Diario dei progressi

Versione	Data	Redattore	Descrizione
0.2	25/06/2025	Davide Marin	Aggiunta sezione “Mercoledì 25/06/2025”
0.1	24/06/2025	Davide Marin	Creazione documento, inserimento riassunto e aggiornamento odierno

1. Prima settimana (19-27/06)

1.1 Martedì 24/06/2025

1.1.1 Riassunto giorni passati

Da giovedì 19 a lunedì 23 ho effettuato uno studio il più approfondito possibile, ma prettamente teorico, sullo strumento antivirus BitDefender GravityZone. Ho steso un file di appunti personali su ciò che ho visto sulle pagine di documentazione di BitDefender a mano a mano che approfondivo le diverse funzionalità del portale.

Nel frattempo, ho studiato e approfondito personali lacune nelle informazioni che leggevo, come le tecnologie di prevenzione, protezione e mitigazione da parte dell'antivirus, e quelle relative alle modalità di attacco utilizzate comunemente.

Ieri, lunedì 23, ho inoltre iniziato ad applicare alcune politiche alla mia macchina, per vedere se riuscissi a gestirne il funzionamento; purtroppo ho avuto difficoltà e i miei tentativi di applicare regole, in particolare limitazioni web e di applicazioni, non hanno avuto successo.

1.1.2 Cose fatte oggi

Oggi sono riuscito a trovare e risolvere i problemi riscontrati ieri. Per la parte web, si trattava di selezionare l'opzione di scannerizzare anche il traffico criptato, in questo modo si rende possibile all'antivirus di effettuare il blocco anche dei siti con protocollo HTTPS. Per quanto riguarda il blocco applicazioni, invece, mi sono assicurato che il percorso segnalato fosse privo di caratteri "speciali".

Ho iniziato anche una parte di testing per controllare il giusto funzionamento dell'anti-malware: ho simulato "attacchi" innocui sia tramite file sia fileless, i primi tramite la stringa nota fornita da EICAR:

X5O!P%@AP[4PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

i secondi, tramite comando PowerShell innocuo, ma che simula il possibile comportamento di un attacco fileless:

powershell -nop -w hidden -c " IEX ' Write Output TestFilelessAttack ' "

In questo modo, ho testato (e verificato) il giusto comportamento di:

- **Anti-malware On-Access (file)** Il file è stato individuato ed eliminato non appena l'ho creato e salvato; ho provato inoltre a disattivare il controllo per crearlo, riattivare il controllo e poi aprire il file e, correttamente, all'apertura il file viene bloccato ed eliminato.
- **Anti-malware On-Execute Fileless Attack Protection (fileless)** Il comando è stato bloccato con relativo messaggio di errore.
- **Web Protection Web Traffic Scan (file)** Scaricando il file di test (direttamente dal sito EICAR) BitDefender individua file e .zip contente il file di test, e ne blocca il download.

tutti gli eventi sono stati inoltre registrati sul portale di GravityZone.

Ho anche testato l'impostazione di altre funzionalità di GravityZone:

- Anti-malware "On-Demand", lanciando una "full scan" programmata del mio pc.
- Blocco dispositivi, bloccando tutte le USB tranne una aggiungendola come esclusione.

1.1.3 Difficoltà riscontrate

- Sembra non essere possibile aggiungere agli endpoint il modulo "Integrity Monitoring", in quanto, a differenza di come mostrato nella guida non è presente tra le opzioni nella configurazione dell'agent. Inoltre, anche nella pagina dedicata, non è possibile creare regole: la documentazione parla di un pulsante "Action" che però non è presente nel portale.

- Ho provato a testare la funzionalità di “Ransomware activity” che dovrebbe permettere di ripristinare i file affetti da attacchi ransomware dall’interfaccia di GravityZone. Purtroppo, provando ad eseguire un semplice script che convertiva un file di testo “cavia” in B64, non ho attirato l’attenzione da parte di BitDefender, e non ho quindi potuto verificarne la funzionalità.

1.2 Mercoledì 25/06/2025

1.2.1 Cose fatte oggi

Oggi ho studiato anche la parte relativa alla sicurezza mobile, anche se non ho potuto testarla per (credo) mancanza di dispositivi registrati.

Ho testato la funzionalità del Sandbox Analyzer: il sistema permette di inviare al Sandbox qualsiasi file se si avesse il dubbio che possa essere pericoloso, in pochi minuti nella pagina dedicata si riceverà un resoconto della “detonazione” del file, con relativi livelli di severità e comportamenti.

Ho testato la configurazione di ulteriori politiche, arricchendo ciò che era stato fatto nei giorni precedenti.

Ho inoltre configurato una repo GitHub per garantire il versioning della documentazione che sto redando, la pagina della documentazione aggiornata è disponibile al link:

https://marindavide.github.io/stage-BitDefender/

1.2.2 Difficoltà riscontrate

Dubbi sulla utilità di alcuni moduli. Incongruenze tra la documentazione e il portale GravityZone, che rallentano il lavoro durante la messa in pratica di alcune operazioni.