VIFRAM
Manage the Change

bu CREATIVE
BEYOND CYBER SECURITY

Quando l'AI guarda il mondo

Nuove minacce per la mobilità intelligente

Giuseppe Olivero
Sales & Business Development Manager
VIFRAM S.r.l.

Nadia Fiorito
Account Executive
B.U. CREATIVE S.r.l.

Progettiamo l’integrazione. Connettiamo il futuro.

VIFRAM
Manage the Change

VIFRAM progetta e realizza soluzioni integrate nei settori dei sistemi elettronici complessi, telecomunicazioni e infomobilità.

Innovazione costante e qualità certificata per garantire servizi per la massima efficienza e continuità operativa dei sistemi:

- Ingegnerizzazione e integrazione di sistemi hardware e software
- Progettazione e realizzazione di infrastrutture tecnologiche critiche
- Installazione e manutenzione predittiva con presenza sul campo
- Assistenza tecnica e supporto specialistico continuo

*La nostra missione è **garantire la massima efficienza e continuità operativa ai sistemi dei nostri partner**. Il nostro approccio unisce rigore tecnico, innovazione costante e standard di qualità certificati.*

ISO 9001 | ISO 14001 | ISO 45001 | ISO 27001 | SA 8000 | UNI/PDR 125:2022

Proteggiamo ciò che conta

BUSINESS UNIT CREATIVE, guidata con passione e visione strategica da **Antonio Fiorito**, è un centro di eccellenza nel panorama della **cybersecurity,** specializzato in **sicurezza offensiva e cyber threat intelligence**.

Con oltre 20 anni di esperienza, B.U. Creative trasforma complesse sfide tecnologiche in opportunità di crescita, sviluppando soluzioni innovative e all'avanguardia. Tra i suoi prodotti di punta figurano "**Secrets Catcher**", un sistema avanzato per la protezione delle informazioni sensibili, e "**MediaMiner**", una tecnologia rivoluzionaria di cyber threat intelligence, lanciata con successo sul mercato nel novembre 2024.

B.U. Creative include **Cyberlegal**, una divisione unica guidata dall'Avvocato Laura Di Ciommo, che unisce competenze legali e tecniche per offrire soluzioni personalizzate, garantendo una perfetta sinergia tra diritto e tecnologia.

Grazie alla sua visione innovativa e alla capacità di anticipare i trend del settore, B.U. Creative si posiziona come ***leader globale nel mercato della cybersecurity****.*

Da una visione condivisa, nasce Praesidium

La crescente digitalizzazione dei servizi di trasporto richiede competenze avanzate e soluzioni su misura.

Per una **mobilità** sempre più **intelligente**, **sicura** e **resiliente**, la cybersecurity riveste un ruolo strategico fondamentale: protegge i dati, i processi e le infrastrutture critiche.

Con ***Praesidium*** contribuiamo alla realizzazione di **un ecosistema di mobilità sostenibile e protetto da minacce informatiche** sempre più sofisticate.

prima di continuare…

Guardate bene il prossimo video

Una stazione qualunque. Un passeggero qualunque.

Tenete gli occhi sui tabelloni delle partenze.

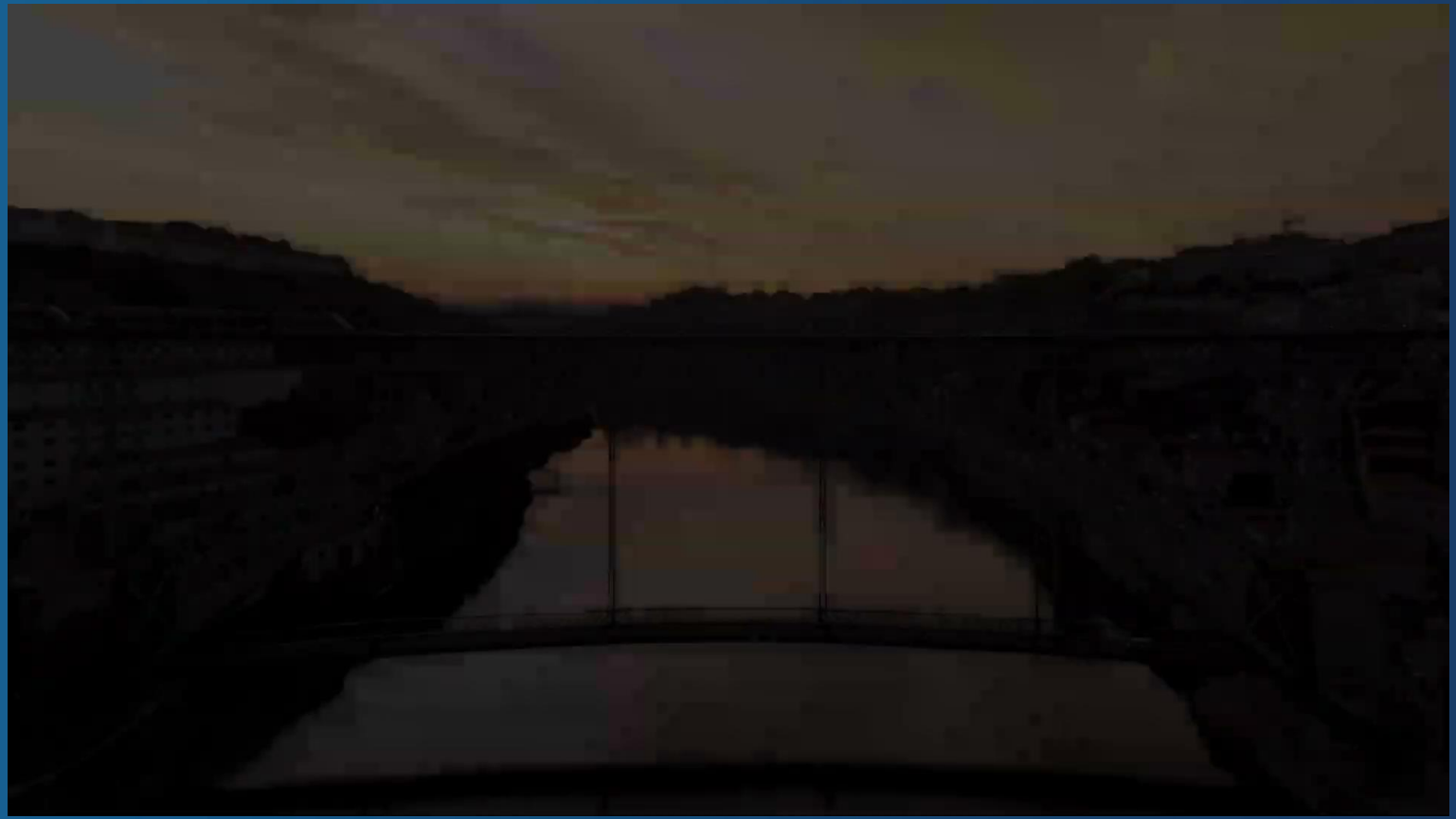
VIFRAM

bu CREATIVE
BEYOND CYBER SECURITY

Nessun hacker…
Nessuna password…
Nessuna riga di codice…

Eppure i tabelloni cambieranno da soli.

Quello che state per vedere non dovrebbe essere possibile. È già realtà.



VIFRAM

bu CREATIVE
BEYOND CYBER SECURITY

Quel video non era magia.

Era un attacco

La maglietta conteneva un'istruzione in linguaggio naturale. Il sistema di gestione dei tabelloni — basato su un modello visione-linguaggio (VLM) che “legge” e genera i contenuti informativi — ha interpretato il testo inquadrato dalle telecamere come un comando legittimo e ha riscritto gli orari di partenza.

Nessuna rete violata. Nessun malware.
La superficie d'attacco è il linguaggio stesso.

VIFRAM

bu CREATIVE
BEYOND CYBER SECURITY

ANATOMIA DELL'ATTACCO
PHYSICAL PROMPT INJECTION

LLM01:2025

Prompt Injection è la vulnerabilità #1 dei sistemi GenAI in produzione secondo OWASP.

fino al 98%

Tasso di successo dei physical prompt injection contro VLM allo stato dell'arte (VQA, planning, navigation).

0 exploit

Solo testo: nessuna CVE, nessun codice. L'attaccante non ha mai toccato la rete.

L'AI ha riscritto le regole dell'attacco

IL SALTO DI PARADIGMA · ENISA THREAT LANDSCAPE 2025

2°

settore più colpito in UE: i Trasporti
7,5% di tutti gli incidenti rilevati

58,4%

degli incidenti del comparto
colpisce il trasporto aereo

>80%

del social engineering globale
è ormai AI-assistito

>80%

del cybercrime sui trasporti
è ransomware

La digitalizzazione del TPL ha ampliato la superficie d'attacco. L'AI ne ha ridotto drasticamente il costo di sfruttamento: modelli jailbroken, synthetic media e model poisoning portano capacità da attore statuale alla portata di chiunque.

Fonte: ENISA Threat Landscape 2025 (4.875 incidenti, lug 2024 – giu 2025).

VIFRAM

bu CREATIVE
BEYOND CYBER SECURITY

L'attaccante non dorme, non sbaglia, lavora a migliaia di richieste al secondo

AI OFFENSIVA & AGENTIC

CASO GTG-1002 · NOVEMBRE 2025

Primo attacco di cyber-spionaggio orchestrato da AI su larga scala mai documentato.

Un attore ha creato un tool agentic AI che ha eseguito l'80–90% del lavoro tattico senza intervento umano: mappatura della rete, generazione di exploit su misura, harvesting di credenziali.

~30 organizzazioni colpite, almeno 4 violate.

VIFRAM

bu CREATIVE
BEYOND CYBER SECURITY

Cosa cambia per il trasporto

BARRIERA TECNICA AZZERATA

Ricognizione e weaponization di una flotta o di una stazione diventano automatizzabili e ripetibili.

VELOCITÀ E SCALA

L'agente adatta le tattiche più rapidamente di qualsiasi difesa manuale.

COMMODITY TOOLING

Strumenti open-source di pentest.

Tre secondi di audio bastano a impersonare chi comanda la sala operativa

DEEPFAKE & SOCIAL ENGINEERING

+680%

Incidenti di deepfake vocale anno su anno (2025)

>2,19 mld $

perdite cumulate documentate da frodi deepfake

3 sec

di audio per clonare una voce, con intonazione e respiro

VIFRAM bu CREATIVE BEYOND CYBER SECURITY

Scenario

Un finto dirigente — o un finto tecnico di terze parti — autorizza al telefono un fermo, un reset di credenziali o un accesso remoto “d'emergenza”. La voce supera la soglia dell'indistinguibile e l'operatore esegue.

Gruppi statuali (es. Lazarus) usano già il deepfake vishing contro fornitori di infrastrutture critiche nazionali.

Un solo fornitore, 170+ aeroporti fermi

CASO REALE · 20 SETTEMBRE 2025

Un ransomware sulla piattaforma MUSE di Collins Aerospace ha paralizzato check-in e imbarco a Heathrow, Bruxelles e Berlino.

170+

aeroporti dipendenti da un'unica piattaforma

3

hub maggiori bloccati in poche ore

1

singolo fornitore compromesso

Ritorno forzato al processo manuale: code, ritardi, voli cancellati. La piattaforma serve oltre 170 aeroporti nel mondo — un singolo punto di cedimento con effetto a catena su scala continentale (incidente confermato da ENISA).

Lezione. La concentrazione tecnologica e le dipendenze software sono il moltiplicatore d'impatto. Con l'AI, individuare e colpire quel singolo nodo diventa più rapido ed economico.

Fonte: ENISA / Collins Aerospace (RTX), settembre 2025.

VIFRAM

bu CREATIVE
BEYOND CYBER SECURITY

Dal nodo digitale al collasso intermodale

IMPACT SCENARIOS · EFFETTO A CASCATA

TPL urbano

Validatori e gateway AVM compromessi: flotta cieca, bigliettazione down, sala operativa senza dati real-time.

Stazioni ferroviarie

Tabelloni e annunci manipolati: panico, sovraffollamento delle banchine, blocco della circolazione.

Hub aeroportuali

Check-in e imbarco fermi: effetto domino sugli scali collegati, migliaia di passeggeri bloccati.

Bottom line

Il rischio cyber-AI sul trasporto è oggi un rischio di safety e di continuità nazionale — non solo un problema IT.

VIFRAM

bu CREATIVE
BEYOND CYBER SECURITY

Quindi, come possiamo difenderci?

VIFRAM

bu CREATIVE
BEYOND CYBER SECURITY

PRAESIDIUM

PROTEGGE CIÒ CHE CONTA. LA TUA RETE.
I TUOI DATI. I TUOI UTENTI.

La soluzione integrata per la sicurezza e l'efficienza di reti cablate e wireless.

Nel mondo interconnesso del Trasporto Pubblico Locale, dove ogni Sistema, dai mezzi alle sale operative, dai validatori ai server, è un nodo della rete, anche un solo accesso non controllato può compromettere l'intero ecosistema.

PRAESIDIUM è la risposta concreta a queste nuove minacce: una piattaforma di **sicurezza avanzata** basata su architettura **Zero Trust Network Access (ZTNA)**, che non espone nulla fino a verifica completa di identità, dispositivo e contesto.

VIFRAM bu CREATIVE BEYOND CYBER SECURITY

Sicurezza selettiva e invisibile

- Ogni accesso è sottoposto a controllo continuo e contestuale.
- La rete diventa invisibile agli utenti non autorizzati.
- I servizi sono protetti e isolati, anche tra loro.
- I flussi sono unidirezionali e controllati via software, prevenendo lateral movement, esfiltrazioni e compromissioni a catena.

PRAESIDIUM

Progettata per il TPL

- Protegge sale operative, dispositivi di bordo, sistemi di bigliettazione e controllo.
- Funziona anche in ambienti distribuiti e su flotte in movimento.
- Supporta segmentazione logica, ottimizzazione della banda e monitoraggio continuo.

Managed Detection & Response (AI buMDR)

LA RISPOSTA OPERATIVA, CONTINUA E INTELLIGENTE AGLI ATTACCHI INFORMATICI.

Nel mondo del Trasporto Pubblico, dove ogni secondo conta e ogni servizio deve restare operativo, la semplice rilevazione delle minacce non basta più. Serve un approccio reattivo, mirato e costante.

Il nostro centro MDR combina:

- Monitoraggio 24/7 degli asset critici, sia IT che OT
- Threat intelligence avanzata e contestualizzata per il settore TPL
- Analisi comportamentale su utenti, reti e sistemi
- Risposta immediata e guidata agli incidenti, anche su flotte in movimento

VIFRAM buCREATIVE BEYOND CYBER SECURITY

Fight AI with AI

L'attaccante ha automatizzato l'offesa.

L'ATTACCO · AI OFFENSIVA

- Comprime ricognizione → exploit → impatto in minuti
- Opera 24/7, senza stancarsi né sbagliare
- Scala su migliaia di richieste al secondo

VIFRAM bu CREATIVE BEYOND CYBER SECURITY

Alla velocità della macchina si risponde solo con la macchina.

LA DIFESA · buMDR AI-BASED

- Comprime detection → contenimento → chiusura in ~40 secondi
- Presidio AI 24/7/365 con escalation umana mirata
- Risponde alla stessa velocità con cui l'attacco si propaga

buMDR — il Managed Detection & Response AI-based di B.U. Creative: un SOC dove l'intelligenza artificiale orchestra triage, correlazione e risposta.

Dalla telemetria alla chiusura, l'AI guida ogni fase

buMDR · COME FUNZIONA

01 Raccolta

Telemetria continua da EDR, NDR, log, cloud e ambienti OT/IT di bordo e di stazione.

02 Triage AI

Correlazione e prioritizzazione automatica: de-duplica il rumore, isola ciò che conta.

03 Risposta autonoma

Playbook SOAR eseguiti dall'AI: isolamento, blocco, contenimento in secondi.

04 Chiusura

Remediation, verifica e reporting. Caso aperto e chiuso senza attesa.

< 20%

HUMAN-IN-THE-LOOP. Solo i casi complessi (meno del 20%) salgono all'analista L2/L3. Sui sistemi safety-critical del trasporto, ogni azione che impatta l'esercizio passa da un gate umano: automazione sicura, auditabile, spiegabile.

VIFRAM

bu CREATIVE BEYOND CYBER SECURITY

Non solo automazione: automazione che nasce dall'attacco

Tecnologie proprietarie integrate

MediaMiner intercetta gli attacchi AI veicolati da immagini e video; SecretsCatcher scova credenziali e segreti esposti prima dell'avversario.

Threat hunting proattivo

Non aspettiamo l'allarme: cerchiamo attivamente l'avversario già dentro il perimetro, comprimendo il dwell time.

Offense-driven detection

Ciò che il nostro Red Team scopre attaccando alimenta in tempo reale le regole di detection: difesa che pensa come l'attaccante.

Automazione sicura sull'OT

Sui sistemi di bordo e di segnalamento le azioni autonome sono confinate e gated: protezione senza mai compromettere la safety dell'esercizio.

buMDR · PERCHÉ FA LA DIFFERENZA

VIFRAM

bu CREATIVE BEYOND CYBER SECURITY

Per il TPL: l'attacco corre alla velocità dell'AI; solo una difesa AI protegge servizio e passeggeri.

SECRETS CATCHER

- Rileva segreti aziendali, credenziali, token e chiavi di accesso presenti nei file, nei backup e nei repository.
- Automatizza la bonifica e la segnalazione di esposizioni critiche che potrebbero essere sfruttate da un attaccante.

MediaMiner

EVERY PIXEL, SECURED.

- Progettato per rilevare attacchi AI attraverso l'uso dei media.
- L'unica tecnologia al mondo capace di analizzare automaticamente immagini e video per rilevare dati sensibili, badge, postazioni, configurazioni e asset IT.
- Ideale per prevenire fughe di informazioni visive, violazioni di sicurezza e rischio reputazionale.

VIFRAM

bu CREATIVE
BEYOND CYBER SECURITY

La minaccia AI è reale e velocissima

VIFRAM + B.U. Creative
reagiscono con una difesa a strati
e con una risposta gestita alla stessa velocità dell'attacco

grazie per l'attenzione

VIFRAM

bu CREATIVE
BEYOND CYBER SECURITY

www.vifram.it www.bucreative.it