Asset	Value	Objective
Dati cliente	300.000-500.000€	Authentication, Integrity, Confidentiality, Availability
Dati GPS	150.000-250.000€	Integrity, Confidentiality, Availability
Dati corriere	250.000-450.000€	Integrity, Confidentiality, Availability
Dati pagamento	600.000-750.000€	Authentication, Integrity, Confidentiality, Accountability, Availability
Dati utente di sistema	500.000-600.000€	Authentication, Integrity, Confidentiality, Accountability, Authorization, Availability

Project	Azienda di spedizioni				
Year	2025	Team ID	3	Team	Luca Barcaroli, Andrea Bargilli, Alessio D'Eugenio, Dario Tommasi
Sprint		Start		End	

Asset	Value	Spoofing	Tampering	Repudiation	Information disclosure	DOS	Elevation of privilege	Danger	Unreliability	Absence of Resilience	Exposure	Attack	Inherent Probability	Inherent Risk	Control	Cost	Feasibility	Residual Probability	Residual Impact	Residual Risk	R.o.C	Overall Cost
Dati utente di sistema	500.000-600.000€	X									50.000-60.000€	Authentication Abuse (CAPEC 114)	40-60%	20.000-36.000€	• Autenticazione MFA	5.000-10.000€	Fattibile, sono disponibili librerie già testate e pronte all'uso	4% - 6%	20.000-36.000€	800-2.160€	2,84 - 2,38	5.800€ - 12.160€
							X				150.000-250.000€	Privilage Escalation (CAPEC 233)	5-15%	7.500-37.500€	• Applicare MFA per azioni sensibili; • Controllare periodicamente file di configurazione; • Effettuare audit periodici del sistema; • Mantenere aggiornati i programmi, le librerie e framework in uso;	9.000-15.000€	Fattibile, è richiesto un controllo continuo	1% - 2%	7.500-15.000€	75-300€	-0,18 - 1,48	9.075€ - 15.300€
			X	X	X	X		X		X	100.000-200.000€	Targeted Malware (CAPEC 542)	25-35%	25.000-70.000€	•Mantenere aggiornati sistemi e software; •Implementare strumenti di rilevamento come antivirus e firewall; • Effettuare degli audit del sistema andando ad analizzare manualmente processi e servizi in esecuzione.	10.000-17.000€	Fattibile, la parte si segmentazione della rete richiede competenze più elevate	3% - 4%	25.000-30.000€	750-1.200€	1,43 - 3,05	10.750€ - 18.200€
		X			X						40.000-50.000€	Phishing (CAPEC 98)	65-75%	26.000-37.500€	Non seguire alcun link che si riceve all'interno delle e-mail e non inserire credenziali di accesso su alcun sito web proveniente da e-mail sospette.	7.000-12.000€	Fattibile	7% - 8%	25.000-30.000€	1.750-2.400€	2,46 - 1,93	8.750€ - 14.400€
		X	X		X						80.000-100.000€	Adversary in the Middle (AiTM) (CAPEC 94)	10-20%	8.000-20.000€	•Chiavi pubbliche firmate da CA attendibili. • Crittografia del traffico (SSL/TLS/SSH). • Autenticazione reciproca forte. • Scambio sicuro delle chiavi pubbliche.	5.000-8.000€	Fattibile	1% - 2%	8.000-20.000€	80-400€	0,58 - 1,45	5.080€ - 8.400€
		X									50.000-70.000€	Reusing Session Id (Session Replay) (CAPEC 60)	20-30%	10.000-21.000€	• Invalidare sempre un ID di sessione dopo il logout dell'utente. • Impostare un timeout di sessione per gli ID di sessione. • Non codificare l'ID di invio della sessione con il metodo GET, altrimenti l'ID della sessione verrà copiato nell'URL. In generale, evitare di scrivere gli ID di sessione negli URL. Gli URL possono accedere ai file di registro, che sono vulnerabili a un utente malintenzionato. • Crittografare i dati della sessione associati all'ID della sessione. • Usare l'autenticazione a più fattori.	8.000-11.000€	Fattibile	2% - 3%	2.000-8.000€	40-240€	0,25 - 0,89	8.040€ - 11.240€

					X						50.000-70.000€	Password Brute Forcing (CAPEC 49)	55-65%	27.500-45.500€	• Invalidare sempre un ID di sessione dopo il logout dell'utente. • Impostare un timeout di sessione per gli ID di sessione. • Non codificare l'ID di invio della sessione con il metodo GET, altrimenti l'ID della sessione verrà copiato nell'URL. In generale, evitare di scrivere gli ID di sessione negli URL. Gli URL possono accedere ai file di registro, che sono vulnerabili a un utente malintenzionato. • Crittografare i dati della sessione associati all'ID della sessione. • Usare l'autenticazione a più fattori.	7.000-10.000€	Fattibile	6% - 7%	27.500-45.500€	1.650-3.185€	2,69 - 3,23	8.650€ - 13.185€
		X			X						50.000-70.000€	Try Common or Default Usernames and Passwords (CAPEC 70)	60-70%	30.000-49.000€	• Elimina tutte le credenziali predefinite dell'account che possono essere inserite dal fornitore del prodotto. • Implementare un meccanismo di limitazione delle password. Questo meccanismo dovrebbe prendere in considerazione sia l'indirizzo IP che il nome di accesso dell'utente. • Metti insieme una politica di password forte e assicurati che tutte le password create dagli utenti siano conformi. Inalternativa, genera automaticamente password complesse per gli utenti. • Le password devono essere riciclate per prevenire l'invecchiamento, cioè ogni tanto deve essere scelta una nuova password.	8.000-11.000€	Fattibile	6% - 7%	30.000-49.000€	1.800-3.430€	2,53 - 3,14	9.800€ - 14.430€
		X			X						50.000-70.000€	Dictionary-based Password Attack (CAPEC 16)	60-75%	30.000-52.500€	• Crea una politica di password complessa e assicurati che il tuo sistema applichi questa politica; • Implementare un meccanismo intelligente di limitazione delle password. È necessario fare attenzione a garantire che questi meccanismi non consentano eccessivamente gli attacchi di blocco dell'account come CAPEC-2; • Sfrutta l'autenticazione a più fattori per tutti i servizi di autenticazione.	7.000-10.000€	Fattibile	6% - 8%	30.000-52.500€	1.800-4.200€	3,03 - 3,83	8.800€ - 14.200€
		X			X						50.000-70.000€	Credential Stuffing (CAPEC 600)	70-80%	35.000-56.000€	•Utilizzare l'autenticazione a più fattori per tutti i servizi di autenticazione e prima di concedere a un'entità l'accesso alla rete del dominio. • Crea una politica di password complessa e assicurarsi che il sistema applichi questa politica; • Assicurarsi che gli utenti non riutilizzino combinazioni nome utente/password per più sistemi, applicazioni o servizi. • Non riutilizzare le credenziali dell'account amministratore locale su tutti i sistemi; • Nega l'uso remoto delle credenziali di amministratore locali per accedere ai sistemi di dominio; • Non consentire agli account di essere un amministratore locale su più di un sistema; • Implementare un meccanismo intelligente di	7.000-10.000€	Fattibile	7% - 8%	35.000-56.000€	2.450-4.480€	3,65 - 4,15	9.450€ - 14.480€

														limitazione delle password. È necessario fare attenzione a garantire che questi meccanismi non consentano eccessivamente gli attacchi di blocco dell'account come CAPEC-2; • Monitorare i registri di sistema e di dominio per l'accesso anomalo alle credenziali.							
Dati GPS	150.000-250.000€		X	X		X			X		30.000-40.000€	Traffic Injection (CAPEC 594)	20-30%	6.000-12.000€	• Usare TLS per tutte le comunicazioni di rete, così da proteggere confidenzialità e integrità, rendendo più difficile l'iniezione di pacchetti malevoli. • Verificare l'identità degli endpoint dirette tramite protocolli sicuri (TLS,IPsec)per assicurarsi che i dati provengano da fonti legittime. • Implementare ingress filtering per bloccare pacchetti con indirizzi IP falsificati, riducendo la possibilità di spoofing e injection. •Deployare sistemi di rilevamento/prevenzione delle intrusioni per analizzare il traffico di rete e bloccare pattern sospetti o iniettati. • Configurare policy dirette che negano per default il traffico non autorizzato, consentendo solo le comunicazioni esplicitamente permesse. • In ambienti aziendali, usare la decrittazione controllata del TLS presso punti di sicurezza per permettere l'analisi del traffico cifrato senza compromettere la sicurezza. • Usare firewall e limiti di traffico per evitare sovraccarichi o pacchetti in eccesso.	5.000-7.000€	Fattibile, richieste compentenze tecniche alte	2% - 3%	10.000-20.000€	200-600€	0,16 - 0,63	5.200€ - 7.600€
		X	X					X		40.000-70.000€	Carry-Off GPS Attack (CAPEC 628)	10-20%	4.000-14.000€	• Integrare dati non-GPS per verificare e correggere la posizione quando il segnale appare sospetto. • Utilizzare segnali autenticati. • Escludere automaticamente il GPS dalla navigazione quando rilevato come inattendibile. • Passare a una modalità di guida/navigazione degradata ma affidabile quando il GPS risulta compromesso.	2.000-6.000€	Fattibile	1% - 2%	10.000-50.000€	100-1.000€	0,95 - 1,17	2.100€ - 7.000€
			X	X					X		50.000-70.000€	Counterfeit GPS Signals (CAPEC 627)	10-20%	5.000-14.000€	• Riconoscere quando un segnale GPS non è autentico e nel ridurre la dipendenza dal GPS stesso. • È utile confrontare continuamente la posizione ricevuta con altre fonti, come sensori interni, mappe, altri sistemi satellitari o dati provenienti da reti terrestri. • La coerenza del movimento deve essere monitorata: cambiamenti troppo rapidi o improvvisi sono indizi di spoofing. • A livello hardware si possono usare ricevitori avanzati e antenne progettate per filtrare segnali sospetti.	3.000-5.000€	Fattibile	1% - 2%	10.000-50.000€	100-1.000€	0,63 - 1,60	3.100€ - 6.000€

		X	X		X						50.000-60.000€	Transaction or Event Tampering via Application API Manipulation (CAPEC 385)	20-30%	10.000-18.000€	• Validazione dei parametri delle API; • Utilizzo di un "SchemaValidation", rifiutando le richieste con uno schema strutturale differente dallo schema previsto; • Implementazione di meccanismi di autenticazione e autorizzazione robusti per limitare l'accesso alle API solo agli utenti e ai sistemi autorizzati.	9.000-12.000€	Fattibile, richieste compentenze tecniche alte	2% - 3%	10.000-20.000€	200-600€	0,09 - 0,45	9.200€ - 12.600€
		X	X		X		X	X	X		90.000-120.000€	Server Side Request Forgery (CAPEC 664)	20-40%	18.000-48.000€	• La prima linea d'azione per mitigare questa vulnerabilità è la gestione sicura delle richieste in arrivo. Questo può essere fatto tramite la convalida degli URL; • Più avanti nel flusso del processo, un altro modo per proteggere il server è esaminare la risposta e verificare che sia come previsto prima dell'invio; • Un'altra efficace misura di sicurezza è quella di consentire l'accesso al nome DNS o all'indirizzo IP di ogni servizio che l'applicazione web deve utilizzare. In questo modo, il server non può effettuare richieste esterne a servizi arbitrari; • Richiedere l'autenticazione per i servizi locali aggiunge un ulteriore livello di sicurezza tra l'avversario e i servizi interni in esecuzione sul server. Imponendo l'autenticazione locale, un avversario non potrà accedere a tutti i servizi interni solo tramite l'accesso al server.	15.000-20.000€	Fattibile, richieste compentenze tecniche alte	2% - 4%	40.000-60.000€	800-2.400€	0,15 - 1,28	15.800€ - 22.400€
						X		X	X	X	50.000-60.000€	Input data manipulation (CAPEC 153)	30-40%	15.000-24.000€	• Convalida rigorosa dell'input; • Utilizzo di librerie sicure per il parsing dei dati; • Limitazione dei valori sensibili modificabili dall'utente.	10.000-15.000€	Fattibile	3% - 4%	20.000-40.000€	600-1.600€	0,44 - 0,49	10.600€ - 16.600€
		X			X						40.000-50.000€	Fake the Source of Data (CAPEC 194)	25-35%	10.000-17.500€	• Autenticazione forte della sorgente dei dati; • Validazione della provenienza; • Crittografia end-to-end; • Limitazione dei canali di input.	8.000-10.000€	Fattibile	3% - 4%	20.000-30.000€	600-1.200€	0,18 - 0,63	8.600€ - 11.200€
Dati cliente	300.000-500.000€	X			X						20.000-30.000€	Phishing (CAPEC 98)	40-50%	8.000-15.000€	Non seguire alcun link che si riceve all'interno delle e-mail e non inserire credenziali di accesso su alcun sito web proveniente da e-mail sospette.	7.000-12.000€	Fattibile	4% - 5%	8.000-15.000€	320-750€	0,10 - 0,19	7.320€ - 12.750€

		X			X					80.000-100.000€	Credential Stuffing (CAPEC 600)	70-80%	56.000-80.000€	•Utilizzare l'autenticazione a più fattori per tutti i servizi di autenticazione e prima di concedere a un'entità l'accesso alla rete del dominio. • Crea una politica di password complessa e assicurarsi che il sistema applichi questa politica; • Assicurarsi che gli utenti non riutilizzino combinazioni nome utente/password per più sistemi, applicazioni o servizi. • Non riutilizzare le credenziali dell'account amministratore locale su tutti i sistemi; • Nega l'uso remoto delle credenziali di amministratore locali per accedere ai sistemi di dominio; • Non consentire agli account di essere un amministratore locale su più di un sistema; • Implementare un meccanismo intelligente di limitazione delle password. È necessario fare attenzione a garantire che questi meccanismi non consentano eccessivamente gli attacchi di blocco dell'account come CAPEC-2; • Monitorare i registri di sistema e di dominio per l'accesso anomalo alle credenziali.	7.000-10.000€	Fattibile	7% - 8%	35.000-56.000€	2.450-4.480€	6,65 - 6,55	9.450€ - 14.480€
		X	X							40.000-50.000€	Content Spoofing (CAPEC 148)	20-30%	8.000-15.000€	• Validazione e sanificazione dell'input; • Crittografia e integrità dei contenuti; • Prevenzione dello spoofing dell'interfaccia.	5.000-7.000€	Fattibile	2% - 3%	8.000-15.000	160-450€	0,57 - 1,08	5.160€ - 7.450€
		X	X		X					50.000-70.000€	Adversary in the Middle (AiTM) (CAPEC 94)	15-25%	7.500-17.500€	•Chiavi pubbliche firmate da CA attendibili. • Crittografia del traffico (SSL/TLS/SSH). • Autenticazione reciproca forte. • Scambio sicuro delle chiavi pubbliche.	5.000-8.000€	Fattibile	2% - 3%	25.000-30.000€	500-900€	0,40 - 1,08	5.500€ - 8.900€
			X	X	X		X		X	90.000-120.000€	Server Side Request Forgery (CAPEC 664)	20-40%	18.000-48.000€	• La prima linea d'azione per mitigare questa vulnerabilità è la gestione sicura delle richieste in arrivo. Questo può essere fatto tramite la convalida degli URL; • Più avanti nel flusso del processo, un altro modo per proteggere il server è esaminare la risposta e verificare che sia come previsto prima dell'invio; • Un'altra efficace misura di sicurezza è quella di consentire l'accesso al nome DNS o all'indirizzo IP di ogni servizio che l'applicazione web deve utilizzare. In questo modo, il server non può effettuare richieste esterne a servizi arbitrari; • Richiedere l'autenticazione per i servizi locali aggiunge un ulteriore livello di sicurezza tra l'avversario e i servizi interni in esecuzione sul server. Imponendo l'autenticazione locale, un avversario non potrà accedere a tutti i servizi interni solo tramite l'accesso al server.	15.000-20.000€	Fattibile, richieste compentenze tecniche alte	2% - 4%	18.000-48.000€	360-1.920€	0,18 - 1,30	15.360€ - 21.920€
			X	X	X	X		X		X	100.000-150.000€	Targeted Malware (CAPEC 542)	50-60%	50.000-90.000€	•Mantenere aggiornati sistemi e software; •Implementare strumenti di rilevamento come antivirus e firewall; • Effettuare degli audit del sistema andando ad analizzare manualmente processi e servizi in esecuzione.	12.000-17.000€	Fattibile, la parte si segmentazione della rete richiede competenze più elevate	5% - 6%	30.000-60.000€	1.500-3.600€	3,04 - 4,08	13.500€ - 20.600€

Dati pagamento	600.000-750.000€		X	X	X	X		X		X	170.000-200.000€	Targeted Malware (CAPEC 542)	60-70%	102.000-140.000€	•Mantenere aggiornati sistemi e software; •Implementare strumenti di rilevamento come antivirus e firewall; • Effettuare degli audit del sistema andando ad analizzare manualmente processi e servizi in esecuzione.	12.000-17.000€	Fattibile, la parte si segmentazione della rete richiede competenze più elevate	6% - 7%	60.000-80.000€	3.600-5.600€	7,20 - 6,91	15.600€ - 22.600€
		X									100.000-120.000€	Identity Spoofing (CAPEC 151)	40-50%	40.000-60.000€	Utilizzare processi di autenticazione robusti (ad esempio, autenticazione a più fattori).	10.000-13.000€	Fattibile	4% - 5%	40.000-60.000€	1.600-3.000€	2,84 - 3,38	11.600€ - 16.000€
		X			X						40.000-50.000€	Phishing (CAPEC 98)	65-75%	26.000-37.500€	Non seguire alcun link che si riceve all'interno delle e-mail e non inserire credenziali di accesso su alcun sito web proveniente da e-mail sospette.	7.000-12.000€	Fattibile	7% - 8%	25.000-30.000€	1.750-2.400€	2,46 - 1,93	8.750€ - 14.400€
			X	X	X		X	X			90.000-120.000€	Log Injection-Tampering-Forging (CAPEC 93)	30-40%	27.000-48.000€	• Controlla attentamente l'accesso ai file di registro fisici; • Non consentire che i dati contaminati siano scritti nel file di registro senza previa convalida dell'input. Un elenco di permessi può essere utilizzato per convalidare correttamente i dati; • Usa la sincronizzazione per controllare il flusso di esecuzione; • Usa gli strumenti di analisi statica per identificare le vulnerabilità di log forging; • Evita di visualizzare i registri con strumenti che possono interpretare i caratteri di controllo nel file, come le shell della riga di comando.	15.000-20.000€	Fattibile, richieste compentenze tecniche alte	3% - 4%	27.000-48.000€	810-1.920€	0,75 - 1,30	15.810€ - 21.920€
			X		X						100.000-200.000€	Clickjacking (CAPEC 103)	40-50%	40.000-100.000€	• Se usi il browser Firefox, usa il plug-in NoScript che aiuterà a vietare iFrames; • Disattiva Java Script, Flash e disabilita CSS; • Quando si mantiene una sessione autenticata con un sistema di destinazione privilegiato, non utilizzare lo stesso browser per navigare su siti sconosciuti per eseguire altre attività. Termina di lavorare con il sistema di destinazione e disconnetti prima di procedere ad altre attività.	30.000-40.000€	Fattibile	4% - 5%	75.000-100.000€	3.000-5.000€	0,23 - 1,38	33.000€ - 45.000€
		X	X		X						50.000-70.000€	Adversary in the Middle (AiTM) (CAPEC 94)	15-25%	7.500-17.500€	•Chiavi pubbliche firmate da CA attendibili. • Crittografia del traffico (SSL/TLS/SSH). • Autenticazione reciproca forte. • Scambio sicuro delle chiavi pubbliche.	5.000-8.000€	Fattibile	2% - 3%	25.000-30.000€	500-900€	0,40 - 1,08	5.500€ - 8.900€
		X	X		X						50.000-60.000€	Transaction or Event Tampering via Application API Manipulation (CAPEC 385)	20-30%	10.000-18.000€	• Validazione dei parametri delle API; • Utilizzo di un "SchemaValidation", rifiutando le richieste con uno schema strutturale differente dallo schema previsto; • Implementazione di meccanismi di autenticazione e autorizzazione robusti per limitare l'accesso alle API solo agli utenti e ai sistemi autorizzati.	9.000-12.000€	Fattibile, richieste compentenze tecniche alte	2% - 3%	10.000-20.000€	200-600€	0,09 - 0,45	9.200€ - 12.600€
Dati corriere	250.000-450.000€	X			X						20.000-30.000€	Phishing (CAPEC 98)	40-50%	8.000-15.000€	Non seguire alcun link che si riceve all'interno delle e-mail e non inserire credenziali di accesso su alcun sito web proveniente da e-mail sospette.	7.000-12.000€	Fattibile	4% - 5%	8.000-15.000€	320-750€	0,10 - 0,19	7.320€ - 12.750€
		X	X								30.000-40.000€	Content Spoofing (CAPEC 148)	20-30%	6.000-12.000€	• Validazione e sanificazione dell'input; • Crittografia e integrità dei contenuti; • Prevenzione dello spoofing dell'interfaccia.	5.000-7.000€	Fattibile	2% - 3%	5.000-7.000€	100-210€	0,18 - 0,68	5.100€ - 7.210€

		X	X		X						50.000-70.000€	Adversary in the Middle (AiTM) (CAPEC 94)	15-25%	7.500-17.500€	•Chiavi pubbliche firmate da CA attendibili. • Crittografia del traffico (SSL/TLS/SSH). • Autenticazione reciproca forte. • Scambio sicuro delle chiavi pubbliche.	5.000-8.000€	Fattibile	2% - 3%	25.000-30.000€	500-900€	0,40 - 1,08	5.500€ - 8.900€
			X	X	X	X	X		X	X	90.000-120.000€	Server Side Request Forgery (CAPEC 664)	20-40%	18.000-48.000€	• La prima linea d'azione per mitigare questa vulnerabilità è la gestione sicura delle richieste in arrivo. Questo può essere fatto tramite la convalida degli URL; • Più avanti nel flusso del processo, un altro modo per proteggere il server è esaminare la risposta e verificare che sia come previsto prima dell'invio; • Un'altra efficace misura di sicurezza è quella di consentire l'accesso al nome DNS o all'indirizzo IP di ogni servizio che l'applicazione web deve utilizzare. In questo modo, il server non può effettuare richieste esterne a servizi arbitrari; • Richiedere l'autenticazione per i servizi locali aggiunge un ulteriore livello di sicurezza tra l'avversario e i servizi interni in esecuzione sul server. Imponendo l'autenticazione locale, un avversario non potrà accedere a tutti i servizi interni solo tramite l'accesso al server.	15.000-20.000€	Fattibile, richieste compentenze tecniche alte	2% - 4%	18.000-48.000€	360-1.920€	0,18 - 1,30	15.360€ - 21.920€
			X	X	X	X		X		X	100.000-150.000€	Targeted Malware (CAPEC 542)	50-60%	50.000-90.000€	•Mantenere aggiornati sistemi e software; •Implementare strumenti di rilevamento come antivirus e firewall; • Effettuare degli audit del sistema andando ad analizzare manualmente processi e servizi in esecuzione.	10.000-17.000€	Fattibile, la parte si segmentazione della rete richiede competenze più elevate	5% - 6%	30.000-60.000€	1.500-3.600€	3,85 - 4,08	11.500€ - 20.600€