



Laurea Triennale in informatica - Università di Salerno
Corso di *Ingegneria del Software* - Prof.ssa F. Ferrucci



GUARDIAN FLOW
FEELING SAFE

Requirements Analysis Document

Guardian Flow

Riferimento	
Versione	1.6
Data	24/11/2023
Destinatario	Prof.ssa F. Ferrucci
Presentato da	Intero team
Approvato da	Raffaele Mezza, Martina Mingione



Sommario

Revision History	4
1. Introduzione	5
1.1 Obiettivo del sistema.....	5
1.2 Ambito del sistema.....	5
1.3 Obiettivi e criteri di successo.....	7
1.3.1 Obiettivi	7
1.3.2 Criteri di successo	7
1.4 Definizioni, acronimi e abbreviazioni	7
1.4.1 Definizioni.....	7
1.4.2 Acronimi e Abbreviazioni.....	8
1.5 Riferimenti.....	8
1.6 Organizzazione del documento	8
2. Sistema attuale	9
2.1 Diagramma delle attività -Sistema Attuale.....	10
2.1.1 Installazione del sistema.....	10
2.1.2 Sistema basato su firme	11
3. Sistema proposto.....	12
3.1 Diagramma delle attività -Sistema Proposto.....	12
3.1.1 Attivazione del sistema.....	12
3.1.2 Rilevazione di anomalie	13
3.2 Requisiti Funzionali.....	13
3.2.4 Specifica User Stories	14
3.3 Requisiti non funzionali	20
3.4 Modello del sistema	20
3.4.1 Scenari	20
3.4.2 Use Case	32
3.4.3 Modello ad Oggetti.....	38
3.4.3.1 Diagrammi delle entità	38
3.4.3.2 Diagrammi ad Oggetti.....	39
3.4.4 Modello Dinamico	42



3.4.4.1 Statechart Diagrams	42
3.4.4.2 SequenceDiagrams	45
3.4.5 Interfaccia Utente – Percorsi di Navigazione e Mock-up	48
3.4.5.1 NP_01 Percorsi di navigazione da parte dell'acquirete.....	48
3.4.5.2 NP_02 Percorsi di navigazione da parte degli utenti.....	48
3.4.5.2 Mock-up.....	49
4.Glossario	58



Revision History

Data	Versione	Descrizione	Autori
24/10/2023	0.1	Sistema attuale	Danilo Gisolfi Mattia Guariglia
26/10/2023	0.2	Diagramma delle attività del sistema attuale	Tutto il team
31/10/2023	0.3	Introduzione	Edmondo De Simone Giuseppe Cerella
06/11/2023	0.4	Diagramma delle attività del sistema preposto	Danilo Gisolfi Mattia Guariglia Tommaso Nardi
07/11/2023	0.5	Aggiunta RF e RNF	Tutto il team
08/11/2023	0.6	Aggiunta scenari	Tutto il team
09/11/2023	0.7	Aggiunta UseCase	Tutto il team
14/11/2023	0.8	Aggiunta Class Diagram	Tutto il team
15/11/2023	0.9	Stesura Modello a oggetti	Danilo Gisolfi
16/11/2023	1.0	Aggiunta SequenceDiagram	Tutto il team
16/11/2023	1.1	Aggiunta StateChart	Tutto il team
22/11/2023	1.2	Aggiunta Mock-ups e NP	Edmondo De Simone Giuseppe Cerella
23/11/2023	1.3	Introduzione seconda parte	Edmondo De Simone Giuseppe Cerella
24/11/2023	1.4	Glossario	Vincenzo Maiellaro
24/11/2023	1.5	Revisione documento	Edmondo De Simone
24/11/2023	1.6	Approvato	Martina Mingione Raffaele Mezza



1. Introduzione

Il sistema Guardian Flow rappresenta una soluzione per l'analisi del traffico di rete all'interno delle aziende, offre la possibilità di costruire una baseline personalizzata per ogni cliente e permette di rilevare efficacemente le anomalie della rete, contribuendo così a rafforzare la sicurezza informatica aziendale.

1.1 Obiettivo del sistema

L'obiettivo principale del sistema Guardian Flow è la rilevazione di anomalie attraverso una piattaforma intuitiva e dinamica, costruendo una baseline personalizzata per il cliente e mettendo a disposizione una dashboard, la quale permette al cliente di visualizzare in tempo reale il traffico di rete analizzato e le eventuali anomalie rilevate. La flessibilità del sistema Guardian Flow si estende anche alla possibilità di modificare agilmente il piano d'abbonamento, offrendo agli utenti la libertà di adattare le funzionalità e le risorse disponibili alle specifiche esigenze dell'azienda. Con Guardian Flow, si propone di rendere l'analisi del traffico di rete accessibile, efficiente e personalizzabile per garantire una gestione ottimale delle risorse e della sicurezza del sistema.

1.2 Ambito del sistema

Il sistema Guardian Flow nasce dalla necessità di implementare una solida infrastruttura digitale per il controllo del traffico di rete all'interno di un'azienda, cercando di semplificare e modernizzare il processo esistente. L'analisi del sistema attuale ha rivelato importanti problematiche legate all'inefficiente rilevazione di anomalie nel traffico di rete, richiedendo un approccio più avanzato e scalabile.

Il sistema proposto si prefissa di supportare diversi servizi chiave, tra cui:

1. Gestione dell'Utente:

- Autenticazione degli utenti nel sistema;
- Possibilità di creare account subordinati;
- Logout per garantire la sicurezza delle sessioni.



2. Controllo del Traffico Dati:

- Analisi dettagliata del traffico dati in tempo reale;
- Identificazione delle anomalie emerse durante l'analisi;
- Costruzione di una baseline personalizzata per ogni cliente.

3. Dashboard Interattiva:

- Visualizzazione di una dashboard intuitiva per consultare l'andamento dell'analisi del traffico.

4. Notifiche e Alert:

- Servizi di notifica per segnalare eventuali anomalie nel traffico.

5. Gestione delle Configurazioni:

- Capacità di modificare il piano d'abbonamento in base alle esigenze aziendali;
- Adattabilità del sistema a variazioni della rete del cliente.

6. Rapporti:

- Generazione di report periodici sull'analisi del traffico.

Guardian Flow sarà il pilastro attraverso il quale l'azienda potrà gestire e ottimizzare l'analisi del traffico dati, garantendo sicurezza ed efficienza.



1.3 Obiettivi e criteri di successo

1.3.1 Obiettivi

L'obiettivo principale è la realizzazione di un sistema per la rilevazione delle anomalie efficiente e scalabile, grazie all'utilizzo di un'intelligenza artificiale non supervisionata e all'implementazione in cloud, la quale a differenza di quella hardware ha la possibilità di adattarsi a qualsiasi topologia di rete.

1.3.2 Criteri di successo

- Facilità di Utilizzo: la piattaforma dovrà garantire un'interfaccia utente intuitiva e di facile utilizzo;
- Rilevazione efficace: il sistema dovrà garantire una rilevazione delle anomalie efficace;
- Tempestività delle notifiche: le notifiche di rilevazione dovranno essere tempestive e affidabili;
- Scalabilità: il sistema dovrà essere facilmente adattabile alle mutevoli esigenze aziendali.

1.4 Definizioni, acronimi e abbreviazioni

1.4.1 Definizioni

- Dashboard: interfaccia visuale progettata per monitorare e comprendere facilmente grandi quantità di dati in tempo reale;
- Falso positivo: rilevazione di un'anomalia quando questa non è effettivamente tale;
- Anomalia: comportamento insolito rispetto a modelli di traffico di rete considerati normali;
- Alert: avviso progettato per attirare l'attenzione su qualcosa di importante o di cui è necessario essere informati;
- Analisi di rete: questo tipo di analisi riguarda l'esame delle connessioni e delle attività all'interno di una rete informatica. Si possono analizzare flussi di dati, individuare possibili vulnerabilità di sicurezza, monitorare il traffico di rete per rilevare comportamenti anomali;
- Variazioni della rete: in generale, la variazione della rete si riferisce a qualsiasi cambiamento rilevante o modificazione che si verifica all'interno di una rete.



1.4.2 Acronimi e Abbreviazioni

- GDPR: General Data Protection Regulation;
- IPS: Intrusion Prevention System;
- IDS: Intrusion Detection System;
- NP: Navigation Path;
- RAD: Requirements Analysis Document;
- RNF: Requisito Non Funzionale;
- RF: Requisito Funzionale;
- SCD: StateChart Diagram;
- SD: Sequence Diagram;
- UC: Use Case;
- UCD: Use Case Diagram.

1.5 Riferimenti

- https://help.deepsecurity.trendmicro.com/20_0/on-premise/dashboard.html

1.6 Organizzazione del documento

Il presente documento è strutturato nel seguente modo:

Nel secondo paragrafo del testo, si esamina il sistema attuale, mettendo in luce le procedure in atto e identificando sia le pratiche ottimali che eventuali imperfezioni. Allo stesso tempo, verrà presentato un diagramma di attività che illustra il processo corrente per il rilevamento di anomalie basato su firme il quale presenta degli aspetti critici.

Al terzo punto viene descritto il sistema preposto e con due diagrammi delle attività vengono illustrate l'attivazione del sistema e la rilevazione delle anomalie. Successivamente alla panoramica iniziale sulla trasformazione dei processi aziendali, vengono presentati i risultati derivanti dalla dettagliata analisi dei requisiti.

In particolare, vengono riportati tutti i dati emersi da tale analisi specifica:

- Il [paragrafo 3.2](#) riporta la specifica dei requisiti funzionali e la specifica tramite User Stories;



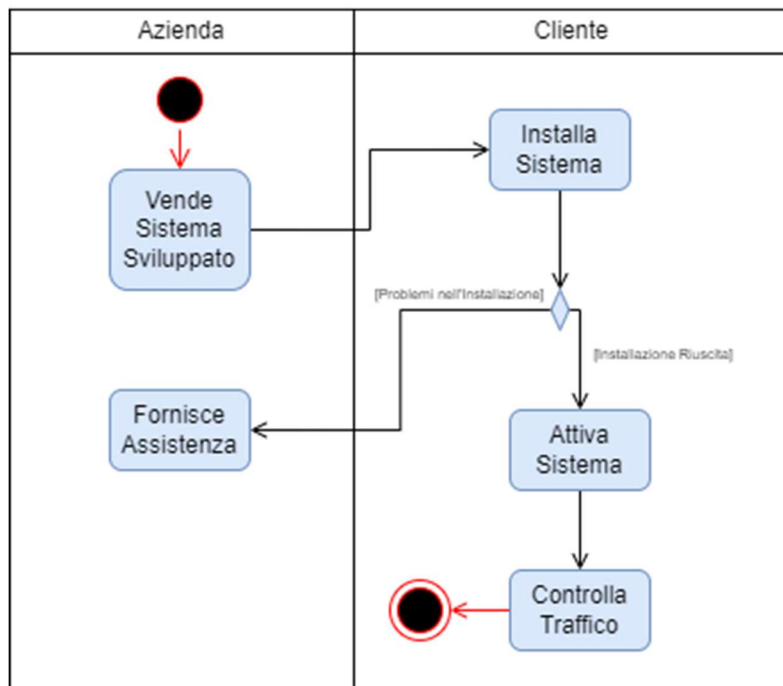
- Il [paragrafo 3.3](#) riporta la specifica dei requisiti non funzionali;
- Il [paragrafo 3.4](#) è dedicato all'analisi del modello del sistema:
 - I primi due punti includono, gli scenari e i casi d'uso;
 - In seguito, sono stati inseriti gli strumenti di esame: modelli basati su oggetti e modelli dinamici;
 - Alla conclusione del paragrafo sono inclusi i mock-ups, che offrono una versione iniziale del prototipo del sistema.

2. Sistema attuale

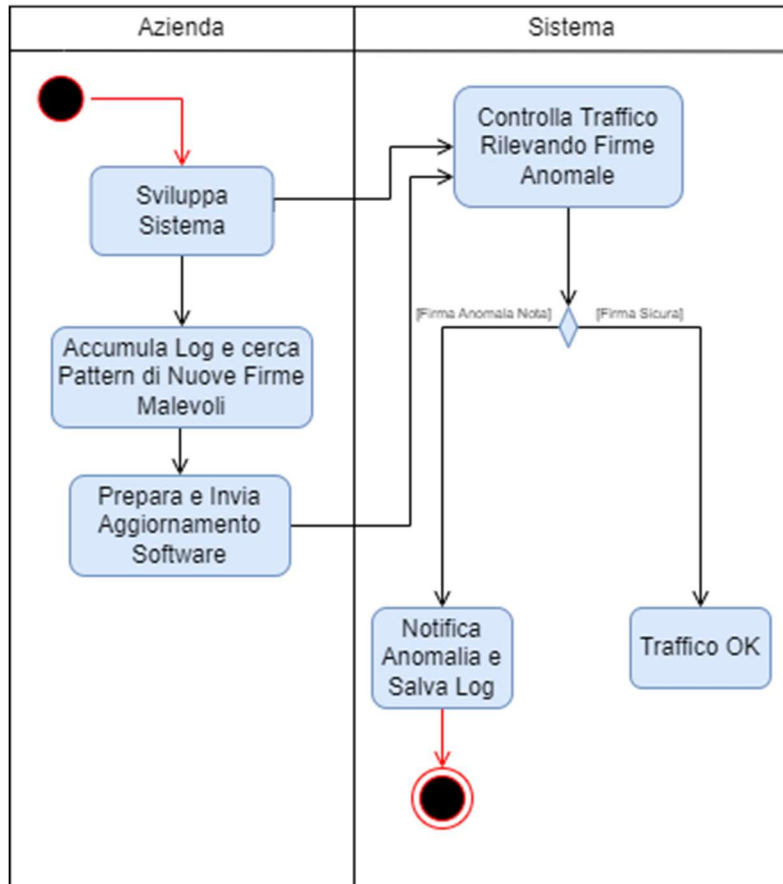
Oggi, la maggior parte delle aziende che operano in rete utilizzano sistemi di rilevamento delle intrusioni (IDS), di prevenzione delle intrusioni (IPS) e firewall con apprendimento e firme al fine di proteggersi dai pericoli informatici. Tuttavia, queste soluzioni presentano degli aspetti critici, in primo luogo, non sono scalabili, quando il traffico di rete aumenta questi sistemi che spesso sono su appliance, hanno difficoltà a gestirlo in tempo reale. Inoltre, si basano su firme, il che significa che rilevano soltanto pericoli già conosciuti e quando si tratta di rischi sconosciuti ciò può portare a falsi negativi. Infine, mantenere un elenco aggiornato di tutti i rischi richiede manutenzione, ma questa operazione è difficile e costosa dal punto di vista economico. Le minacce informatiche sono in continua evoluzione, diventano sempre più complesse da identificare e non sempre è possibile tenere il passo con questa crescente complessità e quantità di dati da etichettare.

2.1 Diagramma delle attività -Sistema Attuale

2.1.1 Installazione del sistema



2.1.2 Sistema basato su firme

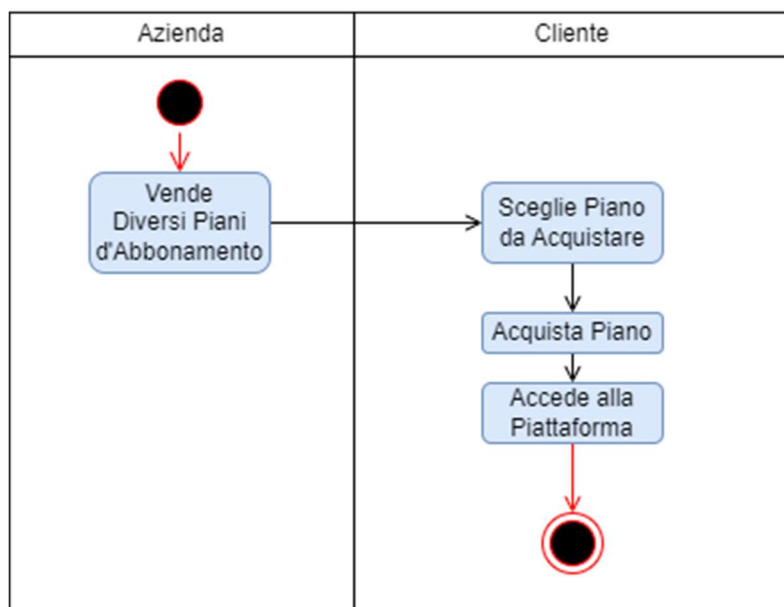


3. Sistema proposto

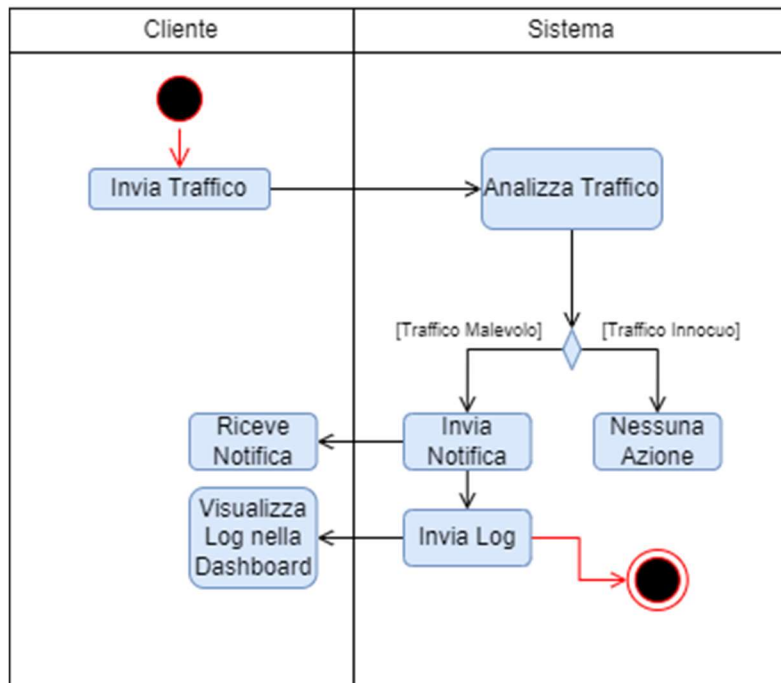
Il sistema proposto, si occupa di monitorare il traffico di rete di un'azienda attraverso l'utilizzo di un'intelligenza artificiale non supervisionata la quale andrà a rilevare eventuali anomalie all'interno del traffico di rete, le quali verranno notificate all'utente. Inoltre, verrà costruita una baseline personalizzata. L'utente potrà selezionare un piano d'abbonamento tra quelli disponibili per poi procedere con il pagamento, di seguito gli verrà inviata un email contenente le credenziali da utilizzare per il primo accesso. Successivamente, l'utente avrà accesso ad una dashboard dalla quale avrà una visione completa di tutte le informazioni elaborate, in particolare avrà la possibilità di visualizzare lo storico delle anomalie rilevate, degli accessi alla dashboard e tramite una sezione dedicata si potranno creare degli account subordinati. La realizzazione del sistema andrà non solo a migliorare la sicurezza aziendale ma a semplificare l'accesso a tali informazioni senza intaccare la sicurezza.

3.1 Diagramma delle attività - Sistema Proposto

3.1.1 Attivazione del sistema



3.1.2 Rilevazione di anomalie



3.2 Requisiti Funzionali

I Requisiti funzionali vengono presentati tramite un documento Excel separato, distinto dal documento principale. Questa decisione è stata presa al fine di sfruttare il formato tabellare, che offre una struttura organizzata e chiara per la gestione dei dati.

[C15_Requisiti.xlsx](#)



3.2.4 Specifica User Stories

Identificazione

Titolo della storia	Attivazione autenticazione a 2 fattori
ID della storia	US_GA_05
Area funzionale	Gestione Accesso
Priorità	Alta

User Story

In qualità di	Utente
Quando	Accedo al mio account
Io vorrei ...	Attivare l'autenticazione a due fattori
In modo da	Aumentare la sicurezza del mio account

Criteri di accettazione

1	<ol style="list-style-type: none">1. Poiché un utente vuole attivare l'autenticazione a due fattori;2. Quando preme per attivarla;3. Allora il sistema richiederà sia la password che il secondo fattore alle prossime autenticazioni.
----------	--



Identificazione

Titolo della storia	Modifica piano d'abbonamento
ID della storia	US_FU_02
Area funzionale	Funzionalità Utente
Priorità	Media

User Story

In qualità di	Utente admin
Quando	Desidero modificare il mio piano d'abbonamento
Io vorrei ...	Avere la possibilità di selezionare e cambiare il piano d'abbonamento
In modo da	Garantire una gestione efficiente delle risorse e adattarmi alle esigenze dell'azienda

Criteri di accettazione

1	<ol style="list-style-type: none">1. Dato che l'utente è autenticato come admin;2. Quando accede alla sezione dedicata al piano d'abbonamento;3. Allora il sistema consente la modifica.
----------	--



Identificazione

Titolo della storia	Segnalazione di falsi positivi
ID della storia	US_FU_04
Area funzionale	Funzionalità Utente
Priorità	Alta

User Story

In qualità di	Utente admin
Quando	Visualizzo una minaccia
Io vorrei ...	Etichettarla come falso positivo
In modo da	Confermare che si tratta di un falso allarme

Criteri di accettazione

1	<ol style="list-style-type: none">1. Dato che l'utente è autenticato come admin2. Quando visualizza le minacce e etichetta un falso positivo3. Allora il sistema deve registrare questa azione
----------	--



Identificazione

Titolo della storia	Modifica della password
ID della storia	US_GA_04
Area funzionale	Gestione Accesso
Priorità	Media

User Story

In qualità di	Utente
Quando	Decido di aggiornare la mia password
Io vorrei ...	Avere la possibilità di inserirne una nuova
In modo da	Garantire sicurezza al mio account

Criteri di accettazione

1	<ol style="list-style-type: none">1. Dato che l'utente è autenticato al sistema2. Quando accede alle impostazioni dell'account per modificare la password e ne inserisce una nuova3. Allora il sistema verifica che rispetti i requisiti minimi di sicurezza e la modifica con successo
----------	---



Identificazione

Titolo della storia	Notifica di una anomalia
ID della storia	US_FS_04
Area funzionale	Funzionalità Sistema
Priorità	Alta

User Story

In qualità di	Utente
Quando	Viene rilevata una minaccia
Io vorrei ...	Essere tempestivamente notificato
In modo da	Proteggere la sicurezza della mia azienda

Criteri di accettazione

1	<ol style="list-style-type: none">1. Dato che l'utente è un dipendente dell'azienda2. Quando si analizza traffico di rete e si incorre in una minaccia3. Allora riceve una notifica
----------	---



Identificazione

Titolo della storia	Gestione Utenti
ID della storia	US_FU_03
Area funzionale	Funzionalità Utente
Priorità	Media

User Story

In qualità di	Utente admin
Quando	C'è bisogno di gestire i permessi di un altro utente
Io vorrei ...	Concedere o revocare i permessi ad un altro utente
In modo da	Adattare le autorizzazioni alle necessità aziendali

Criteri di accettazione

1	<ol style="list-style-type: none">1. Dato che l'utente è autenticato come admin2. Quando accede alle impostazioni di gestione dei permessi3. Allora deve selezionare un utente specifico e concedere o revocare i suoi permessi
----------	---



3.3 Requisiti non funzionali

I Requisiti non funzionali vengono presentati tramite un documento Excel separato, distinto dal documento principale. Questa decisione è stata presa al fine di sfruttare il formato tabellare, che offre una struttura organizzata e chiara per la gestione dei dati.

[C15_Requisiti.xlsx](#)

3.4 Modello del sistema

3.4.1 Scenari

Nome Scenario	SC_GA_01: Gestione Accesso - Login	
Partecipanti	Edmondo: l'utente che lavora in una azienda	
Descrizione	Lo scenario mostra l'utente che accede al sistema inserendo le proprie credenziali.	
Vantaggi	Si impedisce l'accesso alle risorse del sistema ad utenti non autorizzati.	
Flusso degli Eventi	Utente	Sistema
	1. Edmondo vuole accedere al sistema così clicca sul pulsante del login.	2. Il sistema mostra la pagina relativa all'accesso.
	3. Edmondo a quel punto inserisce email e password e preme il tasto per accedere.	4. Il sistema verifica le sue credenziali. Se sono corrette mostra la dashboard a Edmondo.



Nome Scenario	SC_GA_03: Gestione Accesso - Recupero della password	
Partecipanti	Edmondo: l'utente che lavora in una azienda	
Descrizione	Lo scenario mostra il meccanismo per recuperare la password dell'utente.	
Vantaggi	Permette all'utente di riottenere l'accesso all'account in caso abbia dimenticato la password.	
Flusso degli Eventi	Utente	Sistema
	1. Edmondo vorrebbe accedere al sistema ma non ricorda la password, così clicca sul pulsante per recuperarla.	2. Il sistema invia a Edmondo un link per verificare la sua identità.
	3. Edmondo lo clicca.	4. Il sistema mostra la pagina per reimpostare la password.
	5. Edmondo scrive la nuova password e la conferma.	6. Il sistema verifica che le due password corrispondano e aggiorna le credenziali di Edmondo.
	7. Edmondo può nuovamente accedere alla piattaforma.	



Nome Scenario	SC_FS_02: Funzionalità Sistema – Costruzione Baseline	
Partecipanti	Azienda: l'azienda di un cliente la cui rete genera traffico da analizzare	
Descrizione	Lo scenario mostra la costruzione di una baseline personalizzata per ogni utente.	
Vantaggi	Il vantaggio principale che si ha nella costruzione corretta di una baseline è che essa permette al sistema di essere sin da subito in grado di classificare adeguatamente il traffico ricevuto.	
Flusso degli Eventi	Azienda	Sistema
	1. La rete dell'azienda inizia a usufruire del servizio e a generare traffico che viene inoltrato al sistema tramite sniffer o protocollo di rete.	2. Il sistema riceve il traffico di rete e lo utilizza per addestrare il suo modello.
	3. La rete continua a generare traffico che verrà inoltrato al sistema e verrà usato continuamente per l'addestramento.	



Nome Scenario	SC_GA_04: Gestione Accesso – Modifica della password	
Partecipanti	Vincenzo: l'utente che lavora in una azienda	
Descrizione	Lo scenario mostra l'utente che modifica la propria password.	
Vantaggi	Il vantaggio principale che si ha con la modifica della password è di mantenere sicure le proprie credenziali.	
Flusso degli Eventi	Utente	Sistema
	1. Vincenzo accede al sistema inserendo email e password.	2. Il sistema verifica le credenziali e se corrette gli mostra la dashboard.
	3. Vincenzo si reca nella sezione relativa ai suoi dati personali.	4. Il sistema mostra correttamente questa pagina.
	5. Vincenzo imposta una nuova password conforme alle politiche di sicurezza.	6. Il sistema aggiorna e sostituisce quella precedente.
	7. Vincenzo deve autenticarsi con la nuova password.	



Nome Scenario	SC_FS_04: Funzionalità Sistema - Notifica di una anomalia	
Partecipanti	Tommaso: l'utente che lavora in una azienda	
Descrizione	Lo scenario mostra l'arrivo di una notifica che indica il rilevamento di una anomalia.	
Vantaggi	Il vantaggio principale che si ha con l'arrivo di una notifica di rilevazione di un'anomalia è che il proprietario dell'azienda o un suo subordinato vengano avvisati in tempo reale della presenza di una minaccia per poter agire tempestivamente.	
Flusso degli Eventi	Utente	Sistema
	1. L'azienda per cui lavora Tommaso genera traffico di rete.	2. Il sistema analizza il traffico di rete e se rileva un'anomalia la quale potrebbe essere una seria minaccia alla sicurezza dell'azienda. Procede all'invio automatico di una notifica utile ad allertare gli utenti addetti.
	3. Tommaso riceve tempestivamente sul suo dispositivo una notifica che lo informa del rilevamento di una anomalia e potrà agire di conseguenza.	



Nome Scenario	SC_GA_05: Gestione Accesso – Attivazione 2FA	
Partecipanti	Tommaso: l'utente che lavora in una azienda	
Descrizione	Lo scenario mostra l'utente che attiva l'autenticazione a due fattori.	
Vantaggi	Il vantaggio principale che si aggiunge un ulteriore livello di protezione all'account dell'utente.	
Flusso degli Eventi	Utente	Sistema
	1. Tommaso accede con le credenziali.	2. Il sistema verifica le credenziali e se sono corrette, reindirizza Tommaso alla dashboard.
	3. Tommaso si reca nella sezione Profilo.	4. Il sistema gli mostra la pagina del suo profilo.
	5. Tommaso sceglie di attivare l'autenticazione a due fattori.	6. Il sistema gli mostra la pagina di attivazione.
	7. Tommaso clicca su "attiva autenticazione a due fattori".	8. Il sistema mostra il codice di attivazione.
	9. Tommaso inserisce il codice, attiva l'autenticazione a due fattori sul proprio dispositivo e inserisce il codice visualizzato.	10. Il sistema conferma l'operazione



Nome Scenario	SC_FU_04: Funzionalità Utente – Segnalazione di un falso positivo	
Partecipanti	Danilo: l'amministratore di un'azienda	
Descrizione	Lo scenario mostra l'amministratore che etichetta un'anomalia come falso positivo.	
Vantaggi	Il vantaggio principale che si ha nel segnalare un falso positivo è migliorare l'accuratezza del sistema e in secondo luogo ridurre i falsi allarmi.	
Flusso degli Eventi	Utente	Sistema
	1. Danilo accede al sistema inserendo email e password.	2. Il sistema verifica le credenziali e se sono corrette gli mostra la dashboard.
	3. Danilo si reca nella sezione relativa alle anomalie.	4. Il sistema mostra correttamente questa pagina.
	5. Danilo le esamina e conclude che una di essa in realtà non è una vera e propria minaccia così segnala che l'evento è un falso positivo.	6. Il sistema riceve il suo comando e aggiorna lo stato dell'anomalia.



Nome Scenario	SC_FU_01: Funzionalità Sistema – Visualizza Traffico Analizzato	
Partecipanti	Danilo: l'utente che lavora in un'azienda	
Descrizione	Lo scenario mostra l'utente che accede alla dashboard dell'azienda per avere un resoconto del traffico analizzato.	
Vantaggi	Il vantaggio principale che si ha è la chiarezza di cosa è stato analizzato e in che categoria si trova.	
Flusso degli Eventi	Utente	Sistema
	1. Danilo accede con l'email e la password.	2. Il sistema verifica le credenziali e se corrette, Danilo viene reindirizzato alla Dashboard.
	3. Danilo si reca nella sezione relativa al traffico analizzato.	4. Il sistema mostra il resoconto del traffico analizzato.
	5. Danilo può correttamente visualizzarlo.	



Nome Scenario	SC_FS_01: Funzionalità Sistema – Ricezione Traffico	
Partecipanti	Azienda: l'azienda di un cliente la cui rete genera traffico da analizzare	
Descrizione	Lo scenario mostra come il traffico di rete generato da parte dell'azienda viene ricevuto dal sistema.	
Vantaggi	Il vantaggio principale che si ha è l'efficienza e affidabilità.	
Flusso degli Eventi	Azienda	Sistema
	1. La rete dell'azienda di Giuseppe invia il traffico generato al sistema, tramite sniffer o protocollo di rete.	2. Il sistema riceve il traffico di rete generato e ne memorizza le informazioni.
	3. La rete dell'azienda continua a generare e inviare traffico.	



Nome Scenario	SC_FU_02: Funzionalità Utente – Modifica Piano	
Partecipanti	Giuseppe: l'amministratore di un'azienda	
Descrizione	Lo scenario mostra l'amministratore che modifica il piano della sua azienda per soddisfare al meglio le proprie esigenze.	
Vantaggi	Il vantaggio principale che si ha è la flessibilità per l'azienda di scegliere un piano adatto in base alle proprie esigenze.	
Flusso degli Eventi	Amministratore	Sistema
	1. Giuseppe ha bisogno di modificare il piano d'abbonamento dell'azienda, così accede con le sue credenziali.	2. Il sistema verifica le credenziali e se corrette, porta Giuseppe alla Dashboard.
	3. Giuseppe si reca nella pagina utente e va nella sezione del piano d'abbonamento.	4. Il sistema gli mostra la pagina utente e le informazioni relative al piano attualmente attivo.
	5. Giuseppe sceglie di modificare il piano d'abbonamento.	6. Il sistema gli mostra una pagina con tutti i piani a disposizione e i relativi prezzi.
	7. Giuseppe sceglie il nuovo piano d'abbonamento da sottoscrivere.	8. Il sistema fa procedere Giuseppe all'acquisto.
	9. Giuseppe completa l'acquisto.	

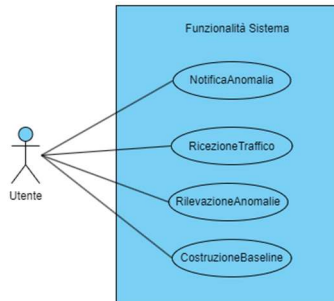


Nome Scenario	SC_GA_02: Gestione Accesso – Logout	
Partecipanti	Mattia: l'utente che lavora in una azienda	
Descrizione	Lo scenario mostra l'utente che termina la sua sessione nel sistema disconnettendosi.	
Vantaggi	Assicura che l'utente possa uscire in modo sicuro dal sistema evitando accessi non autorizzati a causa di sessioni non terminate.	
Flusso degli Eventi	Utente	Sistema
	1. Mattia vuole disconnettersi dal sistema così clicca sul tasto del logout.	2. Il sistema chiede a Mattia se è sicuro di volersi disconnettere.
	3. Mattia clicca di sì.	4. Il sistema termina la sessione di Mattia e lo reindirizza alla pagina di login.

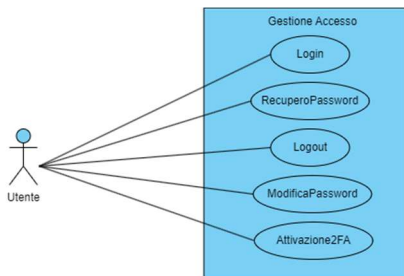


Nome Scenario	SC_FU_03: Funzionalità Utente – Gestione Utenti	
Partecipanti	Mattia: l'amministratore di un'azienda	
Descrizione	Lo scenario mostra l'amministratore che modifica i permessi concessi a dipendenti della stessa, registrati nel sistema.	
Vantaggi	Il vantaggio principale che si ha è la rapida gestione di permessi per tutti gli utenti di un'azienda registrati nel sistema.	
Flusso degli Eventi	Amministratore	Sistema
	1. Mattia accede con l'email e la password.	2. Il sistema verifica le credenziali e, se corrette, manda Mattia alla dashboard.
	3. Mattia si reca nella sezione dedicata agli utenti subordinati.	4. Il sistema gli mostra tutti gli utenti subordinati associati all'azienda e i loro permessi.
	5. Mattia sceglie di gestire un utente.	6. Il sistema gli mostra tutti i dati disponibili.
	7. Mattia apporta le opportune modifiche e conferma.	

3.4.2 Use Case



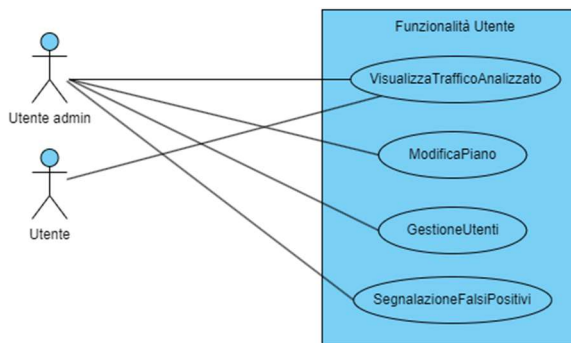
Identificativo UC_FS_04	Notifica di una anomalia	Data		09/11/2023
		Vers.		0.00.001
		Autore		De Simone Edmondo
Descrizione	Il caso d'uso specifica che un attore riceve una notifica al rilevamento di una anomalia.			
Attore Principale	Utente Colui che lavora in un'azienda.			
Attori secondari	Azienda È l'azienda dell'amministratore la cui rete genera traffico			
Entry Condition	L'utente deve aver configurato le preferenze di notifica del sistema.			
Exit condition On success	L'utente ha ricevuto con successo la notifica.			
Exit condition On failure	L'utente non riceve la notifica.			
Rilevanza/User Priority	Alta			
Frequenza stimata	100/settimana			
Extension point	N/A			
Generalization of	N/A			
FLUSSO DI EVENTI PRINCIPALE/MAIN SCENARIO				
1	Azienda:	Effettua traffico di rete.		
2	Sistema:	Analizza il traffico di rete.		
3	Sistema:	Rileva un'anomalia.		
4	Sistema:	Invia la notifica all'amministratore.		
5	Utente:	Riceve la notifica con successo.		
I Scenario/Flusso di eventi Alternativo: Anomalia non rilevata				
3.1	Sistema:	Non rileva alcuna anomalia nel traffico di rete.		
3.2	Sistema:	Prosegue con l'analisi del traffico.		
Special Requirements	Il sistema deve continuamente monitorare il traffico di rete.			



Identificativo UC_GA_04	Modifica password	Data	09/11/2023
		Vers.	0.00.001
		Autore	Maiellaro Vincenzo
Descrizione	Il caso d'uso mostra la modifica della password da parte di un utente.		
Attore Principale	Utente Colui che lavora in una azienda.		
Attori secondari	N/A		
Entry Condition	L'utente deve possedere un account.		
Exit condition On success	L'utente modifica con successo la reportistica.		
Exit condition On failure	L'utente non modifica la password.		
Rilevanza/User Priority	Media		
Frequenza stimata	1/mese		
Extension point	N/A		
Generalization of	N/A		
FLUSSO DI EVENTI PRINCIPALE/MAIN SCENARIO			
1	Utente:	Si reca nella sezione relativa ai suoi dati personali.	
2	Sistema:	Mostra la pagina relativa ai dati personali dell'utente.	
3	Utente:	Imposta una nuova password.	
4	Sistema:	Aggiorna e sostituisce la password precedente.	
I Scenario/Flusso di eventi Alternativo			
3.1	Sistema:	Visualizza un messaggio con scritto che la password non rispetta i requisiti di sicurezza.	
Note		N/A	
Special Requirements		La password deve essere lunga almeno 8 caratteri, deve contenere almeno una lettera maiuscola, un numero e un carattere speciale.	



Identificativo UC_GA_05	Attivazione 2FA	Data	09/11/2023
		Vers.	0.00.001
		Autore	Nardi Tommaso
Descrizione	Il caso d'uso mostra il processo di attivazione, da parte dell'utente, dell'autenticazione a due fattori.		
Attore Principale	Utente Colui che è registrato al sistema.		
Attori secondari	N/A		
Entry Condition	L'utente effettua l'accesso alla piattaforma.		
Exit condition On success	L'utente attiva con successo il 2FA.		
Exit condition On failure	Il sistema non permette di effettuare l'attivazione.		
Rilevanza/User Priority	Alta		
Frequenza stimata	5/giorno		
Extension point	N/A		
Generalization of	N/A		
FLUSSO DI EVENTI PRINCIPALE/MAIN SCENARIO			
1	Utente:	Si reca nella sezione relativa al proprio account.	
2	Sistema:	Mostra la pagina.	
3	Utente:	Seleziona di visualizzare la pagina del 2FA	
4	Sistema:	Riceve il comando e mostra all'utente la pagina relativa al 2FA.	
5	Utente:	Sceglie di attivare il 2FA.	
6	Sistema:	Mostra i codici per l'attivazione del 2FA.	
7	Utente:	Attiva il 2FA sul proprio dispositivo e inserisce il codice visualizzato.	
8	Sistema:	Conferma l'operazione e riporta l'utente alla pagina dell'account	
Note	N/A		
Special Requirements	Il 2FA del sistema deve essere compatibile con le applicazioni di 2FA più utilizzate.		



Identificativo UC_FU_04	Segnalazione di falsi positivi	Data	09/11/2023
		Vers.	0.00.001
		Autore	Gisolfi Danilo
Descrizione	Il caso d'uso mostra l'etichettatura di un falso positivo da parte di un utente che trova una finta minaccia.		
Attore Principale	Amministratore È il dirigente di un'azienda.		
Attori secondari	N/A		
Entry Condition	L'utente admin effettua l'accesso alla piattaforma.		
Exit condition On success	L'utente admin segnala con successo il falso positivo.		
Exit condition On failure	Il sistema non permette di effettuare la segnalazione.		
Rilevanza/User Priority	Alta		
Frequenza stimata	1/giorno		
Extension point	N/A		
Generalization of	N/A		
FLUSSO DI EVENTI PRINCIPALE/MAIN SCENARIO			
1	Amministratore:	Si reca nella sezione relativa alle anomalie.	
2	Sistema:	Mostra la pagina.	
3	Amministratore:	Etichetta una minaccia come falso positivo.	
4	Sistema:	Riceve il comando e aggiorna la pagina.	
5	Amministratore:	Vede la pagina correttamente aggiornata.	
I Scenario/Flusso di eventi Alternativo: Il sistema non riceve il comando			
4.1	Sistema:	Mostra una pagina di errore oppure un messaggio di errore con scritto di riprovare più tardi o di contattare l'assistenza.	
Note	N/A		
Special Requirements	L'utente admin deve spiegare perché non è una vera minaccia.		

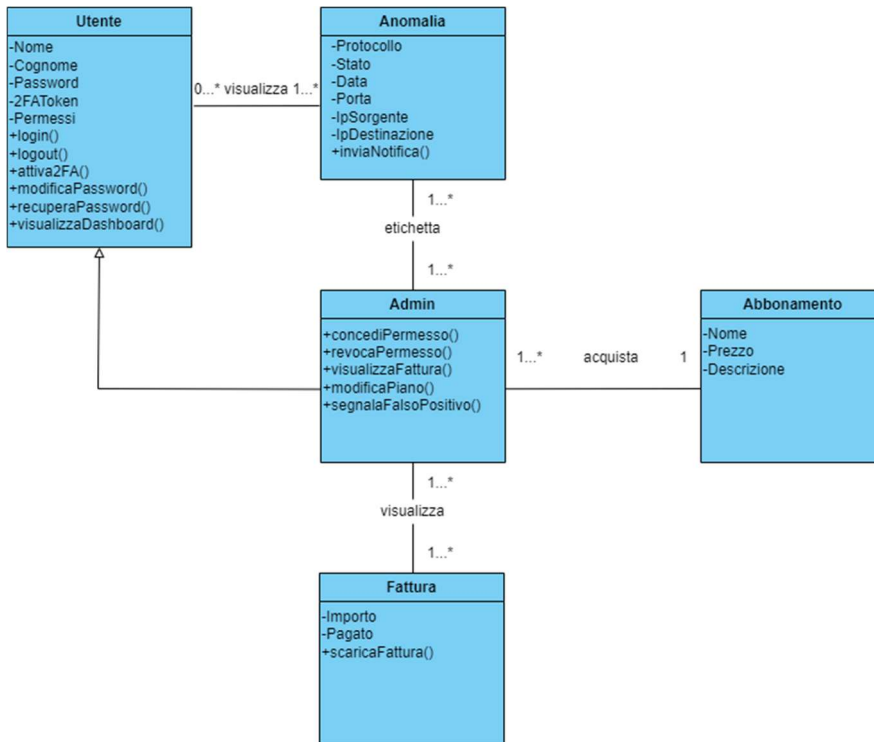


Identificativo UC_FU_02		Modifica Piano	Data	09/11/2023
			Vers.	0.00.001
			Autore	Cerella Giuseppe
Descrizione		Il caso d'uso mostra come l'amministratore di un'azienda viene guidato alla modifica del piano già acquistato.		
Attore Principale		Amministratore È il dirigente di un'azienda.		
Attori secondari		N/A		
Entry Condition		L'amministratore effettua l'accesso alla piattaforma.		
Exit condition On success		Il sistema conferma l'acquisto di un nuovo piano.		
Exit condition On failure		Il sistema non riesce a confermare l'acquisto.		
Rilevanza/User Priority		Media		
Frequenza stimata		3/giorno		
Extension point		N/A		
Generalization of		N/A		
FLUSSO DI EVENTI PRINCIPALE/MAIN SCENARIO				
1	Amministratore:	Si reca nella sezione relativa al piano acquistato.		
2	Sistema:	Mostra la pagina.		
3	Amministratore:	Seleziona la voce per modificare il piano.		
4	Sistema:	Mostra la pagina del negozio.		
5	Amministratore:	Sceglie il nuovo piano che intende acquistare.		
6	Sistema:	Mostra la pagina del checkout.		
7	Amministratore:	Sceglie il metodo di pagamento.		
8	Sistema:	Crea la finestra di pagamento.		
9	Amministratore:	Effettua il pagamento inserendo i dati della carta.		
10	Sistema:	Conferma il pagamento, aggiorna i dati del piano e riporta l'utente alla pagina del profilo.		
I Scenario/Flusso di eventi Alternativo: Finestra del pagamento scaduta				
8.1	Amministratore:	Non effettua il pagamento nella finestra di tempo concessa.		
8.2	Sistema:	Genera un'altra finestra di pagamento.		
Note		N/A		
Special Requirements		Il sistema deve permettere l'utilizzo di vari tipi di metodi di pagamento (es: Carte di Credito, Carte di Debito, PayPal).		



Identificativo UC_FU_03	Gestione Utenti	Data	09/11/2023
		Vers.	0.00.001
		Autore	Guariglia Mattia
Descrizione	Il caso d'uso specifica come un amministratore di un'azienda può gestire gli account delegati.		
Attore Principale	Amministratore È il dirigente di un'azienda.		
Attori secondari	N/A		
Entry Condition	L'amministratore effettua l'accesso alla piattaforma.		
Exit condition On success	L'amministratore completa con successo la gestione dell'utente delegato.		
Exit condition On failure	Il sistema non permette il compimento dell'azione.		
Rilevanza/User Priority	Alta		
Frequenza stimata	5/giorno		
Extension point	N/A		
Generalization of	N/A		
FLUSSO DI EVENTI PRINCIPALE/MAIN SCENARIO			
1	Amministratore:	Si reca nella sezione relativa agli utenti subordinati.	
2	Sistema:	Mostra la pagina con i dettagli.	
3	Amministratore:	Sceglie di gestire un utente subordinato.	
4	Sistema:	Mostra tutte le informazioni disponibili relative all'utente subordinato selezionato.	
5	Amministratore:	Effettua le opportune azioni riguardanti: <ul style="list-style-type: none">EmailPasswordNomeCognomePermessi Infine conferma.	
6	Sistema:	Applica le modifiche o inserisce l'utente delegato e visualizza un messaggio di conferma.	
Note	N/A		
Special Requirements	Solo l'utente admin deve poter gestire gli account delegati.		

3.4.3 Modello ad Oggetti



3.4.3.1 Diagrammi delle entità

Nome	Tipologia	Descrizione
Utente	Entity	Rappresenta un singolo utente che può essere sia standard che admin.
Abbonamento	Entity	Rappresenta un singolo piano d'abbonamento.
Segnalazione	Entity	Rappresenta una singola segnalazione.



3.4.3.2 Diagrammi ad Oggetti

Nome	Tipologia	Descrizione
ProfiloButton	Boundary	Bottone, presente nella dashboard, usato dall'utente per accedere alla pagina riguardante i suoi dati personali.
NuovaPasswordForm	Boundary	Form usata dall'utente per inserire la nuova password e confermarla.
2FA_A_Button	Boundary	Bottone usato dall'utente per attivare l'autenticazione a due fattori.
2FA_A_Confirm	Boundary	Bottone usato dall'utente per confermare la volontà di attivare l'autenticazione a due fattori.
2FA_A_Code	Boundary	Form usata dall'utente per inserire il codice generato dall'applicazione utilizzata per l'autenticazione a due fattori.
EtichettaButton	Boundary	Bottone usato dall'utente per etichettare una segnalazione ricevuta come falso positivo.
PianoAbbonamentoButton	Boundary	Bottone usato dall'utente per accedere ai piani d'abbonamento disponibili.
PagamentoForm	Boundary	Form compilata dall'utente per inserire i dati riguardanti un metodo di pagamento.
AziendaButton	Boundary	Bottone usato dall'utente admin per accedere alla pagina relativa agli utenti della propria azienda.



Gest_Dip_Button	Boundary	Bottone usato dall'utente admin per gestire un utente subordinato.
Gest_Dip_Form	Boundary	Form usata dall'utente admin per gestire i dati relativi a un utente subordinato.
InviaNotificaControl	Control	Control che coordina le operazioni relative all'invio della notifica al rilevamento di una anomalia.
SezioneAnomalieControl	Control	Control che coordina le operazioni relative alle anomalie rilevate e salvate nella dashboard.
ProfiloControl	Control	Control che coordina le operazioni relative al profilo dell'utente della sessione.
AggiornaPasswordControl	Control	Control che coordina le operazioni relative all'aggiornamento della password.
AziendaControl	Control	Control che coordina le operazioni relative alla ricerca degli account dell'azienda.
Gest_Dip_Control	Control	Control che coordina le operazioni relative alla gestione di utenti subordinati.
2FA_A_Control	Control	Control che coordina le operazioni relative all'attivazione dell'autenticazione a due fattori.
SegnalazioneFalsoPositivo Control	Control	Control che coordina le operazioni relative all'etichettatura di una minaccia che in realtà è un falso positivo.

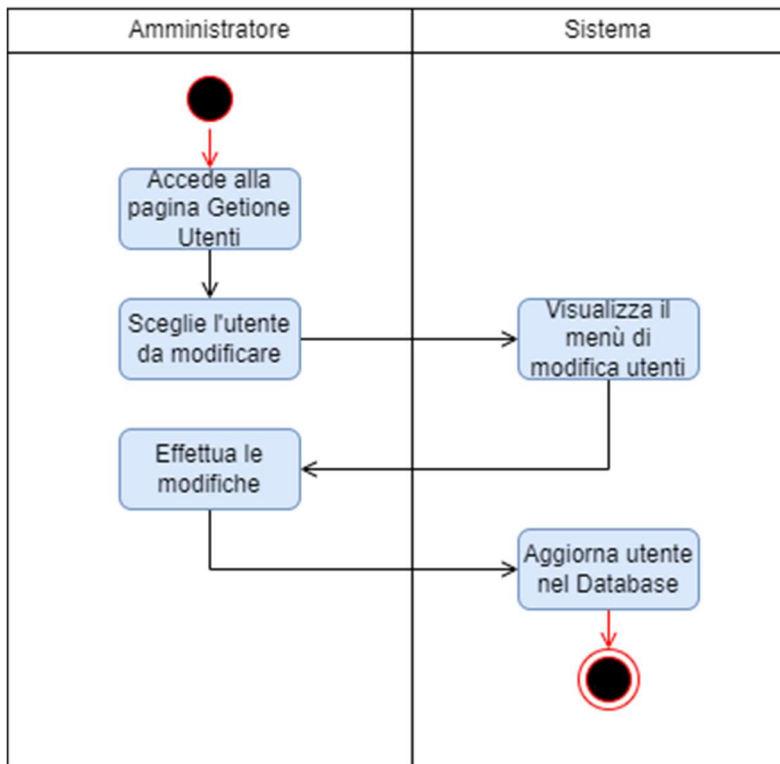


ModificaPianoControl	Control	Control che coordina le operazioni relative alla modifica del piano d'abbonamento.
ActivationVerifier	Control	Control che verifica se l'utente ha attivato l'autenticazione a due fattori.

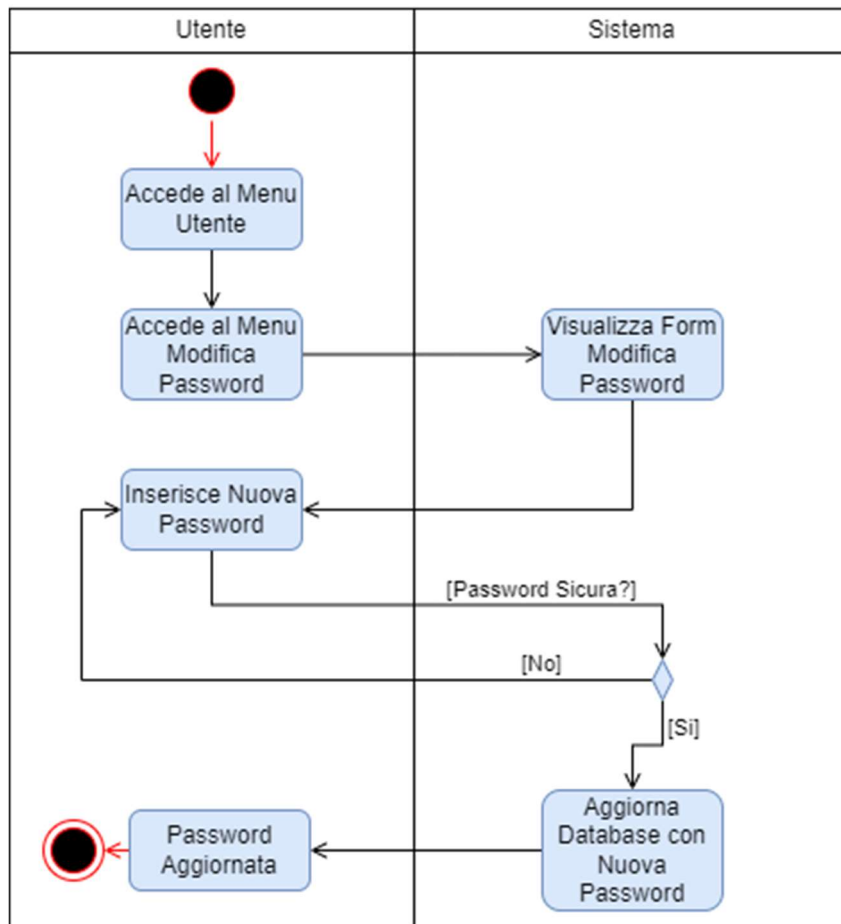
3.4.4 Modello Dinamico

3.4.4.1 Activity Diagrams

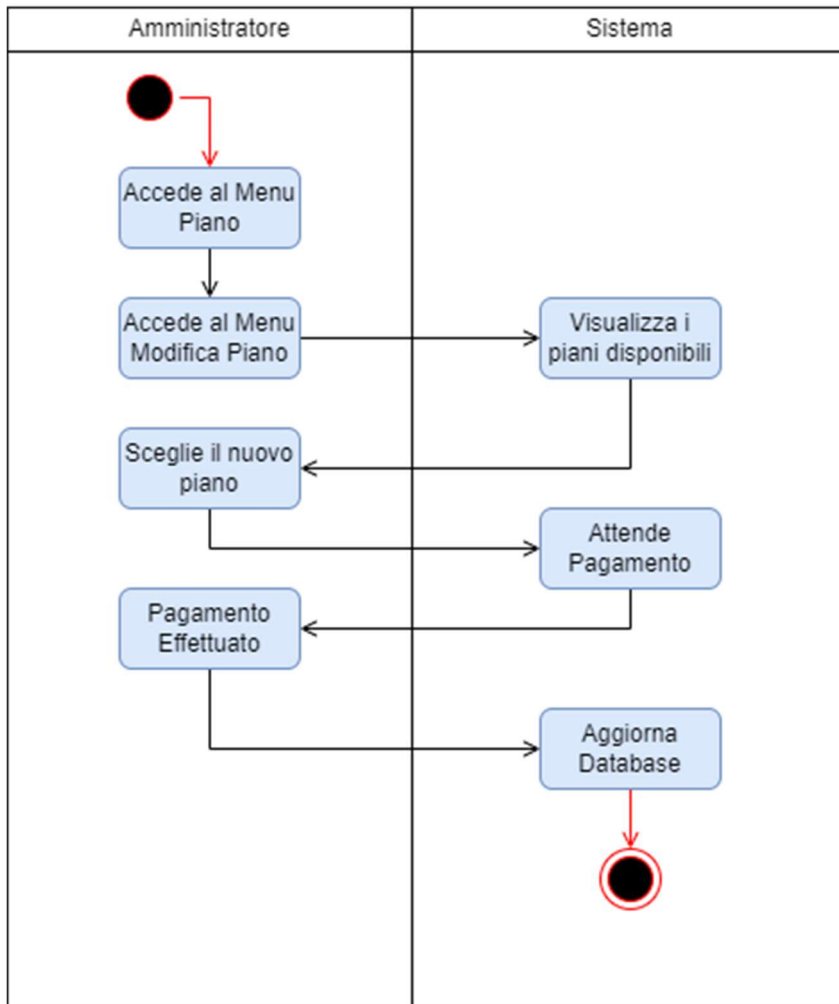
AD_FU_03 - De Simone - Cerella



AD_GA_04 - Gisolfi - Nardi

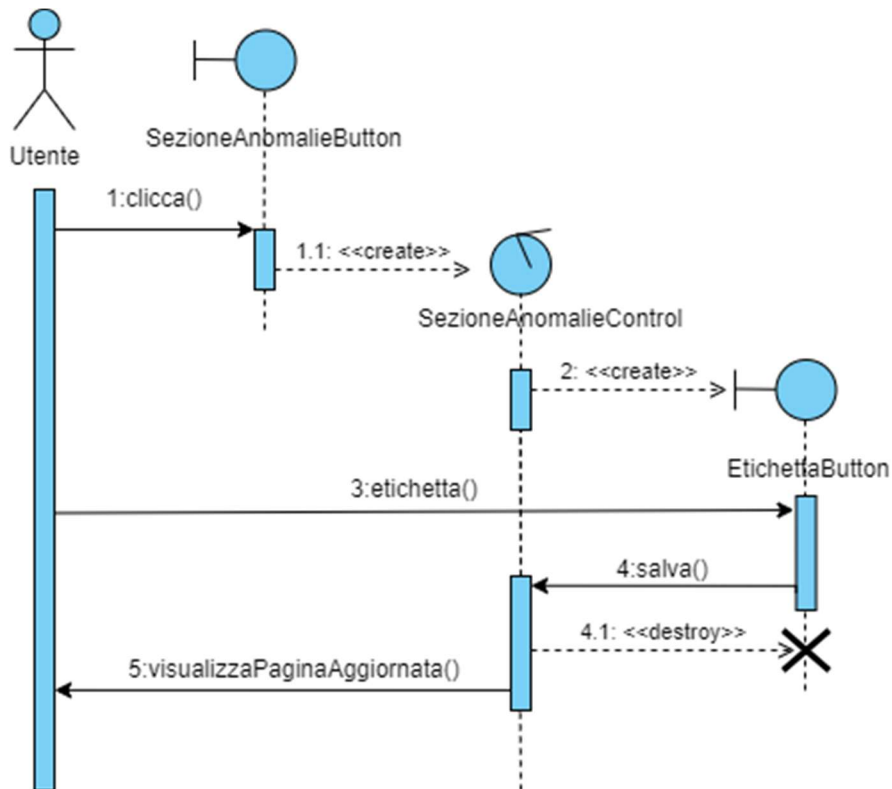


AD_FU_02 - Guariglia - Maiellaro

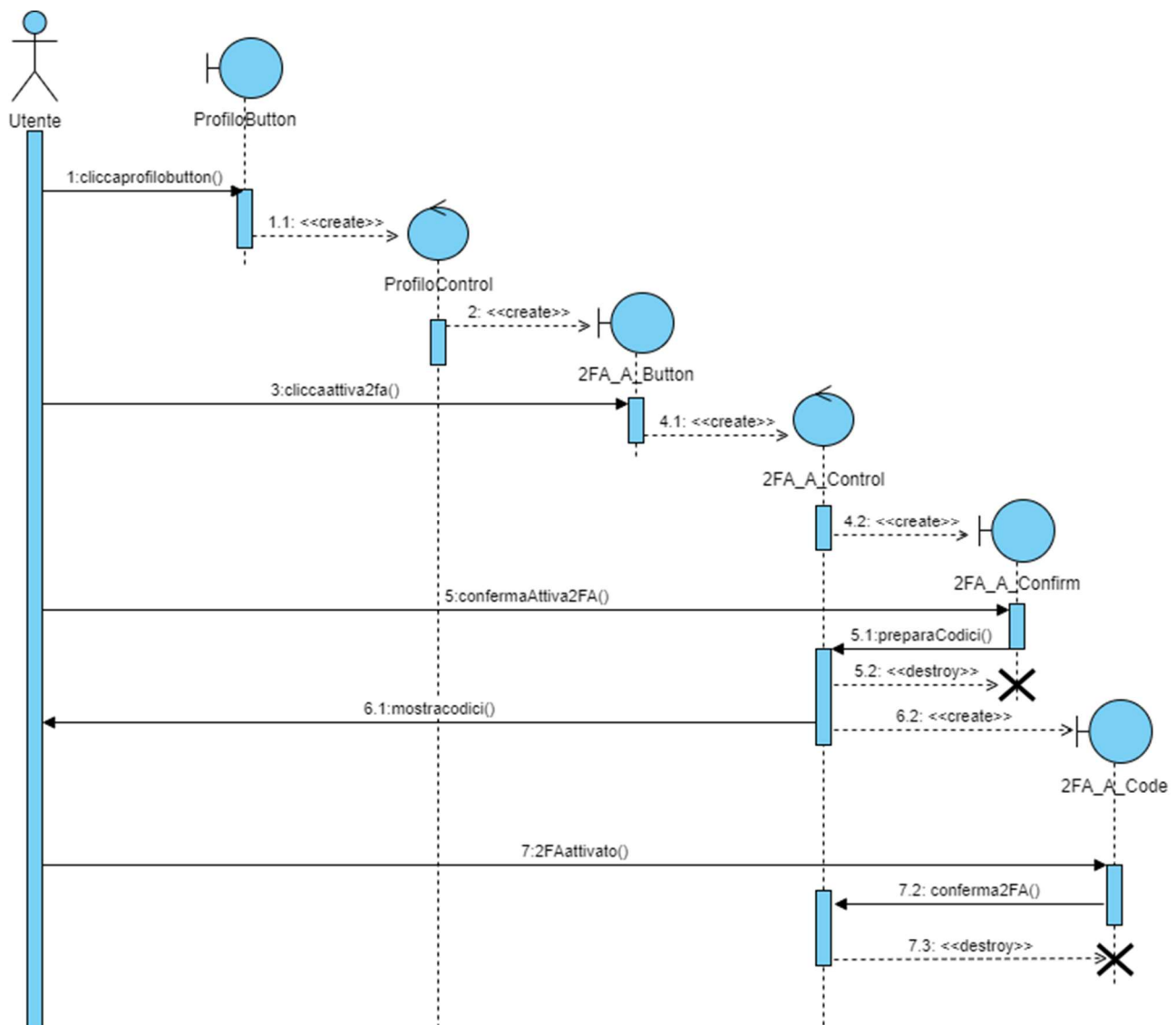


3.4.4.2 SequenceDiagrams

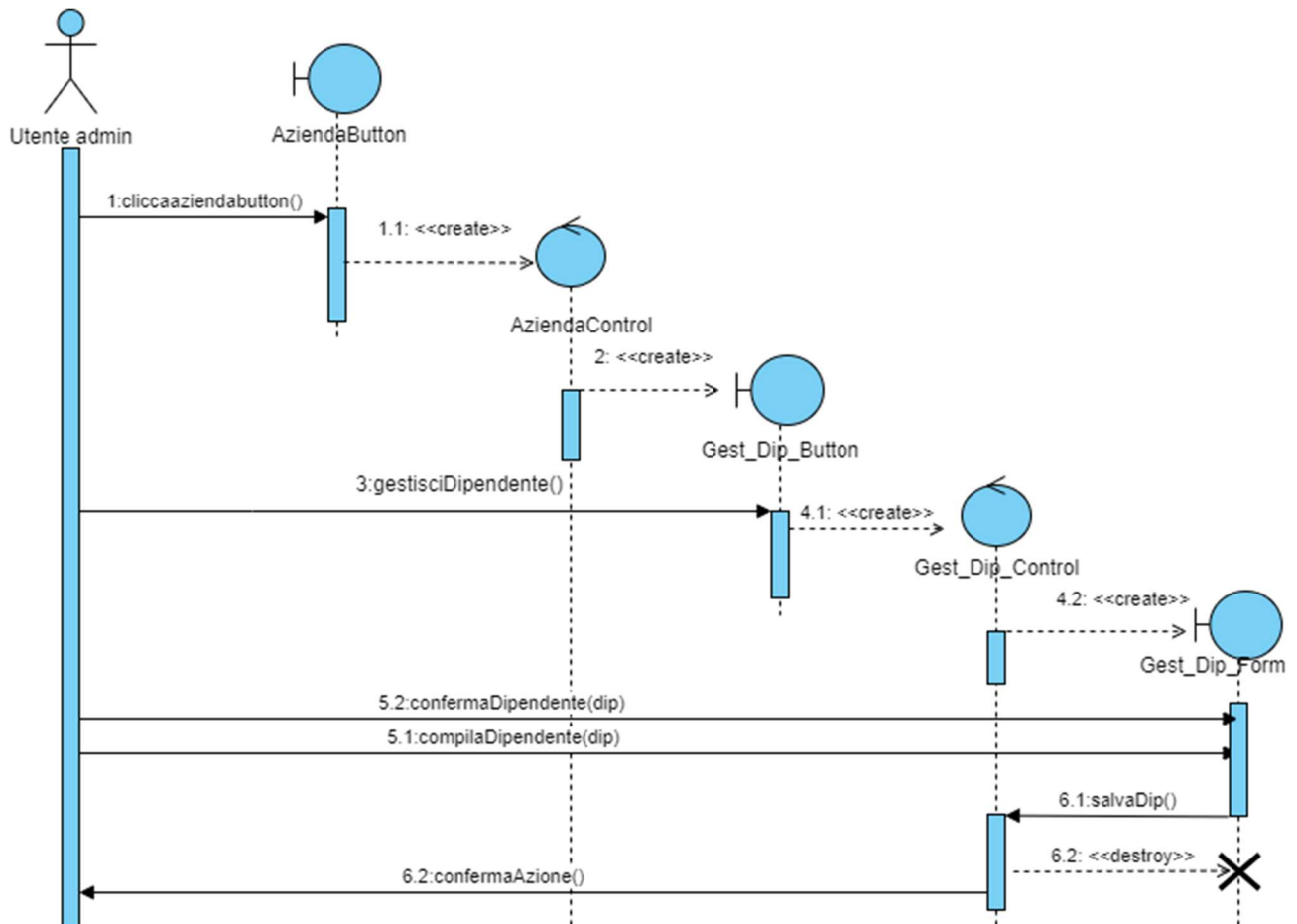
SD_FU_04 SegnalazioneFalsiPositivi – De Simone - Cerella



SD_GA_05 Attiva2FA – Gisolfi - Nardi

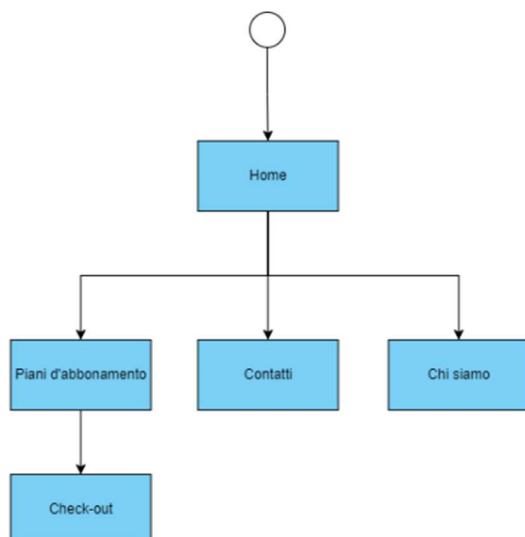


SD_FU_03 GestioneUtenti - Guariglia - Maiellaro

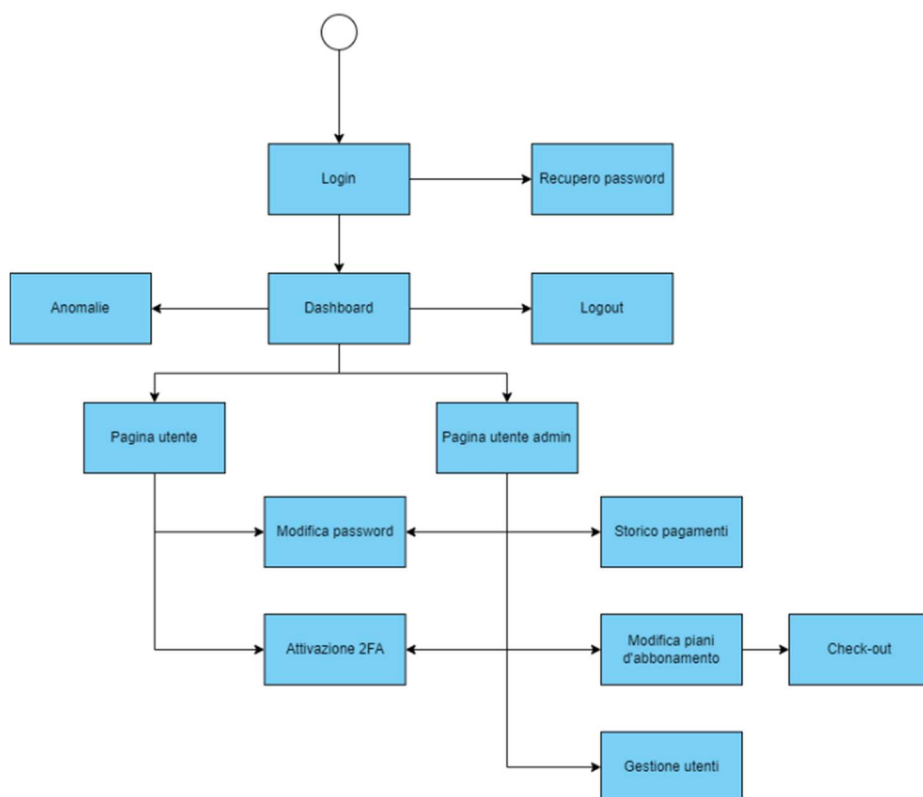


3.4.5 Interfaccia Utente – Percorsi di Navigazione e Mock-up

3.4.5.1 NP_01 Percorsi di navigazione da parte dell'acquirente



3.4.5.2 NP_02 Percorsi di navigazione da parte degli utenti





3.4.5.2 Mock-up

UI_GA_01 HOME



[HOME](#) [PIANI](#) [CHI SIAMO](#) [CONTATTI](#)

Benvenuto su Guardian Flow!

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse



UI_FU_02 PAGINA SCELTA PIANO



[HOME](#) [PIANI](#) [CHI SIAMO](#) [CONTATTI](#)

Scegli il piano più adatto a te

Basic	Starter	Medium	Advance
Acquista	Acquista	Acquista	Acquista



UI_FU_03 PAGINA CHECKOUT



[HOME](#) [PIANI](#) [CHI SIAMO](#) [CONTATTI](#)

Cosa include il piano Basic

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse

Check-out

Nome	<input type="text"/>	Cognome	<input type="text"/>
Nome azienda	<input type="text"/>	P.IVA	<input type="text"/>
Email	<input type="text"/>	Numero di telefono	<input type="text"/>
Indirizzo di fatturazione	<input type="text"/>	CAP	<input type="text"/>

PAGA

UI_GA_02 PAGINA CONTATTI



[HOME](#) [PIANI](#) [CHI SIAMO](#) [CONTATTI](#)

Contattaci

Hai bisogno di maggiori informazioni?

Non esitare a contattarci, il nostro team addetto alle vendite sarà pronto a rispondere alle tue domande.

Numero Verde
(attivo dal Lun-Ven dalle 8:00 alle 19:00)

803 404 404

Oppure tramite e-mail
info@guardianflow.com

INVIA UN EMAIL

Email	<input type="text"/>
Nome e cognome	<input type="text"/>
Messaggio	<div></div>

INVIA



Laurea Triennale in informatica - Università di Salerno
Corso di *Ingegneria del Software* - Prof.ssa F. Ferrucci

UI_GA_03 LOGIN

Login

Email

Password

Hai dimenticato la password?

UI_GA_04 RESET PASSWORD

Hai dimenticato la tua password?

Inserisci l'indirizzo e-mail associato al tuo account e
ti invieremo un link per reimpostare la tua password.

Email



UI_FU_01 DASHBOARD



Ciao, Giuseppe

Benvenuto sulla Dashboard!

Security Warnings

Ultimi warning

	Age
Empty Relay Group Assigned	3 days
Empty Relay Group Assigned	5 days
Empty Relay Group Assigned	3 days
Empty Relay Group Assigned	3 days

Warnings Status



● Critical
● Warning
● Resolved

Il Tuo Account

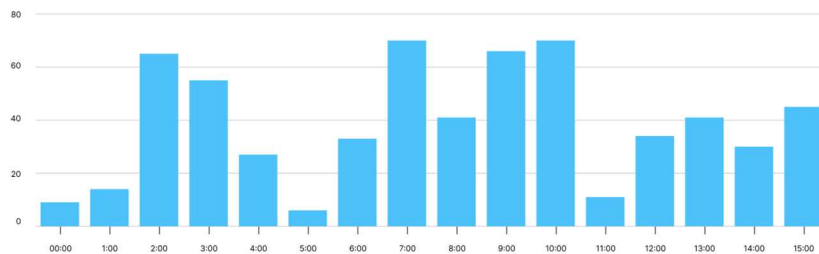
Master Admin

Permessi
Accesso Completo

Ultimo Log-in
7 Novembre 2023

33

Login nell'ultimo mese



UI_FU_04 PAGINA UTENTE – ADMIN



Ciao, Giuseppe

Ecco tutte le informazioni del tuo account!

Il Tuo Piano

Organization ATTIVO
Il nostro miglior piano per le aziende

50\$
al mese

Fatture da pagare

Visualizza fatture da pagare

SCARICA FATTURA PDF

PAGA ORA

UPGRADE

Login History

	DATA	ESITO
●	7 Novembre 2023	Successo
●	5 Novembre 2023	Successo
●	31 Ottobre 2023	Successo
●	29 Ottobre 2023	Successo
●	18 Ottobre 2023	Successo

Account Info

Nome e Cognome: Giuseppe Cerella
Email: g.cerella@gmail.com
Permessi: Master Admin

MODIFICA
PASSWORD

Autenticazione a due fattori



NON ATTIVA ●

Storico pagamenti

Data pagamento	Mensilità	Totale	Stato	Tipo Piano	Opzioni
05/07/2023	Ottobre	394€	Pagato ●	Basic	...
05/07/2023	Ottobre	394€	Pagato ●	Basic	...



UI_GA_05 MODIFICA DELLA PASSWORD

Ciao, Giuseppe
Ecco tutte le informazioni del tuo account!

Modifica la tua password

Password attuale

Nuova Password

Conferma Password

MODIFICA PASSWORD

ESITO
Successo
Successo
Successo
Successo

Storico pagamenti

Data pagamento	Mensilità	Totale	Stato	Tipo Piano	Opzioni
05/07/2023	Ottobre	394€	Pagato	Basic	...
05/07/2023	Ottobre	394€	Pagato	Basic	...
05/07/2023	Ottobre	394€	Pagato	Basic	...

UI_FU_05 STORICO PAGAMENTI – ADMIN

Storico pagamenti

Data pagamento	Mensilità	Totale	Stato	Tipo Piano	Opzioni
05/07/2023	Ottobre	394€	Pagato	Basic	...
05/07/2023	Ottobre	394€	Pagato	Basic	...
05/07/2023	Ottobre	394€	Pagato	Basic	...
05/07/2023	Ottobre	394€	Pagato	Basic	...
05/07/2023	Ottobre	394€	Pagato	Basic	...
05/07/2023	Ottobre	394€	Pagato	Basic	...
05/07/2023	Ottobre	394€	Pagato	Basic	...
05/07/2023	Ottobre	394€	Pagato	Basic	...
05/07/2023	Ottobre	394€	Pagato	Basic	...
05/07/2023	Ottobre	394€	Pagato	Basic	...



STORICO PAGAMENTI – ADMIN ONCLIK



Storico pagamenti

Data pagamento	Mensilità	Totale	Stato	Tipo Piano	Opzioni
05/07/2023	Ottobre	394€	Pagato 	Basic	<div><div><div></div></div><div>Fattura Elimina</div></div>
05/07/2023	Ottobre	394€	Pagato 	Basic	
05/07/2023	Ottobre	394€	Pagato 	Basic	...
05/07/2023	Ottobre	394€	Pagato 	Basic	...
05/07/2023	Ottobre	394€	Pagato 	Basic	...
05/07/2023	Ottobre	394€	Pagato 	Basic	...
05/07/2023	Ottobre	394€	Pagato 	Basic	...
05/07/2023	Ottobre	394€	Pagato 	Basic	...
05/07/2023	Ottobre	394€	Pagato 	Basic	...
05/07/2023	Ottobre	394€	Pagato 	Basic	...

UI_FU_06 GESTIONE UTENTE – ADMIN



Laurea Triennale in informatica - Università di Salerno Corso di *Ingegneria del Software* - Prof.ssa F. Ferrucci



Gestione utenti



Utenti



Creazione	Email	Permessi	Ultimo accesso	Opzioni
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...

GESTIONE UTENTE – ADMIN ONCLICK



Gestione utenti



Utenti



Creazione	Email	Permessi	Ultimo accesso	Opzioni
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...
05/07/2023	edmondo888@gmail.com	Moderatore	07/07/2023	...



Modifica
Elimina

GESTIONE UTENTI – CREA ACCOUNT SUBORDINATO



Gestione utenti



Utenti



Crea un account subordinato

E-mail

Password

Permessi



Conferma Password

SALVA

USER PAGE – SUBORDINATO



Ciao, Tommaso

Ecco tutte le informazioni del tuo account!



Account Info

Nome e Cognome: Tommaso Nardi
Email: t.nardi@gmail.com
Permessi: Moderatore

MODIFICA
PASSWORD

Autenticazione a due fattori



NON ATTIVA



Login History

	DATA	ESITO
●	7 Novembre 2023	Successo
●	5 Novembre 2023	Successo
●	31 Ottobre 2023	Successo
●	29 Ottobre 2023	Successo
●	18 Ottobre 2023	Successo

UI_FU_06 ANOMALIE PAGE



Anomalie

Identificativo	Data rilevazione	Protocollo	Porta	IP Sorgente	IP Destinazione	Stato	Opzioni
1	20/11/2023	Protocollo	Porta	192.0.0.0	193.0.0.0	●	...
1	20/11/2023	Protocollo	Porta	192.0.0.0	193.0.0.0	●	...
1	20/11/2023	Protocollo	Porta	192.0.0.0	193.0.0.0	●	...
1	20/11/2023	Protocollo	Porta	192.0.0.0	193.0.0.0	●	...
1	20/11/2023	Protocollo	Porta	192.0.0.0	193.0.0.0	●	...
1	20/11/2023	Protocollo	Porta	192.0.0.0	193.0.0.0	●	...
1	20/11/2023	Protocollo	Porta	192.0.0.0	193.0.0.0	●	...
1	20/11/2023	Protocollo	Porta	192.0.0.0	193.0.0.0	●	...
1	20/11/2023	Protocollo	Porta	192.0.0.0	193.0.0.0	●	...
1	20/11/2023	Protocollo	Porta	192.0.0.0	193.0.0.0	●	...



4. Glossario

A

Appliance

In alcuni casi, le reti possono essere progettate in modo tale che la maggior parte delle funzionalità di rete sia gestita attraverso l'uso di appliance, cioè dispositivi hardware specifici progettati per scopi particolari all'interno della rete.

B

Baseline

Un insieme di dati correlati, rappresentativi del traffico ordinario e delle attività aziendali, utilizzato per addestrare un modello di intelligenza artificiale. Questo gruppo di dati è essenziale per garantire che il modello sia ben adattato alle condizioni reali dell'azienda, consentendo un apprendimento efficace e una migliore capacità predittiva nei confronti delle operazioni quotidiane dell'azienda.

I

Infrastruttura digitale

L'infrastruttura digitale è il sistema di componenti tecnologiche e risorse informatiche che costituiscono la base per la gestione, lo scambio e l'elaborazione di informazioni digitali.

Intelligenza artificiale

L'intelligenza artificiale è un campo dell'informatica che si occupa dello sviluppo di sistemi e programmi informatici in grado di eseguire compiti che richiedono tipicamente l'intelligenza umana. Questi compiti includono il riconoscimento di modelli, il linguaggio naturale, la risoluzione di problemi, l'apprendimento e l'adattamento a nuove situazioni.

F

Firewall

Un firewall è un dispositivo hardware o software progettato per monitorare, filtrare e controllare il traffico di rete tra una rete privata e una rete pubblica (come Internet).

Firme

Vengono utilizzate per identificare e rilevare comportamenti sospetti o dannosi all'interno di sistemi informatici, esse, sono contenute in database di firme, i quali associano ad ogni firma informazioni su modelli di comportamento associati a malware, intrusioni o minacce alla sicurezza.



Flessibilità

La flessibilità è la capacità di adattarsi, piegarsi o modificarsi facilmente in risposta a nuove circostanze, cambiamenti o esigenze.

Framework

Un framework è un insieme di strumenti, librerie, convenzioni e linee guida che forniscono una struttura comune per lo sviluppo di software.

G

Gdpr

Il GDPR, o General Data Protection Regulation, è un regolamento dell'Unione Europea che disciplina la protezione dei dati personali dei cittadini dell'UE e dello Spazio Economico Europeo.

Login

È la procedura di accesso alla piattaforma che prevede, dopo aver effettuato una registrazione, l'inserimento delle credenziali d'accesso.

Logout

È la procedura di disconnessione dalla piattaforma a cui si aveva fatto accesso tramite l'opzione login.

P

Password

Generata quando si effettua la registrazione alla piattaforma si tratta di un insieme di caratteri utilizzato per accedere in modo univoco al sistema. Questa potrebbe essere cambiata successivamente a seguito di una richiesta da parte di un utente.

S

Scalabile

Un sistema scalabile è un sistema che può gestire un aumento del carico o delle risorse senza subire una significativa perdita di prestazioni. In altre parole, la scalabilità si riferisce alla capacità di un sistema di adattarsi e crescere efficacemente per gestire una quantità crescente di lavoro, traffico o dati.

Sistema

Un sistema informatico è un insieme di componenti hardware, software, reti e procedure che lavorano insieme per elaborare, memorizzare e trasmettere informazioni.



Subordinati

Un account subordinato è un account collegato a un account principale, spesso con livelli di accesso o autorizzazioni inferiori.

Supervisionato

Nell'ambito del machine learning, l'apprendimento supervisionato è un tipo di approccio in cui un modello viene addestrato su un insieme di dati di input e output noti.