

Varonis and GDPR Operational Journey



Antonio Soriano, Jr.
Senior Systems Engineer/ Pre-sales- ASIA
Varonis Singapore



Fighting a different battle than
conventional cybersecurity companies.



Operational Journey for GDPR

May 15, 2018

Agenda

- ◆ GDPR Intro
- ◆ Relevant GDPR Articles
- ◆ How Varonis Helps (Operational Journey)
- ◆ GDPR Readiness Assessment



World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 24rd September 2016)

YEAR

BUBBLE COLOUR

YEAR

METHOD OF LEAK

BUBBLE SIZE

NO OF RECORDS STOLEN

DATA SENSITIVITY

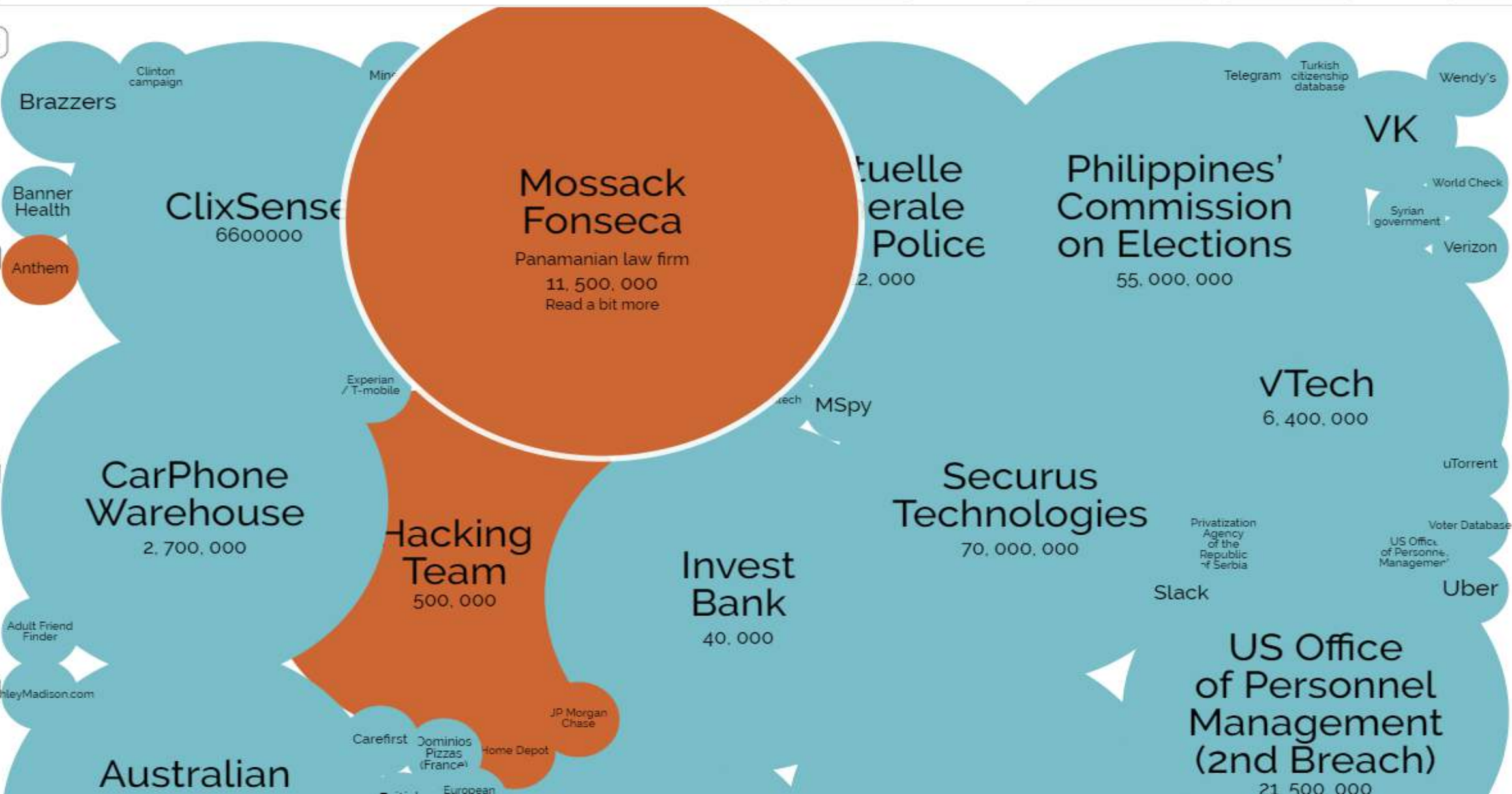
SHOW FILTER

latest

2016

2015

2014



GDPR Legislates Common Sense

- ◆ Puts processes around cybersecurity and data protection
- ◆ Turns IT and data security best practices into law
- ◆ Article 40 will eventually align GDPR with other data security standards, like PCI-DSS and ISO 27001

How much personal data lurks in these data stores?



Relevant GDPR Articles

◆ **Article 15:** Right of Access

- Fulfill data subject access requests (DSARs) by locating personal data, where it's stored, who has access, and who has been using it.

◆ **Article 25:** Data Protection by Design

- Discover of GDPR data, show who has access, and highlight personal information that is overexposed. Minimize personal data by automatically disposing of sensitive and stale data.

◆ **Article 17:** Right to Erasure

- Find personal data across data repositories and perform deletion to satisfy a “right to be forgotten” request.

◆ **Article 30:** Records of Processing

- Conduct data security reviews and generate reports based on type of data, access activity, and more.

Relevant GDPR Articles

◆ **Article 32:** Security of Processing

- Ensure least privilege access and provide reports that prove policies and procedures are in place and successful.

◆ **Article 35:** Data Protection Impact Assessment

- Continual risk analysis on GDPR data with actionable recommendations for reducing exposure.

◆ **Article 33:** Notification of Data Breach

- Detect and arrest suspicious activity and provide investigation and forensics capabilities to do breach reporting.



How Varonis Helps



DETECT

insider threats by analyzing data, account activity, and user behavior.



PREVENT

disaster by locking down sensitive and stale data, reducing broad access, and simplifying permissions.



SUSTAIN

a secure state by automating authorizations, migrations, & disposition.

Detect: Prepare – Articles

Article 35
Data Protection
Impact Assessment

Perform risk analysis on GDPR data with actionable recommendations for reducing exposure.

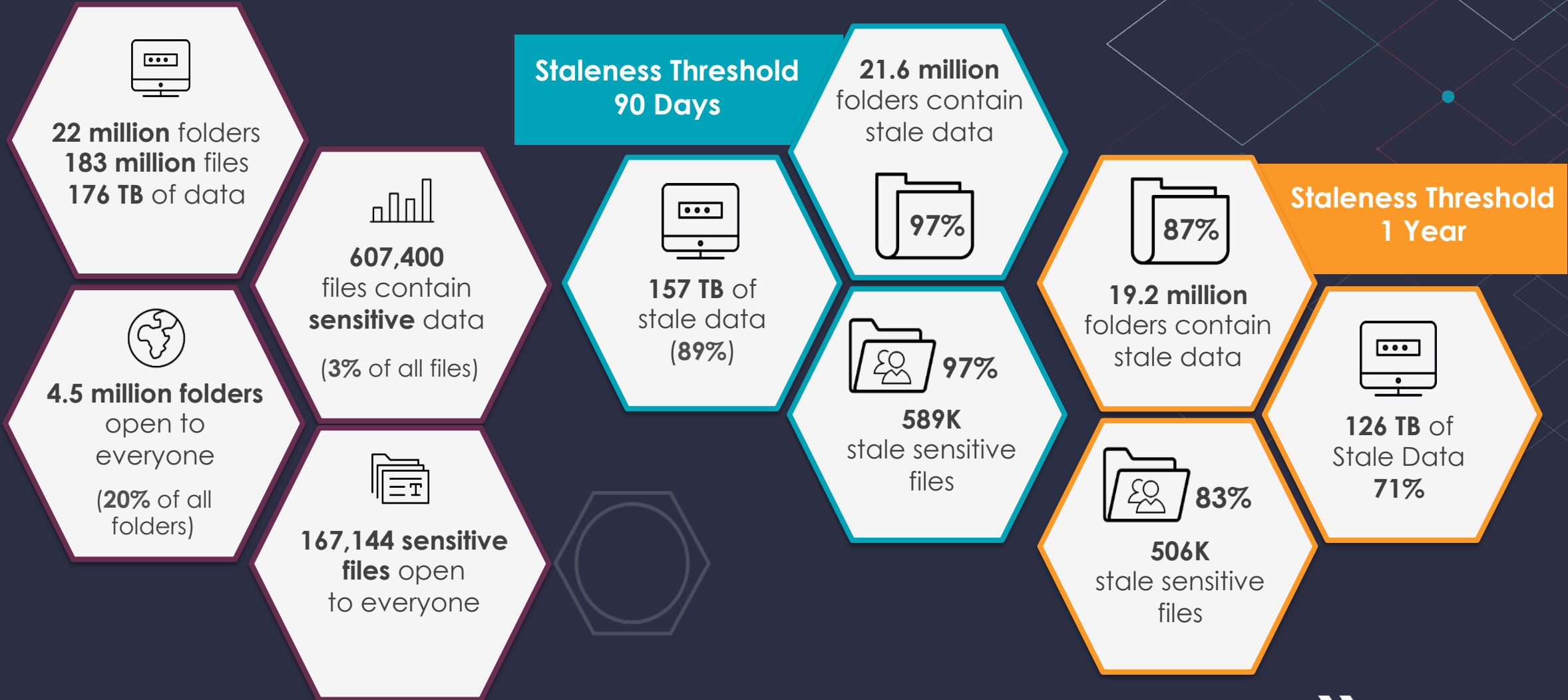
Article 25
Data Protection by
Design

Discover of GDPR data, show who has access, and highlight personal information that is overexposed.

Article 30
Records of
Processing

Monitor, analyze, and report on user access to data and flag anomalous activity.

Real World Example Data Impact Assessment



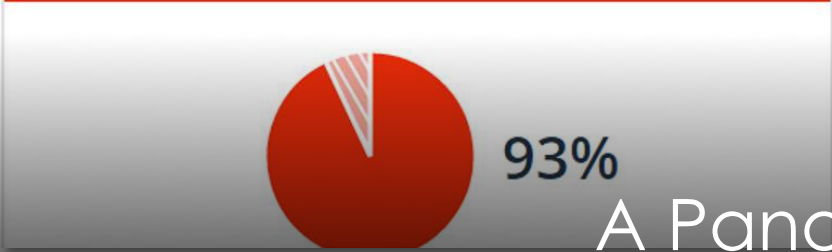
No. Of Sensitive Files

336 Files

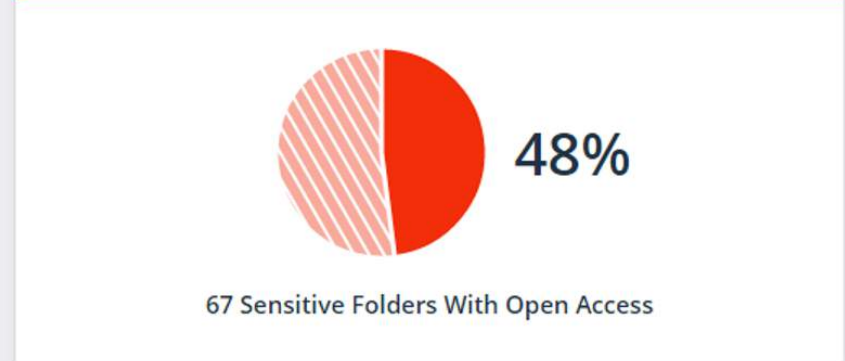
No. Of Stale Sensitive Files

77 Files
0.84% Stale Sensitive Files

No. Of Folders With Stale Data



No. Of Sensitive Folders With Open Access

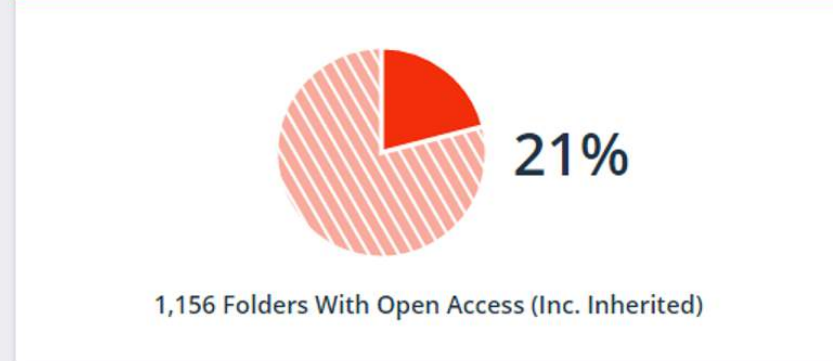


No. Of Sensitive Files With Open Access

201 Files
60% Sensitive Files With Open Access

No. Of Folders With Unresolved SIDs

No. Of Folders With Open Access (Inc. Inherited)



Size Of Folders With Stale Data(GB)

0.17 GB

Size Of All Files And Folders(GB)

1.17 GB

No. Of Folders With Inconsistent Permissions

A Panoramic View of Risk to GDPR Data

Alerts

Servers [] 01/19/2018 12:00 AM - 01/27/2018 11:59 PM [v]

Classification Rules any of (GDPR UK, GDPR France) [x] Is Sensitive = Yes [x]

Results (Including 48 events)

27 Alerts with high severity

20 Failed events

48 Events on sensitive data ⓘ

48 Alerted events ⓘ

Select Columns [] Export []

Drag columns to group

Device Name	File Server	Object Name (Event On)	Event Time	Event Operati.	Event Type	Threat Model Name
an-PC	corpfs02	Jim Gross.txt	01/23/2018 10:10 AM	Accessed	File opened	Abnormal behavior: accumulative increase in amount of idle and se
an-PC	corpfs02	Benjamin J. Morgan.txt	01/23/2018 11:49 AM	Accessed	File opened	Abnormal behavior: accumulative increase in amount of idle and se
an-PC	corpfs02	Benjamin J. Morgan.txt	01/23/2018 7:34 AM	Accessed	File opened	Abnormal behavior: accumulative increase in amount of idle and se
an-PC	corpfs02	Christopher Hall.txt	01/23/2018 7:47 AM	Accessed	File opened	Abnormal behavior: accumulative increase in amount of idle and se
an-PC	corpfs02	Paul Barrientos.txt	01/23/2018 9:52 AM	Accessed	File opened	Abnormal behavior: accumulative increase in amount of idle and se
an-PC	corpfs02	Della M. Johnson.txt	01/23/2018 7:54 AM	Accessed	File opened	Abnormal behavior: accumulative increase in amount of idle and se
an-PC	corpfs02	Jim Gross.txt	01/23/2018 7:46 AM	Accessed	File opened	Abnormal behavior: accumulative increase in amount of idle and se
X0rPC	corpfs02	Craig Magann.txt	01/24/2018 11:45 AM	Accessed	File opened	Abnormal behavior: accumulative increase in amount of idle and se
X0rPC	corpfs02	Paul Barrientos.txt	01/24/2018 7:31 AM	Accessed	File opened	Abnormal behavior: accumulative increase in amount of idle and se
X0rPC	corpfs02	Della M. Johnson.txt	01/24/2018 11:45 AM	Accessed	File opened	Abnormal behavior: accumulative increase in amount of idle and se
X0rPC	corpfs02	Jim Gross.txt	01/24/2018 8:36 AM	Accessed	File opened	Abnormal behavior: accumulative increase in amount of idle and se

Sortable, Searchable Record of GDPR Data Access

Detect: Operationalize – Articles

Article 32 Security of Processing	Ensure least privilege access and provide reports that prove policies and procedures are in place and successful.
Article 33 Notification of Data Breach	Detect and arrest suspicious activity and provide investigation and forensics capabilities to do breach reporting.
Article 15 Right of Access	Fulfill data subject access requests (DSARs) by locating personal data, where it's stored, who has access, and who has been using it.
Article 17 Right to Erasure	Find personal data across data repositories and perform deletion to satisfy a "right to be forgotten" request.

ALERTS

All Resources

Last 24h

Alert Details Category = Exfiltration

Found 1,000 Alerts within results:

300 ALERTS WITH HIGH SEVERITY

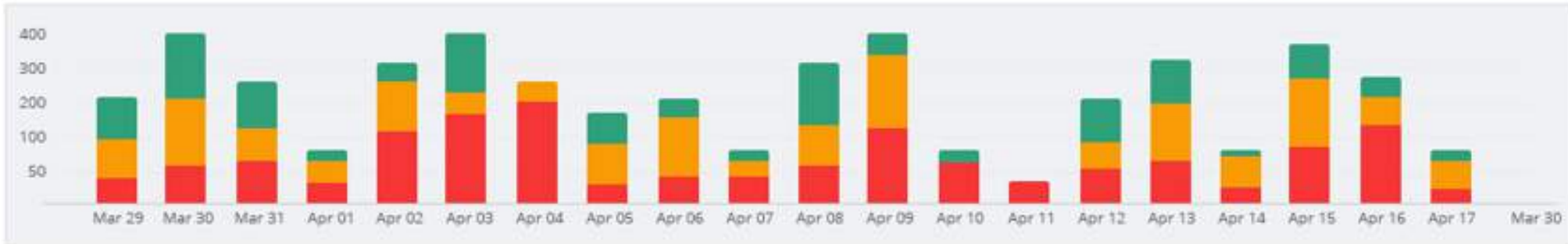
638 ALERTS ON SENSITIVE DATA

62 ALERTS BY ADMIN ACCOUNT

ALERTS

TIMELINE | 1 Day Per Column

Alerts Sevirity: High Medium Low



ALERTS LIST | Showing 100 of 1024 events

Column Picker

Drag column to Group By

User	Severity	Category	Assets	Rule	Event Count	Alert Count
<input type="checkbox"/> John Williams	High	Exfiltration	PM-Windows1\c\$\Docu...	Abnormal behavior:...	2 Events	1 Alerts
<input type="checkbox"/> Aaron Jones	High	Exfiltration	PM-Windows1\c\$\Docu...	Abnormal service be...	1 Events	1 Alerts
<input type="checkbox"/> Bill Carlson	Medium	Exfiltration	PM-Windows1\c\$\Docu...	Abnormal service be...	1 Events	1 Alerts

Alert on Anomalous Access to GDPR Data

EXPLORE

2012 Connected events

REFINE

ALERTS DETAILS (1000)

Category (12)

Severity (2)

Rules (2)

ALERTS BY USER (3)

Users (742)

Groups (34)

Department (4)

Location (2)

ALERTS ON RESOURCES (3)

Object Type (1)

Access to an unusual number of idle GDPR files

corp.local\Hijacked Helen accessed N/A idle GDPR files, exceeding normal behavior (1,218 files) by 87%

[Threat model info](#) v

RISK ASSESSMENT INSIGHTS

USERS



corp.local\Hijacked Helen
Engineering

Account was not **changed** in the 7 days prior to the current alert

User is not on the **Watch List**

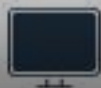
Is not a **disabled/deleted** account

Is not a **privileged** account

Triggered 6 **alerts** in the 7 days prior to the current alert

[2 Additional insights](#)

DEVICES



H4xX0rPC

All devices **were used** by the user in the 90 days prior to the current alert

H4xX0rPC was involved in 6 **alerts** in the past 7 days

Alert on Anomalous Access to GDPR Data

Prevent: Fix – Articles

Article 25 Data Protection by Design

Get to a least privilege model by repairing permissions issues and systematically revoking excessive access to GDPR data.

New Group * New Filter Remove Selected Reset Import/Export Filter Filter Sort

and

Classification results

Rule names Contained in GDPR Hungary, GDPR Czech, GDPR Greece, GDPR UK, GDPR France, GDP

and

Selected object types Contained in Folders containing files with hits, Ancestor folders

and

Hit count (on selected rules) Greater than 0

Run

Preview

Up

Report 12.I.02, Open Access on Sensitive Data

This report displays the folders with open access that contain files with hits on the selected classification rules. It is ordered according to the total number of hits on the files in the folders.

i Open access refers to folders with permissions granted to global access groups through both Share and NTFS permissions.

The report includes the following columns:

Field	Description
File Server	The name of the file server on which the folder resides.
Access Path	The path name of the folder that has NTFS and Share permissions for global access groups.
Group with Share Permissions	The name of the group with Share permissions on the folder.

Quickly Report on Open Access to Sensitive GDPR Data

Permissions Visibility

Look for:

Resources: fileserver01

Directory	Permissions	Size	Sensitive Data
DSR		25.4 GB	
Finan		1.2 TB	
Engin		34.9 GB	
Legal		235 GB	Visa (35), US SSN (200)
Marke			
Medic			
Mobil			
OEM			
PRS			

Simulation Results

Users impacted:

- Allen Carey (CORP)
- Angela Martin (CORP)
- Erin Hannon (CORP)
- Pam Beesly (CORP)

Commit

Directory	Permissions
Everyone (Abstract)	Protection added to C:\Share\legal
Legal (CORP)	Add RXL for Legal (CORP) to C:\Share\legal

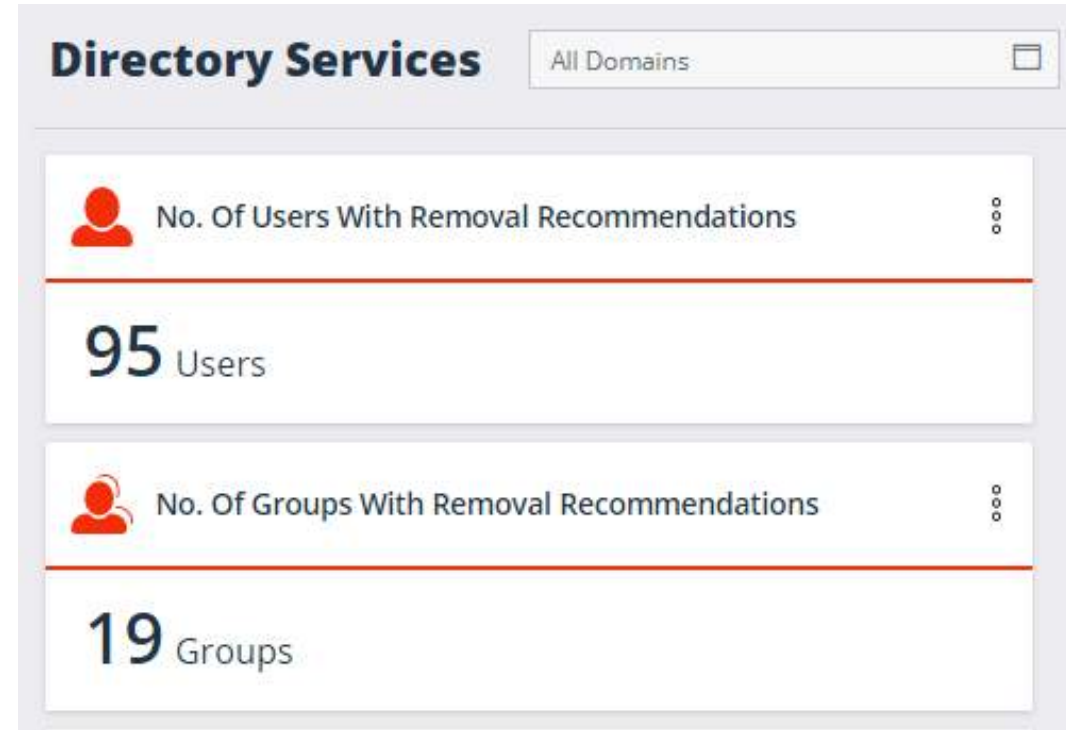
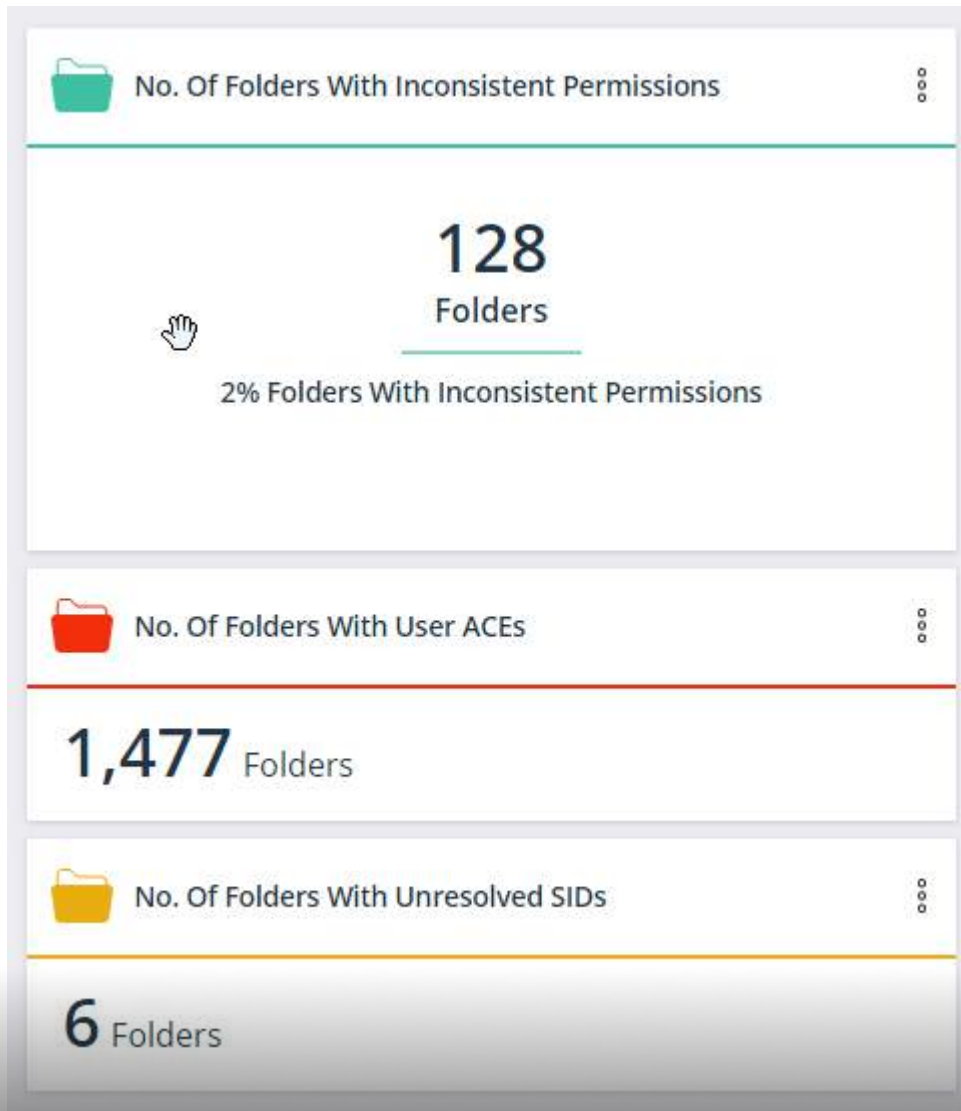
Immediate
 Schedule on:

Safely Revoke Global or Excessive Access to GDPR Data

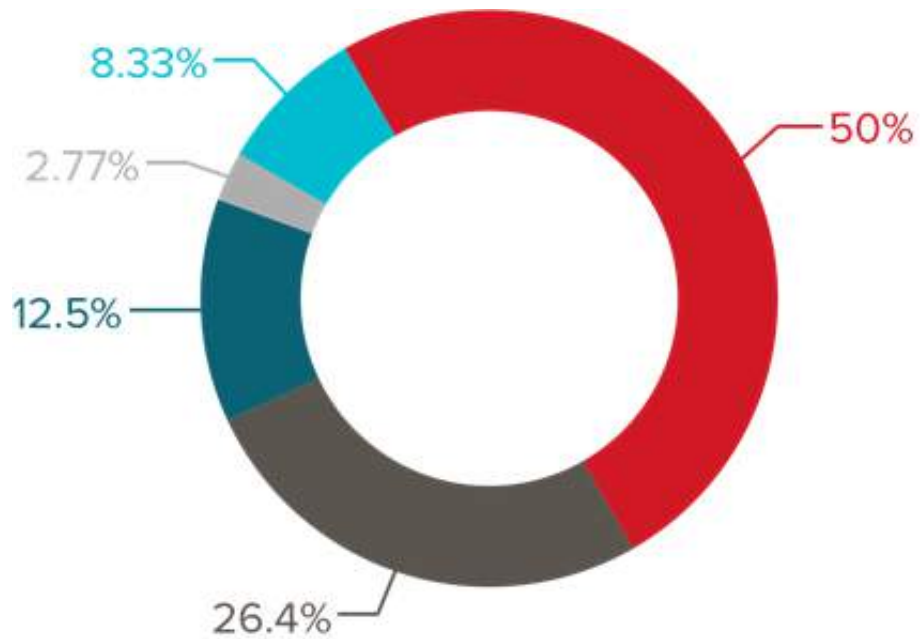
Prevent: Transform – Articles

Article 25 Data Protection by Design

Identify data owners, simplify permissions structures, and prune unnecessary access to make a least privilege model attainable.



Identify & Fix Misconfigurations that Could Expose GDPR Data



Allen Carey (CORP)

Margaret Coakley (CORP)

Crystal Grove (CORP)

Andrew Weirich (CORP)

Anne Thornton (CORP)

VARONIS DATAPRIVILEGE Analyze Reports

DATA OWNERSHIP SURVEY > SURVEY Domain: Database: Mail Server:

HELP

You have been identified as a potential data owner for the list of directories to the right.

If you are not the owner of a particular directory, please select "No". If you think you know the data owner, please fill out the suggestion input box. Once you start typing a name, a list of matching users will appear. Click on the user to set them as a suggested user.

CYCLOPS DATA OWNER SURVEY

Path	Are you the Owner?	
R-WinFS C:\ShareOne\Folder-2	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
	<input type="text" value="Suggest Owner"/>	
R-WinFS C:\ShareOne\Folder-1	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
R-WinFS C:\ShareOne\Folder-2	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
R-WinFS C:\ShareOne\Folder-3	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No

Use Analytics & Surveys to Identify Data Owners

Sustain: Automate – Articles

Article 25 Data Minimization

Enforce data retention and deletion policies with automatic rules to eliminate data no longer necessary to the original collection purpose.

Article 25 Data Protection by Design

Sustain a least privilege model by automating entitlement reviews and authorization workflows.

Article 32 Security of Processing

Ensure least privilege access and provide reports that prove policies and procedures are in place and successful.

Rules

Commit

Groups

Permission Mapping

Rules

Create, edit and view all pending, running and historical rules



Edit Rule



Clone Rule



Calculate



Last run time:

Start



15

End

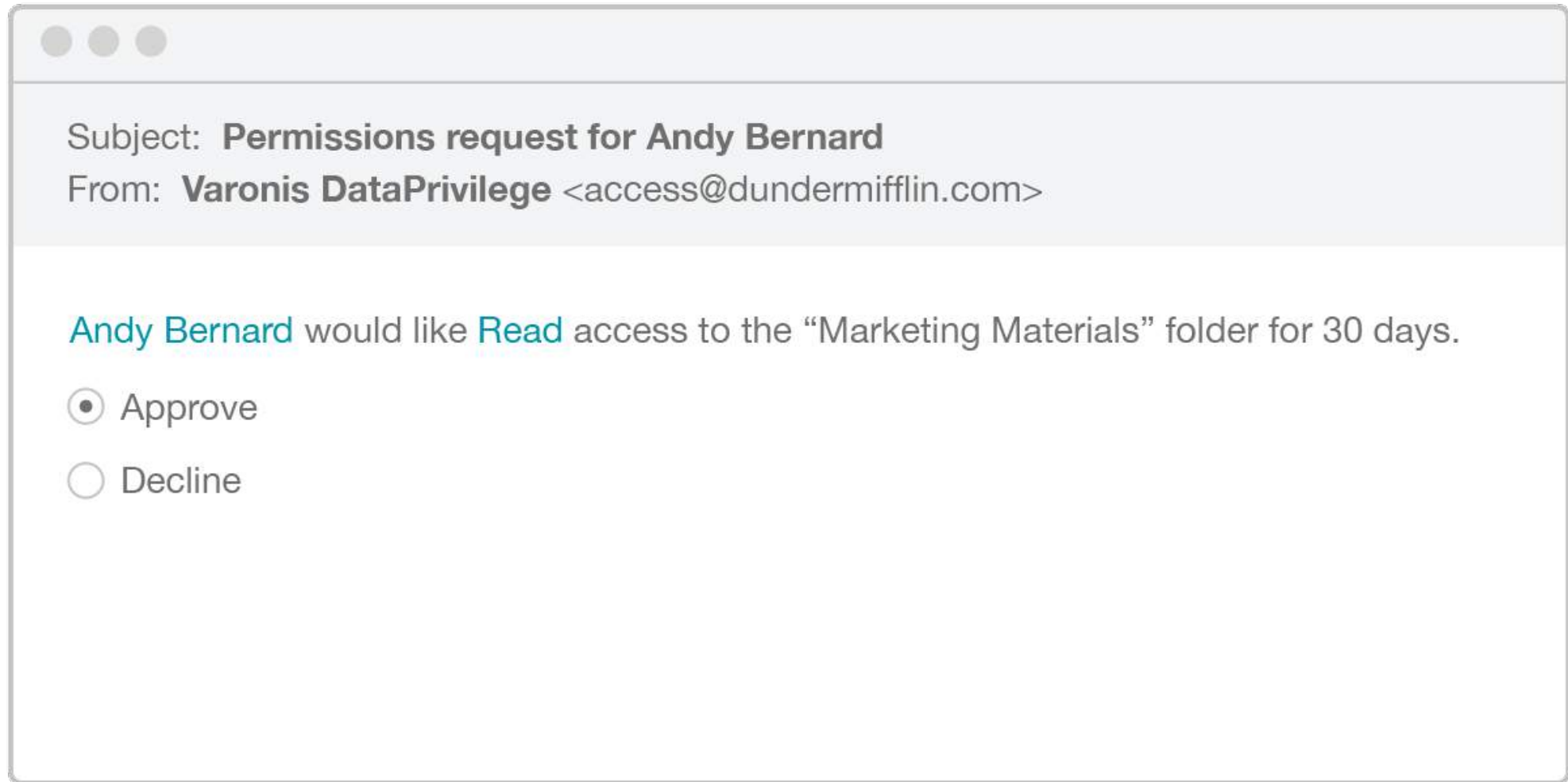


15

Rule Name	Type	Status	Progress (%)	Last Run	Schedule
Department Archival Rule	Regular	Ready to run			No Schedule
Media File Removal	Regular	Ready to run			No Schedule
HR Historical Record Archive...	Regular	Ready to run			No Schedule
GDPR Quarantine	Regular	Ready to run			No Schedule
Replication of Sales Data	Mirror	No sources found			No Schedule

Total number of rules: 5

Create Rules to Automatically Move, Archive, Delete Data
And Enforce Policies



Automate Authorization Workflows to Ensure the *Right* People are in Control of Granting & Revoking Access



This group provides access to GDPR data! Review carefully!

Status	Users	Permission	Decision and Explanation	
	 Allison Scafer (CORP)	Exe-Write	<input checked="" type="radio"/> Keep	<input type="radio"/> Remove
	 Andrew Carlisle (CORP)	Exe-Write	<input checked="" type="radio"/> Keep	<input type="radio"/> Remove
	 Andrew Weirich (CORP)	NA	<input type="radio"/> Keep	<input checked="" type="radio"/> Remove
	 Andy Welch (CORP)	Execute	<input checked="" type="radio"/> Keep	<input type="radio"/> Remove
	 Anne Lampkin (CORP)	Execute	<input checked="" type="radio"/> Keep	<input type="radio"/> Remove

Automate Entitlement Reviews with GDPR Context

Sustain: Improve – Articles

Article 35 Data Protection Impact Assessment

Continual risk analysis on GDPR data with actionable recommendations for reducing exposure.

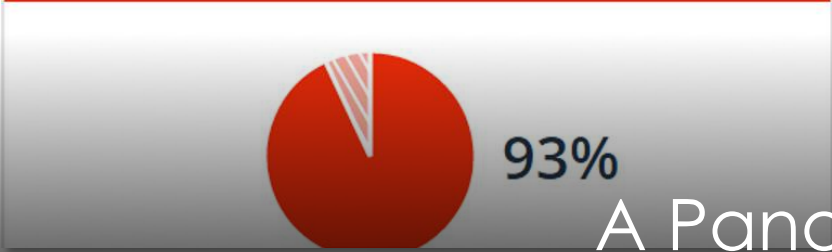
No. Of Sensitive Files

336 Files

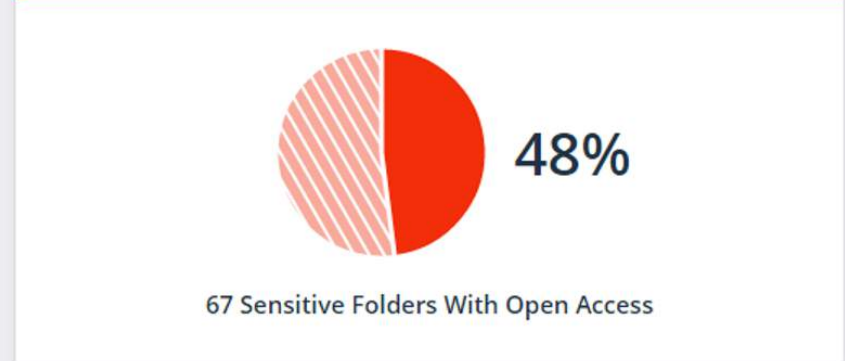
No. Of Stale Sensitive Files

77 Files
0.84% Stale Sensitive Files

No. Of Folders With Stale Data



No. Of Sensitive Folders With Open Access



No. Of Sensitive Files With Open Access

201 Files
60% Sensitive Files With Open Access

No. Of Folders With Unresolved SIDs

No. Of Folders With Open Access (Inc. Inherited)



Size Of Folders With Stale Data(GB)

0.17 GB

Size Of All Files And Folders(GB)

1.17 GB

No. Of Folders With Inconsistent Permissions

A Panoramic View of Risk to GDPR Data

Journey of Value

— Risk Reduction
— Efficiency Gains



DETECT:
1. Prepare

Deploy Varonis

Prioritize and assess risks | DA, DCE



DETECT:
2. Operationalize

Create incident response plan based on alerts, including automation | DLS

Train staff on the basics - managing perms and finding lost files | DA



PREVENT:
3. Fix

Fix broken ACL's | DA, AE

Eliminate global access to sensitive data | DA, DCE, AE

Eliminate remaining global access groups | DA, AE

Eliminate unnecessary AD artifacts (unused security groups, non-expiring passwords, etc.) | DA

Quarantine/archive/delete stale data | DA, DTE



PREVENT:
4. Transformation

Identify folders that need owners | DA

Identify data owners | DA

Simplify permissions structure | DA, DP

Provide owners reports about their data | DA



SUSTAIN:
5. Automation

Automate authorization workflow via Data Owners | DP

Automate periodic entitlement reviews | DP

Automate disposition, quarantining, policy enforcement | DLS, DTE, DCE



SUSTAIN:
6. Improve

Regularly review risks, alerts and processes to ensure continuous improvement | DA, DP, DLS, DCE, DTE

DA | DatAdvantage
 DLS | DatAlert Suite
 DCE | Data Classification Engine
 AE | Automation Engine
 DTE | Data Transport Engine
 DP | DataPrivilege



...so what now?

GDPR Readiness Assessment

- ◆ Discover GDPR eligible data
- ◆ Lock down access to overexposed data
- ◆ Audit user activity and detect suspicious behavior
- ◆ Identify and prioritize gaps in GDPR compliance



Thank You

Antonio Soriano Jr

Philippines: +63 927 888 3055

Singapore: +65 9769 1439

e: asoriano@varonis.com



Philippine/Local Partner:

Next Innovation Inc.

Hans Jeremy Ong

Philippines: +63 917 832 2119

e: hans.Jeremy.ong@nii.ph