Varonis and GDPR Operational Journey

Antonio Soriano, Jr.

Senior Systems Engineer/ Pre-sales- ASIA

Varonis Singapore

VARONIS

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

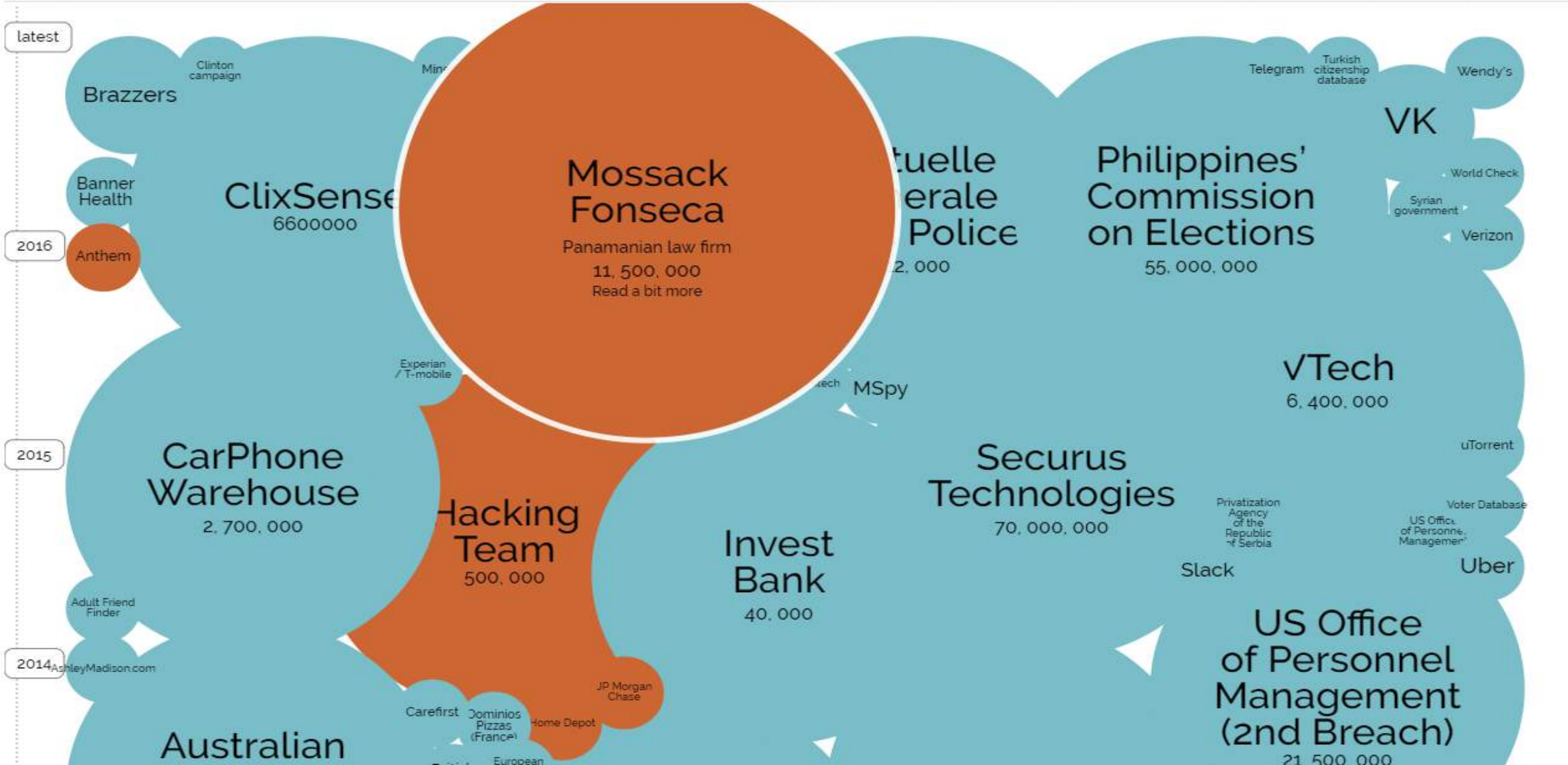
World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 24rd September 2016)

interesting story

YEAR | BUBBLE COLOUR: YEAR | METHOD OF LEAK | BUBBLE SIZE: NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER



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?

NAS

WINDOWS

UNIX/LINUX

Directory Services

OFFICE 365

MS ACTIVE DIRECTORY

SHAREPOINT

EXCHANGE

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.

VARONIS

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.

VARONIS

Real World Example Data Impact Assessment

22 million folders
183 million files
176 TB of data

4.5 million folders open to everyone
(**20%** of all folders)

607,400 files contain **sensitive** data
(**3%** of all files)

167,144 sensitive files open to everyone

Staleness Threshold 90 Days

157 TB of stale data (**89%**)

21.6 million folders contain stale data

97%

97%
589K stale sensitive files

Staleness Threshold 1 Year

87%
19.2 million folders contain stale data

126 TB of Stale Data
71%

83%
506K stale sensitive files

VARONIS

VARONIS DATALERT

Dashboards | Analytics

File Servers

corpfs02b

Add Widget

No. Of Sensitive Files

336 Files

No. Of Stale Sensitive Files

77
Files

0.84% Stale Sensitive Files

No. Of Folders With Stale Data

93%

No. Of Sensitive Folders With Open Access

48%

67 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)

21%

1,156 Folders With Open Access (Inc. Inherited)

Size Of Folders With Stale Data(GB)

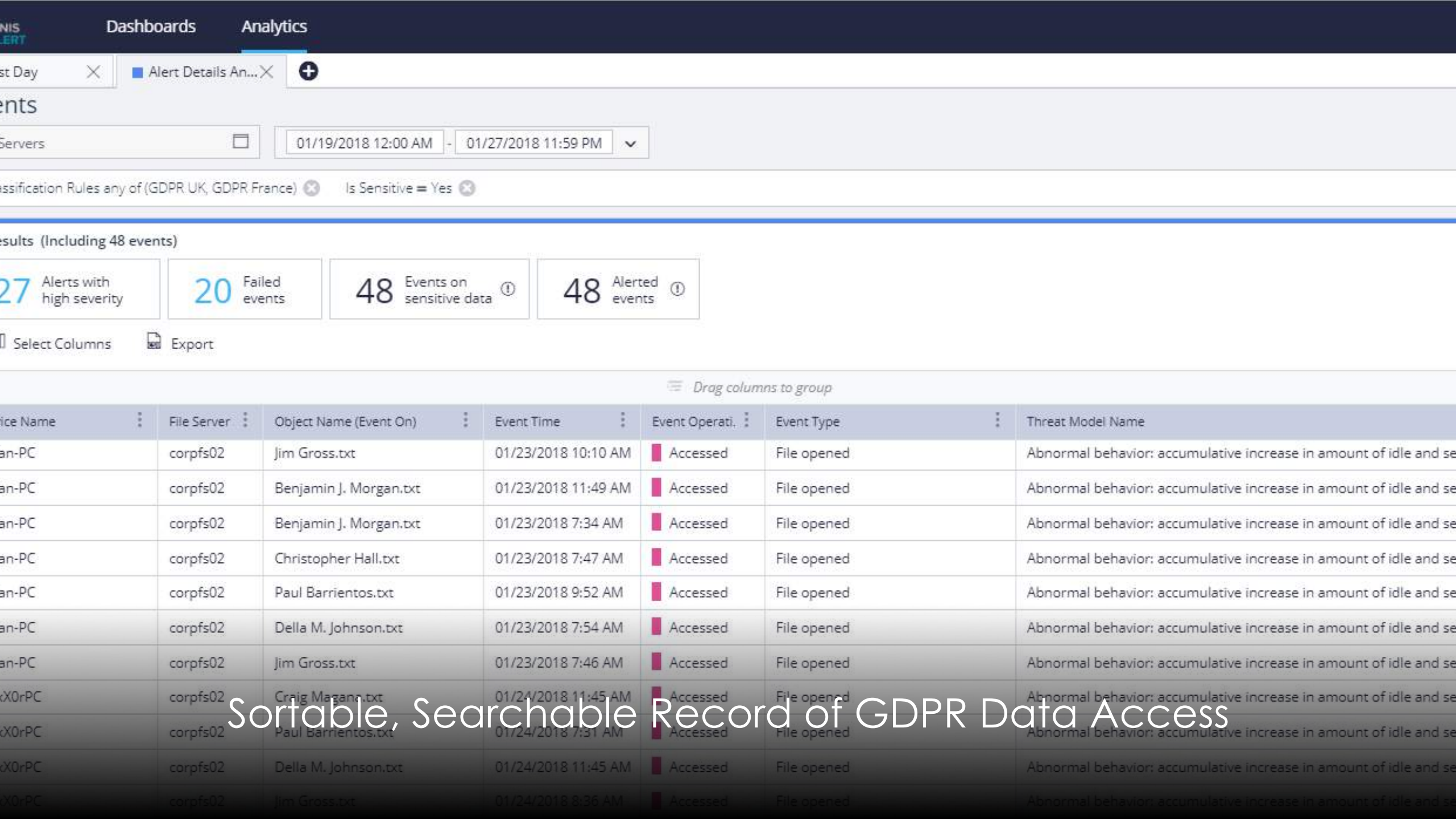
0.17 GB

Size Of All Files And Folders(GB)

1.17 GB

No. Of Folders With Inconsistent Permissions

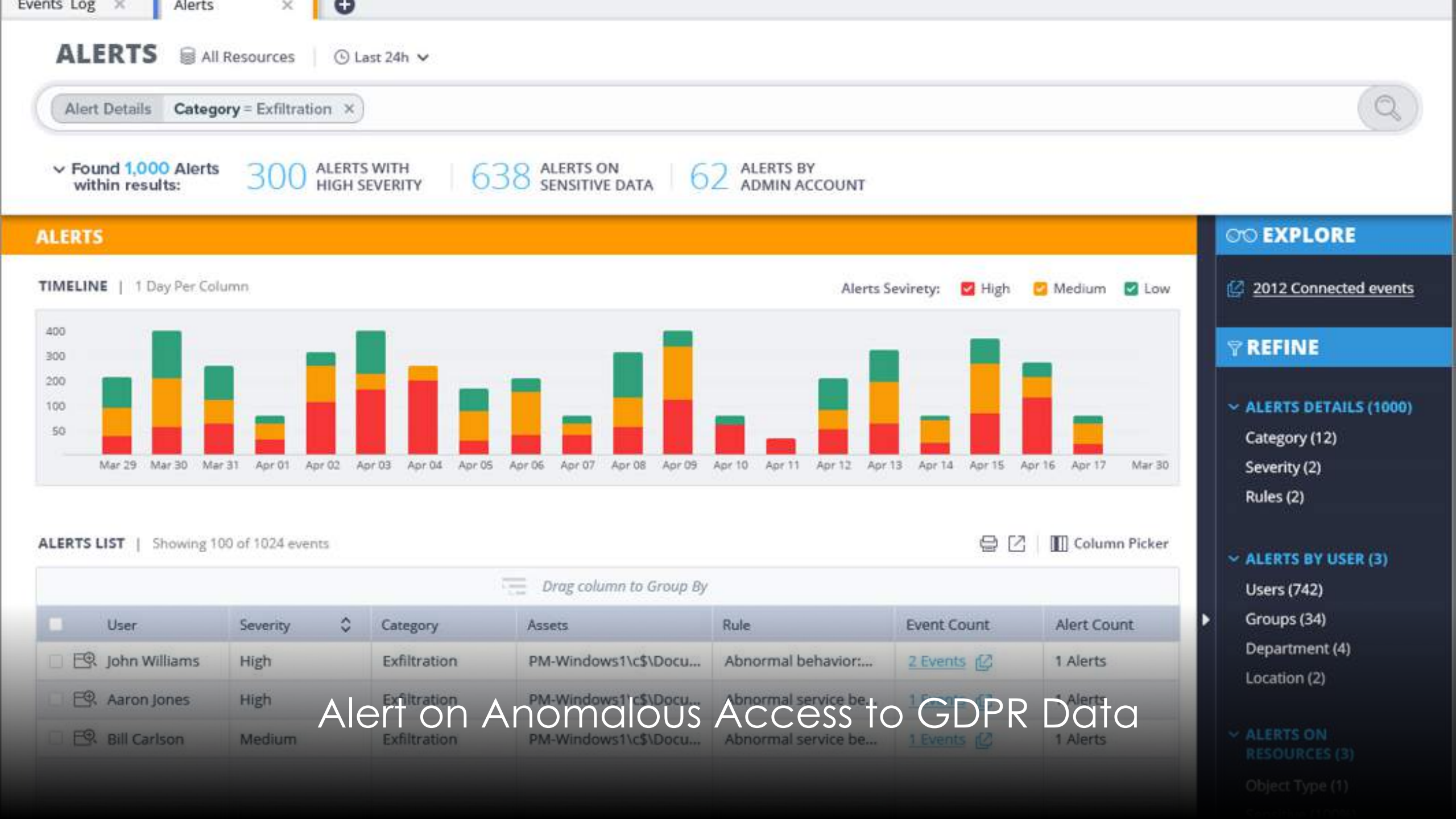
A Panoramic View of Risk to GDPR Data



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.



Alert on Anomalous Access to GDPR Data

Emergency | Exfiltration | Status: Open

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

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

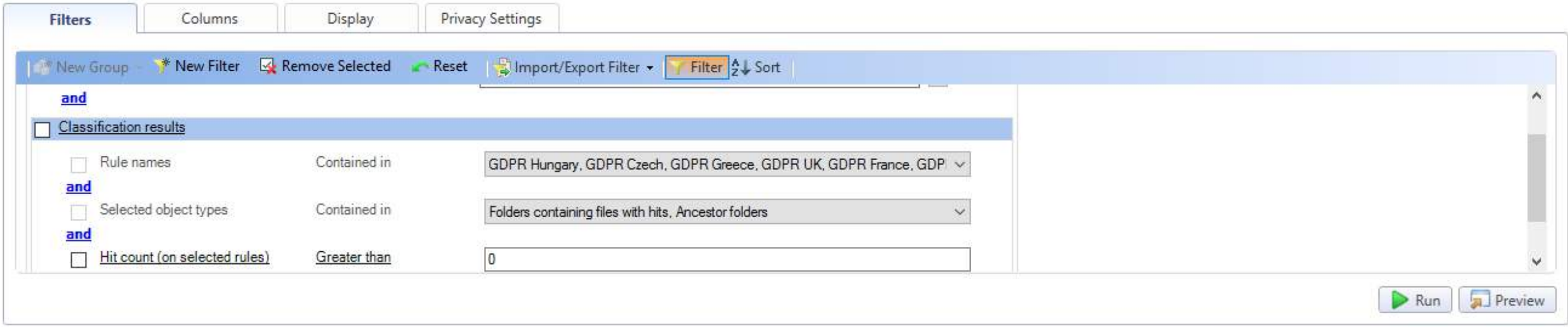
H4xX0rPC

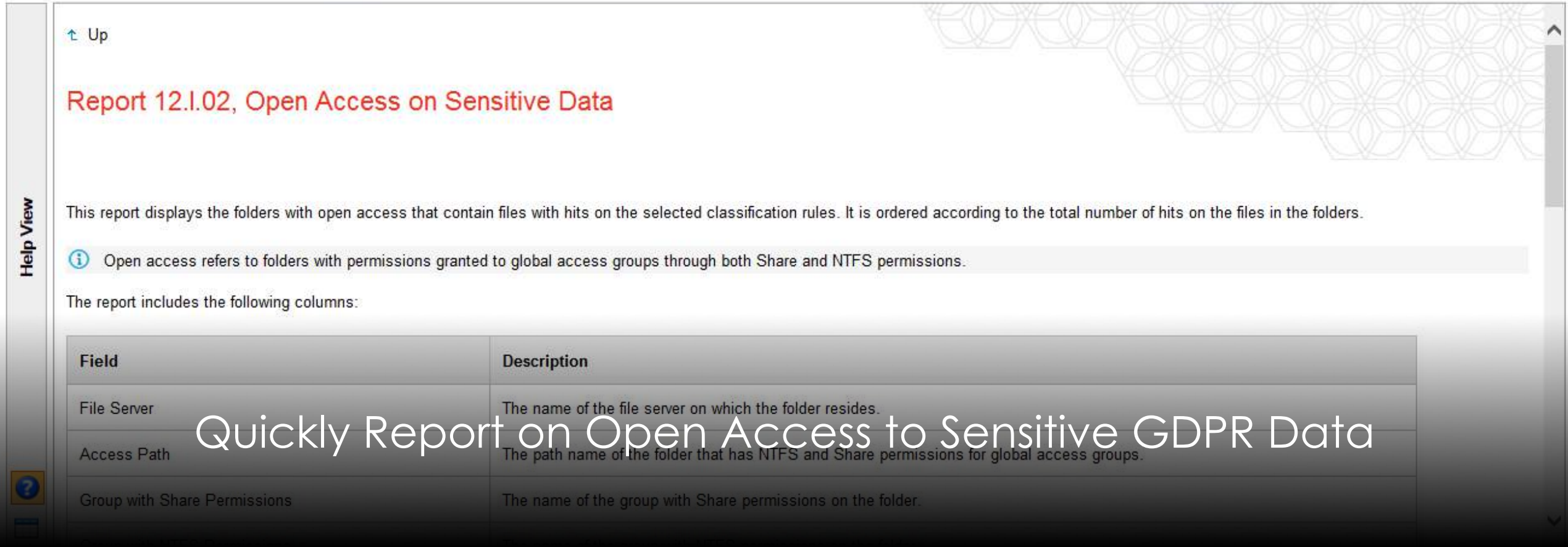
All devices **were used** by the user in the 90 days prior to the current alert
H4xX0rPC was involved in 6 **alerts** in the past 7 days
1 Additional insight

Alert on Anomalous Access to GDPR Data

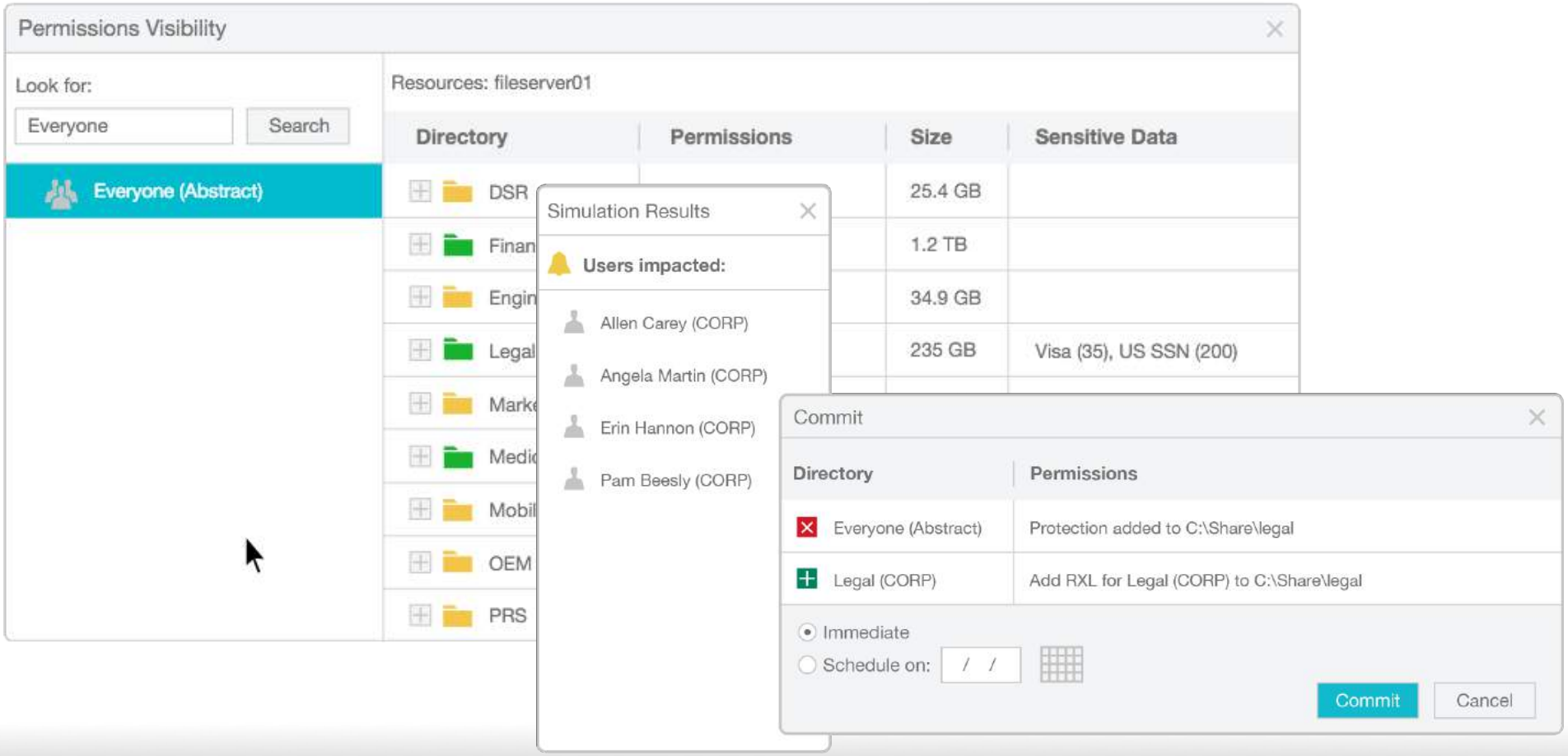
Prevent: Fix – Articles

Article 25 Data Protection by Design	Get to a least privilege model by repairing permissions issues and systematically revoking excessive access to GDPR data.





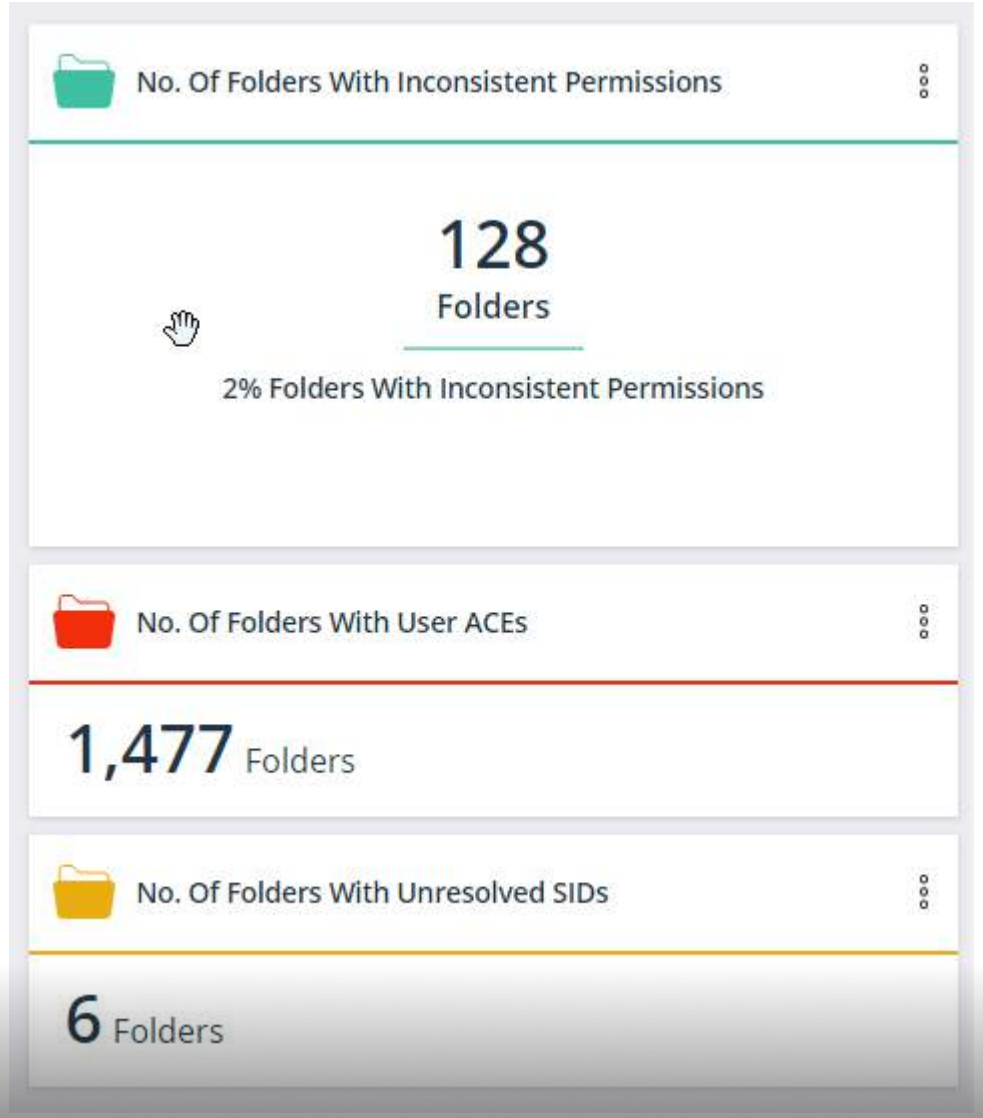
Quickly Report on Open Access to Sensitive GDPR Data

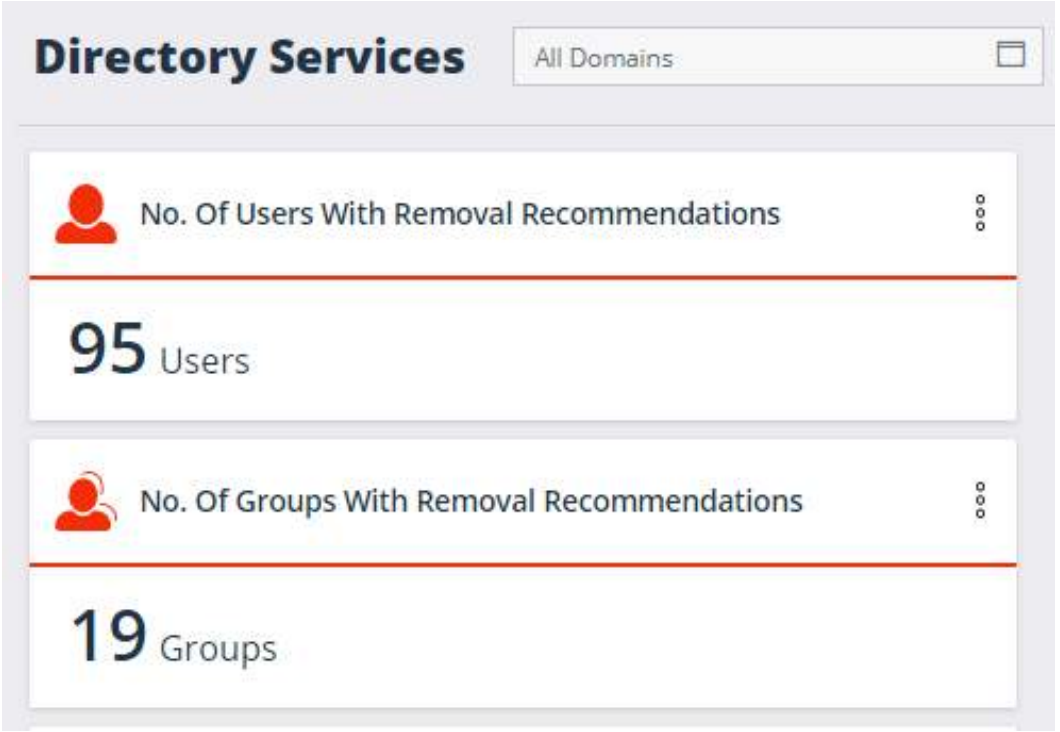


Safely Revoke Global or Excessive Access to GDPR Data

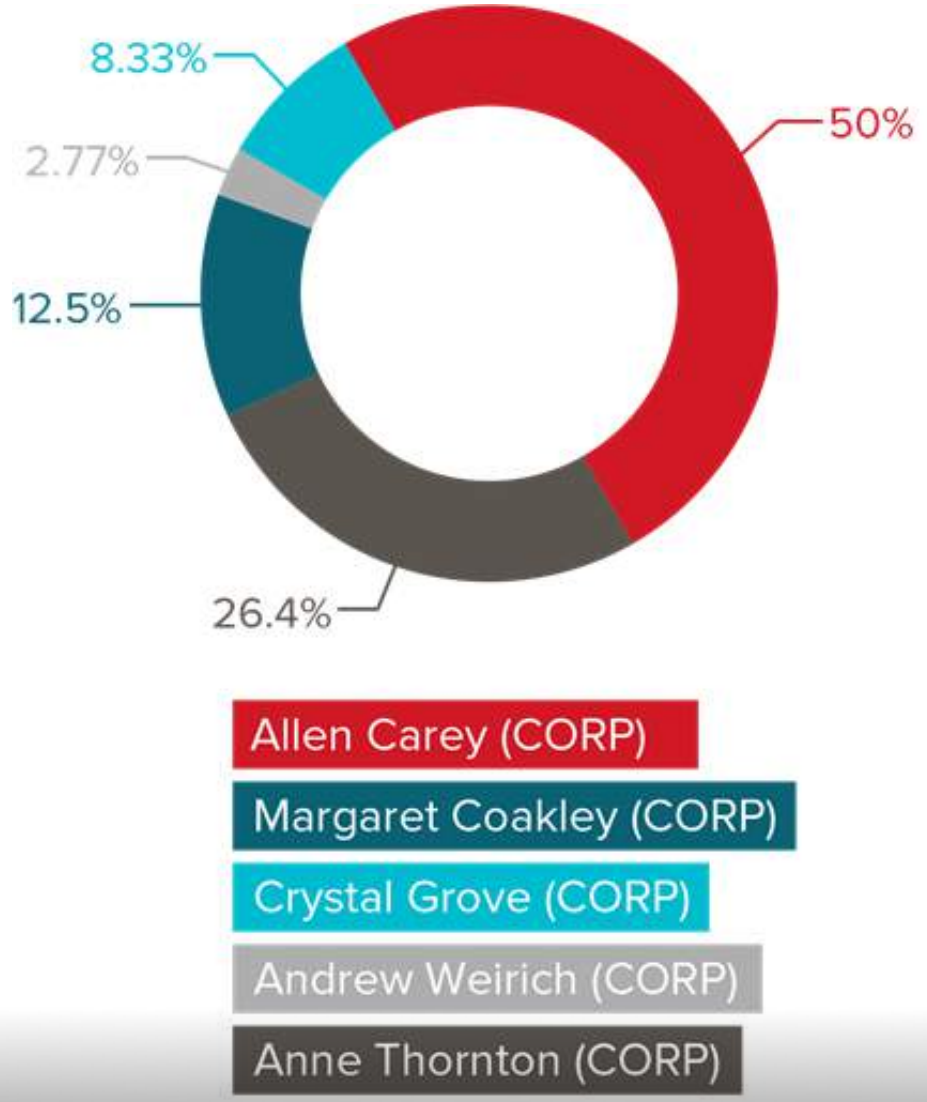
Prevent: Transform – Articles

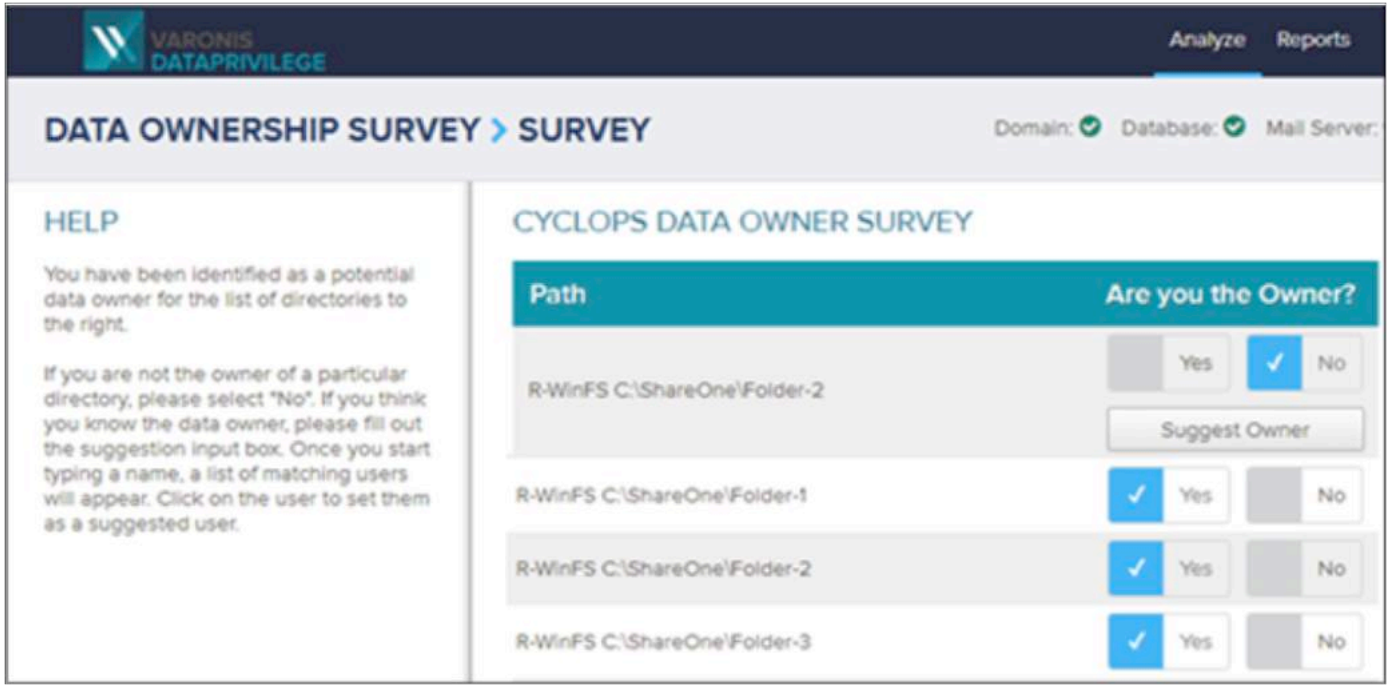
Article 25 Data Protection by Design	Identify data owners, simplify permissions structures, and prune unnecessary access to make a least privilege model attainable.





Identify & Fix Misconfigurations that Could Expose GDPR Data

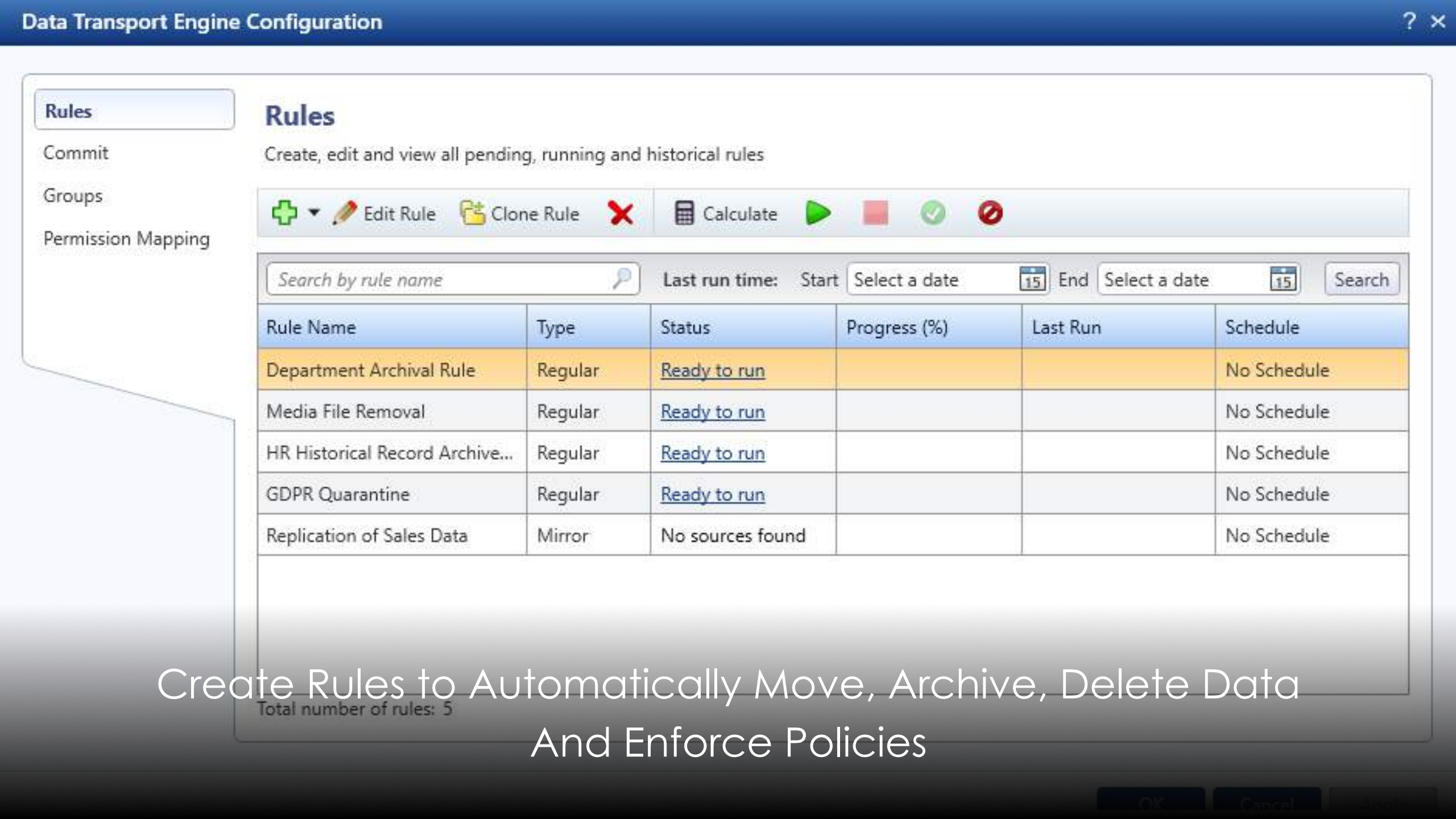


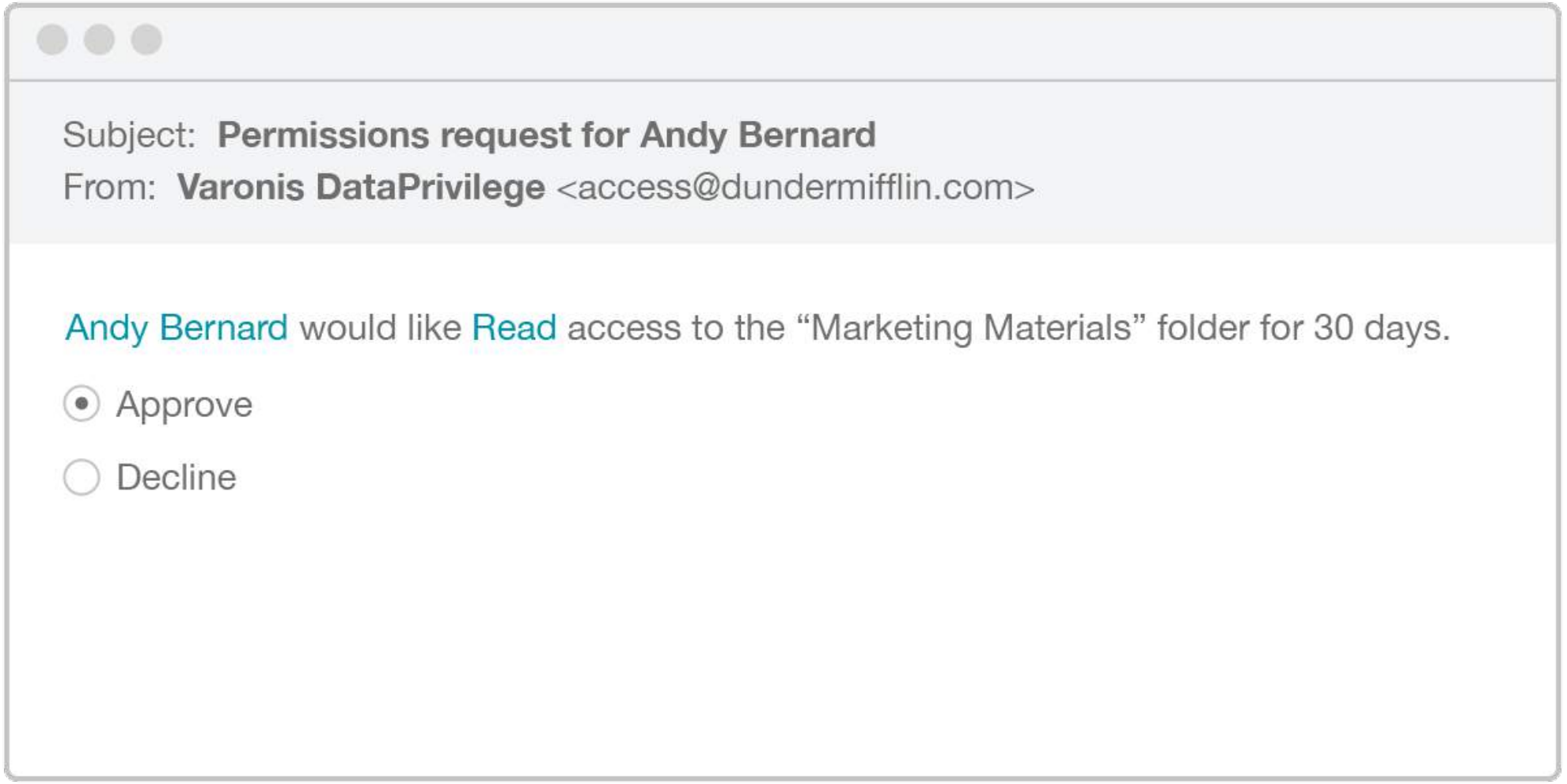


Use Analytics & Surveys to Identify Data Owners

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.


Data Transport Engine Configuration
Rules
Commit
Groups
Permission Mapping
Rules
Create, edit and view all pending, running and historical rules
Edit Rule
Clone Rule
Calculate
Search by rule name
Last run time:
Start
Select a date
End
Select a date
Search
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	(•) Keep ( ) Remove
	Andrew Carlisle (CORP)	Exe-Write	(•) Keep ( ) Remove
✕	Andrew Weirich (CORP)	NA	( ) Keep (•) Remove
	Andy Welch (CORP)	Execute	(•) Keep ( ) Remove
	Anne Lampkin (CORP)	Execute	(•) Keep ( ) 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.

VARONIS DATALERT

Dashboards | Analytics

File Servers

corpfs02b

Add Widget

No. Of Sensitive Files

336 Files

No. Of Stale Sensitive Files

77
Files

0.84% Stale Sensitive Files

No. Of Folders With Stale Data

93%

No. Of Sensitive Folders With Open Access

48%

67 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)

21%

1,156 Folders With Open Access (Inc. Inherited)

Size Of Folders With Stale Data(GB)

0.17 GB

Size Of All Files And Folders(GB)

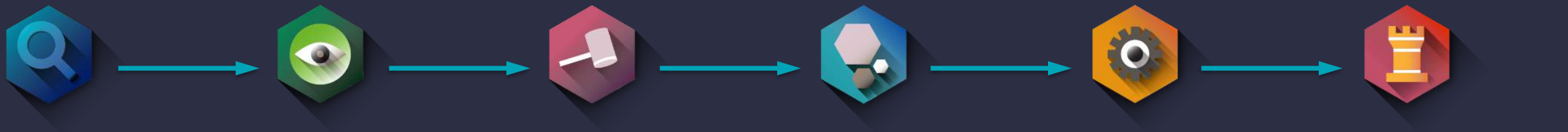
1.17 GB

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

VARONIS

…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