VARONIS

“

Defenders live in a world of uncertainty.

The goal is to reduce the attacker’s window of opportunity and reduce uncertainty.

Visibility is the game.

”

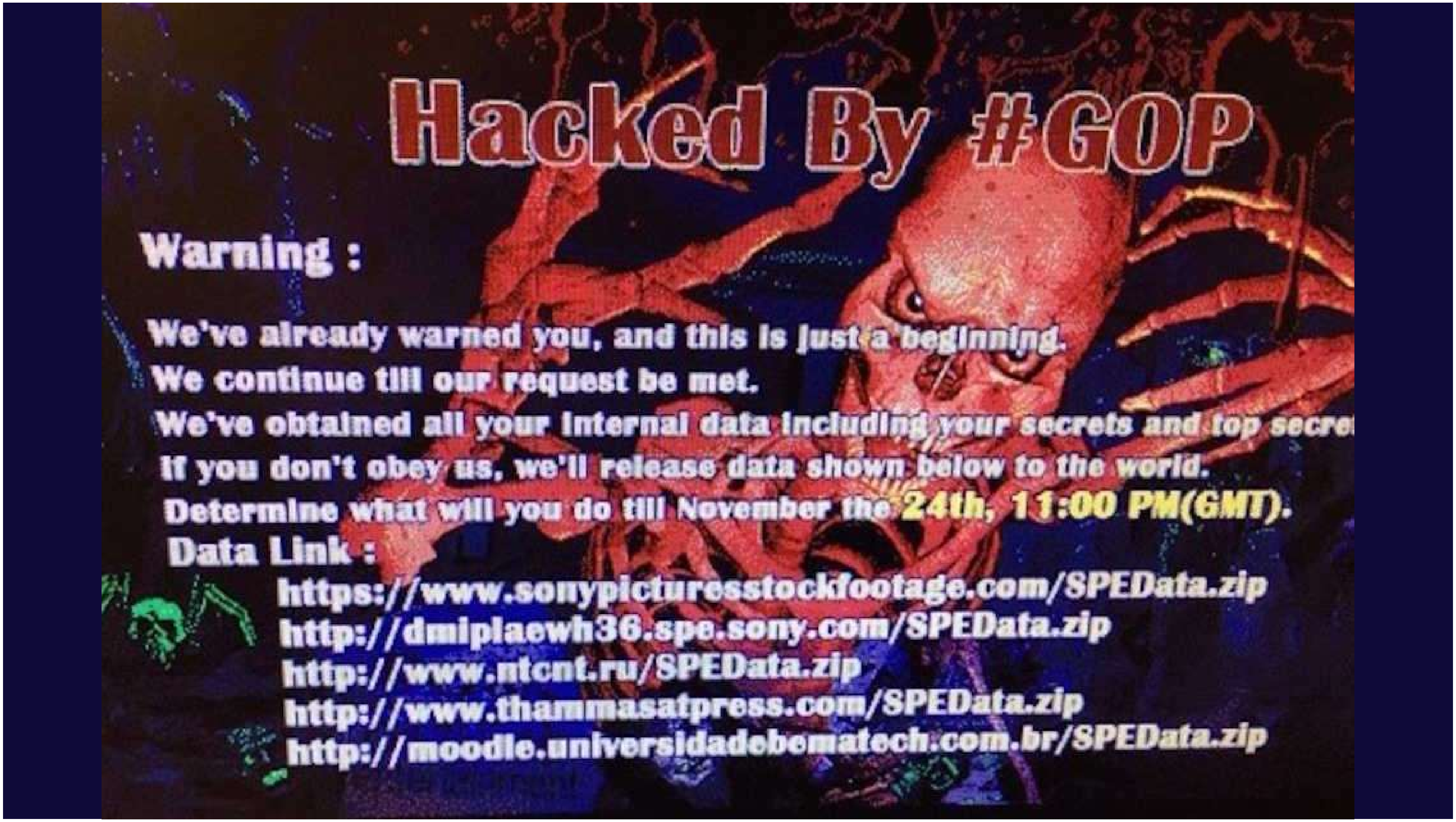
Yossi Sassi

Yossi Sassi is a white hat hacker and consultant, and believes strongly that given enough time and motivation, any system can be hacked. Defenders live in a world of uncertainty. To succeed, they need to limit the access and time an attacker has.

DATA-CENTRIC SECURITY – FUNDAMENTAL FOR THREAT DETECTION IN 2019 AND BEYOND

CommonwealthBank

“Forensic investigators hired to assess the breach retraced the route of the truck to determine whether they could locate the drives along this route, but were unable to find any trace of them.”



Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.
We continue till our request be met.
We've obtained all your internal data including your secrets and top secre
If you don't obey us, we'll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Data Link :
https://www.sonypicturesstockfootage.com/SPEData.zip
http://dmiplaewh36.spe.sony.com/SPEData.zip
http://www.ntcnt.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebematech.com.br/SPEData.zip

LinkedIn

Hacked: 2012
Leaked: 2016

Dropbox

Hacked: 2012
Leaked: 2016

DISQUS

Hacked: 2014
Leaked: 2017

imgur

Hacked: 2013
Leaked: 2017

> “Organizations are failing at early breach detection, with fewer than 20% of breaches detected internally.”

Gartner

Using SIEM for Targeted Attack Detection
Oliver Rochford & Kelly M. Kavanagh

Highlights from the Varonis

2019 Global Data Risk Report

of all folders are open to **every employee**

53%

of companies have 1,000+ sensitive files open to **every employee**

87%

of companies have 1,000+ **stale sensitive files**

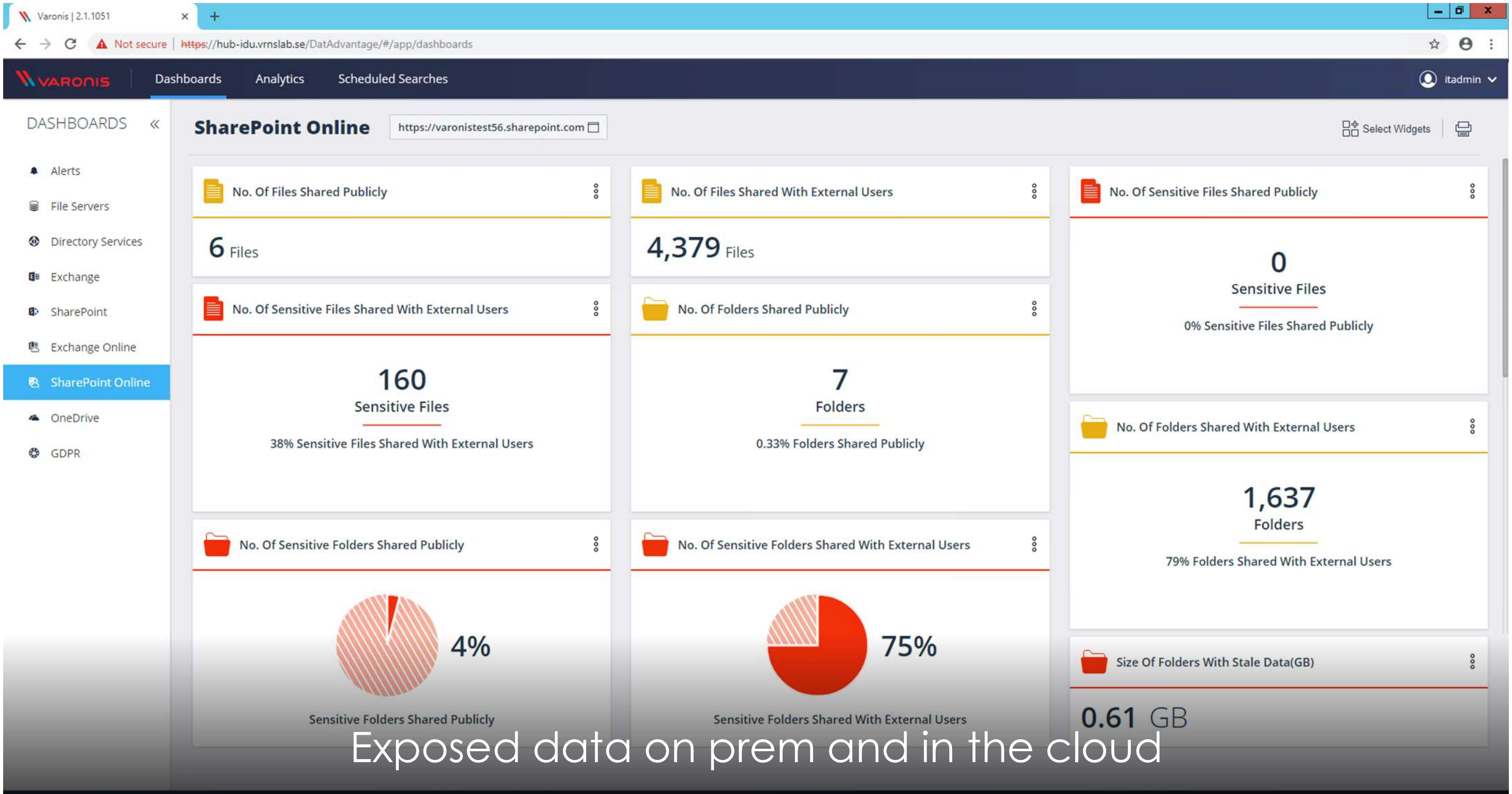
17M

files are open to **every employee** on average

of users have **passwords** that **never expire**

Read the full study: https://www.varonis.com/2019-data-risk-report

VARONIS



SharePoint Online https://varonistest56.sharepoint.com

No. Of Files Shared Publicly: 6 Files

No. Of Files Shared With External Users: 4,379 Files

No. Of Sensitive Files Shared Publicly: 0 Sensitive Files — 0% Sensitive Files Shared Publicly

No. Of Sensitive Files Shared With External Users: 160 Sensitive Files — 38% Sensitive Files Shared With External Users

No. Of Folders Shared Publicly: 7 Folders — 0.33% Folders Shared Publicly

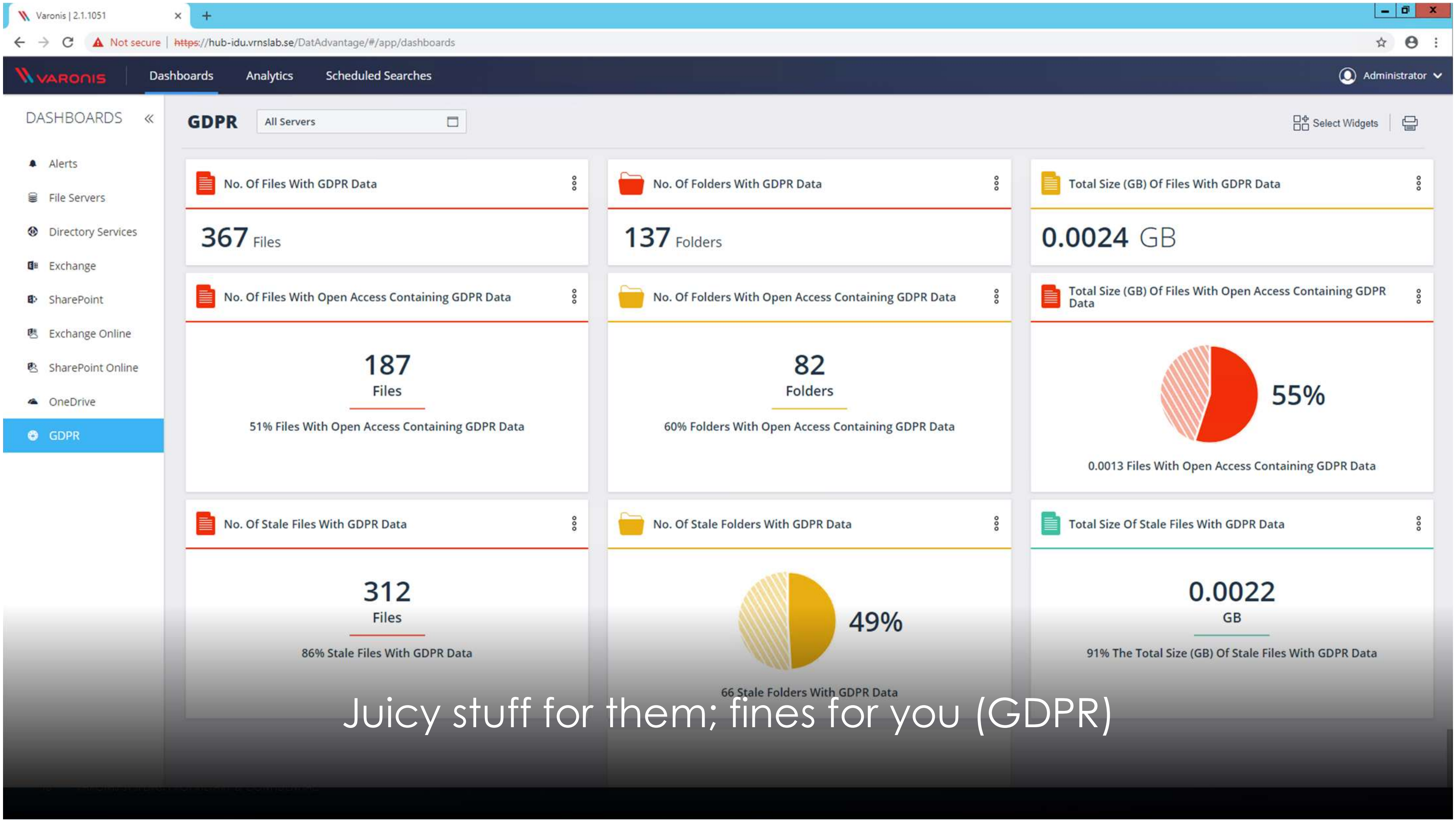
No. Of Folders Shared With External Users: 1,637 Folders — 79% Folders Shared With External Users

No. Of Sensitive Folders Shared Publicly: 4% Sensitive Folders Shared Publicly

No. Of Sensitive Folders Shared With External Users: 75% Sensitive Folders Shared With External Users

Size Of Folders With Stale Data(GB): 0.61 GB

Exposed data on prem and in the cloud



GDPR

No. Of Files With GDPR Data
367 Files

No. Of Folders With GDPR Data
137 Folders

Total Size (GB) Of Files With GDPR Data
0.0024 GB

No. Of Files With Open Access Containing GDPR Data
187 Files
51% Files With Open Access Containing GDPR Data

No. Of Folders With Open Access Containing GDPR Data
82 Folders
60% Folders With Open Access Containing GDPR Data

Total Size (GB) Of Files With Open Access Containing GDPR Data
55%
0.0013 Files With Open Access Containing GDPR Data

No. Of Stale Files With GDPR Data
312 Files
86% Stale Files With GDPR Data

No. Of Stale Folders With GDPR Data
49%
66 Stale Folders With GDPR Data

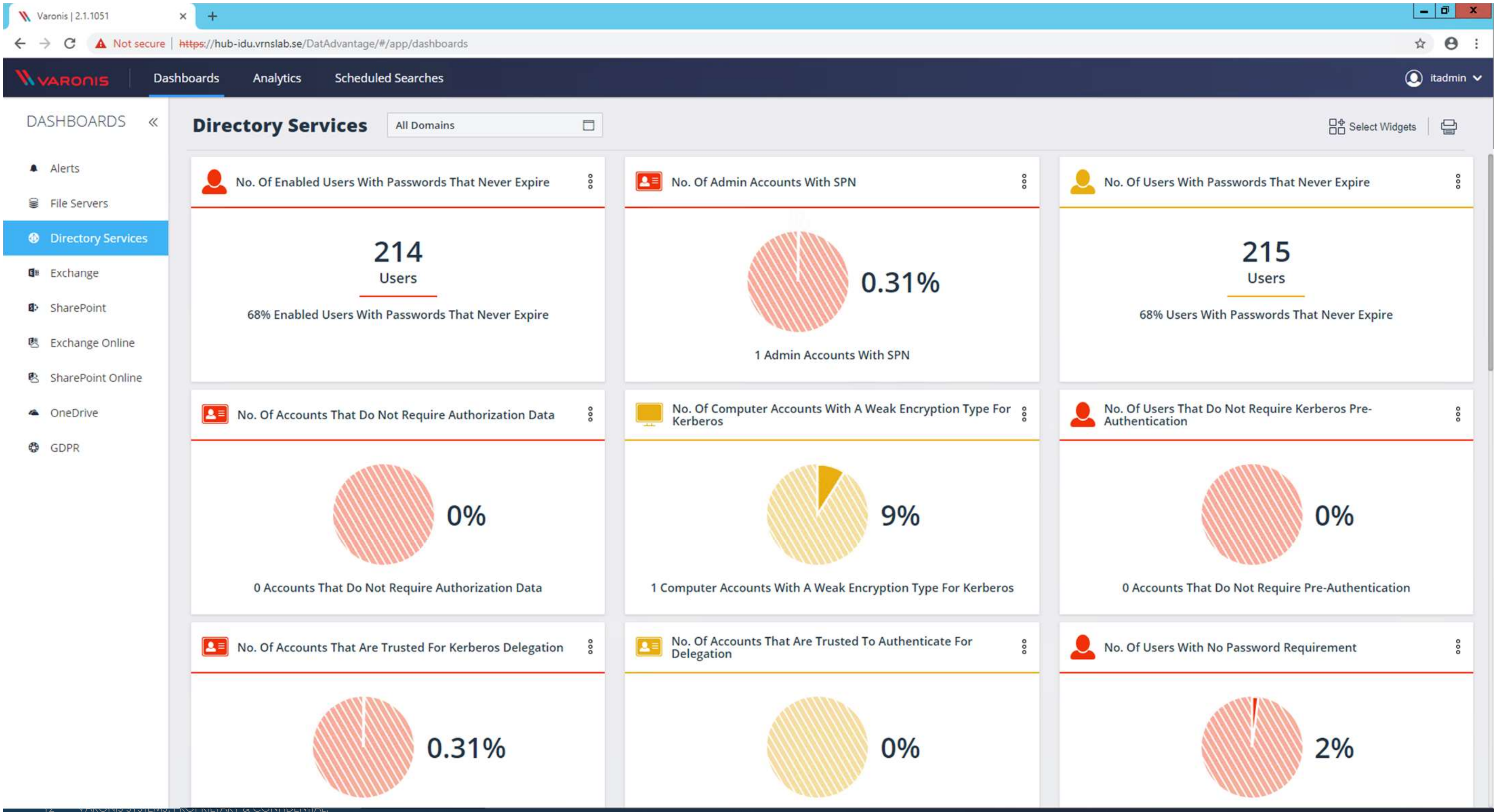
Total Size Of Stale Files With GDPR Data
0.0022 GB
91% The Total Size (GB) Of Stale Files With GDPR Data

Juicy stuff for them; fines for you (GDPR)

USER CONTINUALLY IS GETTING LOCKED OUT OF HER ACTIVE DIRECTORY ACCOUNT
FINALLY FOUND THE CAUSE AFTER 3 DAYS
made on imgur

AD is complex, and almost endlessly configurable.

Plus lots of AD vulnerabilities to help me



Directory Services

No. Of Enabled Users With Passwords That Never Expire

214
Users

68% Enabled Users With Passwords That Never Expire

No. Of Admin Accounts With SPN

0.31%

1 Admin Accounts With SPN

No. Of Users With Passwords That Never Expire

215
Users

68% Users With Passwords That Never Expire

No. Of Accounts That Do Not Require Authorization Data

0%

0 Accounts That Do Not Require Authorization Data

No. Of Computer Accounts With A Weak Encryption Type For Kerberos

9%

1 Computer Accounts With A Weak Encryption Type For Kerberos

No. Of Users That Do Not Require Kerberos Pre-Authentication

0%

0 Accounts That Do Not Require Pre-Authentication

No. Of Accounts That Are Trusted For Kerberos Delegation

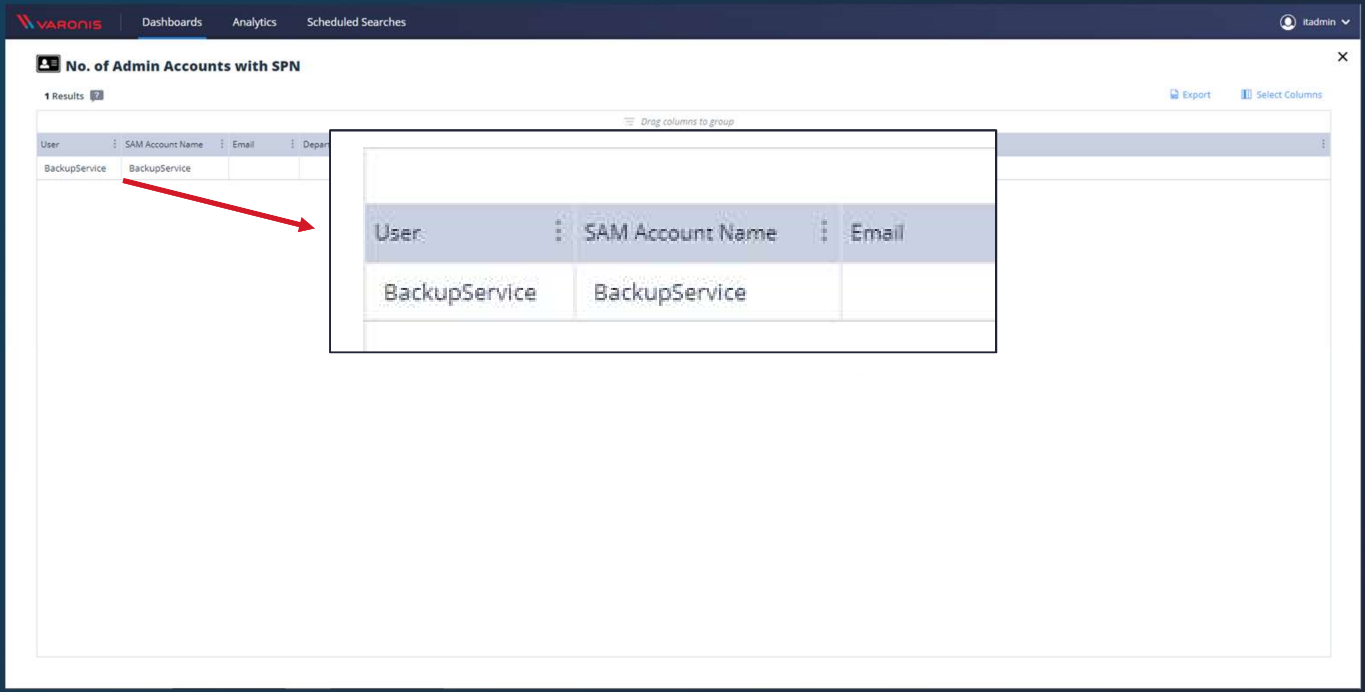
0.31%

No. Of Accounts That Are Trusted To Authenticate For Delegation

0%

No. Of Users With No Password Requirement

2%



No. of Admin Accounts with SPN

1 Results

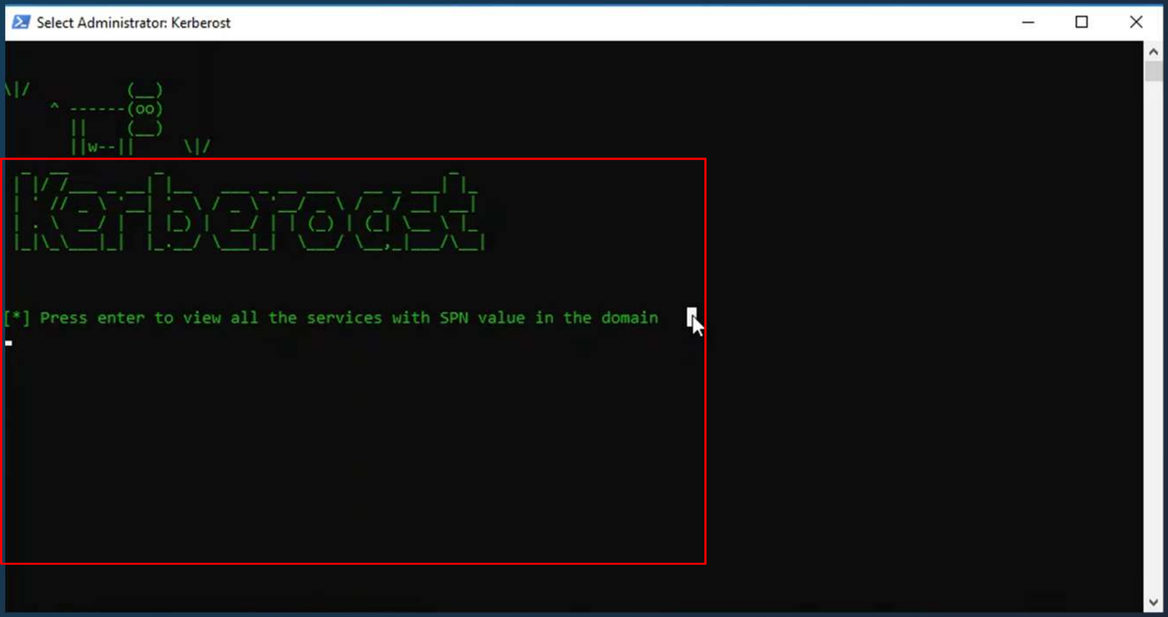
User	SAM Account Name	Email	Depar
BackupService	BackupService		

User	SAM Account Name	Email
BackupService	BackupService	

Here’s an attack we detected recently

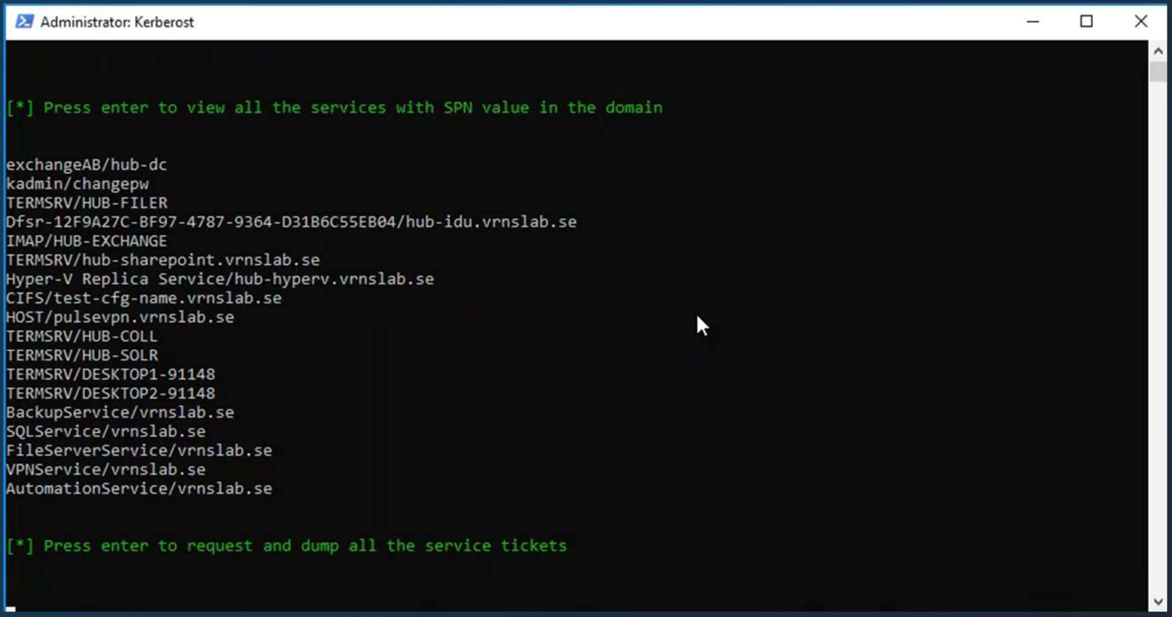
- A savvy engineer decides to monetize corporate secrets
- Compromises a service account with Domain Admin (Kerberoasting)
- Uses personal workstation crack the account’s password
- With privileged service account, user scans file shares for confidential files
- ZIPs the files and exfiltrates via personal Gmail account

Attackers might be exploiting these right now. Let’s see how.



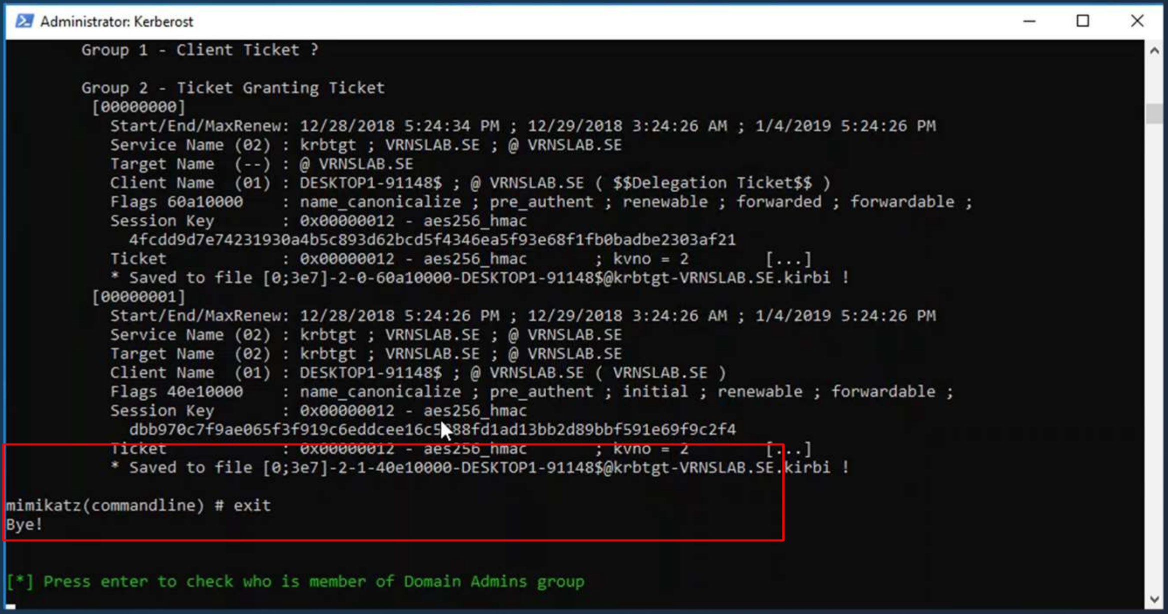
```
[*] Press enter to view all the services with SPN value in the domain
```

Step 1: find accounts with Service Principal Names



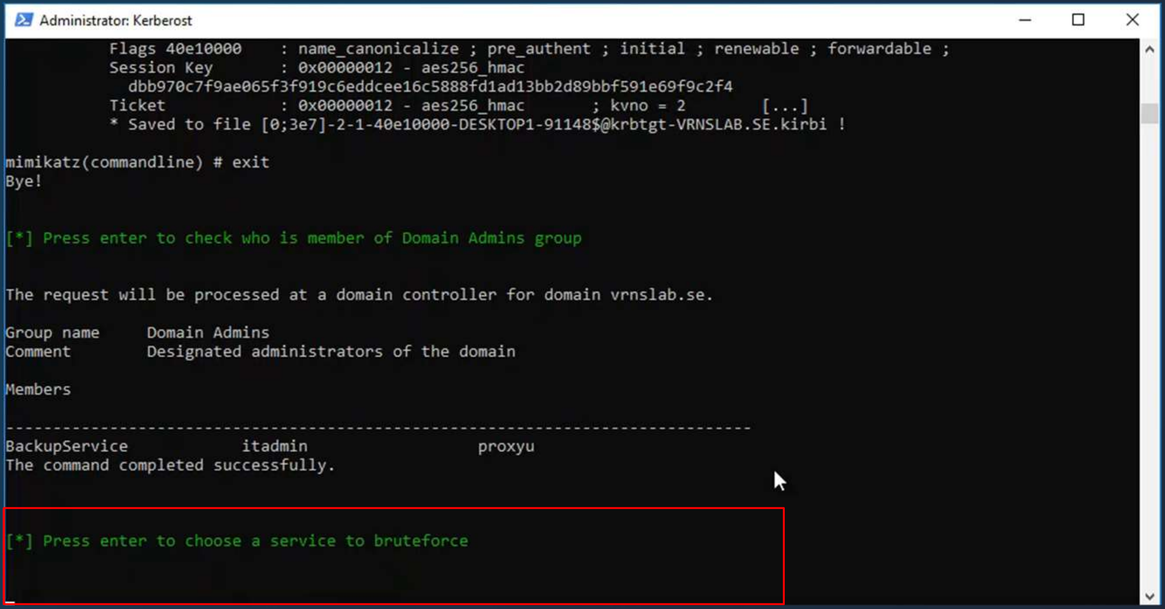
```
[*] Press enter to view all the services with SPN value in the domain


exchangeAB/hub-dc
kadmin/changepw
TERMSRV/HUB-FILER
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/hub-idu.vrnslab.se
IMAP/HUB-EXCHANGE
TERMSRV/hub-sharepoint.vrnslab.se
Hyper-V Replica Service/hub-hyperv.vrnslab.se
CIFS/test-cfg-name.vrnslab.se
HOST/pulsevpn.vrnslab.se
TERMSRV/HUB-COLL
TERMSRV/HUB-SOLR
TERMSRV/DESKTOP1-91148
TERMSRV/DESKTOP2-91148
BackupService/vrnslab.se
SQLService/vrnslab.se
FileServerService/vrnslab.se
VPNService/vrnslab.se
AutomationService/vrnslab.se


[*] Press enter to request and dump all the service tickets
```

Step 2: Get their Kerberos tickets (requesting weak encryption)



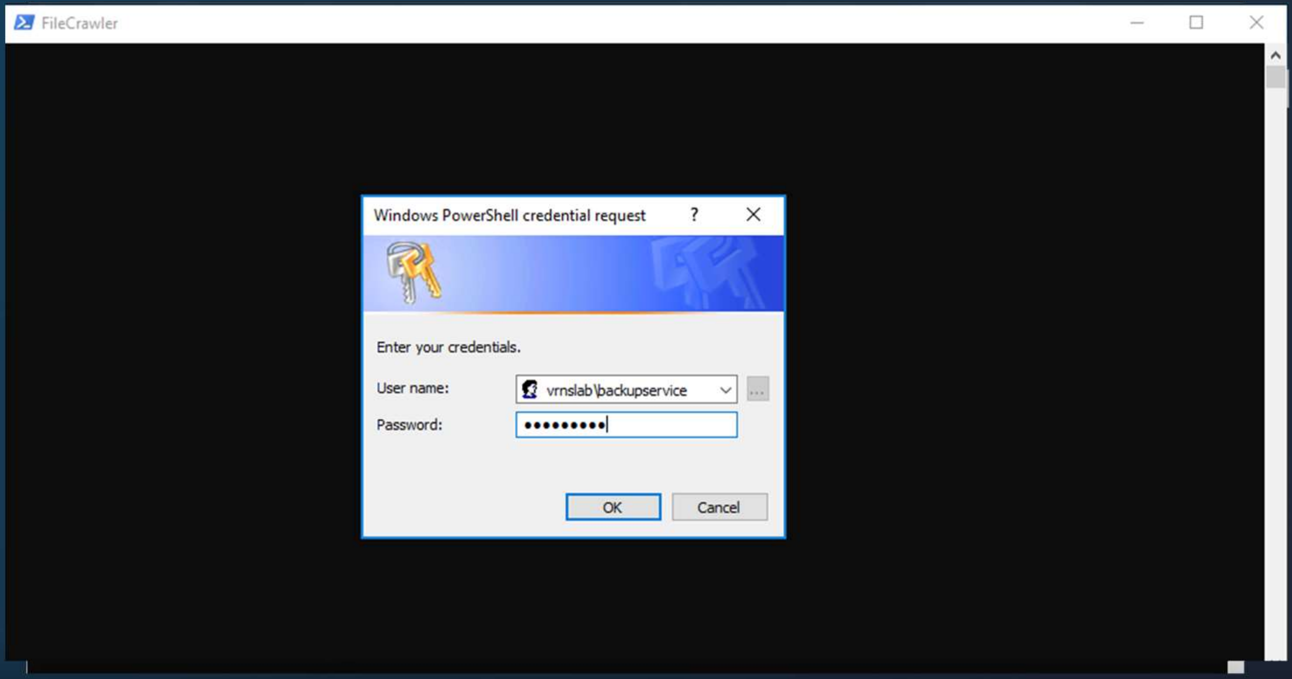
```
        Group 1 - Client Ticket ?

        Group 2 - Ticket Granting Ticket
         [00000000]
           Start/End/MaxRenew: 12/28/2018 5:24:34 PM ; 12/29/2018 3:24:26 AM ; 1/4/2019 5:24:26 PM
           Service Name (02) : krbtgt ; VRNSLAB.SE ; @ VRNSLAB.SE
           Target Name  (--) : @ VRNSLAB.SE
           Client Name  (01) : DESKTOP1-91148$ ; @ VRNSLAB.SE ( $$Delegation Ticket$$ )
           Flags 60a10000    : name_canonicalize ; pre_authent ; renewable ; forwarded ; forwardable ;
           Session Key       : 0x00000012 - aes256_hmac
             4fcdd9d7e74231930a4b5c893d62bcd5f4346ea5f93e68f1fb0badbe2303af21
           Ticket            : 0x00000012 - aes256_hmac       ; kvno = 2        [...]
           * Saved to file [0;3e7]-2-0-60a10000-DESKTOP1-91148$@krbtgt-VRNSLAB.SE.kirbi !
         [00000001]
           Start/End/MaxRenew: 12/28/2018 5:24:26 PM ; 12/29/2018 3:24:26 AM ; 1/4/2019 5:24:26 PM
           Service Name (02) : krbtgt ; VRNSLAB.SE ; @ VRNSLAB.SE
           Target Name  (02) : krbtgt ; VRNSLAB.SE ; @ VRNSLAB.SE
           Client Name  (01) : DESKTOP1-91148$ ; @ VRNSLAB.SE ( VRNSLAB.SE )
           Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
           Session Key       : 0x00000012 - aes256_hmac
             dbb970c7f9ae065f3f919c6eddcee16c5[illegible]88fd1ad13bb2d89bbf591e69f9c2f4
           Ticket            : 0x00000012 - aes256_hmac       ; kvno = 2        [...]
           * Saved to file [0;3e7]-2-1-40e10000-DESKTOP1-91148$@krbtgt-VRNSLAB.SE.kirbi !

mimikatz(commandline) # exit
Bye!


[*] Press enter to check who is member of Domain Admins group
```

Step 3: Which these accounts have elevated privileges?



```
          Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
          Session Key       : 0x00000012 - aes256_hmac
            dbb970c7f9ae065f3f919c6eddcee16c5888fd1ad13bb2d89bbf591e69f9c2f4
          Ticket            : 0x00000012 - aes256_hmac       ; kvno = 2        [...]
          * Saved to file [0;3e7]-2-1-40e10000-DESKTOP1-91148$@krbtgt-VRNSLAB.SE.kirbi !

mimikatz(commandline) # exit
Bye!


[*] Press enter to check who is member of Domain Admins group


The request will be processed at a domain controller for domain vrnslab.se.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
BackupService            itadmin                  proxyu
The command completed successfully.



[*] Press enter to choose a service to bruteforce


_
```

Step 4: Let’s crack one (offline)

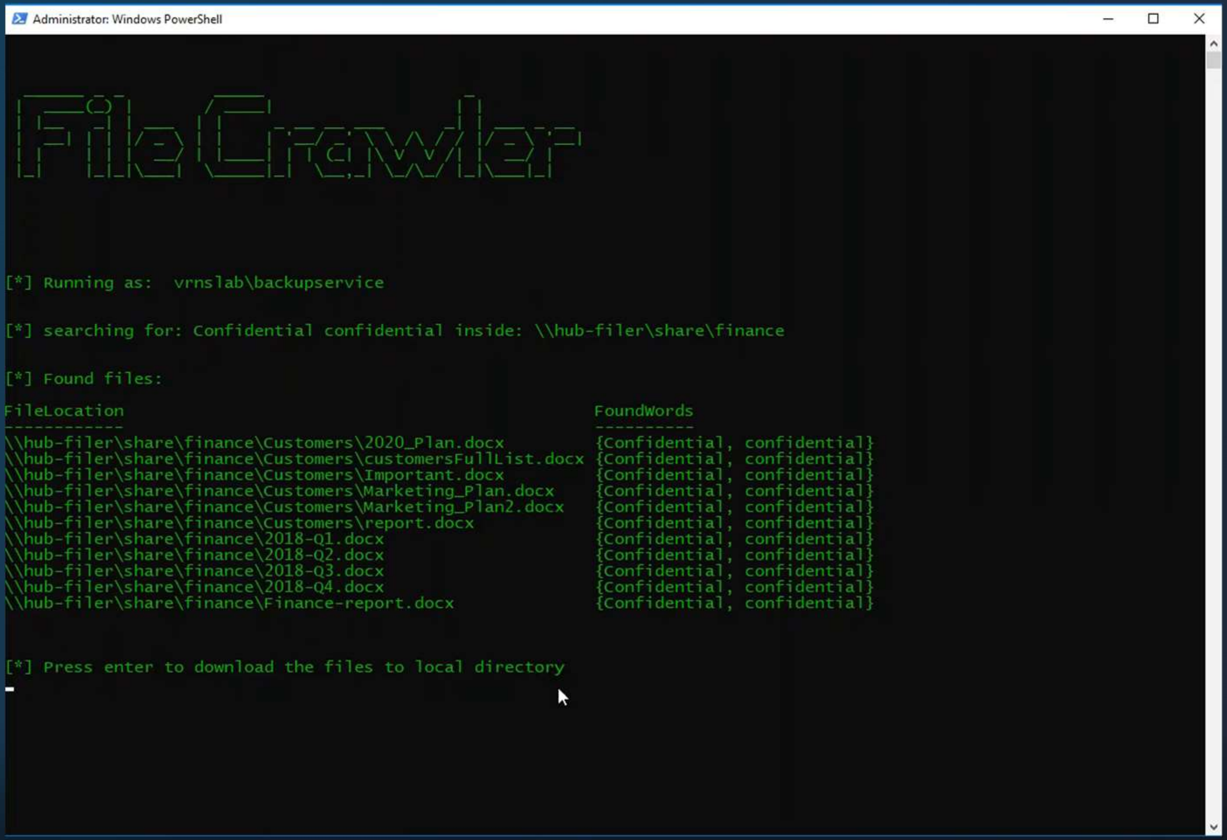


Enter your credentials.

User name: vrnslab\backupservice

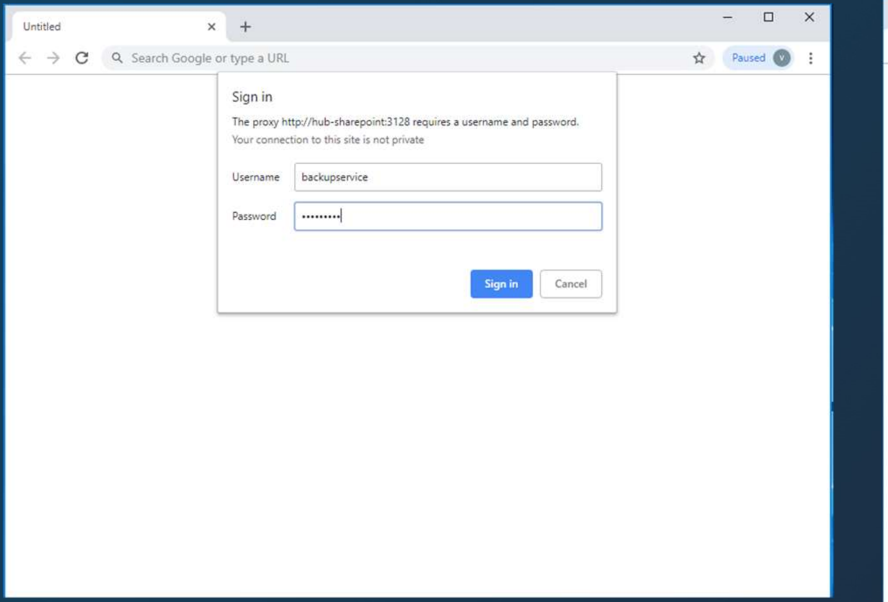
Password: ●●●●●●●●●

Step 5: Let’s use our new account to find some files



```
[*] Running as:  vrnslab\backupservice


[*] searching for: Confidential confidential inside: \\hub-filer\share\finance


[*] Found files:

FileLocation                                               FoundWords
------------                                               ----------
\\hub-filer\share\finance\Customers\2020_Plan.docx         {Confidential, confidential}
\\hub-filer\share\finance\Customers\customersFullList.docx {Confidential, confidential}
\\hub-filer\share\finance\Customers\Important.docx         {Confidential, confidential}
\\hub-filer\share\finance\Customers\Marketing_Plan.docx    {Confidential, confidential}
\\hub-filer\share\finance\Customers\Marketing_Plan2.docx   {Confidential, confidential}
\\hub-filer\share\finance\Customers\report.docx            {Confidential, confidential}
\\hub-filer\share\finance\2018-Q1.docx                     {Confidential, confidential}
\\hub-filer\share\finance\2018-Q2.docx                     {Confidential, confidential}
\\hub-filer\share\finance\2018-Q3.docx                     {Confidential, confidential}
\\hub-filer\share\finance\2018-Q4.docx                     {Confidential, confidential}
\\hub-filer\share\finance\Finance-report.docx              {Confidential, confidential}



[*] Press enter to download the files to local directory
```

Step 6: Put them in a zip file



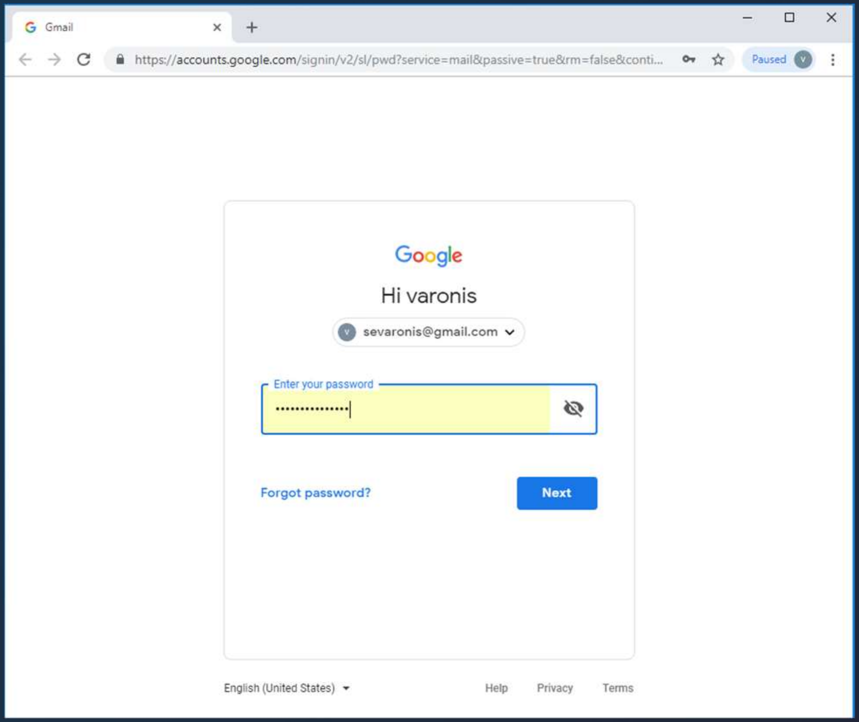
Sign in

The proxy http://hub-sharepoint:3128 requires a username and password.

Your connection to this site is not private

Username: backupservice

Password: •••••••••



https://accounts.google.com/signin/v2/sl/pwd?service=mail&passive=true&rm=false&conti...

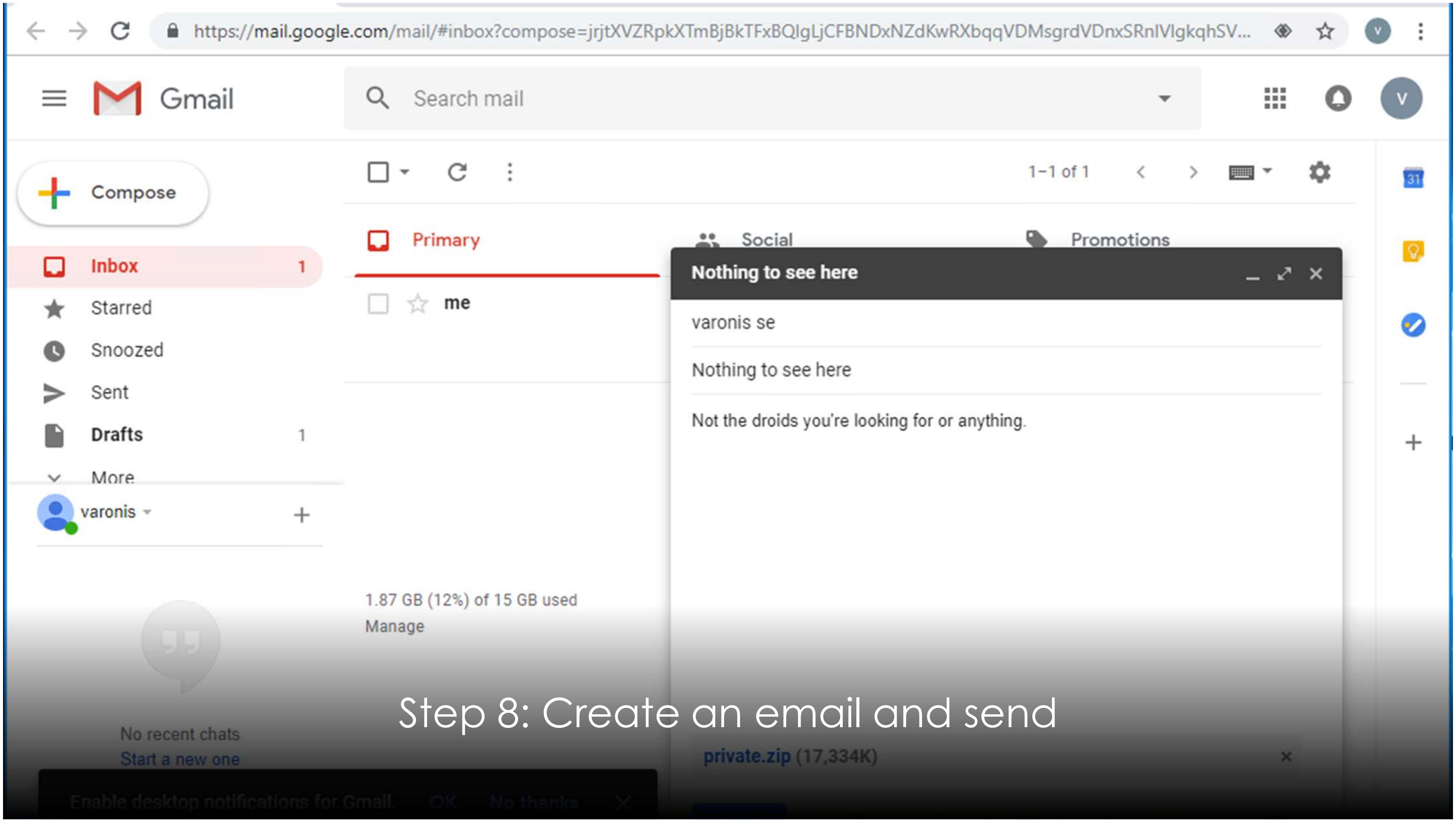
Google

Hi varonis

sevaronis@gmail.com

Enter your password: •••••••••••••••

Step 7: Use Service Account to login to web proxy and Gmail



https://mail.google.com/mail/#inbox?compose=jrjtXVZRpkXTmBjBkTFxBQlgLjCFBNDxNZdKwRXbqqVDMsgrdVDnxSRnlVlgkqhSV...

Nothing to see here

varonis se

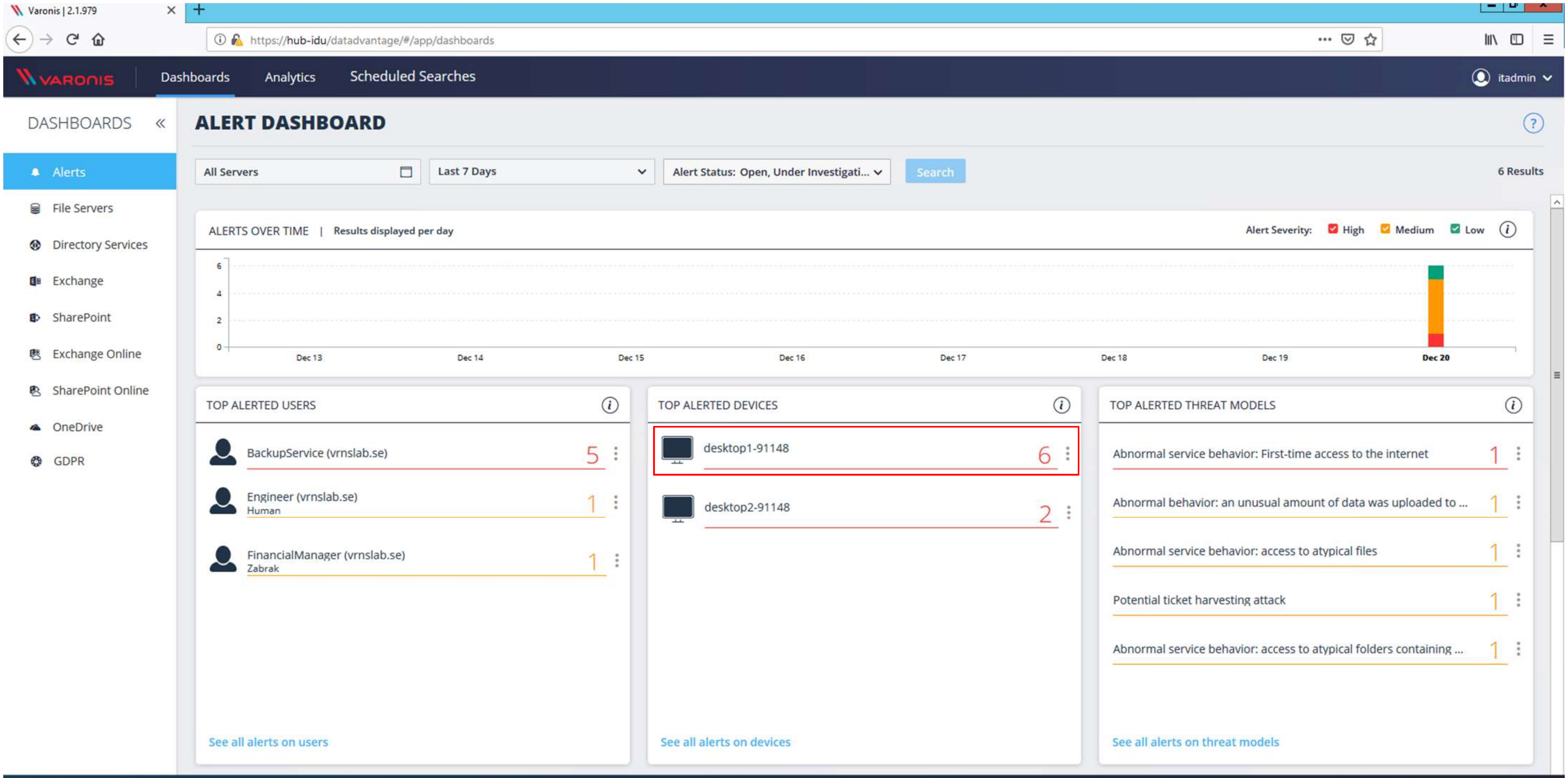
Nothing to see here

Not the droids you're looking for or anything.

private.zip (17,334K)

Step 8: Create an email and send

Oh no…



ALERT DASHBOARD

All Servers | Last 7 Days | Alert Status: Open, Under Investigati...

6 Results

ALERTS OVER TIME | Results displayed per day

TOP ALERTED USERS

BackupService (vrnslab.se)	5
Engineer (vrnslab.se) Human	1
FinancialManager (vrnslab.se) Zabrak	1

See all alerts on users

TOP ALERTED DEVICES

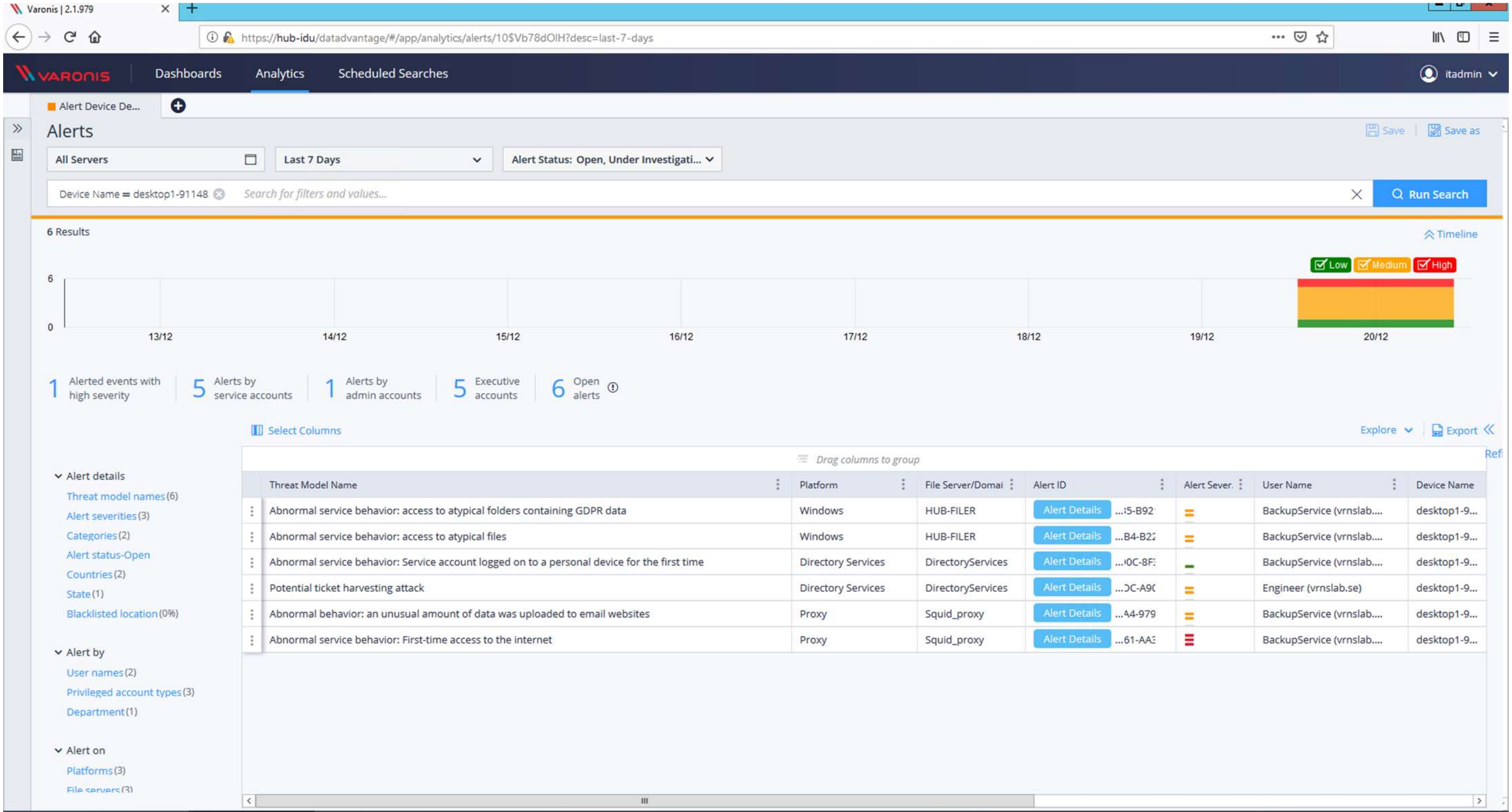
desktop1-91148	6
desktop2-91148	2

See all alerts on devices

TOP ALERTED THREAT MODELS

Abnormal service behavior: First-time access to the internet	1
Abnormal behavior: an unusual amount of data was uploaded to ...	1
Abnormal service behavior: access to atypical files	1
Potential ticket harvesting attack	1
Abnormal service behavior: access to atypical folders containing ...	1

See all alerts on threat models



Alerts

All Servers

Last 7 Days

Alert Status: Open, Under Investigati...

Device Name = desktop1-91148

Search for filters and values...

6 Results

1 Alerted events with high severity

5 Alerts by service accounts

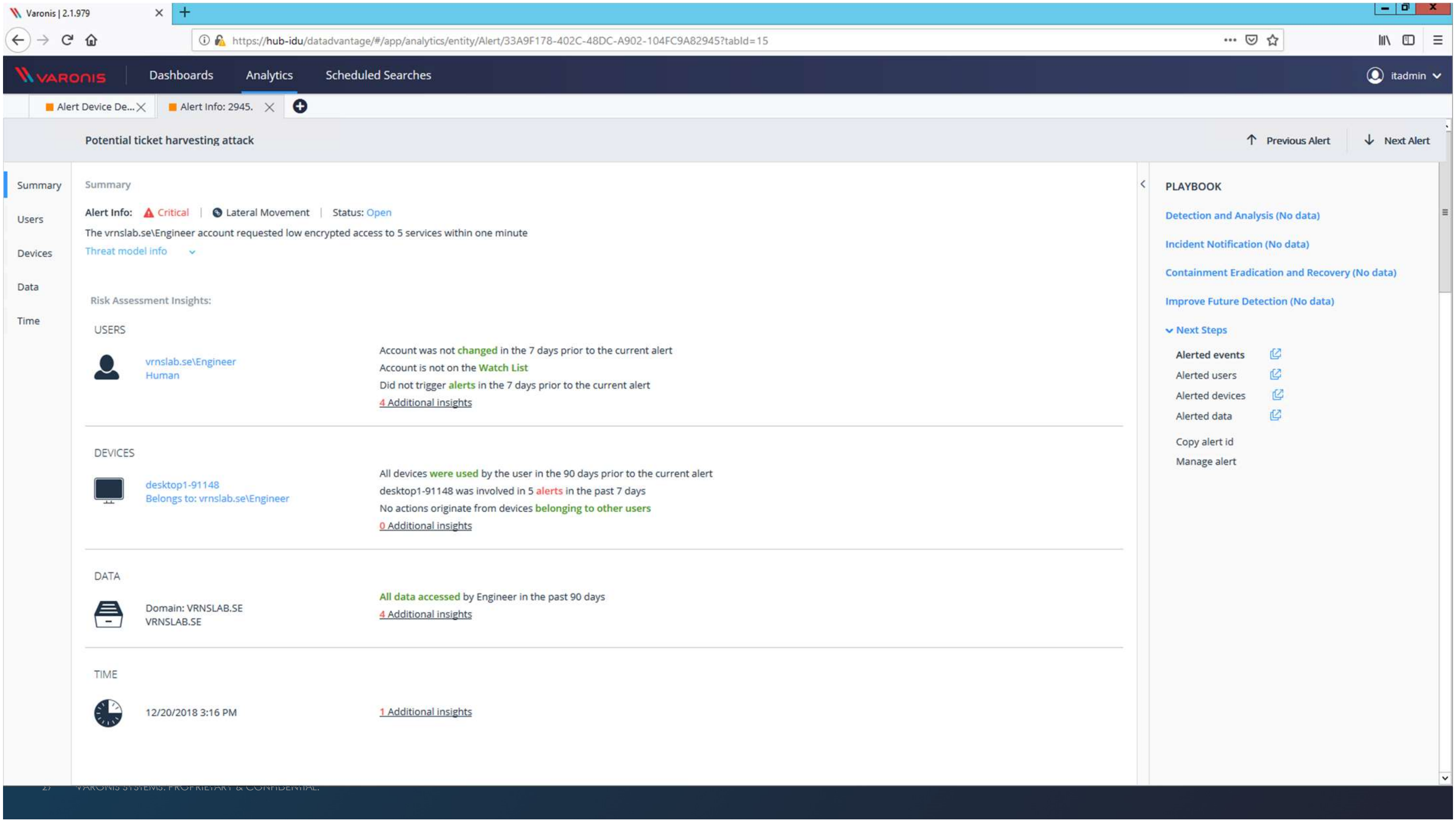
1 Alerts by admin accounts

5 Executive accounts

6 Open alerts

- Alert details
  - Threat model names (6)
  - Alert severities (3)
  - Categories (2)
  - Alert status-Open
  - Countries (2)
  - State (1)
  - Blacklisted location (0%)
- Alert by
  - User names (2)
  - Privileged account types (3)
  - Department (1)
- Alert on
  - Platforms (3)
  - File servers (3)

Threat Model Name	Platform	File Server/Domai	Alert ID	Alert Sever.	User Name	Device Name
Abnormal service behavior: access to atypical folders containing GDPR data	Windows	HUB-FILER	Alert Details ...I5-B92	=	BackupService (vrnslab....	desktop1-9...
Abnormal service behavior: access to atypical files	Windows	HUB-FILER	Alert Details ...B4-B2	=	BackupService (vrnslab....	desktop1-9...
Abnormal service behavior: Service account logged on to a personal device for the first time	Directory Services	DirectoryServices	Alert Details ...0C-8F	—	BackupService (vrnslab....	desktop1-9...
Potential ticket harvesting attack	Directory Services	DirectoryServices	Alert Details ...DC-A9	=	Engineer (vrnslab.se)	desktop1-9...
Abnormal behavior: an unusual amount of data was uploaded to email websites	Proxy	Squid_proxy	Alert Details ...A4-979	=	BackupService (vrnslab....	desktop1-9...
Abnormal service behavior: First-time access to the internet	Proxy	Squid_proxy	Alert Details ...61-AA	≡	BackupService (vrnslab....	desktop1-9...



Potential ticket harvesting attack

Summary

Alert Info: Critical | Lateral Movement | Status: Open

The vrnslab.se\Engineer account requested low encrypted access to 5 services within one minute

Threat model info

Risk Assessment Insights:

USERS

vrnslab.se\Engineer
Human

Account was not changed in the 7 days prior to the current alert
Account is not on the Watch List
Did not trigger alerts in the 7 days prior to the current alert
4 Additional insights

DEVICES

desktop1-91148
Belongs to: vrnslab.se\Engineer

All devices were used by the user in the 90 days prior to the current alert
desktop1-91148 was involved in 5 alerts in the past 7 days
No actions originate from devices belonging to other users
0 Additional insights

DATA

Domain: VRNSLAB.SE
VRNSLAB.SE

All data accessed by Engineer in the past 90 days
4 Additional insights

TIME

12/20/2018 3:16 PM

1 Additional insights

PLAYBOOK

Detection and Analysis (No data)

Incident Notification (No data)

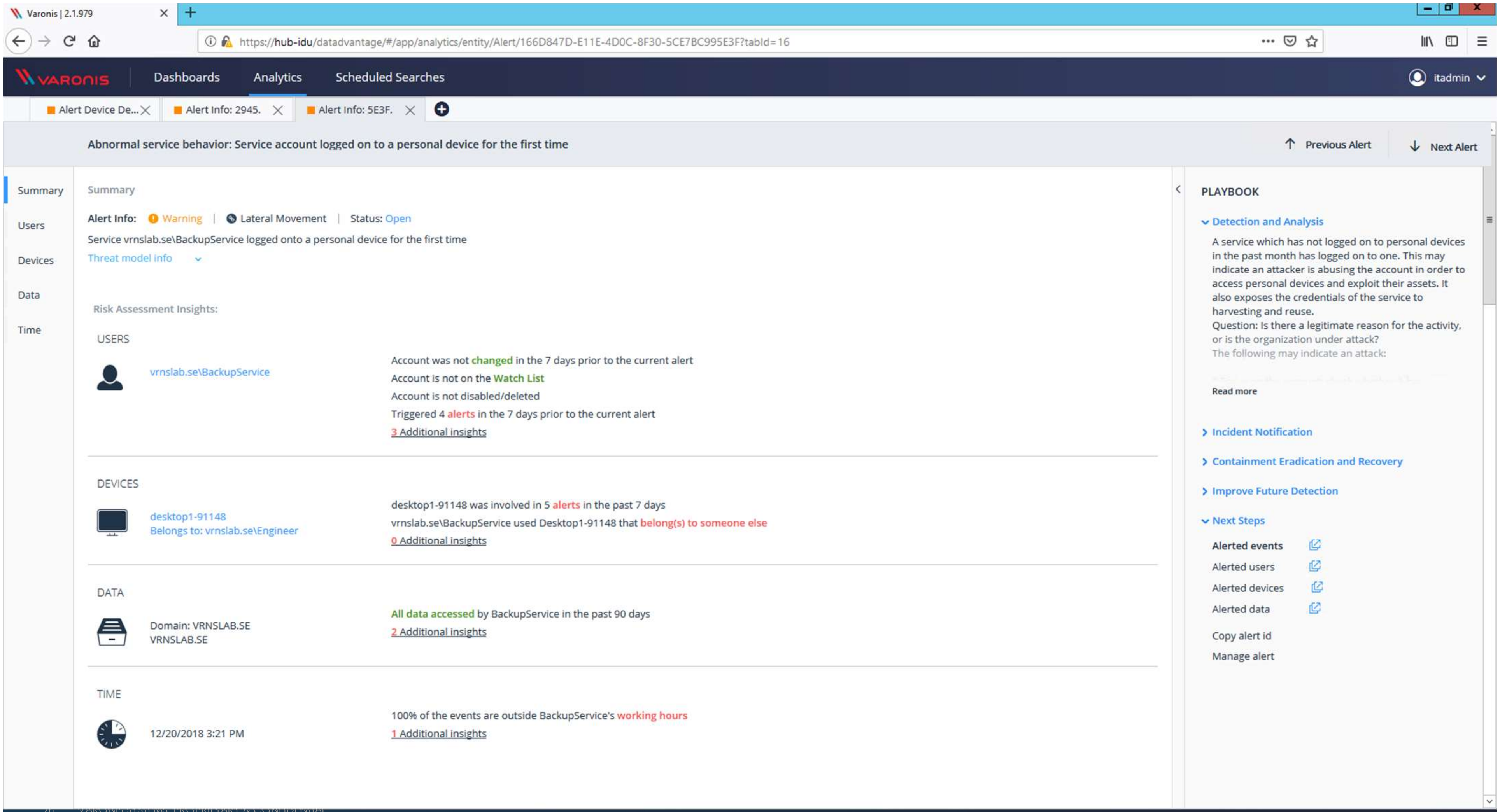
Containment Eradication and Recovery (No data)

Improve Future Detection (No data)

Next Steps

Alerted events
Alerted users
Alerted devices
Alerted data

Copy alert id
Manage alert



Abnormal service behavior: Service account logged on to a personal device for the first time

Summary

Alert Info: Warning | Lateral Movement | Status: Open

Service vrnslab.se\BackupService logged onto a personal device for the first time

Threat model info

Risk Assessment Insights:

USERS

vrnslab.se\BackupService

Account was not changed in the 7 days prior to the current alert
Account is not on the Watch List
Account is not disabled/deleted
Triggered 4 alerts in the 7 days prior to the current alert
3 Additional insights

DEVICES

desktop1-91148
Belongs to: vrnslab.se\Engineer

desktop1-91148 was involved in 5 alerts in the past 7 days
vrnslab.se\BackupService used Desktop1-91148 that belong(s) to someone else
0 Additional insights

DATA

Domain: VRNSLAB.SE
VRNSLAB.SE

All data accessed by BackupService in the past 90 days
2 Additional insights

TIME

12/20/2018 3:21 PM

100% of the events are outside BackupService's working hours
1 Additional insights

PLAYBOOK

Detection and Analysis

A service which has not logged on to personal devices in the past month has logged on to one. This may indicate an attacker is abusing the account in order to access personal devices and exploit their assets. It also exposes the credentials of the service to harvesting and reuse.
Question: Is there a legitimate reason for the activity, or is the organization under attack?
The following may indicate an attack:

Read more

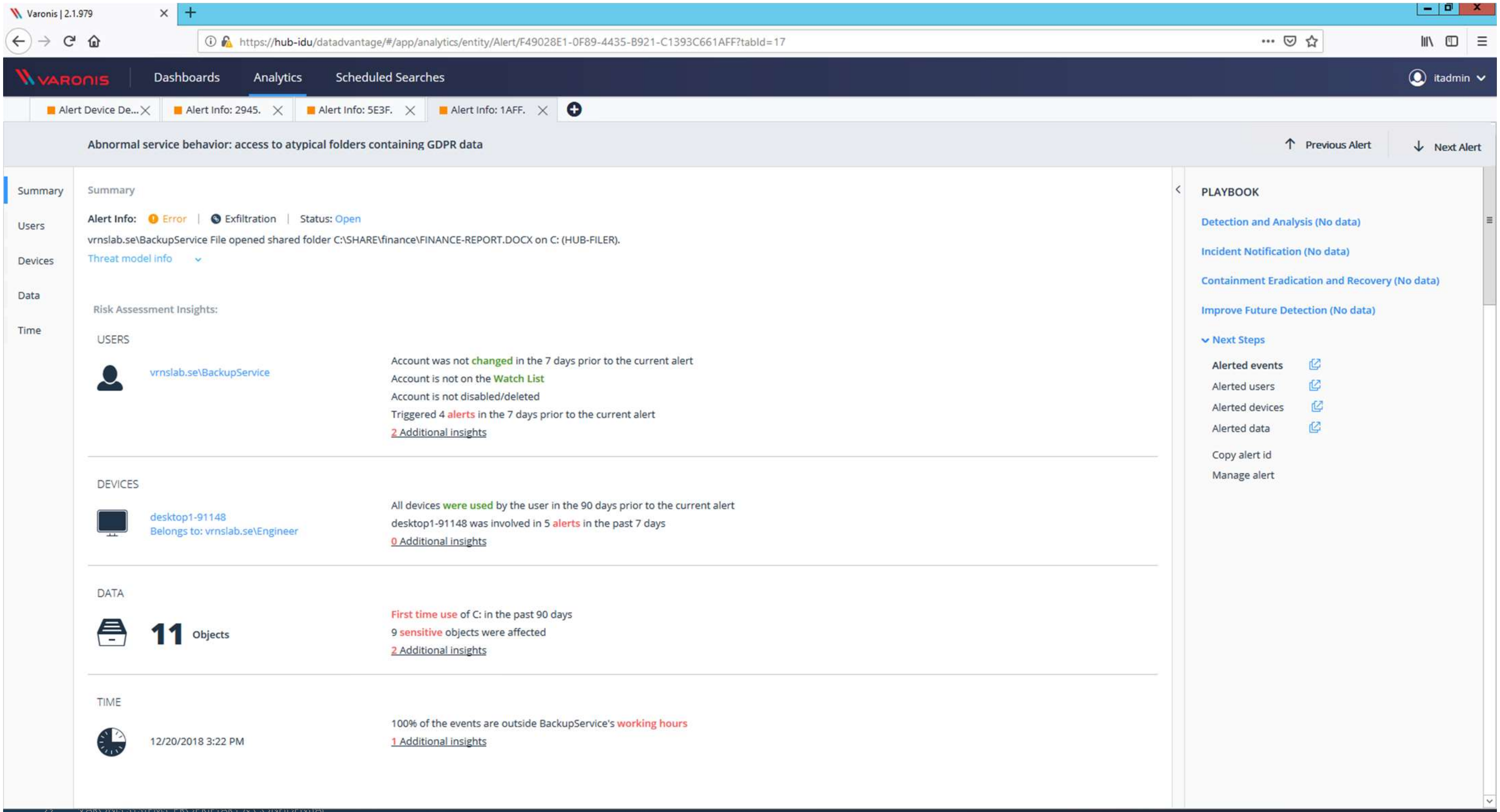
Incident Notification

Containment Eradication and Recovery

Improve Future Detection

Next Steps

Alerted events
Alerted users
Alerted devices
Alerted data
Copy alert id
Manage alert



Abnormal service behavior: access to atypical folders containing GDPR data

Summary

Alert Info: Error | Exfiltration | Status: Open

vrnslab.se\BackupService File opened shared folder C:\SHARE\finance\FINANCE-REPORT.DOCX on C: (HUB-FILER).

Threat model info

Risk Assessment Insights:

USERS

vrnslab.se\BackupService

Account was not changed in the 7 days prior to the current alert
Account is not on the Watch List
Account is not disabled/deleted
Triggered 4 alerts in the 7 days prior to the current alert
2 Additional insights

DEVICES

desktop1-91148
Belongs to: vrnslab.se\Engineer

All devices were used by the user in the 90 days prior to the current alert
desktop1-91148 was involved in 5 alerts in the past 7 days
0 Additional insights

DATA

11 Objects

First time use of C: in the past 90 days
9 sensitive objects were affected
2 Additional insights

TIME

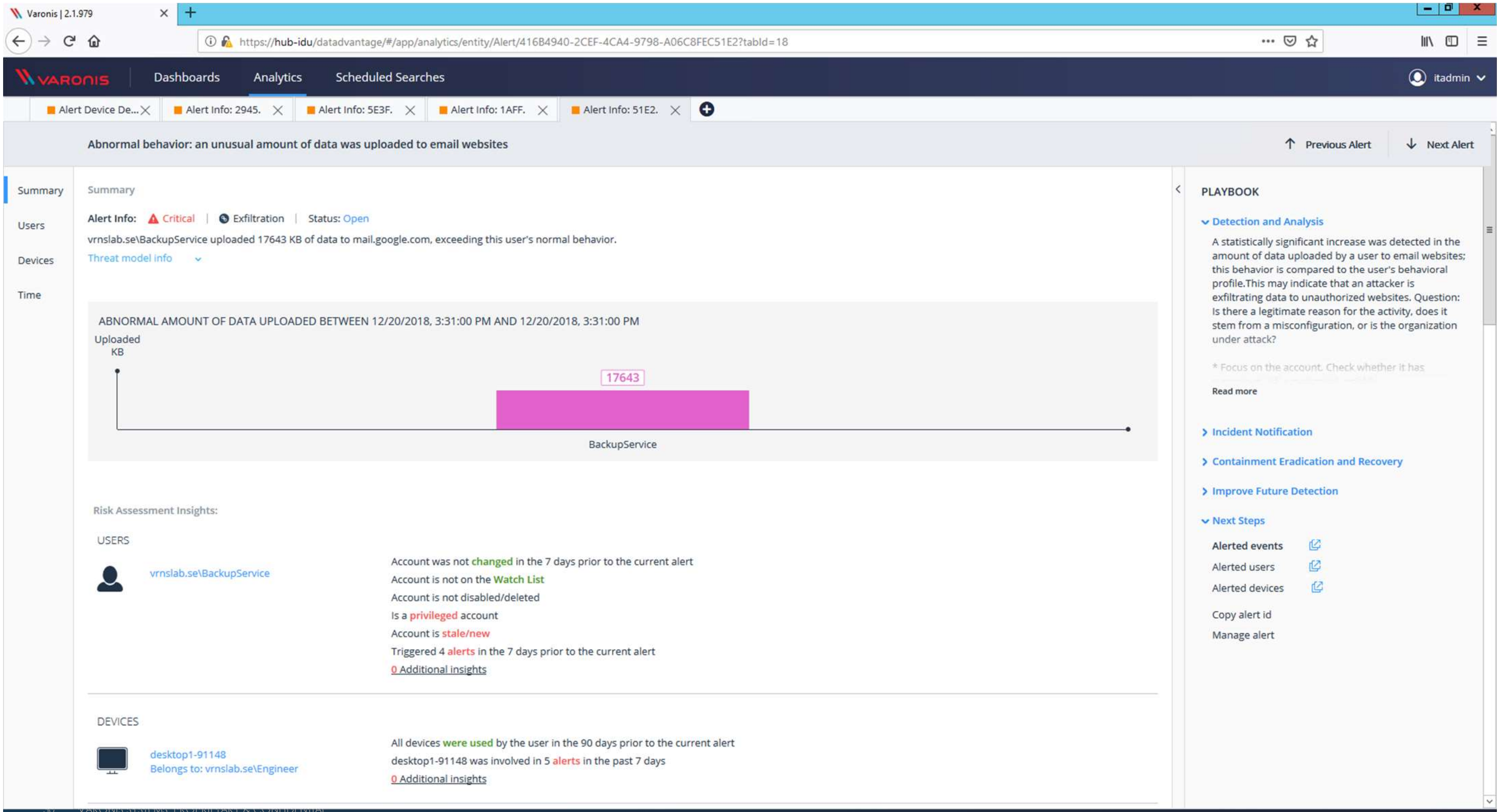
12/20/2018 3:22 PM

100% of the events are outside BackupService's working hours
1 Additional insights

PLAYBOOK

Detection and Analysis (No data)
Incident Notification (No data)
Containment Eradication and Recovery (No data)
Improve Future Detection (No data)

Next Steps
Alerted events
Alerted users
Alerted devices
Alerted data
Copy alert id
Manage alert



Abnormal behavior: an unusual amount of data was uploaded to email websites

Summary

Alert Info: Critical | Exfiltration | Status: Open

vrnslab.se\BackupService uploaded 17643 KB of data to mail.google.com, exceeding this user's normal behavior.

Threat model info

ABNORMAL AMOUNT OF DATA UPLOADED BETWEEN 12/20/2018, 3:31:00 PM AND 12/20/2018, 3:31:00 PM

Risk Assessment Insights:

USERS

vrnslab.se\BackupService

Account was not changed in the 7 days prior to the current alert
Account is not on the Watch List
Account is not disabled/deleted
Is a privileged account
Account is stale/new
Triggered 4 alerts in the 7 days prior to the current alert
0 Additional insights

DEVICES

desktop1-91148
Belongs to: vrnslab.se\Engineer

All devices were used by the user in the 90 days prior to the current alert
desktop1-91148 was involved in 5 alerts in the past 7 days
0 Additional insights

PLAYBOOK

Detection and Analysis

A statistically significant increase was detected in the amount of data uploaded by a user to email websites; this behavior is compared to the user's behavioral profile.This may indicate that an attacker is exfiltrating data to unauthorized websites. Question: Is there a legitimate reason for the activity, does it stem from a misconfiguration, or is the organization under attack?

* Focus on the account. Check whether it has

Read more

Incident Notification

Containment Eradication and Recovery

Improve Future Detection

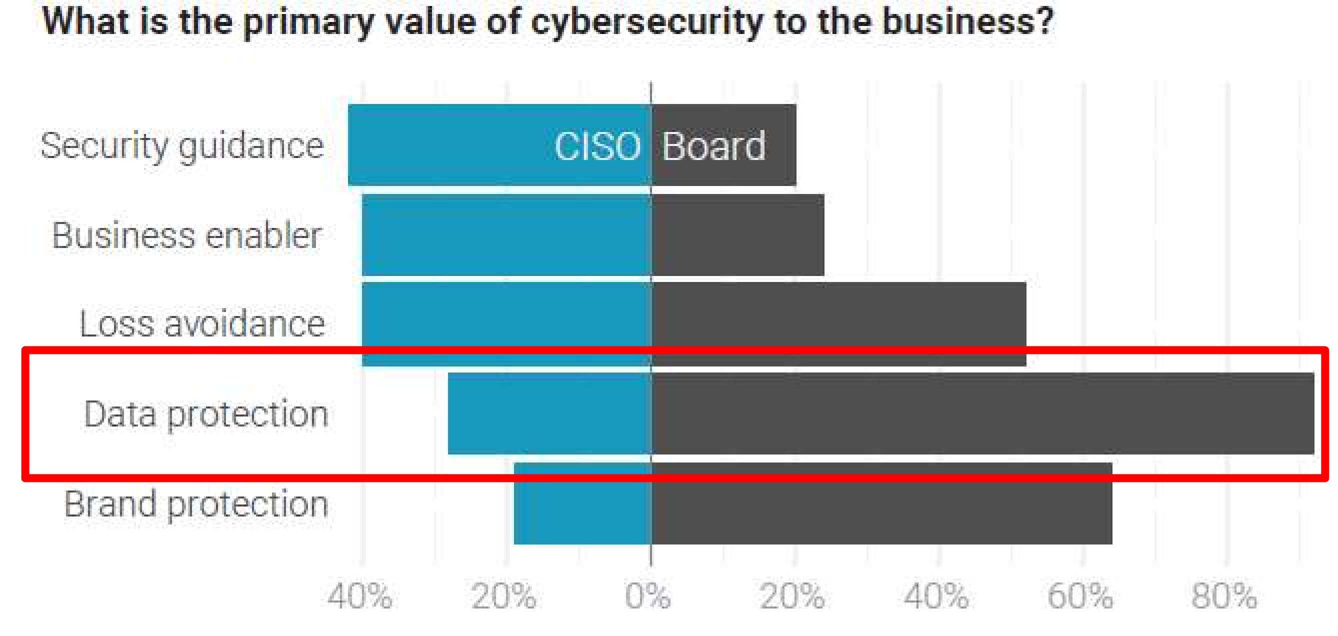
Next Steps

- Alerted events
- Alerted users
- Alerted devices
- Copy alert id
- Manage alert

How quickly & accurately can you answer the most important question:

“Is our **data** safe?”

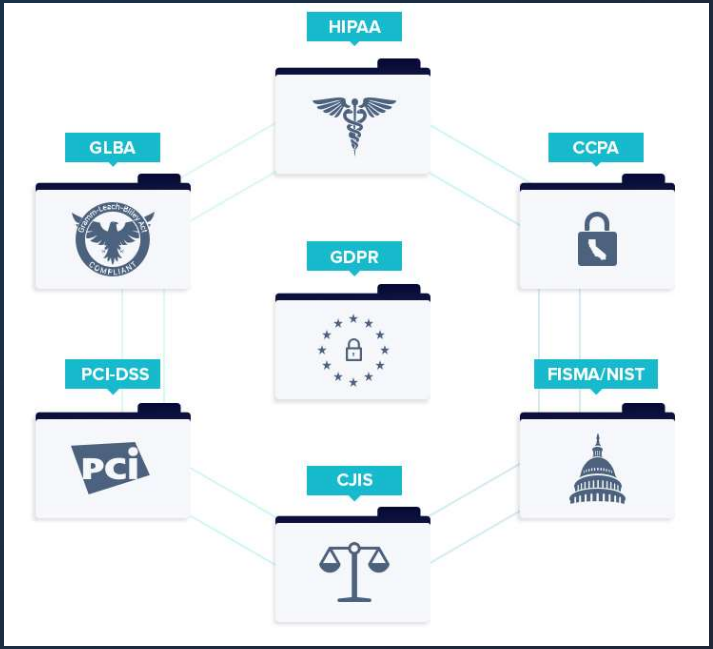
The CISO / Board Disconnect



Source: Source: The Cyber Balance Sheet, Cyentia Institute

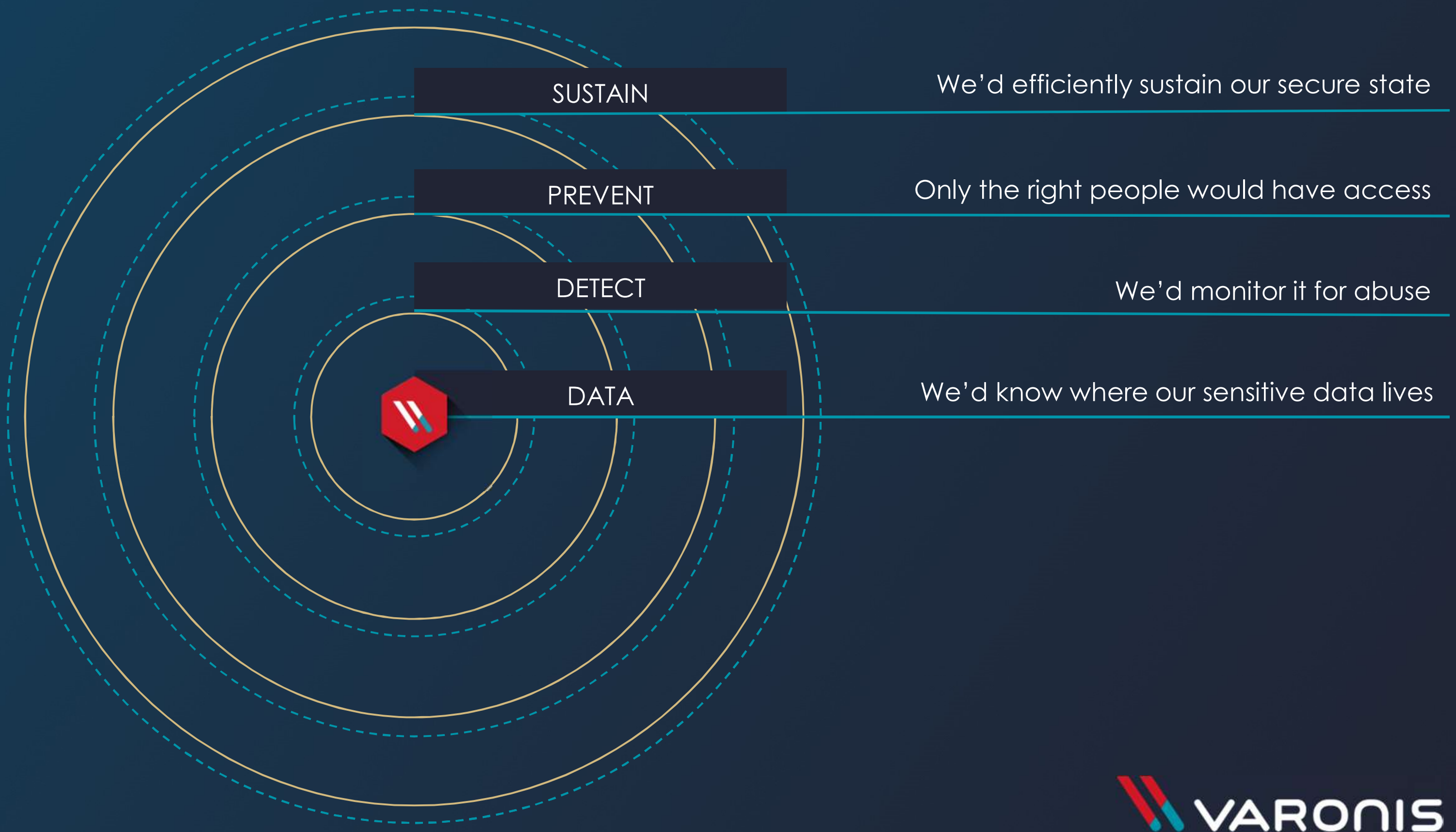
Modern regulations are **data-centric**

- Where is your regulated data located?
- Is any of that data exposed and at-risk?
- Do only the right people have access?
- How is regulated data being processed?
- Can you find and delete personal data?



VARONIS

What if security started with data?



SUSTAIN — We’d efficiently sustain our secure state

PREVENT — Only the right people would have access

DETECT — We’d monitor it for abuse

DATA — We’d know where our sensitive data lives

For many data stores…

Windows

Office 365

Unix/Linux

SharePoint

Exchange

NAS

Box

Many questions

Is my data at risk?

- Is it locked down?
- Who is accessing it?
- Who does it belong to?

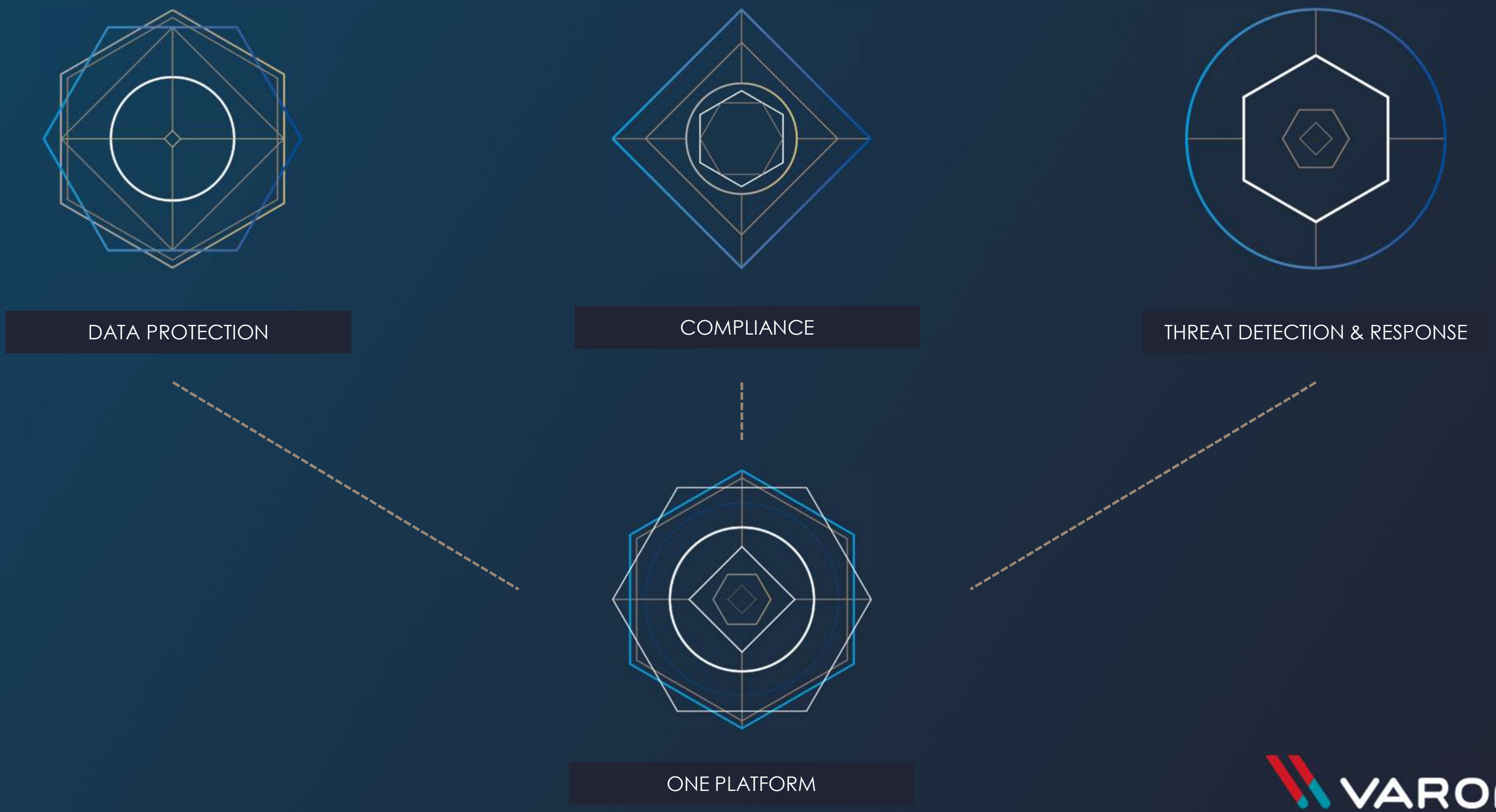
Am I compliant?

- Where is my regulated and sensitive data?
- Can I delete it?
- Can I prove compliance?

Can I detect a breach?

- Is anyone stealing it?
- From where?
- Can I investigate quickly?

THREE USE CASES



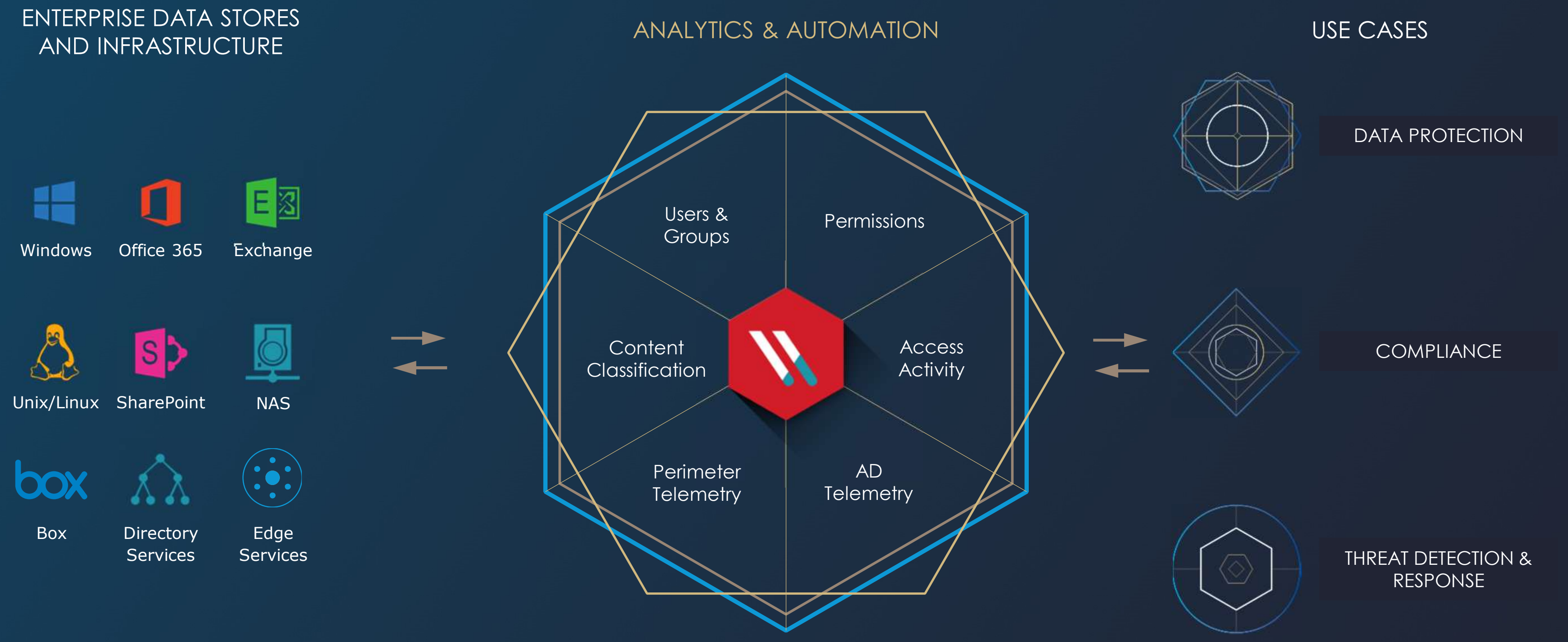
DATA PROTECTION

COMPLIANCE

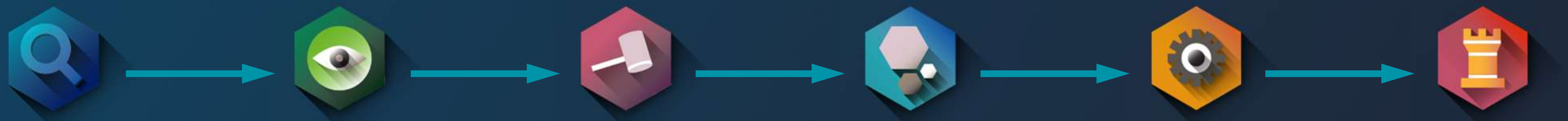
THREAT DETECTION & RESPONSE

ONE PLATFORM

Varonis Data Security Platform



Varonis Operational Journey



DEPLOY

- Deploy Varonis
- Discover privileged accounts
- Classify sensitive data
- Baseline activity
- Prioritise risk

OPERATIONALISE

- Enable alerts and automate response
- Connect to SIEM
- Create and test incident response plans
- Operationalize reporting
- Apply labels
- Index for compliance

FIX

- Remediate exposed sensitive data
- Eliminate remaining global access groups
- Eliminate AD artifacts
- Quarantine sensitive data
- Archive/delete stale data

TRANSFORM

- Identify and assign data owners
- Simplify permissions structure
- Enable data-driven reporting

AUTOMATE

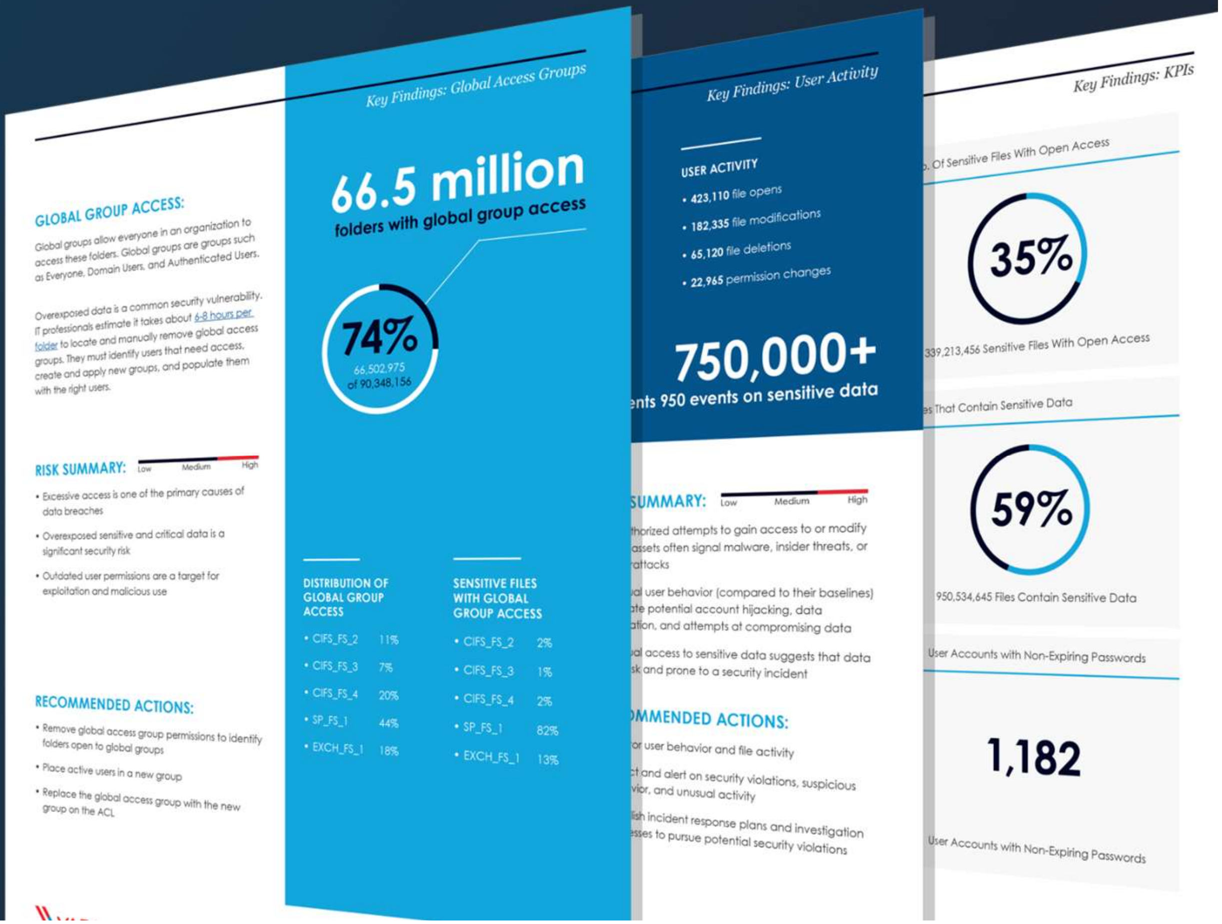
- Automate authorisation workflow via Data Owners
- Automate periodic entitlement reviews
- Automate disposition, quarantining, policy enforcement

IMPROVE

- Regularly review risks, alerts and processes to ensure continuous improvement

Risk Assessments Reduce Uncertainty

- What kind of sensitive data do I have?
- Where is sensitive data overexposed?
- Where are users acting strangely or maliciously?
- What's being used and what's not?



GLOBAL GROUP ACCESS:

Global groups allow everyone in an organization to access these folders. Global groups are groups such as Everyone, Domain Users, and Authenticated Users.

Overexposed data is a common security vulnerability. IT professionals estimate it takes about 6-8 hours per folder to locate and manually remove global access groups. They must identify users that need access, create and apply new groups, and populate them with the right users.

RISK SUMMARY: Low Medium High

- Excessive access is one of the primary causes of data breaches
- Overexposed sensitive and critical data is a significant security risk
- Outdated user permissions are a target for exploitation and malicious use

RECOMMENDED ACTIONS:

- Remove global access group permissions to identify folders open to global groups
- Place active users in a new group
- Replace the global access group with the new group on the ACL

Key Findings: Global Access Groups

66.5 million folders with global group access

74% 66,502,975 of 90,348,156

DISTRIBUTION OF GLOBAL GROUP ACCESS	
• CIFS_FS_2	11%
• CIFS_FS_3	7%
• CIFS_FS_4	20%
• SP_FS_1	44%
• EXCH_FS_1	18%

SENSITIVE FILES WITH GLOBAL GROUP ACCESS	
• CIFS_FS_2	2%
• CIFS_FS_3	1%
• CIFS_FS_4	2%
• SP_FS_1	82%
• EXCH_FS_1	13%

Key Findings: User Activity

USER ACTIVITY

- 423,110 file opens
- 182,335 file modifications
- 65,120 file deletions
- 22,965 permission changes

750,000+

ents 950 events on sensitive data

SUMMARY: Low Medium High

thorized attempts to gain access to or modify assets often signal malware, insider threats, or attacks

al user behavior (compared to their baselines) ate potential account hijacking, data ation, and attempts at compromising data

al access to sensitive data suggests that data sk and prone to a security incident

MMENDED ACTIONS:

or user behavior and file activity

ct and alert on security violations, suspicious vior, and unusual activity

ish incident response plans and investigation esses to pursue potential security violations

Key Findings: KPIs

. Of Sensitive Files With Open Access

35%

339,213,456 Sensitive Files With Open Access

es That Contain Sensitive Data

59%

950,534,645 Files Contain Sensitive Data

User Accounts with Non-Expiring Passwords

1,182

User Accounts with Non-Expiring Passwords

Thank You

Matt Lock
mlock@varonis.com
+44 7795 153 900