Laurea Magistrale in informatica-Università di Salerno
Corso di *Gestione dei Progetti Software*- Prof.ssa F. Ferrucci

GUARDIAN FLOW

FEELING SAFE

Business Case

Guardian Flow

Riferimento	
Versione	0.3
Data	20/12/2023
Destinatario	Prof.ssa F. Ferrucci
Presentato da	Raffaele Mezza, Martina Mingione
Approvato da	

Sommario

Revision History

Data	Versione	Descrizione	Autori
07/11/2023	0.1	Prima stesura	Raffaele Mezza Martina Mingione
21/11/2023	0.2	Aggiunta riserva di contingenza	Raffaele Mezza Martina Mingione
20/12/2023	0.4	Modifca valore riserva di contingenza	Raffaele Mezza Martina Mingione

Business Case (BC) del Progetto

Guardian Flow

1. Introduzione

Guardian Flow, organizzazione leader nel settore della cybersecurity, si impegna a proteggere le aziende clienti da minacce digitali sempre più sofisticate. In un mondo in cui la sicurezza informatica è essenziale, Guardian Flow ha deciso di sollevare l'asticella dell'eccellenza con un nuovo progetto innovativo. Si propone lo sviluppo di un sistema avanzato di rilevazione delle anomalie nel traffico di rete al fine di anticipare e rilevare minacce digitali in tempo reale, superando le limitazioni dei metodi di rilevamento tradizionali.

2. Obiettivi di Business

Guardian Flow intende progettare una soluzione evoluta ed agile per la rilevazione degli attacchi informatici alle reti aziendali in modo da rendere la rilevazione più efficace e semplificare l'infrastruttura di rete dei clienti. A tal scopo si offre un sistema di rilevazioni basato su intelligenza artificiale non supervisionata eseguita in cloud per analizzare il traffico. Questo approccio non solo eleva l'efficacia della rilevazione, anticipando le minacce in tempo reale, ma semplifica anche l'infrastruttura di rete dei clienti, offrendo una soluzione agile ed evoluta.

3. Situazione Corrente e Problemi

I sistemi IDS (Intrusion Detection System) ed in particolare i NIDS (Network Intrusion Detection System) basano la rilevazione delle anomalie, nel traffico di rete, sul riconoscimento di firme o pattern noti di attacco. Questo approccio presenta dei limiti nell'affrontare attacchi complessi ed attacchi di tipo 0-day in quanto non rientrano negli elenchi di firme note, inoltre i virus polimorfi possono mutare la propria firma per eludere la rilevazione. Un ulteriore strategia implementata nei sistemi NIDS è il riconoscimento delle anomalie nel traffico di rete tramite un AI supervisionata, tale approccio però presenta dei limiti derivanti dall'addestramento con dataset etichettati poiché risulta inefficace nella rilevazione degli attacchi non noti.

Inoltre le aziende, per fronteggiare queste minacce, sono costrette ad investire in costosi appliance di sicurezza che risultano spesso complessi ed onerosi da gestire. Un secondo aspetto da considerare è che tali appliance hanno un hardware dimensionato per la quantità di traffico che dovranno analizzare, quindi al crescere delle esigenze dell'azienda dovrà essere rinnovato il costoso hardware. Infine, le aziende potrebbero avere esigenze variabili nel tempo, periodi di traffico elevati ed altri periodi con traffico debole, tutto ciò porta a non sfruttare a pieno l' hardware acquistato.

4. Assunzioni Critiche e Vincoli

Considerando il sistema proposto, sarà necessario che le aziende clienti possano inoltrarci il traffico di rete da analizzare. Il cliente si impegna a fornirci il traffico già anonimizzato senza riferimenti a persone o dipendenti. Le prestazioni del sistema saranno strettamente dipendenti dal pacchetto scelto dal cliente ed inoltre i tempi massimi garantiti nel rilevare eventuali anomalie vengono calcolati dal momento in cui il traffico del cliente viene ricevuto dal sistema.

5. Analisi delle Opzioni e Raccomandazioni

Ci sono tre opzioni:

- Non fare nulla: mantenere lo stato attuale, fornendo i servizi di IDS basati su firme attraverso appliance acquistati dal cliente. Questo approccio, tuttavia, limita la gamma di attacchi che possono essere rilevati;
- Implementare un servizio di IDS basato su AI non supervisionata ed eseguito su appliance: opzione di transizione che integra l'intelligenza artificiale non supervisionata mantenendo l'esecuzione su appliance. Tuttavia, questa scelta potrebbe presentare alcune limitazioni in termini di flessibilità e scalabilità;
- Implementare un servizio di IDS basato su AI non supervisionata ed eseguita su cloud.

I project manager raccomandano fortemente la terza opzione per consentire ai sistemi di rilevare gli attacchi 0-day e pattern sconosciuti, fornendo al contempo una maggiore flessibilità nella distribuzione del servizio e la gestione efficace dei volumi di traffico variabili delle aziende.

Si tratta di una soluzione avanzata che si allinea alle esigenze dinamiche e alle sfide sempre crescenti nel panorama della sicurezza informatica.

6. Requisisti di progetto preliminari

In linea con quanto precedentemente illustrato, il progetto dovrà fornire un servizio di rilevazione delle anomalie nel traffico di rete basato su AI non supervisionata e tecnologie cloud.
Per queste ragioni il sistema dovrà necessariamente offrire i seguenti servizi:

- Ricezione del traffico da analizzare;
- Creazione di una base-line personalizzata per ogni cliente;
- Analisi del traffico con AI non supervisionata;
- Notifiche tempestive per anomalie rilevate;
- Report sul traffico analizzato;
- Possibilità di cambiare facilmente il pacchetto acquistato in base alle esigenze;
- Dashboard chiara ed intuitiva.

7. Stima del Budget ed Analisi Finanziaria

Una valutazione iniziale dei costi si attesta a 32.000€, considerando le ore lavorative dei project manager e dei membri del team. Si ipotizza un compenso orario di 70€ per i project manager e 50€ per i membri del team, con un impegno previsto di 50 ore per ciascun individuo. A questi costi si sommano ulteriori 4.000€ relativi alle spese pubblicitarie. Questa cifra è stata calcolata considerando la partecipazione di due dipendenti incaricati di presentare il prodotto ai clienti, retribuiti a un tasso orario di 25 euro, con un totale previsto di 80 ore ciascuno. A questi costi si aggiungono ulteriori 6.000 euro relativi a spese hardware e software. Questa cifra copre gli investimenti necessari per garantire un'adeguata infrastruttura tecnologica e dei servizi correlati al progetto.

Una valutazione preliminare dei benefici ammonta a 29.700€ per il primo anno, 47.520€ per il secondo anno e 71.280€ per il terzo anno. Questa stima deriva dall'analisi dell'utilizzo del sistema, basata sui clienti attuali dell'azienda che hanno manifestato interesse nel nuovo prodotto. Tra questi clienti, il 10% è interessato al pacchetto "small", il 30% al "medium", il 40% al "large" e il 20% all' "huge"

Si prevedono 5.000€ per la manutenzione correttiva e 10.000€ per la manutenzione evolutiva. Inizialmente, si ipotizza un maggiore impiego di ore per la manutenzione correttiva, riflettendo la fase iniziale del progetto. Nel corso del tempo, ci si aspetta che le ore dedicate alla manutenzione evolutiva aumentino, in linea con l'evoluzione del sistema e le esigenze in continua mutazione degli utenti.

8. Stima dello schedule

Si preventiva di consegnare il progetto entro gennaio 2023, nella data del preappello. La stima per lo sviluppo del prodotto, considerando un impegno di 50 ore per ogni membro del team, compresi i project manager, è di circa 3 mesi a partire dall'avvio del progetto. Si prevede che il prodotto avrà un ciclo di vita di circa tre anni prima di valutare la possibilità di introdurre nuove soluzioni o apportare modifiche al sistema tramite una reingegnerizzazione.

9. Potenziali Rischi

Nel contesto della realizzazione del progetto per un sistema di anomaly detection del traffico di rete basato su AI non supervisionata ed eseguito in cloud, è essenziale considerare diversi potenziali rischi. La sicurezza dei dati svolge un ruolo cruciale, poiché la gestione di informazioni sensibili nel cloud potrebbe esporre l'organizzazione a rischi come accessi non autorizzati o violazioni della privacy. La dipendenza da un provider di servizi cloud introduce il rischio di interruzioni del servizio o problemi di prestazioni, richiedendo una valutazione approfondita della reputazione e dell'affidabilità del fornitore.

Un altro aspetto critico riguarda l'adattabilità del modello di AI nel rilevare anomalie, poiché cambiamenti nel comportamento del traffico possono influire sulla sua efficacia nel tempo. L'utilizzo di AI non supervisionata, sebbene avanzato, può incontrare sfide significative, tra cui la possibilità di generare falsi positivi. Questo fenomeno si verifica quando il sistema rileva erroneamente un normale comportamento come potenzialmente anomalo, generando allarmi. La gestione di falsi positivi può comportare un aumento del carico di lavoro per il personale, oltre a minare la fiducia nell'efficacia del sistema. Ciò richiede una continua revisione e ottimizzazione del modello per ridurre il rischio di falsi positivi e migliorare la precisione della rilevazione.

Inoltre vi sono tutti i rischi legati alle risorse umane.

Dall'analisi dei rischi individuati, è stata effettuata un'allocazione di 5.000 euro come riserva per le contingenze. Questa somma è stata identificata e riservata come misura precauzionale per affrontare eventuali situazioni che potrebbero impattare negativamente sulle attività del progetto oppure contemplare spese non previste.

10. Maggiori informazioni

Per una visione approfondita dell'analisi finanziaria, con indicatori chiave come NPV, ROI e Payback, si consiglia di fare riferimento al documento di analisi finanziaria.