Diario dei progressi

Versione	Data	Redattore	Descrizione
0.10	10/07	Davide Marin	Aggiunte sezioni “Martedì 08, Mercoledì 09 e Giovedì 10/07”
0.9	09/07	0.9	02/07
Davide Marin	Aggiunta sezione “Lunedì 07/07”	0.8	02/07
Davide Marin	Aggiunta sezione “Venerdì 04/07”	0.7	02/07
Davide Marin	Aggiunta sezione “Giovedì 03/07”	0.6	02/07
Davide Marin	Aggiunta sezione “Mercoledì 02/07”	0.5	01/07
Davide Marin	Aggiunte sezioni “Lunedì 30/06” e “Martedì 01/07”	0.4	27/06
Davide Marin	Aggiunta sezione “Venerdì 27/06”	0.3	26/06
Davide Marin	Aggiunta sezione “Giovedì 26/06”	0.2	25/06
Davide Marin	Aggiunta sezione “Mercoledì 25/06”	0.1	24/06
Davide Marin	Creazione documento, aggiunte sezioni riassunto e “Lunedì 24/06”		

1. Prima settimana (19-27/06)

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.

1.2. Martedì 24/06

1.2.1. 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.

1.2.2. 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.

1.3. Mercoledì 25/06

1.3.1. 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/

1.3.2. 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.

1.4. Giovedì 26/06

1.4.1. Cose fatte oggi

Ho iniziato a studiare la parte di deply del prodotto, seguendo la “tabella di marcia” del piano di progetto e iniziato a redigere la documentazione relativa.

Ho testato la creazione di pacchetti di installazione per gli agenti, e la loro installazione su un endpoint remoto, che hano avuto successo.

Ho iniziato a studiare la parte di integrazione di Active Directory, e la sua configurazione.

1.4.2. Difficoltà riscontrate

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

1.5. Venerdì 27/06

1.5.1. Cose fatte oggi

Ho creato una policy personalizzata che comprenda una whitelist per i domini e gli IP necessari per il funzionamneto di PhishBrain, e applicata ad altri endpoint aziendali.

Ho continuato a redigere la documentazione relativa al deploy del prodotto.

Ho approfondito la parte di sicurezza per le mail, in particolare come poter gestire le soluzioni che utilizzano Microsoft 365 in cloud.

Ho trovato e provato come impostare il PowerUser su un endpoint:

- Inserire nel pacchetto di installazione il modulo "PowerUser"
- Selezionare, all'interno della Policy che si applicherà all'endpoint, la spunta "Power User" ed inserire la password desiderata.
- Applicare la policy all'endpoint.
- Sull'endpoint, è possibile accedere alla CLI del Power User selezionando l'opzione omonima dopo aver cliccato con il tasto destro sull'icona di Bitdefender (che si trova in "icone nascoste" nella barra delle applicazioni).
- È inoltre possibile accedere alla GUI del Power User, per farlo bisogna aprire il file `EPPowerConsole.exe` che si trova in:

```
c:\Program Files\Bitdefender\Endpoint Security
```

Inoltre, ho preso failiarità sia con la CLI del Power User, sia con quella dell'utente normale, che potrebbe tornare utile in caso di macchine virtuali senza GUI. Per futuro utilizzo, i comandi disponibili per l'utente normale sono disponibili **qui** mentre quelli per il Power User sono disponibili **qui**.

1.5.2. Difficoltà riscontrate

Documentazione scarsa e poco chiara per quanto riguarda l'integrazione della sicurezza delle mail con Microsoft 365, inoltre sono incapacitato di testare la funzionalità perché l'azienda possiede già un servizio di sicurezza mail che andrebbe in conflitto con quello di Bitdefender.

2. Seconda settimana (30/06-04/07)

2.1. Lunedì 30/06

2.1.1. Cose fatte oggi

Oggi ho studiato la parte relativa ai security containers. Inoltre, ho iniziato a vedere la parte di API e provato alcune chiamate tramire script in Python.

2.1.2. Difficoltà riscontrate

nessuna difficoltà particolare.

2.2. Martedì 01/07

2.2.1. Cose fatte oggi

Oggi mi sono concentrato sulla parte di API, e di monitoraggio e mitigiazione del rischio degli endpoint

2.2.2. Difficoltà riscontrate

La piattaforma non permette di visualizzare le modifiche effettuate, per la mitigazione dei rischi, in tempo reale, il che rende difficile avere un riscontro delle modifiche effettuate.

2.3. Mercoledì 02/07

2.3.1. Cose fatte oggi

Tra le varie operazioni di oggi, ho esplorato la funzionalità “search” degli incidenti.

2.3.2. Difficoltà riscontrate

Nessuna difficoltà particolare.

2.4. Giovedì 03/07

2.4.1. Cose fatte oggi

In mattinata ho ripassato e organizzato le idee per la presentazione ai colleghi del pomeriggio. Nel complesso la presentazione si può ritenere soddisfacente, anche se carente nella parte di presentazione iniziale del prodotto.

2.4.2. Difficoltà riscontrate

Nessuna difficoltà tecnica, ne ho riscontrate nell’organizzare la presentazione.

2.5. Venerdì 04/07

2.5.1. Cose fatte oggi

Oggi ho controllato alcune funzionalità, in base ai feedback ricevuti dai colleghi durante la presentazione di ieri.

Ho lavorato per portare il mio endpoint a 0 vulnerabilità e rischi, in modo da poterlo replicare in futuro su altre macchine.

Ho iniziato a verificare il funzionamento della parte di reportistica e di politiche di detection e esclusione personalizzate.

2.5.2. Difficoltà riscontrate

La parte di detection e esclusione personalizzate non è molto chiara, sembrano esserci notevoli limiti nella corretta esecuzione delle regole.

3. Terza settimana (07-11/07)

3.1. Lunedì 07/07

3.1.1. Cose fatte oggi

Ho continuato a lavorare sulla parte di detection e esclusione personalizzate. Ho inoltre visto il funzionamento della blocklist, che permette di bloccare l'esecuzione di file e processi specifici.

3.2. Martedì 08/07 e Mercoledì 09/07

3.2.1. Cose fatte

Ho rivisto tutte le funzionalità del prodotto e la documentazione redatta, apportando aggiunte e modifiche, in vista della futura applicazione su clienti reali.

3.3. Giovedì 10/07

3.3.1. Cose fatte oggi