**CyberEscape: Scenari di gameplay e storyline**

**Waiting Room e Tutorial**

In questa scena preliminare il giocatore interagisce con una stanza vuota e attraverso UI vengono spiegati i comandi di per muoversi nello spazio, muovere la visuale e interagire con gli oggetti.

**Introduzione**

Sei il nuovo CISO/Responsabile IT di un’azienda, (i colleghi sono tutti in vacanza) e devi effettuare le ultime pratiche prima di lasciare l’ufficio. Qui puoi muoverti all’interno della sala server e interagire con diversi terminali, tra cui quello principale che usi per controllare tutti i sistemi.

All’inizio della partita viene assegnata una difficoltà standard con valore 0 = Facile e in base alle azioni intraprese cambia il valore di questa difficoltà (**aumenta** +1, **diminuisce** -1, **difficoltà invariata**) o viene caricato direttamente uno scenario nel caso di un’azione speciale.

Qui finisce l’introduzione e si entra nella partita, in base al tipo di attacco previsto si caricherà uno dei seguenti scenari.

**Phishing/Whaling**

Arriva la chiamata di un collega che ti chiede di smistare le ultime mail rimaste da leggere, tra queste alcune sono tentativi di phishing, altre invece vanno aperte e inoltrate al capo.

**Livello 1 Setup difficoltà livello e arrivo minaccia informatica**

Obiettivo del primo livello è filtrare correttamente tutte le mail, le azioni intraprese in questo scenario, decideranno la difficoltà della partita nei seguenti modi:

Azione 1: Mail affidabile segnalata e non inoltrata

In questo caso la difficoltà diminuisce o rimane invariata in base al tipo di mail che è stata inoltrata e inoltre comporta una perdita di punteggio e giorni di ferie da parte del capo che prende provvedimenti per una perdita dell’azienda in termini di tempo e soldi:

Mail affidabile facile da riconoscere, **diminuisce difficoltà** e perdita di punteggio;

Mail affidabile difficile da riconoscere o ambigua, **difficoltà invariata** e perdita di punteggio.

Azione 2: Apri una mail sospetta e subisci un attacco di phishing

Tra le mail che devi smistare, ne apri una con link sospetti e mittenti non verificati, questo scatena un logout dall’account aziendale improvviso, con un messaggio di errore: “password account aziendale errata, sei stato disconnesso dal tuo account”.

Questo comporta una perdita di punti e a una diminuzione della difficoltà proporzionata alla mail che è stata aperta:

Mail facilmente riconoscibile **Valutazione su riconoscimento phising bassa**, e grande perdita punti/giorni di ferie. Difficoltà minima = 0

Mail difficilmente riconoscibile **Valutazione su riconoscimento phising medio-alta**, e perdita punti/giorni di ferie. Diminuisce difficoltà attuale di -1

Passi direttamente al Livello 2 con la difficoltà ottenuta

Azione 3: Segnali mail per Phishing

Aumento difficoltà e valutazione finale in base alla mail che è stata segnalata:

Facilmente riconoscibile, **difficoltà invariata** e aumento piccolo di punteggio/giorni di ferie

Difficilmente riconoscibile, **aumento difficoltà** e aumento significativo di punteggio/giorni di ferie

Azione 4: Non hai aperto mail di phishing e hai inoltrato tutte le mail affidabili al capo

La difficoltà viene impostata al massimo.

Ricevi una chiamata dal capo che ti avvisa di aver ricevuto tutte le mail inoltrate e dice di aver cliccato su una mail per inviare un bonifico urgente (attacco di whaling) e che adesso non può più accedere al suo conto/account aziendale. Ti fai comunicare mail e password (estremamente facile da forzare, es. nome + data di nascita) e ti costringe a rimanere in ufficio per risolvere la questione e recuperare l’account.

**Livello 2 Segnalazione**

Questo livello cambia in base alla difficoltà in termini di tempo (termine non oltre il quale bisogna mandare la segnalazione), e nella presenza di aiuti visivi e interattivi (collega che ti spiega e guida nelle cose da fare, manuale a portata di mano).

Obiettivo del secondo livello è verificare la conoscenza del giocatore su argomenti di cybersecurity e attacchi informatici.

Goal del Livello è riconoscere il tipo di minaccia tra le varie possibili e segnalare al CSIRT o ente incaricato di raccogliere le segnalazioni a livello nazionale, la minaccia corretta tra quelle proposte con l’uso del telefono aziendale. Tra le proposte in base allo scenario avrai Phishing o Whaling a seconda del tipo di attacco che è arrivato.

Scenario 1: Segnalazione effettuata correttamente

Compare sullo schermo un breve video/descrizione dell’attacco e un riferimento al manuale che bisogna utilizzare in questi casi e si passa direttamente al Livello 3.

Scenario 2: Segnalazione dell’attacco errata

Compare sullo schermo un breve video/descrizione dell’attacco e un riferimento al manuale che bisogna utilizzare in questi casi, ma finto questo si ripete il Livello 1 contando tra il punteggio l’errore commesso.

Scenario 3 Tempo scaduto

Ripeti livello, difficoltà -1.

**Livello 3 Effettua azioni correttive**

Questa fase serve a sensibilizzare il personale sugli effetti che può avere un attacco di phishing e quanto esso possa influenzare l’intera organizzazione e interrompere la produzione.

Questo livello cambia in base alla difficoltà in termini di tempo (termine non oltre il quale bisogna mandare la segnalazione), e nella presenza di aiuti visivi e interattivi (collega che ti spiega e guida nelle cose da fare, manuale a portata di mano).

Dal terminale collegato direttamente ai server disattiva l’accesso di tutti gli IP sospetti e disattiva account compromessi tra quelli presenti nella lista.

In base alla difficoltà aumentano le mail di phishing inviate e ci possono essere dei Data breach.

**Livello 4 Ripristino dei Sistemi**

Obiettivo di questo livello è sensibilizzare il giocatore sulle buone pratiche da seguire per un utilizzo corretto delle credenziali di accesso per un account aziendale.

Attraverso l’uso del manuale decidi una nuova password coerente con gli standard di sicurezza, e attiva autenticazione a due fattori con l’inserimento del codice ricevuto.

**Ransomware**

Arriva ala chiamata di un collega che ti chiede di smistare i file su computer per effettuare il backup prima di andare via, a seconda del tipo di file vanno smistati in ordine di importanza e con certi criteri di cryptazione e sicurezza.

In base al tempo e al modo in cui vengono smistati i file si deciderà la diffioltà con cui verrà affrontata la partita.

**DDos**

Arriva la chiamata di un collega, che ti chiede di …

**Conclusione**

Attraverso l’analisi dei dati rilevativi al tempo di completamente di ciascun livello, alle scelte intraprese e alla difficoltà con la quale è stata svolta la partita si tira fuori un punteggio complessivo per diversi campi riguardanti il tema affrontato.