Riepilogo esecutivo di Active View

Fonte dati del rapporto: Active View
Data di origine: lunedì 9 giugno 2025

Preparato per: Boxline
Businessgroup: Enterprise Admins
Data di generazione: lunedì 9 giugno 2025 Opzioni dati: Predefinito | Includi rischio accettabile | Finestra di 90 giorni | Metodo di valutazione: DDI

BeSafe S.r.l
Sede Legale e Operativa: Via G.Garibaldi, 4/A - 25020 Flero (BS)
REA: BS-457746 - REG. IMP.BS - P.IVA – C.F. 02529120988
Cap. Soc. € 10.000,00
Tel: 0302501453 – Fax: 0302702941 - email: info@besafe.it

1 Panoramica

Questo rapporto fornisce un riepilogo per Boxline e copre 232 risorse. Gli asset presentano 60 occorrenze di 3 vulnerabilità di gravità critica, 60 occorrenze di 13 vulnerabilità di elevata gravità, 67 occorrenze di 14 vulnerabilità di media gravità, 183 occorrenze di 10 vulnerabilità di bassa gravità e 1606 occorrenze di 23 vulnerabilità di gravità trascurabile.

Posizione generale di **sicurezza: B-**

In base alle vulnerabilità esistenti, alle valutazioni degli asset associate e al rischio aziendale assegnato ai singoli asset, il GPA di sicurezza complessivo per Boxline è **2,39** (B-).

I dati per questo rapporto provengono da Active View a partire da lunedì 9 giugno 2025 alle 15:00. I dettagli relativi al sistema di classificazione sono forniti nell'Appendice.

2 Informazioni sulla vulnerabilità degli asset

La gravità attribuita a ciascuna risorsa contribuisce allo stato generale di sicurezza. Le cifre fornite hanno lo scopo di aiutare a eseguire un'analisi qualitativa dello stato di sicurezza di Boxline.

2.1 Panoramica completa della valutazione degli asset

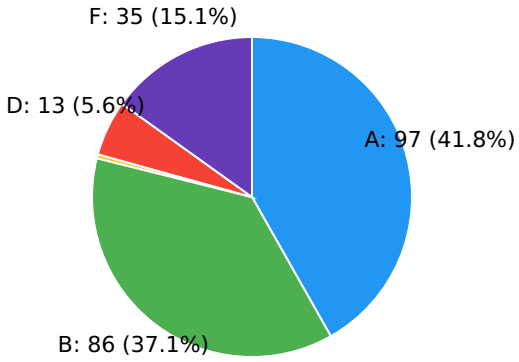

Figura 2.1: Numero e percentuale di asset coperti da questo rapporto che hanno un determinato rating patrimoniale.

2.2 La vulnerabilità viene contata in base alla gravità

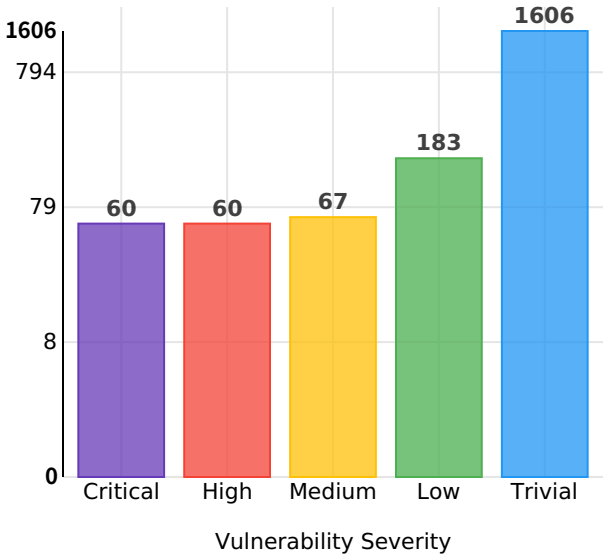

Figura 2.2: Numero di vulnerabilità per classificazione di gravità presenti negli asset coperti da questo rapporto.

3 Informazioni sulle tendenze

Trending fornisce un modo semplice e veloce per vedere i tuoi risultati nel tempo.

3.1 Tendenze del GPA in materia di sicurezza

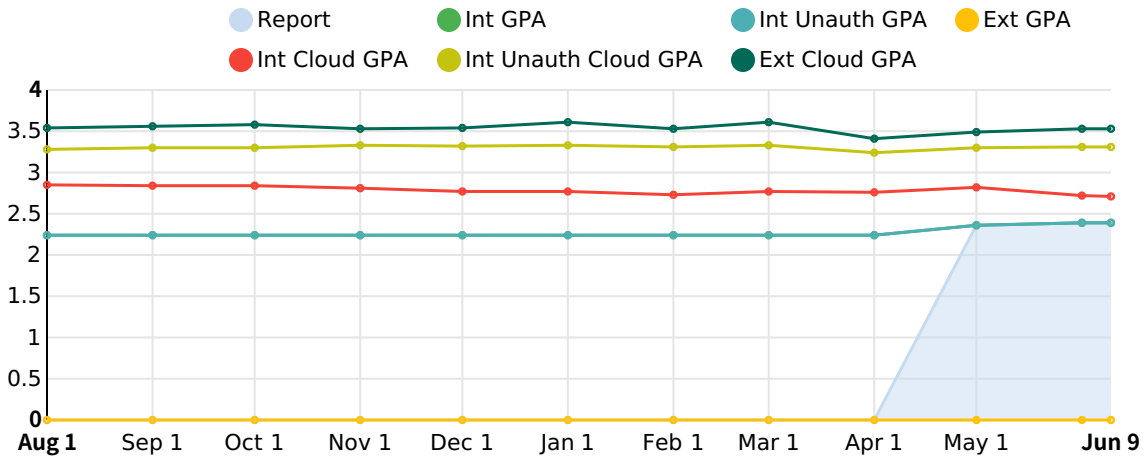

Figura 3.1: I grafici delle tendenze del Security GPA mostrano le tendenze dell'ultimo anno per tutti gli asset inclusi in questo rapporto.

3.2 Tendenze della gravità delle vulnerabilità

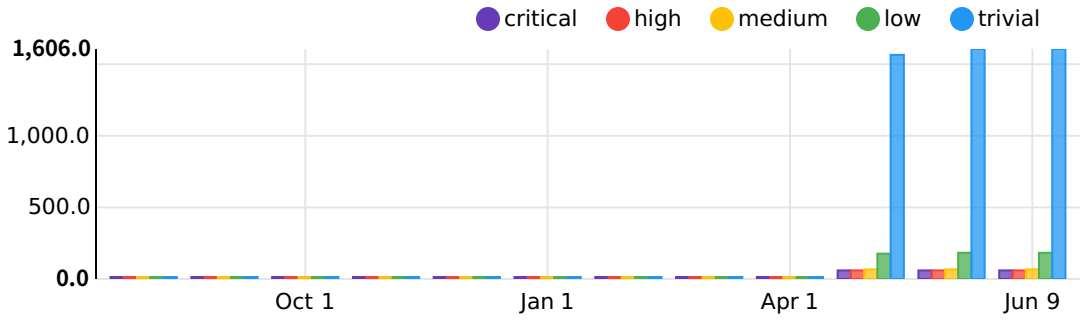

Figura 3.2: L'andamento della gravità delle vulnerabilità mostra le tendenze nell'ultimo anno per tutte le vulnerabilità in questo rapporto.

3.3 Tendenze dello stato di vulnerabilità

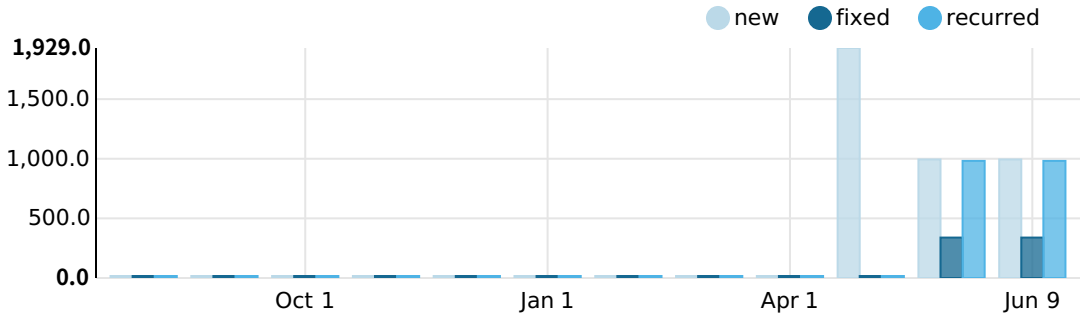

Figura 3.3: L'andamento dello stato di vulnerabilità mostra le tendenze nell'ultimo anno per tutte le vulnerabilità in

questo rapporto.

Appendice A

A.1 Processo di valutazione

I paragrafi seguenti descrivono il sistema Fortra di valutazione delle vulnerabilità e del livello di sicurezza.

A.1.1 Definizioni della gravità delle vulnerabilità

Le vulnerabilità sono difetti noti o sconosciuti che possono essere rilevati nell'hardware, nel software o nella configurazione di una risorsa. Gli aggressori sfruttano le vulnerabilità per accedere o acquisire informazioni dagli asset bersaglio. A ciascuna vulnerabilità è associato un livello di gravità, basato sull'impatto che l'attacco avrebbe sulla riservatezza, l'integrità e la disponibilità di una risorsa.

A.1.1.1 Livelli Fortra di gravità

Critico	Se sfruttato, un utente malintenzionato acquisirà il controllo completo della risorsa. È noto che le vulnerabilità di livello critico sono caratterizzate da exploit accessibili al pubblico che richiedono poche o nessuna conoscenza specialistica per essere utilizzati. In alcuni casi, la presenza di vulnerabilità di livello critico indica che l'asset è già stato compromesso. È necessario intervenire immediatamente per risolvere queste vulnerabilità.
Elevato	Se sfruttato, un utente malintenzionato potrebbe ottenere l'accesso utente o amministrativo alla risorsa ed essere in grado di eseguire comandi, accedere o eliminare file e lanciare attacchi contro altre risorse. Le vulnerabilità di alto livello spesso richiedono conoscenze specialistiche per essere sfruttate e gli exploit accessibili al pubblico potrebbero non essere disponibili. Queste vulnerabilità dovrebbero essere risolte il prima possibile.
Medio	Se sfruttato, un utente malintenzionato otterrebbe informazioni preziose sulla risorsa, che aiuterebbero ad accedervi. In molti casi, le vulnerabilità di medio livello sono il risultato di servizi configurati in modo errato, configurazioni di sicurezza deboli o assenti o account ad accesso limitato non protetti. Queste vulnerabilità devono essere risolte in tempi ragionevoli.
Basso	Se sfruttato, un utente malintenzionato potrebbe ottenere informazioni sulla risorsa, ma ciò non comporterebbe necessariamente l'accesso. Le vulnerabilità di basso livello possono essere risolte in genere applicando pratiche di rafforzamento della sicurezza o disabilitando i servizi.

Banale	Se sfruttato, un utente malintenzionato potrebbe ottenere informazioni sulla risorsa, ma non dovrebbe consentire l'accesso. In molti casi le vulnerabilità di livello banale non hanno una soluzione possibile a causa delle limitazioni del sistema operativo e rappresentano un rischio minimo per la sicurezza dell'asset.
Informazioni	Informazioni fornite da una risorsa o da un servizio che non sono considerate una vulnerabilità.

A.1.2 Valutazioni degli asset

A ogni asset viene assegnato un rating basato sulla gravità delle vulnerabilità che presenta. Questi rating vengono calcolati identificando le vulnerabilità più gravi dell'asset e quindi scegliendo il rating dell'asset corrispondente.

A.1.2.1 Livelli di rating FVM

F	L'asset presenta una o più vulnerabilità di livello critico.
D	L'asset presenta una o più vulnerabilità di alto livello.
C	L'asset presenta una o più vulnerabilità di medio livello.
B	L'asset presenta una o più vulnerabilità di basso livello.
A	L'asset presenta zero o più vulnerabilità di livello banale.

A.2 Definizioni della valutazione complessiva

La valutazione complessiva si basa sui valori medi di valutazione di ogni asset nel rapporto.

GPA Fortra di sicurezza di A.2.1

F	La media ponderata del GPA di sicurezza degli asset è 0,00 - 0,33.
D-	Il GPA medio ponderato per la sicurezza degli asset è 0,34 - 0,67.
D	Il GPA medio ponderato per la sicurezza degli asset è 0,68 - 1,00.
D+	La media ponderata del GPA per la sicurezza degli asset è 1,01 - 1,33.
C-	La media ponderata del GPA per la sicurezza degli asset è 1,34 - 1,67.
C	La media ponderata del GPA per la sicurezza degli asset è 1,68 - 2,00.

C++	La media ponderata del GPA per la sicurezza degli asset è 2,01 - 2,33.
B-	La media ponderata del GPA per la sicurezza degli asset è 2,34 - 2,67.
B	Il GPA medio ponderato per la sicurezza degli asset è 2,68 - 3,00.
B+	Il GPA medio ponderato per la sicurezza degli asset è 3,01 - 3,33.
A-	Il GPA medio ponderato per la sicurezza degli asset è 3,34 - 3,67.
A	Il GPA medio ponderato per la sicurezza degli asset è 3,68 - 4,00.