VARONIS
DATALERT

VARONIS DATALERT

70% of companies find out about breaches through their customers and third parties.

MANY ORGANIZATIONS HAVE NO WAY TO DETECT WHEN:

- Sensitive files are accessed or deleted
- Security groups, GPOs, and other Active Directory objects are modified or removed
- Unwarranted privilege escalations occur
- Permissions on sensitive directories are modified

To answer these questions requires continuous and non-intrusive auditing of every single access event on your network.

Improve your ability to detect possible security breaches, misconfigurations, and other issues with Varonis DatAlert. Varonis DatAlert provides real-time alerting based on file activity, Active Directory changes, permissions changes, and other events.

Alert criteria and output are easily configurable so that the right people and systems can be notified about the right things, at the right times in the right ways.

COMMMON USE CASES:

- Monitor sensitive configuration files on Windows and UNIX/Linux servers
- Detect changes made outside of change control windows
- Alert on access to highly sensitive data
- Alert on privilege escalations
- Automatically disable user access based on the number of events that occur within a given time period by setting thresholds

RECEIVE IMMEDIATE NOTIFICATIONS ON:

- Files accessed, modified, and/or deleted
- Group membership, group policy and other Active Directory changes
- Permissions changes

GET ALERTS THE WAY YOU WANT THEM:

- Syslog, Event Log, SNMP, Email
- Trigger command line execution
- Easily integrate with SIEM and network management solutions
- Generate alerts based on event thresholds

WHAT EVENTS CAN DATALERT TELL YOU ABOUT IN REAL-TIME?

Below is a summary of many of the events that DatAlert can trigger real-time alerts on. For a complete list, along with compatibility across supported platforms and versions, visit: http://www.varonis.com/products/datalert

Many of the events below can be used in conjunction with our data classification results, so you can alert on, for instance, access to or deletion of sensitive content.

CIFS AND NFS EVENTS

- File Create
- File Delete
- File Open
- File Rename
- File Modify
- File Set Permissions
- Directory Create
- Directory Delete

- Directory Rename
- Directory Set Permissions
- Access Denied - File Open
- Access Denied - File Delete
- Access Denied - File Set Permissions
- Access Denied - Directory Delete
- Access Denied - Directory Set Permissions

Supported CIFS and NFS platforms include Windows, NetApp, EMC VNX/Celerra, HP IBRIX, Hitachi NAS, UNIX, Linux, Solaris, AIX.

SHAREPOINT EVENTS

- File Create
- File Delete
- File Open
- File Rename
- File Modify
- File Set Security

- Directory Create
- Directory Delete
- Directory Rename
- Directory Set Security
- Role Set
- Site Create

- List Item Create
- List Item Delete
- List Item Open
- List Item Rename
- List Item Modify

EXCHANGE EVENTS

- Open Folder
- Create Folder
- Delete Folder
- Rename Folder
- Add Folder Permissions
- Remove Folder Permissions
- Change Folder Permissions
- Move Folder
- Empty Folder
- Copy Folder
- Mark All as Read
- Send Message

- Send Message (On behalf of X)
- Send Message (As X)
- Message received
- Edit Message
- Delete Message
- Copy Message
- Move Message
- Create Message
- Message Marked as Unread
- Message Marked as Read
- Logon

ACTIVE DIRECTORY EVENTS

- Creation and deletion of all objects
- Changes in group membership
- Changes in directory service object properties for any property
- Reset password
- Lock/unlock accounts
- Enable or disable account
- Group membership changes