

**Incident**

**Response**

**Plan (IRP)**

[NOME AZIENDA] [DATA ELABORAZIONE]

**HISOLUTION SRL**

Via della Canapiglia 5,  
56019 Vecchiano, PI, Italia  
Tel: +39 050 6397401  
info@hisol

Indice dei contenuti

[1. Introduzione 5](#_Toc213144847)

[1.1 Introduzione 5](#_Toc213144848)

[1.2. Obiettivo 5](#_Toc213144849)

[1.3. Ambito 6](#_Toc213144850)

[1.4. Governance 8](#_Toc213144851)

[1.5. Formazione e Test 8](#_Toc213144852)

[1.6. Lista di controllo IR per i Dipartimenti 9](#_Toc213144853)

[1.7. Obiettivi 10](#_Toc213144854)

[1.8. Processo di gestione IR 10](#_Toc213144855)

[1.9. Il ciclo OODA 12](#_Toc213144856)

[2. Classificazione della gravità 14](#_Toc213144857)

[2.1. Valutazione della gravità 14](#_Toc213144858)

[2.2. Severity Classification 15](#_Toc213144859)

[3. Definizione di Ruoli e Responsabilità 18](#_Toc213144860)

[3.1. Ruoli e Responsabilità 20](#_Toc213144861)

[3.2. Informazioni di Contatto 21](#_Toc213144862)

[4. Piano di Comunicazione 22](#_Toc213144863)

[4.1. Canali di Comunicazione d’Emergenza 22](#_Toc213144864)

[4.2. Comunicazioni con Parti Esterne 22](#_Toc213144865)

[4.3. Piano di Comunicazione Interna 24](#_Toc213144866)

[4.4. Frequenza delle riunioni 25](#_Toc213144867)

[4.5. Notifiche 25](#_Toc213144868)

[4.6. Modello di notifica 26](#_Toc213144869)

[5. Incident Response Framework – Quadro di riferimento per la gestione degli incidenti 27](#_Toc213144870)

[6. Preparazione 31](#_Toc213144871)

[6.1. Infrastruttura 32](#_Toc213144872)

[7. Rilevamento e Analisi 34](#_Toc213144873)

[7.1. Dichiarazione dell’incidente 34](#_Toc213144874)

[7.2. Attivazione della “Situation Room” 36](#_Toc213144875)

[7.3. Valutazione dell’ambito 37](#_Toc213144876)

[7.4. Attività di rilevamento e analisi 38](#_Toc213144877)

[7.5. Attribuzione dell’Avversario 40](#_Toc213144878)

[7.6. Coinvolgimento Risorse Esterne 40](#_Toc213144879)

[7.7. Conservazione delle Prove 42](#_Toc213144880)

[8. Contenimento, eradicazione e ripristino 43](#_Toc213144881)

[8.1. Contenimento 43](#_Toc213144882)

[8.1.1. Strategie di Contenimento 43](#_Toc213144883)

[8.2. Eradicazione e ripristino 44](#_Toc213144884)

[8.3. Uscita dalla Fase di Contenimento, Eradicazione e Ripristino 45](#_Toc213144885)

[9. Post-Incident Activity 47](#_Toc213144886)

[9.1. Analisi post incidente 48](#_Toc213144887)

[9.2. Revisione e aggiornamento del piano IR 51](#_Toc213144888)

[9.3. Tempistiche per l’implementazione 51](#_Toc213144889)

[10. Appendice 53](#_Toc213144890)

[10.1. Incident Response Templates 53](#_Toc213144891)

[10.1.1. Incident Response Timeline Template 54](#_Toc213144892)

[10.1.2. Template per la Root Cause Analisi 55](#_Toc213144893)

[10.1.3. Template di Revisione Post-Incidente 56](#_Toc213144894)

[10.2. Addendum al Processo di RCA 57](#_Toc213144895)

[10.2.1. Passaggi del Processo RCA 58](#_Toc213144896)

[10.3. Addendumm al Processo di Revisione Post-Incidente 59](#_Toc213144897)

[10.3.1. Fasi del Processo di Revisione Post-Incidente 60](#_Toc213144898)

[10.4. Playbook 61](#_Toc213144899)

# 1. Introduzione

## 1.1 Introduzione

Questo piano di risposta agli incidenti è stato sviluppato per HiSolution seguendo le linee guida e le raccomandazioni standardizzate di NIST e CISA. Il piano è stato revisionato e approvato dal team di risposta agli incidenti di HiSolution e dal management aziendale. Poiché il panorama delle minacce e la nostra attività sono in continua evoluzione, il piano sarà aggiornato di conseguenza.

Il documento descrive i componenti principali del processo di gestione degli incidenti, tra cui:

* Valutazione della gravità di un incidente
* Definizione dei ruoli e delle responsabilità
* Implementazione di una strategia di comunicazione
* Identificazione, contenimento ed eliminazione efficace delle minacce
* Riduzione dei danni e ripresa delle normali operazioni
* Documentazione e raccolta delle prove forensi per la revisione post-incidente
* Aggiornamento, test e miglioramento del piano di risposta agli incidenti di HiSolution

## 1.2. Obiettivo

Questo Piano di Risposta agli Incidenti mira a delineare un metodo sistematico per affrontare gli incidenti di cybersicurezza, garantendo un contenimento rapido, un'indagine approfondita, l’eradicazione completa, il recupero e la rendicontazione accurata per ridurre l’impatto sulle operazioni aziendali.

## 1.3. Ambito

Il Piano di Risposta agli Incidenti di Cybersicurezza copre tutti gli asset informatici di HiSolution, comprese le applicazioni aziendali, i sistemi di produzione e la proprietà intellettuale. Esso sostituisce i piani di sicurezza per singole unità aziendali, che dovranno essere allineati a questo piano centrale. Ad esempio, una risposta efficace agli incidenti richiede collaborazione tra il CSIRT (Computer Security Incident Response Team) e il Team per la Protezione dei Dati.

Qualsiasi sospetto incidente di cybersicurezza deve essere immediatamente segnalato al Security Operations Center (SOC). La segnalazione tempestiva è essenziale affinché HiSolution possa rispondere in modo efficace e contenere rapidamente l’incidente, inclusi i sistemi coinvolti e gli eventuali dati personali. Un incidente può essere accidentale o intenzionale e può avere impatti su tutte le aree operative, inclusi riservatezza, integrità e disponibilità. I possibili incidenti includono:

|  |  |
| --- | --- |
| **Incidente** | **Descrizione** |
| Malware | |  | | --- | | Software progettato per danneggiare o compromettere computer, reti o dispositivi |  |  | | --- | |  | |
| Ransomware | |  | | --- | | Malware che cripta i dati e richiede il pagamento di un riscatto, spesso si diffonde tramite campagne di phishing o vulnerabilità software |  |  | | --- | |  | |
| Accesso non autorizzato | |  |  | | --- | --- | | |  | | --- | | Accesso non consentito a un sistema, rete o dati. Può avvenire tramite hacking,  sfruttamento di vulnerabilità o uso di credenziali rubate | |  |  | | --- | |  | |
| Esfiltrazione di dati | |  |  |  | | --- | --- | --- | | |  | | --- | | Acquisizione illegale di informazioni sensibili da un computer o rete,  spesso eseguita tramite malware o vulnerabilità dei sistemi |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Compromissione della supply chain |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Violazione della sicurezza attraverso lo sfruttamento delle vulnerabilità della catena  di fornitura, inclusi fornitori terzi, fornitori di software o partner di servizi |  |  | | --- | |  | |  |  | | --- | |  | |
| Phishing | |  |  |  | | --- | --- | --- | | |  | | --- | | Attacco informatico che prevede l’invio di e-mail ingannevoli per indurre gli  utenti a rivelare informazioni sensibili, cliccare su link dannosi o scaricare  software malevoli |  |  | | --- | |  | |  |  | | --- | |  | |
| Compromissione dell’email aziendale | |  |  |  | | --- | --- | --- | | |  | | --- | | Tipo specifico di phishing in cui gli attaccanti utilizzano frodi via e-mail per ingannare i dipendenti inducendoli a divulgare informazioni riservate, trasferire fondi o concedere accessi privilegiati |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Minaccia interna |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Minaccia proveniente dall’interno dell’organizzazione, spesso da  parte di dipendenti, collaboratori o partner commerciali che hanno  accesso a informazioni e sistemi riservati |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Minaccia persistente avanzata (APT) |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Attacco informatico prolungato e mirato, in cui un attaccante non  autorizzato si infiltra nella rete e rimane inosservato per un periodo  prolungato |  |  | | --- | |  | |  |  | | --- | |  | |
| |  | | --- | | Asset compromesso |  |  | | --- | |  | | |  |  |  | | --- | --- | --- | | |  | | --- | | Risorsa (computer, rete o dati) che ha subito una violazione della sicurezza,  consentendo l’accesso o il controllo non autorizzato da parte di un  attaccante |  |  | | --- | |  | |  |  | | --- | |  | |
| DDoS (Distributed Denial of Service) | Attacco che sfrutta numerosi sistemi compromessi per sovraccaricare un obiettivo con traffico eccessivo, esaurendone le risorse |

## 1.4. Governance

Il Team di Cybersicurezza è responsabile dell’implementazione di questo piano, come definito nel Sistema di Gestione della Sicurezza delle Informazioni di HiSolution. Il piano è stato sviluppato con il contributo e l’approvazione del management aziendale.

## 1.5. Formazione e Test

Il responsabile del Programma di Risposta agli Incidenti, in coordinamento con il CISO, è responsabile di garantire che ciascuna unità aziendale abbia accesso e abbia completato la formazione relativa a questo piano. Verranno organizzate esercitazioni periodiche per testare l’efficacia del piano.

Esercitazioni simulate

Le esercitazioni tabletop devono essere effettuate almeno una volta all’anno. Esse devono simulare scenari realistici e testare tutti gli aspetti del piano e del team di risposta agli incidenti.

I partecipanti dovrebbero includere membri del CSIRT e rappresentanti dei principali dipartimenti coinvolti, come IT, Sicurezza, Legal e fornitori terzi. Le esercitazioni dovrebbero fornire indicazioni utili per aggiornare e migliorare il piano di risposta agli incidenti di HiSolution.

**Risorse utili:**

* Pacchetti di esercitazione CISA
* Best Practice Sophos
* Template tabletop forniti da Sophos su richiesta

## 1.6. Lista di controllo IR per i Dipartimenti

L’obiettivo del processo IR (Incident Response) è quello di stabilire un metodo affidabile per costituire un team IR (Team di Risposta agli Incidenti) opportunamente dimensionato, specifico per ciascun incidente. Ogni dipartimento deve mantenere un protocollo di escalation documentato e le relative procedure, per garantire una gestione fluida e interfunzionale del processo IR, come descritto nella checklist riportata di seguito.

|  |  |  |
| --- | --- | --- |
| **Voce** | **Descrizione** | |
| |  | | --- | | Referenti IR dipartimentali |  |  | | --- | |  | | | |  | | --- | | Responsabili dell’attuazione dei processi IR nel dipartimento |  |  | | --- | |  | | |
| |  | | --- | | Team IR dipartimentale |  |  | | --- | |  | | | |  | | --- | | Gruppo responsabile delle attività di risposta |  |  | | --- | |  | | |
| |  | | --- | | Criteri di escalation |  |  | | --- | |  | | | |  | | --- | | Allineati ai livelli di gravità definiti nel piano |  |  | | --- | |  | | |
| |  | | --- | | Processi e playbook |  |  | | --- | |  | | | |  | | --- | | Linee guida operative per la gestione degli incidenti |  |  | | --- | |  | | |
| |  | | --- | | Test dei processi |  |  | | --- | |  | | | |  | | --- | | Per garantire l’efficacia continua delle procedure | | |

## 1.7. Obiettivi

* Identificazione e contenimento rapidi degli incidenti
* Riduzione dei danni alle funzioni aziendali
* Rapida eradicazione e recupero delle operazioni
* Comunicazione efficace e rendicontazione degli incidenti
* Revisione post-incidente per un miglioramento continuo

## 1.8. Processo di gestione IR

Il processo di gestione degli incidenti (IR handling process) rappresenta un approccio organizzato che garantisce continuità, efficienza e collaborazione tra tutte le parti coinvolte. (Vedi figura di seguito)

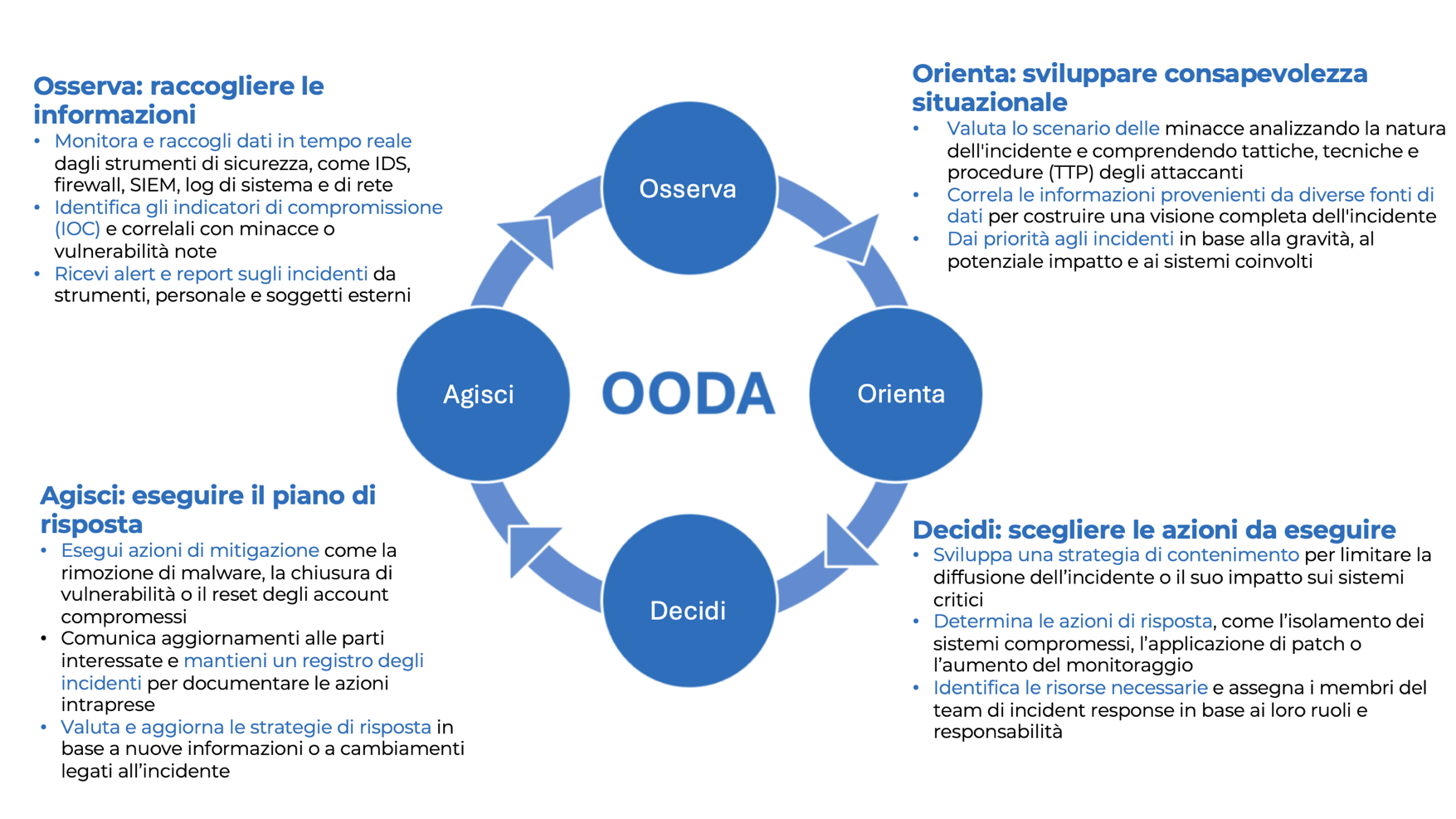
Immagine che contiene Blu elettrico, schermata, blu, Blu cobalto

Il contenuto generato dall'IA potrebbe non essere corretto.

## 1.9. Il ciclo OODA

Gestire un incidente può essere stressante e ostacolare decisioni rapide e accurate. Il ciclo OODA (Osservare, Orientarsi, Decidere, Agire) offre un quadro strutturato per migliorare la consapevolezza della situazione e il processo decisionale.

Applicare il ciclo OODA nella risposta agli incidenti consente una gestione efficiente ed efficace degli eventi informatici. Esso fornisce un metodo organizzato e iterativo per affrontare minacce complesse.



# 2. Classificazione della gravità

Definire i livelli di gravità è essenziale per costruire un sistema efficace di classificazione degli incidenti all’interno di un piano di risposta agli incidenti (Incident Response – IR). Tale classificazione consente di:

* Dare priorità alle azioni di risposta
* Allocare in modo efficiente le risorse
* Applicare protocolli di comunicazione chiari

Gli incidenti ad alta gravità ricevono attenzione immediata, l’allocazione delle risorse necessarie, il rispetto dei requisiti normativi e la guida di miglioramenti strategici, rafforzando così la resilienza dell’organizzazione contro incidenti futuri.

## 2.1. Valutazione della gravità

Il Security Operations Center (SOC) di HiSolution valuta gli incidenti sulla base di criteri specifici per l’analisi della minaccia. Successivamente, il Manager della Risposta agli Incidenti (Incident Response Manager) assegna un livello di gravità.

I criteri utilizzati per assegnare un punteggio agli incidenti includono:

* **Impatto funzionale**: valutazione del grado in cui l’incidente ha compromesso le funzioni operative aziendali
* **Impatto informativo**: determinazione della sensibilità e criticità delle informazioni coinvolte
* **Attività osservata**: identificazione delle azioni malevoli rilevate o sospette
* **Caratterizzazione e attribuzione dell’attore**: determinazione dell’identità e dell’intento dell’aggressore, quando possibile
* **Localizzazione dell’attività osservata**: identificazione delle aree geografiche o infrastrutturali coinvolte
* **Capacità di recupero**: misura in cui è possibile ripristinare i sistemi interessati
* **Impatto potenziale**: stima dei possibili effetti sull’attività aziendale, sulla reputazione e sugli obblighi normativi

Sebbene i criteri di valutazione della gravità garantiscano coerenza, il Manager IR e lo Sponsor Esecutivo hanno l’autorità di modificare il livello di gravità assegnato a un incidente, qualora lo ritengano necessario.

Durante tutto il processo di gestione dell’incidente, la gravità viene rivalutata continuamente e modificata, se opportuno.

## 2.2. Severity Classification

La seguente matrice di classificazione della gravità descrive gli obiettivi di tempo di risposta per gli incidenti di cybersicurezza, sulla base dell’impatto previsto degli incidenti sulla sicurezza delle informazioni aziendali di HiSolution.

Il tempo di risposta viene misurato a partire dal momento in cui all’incidente viene assegnato un livello di gravità.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Gravità** | **Descrizione** | | **Dettagli** | **Tempo di risposta** |
| 0 – Critico | | |  | | --- | | Incidente critico con impatto potenzialmente esistenziale sull’azienda |  |  | | --- | |  | | |  | | --- | | **Furto o esposizione** di grandi volumi di dati altamente sensibili relativi a clienti o dipendenti |  |  | | --- | |  | | Immediato |
| 1 - Alto | | |  | | --- | | Incidente importante con impatto  molto elevato |  |  | | --- | |  | | Funzionalità   * Un servizio rivolto ai client è inattivo o a rischio | 2 ore |
| Informazioni   * Perdita di dati ad alto impatto (es. dati di clienti o dipendenti, codice sorgente, dati finanziari) * Violazione di riservatezza o privacy |
| Recuperabilità   * Presenza di Ransomware su molti sistemi critici |
| Reputazione   * Probabile copertura mediatica * Sicurezza dei clienti compromessa |
| 2 -Medio | | Incidente rilevante con impatto  significativo | Funzionalità   * Un servizio essenziale non è accessibile per alcuni clienti o dipendenti | 48 ore |
| Informazioni   * Violazione della riservatezza di dipendenti o fornitori * Violazione di normative (es. GDPR, PCI, HIPAA) |
| Recuperabilità   * Ransomware su sistemi che ospitano dati a impatto aziendale medio |
| Reputazione   * Possibile o effettiva diffusione sui social media |
| Esempio   * Lista dei client o dipendenti esfiltrata |
| 3 – Basso | | Incidente minore con impatto contenuto | Funzionalità   * Disagio minore per clienti o dipendenti, disponibile una soluzione temporanea | 2 settimane |
| Informazioni   * Compromissione di pochi individui e di dati a basso rischio (es. indirizzi e-mail aziendali) |
| Recuperabilità   * Impatto minimo ma comunque funzionale sulle prestazioni |
| Esempio   * E-mail di phishing segnalata ma non eseguita |

# 3. Definizione di Ruoli e Responsabilità

Definire in modo chiaro i ruoli e le responsabilità è un elemento fondamentale per una strategia efficace di risposta agli incidenti. Una chiara assegnazione dei ruoli stabilisce chi fa cosa, sia nella gestione dell’incidente sia nella sua governance.

Stabilire tali ruoli in anticipo consente all’organizzazione di affrontare gli incidenti in modo sistematico nel momento in cui si verificano, garantendo aspettative precise per ogni fase dell’escalation e della comunicazione durante l’intero ciclo di vita dell’incidente.

All’inizio di un incidente, viene nominato un **Incident Response Manager**, in base al livello di gravità dell’incidente stesso. Questo ruolo può ruotare tra diversi soggetti per assicurare una copertura continua 24 ore su 24, 7 giorni su 7, se necessario.

L’Incident Response Manager è responsabile dell’assegnazione iniziale dei ruoli descritti di seguito, in consultazione con i relativi individui designati. Il diagramma riportato nel documento illustra i ruoli chiave e le rispettive responsabilità nella gestione e nella governance degli incidenti.



## 3.1. Ruoli e Responsabilità

|  |  |
| --- | --- |
| **Ruolo** | **Responsabilità** |
| Incident Response Team | |  | | --- | | Conduce l’investigazione, risponde e contiene gli incidenti. Facilita le attività di “lesson learned”, esegue la bonifica dei sistemi compromessi e contribuisce al miglioramento continuo del piano di risposta. |  |  | | --- | |  | |
| Incident Response Manager | |  | | --- | | Determina il livello di gravità dell’incidente, gestisce l’escalation, definisce la composizione completa del team IR, avvia e coordina l’investigazione. |  |  | | --- | |  | |
| Steering Committee | |  | | --- | | Gruppo responsabile della governance dell’incidente. Include membri senior di Legal, Operations Security, CISO e Comunicazione. |  |  | | --- | |  | |
| Incident Response Program Owner | |  | | --- | | Responsabile della gestione del piano di risposta agli incidenti. Garantisce la prontezza del team, mantiene aggiornato il piano IR ed effettua revisioni periodiche. |  |  | | --- | |  | |
| Communications Lead | |  | | --- | | Gestisce le comunicazioni interne ed esterne, comprese quelle rivolte ai clienti e ai media. |  |  | | --- | |  | |
| Consulente Legale | |  | | --- | | Fornisce consulenza su aspetti normativi, legali e di compliance legati all’incidente. |  |  | | --- | |  | |
| Cyber Insurance | Punto di contatto iniziale per la segnalazione dell’incidente alla compagnia assicurativa. |

## 3.2. Informazioni di Contatto

È fondamentale mantenere aggiornata una lista dei contatti dei membri del team IR (Incident Response Team), includendo anche metodi alternativi di contatto nel caso in cui i sistemi principali siano compromessi.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nome** | **Titolo** | **Ruolo** | **Informazioni di contatto** | **Livello di escalation\*** |
| Luca Salvatori | IT MANAGER | Incident Response Team | 3315815901 hsc.pisa@gmail.com | 3 |
| Luca Salvatori | RISK MANAGER | Incident Response Manager | 3315815901 hsc.pisa@gmail.com | 3 |
| Luca Salvatori | CISO | Steering Committee | 3315815901 hsc.pisa@gmail.com | 3 |
| Luca Salvatori | CTO | Incident Response Program Owner | 3315815901 hsc.pisa@gmail.com | 3 |
| Luca Salvatori | CTO CISO | Communications Lead | 3315815901 hsc.pisa@gmail.com | 3 |
| Luca Salvatori | LEGAL DEPARTMENT | Legal Counsel | 3315815901 hsc.pisa@gmail.com | 3 |
| Luca Salvatori | CISO IT MANAGER | Cyber Insurance | 3315815901 hsc.pisa@gmail.com | 3 |

\****Livello di notifica per escalation:***  
**1.** Notifica per tutti gli incidenti  
**2.** Notifica per tutti gli incidenti gravi e critici  
**3.** Coinvolgimento secondo necessità

# 4. Piano di Comunicazione

È responsabilità dell’**Incident Response Manager** e del **Coordinatore dell’Incidente** garantire l’aderenza al piano di comunicazione, sia per quanto riguarda le comunicazioni interne sia quelle esterne.

## 4.1. Canali di Comunicazione d’Emergenza

L’Incident Response Manager valuterà se è necessario attivare canali di comunicazione d’emergenza qualora una minaccia in corso o una vulnerabilità rappresentino un rischio significativo per i normali sistemi di comunicazione aziendale.

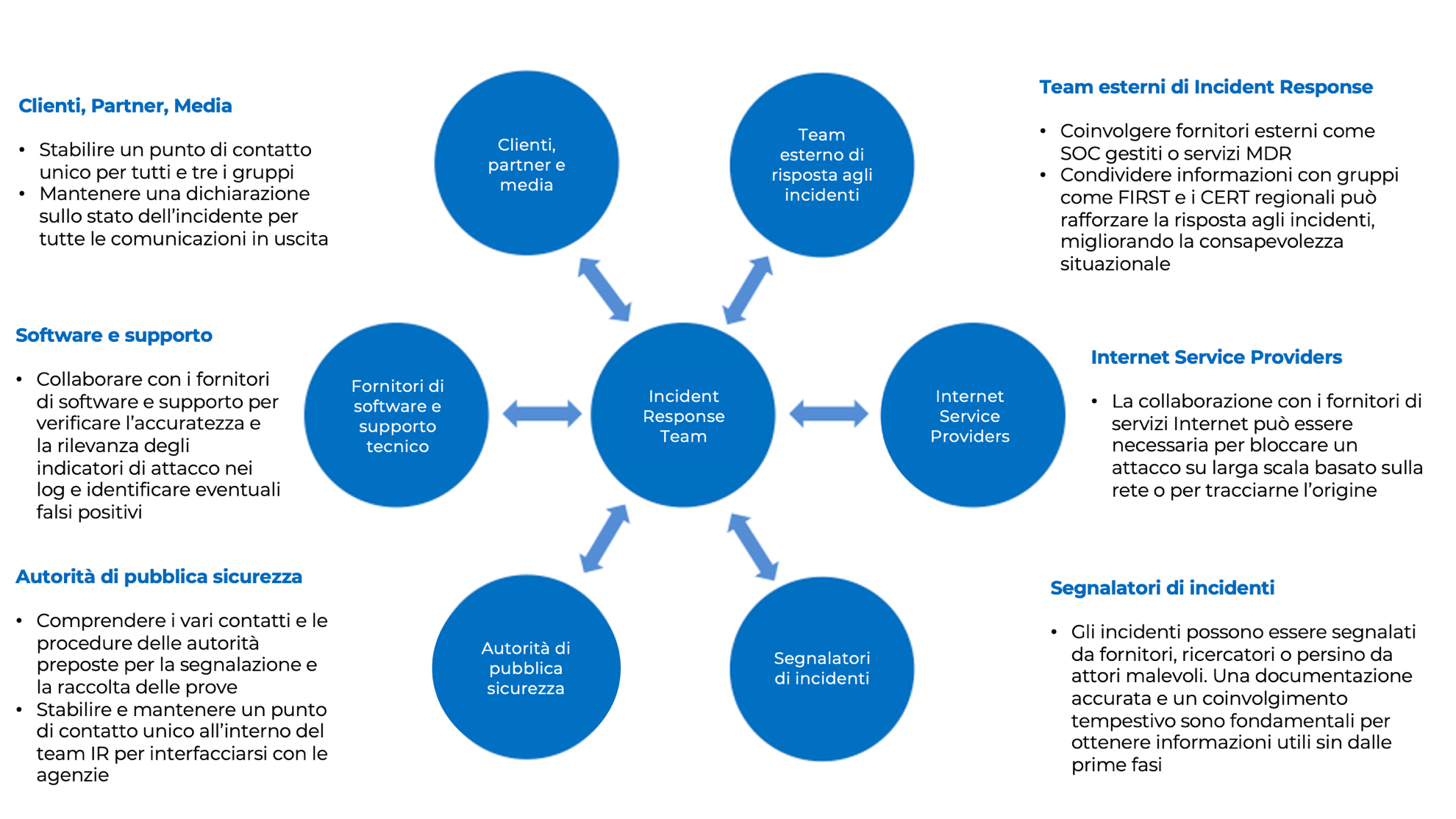
## 4.2. Comunicazioni con Parti Esterne

È fondamentale non solo gestire i rischi interni ma anche informare e collaborare con soggetti esterni in caso di incidente. Le forze dell’ordine dovranno essere coinvolte quando previsto o necessario. Le richieste dei media dovranno essere gestite dal **Consulente Legale** e dall’**Ufficio Comunicazione/Relazioni Pubbliche**.

Solitamente, è necessario coinvolgere anche esperti e fornitori esterni di supporto, come ad esempio provider di servizi internet, compagnie assicurative per la cybersicurezza e autorità di regolamentazione.

È obbligatorio consultare il **Consulente Legale** di HiSolution prima di comunicare con partner, clienti o altri soggetti esterni o autorità. Il Team di Cybersicurezza, con autorizzazione da parte del legale, coordinerà le comunicazioni con soggetti terzi per determinare le informazioni minime da condividere nell’ambito della risposta all’incidente.

Tutte le condivisioni di informazioni richiedono l’approvazione del Consulente Legale e del Chief Information Security Officer (CISO). Le notifiche dovranno essere inviate al contatto designato presso la controparte esterna.

L’immagine mostra i diversi interlocutori esterni e fornisce indicazioni su come comunicare con ciascuno di essi.

## 4.3. Piano di Comunicazione Interna

Per gli incidenti classificati con gravità da **0 a 2**, verrà creato un ticket nella pagina interna degli incidenti di sicurezza, all’interno del sito intranet del dipartimento. Inoltre, sarà predisposto un **canale di comunicazione privato dedicato** per facilitare il coordinamento con il team di risposta agli incidenti.

In aggiunta, potrà essere creata una **cartella protetta e riservata** per l’eventuale condivisione di documentazione. I canali di comunicazione privati (es. Microsoft Teams, Slack, ecc.) saranno utilizzati per le azioni tecniche dettagliate. I membri del team legale e della protezione dei dati avranno accesso a tali canali, se necessario.

Il **Responsabile della Risposta agli Incidenti (IRM)** sarà incaricato di aggiungere gli stakeholder interni a questi canali protetti.

Le comunicazioni interne possono includere, a titolo esemplificativo ma non esaustivo:

* Comunicazioni al Consiglio di Amministrazione
* Comunicazioni alla direzione aziendale
* Comunicazioni generiche o messaggi specifici rivolti ai dipendenti di HiSolution

## 4.4. Frequenza delle riunioni

|  |  |
| --- | --- |
| **Severity** | **Frequenza delle riunioni** |
| Gravità 0 | IR Team: più volte al giorno, con passaggio di consegne (hand-off) programmato fino a 3 volte al giorno se necessario  Steering Committee: più volte al giorno. La cadenza viene stabilita dal Comitato stesso |
| Gravità 1 | IR Team: riunione quotidiana, con hand-off tre volte al giorno se richiesto  Steering Committee: secondo necessità, generalmente ogni giorno. La frequenza viene definita dal Manager IR |
| Gravità 2 | IR Team: una volta al giorno  Steering Committee: su richiesta, a discrezione del Manager IR |
| Gravità 3 | Riunioni solo se necessarie, a discrezione del Manager IR |

## 4.5. Notifiche

La cadenza delle notifiche sullo stato dell’incidente è definita nella tabella sottostante, insieme al modello di notifica da utilizzare.

|  |  |  |  |
| --- | --- | --- | --- |
| **Gravità** | **Responsabile del reporting** | **Destinatario** | **Frequenza** |
| Gravità 0 | Incident Executive Sponsor | CSIRT | Giornaliera: E-mail e chiamata |
| Gravità 1 | IR Manager | Steering Committee | Giornaliera: E-mail |
| Gravità 2 | IR Manager | CISO | Giornaliera: E-mail |
| Gravità 3 | IR Manager | CISO | Giornaliera: E-mail |

## 

## 4.6. Modello di notifica

|  |
| --- |
| **Template di comunicazione interna** |
| * **Nome dell’incidente** * **Gravità**: 0 | 1 | 2 | 3 * **Individui coinvolti** * **Riepilogo dell’incidente**: sequenza degli eventi, azioni intraprese, asset coinvolti * **Impatto sull’attività aziendale** * **Fase dell’incidente**:   + Rilevamento e Analisi   + Contenimento, Eradicazione e Ripristino   + Attività Post-Incidente * **Azioni completate**, **azioni in corso**, **prossimi step** * **Link alla pagina dell’incidente** |

# 5. Incident Response Framework – Quadro di riferimento per la gestione degli incidenti

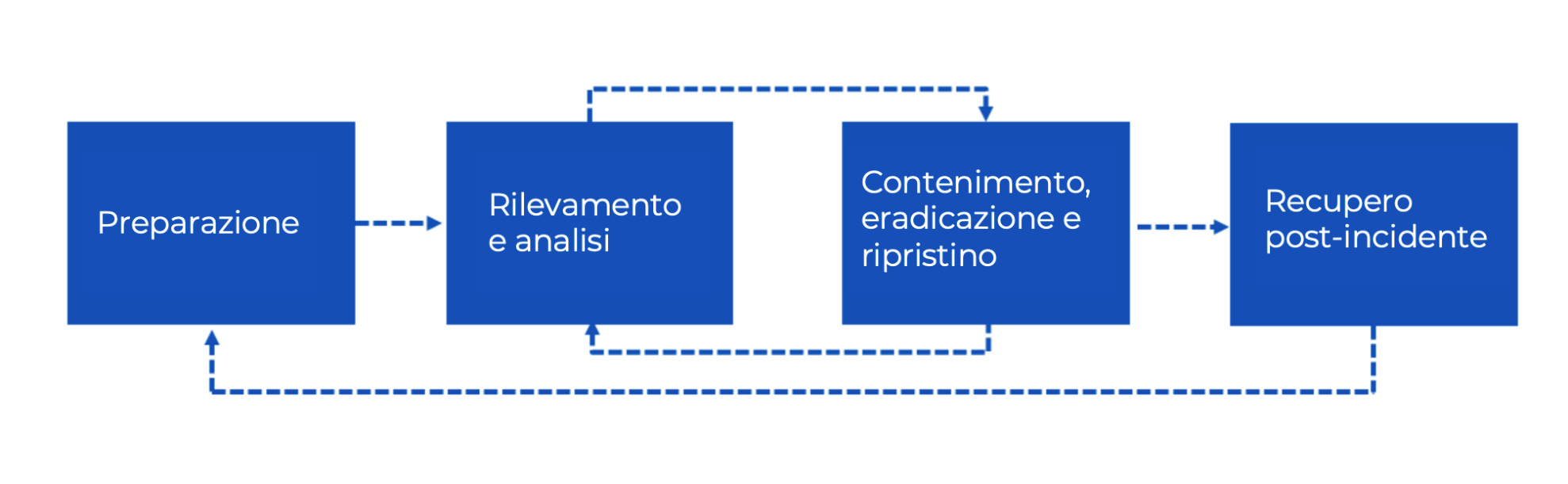
Un framework ben strutturato è fondamentale per proteggere gli asset aziendali, la reputazione e la continuità delle attività di business.

HiSolution adotta il **framework di risposta agli incidenti definito dal NIST** (National Institute of Standards and Technology) durante l’intero processo di indagine sugli incidenti.

Integrare questo framework nella strategia di risposta agli incidenti dell’organizzazione contribuisce a:

* Rafforzare la resilienza
* Migliorare la collaborazione tra i team
* Rafforzare l’approccio generale alla cybersicurezza

Le **quattro fasi chiave** del nostro approccio sono illustrate di seguito.



Preparazione: La fase di preparazione ha lo scopo di sviluppare e implementare **misure proattive** per rispondere in modo efficace agli incidenti. Include:

* Definizione di politiche e procedure
* Formazione del personale
* Distribuzione di strumenti di sicurezza
* Creazione di playbook di risposta agli incidenti

Rilevamento e Analisi: Questa fase si concentra sull’individuazione di **potenziali incidenti di sicurezza** e sull’analisi per comprendere:

* L’origine
* La portata
* L’impatto
* Il livello di gravità

Gli strumenti chiave includono:

* Monitoraggio continuo
* Avvisi automatici
* Reporting tempestivo

Un rilevamento e un’analisi accurati consentono di rispondere in modo rapido, efficace e con cognizione di causa.

Contenimento, eradicazione e recupero: In questa fase vengono adottate misure per **contenere l’incidente** e impedire ulteriori danni.

Successivamente:

* Si procede all’**eradicazione** della causa dell’incidente
* Si ripristinano i sistemi al loro stato normale
* Viene attivato il **piano di recupero** per garantire una ripresa fluida delle operazioni aziendali

È fondamentale che, dopo il contenimento, venga attivato un monitoraggio continuo per **confermare l’effettiva risoluzione** dell’incidente.

Analisi Post-Incidente: Una volta che l’incidente è stato risolto, si procede con la **valutazione dell’intera risposta all’incidente**. Questa fase prevede:

* Una sessione di **“lesson learned”**
* La revisione degli eventi e delle decisioni intraprese
* L’identificazione di eventuali **azioni correttive**

Il team CSIRT aggiornerà il piano di risposta agli incidenti in base agli insegnamenti appresi, con l’obiettivo di migliorare il livello di sicurezza e prevenire la ripetizione di eventi simili.

# 6. Preparazione

Una preparazione rigorosa e coerente è fondamentale per garantire l’efficacia del piano di risposta agli incidenti. Questa fase assicura che **politiche, processi e risorse** siano pronti ad affrontare con efficienza gli incidenti di cybersicurezza.

Le attività principali previste da questa fase includono – ma non si limitano a – quanto segue:

|  |  |
| --- | --- |
| **Processo** | **Descrizione** |
| Formazione del CSIRT | I membri del CSIRT e gli stakeholder dipartimentali devono effettuare formazione regolare sull’utilizzo corretto degli strumenti di rilevamento, monitoraggio e risposta. Questo comprende anche simulazioni pratiche e l’esercizio di scenari incidentali. |
| Formazione dei dipendenti | HiSolution fornirà a tutto il personale una formazione specifica sui rischi informatici e sui protocolli di segnalazione degli incidenti. Il programma comprenderà:   * Sessioni periodiche di sensibilizzazione alla sicurezza informatica * Simulazioni di phishing * Altre iniziative educative per rafforzare la “security awareness” aziendale |
| Test del piano IR | HiSolution condurrà regolarmente **esercitazioni tabletop** coinvolgendo sia il team CSIRT sia gli stakeholder dipartimentali. Questi test mirano a verificare l’efficacia del piano e la prontezza dei team. |
| Personale e Copertura | Il team sicurezza sarà strutturato per fornire un servizio di **monitoraggio e risposta continuativa**, 24 ore su 24, 7 giorni su 7, durante tutto l’anno. Tale copertura sarà integrata **da servizi SOC esterni** (Security Operations Center), al fine di garantire la massima reattività in ogni momento. |

## 6.1. Infrastruttura

Gestire incidenti complessi in modo efficace richiede un’infrastruttura che garantisca:

* Elevata disponibilità dei sistemi
* Tempi di risposta rapidi
* Canali di comunicazione sicuri

Di seguito sono riportati i **componenti chiave dell’infrastruttura** necessaria alla risposta agli incidenti:

|  |  |
| --- | --- |
| **Processo** | **Descrizione** |
| Definizione baselines | Stabilire, in fase preventiva, le **baseline** delle operazioni, dei sistemi e delle reti, per poter identificare prontamente eventuali **deviazioni** sospette nel momento in cui si verifica un incidente. |
| Strumenti di sicurezza | Individuare e implementare strumenti moderni che rafforzino le capacità di:   * Rilevamento * Monitoraggio * Risposta agli incidenti |
| Archiviazione sicura | Il piano di risposta agli incidenti, i playbook e le procedure correlate devono essere conservati all’interno di **soluzioni di archiviazione sicure e altamente disponibili**, accessibili **esclusivamente dai membri autorizzati del team di risposta** |
| Forensics Digitale | Stabilire la **capacità e il processo** per la raccolta di:   * Log * Dati * Prove digitali |
| Patch management | Garantire che tutti gli asset aziendali siano costantemente aggiornati attraverso un processo efficace e tempestivo di:   * Applicazione delle patch * Aggiornamento del software * Monitoraggio delle vulnerabilità note |
| Backup e ripristino | Eseguire con regolarità il backup dei dati e dei sistemi essenziali. I backup devono essere:   * **Cifrati** * **Memorizzati offline** o in ambienti **air-gapped** * Testati periodicamente per verificarne l’affidabilità e la possibilità di recupero |
| Comunicazioni fuori banda | Configurare **canali primari e secondari di comunicazione fuori banda**, da attivare all’inizio di un incidente, nel caso in cui i sistemi interni risultino compromessi o inaccessibili. |
| Controllo degli accessi | Applicare il **principio del privilegio minimo** (least privilege) su tutti i sistemi aziendali. Implementare **l’autenticazione a più fattori (MFA)** per garantire la sicurezza degli accessi e limitare la superficie di attacco. |

# 7. Rilevamento e Analisi

L’identificazione e l’analisi degli eventi sono fondamentali per determinare se rappresentano segnali di un attacco imminente o in corso. È essenziale **distinguere tra cambiamenti normali nel comportamento del sistema e potenziali compromissioni**.

La fase di rilevamento comprende:

* La valutazione degli eventi
* La dichiarazione dell’incidente
* Un’analisi dettagliata dell’impatto dell’incidente

## 7.1. Dichiarazione dell’incidente

Un incidente viene dichiarato quando è stato **identificato** e **confermato** che è in corso o che si verificherà a breve. La dichiarazione ufficiale dell’incidente viene fatta dal **Responsabile della Risposta agli Incidenti (IR Manager)**.

Dopo la dichiarazione dell’incidente, viene avviato il processo di comunicazione del CSIRT per notificare tutti gli stakeholder e i soggetti terzi rilevanti.

Questa decisione (come mostrato nel diagramma di seguito) si basa su segnalazioni:

* Interne
* Esterne
* Derivanti da **intelligence sulle minacce**
* Provenienti dalle attività di **monitoraggio della sicurezza**

**Immagine che contiene testo, schermata, diagramma, design

Il contenuto generato dall'IA potrebbe non essere corretto.**

## 7.2. Attivazione della “Situation Room”

Dopo l’individuazione di un incidente, il primo passo consiste nell’**attivare i canali di comunicazione** e programmare una **riunione del team di risposta all’incidente**.

Il **Responsabile IR** si occupa di:

* Attivare i canali
* Convocare il team
* Gestire la prima riunione

Durante la riunione iniziale, il team dovrà:

* Nominare un **team lead** (se diverso dall’IR Manager)
* Identificare i **membri del team**
* Definire la **frequenza degli incontri successivi**

Nel corso dell’intera indagine, è fondamentale documentare in modo formale e completo la **cronologia dell’incidente**, registrando:

* Tutti gli eventi principali
* Le azioni intraprese
* I responsabili delle attività
* Le decisioni
* I risultati

**Agenda minima standard per le riunioni IR:**

* Stabilire i fatti noti in quel momento
* Fornire aggiornamenti sullo stato delle azioni
* Concordare i passaggi successivi
* Verificare il livello di gravità: 0 | 1 | 2 | 3
* Confermare che tutti i membri interessati siano informati
* Pianificare la prossima riunione
* Documentare i verbali con azioni e decisioni nella timeline dell’incidente

## 7.3. Valutazione dell’ambito

Durante un’indagine, è cruciale ottenere rapidamente una **chiara comprensione dell’ambito** dell’incidente. I seguenti elementi devono essere esaminati per garantire una risposta efficace:

* Quali sono i **fatti noti** al momento?
* Le informazioni coinvolte sono **riservate, protette o confidenziali**?
* Esiste un sospetto fondato di **esfiltrazione di dati**?
* Qual è stato il **punto d’ingresso**? (es. phishing, fornitore terzo, minaccia interna)
* **Quanti asset** potrebbero essere compromessi?
* Qual è **l’entità e la gravità** del danno potenziale?
* Quanto tempo è previsto per il **completo recupero**?
* Quali **risorse interne ed esterne** saranno necessarie?
* Quali sono le **tattiche, tecniche e procedure** (TTP) osservate?
* Sono state sfruttate **vulnerabilità note** o **zero-day**?

## 7.4. Attività di rilevamento e analisi

Nota: Per proteggere i dati, gli artefatti e le prove, **qualsiasi asset compromesso deve essere scollegato dalla rete**. Non deve essere spento per evitare la perdita di dati critici.

Il **framework MITRE ATT&CK** può aiutare gli analisti a guidare le attività di indagine, allineando le attività alle tattiche e tecniche osservate. La seguente tabella mostra esempi di **fonti di evento** su cui concentrarsi in base alle tecniche comunemente utilizzate dagli attori malevoli.

|  |  |  |
| --- | --- | --- |
| **Tattica** | **Tecniche** | **Fonti di Evento** |
| Initial Access ([TA0001](https://attack.mitre.org/tactics/TA0001)) | Phishing ([T1566](https://attack.mitre.org/techniques/T1566)), supply chain ([T1195](https://attack.mitre.org/techniques/T1195)), drive-by compromise ([T1189](https://attack.mitre.org/techniques/T1189)) | |  | | --- | | Log delle email, registri di creazione file, attività del firewall, log IPS, log di applicazioni fornitore |  |  | | --- | |  | |
| Execution ([TA0002](https://attack.mitre.org/tactics/TA0002)) | Command and scripting ([T1059](https://attack.mitre.org/techniques/T1059)), scheduled tasks ([T1053](https://attack.mitre.org/techniques/T1053)), system services ([T1569](https://attack.mitre.org/techniques/T1569)) | |  | | --- | | Log di host per esecuzione comandi e creazione processi, monitoraggio esecuzione script |  |  | | --- | |  | |
| Persistence ([TA0003](https://attack.mitre.org/tactics/TA0003)) | External services ([T1133](https://attack.mitre.org/techniques/T1133)), pre-OS boot ([T1542](https://attack.mitre.org/techniques/T1542)), scheduled tasks ([T1053](https://attack.mitre.org/techniques/T1053)) | |  | | --- | | Log delle applicazioni, registri di autenticazione, log di rete |  |  | | --- | |  | |
| Credential Access ([TA0006](https://attack.mitre.org/tactics/TA0006)) | Brute force ([T1110](https://attack.mitre.org/techniques/T1110)), input capture ([T1056](https://attack.mitre.org/techniques/T1056)), MFA generation ([T1111](https://attack.mitre.org/techniques/T1111)) | |  | | --- | | Log di autenticazione, log di host, audit comandi, query da strumenti XDR |  |  | | --- | |  | |
| Lateral Movement ([TA0008](https://attack.mitre.org/tactics/TA0008)) | Remote services ([T1021](https://attack.mitre.org/techniques/T1021)), session hijacking ([T1563](https://attack.mitre.org/techniques/T1563)), software deployment tools ([T1072](https://attack.mitre.org/techniques/T1072)) | |  | | --- | | Log endpoint/server, rilevamento rete, log di applicazioni web |  |  | | --- | |  | |
| Command and Control ([TA0011](https://attack.mitre.org/tactics/TA0011)) | Application layer protocol ([T1071](https://attack.mitre.org/techniques/T1071)), encrypted channel ([T1573](https://attack.mitre.org/techniques/T1573)), remote access software ([T1219](https://attack.mitre.org/techniques/T1219)) | Log di firewall e DNS, monitoraggio traffico di rete, log IPS |
| Exfiltration ([TA0010](https://attack.mitre.org/tactics/TA0010)) | Exfiltration over C2 channel ([T1041](https://attack.mitre.org/techniques/T1041)), Scheduled transfer ([T1029](https://attack.mitre.org/techniques/T1029)) | Log firewall, log di host, DNS, rilevamento rete, dispositivi non gestiti |

## 7.5. Attribuzione dell’Avversario

Identificare la **fonte** o l’**identità** dell’attaccante può far risparmiare tempo e aiutare a definire meglio le tattiche di risposta. Aiuta anche il CSIRT a comprendere:

* Le **motivazioni**
* L’**identità probabile**
* Le **capacità** degli attori della minaccia

I seguenti passaggi possono supportare il processo di attribuzione:

* Quali **tattiche, tecniche e procedure** sono state osservate?
* Sono state sfruttate vulnerabilità **note o zero-day**?
* Classificare TTP tramite MITRE ATT&CK
* Identificare **indicatori di compromissione (IoC)** e associarli a TTP rilevati
* Analizzare vulnerabilità note sfruttate da **gruppi di minaccia** specifici
* Eseguire query pianificate XDR/EDR per cercare IoC/TTP noti nella rete
* Consultare fonti di **threat intelligence** per collegare i dati osservati ad attori noti

## 7.6. Coinvolgimento Risorse Esterne

Durante la gestione di un incidente, potrebbe essere necessario il coinvolgimento di:

* Agenzie governative
* Autorità statali o federali
* Aziende esterne specializzate in IR

⚠️ Questo elenco deve essere aggiornato periodicamente durante la **manutenzione del piano IR** e in fase di testing.

|  |  |  |
| --- | --- | --- |
| **Resource** | **Contact** | **Notes** |
| National Cybersecurity and Communications Integrations Center (NCCIC) | +1 8882820870 | [www.us-cert.gov](http://www.us-cert.gov) – Supporto governativo per eradicazione e ripristino |
| Germany Cyber Security Authority | <https://mip2.bsi.bund.de/meldestellen-uebersicht/> | Federal Incident Response resources and vetted Incident Response firms |
| Cyber Insurance |  | |  | | --- | | Contattare tempestivamente per avviare l’erogazione dei servizi previsti |  |  | | --- | |  | |
| No More Ransom | [https://www.nomoreransom.org](https://www.nomoreransom.org/) | |  | | --- | | Permette l’analisi di file criptati tramite Crypto Sheriff per identificare un eventuale decryptor noto |  |  | | --- | |  | |
| Sophos Incident Response | * Australia: +61 272084454 * Austria: +43 73265575520 * Canada: +1 7785897255 * France: +33 186539880 * Germany: +49 61171186766 * Italy: +39 0294752897 * Netherlands: +31 162708600 * Spain: +34 913758065 * Sweden: +46 858400610 * Switzerland: +41 445152286 * United Kingdom: +44 1235635329 * USA: +1 4087461064 | [Sophos Rapid Response](https://www.sophos.com/en-us/products/managed-detection-and-response/incident-response-services) –  Servizio 24/7 di risposta completa agli incidenti: investigazione, ripristino e analisi delle cause |

## 

## 7.7. Conservazione delle Prove

Raccogliere e conservare le prove digitali durante il processo di risposta è cruciale per:

* Attribuire correttamente l’attacco
* Classificare il tipo di minaccia
* Supportare l’analisi delle cause
* Velocizzare eventuali indagini legali

Le principali linee guida includono:

* Raccogliere log da firewall, email, IPS, dati XDR
* Estrarre registri di autenticazione e MFA
* Acquisire audit log da host e server
* Effettuare il **dump della memoria** e immagini del disco per l’analisi forense
* **Isolare** o **disconnettere** i sistemi compromessi (evitare lo spegnimento)
* Assicurare che tutte le prove siano custodite in modo tracciabile
* **Catturare screenshot** delle evidenze rilevanti

# 8. Contenimento, eradicazione e ripristino

## 8.1. Contenimento

L’obiettivo del contenimento è **bloccare gli effetti di un incidente prima che possano causare ulteriori danni**. Una volta che l’incidente è stato contenuto, il Team di Risposta agli Incidenti (IR Team) ha il tempo necessario per pianificare i prossimi passi, che includono:

* L’individuazione e risoluzione della **causa principale**
* Il **ripristino dei sistemi** al loro stato operativo normale

Il **Responsabile della Risposta agli Incidenti (Incident Response Manager – IRM)** è responsabile della **gestione del contenimento**, mentre il **team IR** si occupa di attuare le strategie di contenimento definite dall’IRM.

Il team deve essere pronto ad attivare un insieme di **strategie e procedure predefinite**, come riportato nei **playbook di gestione degli incidenti** inclusi in appendice.

## 8.1.1. Strategie di Contenimento

L’identificazione anticipata delle tecniche di contenimento è fondamentale per **ridurre la portata e l’impatto** di un incidente. Un contenimento efficace consente al CSIRT di guadagnare tempo prezioso per il ripristino.

Utilizzare il **ciclo OODA** e una forte **consapevolezza situazionale** aiuta a scegliere una strategia adatta a ottenere risultati rapidi ed efficaci.

Le strategie di contenimento possono variare in base al tipo di incidente e devono tenere conto dei seguenti criteri:

* **Importanza e criticità dei sistemi colpiti** per le attività aziendali fondamentali
* **Natura e gravità** dell’incidente
* **Tempo e risorse** richieste per attuare il contenimento
* **Disponibilità dei servizi** (es. accesso a servizi di terze parti, continuità dei servizi interni)
* **Esigenze legate alla conservazione delle prove**
* **Durata della soluzione** (es. rimedio temporaneo vs. correzione definitiva)

Le tecniche chiave di contenimento possono includere:

* **Isolamento di sistemi, asset o reti compromesse** per bloccare la diffusione o il movimento laterale
* **Revoca degli accessi attivi**, ad esempio tramite reimpostazione delle credenziali di amministratori, utenti e account di servizio
* **Deviazione degli attaccanti in ambienti sandbox**, previo consulto con il team legale in merito ai livelli di rischio accettabili
* **Revisione delle policy di controllo accessi e firewall** per chiudere le porte vulnerabili e ignorare in modo silente le fonti malevole
* **Applicazione di aggiornamenti e patch di sicurezza** per minimizzare l’esposizione alle vulnerabilità
* **Attivazione delle policy di isolamento XDR/EDR** su sistemi compromessi

## 8.2. Eradicazione e ripristino

Un approccio efficace alla fase di eradicazione e ripristino deve:

* **Eliminare ogni traccia della compromissione**
* **Rimuovere completamente la presenza dell’aggressore**
* **Prevenire il ripetersi dell’incidente**

L’**Incident Response Manager** è responsabile della **conferma della risoluzione dell’incidente**. Il **team IR** ha il compito di assicurarsi che tutte le attività individuate dall’IRM siano assegnate, eseguite e completate.

**Attività comuni** di eradicazione e ripristino includono:

* **Ripristino degli asset** da backup verificati come “puliti”
* Implementazione di **modifiche di configurazione o di codice** nelle applicazioni impattate
* **Sostituzione, reimaging o disattivazione** di sistemi compromessi o istanze cloud
* **Rimozione di funzionalità compromesse o vulnerabili**
* **Eliminazione di ogni artefatto malware** e sostituzione dei file infetti con versioni sicure
* **Disattivazione o eliminazione** degli account utente coinvolti
* Identificazione e **correzione di tutte le vulnerabilità sfruttate**
* **Notifica alle parti interne e/o esterne** di eventuali modifiche importanti a livello di sicurezza
* **Rafforzamento del logging** per rilevare la ricomparsa di TTP (tattiche, tecniche e procedure) o IoC (indicatori di compromissione) già osservati

## 8.3. Uscita dalla Fase di Contenimento, Eradicazione e Ripristino

L’incidente deve **rimanere aperto** finché tutte le azioni descritte nel piano di risposta non sono state:

* Completate  
  **oppure**
* Formalmente assegnate a responsabili specifici, con approvazione da parte dell’Incident Response Manager

L’uscita da questa fase richiede **la conferma che i sistemi e le operazioni siano stati riportati ai parametri normali di base**. È essenziale garantire che non vi siano **ulteriori segni o residui** di attività malevola.

Usare la seguente **checklist** per assicurarsi che ogni passaggio sia stato completato con successo:

* **Scansioni approfondite**: usare strumenti antivirus e antimalware aggiornati per verificare che tutte le tracce della minaccia siano state eliminate
* **Verifica di patch e azioni correttive**: accertarsi che tutte le vulnerabilità individuate siano state corrette e che le configurazioni siano state aggiornate
* **Audit di sistema**: controllare l’integrità dei sistemi e dei file per verificarne la corrispondenza con baseline sicure
* **Test di funzionalità dei sistemi**: assicurarsi che tutti i sistemi, le applicazioni e i servizi siano operativi e funzionanti
* **Test di accettazione da parte degli utenti (UAT)**: coinvolgere gli utenti finali per validare il ritorno alla piena operatività
* **Revisione e approvazione finale**: i membri del team IR e gli stakeholder devono convalidare formalmente che le fasi di contenimento, eradicazione e ripristino siano concluse

# 9. Post-Incident Activity

Una volta che l’incidente è stato risolto, è essenziale **condurre una sessione di analisi post-incidente**.

Questa sessione deve coinvolgere:

* Il **team di risposta agli incidenti**
* Gli **stakeholder informati e coinvolti durante la gestione**

L’obiettivo principale di questa fase è quello di:

* Valutare le **lezioni apprese**
* Riesaminare la sequenza degli eventi
* Sviluppare un **piano d’azione** per migliorare le procedure e le strategie di risposta agli incidenti

Argomenti chiave da affrontare nella sessione post-incidente:

* Analisi della **timeline dell’incidente** e identificazione della **causa principale**
* Valutazione delle prestazioni del **team IR**, degli stakeholder dipartimentali e degli eventuali partner esterni coinvolti
* Verifica della **conformità al piano di risposta agli incidenti** e dell’efficacia delle procedure adottate
* Identificazione di **azioni o fattori che hanno ostacolato** l’indagine o rallentato le attività di ripristino
* Verifica della disponibilità e adeguatezza degli strumenti e delle risorse utilizzate
* Identificazione e approvazione di **misure correttive** da adottare per migliorare la postura e i processi di sicurezza aziendali

## 9.1. Analisi post incidente

L’**analisi della causa radice (Root Cause Analysis – RCA)** e la **revisione post-incidente (Post-Incident Review – PIR)** sono fasi fondamentali per:

* Identificare l’origine reale dell’incidente
* Evidenziare le aree da migliorare
* Implementare **misure correttive efficaci**

Il diagramma di seguito illustra il flusso di processo RCA/PIR.

Immagine che contiene testo, schermata, Carattere, diagramma

Il contenuto generato dall'IA potrebbe non essere corretto.

Le analisi RCA e PIR **devono essere sempre documentate**.

* Per gli incidenti classificati come **gravità 0, 1 e 2**, è **obbligatorio** redigere **documenti RCA e PIR separati**
* Per gli incidenti di **gravità 3**, è sufficiente **documentare RCA e PIR direttamente sulla pagina dell’incidente**

Quando necessario, il Manager IR (o un suo delegato) può redigere anche un **“Incident Summary Report”** su richiesta del team legale, **distinto da RCA e PIR**.

Questo report deve essere inviato al dipartimento legale, che si occuperà di distribuirlo a:

* Security Operations
* Senior Management Team (SMT)
* Altri stakeholder rilevanti

|  |
| --- |
| **Incident Summary Template** |
| Sommario |
|  |
| **Natura dell’incidente** e tipo di informazioni aziendali coinvolte |
|  |
| **Azioni intraprese** per contenere, eradicare e risolvere l’incidente |
|  |
| **Comunicazioni interne ed esterne** effettuate |
|  |
| **Costi e perdite sostenute** |
|  |
| **Azioni di follow-up consigliate** |
|  |

## 9.2. Revisione e aggiornamento del piano IR

I seguenti passaggi descrivono il processo di manutenzione del piano IR:

* Valutare l’efficacia del piano attuale sulla base dell’esperienza reale
* Raccogliere **raccomandazioni di miglioramento** e classificarle in base alla priorità (es. urgenti vs. da includere nella prossima revisione ciclica)
* Sottoporre le proposte di modifica a **revisione e approvazione da parte di**:
  + Senior Management Team (SMT)
  + Steering Committee
  + Incident Response Team

## 9.3. Tempistiche per l’implementazione

Le modifiche urgenti o critiche devono essere implementate **immediatamente**, con conseguente:

* Aggiornamento e redistribuzione del piano IR
* Notifica agli stakeholder delle business unit
* Revisione dei materiali formativi collegati

Le modifiche non urgenti verranno raccolte e attuate nel **successivo ciclo di aggiornamento programmato** del piano.

|  |  |  |  |
| --- | --- | --- | --- |
| **Priorità** | **Azione** | **Responsabile** | **Tempistiche\*** |
| Alta |  |  | Lungo Termine |
| Media |  |  | Medio Termine |
| Bassa |  |  | Breve Termine |

**\*Legenda delle tempistiche:**

* **Breve termine**: 3–6 mesi
* **Medio termine**: 6–9 mesi
* **Lungo termine**: 9–12 mesi

# 10. Appendice

## 10.1. Incident Response Templates

I seguenti **modelli documentali** possono essere utilizzati da HiSolution per gestire in modo efficace eventuali incidenti futuri. Servono a:

* Tenere traccia cronologica degli eventi
* Garantire che vengano poste le giuste domande durante le fasi di RCA (Root Cause Analysis) e PIR (Post-Incident Review)
* Fornire una struttura standard a supporto delle attività IR

## 10.1.1. Incident Response Timeline Template

Le **timeline** che descrivono eventi e azioni durante tutto il ciclo di vita dell’incidente sono essenziali per redigere documenti accurati di **Root Cause Analysis (RCA)** e **Post Incident Review (PIR)**.

Usare la seguente tabella per registrare eventi significativi, ad esempio:

* Attività malevole rilevata
* Azioni difensive (es. creazione nuova regola firewall, isolamento di un sistema, blocco di un indirizzo IP)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Tipo di Evento | Data e Ora dell’Evento | Data/Ora della scoperta | Descrizione dell’Evento | IoC identificati | Commenti | Registrato da |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |
| --- |
| **Nota per la compilazione corretta della timeline**:   * Usare il formato UTC (GMT) per tutte le date e orari (es. BST = GMT+1) * Utilizzare l’orologio a 24 ore * Formato richiesto: DD:MM:YY - HH:MM:SS * Se l’orario esatto non è noto, indicare l’orario più vicino con fiducia e fornire un commento (es: “circa le 15:00 del 2 agosto” = 02/08/2015 15:00) |

## 10.1.2. Template per la Root Cause Analisi

|  |
| --- |
| **Root Cause Analysis (RCA) Template** |
| **Quando è stato rilevato per la prima volta il problema e da chi?** |
|  |
| **Qual era l’ambito dell’incidente?** |
|  |
| **Qual è stata la causa principale dell’incidente?** |
|  |
| **Quali sono stati altri fattori che hanno contribuito all’incidente?** |
|  |

## 10.1.3. Template di Revisione Post-Incidente

|  |
| --- |
| **Post Incident Review (PIR) Template** |
| **Come è stato contenuto ed eradicato l’incidente?** |
|  |
| **Cosa possiamo fare per prevenire futuri incidenti?** |
|  |
| **Cosa è stato fatto bene?** |
|  |
| **Cosa avremmo potuto fare meglio?** |
|  |
| **Gli strumenti IR sono stati efficaci?** |
|  |

## 10.1.4. Finalizzazione delle Azioni emerse dalla Revisione Post-Incidente

* Le azioni PIR derivano dalla sezione “Cosa possiamo fare per prevenire futuri incidenti?”
* Le azioni possono essere **accettate, rifiutate o modificate** dal team operativo
* Solo le azioni **accettate o approvate** devono essere inserite nella tabella finale
* È essenziale identificare un **responsabile per ogni azione**
* Le azioni approvate devono essere **comunicate a tutti i partecipanti alla riunione PIR**

## 10.2. Addendum al Processo di RCA

L’obiettivo dell’RCA è quello di:

* Identificare il **problema o vulnerabilità specifica** che ha causato l’incidente
* Determinare le **azioni necessarie per prevenire recidive**

Le cause possono includere:

* **Cause dirette** (singole o multiple)
* **Fattori contributivi** che hanno favorito il verificarsi del problema

L’RCA cerca di rispondere alle seguenti **5 domande fondamentali**:

1. Quando è stato rilevato per la prima volta il problema e da chi?
2. Qual è stata la causa diretta dell’incidente?
3. Quali altri fattori hanno contribuito all’incidente?
4. Qual era l’ambito dell’incidente?
5. Quali attività ha svolto il team IR durante l’incidente?

## 10.2.1. Passaggi del Processo RCA

Di seguito è riportato un riepilogo dei sei passaggi che si svolgono durante il processo di analisi delle cause profonde.



## 10.3. Addendumm al Processo di Revisione Post-Incidente

Una Revisione Post-Incidente (Post Incident Review, PIR) si concentra sulle azioni di miglioramento che possono contribuire a migliorare la postura di sicurezza dell’organizzazione e prevenire il verificarsi di incidenti simili.

L’obiettivo del processo di revisione post-incidente è identificare azioni che possano valutare l’efficacia del processo di risposta all’incidente e identificare opportunità di miglioramento.

Una revisione post-incidente mira a rispondere alle seguenti cinque domande:

* La causa radice dell’incidente è stata confermata da tutti i team coinvolti senza disaccordi?
* In che modo l’incidente è stato contenuto ed eradicato?
* Cosa ha fatto bene il team di risposta all’incidente nel gestire l’evento?
* Cosa si sarebbe potuto fare meglio per affrontare, prevenire o mitigare l’incidente?
* Cosa può fare HiSolution per migliorare e prevenire il verificarsi di incidenti simili in futuro?

## 10.3.1. Fasi del Processo di Revisione Post-Incidente

Di seguito è riportato un riepilogo delle cinque fasi che compongono il processo di revisione post-incidente:



## 10.4. Playbook

La creazione e l'utilizzo dei playbook è essenziale per una strategia di risposta agli incidenti efficace, in quanto forniscono passaggi strutturati e ripetibili che possono essere adattati a specifici tipi di incidenti.

Un playbook ben progettato include procedure standardizzate che garantiscono coerenza, riducono gli errori e colmano le potenziali lacune nella gestione degli incidenti. Questo approccio consente agli operatori di risposta di agire rapidamente, riducendo la necessità di decisioni in tempo reale, e rafforza la resilienza dell’organizzazione, riducendo il rischio di violazioni riuscite da parte di attori malevoli

10.1.1. C2/APT (Command and Control / Advanced Persistent Threat)  
  
Il playbook C2/APT è progettato per fornire un approccio metodico all’individuazione e all’analisi del comportamento Command and Control (C2) o Advanced Persistent Threat (APT) all'interno della rete.

L'obiettivo principale è identificare i sistemi compromessi, isolarli e raccogliere informazioni sugli Indicatori di Compromissione (IoC) relativi a C2/APT. Queste informazioni saranno poi utilizzate per identificare ulteriori asset compromessi e bloccare tutti gli IoC noti, al fine di prevenire ulteriori minacce.

Il passaggio finale nel playbook consiste nell'identificare il vettore di attacco utilizzato per accedere al sistema.

|  |  |
| --- | --- |
| **Fase** | **Strategia** |
| Rilevamento e Analisi | * Verificare se la minaccia è stata rilevata dal software di sicurezza endpoint * Eseguire un’analisi forense approfondita sui sistemi compromessi per identificare attività o artefatti sospetti * Raccogliere riferimenti a file, indirizzi IP e qualunque indicatore collegato al C2/APT * Inviare file sospetti a servizi di threat intelligence o analisi malware esterni (es. VirusTotal, Hybrid Analysis) * Utilizzare soluzioni XDR per cercare la presenza degli stessi file su altri endpoint o sistemi * Effettuare controlli di reputazione URL tramite fonti di threat intelligence * Determinare se l’URL è associato ad attività malevola e verificare eventuali dati storici sul dominio * Escalare il livello di gravità dell’incidente nel caso in cui il file venga trovato su più sistemi, indicando una compromissione estesa |
| Contenimento, Eradicazione e Ripristino | * Implementare policy di blocco IP a livello di rete per impedire ulteriori comunicazioni malevole * Eseguire azioni di bonifica quali patching delle vulnerabilità, aggiornamenti di configurazione, rimozione dei file dannosi * Disabilitare l’account utente associato al dispositivo compromesso * Isolare il dispositivo dalla rete per impedire movimenti laterali o ulteriore esfiltrazione * Continuare a monitorare l’ambiente per eventuali allarmi ritardati o attività correlate alla minaccia identificata * Condurre indagini mirate su asset correlati agli IoC alla ricerca di artefatti o tracce di attività malevola, come modifiche a file, account non autorizzati o modifiche al registro di sistema |
| Analisi post-incidente | * Condurre una revisione finale per documentare i risultati, identificare le cause radice, migliorare i meccanismi di rilevamento e aggiornare le procedure di risposta * Documentare tutte le azioni eseguite, le lezioni apprese e i miglioramenti raccomandati per rafforzare la difesa contro futuri incidenti * Condividere gli IoC con partner del settore, piattaforme di threat intelligence e forze dell’ordine |

Immagine che contiene schermata, diagramma, Rettangolo, linea

Il contenuto generato dall'IA potrebbe non essere corretto.

10.1.2. Endpoint Compromesso  
  
Questo playbook descrive i passaggi per indagare e prevenire movimenti laterali a partire da un endpoint compromesso.

L’obiettivo principale è impedire agli attori malevoli di sfruttare l’accesso per esfiltrare dati o muoversi attraverso la rete aziendale, con conseguenti furti di dati, perdite economiche o danni reputazionali.

|  |  |
| --- | --- |
| **Fase** | **Strategia** |
| Rilevamento e Analisi | * Analizzare i log dei sistemi di rilevamento (es. EDR/XDR, log di rete) per ottenere informazioni sulla compromissione * Utilizzare strumenti forensi per analizzare l’endpoint compromesso alla ricerca di artefatti, malware o altri IoC * Verificare se l’endpoint tenta di stabilire connessioni di beaconing (cioè comunicazioni periodiche verso un server C2) * Controllare la presenza di movimenti laterali verso altri host nella rete * Determinare quali account utente sono stati utilizzati sul sistema compromesso * Eseguire file sospetti in ambienti sandbox per osservarne il comportamento e raccogliere ulteriori IoC * Documentare nuovi IoC (indirizzi IP, hash di file, domini) individuati durante l’indagine * Confrontare gli IoC raccolti con fonti di threat intelligence per ottenere contesto aggiuntivo sulla minaccia * Registrare l’incidente e gli IoC nel SIEM per il monitoraggio continuo e la generazione di alert |
| Contenimento, Eradicazione e Ripristino | * Utilizzare gli IoC raccolti per contenere la minaccia nella rete (es. blocco IP, isolamento di macchine, aggiornamento regole firewall) * Rimuovere i file malevoli, correggere le vulnerabilità e applicare misure correttive per eliminare la minaccia * Disabilitare eventuali account associati alla compromissione per evitare accessi non autorizzati * Se necessario, sequestrare fisicamente o logicamente l’asset compromesso per analisi forense più approfondita * Disconnettere completamente il sistema compromesso dalla rete per evitare ulteriori danni o esfiltrazione * Verificare l’efficacia delle attività di contenimento attraverso un monitoraggio attivo |
| Analisi Post-Incidente | * Condurre una revisione finale per documentare i risultati, identificare le cause, migliorare la capacità di rilevamento e aggiornare i playbook * Documentare tutte le azioni intraprese, le lezioni apprese e i miglioramenti suggeriti * Condividere gli IoC con il settore, le piattaforme di intelligence e le autorità competenti |

Immagine che contiene schermata, diagramma, linea, Rettangolo

Il contenuto generato dall'IA potrebbe non essere corretto.

10.1.3. Server Compromesso  
  
Questo playbook per server compromessi delinea le procedure per investigare e fermare i movimenti laterali originati da un server compromesso.

L'obiettivo è prevenire che attori malevoli sfruttino l’accesso per esfiltrare dati o muoversi lateralmente nella rete aziendale, evitando così potenziali furti di dati, perdite finanziarie o danni reputazionali.

|  |  |
| --- | --- |
| **Fase** | **Strategia** |
| Rilevamento e Analisi | * Esaminare i log provenienti da vari sistemi di rilevamento della sicurezza per raccogliere prove iniziali e determinare l’estensione dell’incidente * Identificare vulnerabilità presenti sul server, come software non aggiornato, porte aperte o configurazioni deboli * Aggiornare i software di sicurezza (es. antivirus, regole firewall, firme IDS/IPS) all’ultima versione per migliorare la protezione * Raccogliere dump di memoria, log di sistema e altri dati rilevanti per supportare l’analisi forense e fornire prove della compromissione * Utilizzare gli IoC rilevati sul server per effettuare scansioni alla ricerca di altri host compromessi nella rete * Eseguire file sospetti in un ambiente sandbox per analizzarne il comportamento e raccogliere ulteriori IoC * Identificare eventuali account compromessi in uso sui server e convalidarne l’attività |
| Contenimento, Eradicazione e Ripristino | * Disconnettere il server compromesso dalla rete per prevenire ulteriori movimenti o esfiltrazioni * Bloccare a livello firewall tutti gli indirizzi IP malevoli associati alla compromissione per evitare comunicazioni esterne * Inviare file malevoli o artefatti sospetti a un team di ricerca o a servizi di analisi esterni per approfondimenti * Configurare il sistema SIEM per monitorare specifici IoC e generare alert se rilevati in futuro * Applicare gli IoC raccolti in tutta l’infrastruttura per contenere l’incidente (blocco IP, isolamento dispositivi, aggiornamento policy) * Confermare che le misure di contenimento abbiano isolato efficacemente la minaccia e che non ci siano ulteriori compromissioni * Rimuovere tutti gli elementi malevoli, pulire i file infetti, correggere le vulnerabilità e ripristinare i sistemi colpiti in uno stato sicuro * Assicurarsi che siano disponibili backup recenti e non compromessi per i server coinvolti, in caso sia necessario il ripristino |
| Analisi Post-Incidente | * Condurre una revisione finale per documentare risultati, identificare cause, migliorare il rilevamento e aggiornare le procedure * Documentare tutte le azioni intraprese, le lezioni apprese e i miglioramenti raccomandati * Condividere gli IoC con partner del settore, piattaforme di threat intelligence e forze dell’ordine |

Immagine che contiene testo, schermata, diagramma, Blu elettrico

Il contenuto generato dall'IA potrebbe non essere corretto.

10.1.4. Phishing  
  
Questo playbook per il phishing delinea le procedure per indagare e rispondere agli attacchi di phishing segnalati dagli utenti o identificati tramite eventi significativi nel nostro sistema SIEM.

L’obiettivo è prevenire che attori malevoli sfruttino tecniche di ingegneria sociale per infiltrarsi nei sistemi aziendali, evitando così violazioni di dati, perdite economiche e danni reputazionali.

Il seguente processo mira a ridurre il successo delle campagne di phishing attraverso l’utilizzo di IoC e threat intelligence per **bloccare le email prima della consegna**, rendendo l’attacco economicamente inefficiente per gli attaccanti e costringendoli a cercare bersagli più semplici.

|  |  |
| --- | --- |
| **Fase** | **Strategia** |
| Rilevamento e Analisi | * Confermare la ricezione di un’email di phishing e avviare l’indagine tramite il SIEM o analizzando log/eventi * Verificare se l’email di phishing è stata inviata ad altri utenti nell’organizzazione * Eseguire gli allegati o i link sospetti in un ambiente sandbox per osservare il comportamento * Controllare l’ambiente aziendale alla ricerca di IoC emersi dall’analisi sandbox |
| Contenimento, Eradicazione e Ripristino | * Disconnettere la macchina dalla rete e disabilitare l’account utente * Utilizzare blacklist di URL o domini per bloccare i link dannosi a livello aziendale * Impiegare tecniche di DNS blackholing per bloccare i domini o IP associati all’attacco di phishing * Isolare la macchina compromessa per evitare ulteriore diffusione * Individuare altri dispositivi potenzialmente colpiti dalla campagna di phishing * Informare gli utenti circa l’attacco e le eventuali misure di precauzione da adottare * Passare al playbook “endpoint compromesso” se viene rilevata compromissione |
| Analisi Post-Incidente | * Condurre una revisione finale per documentare l’accaduto, identificare le cause e aggiornare le procedure * Documentare tutte le azioni, le lezioni apprese e le misure di miglioramento * Condividere gli IoC con partner di settore, intelligence e autorità |

10.1.5 Minaccia Interna  
  
Questo playbook sulle minacce interne delinea come indagare su potenziali comportamenti scorretti dei dipendenti, intenzionali o meno, che potrebbero causare furto di dati, perdite finanziarie o danni alla reputazione. L'obiettivo è quello di ricostruire e comprendere il contesto delle azioni di un utente per valutare se rappresentano una minaccia, con l'accuratezza che è fondamentale per evitare gli alti costi della disinformazione.

|  |  |
| --- | --- |
| **Phase** | **Strategy** |
| Rilevamento e Analisi | * Confermare l’attività sospetta tramite alert del SIEM * Identificare gli account utente coinvolti e aggiungerli a un elenco di monitoraggio per ulteriori analisi * Determinare i dispositivi associati all’utente * Analizzare la cronologia di accesso e cercare pattern insoliti o tentativi falliti * Indagare su eventuali trasferimenti non autorizzati di dati da parte dell’utente o dell’account * Determinare se è coinvolto malware e verificare l’eventuale presenza di malware sconosciuto tramite IoC |
| Contenimento, Eradicazione e Ripristino | * Disabilitare temporaneamente l’account dell’utente coinvolto * Mettere in sicurezza il/i dispositivo/i associati all’utente * Creare un’immagine forense completa dei dischi dei dispositivi sequestrati * Continuare a monitorare l’utente e rispondere a nuovi alert o comportamenti sospetti * Applicare misure di contenimento basate sugli IoC identificati * Confermare che gli sforzi di contenimento siano stati efficaci e che la minaccia sia stata neutralizzata |
| Analisi Post-Incidente | * Condurre una revisione dettagliata per comprendere la causa dell’incidente e prevenirne altri in futuro * Documentare tutte le azioni eseguite, le lezioni apprese e i miglioramenti raccomandati * Condividere gli IoC con i partner del settore, le piattaforme di threat intelligence e le autorità competenti |

Immagine che contiene schermata, testo, diagramma, linea

Il contenuto generato dall'IA potrebbe non essere corretto.

Immagine che contiene cerchio, Elementi grafici, Carattere, logo

Il contenuto generato dall'IA potrebbe non essere corretto. **Incident**

**Response**

**Plan (IRP)**