Politecnico di Torino

Corso di Laurea in Ingegneria Informatica
Tesi Magistrale
Anno Accademico 2021/2022

Scouting e Scelta di un Tool per il Mantenimento dell'Efficacia delle Regole per la Protezione di Proprietà Intellettuale

Relatore: Gianpiero Cabodi

Candidata: Claudia Scaletta

Correlatore: Emiliano Orrù

Sommario

Abstract

La protezione della proprietà intellettuale è un tema sempre più all'attenzione delle grandi aziende, in quanto permette la salvaguardia del proprio business.
Una possibile soluzione per affrontare questo problema è l'implementazione di una soluzione di Data Loss Prevention (DLP), che è in grado di limitare il rischio di potenziali violazioni e perdita di dati tramite la definizione di regole di Classificazione, che permettono di riconoscere e classificare i dati che contengono informazioni sensibili, e di Protezione, che permettono di monitorare ed eventualmente interrompere il flusso di dati per salvaguardare la proprietà intellettuale.
Un processo aziendale basato su una soluzione DLP permette di lavorare sull'identificazione dei dati sensibili e di applicare un insieme di regole di protezione che permettano di individuare i soli dati che potrebbero causare una fuoriuscita di dati.
Una soluzione Data Loss Prevention è però onerosa e complessa perché occorre definire e mantenere in perimetro le macchine e gli utenti ad esse associate che elaborano o accedono ai dati critici, intercettare in tempi ragionevoli nuove fonti di dati sensibili e verificare attraverso dei test che le regole di classificazione e protezione dei dati continuino ad essere efficaci anche in seguito al cambio delle condizioni al contorno (es. nuova release, nuovi casi d'uso).
Un corretto ciclo di vita delle regole dovrebbe quindi prevedere le seguenti fasi:

- uno studio approfondito delle fonti e delle possibili azioni che un utente può intraprendere per esportare la proprietà intellettuale;
- l'implementare delle regole di classificazione e di protezione dei dati sensibili, facendo attenzione che non impattino sull'operatività degli utenti;
- la verifica della loro efficacia anche in seguito al cambio delle condizioni al contorno, certificando che le regole continuino a funzionare in modo appropriato.

Obiettivo della tesi è lo scouting e la scelta di un tool esistente che permetta di verificare la correttezza delle regole implementate e il livello della loro efficacia al cambio delle condizioni al contorno, riducendo l'effort manuale che tali attività comportano.

Capitolo 1

1. Data Loss

In questo primo capitolo saranno introdotti i concetti fondamentali per il progetto di tesi. Verrà presentata una panoramica riguardo la gestione dei dati sensibili da parte delle organizzazioni con particolare focus sull'importanza della protezione della proprietà intellettuale descrivendo il concetto di Data Loss, le cause che possono portare alla fuga di informazioni sensibili e alla soluzione adottata.
Infine, sarà descritto il progetto di tesi e la struttura dei capitoli dell'elaborato finale.

1.1 Introduzione

In seguito all'aumento della raccolta dei dati da parte delle aziende e all'uso sempre più frequente di dispositivi e servizi online anche esterni all'IT aziendale, i dati sensibili sono facilmente scambiabili quindi esiste una maggior probabilità che si verifichi una perdita o una fuga di dati sensibili da parte dell'azienda, ossia un Data Loss.
I canali attraverso cui si manifesta più frequentemente un Data Loss sono molteplici, tra i più comuni troviamo il canale email e i dispositivi rimovibili come chiavette USB, hard-disk esterni o CD/DVD ma possono essere causati anche dalla presenza di virus o malware.
La causa principale della maggior parte delle perdite di dati è dovuta all'errore umano, questo accade in quanto gli esseri umani non sono perfetti e ogni giorno manipolano una grande quantità di dati che possono essere eliminati in maniera accidentale, sovrascritti o divulgati in maniera inconsapevole.
Un'altra delle cause principali è dovuta agli attacchi informatici e alla presenza di malware o virus che infettano il computer degli utenti e possono provocare furti ed eliminazione di file non protetti.
La protezione della proprietà intellettuale è un tema sempre più all'attenzione delle grandi aziende, in quanto permette la salvaguardia del proprio business, è nata quindi

l'esigenza di implementare una soluzione che sia in grado di limitare il rischio di potenziali Data Loss.
Una possibile soluzione per affrontare questo problema consiste nell'implementazione di una soluzione di Data Loss Prevention (DLP), cioè un sistema che ha l'obiettivo di proteggere i dati sensibili ed evitare che questi vengano persi o resi inaccessibili.
I processi DLP sono nati per andare incontro a piccole e grandi aziende e hanno come obiettivo quello di garantire un certo livello di sicurezza rispettando gli standard dettati dalla legge.
Un processo aziendale basato su una soluzione DLP permette di identificare i dati sensibili e monitorare le azioni svolte dagli utenti che manipolano questi dati al fine di evitare che ci sia una perdita di dati, questo avviene mediante la definizione di un insieme di regole di classificazione e di protezione.
Le regole di classificazione permettono di identificare i soli dati sensibili attraverso l'applicazione di un tag o un'etichetta di classificazione mentre le regole di protezione permettono di monitorare le azioni svolte dagli utenti che utilizzano i dati sensibili ed eventualmente bloccare l'azione svolta per evitare che ci sia una fuga o una perdita di dati sensibili.
Queste regole devono essere applicate a un perimetro ristretto di utenti e quindi a un numero ristretto di macchine, quelle che vengono utilizzate dai soli utenti che manipolano dati sensibili e non devono impattare negativamente sull'operatività degli utenti.
Per poter creare una regola consistente occorre inoltre che queste siano in grado di individuare nuove fonti di dati sensibili in tempi ragionevoli, che siano efficaci e che continuino a funzionare in modo appropriato anche in seguito al cambio delle condizioni, ad esempio in seguito ad una nuova release.

1.2 Data Loss: le cause

Un Data Loss è una perdita di dati sensibili da parte dell'azienda. Come anticipato l'utilizzo di una soluzione Data Loss Prevention permette di individuare i dati sensibili e bloccare le azioni dell'utente che possono provocare un Data Loss.
Per fare in modo che le azioni pericolose siano gestite secondo quanto concordato attraverso le linee guida dell'organizzazione o semplicemente bloccate occorre identificare i canali attraverso cui si manifesta più frequentemente il Data Loss e quindi la perdita o la fuga di dati all'interno di un'azienda, tra questi troviamo:

- Email: è il canale attraverso cui si manifesta con maggior frequenza la fuga di dati questo perché i dipendenti di un'azienda possono includere in maniera volontaria o involontaria, dei dati sensibili all'interno del corpo del messaggio da inviare o allegare documenti sensibili.

- Social engineering: prevede la partecipazione inconsapevole da parte dell'utente.
  È uno dei modi più semplici e allo stesso tempo più frequente ed efficace per sottrarre dati sensibili, si possono infatti sfruttare sia utenti ingenui che esperti.
  I canali attraverso cui carpire le informazioni utilizzate per accedere ai dati confidenziali sono molteplici: una conversazione, una lettera scritta, una mail o un profilo social.

- Dispositivi di memorizzazione rimovibili come chiavette USB, hard-disk esterni, CD e DVD.
  Questa tipologia di dispositivi può portare sia al furto di dati sensibili che alla perdita delle informazioni in quanto questi supporti possono essere infettati da Malware.

- Dispositivi mobili: con l'utilizzo di dispositivi come smartphone, tablet e laptop attraverso cui ci si può connettere a internet, alla posta elettronica, al cloud e ad applicazioni web, i dipendenti di un'azienda hanno la possibilità di lavorare anche al di fuori dell'ufficio e quindi di utilizzare questi dispositivi al di fuori dei locali aziendali sicuri aumentando la vulnerabilità al furto e la probabilità perdere dati.

- Applicazioni cloud: molte aziende hanno adottato l'utilizzo di applicazioni e servizi in cloud che permettono di lavorare al di fuori dell'ufficio e di avere i dati sempre a disposizione.
  Tra i rischi del cloud c'è la difficoltà nel comprendere come i dati vengano gestiti e la possibilità che questi possano essere esposti a minacce come Data Breach e Data Loss.

- Applicazioni web: molte aziende hanno adottato l'utilizzo di applicazioni web attraverso cui utilizzano i dati sensibili.
  Queste sono esterne rispetto all'organizzazione per cui occorre evitare che ci sia una fuga di informazioni sensibili.

- Stampa: non esiste un modo per tenere traccia dei dati sensibili una volta stampati.
  La stampa può arrivare nelle mani di un utente non autorizzato a visualizzare quei dati, può essere facilmente copiato e distrutto.

- Perdita di dati fisica: la perdita fisica di dati può avvenire in seguito al furto di un dispositivo mobile, questo accade spesso perché può essere portato al di fuori dei locali aziendali sicuri, e in seguito alla distruzione di un dispositivo contenente dati sensibili.
  I guasti fisici possono essere causati da un malfunzionamento, un uso improprio dei dispositivi o da una cattiva gestione dei dispositivi.

- Disastri naturali: la probabilità che si verifichi un disastro naturale come un uragano o un terremoto è bassa ma nel caso in cui si dovesse verificare potrebbe essere un grosso problema per la protezione dei dati in quanto questi possono essere persi e può essere difficile recuperarli.

- Malfunzionamento Hardware: tra tutte le parti del computer, il disco rigido è tra le più fragili. Questo può danneggiarsi a causa del surriscaldamento o all'accumulo di polvere nella macchina o semplicemente a causa del deterioramento.
  La presenza di danni al disco provoca la perdita dei dati.

Analizzando graficamente alcune delle cause sopra elencate emerge che il 32% delle cause principali della perdita di dati avviene in seguito dell'errore umano.

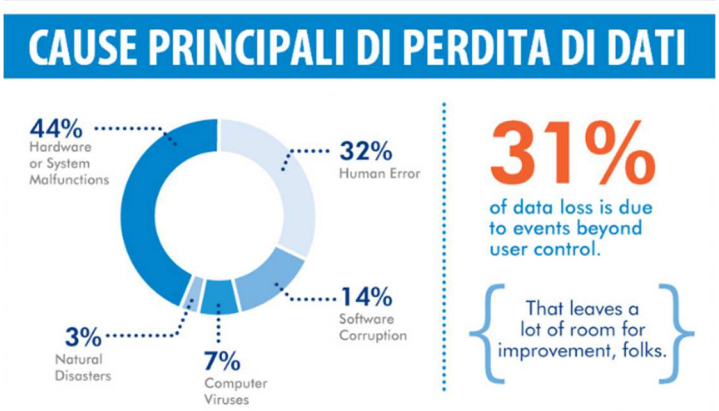

Figura 1. Cause Data Loss

Per proteggere i dati sensibili all'interno di un'organizzazione è necessario identificare questi dati e le operazioni che sono svolte dagli utenti che li utilizzano al fine di bloccare quelle che potrebbero causare un Data Loss.
Diversi esperti hanno tentato di nominare i maggiori casi di Data Loss della storia.
Secondo Statista [1], che riporta il numero di violazioni di record e dati esposti negli Stati Uniti, dalle 157 violazioni di dati segnalate nel 2005 con 66.9 milioni di record esposti si passa ad un aumento sostanziale al 2014 in cui il numero di violazioni arriva a 783 con 85,61 milioni di record.
Questi numeri non hanno fatto altro che aumentare con il passare degli anni fino ad arrivare al 2020 a un totale di 1001 violazioni e 155,8 milioni di persone colpite da esposizioni di dati.
La soluzione aziendale che può essere utilizzata per prevenire la divulgazione non autorizzata dei dati è il Data Loss Prevention cioè un insieme di prodotti, strumenti e procedure utilizzate per la prevenzione della perdita dei dati all'interno dell'azienda.

1.3 Obiettivo della tesi

Al fine di evitare la divulgazione non autorizzata dei dati sensibili all'interno dell'organizzazione è fondamentale conoscere:

- il perimetro di utenti che manipola file che contengono la proprietà intellettuale dell'azienda e quindi le workstation utilizzate da questi utenti,
- i tool utilizzati dagli utenti per generare ed esportare i file sensibili.

Una volta ottenuta la lista dei tool utilizzati dagli utenti in perimetro, viene definito il processo di certificazione.
Questo processo è differente per ognuno dei tool in perimetro ed è applicato sia quando viene utilizzato un nuovo software all'interno dell'organizzazione che quando viene rilasciata una nuova versione di uno dei software già in uso.
Gli step di certificazione si dividono in:

- Analisi con l'Application Owner per imparare ad utilizzare il tool e conoscere le azioni svolte dagli utenti dell'azienda,
- Analisi delle operazioni che generano file sensibili,

- Scrittura delle regole di classificazione al fine di classificare i dati generati dal tool,
- Scrittura delle regole di protezione al fine di monitorare ed eventualmente bloccare le azioni non permesse
- Test di efficacia delle regole.

Nel caso in cui il software da verificare sia una nuova versione di un tool già certificato in precedenza, i test sono definiti Non Regression Test (NRT) e come specificato dal nome hanno lo scopo di controllare se la qualità del software da certificare sia regredita. Per effettuare gli NRT si rieseguono le operazioni di download, salvataggio ed export già eseguite durante la certificazione della versione precedente.
Le principali azioni da eseguire sul tool sono tutte le operazioni di download, export, salvataggio e stampa che si possono effettuare tramite l'uso dell'applicazione.
Dopo aver analizzato queste operazioni è necessario verificare che i file generati siano correttamente classificati attraverso l'uso di un'etichetta di classificazione e che le azioni che possono causare un Data Loss siano bloccate o gestite secondo le regole definite e previste dall'organizzazione.
Tutte queste azioni sono necessarie per la verifica dell'efficacia delle regole già precedentemente implementate.
I test descritti sono un insieme di operazioni ripetitive che restano uguali nel tempo, tranne nel caso in cui con le nuove release siano rilasciate delle nuove funzionalità.
Queste operazioni sono svolte manualmente dal team Data Loss Prevention, il che comporta l'utilizzo di risorse in termini di tempo e una probabilità di errore.
L'obiettivo della tesi è lo scouting e la scelta di un tool esistente che permetta di automatizzare le operazioni di test e verificare la correttezza delle regole implementate e il livello della loro efficacia al cambio delle condizioni riducendo l'effort manuale che queste attività comportano.

1.3 Soluzione proposta

La soluzione proposta per verificare l'efficacia delle regole implementate e ridurre l'effort manuale causato dall'attività di certificazione del tool consiste nell'automatizzare le operazioni di test da eseguire per effettuare i Non Regression Test (NRT) e quindi automatizzare il processo di certificazione di una nuova versione di un tool in uso.

Per poter arrivare alla fase di automazione ho prima effettuato un'analisi attenta dell'ambiente di certificazione, focalizzandomi su tutti i componenti necessari per la verifica dell'efficacia delle regole.
Successivamente ho analizzato nel dettaglio due dei tool per l'automazione già presenti in commercio quali Macro Recorder e Power Automate per conoscerne tutte le funzionalità, i vantaggi e gli svantaggi e capire quale dei due fosse quello più adatto al caso d'uso.
In seguito, attraverso l'utilizzo di strumenti di Sysinternals ho effettuato lo studio dei processi generati dal tool da automatizzare, per la corretta implementazione delle regole di classificazione, al fine di identificare il processo che deve essere avviato e quello che svolge l'operazione di scrittura dei file sensibili.
La fase successiva è quella di studio dell'interfaccia del tool da automatizzare, Teamcenter, per capirne il funzionamento, analizzare tutte le operazioni di download, salvataggio ed export dei file sensibili generati e per trovare all'interno dell'interfaccia degli elementi robusti da poter utilizzare per l'automazione.
Infine, l'ultima fase è quella di sviluppo dell'automazione dei test da effettuare per la certificazione del tool utilizzato dagli utenti dell'azienda e di verifica delle regole al fine di garantire che non si perda la classificazione dei dati sensibili e che le azioni che possono causare un Data Loss siano bloccate.

1.4 Organizzazione della tesi

La tesi è organizzata nel seguente modo:

- Il capitolo 2 tratta nello specifico la soluzione di Data Loss Prevention (DLP) cioè l'insieme degli strumenti utilizzati per risolvere il problema del Data Loss, con particolare focus sulla soluzione di DLP Digital Guardian di cui si analizzano nel dettaglio l'architettura e i componenti, le funzionalità e le regole.
  Si tratta inoltre il processo di validazione delle regole.

- Nel capitolo 3 è analizzata nello specifico l'attività di certificazione da svolgere per i tool utilizzati dai dipendenti dall'azienda che generano file sensibili con particolare focus sull'ambiente di certificazione e sui componenti necessari per la verifica dell'efficacia delle regole.

Contiene inoltre una panoramica dei due tool per la scrittura e la gestione dei test automatici scelti per il progetto di tesi analizzando per ognuno dei due funzionalità, vantaggi e svantaggi.

- Nel capitolo 4 si documenta il lavoro svolto per l'automazione del tool Teamcenter.
  Si descrive nel dettaglio la soluzione implementata a partire dall'installazione del tool per poi passare allo studio dei processi generati all'avvio dell'applicazione, all'analisi di tutte le operazioni di download, salvataggio ed export che si possono eseguire dall'applicazione per generare i file sensibili.
  Durante l'analisi c'è una ricerca degli elementi robusti presenti nell'interfaccia utente del software da automatizzare al fine di trovare degli elementi che restino invariati al cambiare delle versioni per evitare di effettuare delle ulteriori modifiche nel tempo.
  Infine, si passa al processo di automazione implementato attraverso l'utilizzo dei due software Macro Recorder e Power Automate e si sceglie tra i due quello più adatto all'azienda.

- Il capitolo 5 contiene le conclusioni del lavoro svolto e quindi un'analisi dei benefici che può offrire la soluzione implementata evidenziando i possibili sviluppi futuri per migliorare il processo di automazione dei test per la verifica dell'efficacia delle regole ed estendere la soluzione proposta anche per gli altri tool utilizzati all'interno dell'organizzazione.

Capitolo 2

2. Data Loss Prevention (DLP)

In questo capitolo si approfondirà una delle possibili soluzioni per affrontare il problema legato al Data Loss e quindi alla fuga di dati sensibili all'interno dell'azienda trattato nel capitolo precedente.
Il sistema che sarà utilizzato per risolvere il problema è il Data Loss Prevention (DLP) di cui si analizzerà il funzionamento, le funzionalità e l'implementazione delle regole.
Successivamente si passerà all'analisi della soluzione DLP utilizzata per il progetto di testi, quale Digital Guardian di cui si analizzerà nel dettaglio la piattaforma, l'architettura e i componenti necessari per il corretto funzionamento, le funzionalità e le regole di cui si presenterà il processo di validazione.

2.1 Data Loss Prevention: cos'è

Il Data Loss Prevention è l'insieme dei prodotti, degli strumenti e delle procedure utilizzate per la prevenzione della perdita dei dati all'interno dell'azienda.
È un sistema che ha l'obiettivo di proteggere i dati sensibili ed evitare che questi vengano persi, condivisi con utenti non autorizzati, sottratti dai dipendenti o utilizzati in maniera impropria.
I processi DLP hanno come obiettivo quello di identificare tutte le sorgenti di dati sensibili, monitorare i dati sensibili e definire le politiche da applicare in base alle situazioni.
Con il termine Data Loss non si fa riferimento solo alla perdita di dati in seguito ad un attacco o a un data breach ma anche alla perdita di dati sensibili dovuta all'incuria di chi in maniera più o meno inconsapevole li divulga.
Il mercato del DLP è entrato in gioco fin dai primi anni del 2000 infatti è nato quando i dipendenti delle aziende hanno iniziato a utilizzare in maniera sempre più frequente i dispositivi e i servizi online come, ad esempio, l'uso del cloud o di applicazioni web per gestire i dati sensibili dell'organizzazione.

Le aziende hanno implementato questo strumento sia a causa delle minacce che arrivano dall'interno dell'organizzazione che per le stringenti leggi in materia di privacy che richiedono una rigorosa protezione dei dati e controllo degli accessi ai dati. Questo sistema quindi oltre a monitorare il movimento dei file sensibili e impedire che ci sia fuga di informazioni rispetta la conformità di normativa.
Un altro fattore che ha contribuito alla crescita del DLP è l'introduzione del ruolo Chief Information Security Officiers (CISO) che ha il compito di implementare programmi di protezione o mitigazione dei rischi che derivano dall'adozione delle tecnologie digitali, e del Data Protecion Officier (DPO).
Il DPO è una figura prevista dal nuovo regolamento General Data Protecion Regulation (GDPR) e ha la responsabilità di mettere in atto la politica di gestione del trattamento dei dati personali all'interno dell'azienda.
Gartner nella Market Guide for Enterprise Data Loss Prevention [2] definisce le soluzioni DLP. Queste soluzioni sfruttano la classificazione guidata dall'utente, le tecniche di ispezione del contenuto e l'analisi contestuale per identificare il contenuto sensibile e analizzare le azioni relative all'uso di quel contenuto.
Poi monitorano l'attività dei dati e valutano l'adeguatezza delle azioni tentate rispetto a una politica Data Loss Prevention predefinita che dettaglia l'uso accettabile, in contesti specifici, per specifici tipi di contenuto o classificazioni.
Il sistema Data Loss Prevention si focalizza quindi su:

- Classificazione: il processo di classificazione dei file sensibili avviene attraverso l'utilizzo di etichette di classificazione,
- Violazione: le violazioni delle policy devono tener conto dei regolamenti normativi,
- Protezione: è importante realizzare dei sistemi di protezione consistenti al fine di prevenire il Data Loss,
- Compliance: è necessario verificare di avere policy che rispettino le conformità di normativa a cui si deve sottostare.

Per quanto riguarda la classificazione dei file il processo DLP utilizza dei software che classificano i dati definiti sensibili attraverso l'utilizzo di etichette.
A differenza della normale classificazione dei documenti con dati confidenziali, che prevede la presenza di quattro livelli di classificazione, il DLP è come se utilizzasse due soli livelli che definiscono se il file è di dominio pubblico e quindi non contiene dati sensibili o se può essere manipolato solo da un perimetro di utenti e quindi contiene dati sensibili.

Riguardo la violazione come già anticipato questa deve rispettare i regolamenti normativi ed è diversa in base alle aziende in quanto definita internamente all'organizzazione.
È importante identificare la violazione alle policy entro un intervallo di tempo ragionevole e questa deve essere notificata con un alerts generato attraverso un sistema automatico.
Le tre funzionalità principali di un sistema DLP si possono riassumere in:

- Data Inventory per poter identificare e successivamente classificare i dati sensibili,
- Policy Definition per implementare delle regole di gestione consistenti che prevedono azioni diverse in base all'evento che viene generato in seguito all'utilizzo dei dati sensibili,
- Content Monitoring, Filtering & Encryption per poter monitorare le operazioni effettuate e applicare le regole implementate.

I software e gli strumenti adottati dal processo Data Loss Prevention monitorano e controllano sia i file che risiedono fisicamente nelle workstation definite endpoint dei dipendenti dell'organizzazione, che i flussi di dati che transitano in rete e i dati presenti nel cloud.

Figura 2. Enterprise DLP

Per proteggere i dati che risiedono nelle workstation dei dipendenti è fondamentale conoscere il perimetro di utenti che utilizza dati sensibili e quindi le macchine utilizzate da questo set limitato di utenti, una volta definito, ogni endpoint che ne fa parte deve avere il software DLP installato.
Il software permette di monitorare le comunicazioni interne ed esterne, di controllare l'accesso fisico ai dispositivi e di notificare attraverso l'utilizzo di alerts o altre azioni di notifica azioni che possono recare danni all'organizzazione.

In ambito DLP il perimetro di utenti include dipendenti e fornitori che manipolano file che contengono la proprietà intellettuale dell'organizzazione.
Per proteggere i flussi di dati che transitano in rete il software DLP viene installato nei punti di uscita di rete più vicini al perimetro.
Le soluzioni DLP Network hanno quindi diversi punti di controllo che tengono traccia dei dati in movimento e sono poi analizzati da un server di gestione centrale.
L'obiettivo è quello di analizzare il flusso di dati in rete per rilevare i dati sensibili che sono stati inviati verso l'esterno violando le policy definite.
Il DLP oltre le funzionalità già elencate fornisce dei report che hanno lo scopo di identificare eventuali debolezze o anomalie e assicurare la compliance e i requisiti di auditing.
Tra i software Data Loss Prevention in commercio, la lista dei fornitori rappresentativi nella prevenzione della perdita dei dati aziendali stilata da Gartner [3], visibile in figura 3, troviamo Forcepoint, GTB Technologies DLP, McAfee e Digital Guardian.
Il software DLP utilizzato per il progetto di tesi che verrà analizzato nel dettaglio è Digital Guardian.

Table 1: Representative Vendors in Enterprise Data Loss Prevention

Vendor	Product, Service or Solution Name
Clearswift	Adaptive Data Loss Prevention (A-DLP)
CoSoSys	Endpoint Protector
Digital Guardian	Digital Guardian DLP
e-Safe Systems	People Centric DLP
Fidelis	Fidelis Network
Forcepoint	Forcepoint DLP
GhangorCloud	Information Security Enforcer (ISE)
GTB Technologies	GTB Inspector
InfoWatch	InfoWatch Traffic Monitor
McAfee	McAfee Total Protection for Data Loss Prevention
SearchInform	SearchInform DLP
Beijing Skyguard Cybersecurity Technology	Sky Guard DLP

Figura 3. Vendors in Enterprise Data Loss Prevention

2.2 Digital Guardian

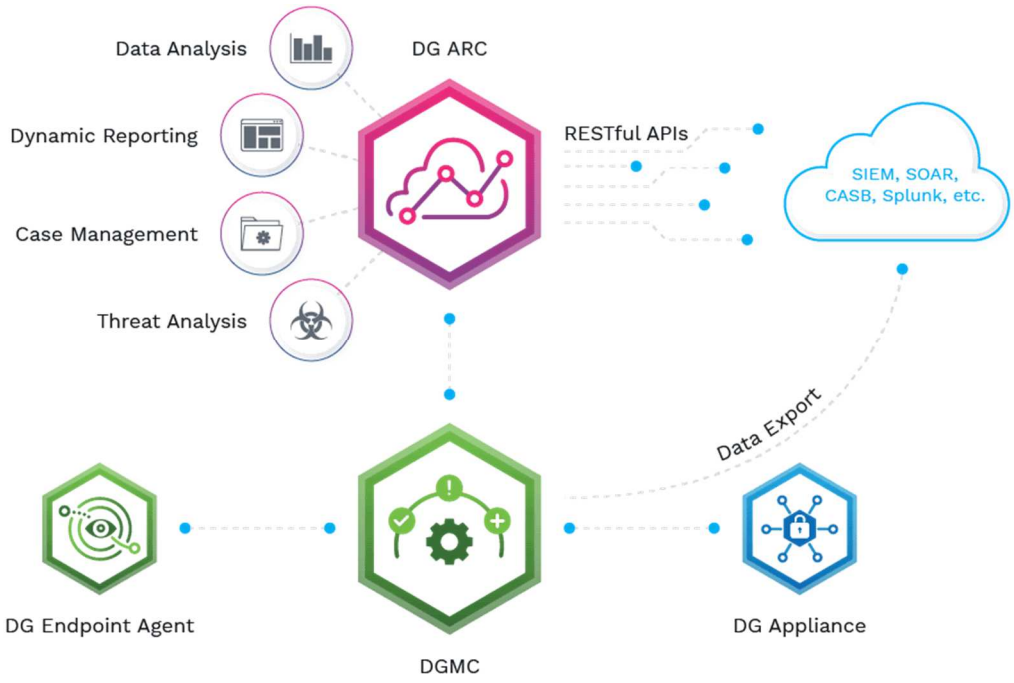

Figura 4. Piattaforma Digital Guardian

Digital Guardian [4] è un software DLP che combina le funzionalità per la prevenzione della perdita di dati (Data Loss Prevention), il rilevamento e la risposta degli endpoint (Endpoint Detection and Response) e l'analisi del comportamento degli utenti e delle entità (User Behavior and Entity Analytics) in un'unica soluzione di sicurezza degli endpoint.

È inoltre l'unica soluzione di Data Loss Prevention distribuita via SaaS (Software as a Service) ma può anche essere disponibile come servizio gestito.

L'azienda Digital Guardian ha sviluppato una piattaforma digitale in cloud che funziona per le reti aziendali, per gli endpoint e per le applicazioni in cloud.

Questa soluzione è stata sviluppata attraverso l'utilizzo di una piattaforma alimentata da Amazon Web Services che unisce DLP, la risposta degli endpoint e gli eventi di rete e registra tutte le informazioni ottenute all'interno di un database centralizzato.

La piattaforma lavora a basso livello e questo permette di avere una visione globale degli eventi, questi vengono divisi in base alla priorità assegnata il che permette di avere una risposta efficace alle minacce.

Per poter identificare automaticamente i file sensibili, il software Digital Guardian verifica la presenza del tag di classificazione, in fase di classificazione applica quindi delle etichette che servono per marcare solo alcuni tipi di dati.
In seguito alla classificazione dei dati sensibili il software organizza i dati e attraverso l'implementazione di regole di protezione, monitora le attività svolte dagli utenti al fine di evitare che ci sia una fuga di dati.

2.3 Architettura

L'architettura di Digital Guardian, visibile in figura 5, è composta da:

- DG Agent: è il software che deve essere installato sulle workstation dei dipendenti quindi sugli endpoint da proteggere.
  Ha il compito di riconoscere i file classificati, di monitorare e registrare tutti gli eventi che scaturiscono dall'uso delle workstation sia a livello utente che a livello di sistema e di rete.
  Il comportamento degli agenti presenti sugli endpoint si può configurare attraverso la console Digital Guardian in modo da poter applicare alle workstation le regole che servono a bloccare attività sospette ed evitare che i dati sensibili vengano persi o divulgati in maniera consapevole o inconsapevole da parte degli utenti.

- Digital Guardian Server: sono i server su cui sono installati i componenti per configurare e far funzionare i DG Agent installati sulle workstation degli utenti. Sono gestiti da una console basata sul web e servono per pianificare le attività della console, acquisire le attività degli utenti e generare report.
  Il primo server in alto ha la Digital Guardian Management Console (DGMC) cioè una console di gestione basata sul web che serve per amministrare e monitorare gli agent ed è quindi il centro di configurazione.
  Ha inoltre la DGComm cioè il servizio web verso cui puntano gli agent e serve per catturare le attività degli utenti (bundle) nel database, e il Job Scheduler cioè un processo per la pianificazone delle attività di DG che serve per sincronizzare le macchine, le active directory e le notifiche di avviso via email.
  Gli altri server hanno la DGComm e il Bundle Processor cioè un servizio che elabora i dati criptati sulle attività degli utenti che vengono inviate dagli agent.

Ha quindi il compito di ricevere i pacchetti, che arrivano cifrati, processarli e inviarli.

- Load Balancer: servono per smistare i pacchetti al DGComm più scarico.

- Database: un database centralizzato all'interno del quale sono memorizzate tutte le attività dei DG Agent.

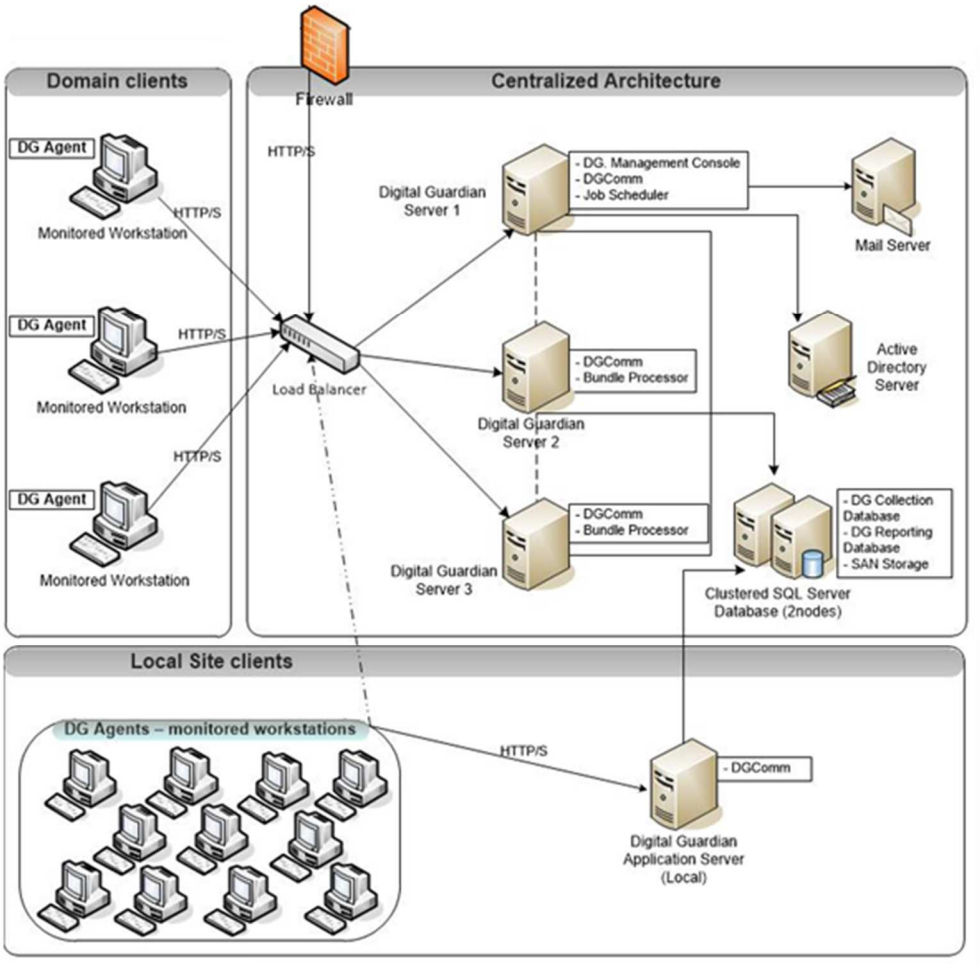

Figura 5. Architettura Digital Guardian

2.4 Funzionalità

Come già detto il software Digital Guardian è in grado di identificare in modo automatico i file sensibili attraverso il tag o etichetta di classificazione e organizza i dati attraverso l'implementazione di regole di protezione che hanno lo scopo di monitorare ed eventualmente bloccare le azioni svolte dagli utenti al fine di evitare che ci sia una fuga di dati sensibili.

La prima funzionalità del software Digital Guardian è quindi legata alla classificazione dei dati, il software riesce a identificare automaticamente i dati sensibili, cioè quelli su cui è stata applicata un'etichetta di classificazione.

L'etichetta o tag di classificazione definisce il tipo di dato.

Oltre ad avere una classificazione automatica, generata dall'identificazione dei file, è possibile inserire una classificazione manuale effettuata direttamente dall'utente.

La classificazione automatica avviene mediante l'implementazione di regole di classificazione.

La seconda funzionalità di Digital Guardian è quella legata alla rilevazione dei dati.

La rilevazione dei dati ha come scopo quello di poter monitorare costantemente il flusso di dati dell'organizzazione al fine di per poter rilevare e successivamente proteggere i dati nel modo corretto.

La rilevazione dei dati non si limita al flusso di dati interno all'organizzazione ma riguarda anche il flusso di dati inviato in rete al di fuori dell'azienda, questo perché gli utenti possono allegare i file sensibili all'interno delle mail o utilizzarli tramite applicazioni web esterne.

Un'altra importante funzionalità è quella della cifratura dei dati sensibili.

La cifratura serve per autorizzare l'accesso ai soli utenti autorizzati e garantire quindi un maggior livello di protezione.

Per poter sfruttare le funzionalità del software Digital Guardian e quindi effettuare la rilevazione dei dati e monitorare le azioni svolte dai dipendenti dell'organizzazione occorre identificare il perimetro di utenti che manipola file sensibili, questo significa definire l'insieme di utenti e di workstation ad essi associate.

Il perimetro è dinamico per cui una volta identificato è di fondamentale importanza occuparsi del suo mantenimento in quanto è possibile che si debba inserire un nuovo utente perché nuovo assunto all'interno dell'organizzazione, perché gli è stato concesso l'accesso agli strumenti che generano file sensibili, o perché la workstation in possesso dell'utente è stata dismessa o formattata.

In qualunque delle situazioni sopra elencate ci si trovi occorre intervenire per evitare che gli utenti possano svolgere azioni che mettano a rischio la proprietà intellettuale dell'azienda e richiedere l'installazione dell'agent sulle workstation in questione.

2.5 Regole

Il software Digital Guardian ha la possibilità di essere utilizzato solo per il monitoraggio e la registrazione di eventi oppure consente di personalizzare le attività attraverso l'utilizzo di regole.
Le regole possono ad esempio prevenire la perdita di dati per la condivisione attraverso supporti rimovibili non controllati, prevenire che i dati sensibili siano divulgati involontariamente, inviare degli alerts in seguito allo svolgimento di azioni non permesse da parte degli utenti.
Una regola è un insieme dei tag Extensible Markup Language e del contenuto che specifica le azioni da intraprendere in base ai file e agli eventi scaturiti.
Le regole possono essere settate in stato "Active" che sono quelle che sono realmente distribuite sulle workstation da proteggere o "Inactive" quindi inattive e non hanno nessun effetto.
L'insieme delle regole forma una policy.

Esistono diverse tipologie di regole:

- Regole di classificazione: permettono di identificare i file sensibili in base a determinati criteri e una volta identificati applicano delle etichette o tag di classificazione che ne definiscono, appunto, la classificazione.
  Dopo aver implementato le regole di classificazione e quindi dopo aver applicato l'etichetta di classificazione al file è possibile scrivere le regole di controllo che servono per regolare l'attività degli utenti in base alla tipologia di classificazione dei file.

- Regole di controllo: servono per gestire le attività intraprese dagli utenti al fine di determinare se il tipo di utilizzo dei dati sensibili può portare a un potenziale Data Loss ed eseguire quindi un'azione di remediation.
  Tra le azioni eseguite attraverso le regole di controllo troviamo il blocco, la richiesta di inserimento di ulteriori informazioni prima di procedere con

l'operazione da voler eseguire (come, ad esempio, l'inserimento delle credenziali dell'utente) o degli avvisi sull'attività in corso.
Tutte queste azioni determinate dalle regole di controllo sono visualizzate sulle workstation degli utenti attraverso un prompt.
Nel caso in cui due o più regole abbiano diverse tipologie di azione scaturite dallo stesso evento l'ordine con cui queste vengono intraprese sarà:

- Blocca
- Crittografa
- Richiede
- Avviso
- Data Vault

Le regole di controllo vengono eseguite indipendentemente dalle regole di filtro e possono essere applicate agli utenti in modo che siano monitorati indipendentemente dal computer a cui accedono.
Le regole di controllo rappresentano la funzionalità principale di Digital Guardian.

- Regole di filtro: servono per escludere le attività al fine di ridurre la generazione di eventi, come i file di log, da parte dei processi in background.
  Queste regole forniscono una riduzione granulare delle attività da registrare, ma il metodo più efficiente per ridurre i log delle attività è configurare il processo di installazione del DG Agent per filtrare intere classi di attività svolte dall'utente.
  Se l'attività innesca una regola di controllo, il Digital Guardian Agent non applicherà le regole di filtro.

- Regole per i processi affidabili: servono per escludere la registrazione o il blocco di azioni generate da specifiche applicazioni.
  Queste regole sono definite prima delle regole di filtro e delle regole di controllo per cui il Digital Guardian Agent non esegue alcuna regola sull'attività generata dai processi definiti affidabili.
  Solitamente queste regole sono utilizzare per firewall, Intrusion Detection System (IDS) e antivirus.

- Regole per i componenti: servono per far riferimento alla definizione di altre regole e sono simili a una funzione in un linguaggio di programmazione.

Queste regole non contengono informazioni sulle azioni ma servono per ridurre la quantità di tempo necessaria per scrivere e mantenere le regole.

- Regole Data Vault: sono un insieme di regole aggiuntive che si possono applicare ad un processo applicativo e servono per registrare un evento senza però intraprendere alcuna azione fino a che non si verifica un ulteriore evento correlato.
  Un Data Vault viene creato quanto l'attività dell'utente soddisfa un insieme di condizioni, una volta creato resta in vigore fin quando l'utente non chiude l'applicazione che lo ha generato.

Dopo aver creato le regole, queste devono essere aggiunte all'interno di una policy altrimenti non avranno alcun effetto.
In seguito all'inserimento di una regola all'interno della policy è possibile associare tale policy agli utenti, una volta associata la policy al gruppo di macchine su cui deve essere applicata, basterà attendere che la workstation comunichi con la console Digital Guardian in modo che si aggiorni la configurazione e da quel momento in avanti la policy sarà attiva e funzionante.

2.6 Processo di validazione delle regole

Per poter validare le regole e applicare le azioni necessarie per evitare che ci sia un Data Loss, il software Digital Guardian fornisce un motore di regole che le elabora al fine di determinare se gli eventi o gli alerts generati su una workstation corrispondono alle configurazioni specificate e quindi se le regole risultano attive.
Quando un utente esegue un'operazione che genera un evento, l'Agent Digital Guardian lo cattura e si avvia il motore di regole.
Il motore di regole valuta l'evento e lo confronta con le regole applicate iniziando da quella con priorità più alta.
Per farlo utilizza un approccio bottom-up per cui parte della fine di ogni regola e verifica i dettagli dell'evento come, ad esempio, il file sorgente o l'estensione del file e li confronta con le clausole presenti all'interno delle regole.
Ogni volta che trova una corrispondenza continua a verificare ulteriori clausole fino ad arrivare nella parte alta della regola.

Il confronto tra l'evento e le regole può portare a:

- Uscire dalla regola se le clausole sono false. Il motore, infatti, interrompe la valutazione della regola se riscontra una clausola non vera e passa alla regola successiva con priorità maggiore.

- Applicare l'azione associata alla regola se tutte le clausole sono true. Il motore per applicare l'azione continua la verifica fin quando ogni clausola di una regola è vera.

Esistono inoltre le variabili di regola che aggiungono un'ulteriore opzione riguardo il comportamento, queste servono per salvare le informazioni sulla regola ed utilizzare successivamente in un'altra regola.

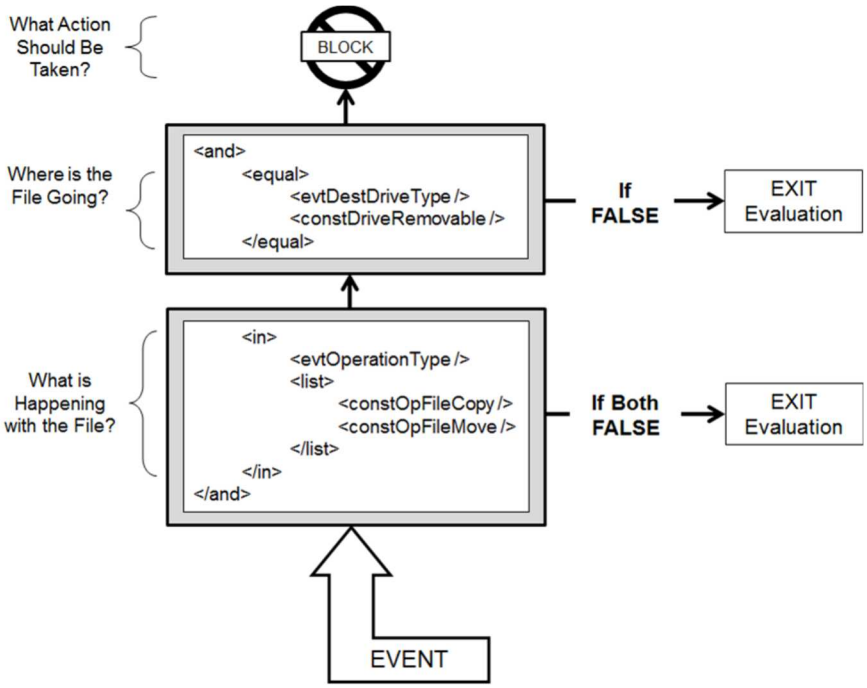

Figura 6. Valutazione di una regola

Il processo di valutazione della regola inizia con lo scaturire di un evento e quindi dallo svolgimento di un'azione sui dati sensibili da parte dell'utente come, ad esempio, un'operazione di scrittura su un file.
Analizzando l'esempio di valutazione della regola [5] presente in figura 6, leggendo la regola dal basso verso l'alto, il primo controllo è quello relativo all'operazione effettuata sul file.

Nel caso in cui l'operazione fosse un'operazione di copia (constOpFileCopy) o di spostamento del file (constOpFileMove) e quindi una delle due clausole fosse settata a "true" allora si passerà alla verifica dell'unità di destinazione del file.
Qualora invece entrambe le clausole fossero false, l'Agent Digital Guardian bloccherà l'evento e quindi si uscirà dalla regola.
Allo stesso modo qualora la destinazione del file fosse un archivio rimovibile (constDriveRemovable) e quindi anche questa clausola fosse "true", si procederà ad eseguire l'azione definita della regola, altrimenti si uscirà dalla regola e l'Agent Digital Guardian bloccherà l'evento.
Le regole si possono scrivere manualmente o attraverso l'utilizzo del "Control Rule Builder Wizard".
Qualora si decidesse di procedere con la scrittura manuale della regola, occorrerà sfruttare la documentazione fornita da Digital Guardian per scegliere le funzioni opportune da utilizzare e inoltre occorrerà considerare la probabilità di errore causata dalla persona che si occuperà della scrittura.
Il "Control Rule Wizard" è integrato all'interno della console Digital Guardian e semplifica la creazione della regola seguendo diversi step:

- Scelta della categoria operazione in cui si può specificare se l'operazione è un'operazione legata ad esempio a un processo, un dispositivo o a un trasferimento di file in rete.
  Questo primo step è rappresentato in figura 9.

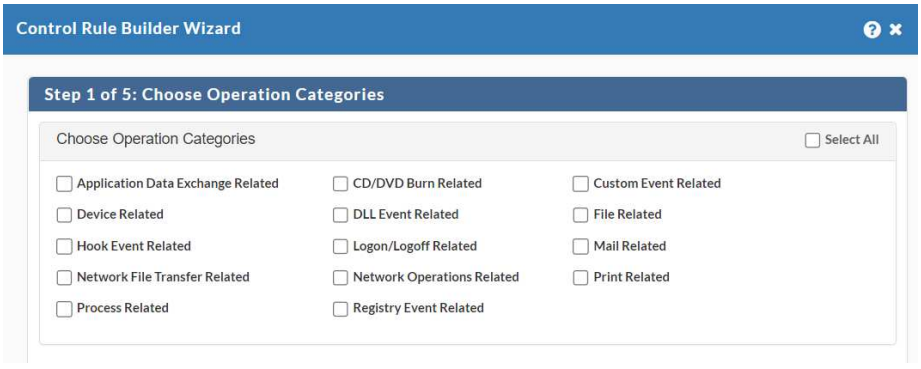

Figura 7. Choose Operation Categories

- Scelta del tipo di operazione per cui nel caso specifico della categoria Process Related potrebbe essere semplicemente l'avvio dell'applicazione o un'azione specifica svolta attraverso l'uso del processo,

- Scelta del numero di processi da inserire all'interno della regola, quindi occorre specificare se si utilizza un solo processo o più di uno,

- Scelta di criteri addizionali da inserire all'interno della regola,

- Revisione del codice XML generato per la regola basato sulle precedenti selezioni.

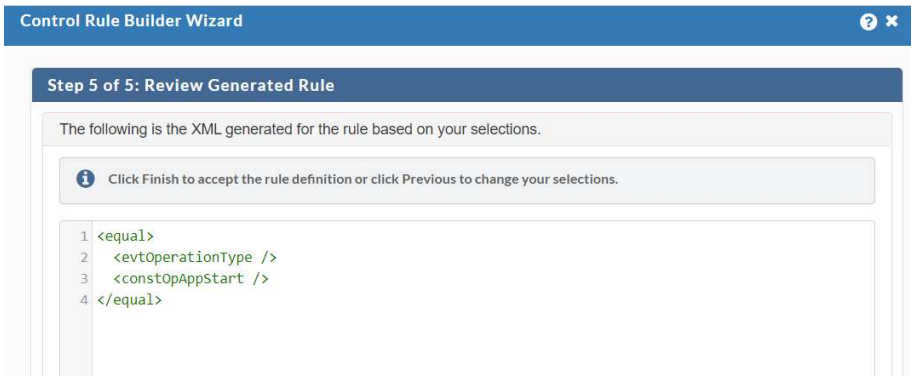

Figura 8. Esempio di codice

Una volta implementata una regola, questa può essere immediatamente distribuita e applicata sulle macchine che hanno il software Digital Guardian installato.
Questo è un grande vantaggio in quanto l'azione di Remediation sarà subito applicata nel caso in cui un utente provasse a svolgere un'azione non autorizzata ma allo stesso tempo è di fondamentale importanza fare in modo di non ostacolare il lavoro svolto dai dipendenti.
Prima di distribuire una regola occorre quindi effettuare accurati test.
Questi non sono effettuati direttamente nell'ambiente di produzione ma viene utilizzato un ambiente di test che simula esattamente quello di produzione.
Solo al termine dei test, la regola sarà copiata nell'ambiente di produzione e applicata alle macchine degli utenti.

Capitolo 3

3. Certificazione dei tool

In questo capitolo è analizzata nello specifico l'attività di certificazione da svolgere per i tool utilizzati dai dipendenti dell'azienda per la creazione dei file sensibili.
Il primo punto di studio sarà sull'ambiente di certificazione e comprenderà tutti i componenti necessari per la verifica dell'efficacia delle regole.
Successivamente sarà presentata una panoramica dei tool per la scrittura e la gestione dei test automatici con particolare focus sull'analisi dei tool Macro Recorder e Power Automate.
Per questi due tool scelti per il progetto di tesi, saranno riportati vantaggi, svantaggi e funzionalità.
Inoltre, saranno successivamente utilizzati per l'automazione dei test per l'applicazione Teamcenter.

3.1 Processo di certificazione

Oltre al perimetro di utenti e quindi ai dipendenti che manipolano file che contengono la proprietà intellettuale dell'organizzazione, esiste un altro concetto di perimetro che serve per definire quali sono i tool utilizzati dagli utenti per generare e visualizzare file sensibili.
Una volta definiti i tool in perimetro inizia il processo di certificazione che viene gestito in due modi in base alla tipologia di software da certificare:

- Se il software da certificare è nuovo, per prima cosa deve essere effettuata un'analisi con l'Application Owner per poter imparare ad utilizzare il tool e in particolare per conoscere tutte le azioni da riprodurre in fase di test.
  Queste azioni riguardano principalmente tutte le modalità di salvataggio ed export dei file sensibili generati.

In seguito all'analisi si passa alla fase di test in cui si scrivono le regole, si svolgono tutte le azioni e si verifica che tutti i file sensibili generati dal tool siano classificati e che le regole di controllo funzionino correttamente.
Per tener traccia di tutti i test effettuati si compila un test plan con tutte le azioni di export e di verifica dei blocchi al fine di verificare l'efficacia delle regole implementate.

- Se il software da verificare è una nuova versione di un tool già certificato in precedenza, si devono svolgere nuovamente le azioni di export definite nel test plan compilato in precedenza al fine di verificare che le regole di classificazione e di controllo funzionino correttamente e si deve verificare che non ci siano delle nuove funzionalità, in questo caso si dovranno modificare le regole precedentemente implementate.

I test effettuati sulle nuove versioni di un tool già in perimetro sono definiti Non Regression Test (NRT).
Gli NRT, come specificato dal nome, hanno lo scopo di controllare se la qualità del software da certificare sia regredita e consistono quindi nel rieseguire le azioni descritte all'interno dei test plan precedentemente creati per verificare le nuove release e garantire che le funzionalità già presenti nelle versioni precedenti del tool mantengano le loro caratteristiche anche in seguito all'introduzione di nuove funzionalità.
Al momento gli NRT sono svolti manualmente dal team Data Loss Prevention che esegue la classificazione NRT al fine di verificare che non si perda la classificazione dei dati sensibili e la protezione NRT al fine di verificare che le azioni che possono provare un Data Loss siano bloccate.
Questo processo, che consiste nell'effettuare l'insieme di operazioni descritte all'interno del test plan, è molto ripetitivo per cui l'obiettivo della tesi è quello di automatizzare il processo di certificazione in modo che sia più efficiente in termini di velocità e precisione e che preveda un effort minore da parte del team DLP.

3.2 Ambiente di Certificazione

Le azioni del test plan da rieseguire durante la certificazione di un tool, al fine di verificare che le regole applicate in produzione siano ancora efficaci, devono essere eseguite su

una macchina di laboratorio che riproduca esattamente la stessa situazione d'uso dell'utente finale.
Per farlo la macchina di test deve essere configurata in console Digital Guardian in modo che su questa siano deployate le stesse policy e regole della macchina dell'utente dell'organizzazione che dovrà utilizzare il tool.
Oltre alle macchine di test sono utilizzati dei componenti fondamentali per la verifica delle regole quali:

- Digital Guardian Content Inspection Application Utility [6] (DCIAPP) è un software che per funzionare deve essere installato su una macchina che abbia a bordo il software Digital Guardian e serve per verificare se le regole di classificazione funzionano correttamente.
  Il DGCIAPP permette di visualizzare informazioni che riguardano:

  - Le informazioni generali del file,
  - La presenza dei pattern e la frequenza con cui sono ripetuti,
  - Il tag di classificazione applicato al file e gli identificativi della regola e della policy associata,
  - Le proprietà del file come la data di creazione e l'estensione.

- Process Explorer è uno strumento che appartiene al software Sysinternals e serve per controllare tutti i processi attivi e tutte le attività che sono in esecuzione sul sistema.
  Mostra informazioni dettagliate grazie all'unione delle funzionalità del Task Manager di Windows XP, di Gestione Attività di Windows Vista e delle ulteriori funzionalità utili per raccogliere informazioni sui processi, librerie in uso e risorse utilizzate.
  Il programma è disponibile solo in lingua inglese e l'interfaccia mostra solo le informazioni principali dei processi in esecuzione, è però possibile personalizzare il programma in modo che si possano visualizzare ulteriori dettagli.
  La configurazione standard [7] prevede:

  - Process, il nome del processo,
  - PID, il Process Identifier,
  - CPU, l'occupazione della CPU da parte del processo,
  - Description, una breve descrizione del processo,

- Company Name, il nome del produttore del processo.

- Process Monitor (Procmon) è un processo che appartiene al software Sysinternals e serve per il monitoraggio avanzato in Windows.
  Procmon permette di visualizzare in tempo reale:

  - I processi/Thread attivi
  - File system
  - Registro di sistema
  - Attività DLL

  e di approfondire un evento grazie all'utilizzo del filtro dell'output che permette di visualizzare informazioni di dettaglio come l'ID di sessione.

- DebugView è un'applicazione che permette di intercettare e visualizzare i dati di debug generati dai processi in esecuzione sul computer locale e in rete e permette di mostrare l'output a livello kernel.
  È un'applicazione semplice da usare e i processi da monitorare non devono funzionare all'interno di un'ambiente controllato.

A queste applicazioni già presenti all'interno dell'ambiente di certificazione si deve aggiungere anche il tool per l'automazione dei test.
In commercio esistono diversi tool per la scrittura e la gestione di test automatici, non esiste uno strumento che sia in grado di soddisfare tutte le esigenze di un'azienda ma hanno tutti dei pro e dei contro e la scelta nell'utilizzo dell'uno o dell'altro dipende unicamente dalle necessità dell'organizzazione.
Tra i software di automazione in commercio esistono: JitBit Macro Recorder, Mouse Recorder, Macro Toolworks, Macro Recorder e Microsoft Power Automate.
Sono stati quindi analizzati diversi strumenti per la gestione automatica dei Non Regression Test e una volta valutato il contesto in cui devono essere utilizzati, cioè delle macchine di laboratorio con sistema operativo Windows, i due tool scelti per lo sviluppo della tesi sono Macro Recorder e Microsoft Power Automate.

3.3 Macro Recorder

Macro Recorder è un software di automazione della Bartels Media GmbH che permette di registrare ed acquisire tutti i movimenti del mouse e della tastiera e creare delle macro per poi riprodurle.
In particolare, permette di registrare i movimenti del mouse, sia il click che le azioni svolte dalla rotellina, di registrare la pressione dei tasti sulla tastiera e gli input di testo, di rilevare le immagini, l'Optical Character Recognition (OCR) e il colore dei pixel.
Fornisce inoltre un editor di passaggi macro e permette di modificare la velocità di produzione e di inserire pause.
È uno degli strumenti adatti effettuare i test del software automatizzati in quanto una volta create le macro, le azioni registrare potranno essere ripetute all'infinito sul computer.
Permette inoltre di effettuare test dell'interfaccia utente in quanto ne emula il comportamento.
Il software è disponibile sia per Windows che per Mac.
Le principali funzionalità di Macro Recorder sono:

- Automazione delle attività ripetitive,
- Compilazione automatica dei moduli,
- Automazione delle attività di manutenzione,
- Accesso automatico agli account,
- Click automatico su programmi e siti,
- Automazione dei test.

La creazione delle macro può avvenire mediante la registrazione delle azioni del mouse e della testiera utilizzando il software come se fosse un vero e proprio registratore oppure creando una nuova macro utilizzando l'integrazione di Macro Recorder con PhraseExpress che permette di ottenere delle funzionalità aggiuntive.
PhraseExpress è un programma di testo automatico progettato per scrivere velocemente attraverso la configurazione di scorciatoie da tastiera.
Il modo più semplice per la creazione delle macro [8] è attraverso la registrazione dello schermo, per farlo basta cliccare sul tasto "Record" presente nell'interfaccia del software e stoppare cliccando sul tasto Stop.

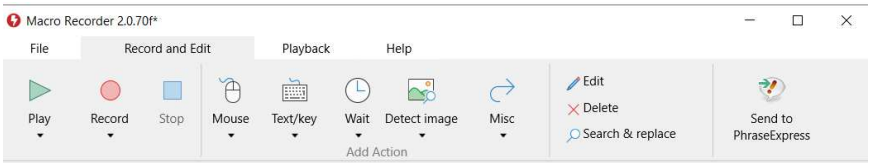

Figura 9. Barra Strumenti Macro Recorder

Questa modalità permette di registrare i movimenti del mouse, il click del mouse, le azioni svolte dalla rotellina del mouse e i tasti premuti sulla tastiera.
In seguito al salvataggio della registrazione è possibile modificare o rimuovere azioni, aggiungere delle pause, regolare la velocità di riproduzione e smussare i percorsi del mouse.

Vantaggi

Il primo vantaggio di Macro Recorder risiede nella semplicità d'utilizzo, è infatti un software molto intuitivo che registra i movimenti del mouse e della pressione della digitazione dei tasti sulla tastiera e li riproduce automaticamente sotto forma di processo.
Il secondo vantaggio riguarda i movimenti del mouse.
Questi sono combinati all'interno di un singolo elemento di azione che può essere rilevato dal click o configurato inserendo le coordinate X/Y o l'offset relativo alla posizione del puntatore.
Inoltre, i movimenti del mouse possono essere trasformati da movimenti instabili a movimenti lineari o curvi fluidi al fine di evitare di visualizzare in riproduzione i movimenti tremolanti svolti da chi ha registrato il processo e i vari percorsi registrati sono visualizzati come una sovrapposizione sul desktop.
Un altro vantaggio relativo ai movimenti del mouse è l'azione di SmartClick che non utilizza le coordinate statiche X/Y ma effettua il click su un'area bitmap predefinita.
Infine, l'ultimo vantaggio del software Macro Recorder è legato al ripristino e alla regolazione automatica della dimensione e della posizione delle finestre utilizzate dal programma.

Svantaggi

Uno degli svantaggi di Macro Recorder consiste nell'impossibilità di collaborare con il team DLP durante la creazione della macro.
È infatti un editor a pagamento e per ottenere le funzionalità legate alla condivisione si deve pagare più dell'una tantum previsto.
Oltre a non poter collaborare durante la creazione della registrazione non è nemmeno possibile condividere l'automazione registrata; quindi, il file Macro Recorder macro-file con estensione "mrf" precedentemente salvato.
Non è quindi possibile la riproduzione della macro su dispositivi differenti da quello utilizzato durante la creazione del file.

Conclusioni

Questi due svantaggi sono stati fondamentali nella scelta del tool da utilizzare durante la tesi in quanto la collaborazione e la possibilità di riproduzione delle azioni registrate su macchine diverse da quella da cui sono state create sono fondamentali per poter certificare i tool.
Questo perché non sempre l'installazione dei software da certificare avviene sulla stessa macchina sui cui era installata una versione precedente, diventa quindi fondamentale poter esportare il file su cui sono state registrate tutte le attività da svolgere per il test plan per poterle riprodurre su tutte le macchine di test che il team Data Loss Prevention ha a disposizione.

3.4 Microsoft Power Automate

Microsoft Power Automate è un servizio della Microsoft basato sul cloud che consente di automatizzare le attività e i processi aziendali.
È uno dei pilastri di Microsoft Power Platform insieme a Microsoft 365, Dynamics 365 e Azure e oltre a Power Automate comprende anche Power BI cioè un'applicazione Desktop per elaborare i dati aziendali, Power Apps e Power Virtual Agents.
Sfrutta la Robotic Process Automation (RPA) per simulare i movimenti del mouse e la digitazione tramite tastiera e mette a disposizione dell'utente un software intuitivo che permette di creare l'automazione attraverso la creazione di flussi di lavoro.

I flussi di lavoro si distinguono in:

- Flussi cloud, si dividono a loro volta in flussi automatizzati, istantanei e pianificati.
  Questa tipologia è adatta quando si desidera che l'automazione si attivi tramite una pianificazione.
  Un esempio del flusso cloud automatizzato può essere la creazione di automazione che viene attivata in seguito all'arrivo di una email, mentre un esempio di un flusso cloud istantaneo può essere l'attivazione dell'automazione attraverso il click di un pulsante.

- Flussi di processo aziendale, servono per eseguire in modo semplificato i processi definiti dall'organizzazione.
  Questa tipologia di flusso fornisce una guida per assicurarsi che gli utenti seguano sempre gli stessi passaggi e inseriscano i dati in modo coerente.
  Per portare a termine un processo aziendale vengono definite delle fasi e ognuna di queste è formata da un gruppo di passaggi che possono essere resi obbligatori in modo che l'utente termini tutti gli step prima di passare alla fase successiva.

- Flussi Desktop, sono utilizzare per l'automazione delle attività che vengono svolte dall'utente sul desktop e sulle applicazioni Web.
  Questa tipologia amplia la funzionalità RPA e permette di automatizzare i processi Desktop.

I flussi desktop possono essere eseguiti sia in modalità manuale, che in modalità automatica.

In modalità manuale viene utilizzata una sessione utente già esistente, la sessione non deve essere bloccata e si consiglia di evitare l'utilizzo del dispositivo fin quando non termina l'esecuzione del processo.

In modalità automatica non è necessaria alcuna supervisione da parte dell'utente, i flussi infatti sono eseguiti sui dispositivi con lo schermo bloccato e al termine dell'esecuzione Power Automate si disconnette dal dispositivo utilizzato.

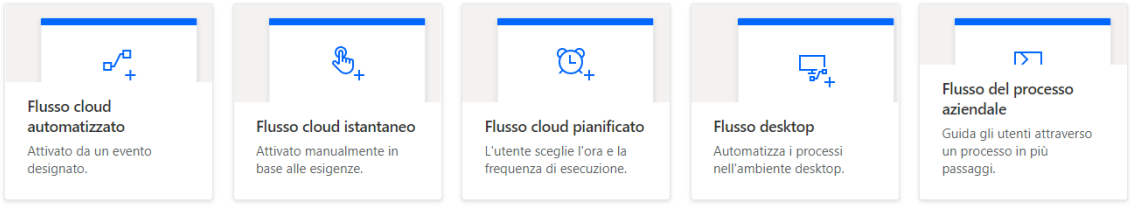

Figura 10. Tipologie di flusso Power Automate

Microsoft Power Automate lavora attraverso l'utilizzo di ambienti.

Un ambiente è uno spazio in cui condividere, archiviare e gestire i dati aziendali.

È creato in un tenant Azure Active (Azure AD) che risulta accessibile ai soli utenti di questo tenant.

L'ambiente è inoltre associato ad una posizione geografica in modo che quando viene creato un processo queste viene instradato ai data center localizzati nell'area geografica in questione.

Si possono creare più ambienti distinti per separare i diversi team di lavoro all'interno dell'organizzione o per distinguere gli ambienti di test con gli ambienti di produzioni delle app.

Un'altra importante caratteristica di Power Automate è la possibilità di eseguire il debug di un flusso desktop.

Questo è molto utile nel caso in cui siano presenti degli errori nel flusso desktop creato o nel caso in cui ci siano delle modifiche nel sistema.

Tra gli strumenti di debug [9] messi a disposizione dall'applicazione troviamo:

- Il riquadro degli errori, cioè un riquadro a comparsa che mostra le informazioni relative all'errore che si è verificato specificando il nome del flusso che contiene l'azione che ha provocato l'errore, il numero dell'azione che ha generato l'errore e il messaggio di errore,

- la possibilità di eseguire il flusso azione per azione sospendendo e riprendendo il flusso di esecuzione per ispezionare le azioni,

- la possibilità di aggiungere dei punti di interruzione che permettono di specificare il punto preciso in cui si vuole interrompere l'esecuzione del flusso

- la possibilità di impostare il ritardo di esecuzione che permette di definire un tempo di attesa da inserire in seguito all'esecuzione di ogni azione.

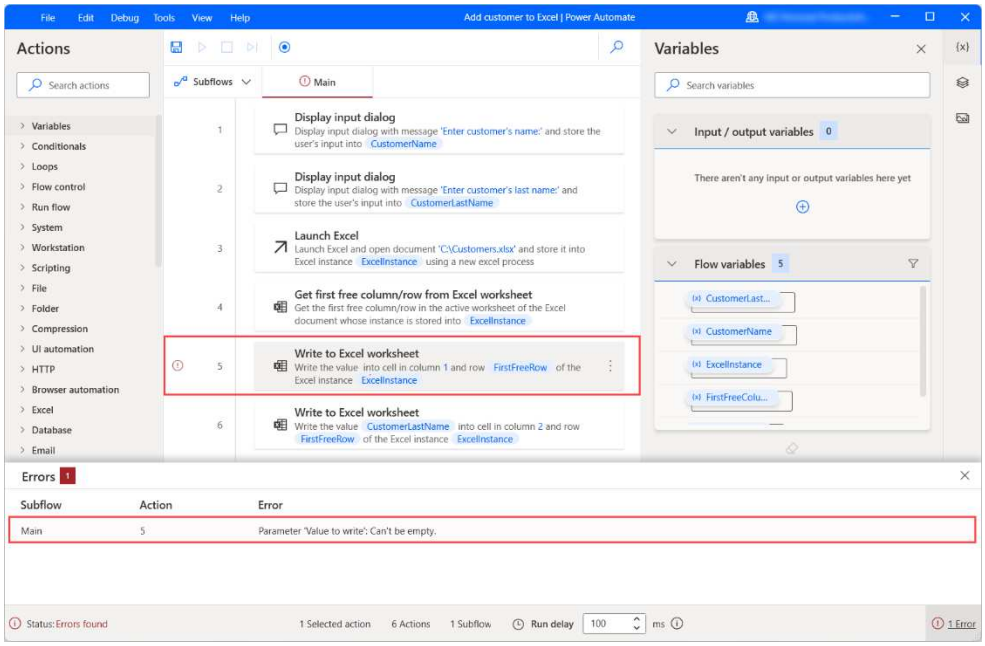

Figura 11. Riquadro degli errori

Vantaggi

Il primo vantaggio di Power Automate risiede nel software intuitivo e semplice da utilizzare che permette di simulare i movimenti del mouse e la digitazione da tastiera creando un'automazione veloce e sicura e aumentando la produttività.
Il secondo vantaggio riguarda la possibilità di utilizzare dei modelli predefiniti per semplificare ancor di più la creazione dell'automazione.
Inoltre, per la configurazione del flusso non è necessario che gli utenti conoscano i linguaggi di programmazione.
Un altro vantaggio riguarda la possibilità di avere accesso alle informazioni da qualunque dispositivo in quanto è una soluzione cloud di Microsoft.
Il vantaggio più grande consiste nella possibilità di condivisione del flusso con altri utenti all'interno dell'organizzazione in modo che anche loro possano utilizzare l'automazione creata.

Svantaggi

Il primo svantaggio ha a che fare con la compatibilità delle versioni di Power Automate.
I flussi creati con versioni precedenti alla versione Desktop 2.14 non possono essere aperti o eseguiti.
Il secondo svantaggio riguarda il registratore che potrebbe non registrate tutte le azioni che passano attraverso il menu Start di Windows o la tool bar, effettuare il click in un posto sbagliato durante l'esecuzione o effettuare il click del tasto destro in posto sbagliato durante l'esecuzione.
Un altro svantaggio riguarda alcune azioni svolte attraverso l'utilizzo di una finestra Remote Desktop Protocol (RDP).

Conclusioni

Uno degli aspetti fondamentali all'interno di un team è la possibilità di collaborazione. Utilizzando Power Automate oltre alla possibilità di automatizzare le azioni svolte all'interno del test plan di certificazione, è anche possibile condividere il flusso desktop creato in modo che questo possa essere modificato dagli altri componenti del team anche durante l'implementazione e soprattutto può essere eseguito dagli altri componenti del team DLP.

Inoltre, per poter utilizzare Power Automate occorre solo una connessione alla rete e l'inserimento delle credenziali il che permette di poter eseguire il processo sviluppato su tutte le macchine di test.

Capitolo 4

4. Contesto Applicativo

In questo capitolo si approfondirà il contesto applicativo e si documenterà il lavoro svolto per il progetto di tesi.
Per iniziare si descriverà nel dettaglio la soluzione implementata a partire dall'installazione del tool, Teamcenter, per poi passare allo studio dei processi generati all'avvio dell'applicazione.
Successivamente si analizzeranno tutte le operazioni di download, salvataggio ed export che si possono eseguire dall'applicazione per generare i file sensibili e si passerà poi alla ricerca degli elementi robusti presenti nell'interfaccia utente del software da automatizzare al fine di trovare degli elementi che restino invariati al cambiare delle versioni.
Infine, si descriverà il processo di automazione implementato attraverso l'utilizzo dei due software Macro Recorder e Power Automate.

4.1 Architettura del lavoro svolto

Dopo aver compreso il processo di certificazione dei tool attualmente adottato, è stato analizzato il problema legato all'attività da svolgere per capire il tipo di approccio da utilizzare per risolverlo sfruttando l'automazione dei test.
Come già detto nel capitolo precedente i Non Regression Test sono svolti manualmente dal team Data Loss Prevention il che provoca un problema legato all'effort manuale che questa attività comporta sia in termini di tempo impiegato sia per la probabilità d'errore umano.
Questo effort può essere ridotto notevolmente sfruttando le funzionalità di un tool già esistente in commercio per ripetere in modo automatico le operazioni quotidianamente svolte dagli utenti dell'organizzazione al fine di automatizzare l'intero processo.

Le azioni da dover ripetere e automatizzare sono già presenti all'interno del test plan precedentemente creato durante il processo di certificazione e validazione delle regole della versione precedente dell'applicazione per cui effettuare i Non Regression Test.
Per poter procedere, oltre allo studio, l'analisi e la scelta dei due tool per la scrittura e la gestione dei test automatici occorre analizzare nel dettaglio l'applicazione oggetto di test con particolare attenzione alle operazioni di salvataggio, export e stampa dei file e alle caratteristiche dei file generati a partire da tutte le possibili estensioni.
Un'altra importante analisi da effettuare è quella che riguarda l'interfaccia utente dell'applicazione da certificare con l'obiettivo di trovare degli elementi robusti da poter utilizzare per l'automazione al fine di evitare che nel passaggio tra una versione e la successiva si debbano apportare modifiche all'automazione.
Dopo aver ottenuto tutte le informazioni necessarie è possibile passare alla fase di sviluppo e implementazione dell'automazione attraverso Macro Recorder e Power Automate.

4.2 Teamcenter

L'applicazione utilizzata dai dipendenti dell'organizzazione e oggetto di tesi è Teamcenter nella versione 12.
Teamcenter è un'applicazione di Siemens Digital Industries Software ed è un sistema Product Lifecycle Management (PLM) per la gestione del ciclo di vita dei prodotti.
Il software utilizza un approccio integrato alle soluzioni CAD come Catia di Dassault e Creo Element di Parametric Technology Corportation, che sarà utilizzato per uno dei test del processo di certificazione.
L'applicazione è in grado di gestire tutte gli aspetti legati alla vita del prodotto quali: creazione, produzione, installazione, manutenzione, ritiro e smaltimento.
Teamcenter permette ai dipendenti dell'organizzazione di poter collaborare al processo di sviluppo del prodotto in modo da poter sfruttare le informazioni di più aree e presenta un'interfaccia di semplice utilizzo.
Per poter effettuare i Non Regression Test come prima cosa occorre richiedere l'installazione del pacchetto di installazione del programma Teamcenter al team di Information and Communication Technologies (ICT) di competenza e contestualmente richiedere l'abilitazione dell'utenza per poter effettuare l'accesso.

Analisi dei processi

Il primo passo per poter implementare delle regole di classificazione efficaci per il tool è quello di analizzare quali sono i processi in esecuzione in seguito all'avvio di Teamcenter e come sono strutturati.
Per farlo viene utilizzato il programma Process Explorer che permette di visualizzare i processi attivi e tutte le attività in esecuzione sul sistema e fornisce le informazioni riguardo il nome del processo, il PID (Process Identifier), CPU in uso e una breve descrizione.
Come visibile in figura 12 i processi in esecuzione sono:

- Teamcenter.exe
- Javaw.exe
- Cmd.exe

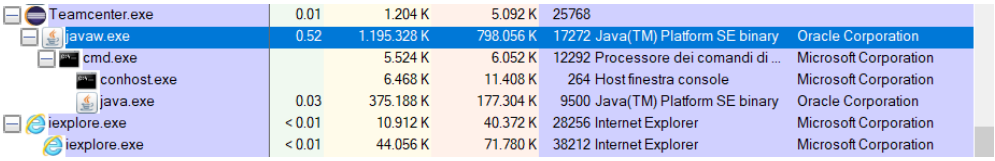

Figura 12. Processi Process Explorer

Analizzando quindi l'albero dei processi il processo padre è Teamcenter.exe che ha come processo figlio javaw.exe e cmd.exe.
Questa prima verifica è fondamentale in quanto per poter scrivere una regola efficace il primo passo è quello di andare a identificare il processo in esecuzione attraverso il quale saranno generati i file sensibili.
Come visto nel capitolo 2, la scrittura di una regola inizia dalla definizione dell'operazione da effettuare, che in questo caso è rappresentata da un'operazione di Start per cui il primo blocco dal basso sarà:

```
<equal>
        <evtOperationType/>
        <constOpAppStart/>
</equal>
```

In seguito all'operazione di avvio, il blocco successivo servirà per la verifica del processo che viene avviato.

Questa verifica avviene attraverso l'utilizzo del nome del processo che viene definito all'interno del blocco attraverso l'utilizzo di una variabile di tipo "string".

Considerando come esempio solo il processo padre, il secondo blocco sarà:

```
<equal>
        <curProcessImageName/>
        <string value="teamcenter.exe"/>
</equal>
```

Il numero di blocchi contenenti i processi sarà pari a quello del processo padre più il numero di processi figli attualmente in esecuzione.

Per questo motivo occorre prestare particolare attenzione al diagramma ad albero visualizzato mediante l'utilizzo del programma Process Explorer.

Un altro processo in esecuzione in seguito all'avvio di Teamcenter è il processo iexplore.exe necessario per inserire le credenziali di accesso, autenticare l'utente ed effettuare il login per poter accedere all'applicazione.

Terminata la procedura di autenticazione se l'utente avrà effettuato correttamente il login si potrà chiudere la pagina web utilizzata e si aprirà automaticamente l'interfaccia utente del programma Teamcenter, visibile in figura 13.

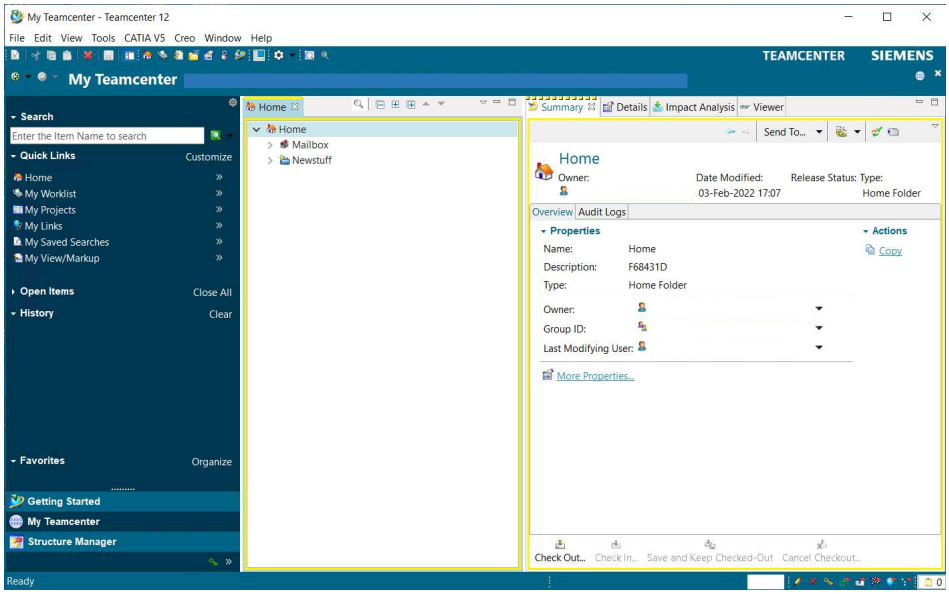

Figura 13. Interfaccia Utente TeamCenter 12

Un'ulteriore verifica è quella relativa all'analisi del processo che esegue l'operazione di File Write sul file generato da Teamcenter nel momento in cui viene effettuata l'operazione di download.
Per effettuare questa verifica è stato utilizzato dapprima il programma Process Explorer che evidenzia il processo figlio java.exe sotto Teamcenter.exe e in seguito il programma Process Monitor in quanto fornisce dei maggiori dettagli visibili in figura 14:

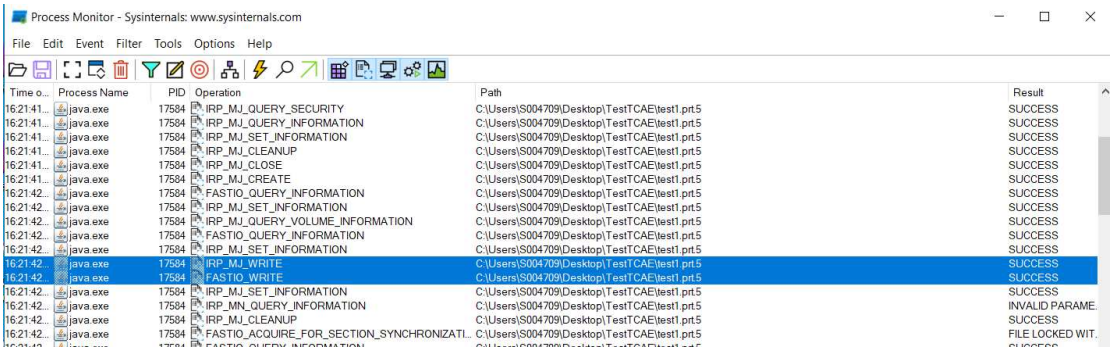

Figura 14. File Write Process Monitor

Studio dell'interfaccia

Il primo obiettivo è quello di analizzare nel dettaglio l'interfaccia utente del programma in modo tale da capire attraverso quali operazioni è possibile scaricare, esportare o stampare i file sensibili che possono essere generati dagli utenti e per ognuna di queste azioni verificare le possibili estensioni che possono essere attribuite al file.
L'applicazione come già anticipato utilizza un approccio integrato alla soluzione CREO attraverso la quale è possibile effettuare delle ulteriori operazioni di export che saranno oggetto di test e fornisce inoltre la funzionalità di visualizzazione e mockup digitale sfruttando Teamcenter Lifecycle Visualization.
Per effettuare gli NRT per prima cosa occorre verificare se sono presenti delle nuove funzionalità. Per farlo è possibile chiedere supporto all'Application Owner o sfruttare il test plan utilizzato per la certificazione della versione precedente del tool.
Successivamente si devono ripetere le operazioni descritte nel test plan e automatizzare le azioni con i due tool scelti.

4.3 Test con Power Automate

Il primo tool utilizzato per automatizzare i Non Regression Test da eseguire durante il processo di certificazione è Microsoft Power Automate.

Per utilizzare Power Automate la prima cosa da fare è accedere alla pagina web Power Automate [10] con le credenziali di accesso e selezionare l'ambiente da utilizzare.

In questo caso è stato utilizzato l'ambiente predefinito, creato automaticamente dal sistema.

Dopo aver scelto l'ambiente e quindi lo spazio in cui condividere, archiviare e gestire i dati aziendali è possibile scegliere il tipo di flusso più adatto da utilizzare per il progetto, in questo caso "Flussi Desktop".

A questo punto per creare e lavorare sul flusso desktop scelto occorre installare l'applicazione Power Automate Desktop, per cui dopo aver effettuato l'accesso alla pagina web Power Automate, si deve scegliere dal menu "Flussi Personali", "Flusso Desktop" e installare il tool.

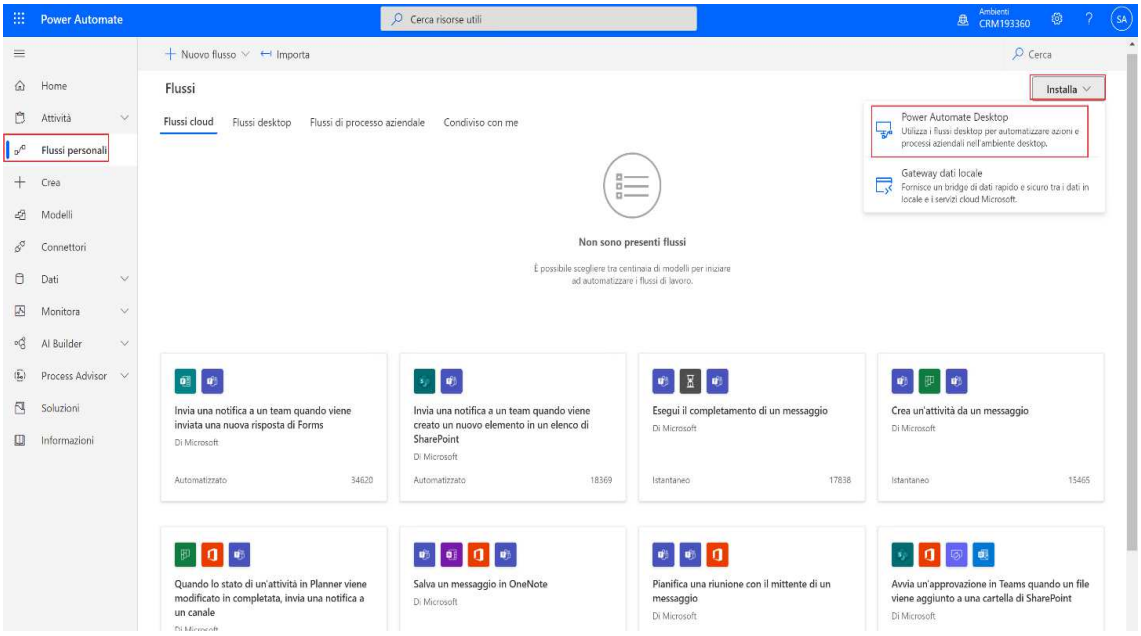

Figura 15. Flussi Personali Power Automate

Il primo passaggio successivo all'installazione di Microsoft Power Automate sulla macchina di test è quello di configurazione per l'autenticazione del proxy di rete.

Per configurare correttamente le impostazioni proxy sono stati modificati due file di configurazione dell'applicazione quali:

- PAD.Console.Host.exe.config,
- PAD.Designer.exe.config

All'interno di ognuno dei due file sono state stato inserite alla fine del codice, all'interno del nodo <configuration>, le seguenti righe di codice xml prese dalla pagina di supporto tecnico Microsoft [11]:

```
    </PAD.Console.Host.Properties.Settings>
  </userSettings>
        <system.net>
          <defaultProxy enabled="true" useDefaultCredentials="true">
          </defaultProxy>
      </system.net>
</configuration>
```

Figura 16. Configurazione proxy

Una volta terminata la configurazione del proxy è stato creato un nuovo flusso Desktop, la tipologia flusso che permette di automatizzare le attività sul desktop o sul Web.
Il flusso desktop creato è suddiviso in: Flusso principale (main) e flussi secondari.
Ognuno dei flussi secondari viene visualizzato in una nuova scheda e contiene un gruppo di azioni che definisce i vari test del test plan da automatizzare e le operazioni comuni come il login, la ricerca dell'item e le operazioni svolte attraverso l'utilizzo del DGCIApp.
Questi flussi secondari sono poi richiamati attraverso l'azione "Esegui Flusso Secondario" all'interno della scheda del flusso principale.
Oltre che per la semplice esecuzione di azioni di test il flusso secondario viene utilizzato anche per la gestione dell'errore.
Questa possibilità è molto utile in quanto permette di far in modo che se anche un'azione dovesse generare un errore, il flusso principale quindi non sarà interrotto ma sarà eseguito un flusso secondario che contiene delle azioni utili a gestire l'errore e procedere con l'esecuzione generale.

4.4 Analisi del flusso desktop

La creazione del flusso desktop inizia con la creazione del flusso principale (main) che contiene alcune operazioni comuni per l'automazione di tutti i test presenti nel test plan come la creazione della cartella dove salvare i file sensibili generati tramite l'applicazione, l'operazione di login, l'esecuzione dei vari eseguibili necessari per effettuare le operazioni di test, più le operazioni necessarie per richiamare ed eseguire i flussi secondari.

Per aggiungere le varie azioni al flusso è necessario selezionare l'azione da svolgere all'interno del menu presente nell'applicazione Power Automate Desktop e trascinarla all'interno del flusso su cui si vuole aggiungere l'operazione.

Le azioni presenti all'interno del flusso principale sono:

- Creazione cartella TestTCAE
- Esecuzione applicazioni DGCIApp, CREO e Teamcenter
- Esecuzione del flusso secondario Login
- Esecuzione del flusso secondario Research
- Esecuzione del flusso secondario Download PRT file
- Esecuzione del flusso secondario PLMXML
- Esecuzione del flusso secondario CREOButton
- Esecuzione del flusso secondario CREOClick
- Esecuzione del flusso secondario LifeCycle
- Esecuzione del flusso secondario DGCIApp

<u>Creazione cartella TestTCAE</u>

Per verificare la classificazione dei file generati dall'applicazione Teamcenter si devono verificare singolarmente tutti i file salvati o esportati dal tool.
La prima operazione effettuata tramite Power Automate prevede la creazione di una cartella all'interno della quale salvare tutti i file generati durante i test.
Prima di procedere con la creazione è stata inserita l'azione "Ottieni Cartella Speciale", questa operazione è necessaria in quanto come specificato nel capitolo 3 i test sono

effettuati attraverso l'utilizzo di una macchina di laboratorio configurata con le stesse policy applicate sulle macchine degli utenti in perimetro.
La macchina di test è accessibile mediante l'utilizzo dell'utenza personale di ognuno dei membri del team Data Loss Prevention o attraverso l'utilizzo dell'utenza condivisa con tutto il team che ha i permessi di amministratore.
L'operazione di creazione della cartella speciale permette di creare una variabile di flusso chiamata %SpecialFolderPath% che può essere richiamata tutte le volte che è necessario utilizzare il percorso desktop specificato indipendentemente dall'utente che esegue il flusso.
Successivamente è stata utilizzata l'operazione "Crea Cartella" che permette di creare una variabile %NewFolder% che contiene i parametri relativi al percorso dove si vuole creare la cartella.
I due parametri da inserire sono il path che sarà inserito utilizzando la variabile %SpecialFolderPath% precedentemente creata, e il nome della cartella.
Anche il nome della cartella verrà inserito attraverso l'utilizzo di una variabile di input di tipo string definita %Folder%.

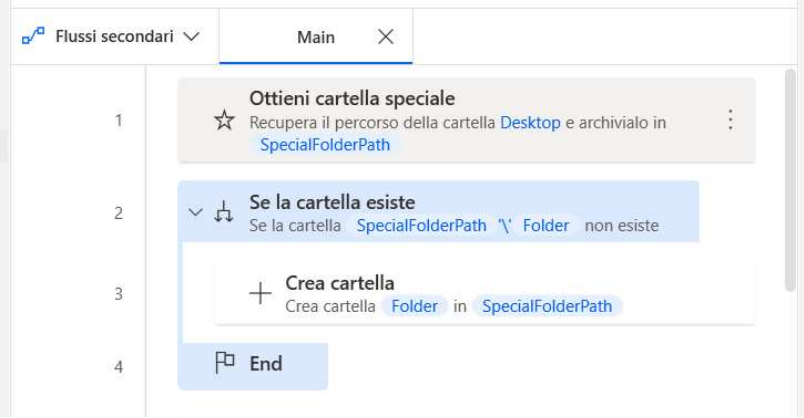

Figura 17. Blocco condizionale Creazione Cartella

L'operazione di creazione, visibile in figura 17, è stata inoltre inserita all'interno di un blocco condizionale di azioni a seconda che la cartella esista o meno per cui qualora la cartella non esistesse verrà creata, altrimenti si passerà all'operazione successiva.

Esecuzione applicazioni CREO, DGCIApp e Teamcenter

Le tre operazioni successive servono per eseguire le applicazioni necessarie per la certificazione quali:

- CREO, che sarà utilizzato per svolgere due delle azioni di test presenti all'interno del test plan,
- DGCIApp, che servirà per verificare se i file esportati sono correttamente classificati attraverso la verifica del tag di classificazione,
- Teamcenter.

Queste tre azioni sono aggiunte all'interno del flusso principale sfruttando l'azione "Esegui Applicazioni" presente all'interno del menù "Sistema" e anche in questo caso sarà necessario specificare il percorso applicazione.

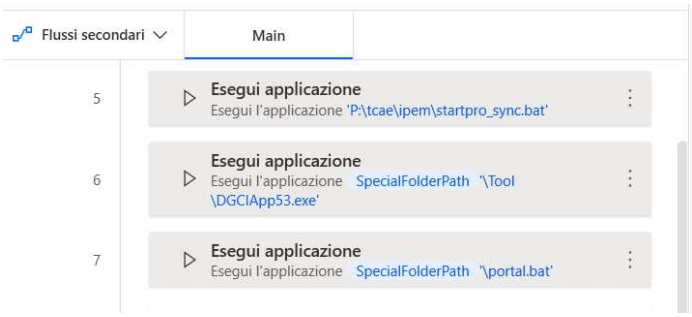

Figura 18. Esecuzione applicazioni

Esecuzione Flusso secondario Login

Come anticipato durante l'analisi dei processi generati all'avvio di Teamcenter, eseguendo l'applicazione Teamcenter.exe viene avviato anche il processo iexplore.exe che rimanda ad una pagina web per l'autenticazione dell'utenza.
L'operazione di Login viene gestita attraverso un flusso secondario chiamato appunto "Login" che attende un intervallo di tempo di dieci secondi in attesa che sia visualizzata la pagina web.

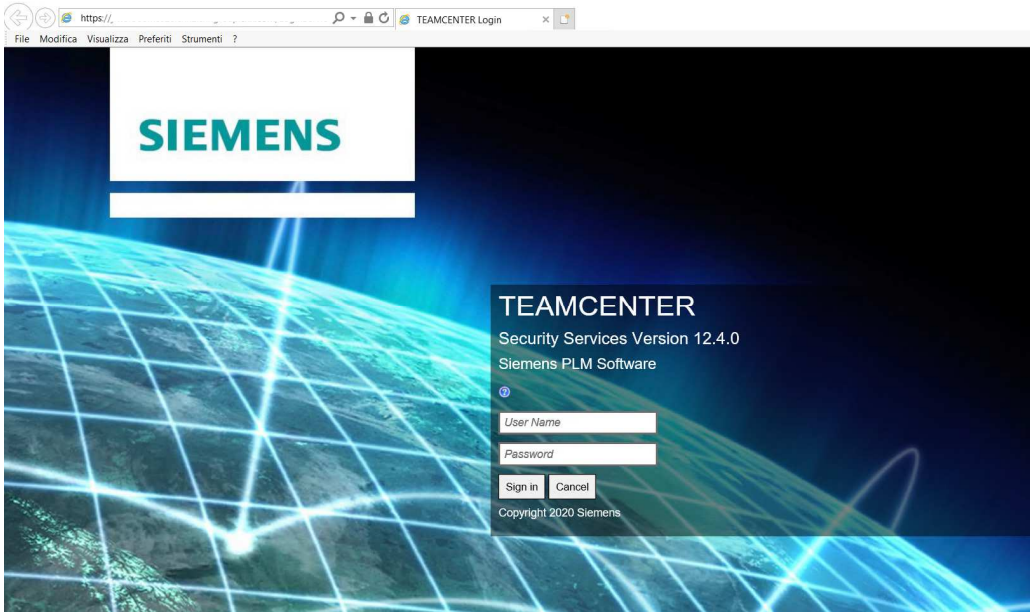

Figura 19. Pagina Login

In seguito, è stata inserita l'operazione "Avvia nuovo Internet Explorer" presente all'interno del menù "Automazione browser" che crea un collegamento con una scheda Internet Explorer con il titolo TEAMCENTER Login, archivia l'istanza all'interno della variabile %Browser% e sospende il flusso fino a quando non viene visualizzato un elemento specifico all'interno della pagina.

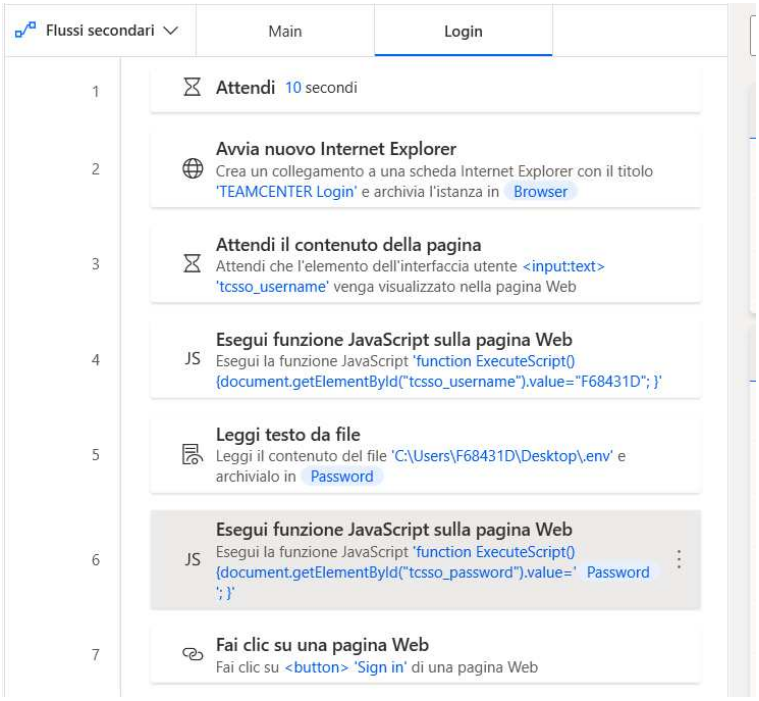

Figura 20. Flusso Secondario Login

L'elemento di attesa per la pagina web è il campo di testo all'interno del quale inserire lo username per l'autenticazione.
Per compilare in modo automatico i due campi di testo della pagina web con l'inserimento di username e password dell'utente è stata utilizzata l'operazione "Esegui funzione JavaScript sulla pagina Web".
Questa operazione necessita dei parametri:

- Istanza Web Browser, all'interno della quale sarà inserita la variabile %Browser% precedentemente creata,
- Funzione JavaScript, cioè la funzione da eseguire sulla pagina Web.

La funzione JavaScript utilizzata per l'inserimento dello username è:

```
function ExecuteScript()
{document.getElementById("tcsso_username").value="Username"; }
```

in cui tcsso_username è l'elemento della pagina web all'interno del quale inserire lo username dell'utenza abilitata per l'applicazione Teamcenter.
La funzione JavaScript utilizzata per l'inserimento della password è invece:

```
function ExecuteScript()
{document.getElementById("tcsso_password").value=%Password%; }
```

in cui tsso_password è l'elemento della pagina web all'interno del quale inserire la password dell'utenza abilitata per l'applicazione Teamcenter.
In questo caso la password non è inserita manualmente all'interno della funzione ma è inserita attraverso una variabile prodotta dall'operazione "Leggi Testo da file".
Infine, una volta inserite le credenziali per l'autenticazione, il flusso secondario di login termina con il click sul bottone "Sign in" presente nella pagina web.
Questo flusso viene eseguito dal flusso principale in seguito all'esecuzione delle applicazioni.

Esecuzione Flusso secondario Research

Il processo di certificazione simula le azioni svolte dai dipendenti dell'azienda, per cui non prevede la creazione di un nuovo progetto da parte del team Data Loss Prevention ma per poter procedere con le varie operazioni di salvataggio, export e stampa è stato fornito un gruppo di progetti di test definiti "Item", già precedentemente creati.
La prossima operazione dell'automazione, gestita attraverso il flusso secondario Research è quindi un'operazione di ricerca dell'item a partire dal nome.
Anche in questo caso la prima operazione del flusso secondario è un'operazione di attesa con lo scopo di attendere la completa visualizzazione dell'interfaccia utente del programma Teamcenter.
L'operazione di attesa è gestita mediante l'azione "Attendi contenuto Finestra" che serve per attendere che l'elemento dell'interfaccia utente Research:Search Item, cioè la barra di ricerca in cui inserire il nome dell'item, sia visualizzata per poi procedere con l'inserimento dell'ItemName e del tasto Enter (Return) per terminare la ricerca dell'elemento e visualizzare il progetto da esportare.
La modalità di ricerca è rimasta invariata rispetto alla versione precedente di Teamcenter per cui per gestirla il nome dell'item è stato definito attraverso una variabile di input di tipo String chiamata appunto %ItemName%.

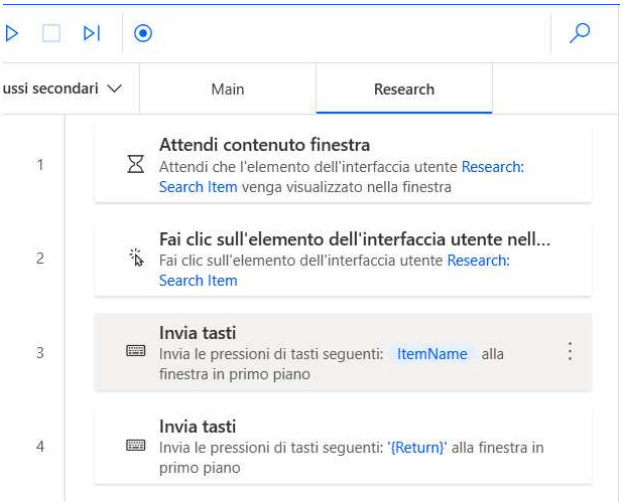

Figura 21. Flusso Secondario Research

Esecuzione Flusso secondario DownloadPRTFile

Con l'esecuzione del flusso secondario Research, termina l'esecuzione dei flussi iniziali e si può proseguire con la prima operazione di download dei file sensibili.
Questa prima operazione di download genererà un file con estensione "prt".
Il flusso secondario inizia con l'azione di click con il tasto destro sull'elemento dell'interfaccia utente Item di cui si vuole effettuare il download, si attende che sia visualizzato il menu nella finestra e si sceglie l'opzione desiderata.
Una volta selezionata l'opzione Named References si attende il contenuto della finestra attraverso cui scegliere l'estensione da attribuire al file ed effettuare l'operazione di Download.
Per la selezione dell'estensione e il click sul button di Download ho scelto di utilizzare l'azione sposta il mouse sul testo nella schermata (OCR).
Questa scelta è dovuta dal fatto che il nome dell'estensione del file così come il testo relativo all'operazione di Download sono spesso presenti nella finestra generata per cui possono essere considerati degli elementi robusti da utilizzare anche per le certificazioni successive.
Una volta effettuato il click sul button di Download si seleziona la scheda generata da Windows per il Download del file, si utilizzano nuovamente le operazioni OCR per selezionare il path dove salvare il file per cui si seleziona prima il Desktop, poi la cartella attraverso l'uso della variabile %Folder% precedentemente definita, in seguito si effettua il click sul button di Download e infine sul button Close.
Nell'ultima operazione di OCR visibile in figura 23, è possibile notare la presenza di una gestione dell'errore.
Gli errori devono essere gestiti mediante un ulteriore flusso secondario per cui in questo caso specifico è gestito attraverso l'esecuzione del flusso secondario Overwrite.
Come regolare generale, il file sensibile generato in seguito all'operazione di Download, sarà salvato automaticamente con lo stesso nome dell'item seguito dall'estensione del file precedentemente scelto.
Qualora sia già stato salvato in precedenza un file con lo stesso nome, in seguito all'operazione di chiusura della finestra, si aprirà una nuova finestra che serve per avvisare l'utente e chiedere se si vuole sovrascrivere il file già esistente.
La scelta è quella di sovrascriverlo per cui si utilizzerà un'ulteriore operazione di OCR sul testo "Yes".
Terminate tutte le operazioni necessarie per il Download del file si può verificare se il file generato risulta classificato.

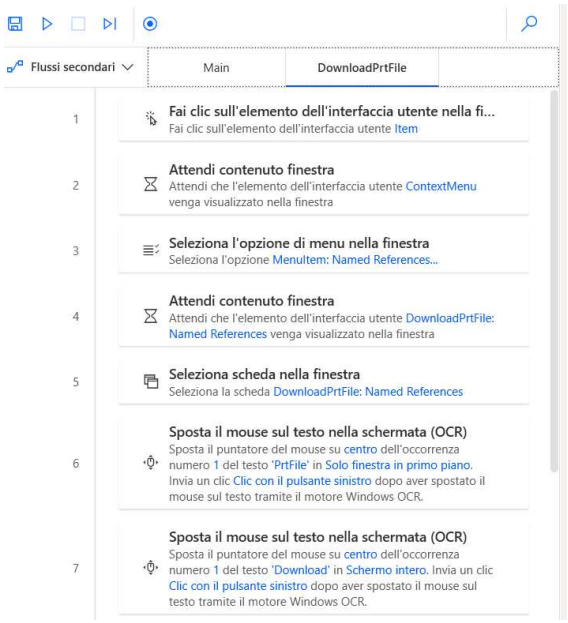

Figura 22. Flusso Secondario Research

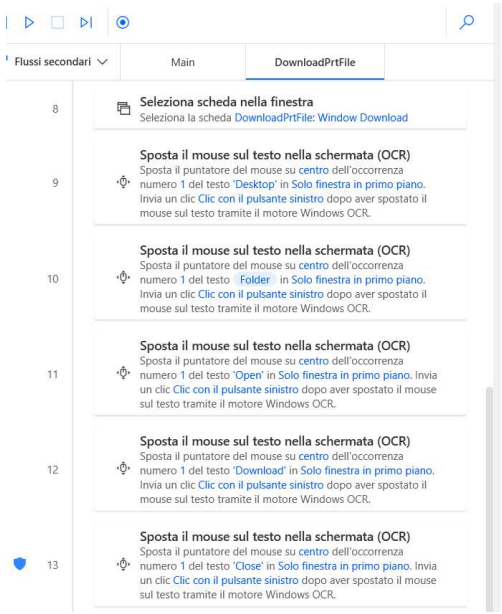

Figura 23. Flusso Secondario Research

Esecuzione Flusso secondario DGCIApp

All'interno del flusso principale (main), terminata l'esecuzione del flusso secondario DownloadPRTFile si dovrà procedere con l'esecuzione del flusso DGCIApp.

La sua esecuzione è inserita all'interno di un blocco condizionale di azioni a seconda che il file con estensione "prt" precedentemente generato e salvato nella cartella TestTCAE12 esista o meno.

Qualora il file non esistesse non si potrà effettuare alcuna verifica.

Se invece il file è stato correttamente salvato nella cartella %Folder% si passerà all'esecuzione del flusso secondario DGCIApp che selezionerà il file generato al termine del flusso secondario DownloadPRTFile e ci permetterà di verificare se le regole di classificazione funzionino correttamente attraverso la visualizzazione delle informazioni sul file.

In particolare, si verifica la presenza del tag di classificazione applicato al file e gli identificativi della regola e la policy associata.

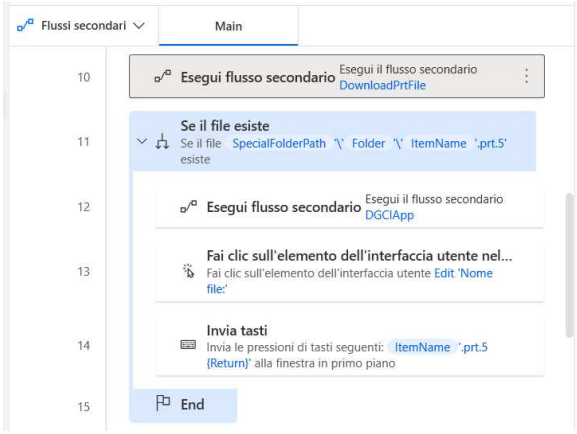

Figura 24. Flusso Secondario Research

Esecuzione Flusso secondario PLMXML

Il flusso secondario PLMXML si occupa dell'export del file in formato XML.
Anche in questo flusso sono state utilizzate le operazioni di attesa e selezione dell'elemento all'interno del menù fino ad arrivare al click sull'elemento dell'interfaccia utente PLMXML: Export Directory, all'inserimento attraverso l'uso delle variabili precedentemente create del path della cartella dove deve essere salvato il file.
Anche in questo caso è stata utilizzata l'operazione "Sposta il mouse sul testo nella schermata (OCR)" per selezionare il button "Download".
Il file generato al termine dell'esecuzione del flusso PLMXLM si chiamerà %ItemName%.xml.
Terminata l'esecuzione del flusso PLMXML nel flusso principale (main) si ripeteranno nuovamente le operazioni necessarie per la verifica dell'esistenza del file e qualora il file esista si procederà con l'esecuzione del flusso secondario DGCIApp per verificarne la classificazione.

Esecuzione Flusso secondario CreoButton

Come già anticipato all'inizio del capitolo Teamcenter utilizza un approccio integrato alle soluzioni CAD.
La soluzione utilizzata dagli utenti e oggetto di due test del test plan è Creo Element di Parametric Technology Corporation.
La prima modalità di export prevede cinque operazioni: la prima è l'operazione di click sull'elemento dell'interfaccia utente Item, la seconda è l'operazione di click sull'elemento

dell'interfaccia utente OpenCreo1: Send to Creo from Explorer ovvero un button con l'icona di Creo che apre la finestra utente del processo CREO.
A questo punto esegue il flusso secondario CREO, descritto successivamente, che sarà richiamato sia all'interno di questo flusso secondario che all'interno del flusso secondario CreoClick in quanto svolge azioni comuni per lo svolgimento di entrambi i test che richiedono l'utilizzo dell'applicazione CREO.
Infine, attraverso l'utilizzo dell'operazione "Invia Tasti" si rinomina il file che verrà salvato inserendo il valore precedentemente definito all'interno della variabile %ItemName% più "_CreoButton" per differenziare la modalità di export utilizzata per eseguire le azioni del test plan e attraverso l'azione "Fai click sull'elemento dell'interfaccia utente" si effettua il click per terminare il download del file.
Questo passaggio è importante in quanto l'estensione del file sarà la stessa sia per questo flusso secondario che per CreoClick.

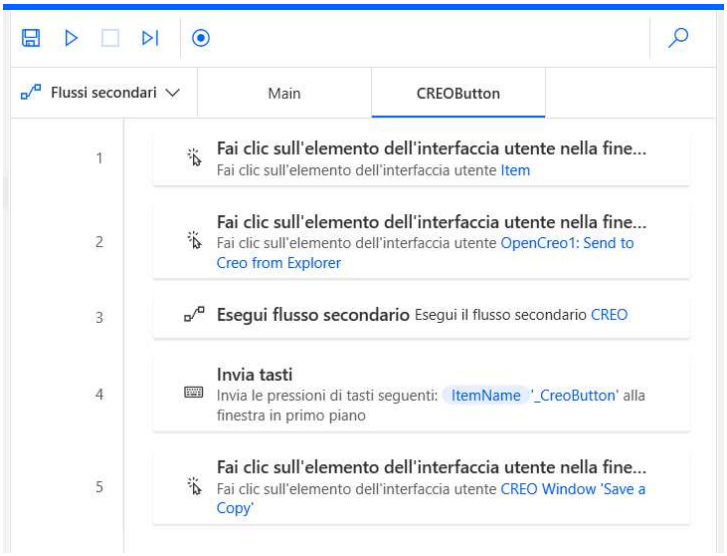

Figura 25. Flusso Secondario CREOButton

Esecuzione Flusso secondario CREOClick

Il flusso secondario CreoClick descrive le operazioni necessarie per eseguire il secondo export dei file attraverso l'uso dell'applicazione CREO.
Anche questo flusso secondario presenta cinque operazioni.
La prima è quella di clic, in questo caso specifico doppio clic, sull'elemento dell'interfaccia utente Item, in seguito al doppio clic sarà mostrata una nuova finestra

utente all'interno della quale è necessario il clic sul testo "Yes" per poter procedere con l'apertura dell'applicazione CREO.
Questa seconda operazione è svolta attraverso l'utilizzo dell'azione "sposta il mouse su testo nella schermata (OCR)".
Successivamente verrà eseguito il flusso secondario CREO per svolgere le azioni sull'interfaccia utente dell'applicazione CREO.
Infine, attraverso l'utilizzo dell'operazione "Invia Tasti" si rinomina il file che verrà salvato inserendo il valore precedentemente definito all'interno della variabile %ItemName% più "_CreoClick" per differenziare la modalità di export utilizzata per eseguire le azioni del test plan e attraverso l'azione "Fai click sull'elemento dell'interfaccia utente" si effettua il click per terminare il download del file.
Questo passaggio è importante in quanto l'estensione del file sarà la stessa sia per questo flusso secondario che per CreoButton.

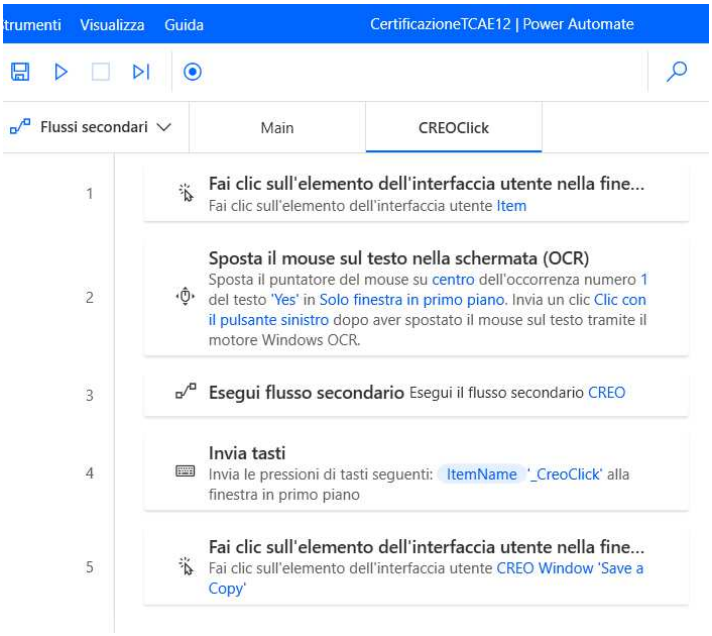

Figura 26. Flusso Secondario CREOClick

Esecuzione Flusso secondario CREO

Come anticipato nella descrizione dei due flussi secondari precedentemente analizzati, il flusso secondario CREO svolge delle operazioni comuni sia al flusso secondario CreoButton che al flusso secondario CreoClick.

Questo flusso secondario descrive le azioni da effettuare attraverso l'interfaccia utente dell'applicazione CREO, aperta attraverso l'operazione "Esegui applicazione" in una delle prime operazioni del flusso principale precedentemente descritta e richiamata in seguito al click sul button "Send to CREO from Explorer" effettuato nel flusso secondario CreoButton o attraverso il doppio click sull'elemento Item effettuato nel flusso secondario CreoClick.

La prima operazione del flusso è quella di attesa per far si che l'interfaccia utente di Creo sia visualizzata correttamente, in seguito si effettua il clic sull'elemento dell'interfaccia utente CREO Windows per aprire l'Item selezionato e il click su File nel menu di Creo per visualizzare le operazioni di salvataggio.

A questo punto attraverso l'utilizzo dell'azione "Sposta il mouse sul testo nella schermata (OCR)" si effettua il click su "Save As" e "Save a Copy" e si effettua il click sulla finestra per poter inserire il path della cartella dove deve essere salvato il file.

Infine, si procede con il click sull'elemento dell'interfaccia utente della finestra per salvare una copia del file nel percorso desiderato.

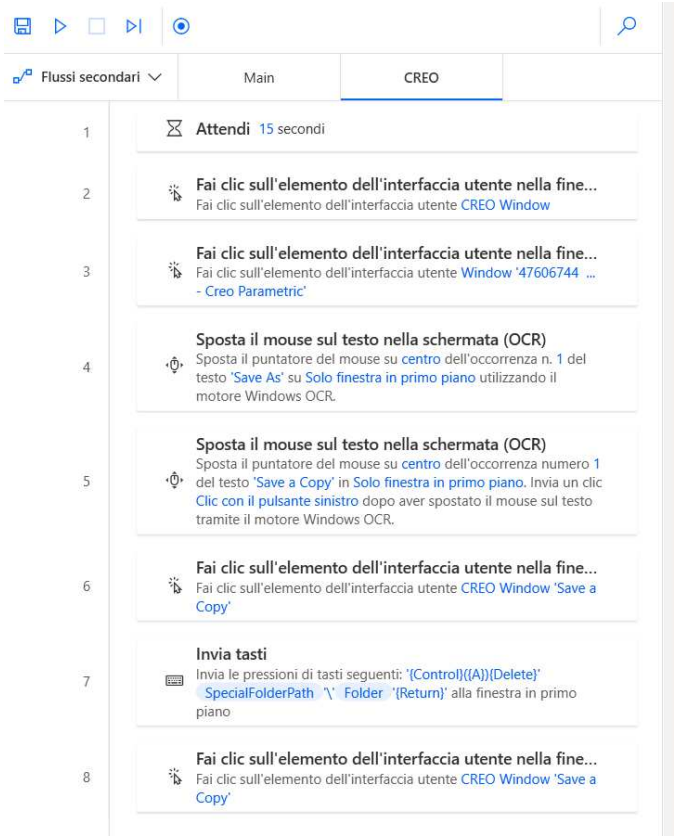

Figura 27. Flusso Secondario CREOClick

Al termine dell'esecuzione del flusso secondario CreoButton e del flusso secondario CreoClick si procederà con l'esecuzione del flusso secondario DGCIApp per verificare che i file sensibili precedentemente salvati si trovino all'interno della cartella TestTCAE e siano correttamente classificati.

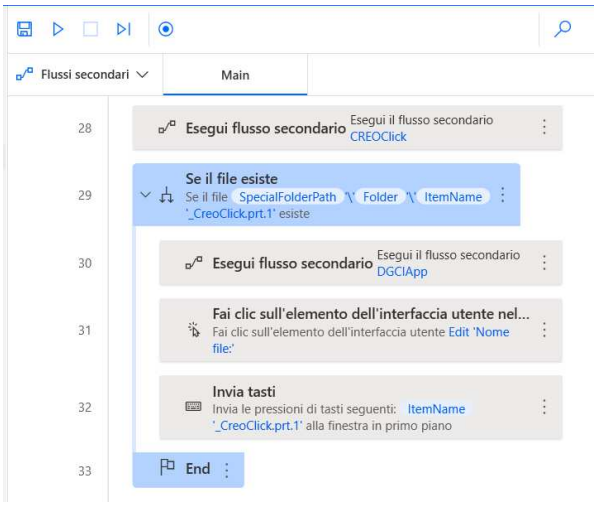

Figura 28. Flusso Secondario DGCIApp

Esecuzione Flusso secondario Lifecycle

L'ultimo test presente nel test plan è quello che prevede l'utilizzo di Lifecycle Visualization cioè una funzionalità di visualizzazione e mockup digitale del progetto creato.

In questo caso la prima operazione del flusso secondario non prevede il clic sull'elemento dell'interfaccia utente Item ma direttamente sull'elemento Lifecycle: Tree item cioè progetto che contiene l'item.

Successivamente, si effettua il clic sull'elemento dell'interfaccia utente Button 'Start/Open in Lifecycle Visualization' ovvero un button con l'icona di LifeCycle che apre la finestra del visualizzatore di Teamcenter.

Anche in questo caso è stata inserita un'operazione di attesa per fare sì che tutti gli elementi della finestra siano caricati correttamente prima di procedere con le operazioni necessarie per il download del file.

Terminata l'attesa attraverso l'utilizzo dell'azione "Sposta il mouse sul testo della finestra (OCR)" si effettua il click su "Menu", "File" e "Save As" e in seguito all'azione "Invia Tasti" per la modifica del nome con cui deve essere salvato il file si procede nuovamente con

l'utilizzo dell'OCR per selezionare la cartella dove salvare il file e terminare l'operazione di salvataggio.
Il file esportato avrà estensione: plmxml.
Anche in questo caso, al termine dell'esecuzione del flusso secondario si procederà con l'esecuzione del flusso secondario DGCIApp per verificare che i file sensibili precedentemente salvati si trovino all'interno della cartella TestTCAE e siano correttamente classificati.

4.5 Verifica regole di protezione

Dopo aver verificato che tutti i file generati dall'applicazione Teamcenter siano correttamente classificati e quindi dopo aver verificato l'efficacia delle regole di classificazione precedentemente implementate, è necessario verificare l'efficacia delle regole di protezione.
All'interno del test plan sono infatti presenti delle azioni da svolgere con i file classificati in modo da verificare che questi non siano condivisi con utenti non autorizzati, o divulgati volontariamente o involontariamente.
Alcuni dei possibili da test da effettuare con questi file sono:

- Rinominare l'estensione del file,
- Allegare il file via email,
- Effettuare l'upload del file su una Network Share Untrusted,
- Inviare il file via Teams,
- Copiare il file all'interno di un disco rimovibile.

Una volta effettuati i seguenti test tutte le azioni sopra elencate dovranno essere bloccate e dovrà apparire il prompt di Digital Guardian che chiede agli utenti di far riferimento alle linee guida sulla protezione della proprietà intellettuale dell'azienda.
Se le azioni saranno bloccate allora la certificazione sarà terminata, il test plan contenente le operazioni di export e di test per la verifica del blocco sarà inviato all'Application Owner dell'applicazione.
Infine, l'Application Owner ha il compito di individuare un gruppo ristretto di utenti che utilizza l'applicazione oggetto di certificazione, definito Key Users, che ha il compito di effettuare i test descritti all'interno del test plan e fornire un feedback al team Data Loss Prevention.

4.6 Test con Macro Recorder

Il secondo tool utilizzato per automatizzare i Non Regression Test è Macro Recorder. Macro Recorder è un software di automazione della Bartels Media GmbH che permette di registrare ed acquisire tutti i movimenti del mouse e della tastiera e creare delle macro per poi riprodurle.

Il primo passaggio per poter utilizzare il programma è quello di installarlo sulla macchina di test utilizzando l'utenza con i privilegi d'amministratore.

Dopo aver scaricato il pacchetto d'installazione dalla pagina web [12] di Macro Recorder basterà effettuare doppio clic sul file d'installazione e seguire le istruzioni presenti sullo schermo.

Infine, una volta terminata la procedura guidata basterà effettuare doppio click sull'icona del programma per poter avviare Macro Recorder.

Con l'utilizzo di Macro Recorder non c'è la possibilità di suddividere il flusso in flusso principale e flussi secondari ma le azioni devono essere svolte e poi successivamente eseguite in modo sequenziale.

Per quanto riguarda la creazione della cartella all'interno della quale salvare i file generati da Teamcenter le azioni da svolgere sono registrate mediante l'utilizzo delle azioni di click del mouse che registrano le coordinate x, y statiche e la pressione dei tasti per l'inserimento del nome della cartella.

Il tempo di attesa "Wait" presente in figura 29, è il tempo reale che ho impiegato per effettuare i click e l'inserimento del testo.

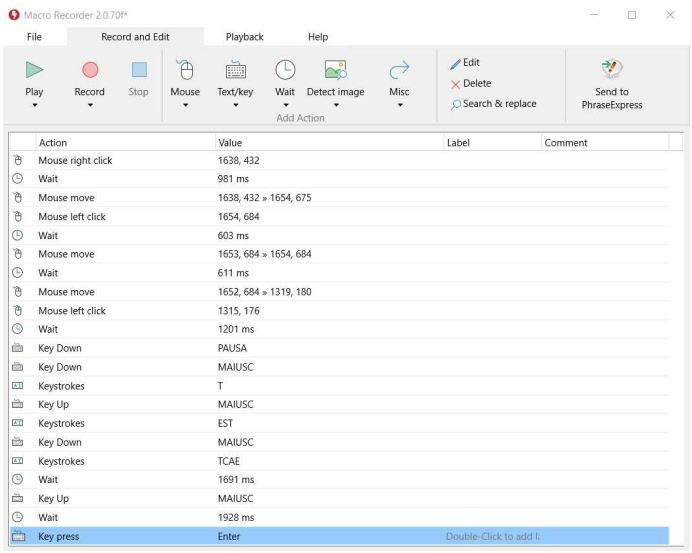

Figura 29. Flusso Secondario DGCIApp

Per quanto riguarda l'esecuzione dei programmi è presente una funzione di controllo "Esegui programma" che permette di inserire il path del programma da eseguire.
A questo punto per procedere con l'inserimento delle credenziali di autenticazione ed effettuare il login si utilizza la funzione trova immagine.
Questa funzione serve per sospendere la riproduzione e attendere che sia visualizzata l'immagine selezionata nella pagina web.
L'immagine selezionata può essere rilevata mediante uno screenshot o mediante un'immagine già precedentemente salvata sulla workstation.
In questo caso l'immagine presenta la scritta Teamcenter ed è stata rilevata attraverso uno screenshot effettuato sulla pagina web.

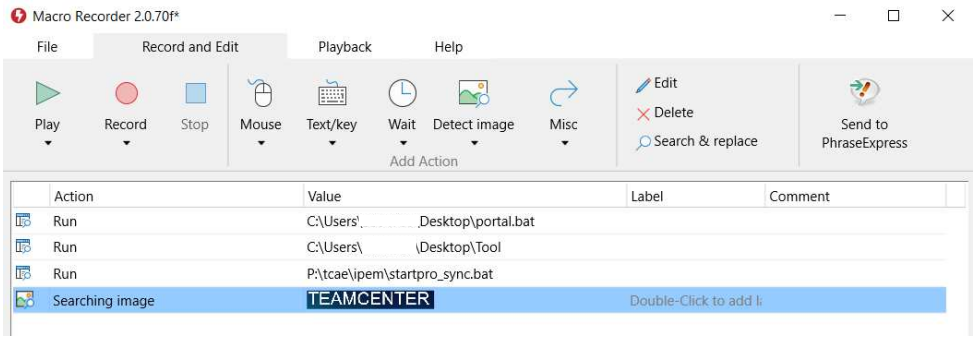

Figura 30. Esegui programma e Trova immagine

Una volta visualizzata l'immagine si può procedere con l'inserimento delle credenziali.
Per procedere con l'inserimento si utilizzano nuovamente le azioni di click del mouse che registrano le coordinate x, y statiche e la pressione dei tasti.
Dopo aver terminato la procedura di autenticazione si deve attendere che l'interfaccia utente di Teamcenter venga caricata correttamente per cui si procede con l'inserimento di un'ulteriore funzione trova immagine che in questo caso identifica la lente di ricerca dell'item.
Terminata l'attesa si possono iniziare ad eseguire i test del test plan.
Per quanto riguarda il download del file con estensione "prt" la prima operazione da effettuare è quella relativa al clic all'interno della barra di ricerca e attraverso l'utilizzo della pressione dei tasti si può procedere con l'inserimento del testo relativo al nome dell'item seguito dal tasto Invio su cui si vuole effettuare l'operazione di Download.
A questo punto si può procedere con il clic con il tasto destro sull'item e con il clic con il tasto sinistro sull'opzione del menu "Named References".
Quest'ultimo aprirà una nuova finestra generata dal processo javaw.exe che avrà un colore differente rispetto alle operazioni svolte nella finestra precedente e nelle

successive e attraverso l'utilizzo dell'OCR si procederà con la selezione dell'estensione del file di tipo PRT.

A questo punto il processo javaw.exe genererà un'ulteriore finestra all'interno della quale sarà utilizzato l'OCR per selezionare il percorso dove inserire il file e per effettuare l'operazione di Download.

Infine, si tornerà alla finestra precedente generata in seguito al clic su Named Reference che verrà chiusa attraverso l'utilizzo dell'OCR sul testo Close.

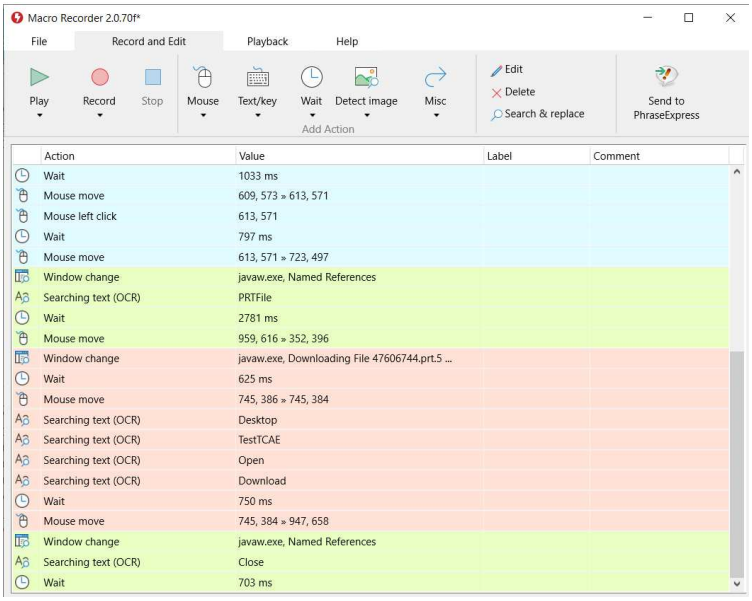

Figura 31. Cambio finestre javaw.exe

Terminata l'operazione di download si dovrà poi procedere con la verifica della classificazione del file.

Il programma DGCIApp è stato precedentemente eseguito per cui come prima operazione utilizzo il trova immagine per cliccare l'immagine della cartella e aprire la finestra dove inserire il path del file da verificare.

Successivamente, con il doppio click sull'icona della cartella TestTCAE apro la cartella dove ho memorizzato il file e copio il path completo.

Questo sarà poi incollato all'interno della finestra del DGCIApp per poter selezionare la cartella corretta e infine attraverso l'utilizzo dell'OCR seleziono il Testo contenente la parola Open e apro il file.

Se il file risulta correttamente classificato si devono eseguire le operazioni di verifica delle regole di protezione.

Allo stesso modo si devono svolgere tutte le operazioni di download generate attraverso CREO quindi entrambe le tipologie di export attraverso il button di creo presente nell'interfaccia utente di Teamcenter e attraverso il doppio clic sull'item.
Per l'automazione attraverso il Creo Button è stata utilizzata la funzione trova immagine sfruttando l'icona di Creo già presente all'interno dell'interfaccia utente di Teamcenter, successivamente è stata utilizzata la funzione OCR per selezionare ed effettuare il clic sul testo "Open", "Save As" e "Save a Copy".

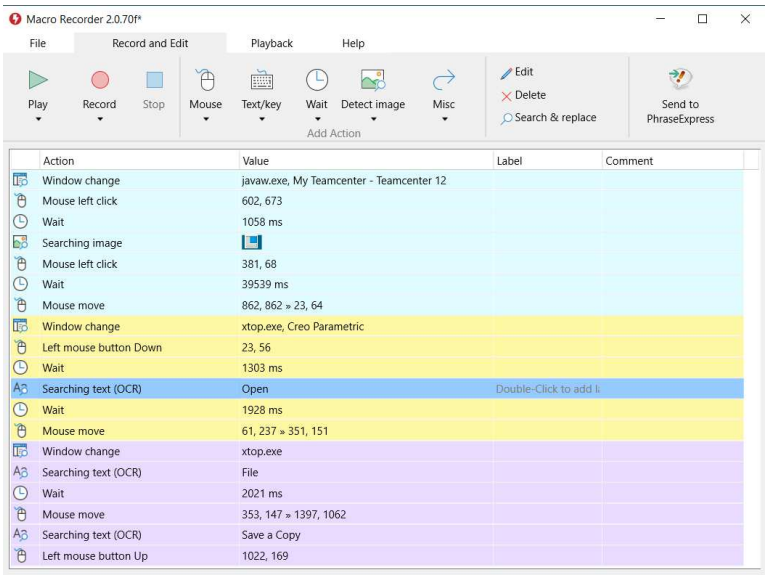

Figura 32. CreoButton

Infine, attraverso l'utilizzo delle funzionalità della tastiera è stato inserito il path della cartella all'interno della quale salvare il file sensibile generato e il nome del file da salvare in modo da poterlo distinguere dalla seconda modalità di export che sfrutta il processo creo.
Una volta terminato l'export si devono ripetere le azioni precedentemente svolte attraverso l'utilizzo del DGCIApp per verificare la classificazione del file generato ed effettuare l'operazione descritta nel test plan affinché si abbia la certezza che questa sia correttamente bloccata da Digital Guardian.
Allo stesso modo per la seconda modalità di export attraverso creo, dopo aver effettuato il doppio clic sull'item da salvare e aver utilizzato l'OCR per selezionare il testo "Yes" necessario per spostarsi all'interno della finestra di Creo, si ripetono le azioni precedentemente descritte per effettuare l'operazione di Save a Copy.
Infine, si inserisce il path della cartella TestTCAE e il nome del file in modo da differenziarlo da quello precedentemente salvato.

Anche in questo caso in seguito al salvataggio occorre verificare che il file sia correttamente classificato e che le regole di protezione siano efficaci.
L'ultima tipologia di download presente all'interno del test plan è quella attraverso l'utilizzo di Lifecycle Visualization.
Anche in questo caso la prima operazione è quella di clic ma non sull'item bensì sul progetto iniziale e successivamente si sfrutta la funzione trova immagine per selezionare e cliccare il button Lifecycle Visualization che permette di aprire il visualizzatore di Teamcenter.
A questo punto si sfruttano nuovamente le operazioni di clic del mouse e dell'OCR per selezionare il percorso della cartella dove salvare il file sensibile generato e si effettua il download.
Infine, si dovranno eseguire per l'ultima volta le operazioni necessarie per l'utilizzo del programma DGCIApp per verificare la corretta classificazione del file ed eseguire le azioni riportate nel test plan per la verifica delle regole di protezione.

Capitolo 5

5. Risultati del lavoro svolto

Il capitolo 5 contiene i risultati del lavoro svolto e quindi il confronto in seguito all'implementazione dell'automazione dei due tool, un'analisi dei benefici che può offrire la soluzione implementata e la scelta dell'automazione più adatta al contesto evidenziando i possibili sviluppi futuri per migliorare il processo di automazione dei test. L'obiettivo dell'automazione effettuata è quello di estendere la soluzione proposta anche per gli altri tool utilizzati all'interno dell'organizzazione in modo da diminuire l'effort manuale da parte del team Data Loss Prevention.

5.1 Confronto tra le implementazioni

Dopo aver studiato e utilizzato le funzionalità presenti in Macro Recorder e in Power Automate, adoperati per l'implementazione della soluzione, è possibile effettuare un confronto in termini di funzionalità ed efficienza tra i due e definire quale sia il più adatto per l'automazione dei Non Regression Test per l'organizzazione.
Analizziamo quindi nel dettaglio i vari step necessari per svolgere tutte le azioni presenti all'interno del test plan evidenziando le differenze in termine di implementazione.

Flusso di lavoro

Il primo confronto è quello relativo alla struttura del flusso per l'automazione.
Attraverso l'utilizzo di Power Automate è possibile suddividere il flusso in flusso principale (main) e flussi secondari, le azioni inoltre possono essere create, inserite e modificate in qualunque momento.
I flussi secondari contengono un gruppo di azioni che definisce le operazioni comuni e i vari test del test plan da eseguire.

I flussi secondari sono creati all'interno di nuove finestre e sono poi richiamati all'interno del flusso principale per poter essere eseguiti.
Servono inoltre per la gestione degli errori per far in modo che l'errore sia gestito senza l'interruzione del flusso principale.
Attraverso l'utilizzo di Macro Recorder non esiste la possibilità di suddividere il flusso se non attraverso la creazione di un numero di file pari al numero di test da voler svolgere.
Qualora si dovesse decidere di utilizzare un file unico con tutte le azioni presenti, questo avrà una dimensione di righe di funzioni troppo elevato, il tempo di esecuzione sarebbe quindi troppo variabile anche per i tempi di attesa necessari per la corretta esecuzione.
Per tutti i motivi appena elencati è possibile aggiungere che in generale c'è un'alta probabilità di errore durante l'esecuzione.
L'errore inoltre non è rilevato dal programma in fase di esecuzione e non esiste una visualizzazione che permette di identificarlo per cui l'automazione continuerebbe ad eseguire le azioni successive.
Sarà quindi compito di chi sta utilizzando il file con le operazioni registrate rendersi conto dell'errore e annullare l'intero flusso di esecuzione.
Le azioni inoltre devono essere registrate in modo sequenziale.
Non esiste la possibilità di registrare il desktop, interrompere la registrazione per aggiungere ad esempio le funzionalità di ricerca come quelle di immagine o testo (OCR) e poi riprenderla.
L'unico modo per poter manipolare le azioni registrate è quello di modificare o eliminare le azioni al termine della registrazione.

Creazione cartella TestTCAE

Per quanto riguarda l'analisi delle varie operazioni eseguite, la prima operazione consiste nella creazione della cartella TestTCAE all'interno della quale salvare tutti i file sensibili di cui è stato effettuato il download durante la fase di test.
Utilizzando Power Automate l'operazione di creazione della cartella è stata inserita all'interno di un flusso condizionale che eseguirà la funzione relativa alla creazione della cartella solo se questa non è già presente nel percorso specificato.
Qualora la cartella non sia già presente, insieme a questa, verrà creata una variabile che contiene il percorso e il nome della cartella.
Entrambe queste informazioni sono state inserite come parametro della funzione attraverso due variabili di input di tipo "string".
In particolare, la variabile utilizzata per specificare il percorso della cartella è il risultato dell'operazione ottieni cartella speciale inserita nel flusso prima del flusso condizionale

ed è necessaria per utilizzare il percorso desktop specificato indipendentemente dall'utente che esegue il flusso.
Questa operazione è fondamentale per il team DLP perché evita di effettuare delle modifiche relativa al path per ogni utenza personale o condivisa utilizzata per accedere alla macchina di test per eseguire il flusso.
Utilizzando invece Macro Recorder le azioni necessarie per la creazione della cartella sono semplici azioni di clic del mouse che registrano le coordinate x, y statiche e azioni di pressione dei tasti per l'inserimento del nome della cartella.
Non esiste la possibilità di inserire delle variabili di input per cui non è possibile tener traccia della stringa che specifica il percorso della cartella per poterla sfruttare successivamente.
Inoltre, non esiste alcun modo per verificare se la cartella di test è già stata creata per cui tutte le volte che verrà eseguita l'automazione proverà a crearla e qualora dovesse già esistere non terminerà l'operazione in quanto necessiterebbe di un'ulteriore azione di clic per confermare l'unione con la cartella con lo stesso nome precedentemente creata.

Esecuzione applicazioni CREO, DGCIApp e Teamcenter

Per quanto riguarda l'esecuzione delle applicazioni necessarie per svolgere i test non c'è alcuna differenza tra i due tool per l'automazione in quanto in entrambi i casi è presente una funzione per l'esecuzione dei processi all'interno della quale deve essere inserito come parametro il percorso specifico del programma.
Basterà quindi inserire il path relativo alla posizione dei programmi Teamcenter, Creo e DGCIApp.
Tuttavia, utilizzando Macro Recorder non esiste la possibilità di utilizzare una variabile che resti invariata e si adatti al contesto indipendentemente dall'utenza utilizzata per accedere alla workstation di test.
Il percorso relativo alla posizione in cui si trovano i tre programmi da mandare in esecuzione deve quindi essere modificato prima dell'esecuzione dell'automazione per poter essere adattato all'utente che vuole utilizzare il file.

Autenticazione e procedura di Login

L'operazione successiva all'esecuzione dei programmi è quella di autenticazione dell'utenza necessaria per terminare l'avvio di Teamcenter.
Questa operazione è stata gestita in Power Automate attraverso l'utilizzo del flusso secondario Login che attende un intervallo di tempo affinché sia terminato il caricamento della pagina web utilizzando un elemento dell'interfaccia utente e si occupa dell'inserimento delle credenziali dell'utente attraverso l'esecuzione di una funzione JavaScript che inserisce all'interno dell'elemento selezionato il valore dello username prima e della password dopo.
L'inserimento della password avviene mediante la lettura del testo all'interno di un file per fare in modo che non sia scritta direttamente all'interno del codice della funzione da eseguire.
L'operazione di login è invece gestita in Macro Recorder attraverso il cambio di pagina dovuto all'apertura del processo iexplore.exe, l'attesa indica il reale tempo di attesa affinché la pagina sia correttamente visualizzata.
Questo tempo non è però sempre uguale in quanto dipende dai parametri relativi alla connessione della workstation, serve quindi effettuare una stima e modificarlo al termine della registrazione delle azioni in modo da evitare che l'esecuzione continui anche senza aver terminato correttamente l'operazione precedente.
Per quanto riguarda invece l'inserimento delle credenziali dell'utenza si possono utilizzare solo le azioni di clic del mouse per individuare le coordinate del desktop dove si devono inserire e la pressione dei tasti per la digitazione dello username prima e della password dopo.
Questo significa che l'unico modo per poter inserire la password all'interno della pagina web consiste nella digitazione per cui il suo valore risulterà visibile all'interno delle azioni dell'automazione.
Al termine dell'autenticazione verrà avviato il programma e si potrà procedere con la ricerca dell'elemento che sarà oggetto di export.

Ricerca dell'item

L'operazione di ricerca è gestita in Power Automate attraverso l'implementazione del flusso secondario Research.
La prima operazione del flusso è nuovamente un'operazione di attesa dell'elemento dell'interfaccia utente rappresentato dalla barra di ricerca dove inserire il nome dell'item da cercare.
Successivamente si può procedere con l'inserimento del nome dell'item seguito dal tasto Enter per terminare la ricerca e visualizzare il progetto da esportare.
In questo caso, così come nel caso della creazione della cartella il nome dell'item è stato definito attraverso l'utilizzo di una variabile di input di tipo string.
Questo permette di poter riutilizzare la variabile in seguito e di velocizzare un'eventuale futura modifica qualora il nome dell'item dovesse cambiare.
Anche in Macro Recorder la prima operazione è un'operazione di attesa con lo scopo che l'interfaccia utente di Teamcenter sia correttamente caricata ma a differenza di Power Automate l'inserimento del nome dell'item da cercare è inserito mediante la memorizzazione del clic con il tasto sinistro all'interno della barra di ricerca e dalla successiva funzione di pressione tasti che serve per registrare il nome dell'item da cercare.

Download file con estensione prt

Terminata l'operazione di ricerca si passa alle operazioni di export del test plan.
La prima operazione è quella di download del file con estensione "prt".
Questa è stata gestita in Power Automate attraverso l'implementazione del flusso secondario DownloadPrtFile che inizia con l'azione di clic con il tasto destro sull'elemento dell'interfaccia utente Item e sfrutta l'azione Seleziona l'opzione di menu nella finestra per selezionare l'opzione all'interno del menu, necessaria per il download quale "Named References".
Inoltre, la scelta dell'estensione del file, della cartella dove questo deve essere memorizzato, e il clic sul tasto Download sono gestiti mediante l'utilizzo della funzione OCR.
Una delle differenze fondamentali con Macro Recorder consiste nella presenza all'interno del flusso di una gestione dell'errore relativa all'operazione di sovrascrittura del file.

Qualora all'interno della cartella selezionata dovesse esistere un file con lo stesso nome di quello appena attribuito, si eseguirà il flusso secondario Overwrite e il file già presente all'interno della cartella TestTCAE verrà sovrascritto.
Se non avessi inserito questa gestione Power Automate avrebbe interrotto il flusso principale in quanto avrebbe riscontrato un errore.
In Macro Recorder non esistono alcune funzionalità legate ai menu per cui le prime operazioni sono gestite interamente mediante le funzionalità del mouse.
Uno dei problemi che si può riscontrare attraverso la memorizzazione delle coordinate è quello relativo alla posizione in cui compare il menu dove selezionare l'azione.
Qualora la finestra di Teamcenter non sia a schermo intero, la posizione del menu che compare in seguito al clic sull'item da esportare può variare.
L'automazione, quindi, procederà e tenterà di svolgere le operazioni successive anche qualora l'operazione di clic sull'opzione "Named References" non dovesse andare a buon fine.
Se l'operazione precedente dovesse andare a buon fine, a partire dalla scelta dell'estensione del file si utilizzerà la ricerca del testo (OCR) come effettuato in Power Automate, la differenza consiste nell'inserimento del testo da cercare in quanto in Power Automate verranno utilizzate le variabili precedentemente create e nella gestione della sovrascrittura del file.
Con l'utilizzo di Macro Recorder qualora dovesse esistere all'interno della cartella TestTCAE un file con lo stesso nome di quello per cui stiamo effettuando l'operazione di Download questo non sarà sovrascritto e l'esecuzione non andrà a buon fine.
Inoltre, non esistendo una gestione dell'errore il flusso procederà con lo svolgimento dell'azione successiva senza che il file sia stato salvato.
L'unica soluzione potrebbe essere quella di dividere i vari file di automazione in modo da avere quello per la ricerca separato rispetto ai primi già elencati, far terminare l'esecuzione dell'automazione con la funzione di trova testo OCR relativa al testo "Download" e qualora all'interno della cartella TestTCAE esistesse un file con lo stesso nome, si procederà con l'operazione di sovrascrittura in modo manuale effettuando il clic necessario per terminare l'operazione di salvataggio.

Verifica della classificazione del file

Dopo aver salvato il file sensibile con estensione “prt” si dovrà procedere con la verifica dell’efficacia delle regole di classificazione precedentemente implementate attraverso l’utilizzo del DGCIApp.

In Power Automate al termine del flusso DownloadPrtFile è stato inserito un flusso condizionale che verifica la presenza del file precedentemente salvato all’interno della cartella TestTCAE e qualora questo esista si procederà con l’esecuzione del flusso secondario DGCIApp.

Questo flusso selezionerà il file generato e permetterà di visualizzare tutte le informazioni necessarie per la classificazione come il tag di classificazione applicato, gli identificativi della regola e la policy associata alla regola.

In Macro Recorder come precedentemente detto non esiste un modo per verificare se il file generato è stato correttamente salvato all’interno della cartella per cui le operazioni per la verifica consistono in funzioni di mouse e pressione dei tasti per arrivare al path della cartella TestTCAE, che in Power Automate è gestito mediante le variabili precedentemente create.

Questa operazione deve essere ripetuta per tutte le varie modalità di export presenti all’interno del test plan.

Come visibile in figura 33, con l’utilizzo di Power Automate è possibile rieseguire il flusso secondario DGCIAPP in seguito ai vari flussi secondari che si occupano della generazione dei file sensibili effettuando le opportune modifiche in base al nome del file da verificare, cambiando in particolare l’estensione del file.

Con l’utilizzo di Macro Recorder invece queste azioni devono essere registrate al termine delle operazioni delle varie modalità di export in quanto la selezione del file avviene mediante clic.

Anche in questo caso può presentarsi un errore in fase di esecuzione del file contenente la verifica in quanto sfruttando la memorizzazione delle coordinate x, y del mouse nel desktop c’è il rischio che la finestra relativa all’apertura della cartella TestTCAE non sia nella stessa posizione, è consigliabile quindi memorizzare le operazioni sfruttando la finestra della cartella a schermo intero.

Inoltre, qualora la posizione del file da verificare dovesse cambiare c’è il rischio che si verifichi la classificazione di un file diverso da quello desiderato o che l’operazione di clic avvenga in una parte della finestra in cui non è presente nessuno dei file precedentemente salvati.

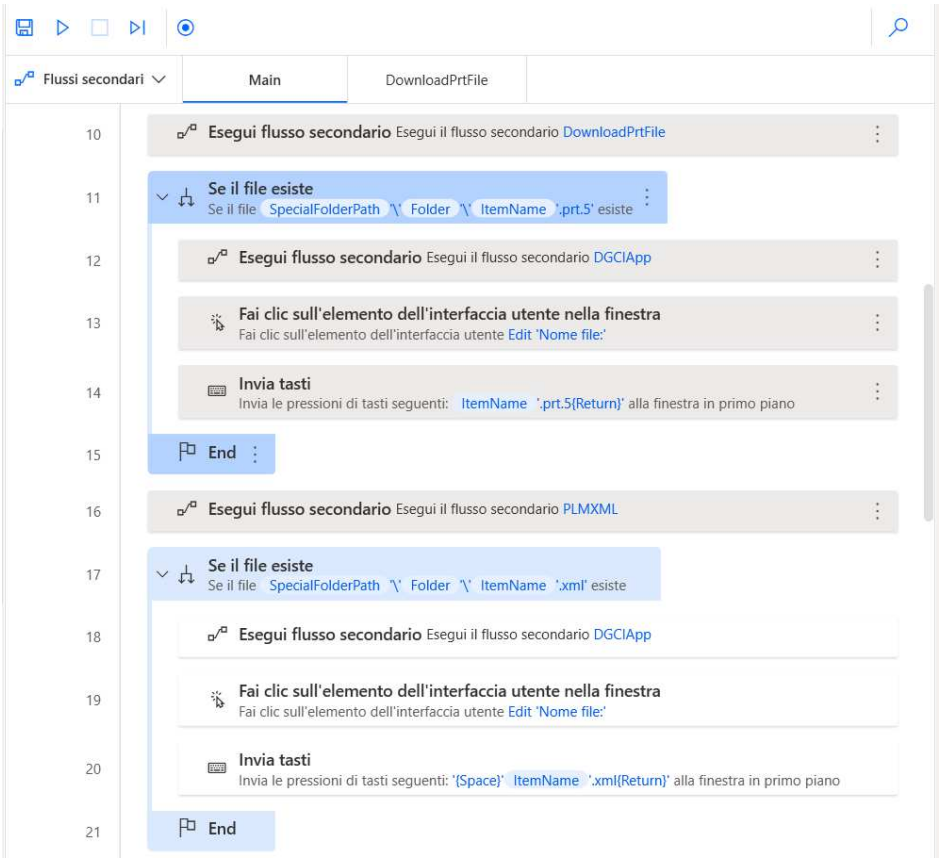

Figura 33. Verifica Classificazione

Download file con estensione xml

La seconda tipologia di Download serve per generare file con estensione xml.
Attraverso l'uso di Power Automate dopo aver effettuato l'operazione di clic sull'item che si desidera esportare, sono nuovamente utilizzate le funzioni per selezionare l'opzione all'interno del menu.
Questo perché per arrivare al salvataggio in xml si devono selezionare due diverse opzioni all'interno di due menu a cascata.
Le operazioni successive riguardo la scelta del path completo per selezionare la cartella di test dove salvare il file esportato sono gestite mediante l'utilizzo delle variabili precedentemente create e mediante l'OCR per effettuare il clic sul bottone relativo al Download.
Per la verifica del file salvato all'interno della cartella TestTCAE si procederà come spiegato all'interno del sotto capitolo "Verifica della classificazione del file" modificando solo l'estensione del file da verificare.

In Macro Recorder come già anticipato non esiste la funzione per la gestione delle opzioni all'interno del menu per cui si procederà con le sole operazioni di clic, l'inserimento attraverso la pressione dei tasti del path completo della cartella dove salvare il file e le successive funzioni di trova testo (OCR) per portare a termine l'operazione di Download.
Come già analizzato nel download del file con estensione "prt" il problema che si può presentare è quello relativo alla posizione del menu all'interno del quale selezionare l'opzione desiderata.
Questo perché qualora la finestra di Teamcenter non fosse a schermo interno le coordinate memorizzate attraverso le funzioni del mouse precedentemente eseguite non corrisponderanno.
Qualora l'operazione di Download del file dovesse andare a buon fine si dovrà procedere con la verifica della classificazione dei file ripetendo tutte le operazioni precedentemente descritte.
In questo caso non esiste la possibilità di riutilizzare il file precedentemente creato per la verifica del file con estensione "prt" in quanto la selezione del file da verificare avviene mediante la posizione del file all'interno della cartella.

Download file con l'utilizzo di Creo

La terza tipologia di Download è quella mediante l'utilizzo dell'applicazione Creo.
Con l'utilizzo di Power Automate sono presenti tre diversi flussi:

- il primo flusso secondario serve per l'invio dell'item selezionato all'applicazione creo mediante il clic sul bottone presente all'interno dell'interfaccia utente di Teamcenter e per rinominare il file sensibile da scaricare in modo da differenziarlo da quello generato mediante il secondo flusso,

- il secondo flusso secondario serve per l'invio dell'item selezionato all'applicazione creo mediante il doppio clic sull'item e per rinominare il file sensibile da scaricare in modo da differenziarlo da quello generato mediante il secondo flusso,

- il terzo flusso secondario serve per svolgere le azioni comuni a entrambi i flussi precedentemente descritti cioè l'attesa della visualizzazione completa dell'interfaccia di creo e le operazioni necessarie per effettuare il download.

Questa suddivisione permette di snellire le azioni presenti all'interno dei primi due flussi secondari e di sfruttare il terzo per svolgere tutte le azioni comuni senza dover registrare due volte le azioni da svolgere.
Il terzo flusso viene quindi richiamato all'interno dei due flussi secondari precedentemente descritti.
Al termine dell'esecuzione di entrambi i flussi si procederà con la verifica dei file salvati all'interno della cartella TestTCAE e si procederà come spiegato all'interno del sotto capitolo "Verifica della classificazione del file" apportando le opportune modifiche per la scelta del file da verificare.
Con l'utilizzo di Macro Recorder non esiste la possibilità di sfruttare delle azioni precedentemente registrate all'interno dei vari file per cui è necessario dividere le azioni all'interno di due file: il primo per l'utilizzo di creo mediante il button presente in Teamcenter e il secondo mediante il doppio clic.
Dopo aver utilizzato le funzioni necessarie per il clic sul button e per il doppio clic sull'item da voler aprire in creo si dovranno quindi ripetere le stesse azioni per entrambe le automazioni.
Infine, si dovrà inserire il nome dei due file da salvare in modo che siano diversi tra loro.
Qualora l'operazione di Download del file dovesse andare a buon fine si dovrà procedere con la verifica della classificazione dei file ripetendo tutte le operazioni precedentemente descritte.
Una delle differenze tra Macro Recorder e Power Automate oltre la possibilità di utilizzo di un flusso condiviso che svolge le azioni comuni a più flussi e riduce quindi il numero di operazioni registrate, è la gestione del cambio delle finestre dei programmi da utilizzare.
Con Power Automate ogni volta che si svolge un'operazione attraverso l'utilizzo di creo, il programma rileva il processo in esecuzione utilizzato per svolgere quella determinata azione.
Questo fa sì che l'interfaccia utente di creo si apra in modo automatico per poter portare a termine l'azione desiderata.
Con Macro Recorder invece non c'è questa possibilità per cui nonostante il programma creo sia stato precedentemente avviato e sia già aperto sulla workstation, è comunque necessario effettuare il clic sull'icona del programma presente nella tool bar per fare in modo che l'interfaccia utente di creo sia visualizzata nel desktop.
Solo dopo aver effettuato il clic si può quindi procedere con la registrazione delle operazioni da svolgere per effettuare il download del file.

Download file con l'utilizzo di Lifecycle Visualization

L'ultima modalità di export presente all'interno del test plan è quella che sfrutta la visualizzazione del progetto contenente l'item attraverso l'utilizzo dello strumento di visualizzazione Lifecycle Visualization.
Le operazioni svolte attraverso l'utilizzo di Power Automate sono simili a quelli utilizzati per creo button per cui utilizza il clic iniziale che sarà però sul progetto invece che sull'item, il successivo clic sul button che consente di visualizzare il progetto attraverso l'utilizzo di Lifecycle Visualization e le azioni che sfruttano l'OCR per portare a termine le operazioni necessarie per completare il download del file con estensione "plmxml".
Al termine dell'esecuzione del flusso si procederà con la verifica dei file salvati all'interno della cartella TestTCAE e si procederà come spiegato all'interno del sotto capitolo "Verifica della classificazione del file" apportando le opportune modifiche per la scelta del file da verificare.
Con l'utilizzo di Macro Recorder si riscontrano le stesse differenze già presentate per effettuare il download del file con creo.
Infatti, per poter utilizzare il visualizzatore e cambiare la finestra di visualizzazione sulla quale svolgere le operazioni è necessario effettuare il clic sull'icona del visualizzatore presente nella tool bar e poi completare la registrazione delle operazioni necessarie per effettuare il download del file con estensione "plmxml".

Qualora l'operazione di Download del file dovesse andare a buon fine si dovrà procedere con la verifica della classificazione dei file ripetendo tutte le operazioni precedentemente descritte.

5.2 Tempo di implementazione

Un altro dei confronti significativi tra le due soluzioni di scrittura per l'automazione dei test è quella relativa ai tempi di implementazione.
Il tool più semplice e veloce da utilizzare è Macro Recorder in quanto permette di registrare tutte le azioni svolte dall'utente con un clic sul tasto "Record" presente nell'interfaccia utente del programma.
In seguito al clic sono memorizzate tutte le operazioni che prevedono l'utilizzo del mouse quali: spostamento, clic con il tasto destro, clic con il tasto sinistro, doppio clic o l'utilizzo della rotellina.
Oltre le azioni del mouse memorizza in modo automatico anche la pressione dei tasti sulla tastiera rendendo l'inserimento del testo molto semplice.
Dopo aver memorizzato la registrazione è possibile modificare o rimuovere azioni, aggiungere azioni come "Trova immagine" o "Trova Testo OCR", aggiungere le pause, regolare la velocità di riproduzione e smussare i percorsi del mouse in modo da rendere l'esecuzione lineare.
Conoscendo quindi l'applicazione Teamcenter e le operazioni da dover svolgere questa modalità di automazione è molto veloce.
Di contro però occorre salvare un ampio numero di registrazioni in base al numero di test da effettuare.
Per portare a termine tutte le azioni di verifica presenti all'interno del test plan serviranno quindi quattordici differenti file che devono essere controllati e mandati in esecuzione dall'utente.
Power Automate invece è più complesso da utilizzare in quanto presenta un vasto menu di azioni all'interno del quale è possibile cercare l'operazione migliore per l'automazione.
L'uso dei flussi condizionali, delle variabili di input, di output e di flusso, e la gestione dell'errore sono dei grandi vantaggi per l'utente.
I flussi condizionali permettono di effettuare delle modifiche ed evitare di svolgere delle azioni se già precedentemente svolte e quindi non necessarie, l'uso delle variabili è fondamentale per la gestione dei vari percorsi relativi alla posizione dei programmi da eseguire e alla posizione della cartella da utilizzare per la verifica della classificazione dei file e la gestione dell'errore evita che si blocchi il flusso principale al verificarsi di un errore durante l'esecuzione e al contrario permette di gestirlo attraverso la creazione di flussi secondari.

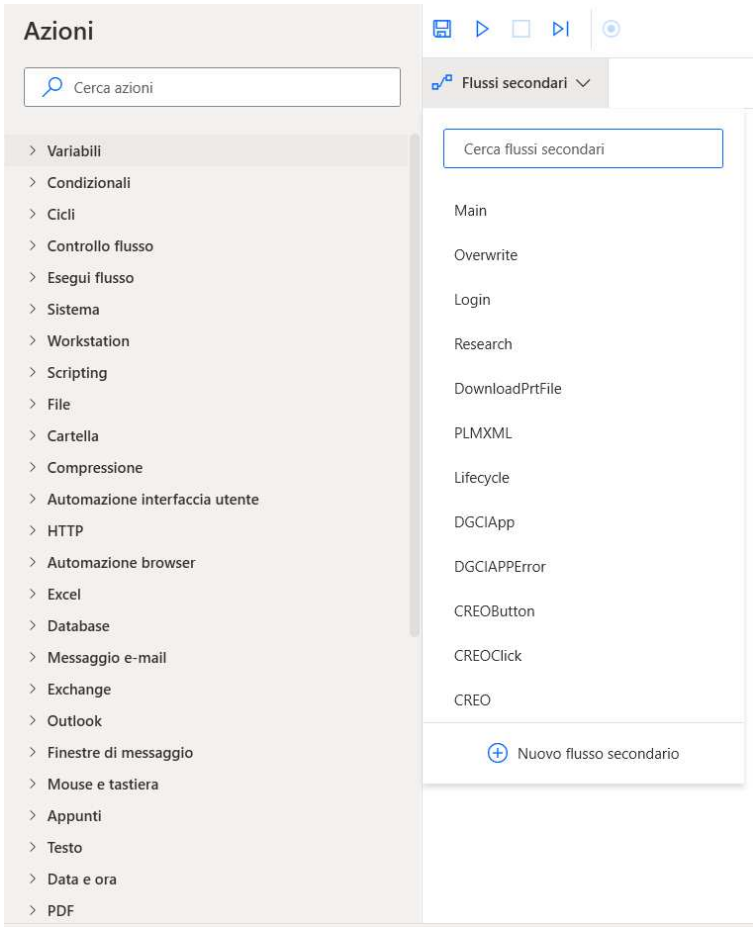

Figura 34. Azioni e Flussi in Power Automate

Tutte queste funzionalità rappresentano degli enormi vantaggi per l'utente ma richiedono un tempo d'implementazione molto maggiore rispetto a quello che richiede la registrazione con Macro Recorder.

Inoltre, la suddivisione dei flussi in flusso principale e flussi secondari permette di frammentare il flusso ed eseguirne solo una parte senza dover necessariamente svolgere delle azioni non necessarie.

5.3 Portabilità dell'automazione

Oltre tutte le differenze presentate fino ad ora esiste un'altra fondamentale differenza che mi ha spinto a scegliere di proseguire l'automazione solo attraverso l'utilizzo di Power Automate ed è quella relativa alla portabilità dell'implementazione creata.
Con Macro Recorder non esiste la possibilità di cooperare durante la creazione dell'implementazione.
L'unica soluzione per poter condividere la macro creata consiste nel pagamento di una somma una tantum.
Oltre a non poter collaborare durante la creazione non esiste nemmeno la possibilità di condividere l'automazione registrata e quindi il macro file con estensione "mrf" precedentemente salvato.
Questo perché l'automazione implementata, come descritto nel capitolo precedente all'interno del paragrafo "Test con Macro Recorder", si basa principalmente sulla registrazione delle coordinate x, y statiche del mouse.
Una volta inviato il file "mrf" con l'automazione sarà quindi impossibile fare in modo che funzioni correttamente in quanto la posizione dei programmi e delle cartelle nel desktop della workstation sulla quale eseguire le operazioni registrate dovrebbero essere perfettamente identiche a quelle presenti sulla workstation da cui sono state registrate le operazioni necessarie per eseguire il test plan.
Con Power Automate il flusso desktop creato per l'automazione può essere visualizzato da qualunque dispositivo in quanto Power Automate è una soluzione cloud di Microsoft. Inoltre, consente di condividere il flusso desktop creato con altri utenti all'interno dell'organizzazione in modo che anche loro possano visualizzare, modificare ed eseguire le azioni presenti all'interno del flusso.
Condividere il flusso desktop è infatti un'operazione molto semplice che viene gestita direttamente dall'area personale della pagina web di Microsoft Power Automate.
Una volta effettuato l'accesso alla pagina con l'utilizzo delle credenziali personali basterà selezionare l'opzione "Flussi Personali" presente sul lato sinistra della schermata, selezionare il flusso desktop che si desidera condividere, selezionare l'opzione Condividi e inserire il nome degli utenti a cui si vuole concedere l'accesso.
È inoltre possibile scegliere quale livello di autorizzazione assegnare all'utente con quale si vuole condividere il flusso.

I due livelli sono:

- Utente, che permette all'utente di effettuare solo l'esecuzione del flusso cloud condiviso. Non è quindi in grado di effettuare alcuna modifica e non può nemmeno eliminare o condividere il flusso. L'utente può però effettuare una copia del flusso in modo da poter comunque lavorare sull'automazione in modo indipendente.

- Comproprietario, che permette all'utente di disporre di tutte le autorizzazioni del flusso desktop condiviso. Potrà quindi modificare il flusso, eliminarlo o condividerlo con altri utenti.

Il livello di accesso da assegnare ai membri del team DLP è quello di comproprietario in quanto è fondamentale collaborare sull'attività da svolgere.

5.4 Conclusioni e sviluppi futuri

Con lo scouting, la scelta del tool per la scrittura e la gestione dei test automatici, Power Automate, e attraverso la progettazione e l'implementazione del flusso automatico di validazione delle regole Data Loss Prevention, sono stati raggiunti tutti gli obiettivi che erano stati prefissati.

Il flusso creato per l'applicazione Teamcenter, per la verifica dell'efficacia delle regole per la protezione della proprietà intellettuale dell'azienda è funzionante e in grado di effettuare in maniera automatica i test necessari per la certificazione del tool.

Le uniche azioni che devono essere svolte manualmente da un membro del team DLP AMS sono l'avvio del programma di automazione Power Automate e l'avvio dell'esecuzione del flusso condiviso.

Il flusso creato è stato provato in modo accurato su diverse workstation di test configurate in modo diverso tra loro.

La differenza consiste principalmente nelle policy e di conseguenza nelle regole applicate che non sono tutte uguali tra loro ma possono presentare delle differenze fondamentali.

Il processo attualmente adottato dall'azienda prevede lo svolgimento manuale dei test per la validazione delle regole e la certificazione dei tool, questo processo prevede lo svolgimento di azioni ripetitive che possono diventare noiose e possono aumentare il rischio di errore.

Qualora una regola venga validata nonostante non funzioni nel modo corretto, il rischio di non proteggere i dati sensibili e la probabilità che si verifichi una fuga di informazioni causando un data loss è molto alto.

L'utilizzo dell'automazione non commette errori di valutazione, che possono essere causati invece dall'essere umano ed esegue le procedure in modo sequenziale e preciso.

Qualora ci fosse un errore durante l'esecuzione del flusso, l'automazione interrompe i test di validazione delle regole e mostra l'errore che si è verificato.

L''utilizzo dell'automazione aumenta l'efficienza del processo del 40% in quanto non è più necessario lo svolgimento manuale del test che come discusso già nel primo capitolo presenta una probabilità di errore.

Inoltre, a differenza del processo manuale nel quale gli utenti possono interrompere l'esecuzione dei test per dare priorità ad altre attività o rallentare lo svolgimento a causa

della stanchezza, l'utilizzo dell'automazione garantisce una velocità di esecuzione costante durata tutta la durata dei test.

Nonostante l'automazione sia completa e correttamente funzionante, può comunque essere necessario apportare delle piccole modifiche come, ad esempio, la modifica del path inserito per l'esecuzione dei programmi, qualora un utente dovesse cambiare la posizione dei processi che devono essere eseguiti all'interno di una delle workstation di test.

L'automazione inoltre dipende da molti degli elementi presenti nell'interfaccia utente di Teamcenter per cui qualora dovessero esserci delle sostanziali modifiche in seguito a nuove release si dovranno modificare alcune delle azioni presenti nei flussi desktop creati.

Dopo aver progettato e implementato l'automazione per l'applicazione Teamcenter e aver verificato il corretto funzionamento dell'implementazione, uno degli sviluppi futuri è quello di estendere l'automazione agli altri tool in perimetro in modo da ridurre in modo sostanziale l'attività manuale del team DLP.

Si può dunque concludere che con l'adozione del tool per la scrittura e la gestione dei test automatici, con l'implementazione automatica dei test per la verifica dell'efficacia delle regole di validazione della proprietà intellettuale e con gli sviluppi futuri si riesce ad aumentare l'efficienza del processo aziendale che ad oggi viene svolto in modo manuale.

Ringraziamenti

Ringrazio il Professor Gianpiero Cabodi per la disponibilità dimostrata sia durante i suoi corsi d'apprendimento che durante lo svolgimento del progetto di tesi.
Ringrazio l'azienda Spike Reply per l'opportunità di tesi in azienda, in particolare Emiliano Orrù per essersi prestato al ruolo di correlatore e Cecilia.
Ringrazio inoltre i colleghi del team Data Loss Prevention per la disponibilità mostrata durante lo svolgimento dei test necessari per il progetto di tesi.

Riferimenti

[1] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ consultato in data 26/11/2022

[2] https://dellfocusaccounts.com/wp-content/uploads/2020/10/Market-Guide-for-Enterprise-Data-Loss-Prevention.pdf consultato in data 28/11/2022

[3] https://dellfocusaccounts.com/wp-content/uploads/2020/10/Market-Guide-for-Enterprise-Data-Loss-Prevention.pdf consultato in data 30/11/2022

[4] https://digitalguardian.com/platform-overview consultato in data 10/12/2022

[5] DigitalGuardian7_5_1_Rule_Implementation_Guide.pdf consultato in data 12/12/2022

[6] DigitalGuardian7_5_1_Utilities_Guide.pdf consultato in data 18/12/2022

[7] https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer consultato in data 20/12/2022

[8] https://www.macrorecorder.com/doc/ consultato in data 04/01/2022

[9] https://docs.microsoft.com/it-it/power-automate/desktop-flows/debugging-flow consultato in data 08/01/2022

[10] https://powerautomate.microsoft.com/it-it/ consultato in data 10/01/2022

[11] https://support.microsoft.com/it-it/topic/non-%C3%A8-possibile-accedere-creare-modificare-salvare-visualizzare-i-flussi-del-desktop-in-pad-493b6b6c-a7de-4c51-9bcc-d05e7f2c8d49 consultato in data 14/01/2022

[12] https://www.macrorecorder.com/download/ consultato in data 06/02/2022