Framework per l'Incident Response ISO/IEC 27035

VINCENZO CALABRÒ

Indice

Standard Incident Response ISO/IEC 27035

- Definizioni
- Obiettivi
- Fasi
- Conclusioni

Finalità

- **Rappresenta la capacità operativa di identificare, preparare e rispondere agli incidenti di sicurezza**
- **Il GDPR e la Direttiva NIS impongono l'adozione di un sistema di gestione degli incidenti di sicurezza (Incident Management)**

Standard Incident Response: ISO/IEC 27035

- È uno standard internazionale che **illustra i concetti e le fasi per la gestione degli incidenti** di sicurezza informatica.
- **Il modello si basa su un approccio strutturato** volto a rilevare, documentare, valutare e rispondere agli incidenti, ed applicare le lezioni apprese.

Approfondimenti

1. Cenni storici
2. Altri standard
3. Terminologia

ISO/IEC 27035: parti

La versione attuale è suddivisa in tre parti:

- **ISO/IEC 27035-1:2016 Part 1:**
  «*Principi per la gestione degli incidenti*»
- **ISO/IEC 27035-2:2016 Part 2:**
  «*Linee guida per pianificare e predisporre la risposta agli incidenti*»
- **ISO/IEC DIS 27035-3 Part 3:** *(in fase di sviluppo)*
  «*Linee guida per le operazioni di risposta agli incidenti nelle ICT*»

ISO/IEC 27035: obiettivi

- **Sviluppare controlli proattivi** per ridurre il numero di incidenti alla sicurezza
- **Definire e sviluppare i metodi di risposta e le strategie di mitigazione**
- **Identificare gli incidenti e le soluzioni** in modo efficace ed efficiente
- **Aggiornare le politiche ed i piani di sicurezza**, comprese le procedure di supporto, le tecniche ed i programmi di formazione, per prevenire il ripetersi di incidenti simili
- **Valutare i rischi aziendali e l'impatto degli incidenti** all'interno ed all'esterno dell'organizzazione (considerare gli stakeholders interni/esterni e gli utenti)
- **Ridurre gli impatti negativi causati dagli incidenti** (perdite economiche, furto dei dati, danni all'immagine o alla reputazione, interruzione dei servizi, ecc.)

ISO/IEC 27035: fasi

La gestione degli incidenti di sicurezza delle informazioni consta di cinque fasi e si sviluppa come un processo ciclico progettato per attuare un miglioramento continuo delle procedure interne.

Le Fasi:

1. Pianificazione e predisposizione
2. Rilevamento e segnalazione
3. Valutazione e decisione
4. Risposta
5. Apprendimento

Caveat

Fase 1: Pianificazione e predisposizione

La capacità di gestire con successo gli incidenti dipende dall'attenzione rivolta alla pianificazione e alla predisposizione.

Pertanto, occorre:

- Sviluppare una policy di gestione degli incidenti di sicurezza delle informazioni specifica per l'organizzazione.
- Istruire il personale dirigente sul loro ruolo durante un incidente ed assicurarsi che sia approvata la policy di gestione degli incidenti.
- Identificare e formalizzare il Team di risposta agli incidenti.
- Creare i processi e le procedure di risposta agli incidenti, insieme ai manuali specifici per gli eventi e gli incidenti più comuni (cd. Playbooks).
- Stabilire i programmi di formazione da erogare al personale che illustrino in dettaglio come identificare e come segnalare un incidente di sicurezza delle informazioni.
- Eseguire l'addestramento ai membri del team sulla risposta agli incidenti.
- Testare le attività di cui sopra contro gli eventi / incidenti simulati e reali.
- Revisionare periodicamente le policy, i processi, le procedure e i programmi di formazione per garantire che siano adeguate alle minacce attuali ed emergenti.

Fase 1: Pianificazione e predisposizione

Passi da seguire:

I. Redigere, e tenere aggiornato, il piano di risposta agli incidenti basato sui seguenti elementi:

- Individuare cosa proteggere (identificazione degli asset)
- Identificare le possibili categorie di minacce e di incidenti
- Capire le possibili ricadute di un incidente sull'organizzazione
- Indirizzare la protezione infrastrutturale e degli end point
- Specificare chi ha la massima responsabile in caso di incidente
- Indicare la composizione e i ruoli del Team di risposta agli incidenti
- Decidere se rivolgersi a competenze esterne all'organizzazione
- Predisporre la comunicazione interna ed esterna in caso di incidente

II. Inserire i seguenti contenuti nel piano di risposta agli incidenti di sicurezza informatica:

- Obiettivi da proteggere: management, processi, organizzazione, persone, conoscenza, informazioni, applicazioni, capitale, infrastrutture
- Elenco delle vulnerabilità e delle minacce potenziali
- Documentazione tecnica per descrivere i sistemi informativi utilizzati, la configurazione di rete, gli account e i diritti di accesso

Fase 1: Pianificazione e predisposizione

Passi da seguire:

III. Creare un team di risposta agli incidenti informatici

- Assegnare le responsabilità ed i ruoli alle persone con gli skill adeguati
- Formalizzare l'Incident Response Team
- Proporzionare la grandezza del Team all'organizzazione di riferimento

IV. Scegliere quando e se rivolgersi ad esperti esterni

- Durante la fase di preparazione
- Quando si verifica un incidente

V. Dotare l'organizzazione degli strumenti per far fronte ad un incidente di sicurezza informatica

- La lista degli esperti da contattare in caso di incidente (Incidente Response Manager, Legale, Forense, ecc.)
- La dotazione hardware e software per la gestione degli incidenti informatici

VI. Preparare la strategia di comunicazione

- Cosa comunicare e a chi comunicarlo
- Identificare gli stakeholders interni ed esterni

VII. Stipulare una polizza assicurati per coprire i danni causati da determinati tipi di incidenti

Fase 2: Rilevamento e segnalazione

Il rilevamento e la segnalazione sono le prime fasi operative del processo di gestione degli incidenti di sicurezza.

Questa fase include anche la segnalazione iniziale dell'evento o dell'incidente agli stakeholder principali, alle agenzie governative e al personale preposto all'interno dell'organizzazione.

La rilevazione tempestiva aiuta a mitigare tempestivamente gli effetti di un incidente e riduce le possibilità di impatto sull'organizzazione. La Threat Intelligence, generata e condivisa tramite la segnalazione degli incidenti, può essere utilizzata da altri attori per mitigare minacce potenzialmente vulnerabili.

Durante questa fase deve essere garantito che le seguenti attività siano eseguite dal personale preposto:

- rilevazione dell'evento di sicurezza o dell'esistenza di una vulnerabilità di sicurezza delle informazioni
- cattura e registrazione delle informazioni relative all'evento di sicurezza
- raccolta e archiviazione sicura delle evidenze digitali
- escalation dell'incidente come richiesto per tutta la fase.

Fase 2: Rilevamento e segnalazione

Passi da seguire:

- **Classificare gli incidenti**
  - Definire l'incidente di cyber sicurezza e la terminologia correlata
  - Identificare le possibili categorie di incidenti di cyber sicurezza
- **Determinare i sistemi di rilevamento degli incidenti**
  - Il personale dell'organizzazione, gli utenti, l'help desk
  - I sistemi di protezioni inclusi nella tecnologia installata e negli endpoint
  - Gli strumenti di rilevamento (lato network e lato host)
- **Definire il modello per la segnalazione iniziale**
  - Identificare il Point of Contact (PoC) 24x7
  - Creare il form per la segnalazione di un evento di sicurezza

Fase 3: Valutazione e decisione

La valutazione e la decisione rappresentano la seconda fase operativa del processo di gestione degli incidenti.

Questa fase prevede la valutazione delle informazioni raccolte durante la fase di rilevazione e segnalazione e copre l'escalation di un incidente.

Devono essere assicurate le seguenti attività:

- Valutazione: determinare se l'evento è un incidente di sicurezza o un falso positivo
- Determinare il tipo di incidente, l'ambito e l'impatto sul business
- Stabilire i requisiti di segnalazione iniziale, sia internamente che esternamente, in aderenza agli standard di segnalazione degli incidenti di sicurezza
- Distribuire le notifiche iniziali sugli incidenti relativi alla sicurezza al personale interessato
- Identificare e assegnare le responsabilità di risposta agli incidenti all'interno dell'IRT
- Seguire le linee guida e le politiche di risposta agli incidenti specifiche dell'intera gestione
- Aggiornare il registro degli incidenti relativi alla sicurezza delle informazioni
- Continuare le attività di registrazione delle azioni e delle decisioni intraprese, oltre alla raccolta e alla conservazione sicura delle evidenze digitali

Fase 4: Risposta

La fase di risposta riguarda principalmente le azioni di contenimento, rimozione/eradicazione e ripristino intraprese dall'IRT.
Queste azioni dovrebbero essere documentate all'interno dei playbooks preesistenti.

Durante la fase di risposta dovrebbe essere eseguite le seguenti attività dal personale preposto:

- Rivalutare la gravità dell'incidente in corso
  - determinare la necessità di risorse e assistenza dall'esterno
  - se necessario, inoltrare l'incidente al team di gestione delle crisi (CSIRT di riferimento)
- Condurre le attività di risposta adeguate con l'intento di mitigare l'incidente
  - contenimento
  - rimozione
  - ripristino
- Comunicare l'incidente a: il vertice amministrativo, i dirigenti, gli enti governativi, gli stakeholders, ecc.
- Continuare le attività di registrazione delle azioni e delle decisioni intraprese, oltre alla raccolta e alla conservazione sicura delle evidenze digitali

Fase 4: Risposta

Passi:

I. Convocare l’Incident Response Team

- Il responsabile degli incidenti e il suo team riferiranno al Vertice, che dovrà convalidare le loro decisioni.

II. Creare la Situation Awareness

- Dopo il rilevamento di un incidente è fondamentale raccogliere tutte le informazioni disponibili sulle attività relative al periodo di tempo dell'incidente. Potrebbe essere necessaria un'indagine forense per raccogliere tutti gli artefatti ed esaminare l'entità dell'attacco.

III. Avviare la fase di contenimento

- Ripristinare velocemente la situazione iniziale oppure raccogliere altre evidenze?
  Contenere un incidente di sicurezza informatica consiste nel limitare il danno e fermare l'attaccante.
  Si deve trovare un modo per limitare il rischio dell’organizzazione e contemporaneamente mantenerlo attivo.
  È necessario impedire che l'incidente si diffonda ulteriormente sia all'interno che all’esterno dell'organizzazione.
- All'inizio di questa fase, l’organizzazione dovrà prendere un'importante decisione strategica: disconnettere immediatamente i sistemi per ripristinarli il più rapidamente possibile? O prendere altro tempo per raccogliere altre evidenze utili a scoprire i criminali informatici che hanno manomesso il sistema ed il loro modus operandi?

Fase 4: Risposta

Passi:

IV. Attuare l’Eradicazione e la Pulizia

- Dopo aver concluso l'indagine, può iniziare l'eradicazione.
  In questa fase è necessario rimuovere tutti i componenti correlati all'incidente, tutti gli artefatti lasciati dall'attaccante (codice malevolo, dati, ecc.), chiudere ogni falla o vulnerabilità utilizzata per compromettere il sistema.
- Non iniziare la pulizia prima di avere un quadro completo dell'incidente!
  Significa che la pulizia dovrebbe iniziare solo dopo aver determinato la causa dell’incidente.
  Inoltre, occorre controllare tutte le macchine che hanno la stessa vulnerabilità.
  Nel momento in cui si decide di sradicare l'incidente, occorre essere veloci, sincronizzati e accurati, per evitare che l'avversario possa correggere l’attacco.
- Il Top Management deve essere informato dei risultati dell'eradicazione, della bonifica e della nuova situazione post incidente.

Fase 4: Risposta

Fasi:

V. Avviare il Recupero

- Questa attività consente il ripristino dei sistemi per tornare a loro normale funzionamento e, se possibile, riparare la vulnerabilità per prevenire incidenti simili.
  Esistono diversi modi per ripristinare i sistemi dopo un incidente di sicurezza informatica.
- Tutti hanno un impatto diverso sui tempi di recupero, sui costi o sulla perdita di dati:
  - Pulire gli artefatti danneggiati e sostituire i file compromessi con versioni pulite
  - Ripristinare da un backup
  - Ricreare il sistema (i) o l'ambiente da zero

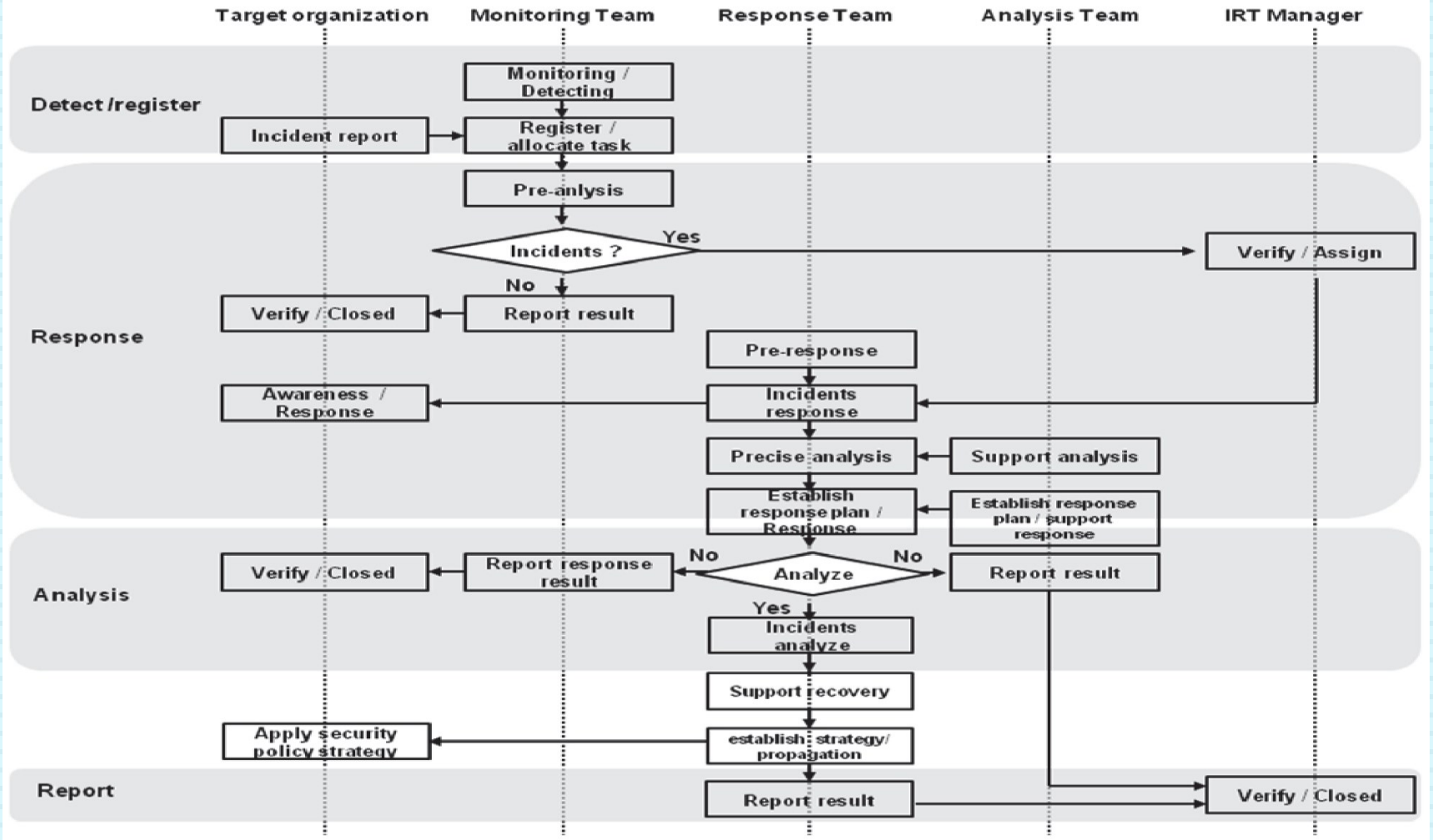
VI. Iniziare l'attività di comunicazione durante l'incidente

- Occorre aver individuato preventivamente:
  - L'elenco degli stakeholders (interni, esterni, agenzie governative)
  - Gli strumenti da utilizzare
  - Il piano di comunicazione
- Adempiere agli obblighi normativi:
  - Comunicare l'incidente al CSIRT Nazionale (ex CERT PA)
  - In caso di data breach di dati sensibili o personali comunicarlo al Garante della Privacy

Fase 5: Apprendimento

L'ultima fase del processo di risposta agli incidenti è avviata dopo che l'incidente è stato risolto.
Prevede la valutazione e l'analisi delle attività svolte durante il processo di risposta agli incidenti.
Lo scopo è quello di offrire l'opportunità per migliorare i processi di risposta ed i playbooks.
Durante la fase di apprendimento, un IRT dovrebbe assicurarsi che siano svolte le seguenti attività:

- Avviare la revisione post incidente (PIR)
  - identificare le lezioni apprese dall'incidente
  - identificare i miglioramenti che potrebbero essere apportati a: controlli, policies, processi e procedure
- Condividere i risultati con la comunità di riferimento
- Rivedere i costi associati alle attività di risposta agli incidenti e alle misure correttive
- Archiviare i registri completi delle attività svolte in conformità con la politica di gestione dei registri



Incident response processes – Fonte ISO/IEC 27035

Conclusioni

- L’incidente informatico è inevitabile
- Prima si rileva, prima si interrompe l’effetto
- I costi dell’IR sono inferiori ai danni causati dagli incidenti informatici
- Gli incidenti devono essere resi noti (anche solo ai propri stakeholders) perché:
  - È meglio gestire la comunicazione che subirla
  - La condivisione delle informazioni, come IoC (Indicatore di Compromissione) o IoA (Indicatore di Attacco) aiutano a migliorare la Detection e la Response
- Documentare tutte le attività agevola il processo di improvement

Approfondimento 1: Cenni storici

- Il 12-10-2004 l'International Organization for Standardization (ISO) pubblica il rapporto tecnico ISO/IEC TR 18044: 2004 con l'obiettivo di presentare una guida alla gestione degli incidenti di sicurezza delle informazioni per gli amministratori dei sistemi e della sicurezza, per gli amministratori dei sistemi di informazione e gli amministratori della sicurezza di qualsiasi organizzazione. La gestione degli incidenti è composta da 4 processi:
  - Pianificazione e predisposizione: è necessario effettuare un'adeguata pianificazione per la risposta a tali incidenti.
  - Attuazione: è il processo di implementazione del piano di gestione degli incidenti di sicurezza. I risultati dell'indagine sugli incidenti vengono rilevati, comunicati, analizzati e classificati.
  - Revisione: l'incidente viene nuovamente convalidato, se necessario, vengono definite le lezioni apprese e sono implementati i processi di miglioramento sulla base delle vulnerabilità rilevate.
  - Miglioramento: il processo di gestione degli incidenti è un processo iterativo, ciò significa che migliora costantemente, sia nelle regole che nella attuazione.
- Nel 2011 l'ISO cambia la natura del documento, da rapporto tecnico a norma internazionale della famiglia di standard ISO 27000. Questo standard è denominato ISO/IEC 27035:2011 Gestione degli incidenti di sicurezza delle informazioni e definisce un approccio strutturato e pianificato per:
  - Rilevare, segnalare e valutare gli incidenti di sicurezza delle informazioni.
  - Rispondere agli incidenti e gestire gli incidenti di sicurezza delle informazioni.
  - Rilevare, valutare e gestire le vulnerabilità di sicurezza delle informazioni.
  - Migliorare di continuo la sicurezza delle informazioni e la gestione degli incidenti.

Approfondimento 2: Altri standard

- RFC 2350 Expectations for Computer Security Incident Response, June 1998
  Author(s): N. Brownlee, E. Guttman
  https://tools.ietf.org/pdf/rfc2350.pdf
- NIST SP.800-61 Rev. 2 Computer Security Incident Handling Guide, August 2012
  Author(s): Paul Cichonski (NIST), Thomas Millar (DHS), Tim Grance (NIST), Karen Scarfone (Scarfone Cybersecurity)
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- CREST Cyber Security Incident Response Guide Ver. 1, August 2013
  Author(s): Jason Creasey, Ian Glover
  https://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide-1.pdf

Approfondimento 3: Terminologia

- **Information security investigation**: Analisi ed interpretazione per aiutare a comprendere l'incidente informatico.
- **Incident response team (IRT):** Team, con competenze per la gestione degli incidenti informatici, che interviene nel caso in cui viene rilevato un incidente informatico. Anche denominato : Computer Emergency Response Team (Cert) o Computer Security Incident Response Team (CSIRT).
- **Information security event:** Evento che può indicare una possibile violazione.
- **Information security incident:** Uno o più information security event che possono arrecare danni agli asset di un'organizzazione.
- **Information security incident management:** Organizzazione della gestione dell'incidente informatico.
- **Incident handling:** Gestione vera e proprio dell'incidente che si sviluppa attraverso le azioni di individuazione, documentazione, risposta e apprendimento dell'incidente informatico.
- **Incident response:** Azione intrapresa per ridurre o risolvere l'incidente informatico, incluso tutto ciò che riguarda la protezione e il ripristino delle normali condizioni dei sistemi informatici e dei dati salvati in essi.
- **Point of contact (POC):** Persona o dipartimento preposta al coordinamento delle attività per la gestione dell'incidente informatico.

Approfondimento Fase 1: Pianificazione e predisposizione

Approfondimento

- Policy
- Incident Response Team (IRT)
- Processi e Procedure
- Training
- Testing

Approfondimento 4: Policy

Ogni organizzazione deve considerare i seguenti elementi, da includere nella policy di gestione degli incidenti in materia di sicurezza delle informazioni, per soddisfare i requisiti generali del sistema di gestione della sicurezza delle informazioni:

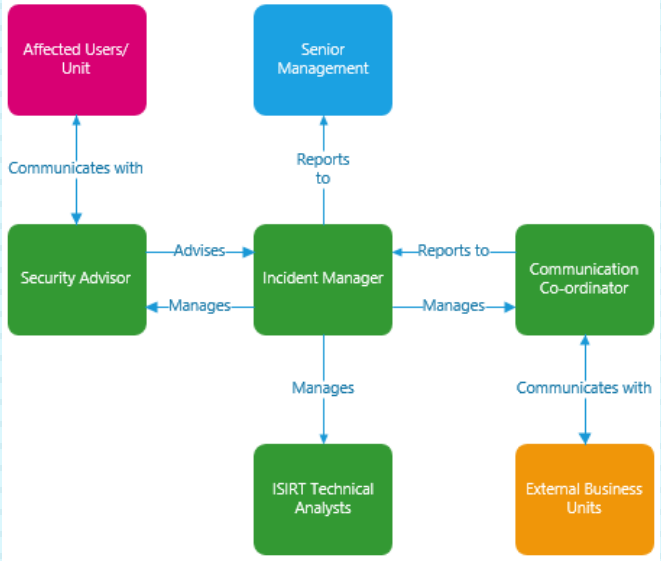
- Un quadro che evidenzi il valore dei processi di gestione degli incidenti: l'impegno dell'alta dirigenza nei confronti della policy e collegamenti chiari tra la risposta agli incidenti con le attività di gestione del rischio.
- Un resoconto delle funzionalità di rilevamento degli eventi e di come utilizzare queste informazioni per determinare gli incidenti relativi alla sicurezza delle informazioni.
- Un elenco dei requisiti di segnalazione per gli stakeholder interni e gli stakeholder esterni.
- Una panoramica degli eventi relativi alla sicurezza delle informazioni e alle valutazioni di escalation degli incidenti.
- Un riepilogo delle attività che seguono la conferma che un evento di sicurezza è un incidente di sicurezza delle informazioni.
- Un riferimento alla necessità di registrare e documentare tutte le attività del processo di risposta agli incidenti, per garantire la raccolta e la conservazione delle evidenze utilizzabili per eventuali analisi o approfondimenti.
- Un riepilogo delle attività poste in essere durante la fase di apprendimento degli insegnamenti del processo di risposta agli incidenti.
- I dettagli su dove sono conservate le procedure di risposta agli incidenti ed i relativi playbooks.
- Uno schema della struttura del team di risposta agli incidenti (IRT) pertinente al contesto dell'organizzazione.
- Una sintesi del programma di training sulla gestione degli incidenti e sulla sensibilizzazione alla consapevolezza degli incidenti.
- Un elenco degli strumenti tecnici e degli altri dispositivi di supporto disponibili.
- Una sintesi degli aspetti legali e regolamentari che dovrebbero essere affrontati o tenuti in considerazione.

Approfondimento 5: Incident Response Team (IRT)

L'istituzione del team di risposta agli incidenti in materia di sicurezza delle informazioni (IRT) è una parte fondamentale della gestione degli incidenti in materia di sicurezza delle informazioni.

Un IRT dovrebbe essere costituito da:

- Responsabile della sicurezza delle informazioni
- Amministratori di rete
- Responsabili / Operatori IT
- Analisti della Sicurezza
- Responsabile Finanziario
- Responsabile Risorse Umane
- Responsabile Affari Legali
- Responsabile della Comunicazione
- Responsabile delle Relazioni Esterne



Approfondimento 6: Processi e Procedure

I processi e le procedure di gestione degli eventi e degli incidenti devono essere sviluppati per supportare le relative policy.

Processi - Ogni organizzazione deve:

- Sviluppare processi interni riguardanti le attività di risposta alla sicurezza delle informazioni. Questi processi possono essere sviluppati modellando i ruoli, le responsabilità e le attività specifiche già definite nella loro politica di gestione degli incidenti.
- Sviluppare o ottenere una serie di manuali di risposta agli incidenti generalizzati e specifici per gestire una varietà di tipi di incidenti (cd. Playbooks).

Procedure - Per supportare i processi definiti, le procedure devono:

- Includere eventuali moduli e strumenti di supporto utilizzati da dipendenti e team di risposta per rilevare, segnalare, documentare, valutare, rispondere o recuperare gli incidenti.
- Includere l'IRT e le procedure operative riguardanti la comunicazione interna ed esterna, come ad esempio:
  - Le informazioni sulla gestione operativa degli incidenti.
  - Il coinvolgimento del team di comunicazione interna per le dichiarazioni ai media o le comunicazioni pubbliche.
  - L'informazione degli stakeholders esterni attraverso la condivisione delle informazioni sulle minacce con i partner.

Approfondimento 7: Training

La formazione dovrebbe essere erogata per massimizzare la consapevolezza, la competenza e l'efficienza della gestione degli incidenti di sicurezza delle informazioni.

Tutti i dipendenti devono essere consapevoli dei rispettivi ruoli e delle responsabilità in merito alla gestione, alla documentazione e alla segnalazione degli incidenti.

I programmi di formazione dovrebbero includere:

- La formazione iniziale per tutto il personale, compresi i concetti base di sicurezza
- La formazione sulla risposta agli incidenti per il Team
- La formazione forense sulle ITC
- La formazione specifica per alcune tematica (p.e. il phishing, la gestione delle password, i ransomware, ecc.)
- Gli adempimenti normativi in tema di incidente informatico e di violazione dei dati personali.

Approfondimento 8: Testing

Prima di implementare l'IRT, dovrebbe aver luogo un test approfondito dei processi e delle procedure.

Ciò consentirebbe il miglioramento del sistema di gestione prima che si verifichi un evento o un incidente di sicurezza.

Pertanto si dovrebbero:

- Eseguire regolarmente dei test sui processi e sulle procedure di risposta agli incidenti attraverso:
  - La simulazione di diversi scenari in base ai quali l'IRT è attivato come se stesse rispondendo ad un incidente reale. In questi scenari i sistemi di produzione non vengono interrotti e il personale dovrebbe partecipare attraverso l'attività di comunicazione del processo decisionale di impatto aziendale.
  - Esercitazioni in cui il personale con ruoli o responsabilità nella risposta agli incidenti si riunisce ed elabora scenari cartacei per verificare se i controlli, i processi e le procedure stabilite sono efficaci nel rilevare e rispondere a potenziali incidenti.
- Formare tutto il personale alla consapevolezza generale della sicurezza e alle attività di risposta appropriate (ad esempio la notifica ai team di sicurezza, la registrazione degli eventi e il salvataggio delle prove).

Le simulazioni eseguite sui processi e/o sulle procedure dovrebbero essere realistiche e uniche tra loro per testare adeguatamente i vari scenari.

Approfondimento Fase 2: Rilevazione e segnalazione

Approfondimento

- Rilevamento
- Registrazione e acquisizione delle informazioni
- Segnalazione iniziale
- Cyber Kill Chain (Modulo 3.1.1)

Approfondimento 9: Rilevamento

Gli eventi di sicurezza possono essere rilevati da varie fonti ed è importante essere consapevoli di tutte le potenziali fonti di notifica di cui un'organizzazione dispone, ciò consente di colmare le lacune dei propri sistemi di rilevamento.

Le fonti standard di rilevamento degli eventi di sicurezza delle informazioni possono includere:

- Gli avvisi automatici prodotti dai sistemi di sicurezza e / o dal monitoraggio della rete
- La scansione delle vulnerabilità o dai penetration test
- L'analisi dei log di sistema
- L'escalation di un evento rilevato da un utente
- Le notifiche da terzi parti, tra cui:
  - Agenzie governative (CSIRT , ENISA)
  - Information Security Services
  - Telecommunication Providers
  - Threat Intelligence Partners.

Approfondimento 10: Registrazione e acquisizione

La registrazione degli eventi e degli incidenti relativi alla sicurezza delle informazioni è una delle attività più importanti del processo di risposta agli incidenti.

L'acquisizione accurata ed efficiente delle informazioni e delle evidenze relative ad un incidente è fondamentale per dimostrare la conformità e la giustificazione delle decisioni prese, documentare le azioni e sviluppare un'analisi post incidente.

Le organizzazione dovrebbero produrre e memorizzare in modo sicuro un registro dettagliato, comprendente la data e l'ora delle seguenti informazioni:

- Le decisioni che vengono prese e da quale autorità
- Le attività intraprese dall'IRT
- I dettagli sul rilevamento degli eventi di origine
- I risultati delle azioni e delle decisioni.

Deve essere eseguita una registrazione simultanea in tutte le fasi del processo di risposta agli incidenti.

Approfondimento 11: Segnalazione iniziale

La segnalazione iniziale è l'azione di informazione indirizzata ai soggetti individuati all'interno dell'organizzazione di un potenziale evento o incidente di sicurezza delle informazioni.

La segnalazione iniziale può provenire da una persona, una struttura oppure può essere veicolata attraverso un sistema di allertamento automatizzato.

Le organizzazione devono definire:

- Le procedure di segnalazione e i punti di contatto dell'IRT
- Le procedure su come e quando inoltrare la segnalazione ai dirigenti e agli stakeholder
- I formati o la modulistica delle segnalazione conformi a quelli indicati nella normativa vigente relative alla segnalazione degli incidenti relativi alla sicurezza delle informazioni

Approfondimento Fase 3: Valutazione e decisione

Approfondimento

- La **Valutazione** (cd. Incident Triage) di un evento di sicurezza informatica è l'attività fondamentale svolta inizialmente dal PoC, mentre durante il processo di risposta agli incidenti informatici è di competenza dell'IRT.
- La valutazione corretta di un evento fornisce una spiegazione facilmente comprensibile dell'incidente al personale meno tecnico (legali, media, ecc.).
- La valutazione fornirà informazioni utili anche agli altri dipartimenti in merito ai loro adempimenti obbligatori di reporting e potrà essere utilizzata per prendere altre decisioni specifiche (interruzione di attività, livelli di escalation, unità aziendali interessate, ecc.)

Fase 4: Risposta

Approfondimento

- Rivalutazione dell'incidente
- Attività di risposta
- Analisi forense
- OODA Loop

Approfondimento 12: Rivalutazione dell'incidente

L'attività di rivalutazione degli incidenti è eseguita durante tutta la fase di risposta agli incidenti, rappresenta il punto di decisione della fase di risposta e determina la scelta delle azioni eseguita dal IRT.

Durante l'esecuzione del processo di risposta si può scoprire che la valutazione iniziale e le decisioni intraprese sono errate e, pertanto, è utile rivalutare l'incidente e modificare, se necessario, le attività di risposta o declassare la gravità dell'incidente. La revisione potrebbe indicare, anche, se sono necessarie risorse esterne.

Anche lo stato di escalation deve essere analizzato durante l'attività di rivalutazione degli incidenti.

Quando è rilevata un escalation, questa deve essere gestita dal responsabile dell'incidente o dal coordinatore della comunicazione. Ciò garantisce che la comunicazione di un incidente provenga da e verso un'unica fonte. I criteri di assegnazione dell'escalation devono essere definiti e concordati all'interno dell'IRT o dell'agenzia governativa.

Se la revisione dell'incidente determina che non vi siano attività di risposta in corso e l'incidente è stato risolto, il responsabile dell'incidente dovrebbe spostare lo stato nella fase di apprendimento del processo di risposta agli incidenti.

Approfondimento 13: Attività di risposta

Le attività di risposta dovrebbero essere guidate principalmente dall'attività di revisione degli incidenti e dai playbooks predefiniti per le diverse categorie di incidenti.

L'IRT dovrebbe:

- Disporre di playbook per la maggior parte dei tipi di incidenti di sicurezza con l'indicazione delle attività da eseguire e i flussi di informazione da gestire:
  - Ogni IRT e le agenzie governative dovrebbero utilizzare uno standard di risposta agli incidenti riconosciuto come base per i loro playbook di risposta. Questi standard includono il Manuale del gestore SANS, la Guida alla gestione degli incidenti di sicurezza informatica del NIST, ISO 27035, ecc.
- Testare i propri processi di risposta interni e i playbooks per determinarne l'efficacia e migliorare i tempi di risposta.
- Eseguire periodicamente programmi di revisione dei processi interni di gestione.

Approfondimento 14: Analisi forense

Alcuni incidenti informatici possono richiedere lo svolgimento di una analisi forense.

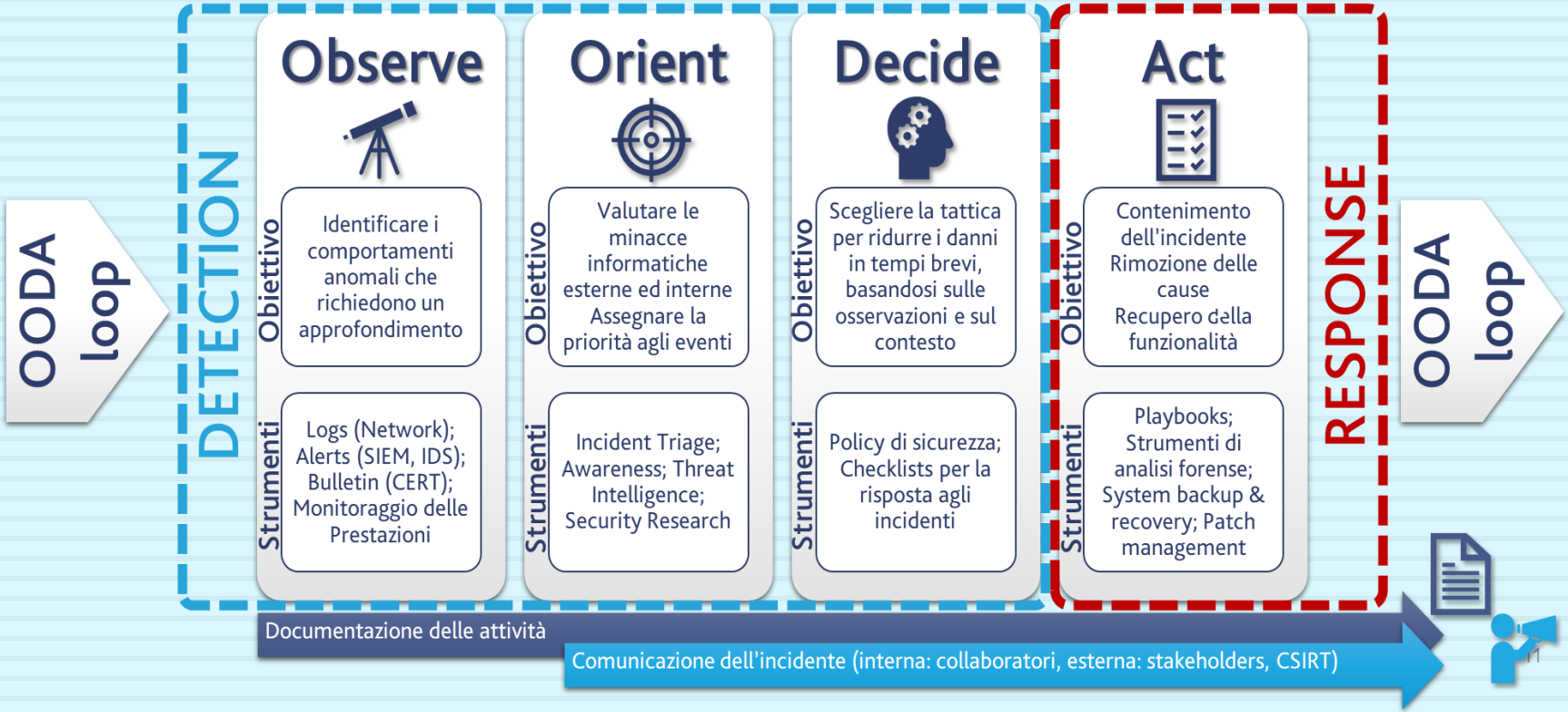
Questa attività può essere necessaria per vari motivi, tra cui, per esempio, stabilire l'attribuzione di un determinato reato, oppure raccogliere e memorizzare evidenze digitali.

Nella maggior parte dei casi è probabile che l'organizzazione non disponga degli strumenti o del personale adeguatamente addestrato per condurre l'analisi forensi.

In questi casi, l'IRT può rivolgersi:

- Ai CSIRT governativi
- Alla Polizia delle Comunicazioni
- Ai Consulenti Esterni

Approfondimento 15: OODA loop



Fase 5: Apprendimento

Approfondimento

- **Revisione post incidente**: La PIR dovrebbe essere un riepilogo di tutte le azioni e le decisioni prese durante il processo di risposta agli incidenti informatici.
  Il report dovrebbe essere strutturato per includere le lezioni apprese, le osservazioni e le raccomandazioni acquisite.
  Dovrebbe essere completato non appena possibile, dopo la chiusura dell'incidente, per garantire che le informazioni non vadano perse.
  Lo sviluppo del report dovrebbe essere un processo collaborativo, che includa il contributo di quante più parti interessate, questo assicura che il rapporto esprima più punti di vista e copra varie discipline.

Grazie!
Domande?

VINCENZOCALABRO.IT