Level 3 – Public Data	None	All public institutional data. While little or no controls are required to protect this data, some levels of controls should be applied to prevent the unauthorized modification or destruction of the data.	Generally accessible institutional data such as information accessible at www.duq.edu that does not require authentication to access.

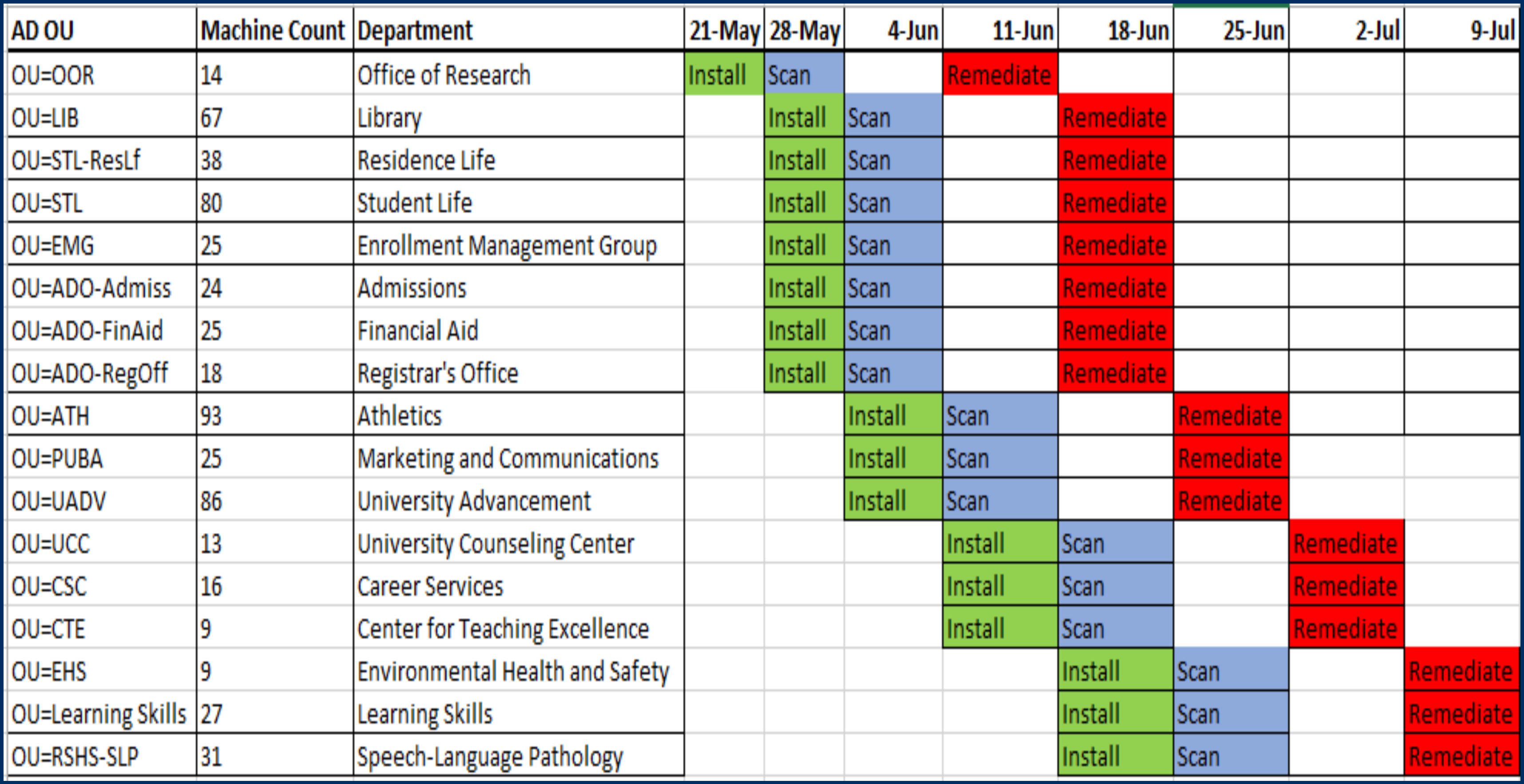
Deployment Options

SCCM – Windows
(Active Directory Integration)

JAMF Pro, formerly Casper Suite – Macs

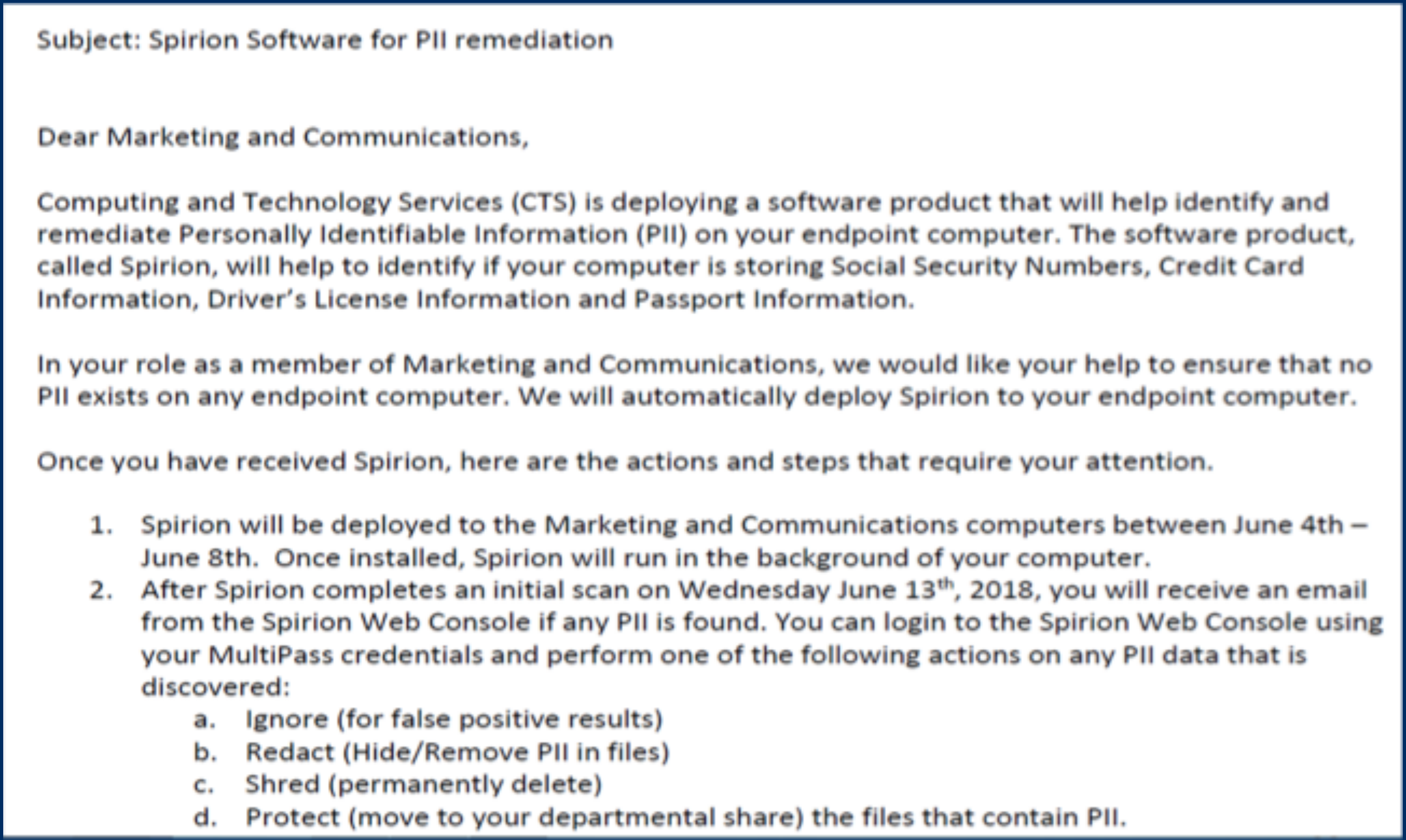
Spirion Console
(Can upgrade client version once installed)

Deployment Schedule Phasing



AD OU	Machine Count	Department	21-May	28-May	4-Jun	11-Jun	18-Jun	25-Jun	2-Jul	9-Jul
OU=OOR	14	Office of Research	Install	Scan		Remediate				
OU=LIB	67	Library		Install	Scan		Remediate			
OU=STL-ResLf	38	Residence Life		Install	Scan		Remediate			
OU=STL	80	Student Life		Install	Scan		Remediate			
OU=EMG	25	Enrollment Management Group		Install	Scan		Remediate			
OU=ADO-Admiss	24	Admissions		Install	Scan		Remediate			
OU=ADO-FinAid	25	Financial Aid		Install	Scan		Remediate			
OU=ADO-RegOff	18	Registrar's Office		Install	Scan		Remediate			
OU=ATH	93	Athletics			Install	Scan		Remediate		
OU=PUBA	25	Marketing and Communications			Install	Scan		Remediate		
OU=UADV	86	University Advancement			Install	Scan		Remediate		
OU=UCC	13	University Counseling Center				Install	Scan		Remediate	
OU=CSC	16	Career Services				Install	Scan		Remediate	
OU=CTE	9	Center for Teaching Excellence				Install	Scan		Remediate	
OU=EHS	9	Environmental Health and Safety					Install	Scan		Remediate
OU=Learning Skills	27	Learning Skills					Install	Scan		Remediate
OU=RSHS-SLP	31	Speech-Language Pathology					Install	Scan		Remediate

Deployment Communications



Subject: Spirion Software for PII remediation

Dear Marketing and Communications,

Computing and Technology Services (CTS) is deploying a software product that will help identify and remediate Personally Identifiable Information (PII) on your endpoint computer. The software product, called Spirion, will help to identify if your computer is storing Social Security Numbers, Credit Card Information, Driver's License Information and Passport Information.

In your role as a member of Marketing and Communications, we would like your help to ensure that no PII exists on any endpoint computer. We will automatically deploy Spirion to your endpoint computer.

Once you have received Spirion, here are the actions and steps that require your attention.

1. Spirion will be deployed to the Marketing and Communications computers between June 4th – June 8th. Once installed, Spirion will run in the background of your computer.
2. After Spirion completes an initial scan on Wednesday June 13th, 2018, you will receive an email from the Spirion Web Console if any PII is found. You can login to the Spirion Web Console using your MultiPass credentials and perform one of the following actions on any PII data that is discovered:
    a. Ignore (for false positive results)
    b. Redact (Hide/Remove PII in files)
    c. Shred (permanently delete)
    d. Protect (move to your departmental share) the files that contain PII.

Deployment: Lessons Learned

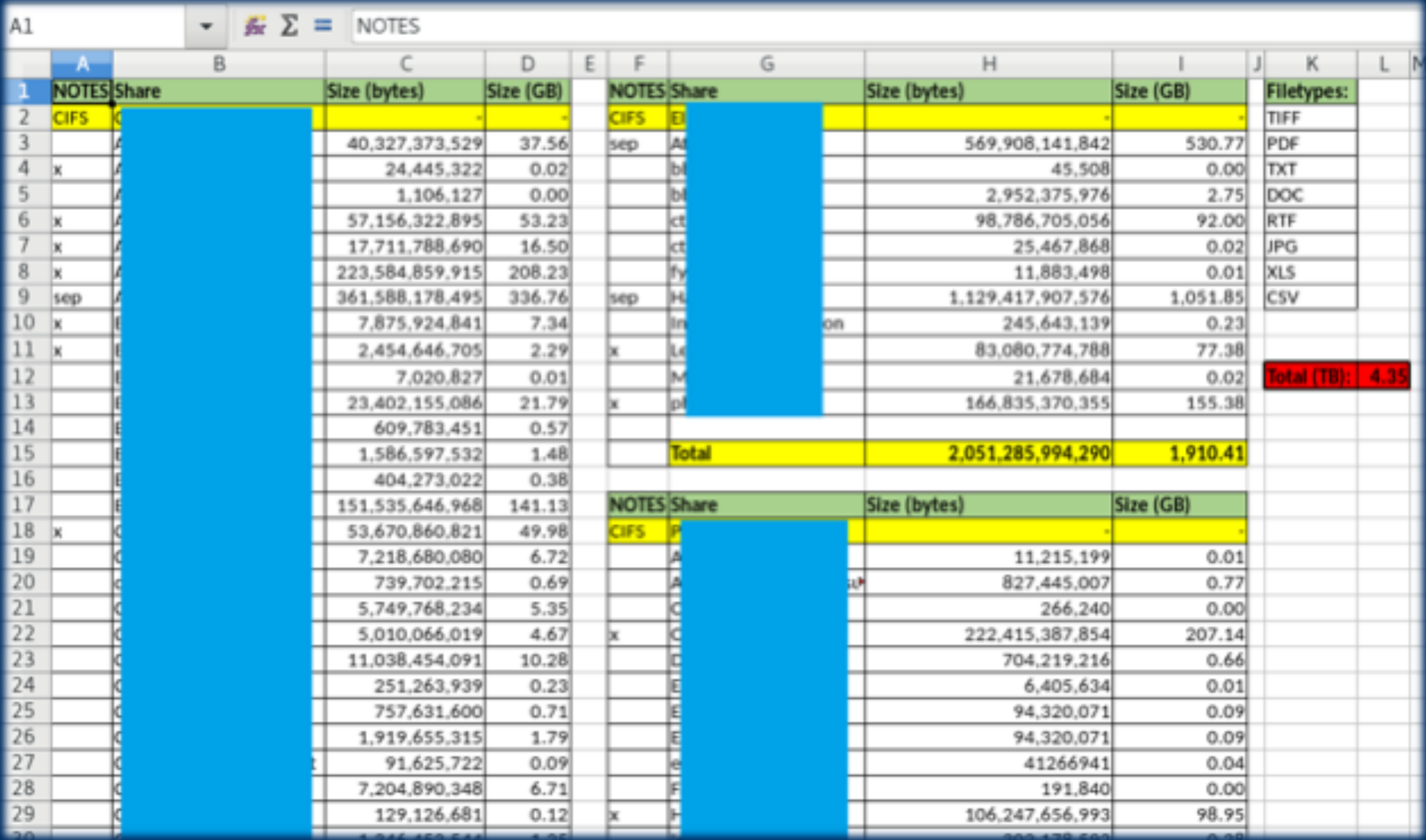
- Rely on expertise of key staff in endpoint, storage areas
- Logical organization of departments for rollout is helpful
- Pre-deployment communication ensures success
- Policy considerations
  - Exclude common areas such as %WINDIR% and /Library/Logs
  - Search common file types (tiff, jpg, png, txt, rtf, doc, xls, csv…)
  - Do not scan while on battery power
  - Run low CPU/IO priority
  - Reset file timestamps back (ie, “last read” or “last access” time)

Discovery

Discovery: Endpoints and File Shares

- Business unit endpoints
  - – More than 1,300 endpoints in scope
  - – Nearly 10,000 searches conducted
  - – Over 230 million files searched
- NetApp Storage VMs
  - – Over 4TB of data in scope
  - – 1.6 million files scanned
  - – Roughly 20 days to complete

Discovery: File Size Assessment



A1 NOTES

NOTES	Share	Size (bytes)	Size (GB)
CIFS	[redacted]	-	-
	[redacted]	40,327,373,529	37.56
x	[redacted]	24,445,322	0.02
	[redacted]	1,106,127	0.00
x	[redacted]	57,156,322,895	53.23
x	[redacted]	17,711,788,690	16.50
x	[redacted]	223,584,859,915	208.23
sep	[redacted]	361,588,178,495	336.76
x	[redacted]	7,875,924,841	7.34
x	[redacted]	2,454,646,705	2.29
	[redacted]	7,020,827	0.01
	[redacted]	23,402,155,086	21.79
	[redacted]	609,783,451	0.57
	[redacted]	1,586,597,532	1.48
	[redacted]	404,273,022	0.38
	[redacted]	151,535,646,968	141.13
x	[redacted]	53,670,860,821	49.98
	[redacted]	7,218,680,080	6.72
	[redacted]	739,702,215	0.69
	[redacted]	5,749,768,234	5.35
	[redacted]	5,010,066,019	4.67
	[redacted]	11,038,454,091	10.28
	[redacted]	251,263,939	0.23
	[redacted]	757,631,600	0.71
	[redacted]	1,919,655,315	1.79
	[redacted]	91,625,722	0.09
	[redacted]	7,204,890,348	6.71
	[redacted]	129,126,681	0.12

NOTES	Share	Size (bytes)	Size (GB)
CIFS	[redacted]	-	-
sep	[redacted]	569,908,141,842	530.77
	[redacted]	45,508	0.00
	[redacted]	2,952,375,976	2.75
	[redacted]	98,786,705,056	92.00
	[redacted]	25,467,868	0.02
	[redacted]	11,883,498	0.01
sep	[redacted]	1,129,417,907,576	1,051.85
	[redacted]	245,643,139	0.23
x	[redacted]	83,080,774,788	77.38
	[redacted]	21,678,684	0.02
x	[redacted]	166,835,370,355	155.38
	Total	2,051,285,994,290	1,910.41

NOTES	Share	Size (bytes)	Size (GB)
CIFS	[redacted]	-	-
	[redacted]	11,215,199	0.01
	[redacted]	827,445,007	0.77
	[redacted]	266,240	0.00
x	[redacted]	222,415,387,854	207.14
	[redacted]	704,219,216	0.66
	[redacted]	6,405,634	0.01
	[redacted]	94,320,071	0.09
	[redacted]	94,320,071	0.09
	[redacted]	41266941	0.04
	[redacted]	191,840	0.00
x	[redacted]	106,247,656,993	98.95

Filetypes:
TIFF
PDF
TXT
DOC
RTF
JPG
XLS
CSV

Total (TB):	4.35

Discovery: Lessons Learned

- Establish an acceptable risk of PII
- Use teamed/load balanced scanning options if possible
- Determine the full scope and size of shared storage scanning
- Policy considerations
    - Exclude common areas such as %WINDIR% and /Library/Logs
    - Search common file types (tiff, jpg, png, txt, rtf, doc, xls, csv…)
    - Enable OCR scanning

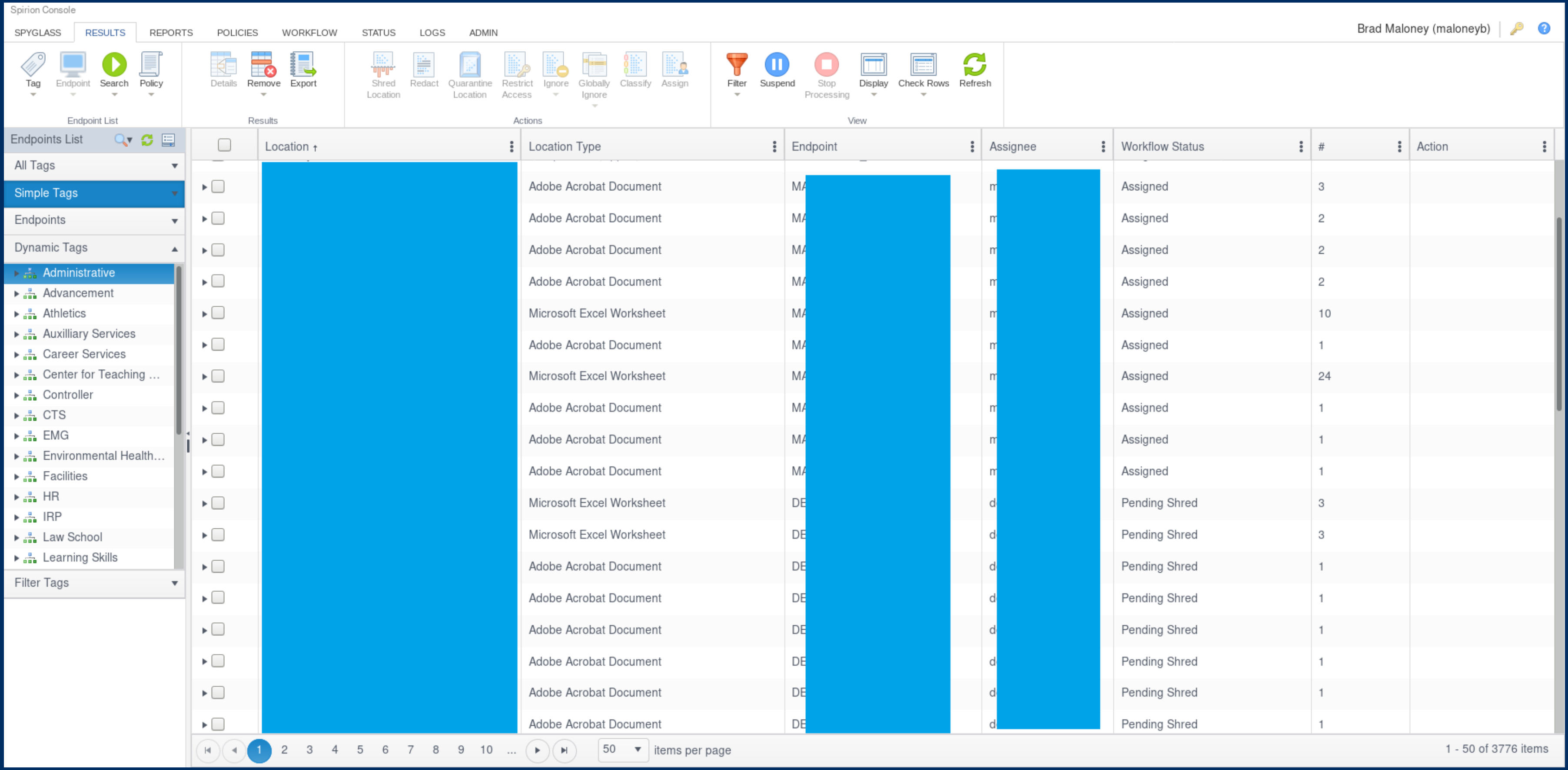
Remediation

Remediation Options

1. **Shred** – bypasses the Recycle Bin, cannot be restored or undone. Wipes data using a Department of Defense standard. Best action to take if you want to fully remove PII data.
2. **Ignore** – only when a false positive is reported. Information won't be searched or displayed in the future.

   Never ignore a file that contains valid PII !!!
3. **Quarantine** – relocates a file to a specific location
4. **Redact** – replaces PII data with masking characters. Keeps the rest of file intact for use. Only works on certain files. (123-45-6789 becomes XXX-XX-XXXX)

Remediation: User Interface



Location ↑	Location Type	Endpoint	Assignee	Workflow Status	#	Action
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Assigned	3	
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Assigned	2	
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Assigned	2	
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Assigned	2	
[redacted]	Microsoft Excel Worksheet	[redacted]	[redacted]	Assigned	10	
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Assigned	1	
[redacted]	Microsoft Excel Worksheet	[redacted]	[redacted]	Assigned	24	
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Assigned	1	
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Assigned	1	
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Assigned	1	
[redacted]	Microsoft Excel Worksheet	[redacted]	[redacted]	Pending Shred	3	
[redacted]	Microsoft Excel Worksheet	[redacted]	[redacted]	Pending Shred	3	
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Pending Shred	1	
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Pending Shred	1	
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Pending Shred	1	
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Pending Shred	1	
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Pending Shred	1	
[redacted]	Adobe Acrobat Document	[redacted]	[redacted]	Pending Shred	1	

1 2 3 4 5 6 7 8 9 10 ... 50 items per page

1 - 50 of 3776 items

Remediation: Results So Far

- Almost 7 million identified records deleted or shredded
- Hundreds of records redacted
- Users continue to review new results and revisit internal processes

Remediation: Lessons Learned

- Be prepared for users seeking guidance
- Do not expect the process to remediate quickly
- Maintain clear, concise messaging
- Establish relationships with departmental heads
- Find your PII removal champions

"You can't protect what you can't see"

Thank You!

Questions?

Brad Maloney | maloneyb@duq.edu
Manager, Secure Integrated Infrastructure

Michael Muto | mutom@duq.edu
Sr. Information Security Engineer