DLP RUN BOOK

L1

Step 1:

Search for the user logs corresponding to the triggered alert.

Step 2:

If the event's risk score is elevated, proceed to retrieve the file onto your host system and initiate its opening.

Step 3:

Examine whether the file constitutes intellectual property owned by the organization and is not intended for external dissemination.

L2

Step 4:

Dispatch an email abstaining from divulging any details regarding the DLP incident.

Step 5:

Ask the user to join the call over team/zoom

Step 6:

Record the call and instruct the user to expunge all duplicates of the file.

Step 7:

Raise INC to GRC team attaching the video to the ticket

Step 8:

Close the INC and Alert