Strategie di difesa: Incident Response e SOC

Indice

Introduzione

Motivazioni

- L'adozione di meccanismi di sicurezza non garantisce protezione assoluta

Obiettivi

- Incidenti informatici: ogni evento anomalo riguardante gli asset IT
- L'organizzazione deve sapere gestire gli incidenti informatici

Incident Management

Definizione

- Un complesso insieme di attività
- Scopo: processare gli incidenti informatici
- Vantaggi attesi:
  - mitigarne l'impatto e la probabilità di accadimento
  - adottare azioni di recupero.

Incident Management e Incident Response

Incident Management

- Include aspetti gestionali, logistici, procedurali, di comunicazione, di coordinamento

Incident Response

- Include tutte le componenti tecniche per il rilevamento e il contenimento degli incidenti

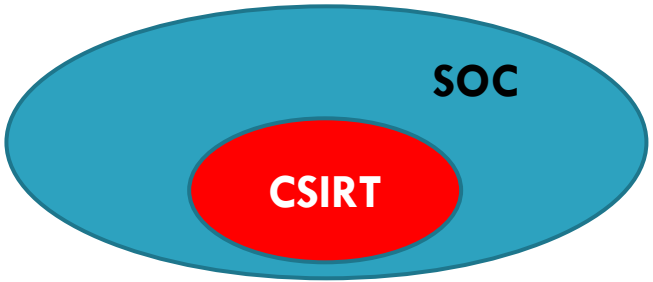
Incident Response: Attuazione

Livello minimo

- CSIRT: Computer Security Incident Response Team

Livello massimo

- SOC: Security Operation Center



Security Operation Center

Tipi

- Interno
- Esterno (outsourced) dedicato
- Esterno condiviso

Macrofunzioni di un SOC

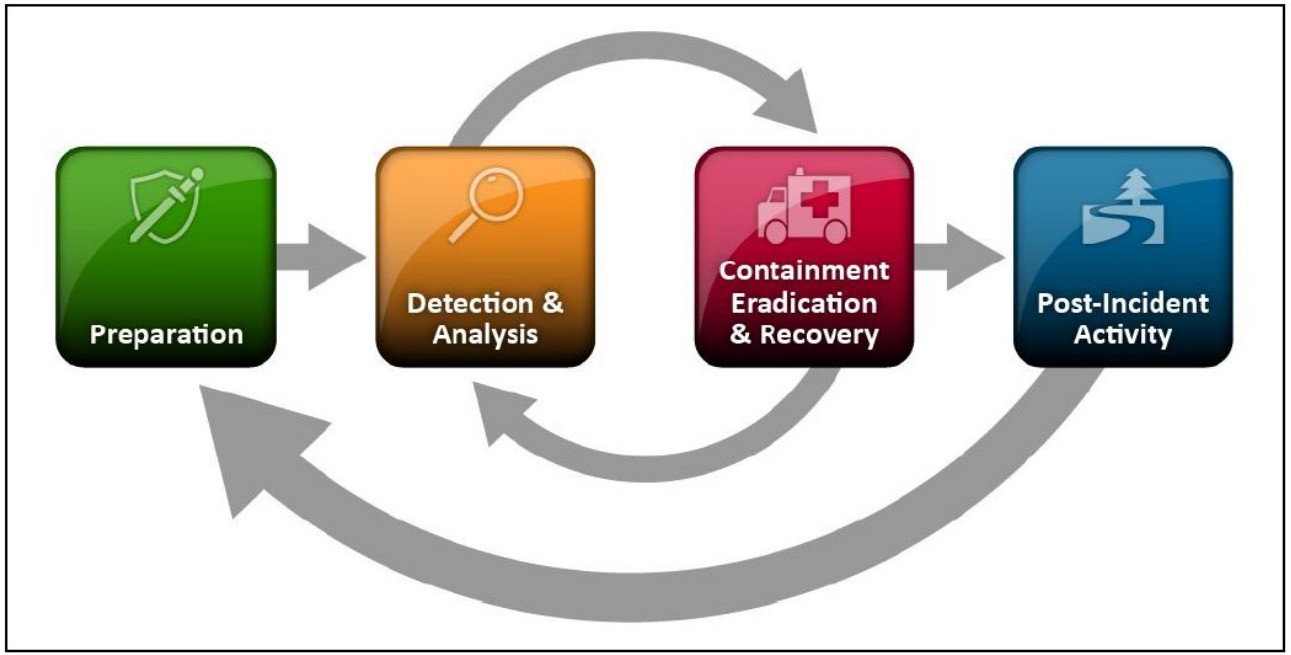
Funzioni di Base

- Governance della sicurezza
- Hardening
- VA e compliance
- Identity Management e Controllo dell'Accesso e PKI
- Servizi per la sicurezza perimetrale
- Gestione Antivirus
- Stretto coordinamento con NOC
- …

Funzioni avanzate

- Processi di gestione degli incidenti
- Red Team & Blue Team
- Attività di Forensics

Le fasi della gestione di un incidente

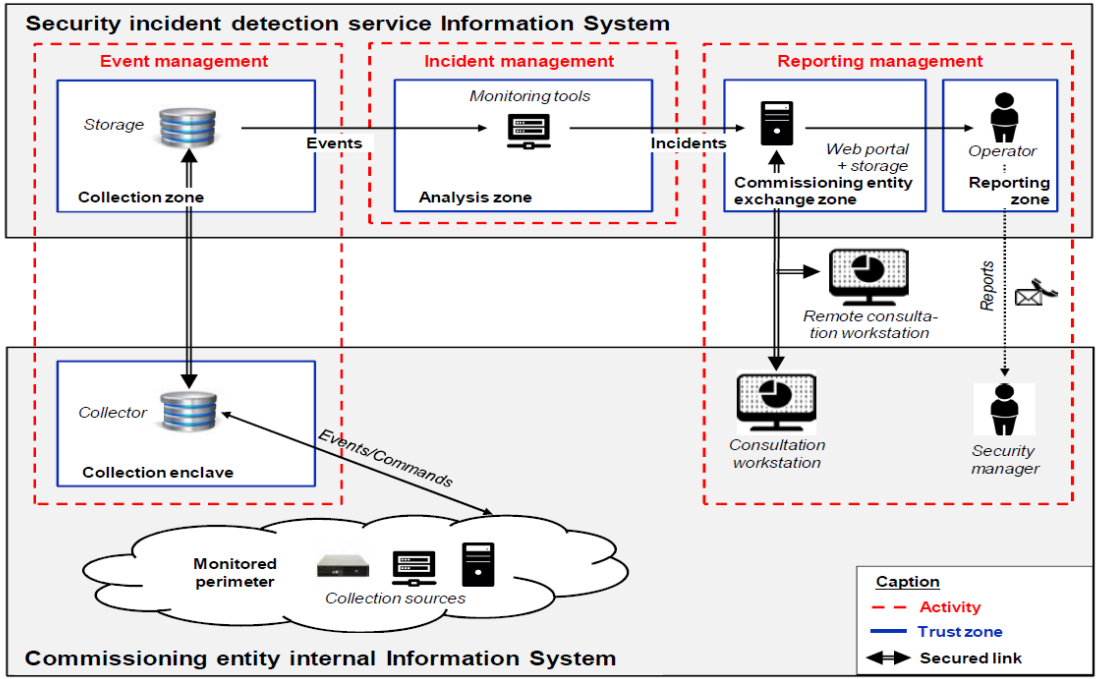


Fonte: standard NIST Special Publication 800-61 Revision 2

Security Incident Detection Service di un SOC

- I servizi di detection in un SOC sono certamente quelli più rilevanti, in cui si concentra il maggiore sforzo (strumenti, personale)
- Questi servizi includono:
  - Attività e strumenti legati alla gestione degli eventi
  - Attività e strumenti legati alla gestione degli incidenti
  - Attività e strumenti legati alle notifica degli incidenti

Architettura di un Security Incident Detection Service



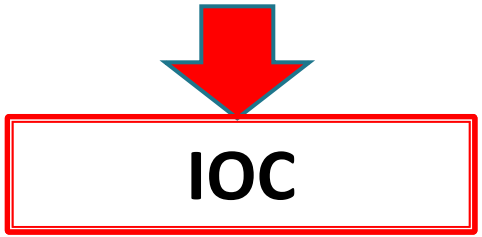
Fonte: standard ETSI GS ISI 007 V1.1.1 (2018-12)

Tool per il Security Incident Detection Service

- Intrution Detection Systems (IDS) e Intrution Prevention Systems (IPS)
- Antivirus e Antispam
- Software per il check dell'integrità dei file
- Servizi di monitoraggio offerti da terze parti
- SIEM (Security Incident and Event Management)
- Firewall e Proxy (es **WAF**, **NGFW**, **SWG**, **AntiDDoS**)
- sistemi di prevenzione della perdita dei dati (**DLP** – Data Loss Prevention)

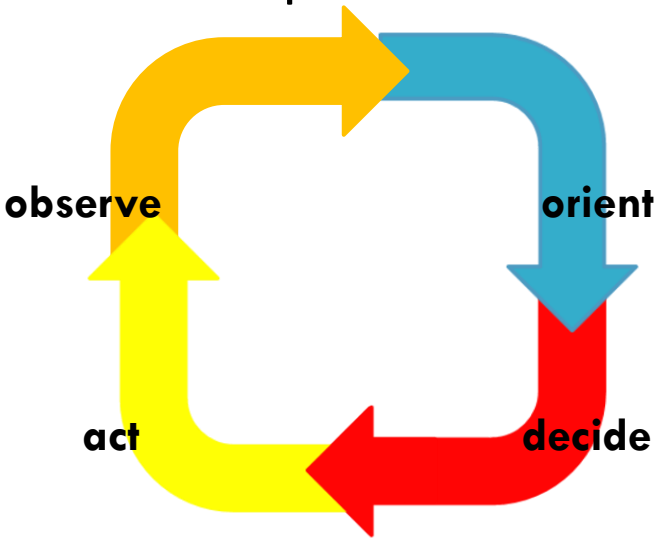
Tool per il Security Incident Detection Service

- Intrusion Detection Systems (IDS) e Intrution Prevention Systems (IPS)
- Antivirus e Antispam
- Software per il check dell'integrità dei file
- Servizi di monitoraggio offerti da terze parti
- SIEM (Security Incident and Event Management)
- Firewall e Proxy (es **WAF**, **NGFW**, **SWG**, **AntiDDoS**)
- Sistemi di prevenzione della perdita dei dati (**DLP** – Data Loss Prevention)



OODA loop per l'incident response

- Recentemente si è affermato un approccio all'incident response mutuato dalla pratica militare: ***OODA loop***



Strumenti a supporto dell'OODA loop

- È possibile fornire una classificazione degli strumenti per l'operatività di un SOC sulla base dell'OODA loop
- Ciò fornisce una visione generale inquadrando in essa anche i tool che forniscono operatività al SOC

Staff del Team di Incident Response di un SOC

- L'esperienza e la competenza del personale è l'elemento cruciale di un SOC
- È presente la figura del SOC-Manager
- Sono previsti diversi livelli (detti anche *Tier Level*)
- I ruoli sono organizzati per livello funzionale, in maniera coerente alle procedure di gestione degli incidenti, prevedendo tra esse *l'escalation*
- È possibile anche organizzare il Team secondo un approccio diverso da quello multi-tier, più *flat* e più orientato ai ruoli, oppure prevedere una combinazione dei due modelli.

Procedure

- È fondamentale codificare in termini di procedure le diverse attività a carico del team di IR
- Tra le procedure particolare rilevanza hanno le procedure di
  - Prioritizzazione degli incidenti
  - Qualificazione degli incidenti
  - Gestione delle diverse tipologie di incidenti

Conclusioni

- La capacità di un’organizzazione di gestire incidenti informatici è cruciale
- Esistono best practice e standard, che si possono tradurre nella costituzione di un SOC dell’organizzazione
- Anche in assenza di un SOC alcune funzioni di IR devono sempre essere presenti.

Approfondimento 1: meccanismi di sicurezza

- I meccanismi di sicurezza sono l'insieme delle metodologie, protocolli e algoritmi, opportunamente supportati dalla tecnologia, atti ad implementare servizi di sicurezza, quali confidenzialità dei dati, confidenzialità del traffico, autenticazione delle entità in rete, autenticazione di messaggi, integrità, controllo dell'accesso, non ripudio. Un sistema informativo (che include una rete) può supportare, a vari livelli dello stack protocollare di rete, i suddetti servizi, ai quali vanno aggiunti requisiti trasversali di disponibilità e accountability. Nonostante il sistema informativo dell'organizzazione incorpora diversi servizi di sicurezza, anche perimetrale (attraverso firewall, intrusion detection system, intrusion prevention system, etc.), la probabilità di incidente informatico non è mai trascurabile.
- La crescente interconnessione delle reti e le esigenze di dematerializzazione rendono i sistemi informativi di un'organizzazione più vulnerabili agli attacchi informatici. I punti di interconnessione con le reti esterne (in primis Internet) rappresentano il punto di accesso privilegiato per un attaccante che ha lo scopo di entrare e rimanere all'interno di un sistema informativo. Non devono essere però trascurate le minacce provenienti dall'interno (*insider*), che sono potenzialmente più insidiose e pericolose.

Approfondimento 2: Asset

- Un asset è una qualsiasi risorsa o entità che ha valore per l'organizzazione, che è mezzo o fine della missione portata a termine dall'organizzazione
- Un asset è un server, una rete, una postazione di lavoro, un software, un processo
- Gli asset quindi possono essere materiali o immateriali
- Gli asset possono essere legati al fine ultimo della missione: ad esempio, per una struttura sanitaria, la salute dei pazienti è un asset.
- Gli asset dell'organizzazione sono ciò che è minacciato dagli attacchi informatici, e ciò che può essere danneggiato o distrutto da un incidente informatico.
- Il primo problema per una organizzazione è avere piena consapevolezza degli asset. Per gli asset materiali ciò significa avere una efficace capacità di inventariare le risorse hw e sw dell'organizzazione.

Approfondimento 3: Introduzione a IM

- È auspicabile pertanto che l'organizzazione, oltre ad avere la capacità di gestire il rischio informatico in maniera adeguata, adottando i controlli di sicurezza sulla base di un approccio *risk-based*, debba avere la capacità di gestire gli incidenti informatici, in tutte le fasi (*pre-durante-post*), attraverso processi e procedure codificate e strutturate
- L'organizzazione deve avere quindi la cultura dell'Incident Management (IM). Al livello di massima maturità, ciò significa mettere in atto infrastrutture fisiche, organizzative, tecniche e logiche dedicate a tale fine, spostando il baricentro della gestione della sicurezza verso l'IM.

Approfondimento 4: impatto e probabilità

- Mitigare l'impatto significa ridurre le conseguenze (anche in termini organizzativi ed economici) dell'indicente informatico in questione. Saper rilevare in maniera precoce un attacco, e adottare strategie di rimedio immediate può significativamente ridurre le conseguenze dell'attacco.
- La probabilità dell'accadimento potrà essere ridotta per diversi motivi. Il primo è che IM significa anche, come vedremo più avanti, adottare misure che tendono al continuo assessment della robustezza dei propri sistemi. Il secondo è legato al fatto che una corretta gestione degli incidenti permette all'organizzazione di avvalersi dell'esperienza acquisita sugli incidenti passati per proteggersi meglio da attacchi futuri, riducendo quindi la probabilità che attacchi simili possano avere successo nel futuro.

Approfondimento 5: IM e IR sinonimi

- Il trend recente (avvalorato anche dallo standard NIST Special Publication 800-61 Revision 2) è di considerare i due termini come sinonimi, al fine di evitare che eventuali processi di natura gestionale attivati nell'organizzazione per implementare le funzioni di IM possano essere visti in maniera scorrelata (anche in termini di ruoli) dai processi di IR. Ciò comprometterebbe significativamente l'efficacia di entrambe le funzioni.
- D'altra parte ha poco senso pensare a processi di Incident Response senza includere gli aspetti logistico-organizzativi-procedurali.

Approfondimento 6: CSIRT e SOC

- In una organizzazione complessa, in partcolare *mission critical*, le azioni di governance della sicurezza e di protezione dagli attacchi non sono sufficienti. In tali casi è necessario attivare le funzioni di IR, almeno attraverso la costituzione di un team di risposta agli incidenti. Tale team viene spesso definito Computer Security Incident Response team – team di risposta agli incidenti di sicurezza informatica (CSIRT) – o computer emergency response (or readiness) team (CERT) – team di risposta/prontezza alle emergenze informatiche (CERT).
- Il SOC è una struttura di centro di comando della sicurezza di una organizzazione, composta da un team di professionisti IT con esperienza nella sicurezza delle informazioni. È responsabile del *monitoraggio*, dell'*analisi*, del *rilevamento* e della *protezione* di un'organizzazione dagli attacchi informatici, includendo le funzioni di *Incident Response*. Nel SOC, il traffico Internet, le reti aziendali, i desktop, i server, le postazioni di lavoro, i database, le applicazioni e altri sistemi sono continuamente esaminati (attraverso una collezione automatica dei log) per rilevare (con gli strumenti opportuni) eventuali segni di un incidente di sicurezza. Il personale SOC può lavorare con altri team o dipartimenti, ma è in genere autonomo con dipendenti che dispongono di competenze informatiche e di sicurezza informatica e delle informazioni di alto livello. Inoltre, la maggior parte dei SOC è in operatività 24 ore su 24, mentre i dipendenti lavorano a turni per registrare e monitorare costantemente l'attività e mitigare eventuali minacce rilevate. Il SOC include uno CSIRT.
- E' da osservare che, secondo alcune accezioni, un SOC non debba necessariamente incorporare le funzioni di CSIRT, rappresentando in tal caso solo la divisione dell'organizzazione in cui si concentra la gestione (anche operativa) della sicurezza aziendale. In tal caso, le funzioni di IR potranno essere implementate in un CSIRT separato. Tale architettura è ritenuta tuttavia obsoleta perché non contribuisce ad implementare una visione olistica della sicurezza.

Approfondimento 7: Tipi di SOC

- Ovviamente un SOC interno prevede significative capacità tecniche e organizzative dell'organizzazione. Allo stato attuale, solo una modesta percentuale di organizzazioni pubbliche o private posseggono un SOC. Non è escluso che un'organizzazione, pur avendo un SOC interno, ne abbia in outsourcing alcune componenti, come ad esempio parte del personale.
- Il SOC esterno è la soluzione spesso adottata in caso di insufficienti risorse interne. Esso può essere dedicato o shared. La disposizione fisica delle varie componenti del SOC dipende in questo caso dal fatto che sia o no dedicato.
- Il SOC outsourced shared può comportare significativi benefici. Fermo restando che un certo grado di condivisione dell'informazione tra diversi SOC/CSIRT a livello nazionale ed internazionale è sempre presente, nel caso in cui un determinato Service Provider fornisce a diverse entità committenti il servizio di SOC (in outsourcing), il grado di condivisione dell'informazione tra le diverse realtà sarà massimo, a beneficio dell'efficacia della detection e della prevenzione.

Approfondimento 8: Funzioni di Base

- Il SOC ha una visione complessiva dei sistemi e delle reti presenti nell'organizzazione e si occupa dell'hardening di server, dei sistemi operativi, delle componenti della rete. Ciò è fatto sulla base di best practice per evitare misconfigurations e sulla base di attività di vulnerability assessment e in stretta collaborazione con il NOC (network operation center). Il VA deve essere considerata come attività di routine da compiersi con frequenza elevata (es. una volta al mese). Attività di penetration test svolte saltuariamente (eventualmente in outsourcing) sono da considerarsi tra le funzioni di base. Il PT diventa una funzione di base se è inquadrata in un approccio di tipo Red-Team/Blue-Team o Purple Team, descritto nel seguito. Rientrano tra le funzioni di base le attività di Governance della sicurezza inclusa la compliance normativa e tecnica.
- Le attività di access control prevedono sia la definizione di policy e la loro implementazione sui vari domini dell'organizzazione. Ciò verrà fatto attraverso le funzioni native di access control combinate con l'adozione di sistemi di gestione delle identità e degli accessi di tipo IAM (Identity Access Management) e PAM (Priviledged Access Managemet), opportunamente combinate. La gestione dell'identità e del controllo degli accessi è divenuto un nodo fondamentale della sicurezza dell'organizzazione.
- Rientrano tra le funzioni di base quelle orientate alla sicurezza perimetrale, quali la configurazione, gestione e manutenzione di firewall, IDS e IPS, nonché le attività di gestione centralizzata degli antivirus e antimalware e dei sistemi di end-user-protection per le postazioni di lavoro.

Approfondimento 9: R/Blue Team & Forensics

- Il modello organizzativo standard per un SOC prevede di includere un insieme di operatori e analisti che governano le funzioni di rilevamento e recovery, avvalendosi degli strumenti presenti nel SOC. Si sta affermando tuttavia un modello che fa convivere, all'interno del SOC, oltre alle funzioni di rilevamento e difesa tipiche del *Blue Team*, anche le funzioni di attacco, per la verifica costante della robustezza dell'infrastruttura sotto controllo. Ciò viene realizzato attraverso la presenza di un team dedicato, chiamato *Red Team*, che talvolta può essere esterno al SOC e ingaggiato periodicamente per svolgere campagne di Vulnerability Assessment e Penetration Test.
- Il modello che si ritiene essere di maggiore efficacia è quello in cui le funzioni di Red Team e Blue Team stiano all'interno del SOC, anche attraverso una squadra che copre entrambe le funzioni che, in questo, caso viene denominata *Purple Team*.
- Gli analisti del SOC sono certamente le figure più adeguate a ricercare dettagli nei log di rete, di sistema o applicativi dell'intera infrastruttura. In caso di indagini forensi, gli analisti aiutano a raccogliere le prove elettroniche e a garantire la catena di custodia di tali prove.

Approfondimento 10: Fasi dell'incident handling 1/2

- **Preparation**. Questa fase riguarda l'adozione delle misure di sicurezza atte a garantire protezione, applicate sulla base di un approccio risk-based. In aggiunta è necessario predisporre i protocolli e i mezzi di comunicazione per la gestione dell'indicente (es, informazioni di contatto, strumenti per il reporting, etc.) e strumenti da usare per l'investigazione da compiere (es., laptop, workstation forensi, packet sniffer, etc.). Nella fase di preparazione rientra anche la definizione e revisione delle procedure. La fase di preparazione può trarre beneficio dall'esperienza di precedenti incidenti.
- **Detection&Analysis**. La detection è il cuore dell'attività di incident response. Una detection pronta e precoce è fondamentale per la mitigazione dell'impatto. L'efficacia della detection dipende strettamente dalla disponibilità nel SOC di strumenti avanzati, e dalla capacità degli analisti di configurare ed utilizzare bene tali strumenti. I principali strumenti sono IDS, IPS, SIEM, Antivirus/Antispam, Software per il check dell'integrità dei file, Information shraring e servizi di terze parti. L'attività di detection si basa anche sulla disponibilità di log, di rete, di sistema operativo ed applicativi. Tutto questo può attivare specifici indicatori di compromissione (IoC). Il team ha come primo compito quello di capire se si è realmente di fronte ad un incidente. Successivamente deve eseguire un'analisi iniziale per determinare l'ambito dell'incidente, ad esempio per individuare le reti, i sistemi o le applicazioni coinvolte, cosa ha originato l'incidente e come si sia verificato (ad es. quali strumenti o metodi di attacco sono stati utilizzati e quali vulnerabilità sono state sfruttate). L'analisi iniziale dovrebbe fornire informazioni sufficienti per guidare le attività successive, dando priorità per esempio al contenimento dell'incidente rispetto ad un'analisi più approfondita degli effetti dell'incidente. In questa fase il compito del Team è anche quello di documentare l'incidente in maniera appropriata e di notificarlo alle parti interessate (interne e/o esterne all'organizzazione). È da osservare ancora che in generale il team processa diversi incidenti in parallelo. E' necessario prioritizzarli e dare precedenza agli incidenti a maggiore impatto.

Approfondimento 10: Fasi dell'incident handling 2/2

- **Containment&Eradication.** In molti casi è necessario prendere decisioni circa il possibile contenimento di un incidente in atto. La decisione non è banale perché può avere impatto su aspetti di natura operativa. Ad esempio, il contenimento può essere ottenuto facendo lo shut down di un server, oppure isolando un segmento di rete, o ancora disabilitando alcuni servizi. Questa attività è tanto più complessa e difficilmente gestibile quanto più vi è assenza di progettazione. In altri termini è necessario predeterminare nelle procedure di gestione degli incidenti quali sono le possibili misure di contenimento e che impatto esse provocano, prevedendo anche come compensarle nel transitorio (finchè i servizi on sono ripristinati). Alla fase di contenimento (in cui le attività di estrazione di evidenze di natura forense deve essere completata accuratamente), segue quella di Eradication e Ripristino dei servizi. Eradicare significa eliminare le cause dell'incidente. Questo può significare quindi eliminare un malware da uno o più host, bloccare account compromessi, disabilitare utenze di email, patchare un sistema per eliminare vulnerabilità sfruttate nell'attacco, etc. Vi sono poi attività di ripristino che possono anche riguardare host non soggetti a Eradication ma la cui funzionalità è stata compromessa dall'incidente. Come si evince dalla figura, le fasi di Containment&Eradication e Detection&Analysis sono eventualmente eseguite in più iterazioni, perché dopo ogni step dell'una è necessario eseguire l'altra per verificare se il task è stato completato.
- **Post-incident activity**. In maniera sintetica, le attività post-incidente hanno lo scopo di rispondere alle seguenti domande. Cosa possiamo fare per evitare incidenti simili nel futuro? Come possiamo migliorare le nostre capacità di rilevamento? Come possono essere migliorate le procedure di contenimento? Quali azioni dobbiamo compiere anche dal punto di vista organizzativo per far si che la lezione appresa dia il giusto feedback alla fase di preparazione per questo tipo di incidenti?

Approfondimento 11: Attività del Security Incident Detection Service di un SOC

- **Gestione degli eventi**. Riguarda tutto ciò, in termini di mezzi tecnici e organizzativi, che il SOC deve mettere in atto per garantire una precisa e significativa raccolta e l'archiviazione degli eventi di sicurezza (log, alert, etc.)
- **Gestione incidenti**. Riguarda i mezzi tecnici e organizzativi per l'identificazione e la qualificazione di un incidente di sicurezza sulla base degli eventi raccolti e monitorati. Anche la memorizzazione degli incidenti di sicurezza al fine di migliorare il servizio rientra in questa attività.
- **Gestione delle notifiche**. Riguarda tutti i mezzi tecnici e organizzativi che consentono di informare le parti interessate degli incidenti di sicurezza rilevati e di archiviare tali notifiche. Nel caso di SOC in outsourcing la notifica riguarda quindi il Committente.

Approfondimento 12: Architettura di un SOC

- In questa architettura ci poniamo nel caso più generale di SOC in outsourcing, per cui appare nell'architettura la presenza di una Commissioning Entity (Committente). Si può affermare che questo è il caso più generale perché, anche nel caso di SOC interno, il SOC deve essere visto come un servizio che definisce un dominio logicamente separato da quello oggetto del monitoraggio e controllo. Pertanto, la Commission Entity è mappata su aree o divisioni interne della stessa organizzazione in caso di SOC interno.
- Lo standard ETSI mostra una descrizione architetturale di un SOC, individuando diverse zone con diversi scopi funzionali. Ogni zona può essere singola o multipla.
- Le **collection zones** (aree di raccolta) comprendono tutti i dispositivi coinvolti nel processo di raccolta per la memorizzazione di eventi e di informazioni di background potenzialmente utili alla detection.
- Le **analysis zones** (aree di analisi), comprendenti tutti i dispositivi coinvolti nel processo di analisi, compresi gli strumenti tecnici per l'analisi degli incidenti di sicurezza;
- Le **reporting zones** (aree per la notifica), comprendenti i sistemi di segnalazione verso e dal Committente. Si intendono quindi i sistemi usati per la notifica degl incidenti, ma anche i meccanismi usati dal team per ricevere ulteriori informazioni da parte del Committente nelle divere fasi di gestione della detection. Le zone di notifica includono *zone di scambio*, comprendenti tutti i dispositivi che consentono al Committente di visualizzare i dettagli delle informazioni sugli incidenti segnalati, e di fornire, ove applicabile, le informazioni necessarie per qualificare l'incidente;
- **Enclaves**. Per ogni perimetro monitorato (eventualmente appartenente al Committente) deve essere predisposta un'area *trusted* che rappresenta una sorta di *insediamento* del SOC all'interno del perimetro, almeno per quanto riguarda l'event managament. Questa area è appunta denominata enclave, mutuandone il significato originale del termine che significa «Territorio situato entro i confini di uno stato ma politicamente dipendente da altro stato». L'enclave dovrà contenere almeno uno o più collettori di log locali, che centralizzano (con eventuale pre-processing) tutti gli eventi di sicurezza che si verificano all'interno del perimetro monitorato. Questo permette di organizzare il trasferimento degli eventi verso le collection zones del SOC in maniera più razionale, e garantendo policy e meccanismi di sicurezza dedicati. Anche le policy di retention potranno essere stabilite in maniera indipendenti da logiche interne al perimetro monitorato.

Approfondimento 13: IDS/IPS

- I sistemi IDS identificano eventi sospetti e registrano i relativi log, tracciando gli elementi temporali che descrivono l'evento, il tipo, e le informazioni TCP/IP che lo caratterizzano (indirizzi IP, porte TCP sorgente e destinazione). Sono sistemi perimetrali più avanzati rispetto ai Firewall, perché hanno lo scopo di identificare pattern di attacco. Se il sistema è configurabile in modo da poter programmare il blocco di tali attività sospette siamo di fronte ad un IPS.

- La maggior parte dei prodotti IDS/IPS utilizza un approccio *signature based,* basato cioè su pattern noti assimilabili a potenziali attacchi. I file di signature, è tipicamente distribuito dal Vendor e tali signature devono essere costantemente aggiornate. Il problema principale degli IDS/IPS signature-based è che il sistema non è in grado di reagire ad attacchi di tipo zero-day o comunque non contemplati dalle signature.

- Per ovviare al limite dell'approccio signature based, gli IDS/IPS di nuova generazione implementano un approccio anomaly-based, spesso combinato con quello signature based. In tal caso però, essendo in generale impossibile codificare attraverso regole i comportamenti non anomali, tali sistemi sono basati su machine learning, e si parla di IDS/IPS comportamentali.
- Il problema principale degli IDS/IPS di ultima generazione è che in generale originano molti falsi positivi.

Approfondimento 14: Antivirus/Antispam

- I sistemi di Antivirus/Antimalware sono di fatto degli IDS/IPS che lavorano a livello di sistema operativo per individuare software malevoli e bloccare la loro azione. Anche per essi tipicamente l'approccio è *rule-based* e si fonda sulla disponibilità di signature costantemente aggiornate.
- I sistemi antivirus più avanzati sono basati su SandBox (macchine virtali), all'interno delle quali il file sospetto viene esploso per verificare che tipo di azioni vengono svolte dal programma. Attraverso questa simulazione di esecuzione, il sistema è in grado di rivelare, ancora attraverso un approccio rule-based, file malevoli.
- Il limite degli antivirus non basati su Sand-Box è quello tipico degli approcci signature-based, aggravato dal fatto che i malware spesso sono polimorfici o metamorfici e quindi sono di difficile detection. Il limite degli antivirus con Sand-Box è dato dal fatto che malware avanzati usano tecniche di evasione durante la fase di esplosione, simulando comportamenti benevoli in quella fase e quindi eludendo la detection.
- Un SOC gestisce sistemi antivirus e antispam in maniera centralizzata, prevedendo anche la raccolta di log ed eventi relativi alle attività di antivirus e antispam.

Approfondimento 15: File Integrity Check

- Si tratta di software che permettono di effettuare di controllo dell'integrità dei file rilevando eventuali modifiche apportate a file individuati come rilevanti (file di sistema di server, ad esempio). La tecnica utilizzata è quella del calcolo di un hash crittografico.

Approfondimento 16: Terze parti

- E’ possibile avvalersi di servizi di monitoraggio offerti da terze parti per il monitoraggio del proprio dominio di IP e dei nomi di dominio. Sono disponibili anche servizi che espongono blacklist pubbliche. Infine è frequente che da altri CSIRT, possano giungere notifiche relative a possibili compromissioni che riguardano il perimetro monitorato dal SOC in questione.

Approfondimento 17: SIEM

- Il SIEM è un sistema che opera su log ed eventi provenienti da vari sistemi collezionati attraverso opportuni agent, e cioè componenti che, installati sui sistemi monitorati, o su collettori intermedi, filtrano, aggregano e inviano al collettore centrale le suddette informazioni.
- I SIEM sono sistemi complessi che includono una serie di funzioni. Essi per esempio includono anche funzioni IDS/IPS, funzioni di controllo dell'accesso, di compliance, di produzione di log forensi. Ma la principale funzione che li caratterizza e li differenzia rispetto agli altri strumenti di semplice difesa perimetrale è la capacità di analizzare i log attraverso correlazione di eventi di diverso tipo, sulla base di opportune regole di detection.
- I log provengono da svariati sistemi, come Firewall, Web Application Firewall, Intrusion Detection Systems, Intrusion Prevention Systems, sistemi antivirus e antospam, concentratori VPN, apparati di rete router, server DNS, server DHCP, server di autenticazione, IAM, PAM, sistemi applicativi, dispositivi degli utenti, etc.
- Le regole di detection sono definite dal vendor e arricchite dagli analisti del SOC, sulla base di eventuali specificità del dominio monitorato.
- I SIEM sono nati circa 20 anni fa, ma dalla nascita hanno subito una significativa evoluzione che li ha resi sempre più potenti (in termini di regole di detection e dominio di azione), più semplici, più precisi.
- La generazione più recente è quella che si fa risalire al 2017 (Gartner), ed è caratterizzata dalla presenza di due tecnologie: due nuove tecnologie (1) l'analisi Machine Learning-Based del comportamento degli utenti e delle entità (User and Entity Behavior Analytics – UEBA) e l'orchestrazione della sicurezza e la risposta automatizzata (Security Orchestration and Automated Response – SOAR), per implementare azioni di remediation automatiche.
- Il SIEM è uno strumento irrinunciabile in un SOC, perché riduce falsi positivi e falsi negativi rispetto agli approcci tradizionali.

Approfondimento 18: IoC

- Tutti i tool hanno lo scopo di rilevare artefatti che rappresentano Indici di Compromissione (IoC). Gli IoC sono definiti dagli analisti del SOC, anche sulla base dei tool a disposizione.
- Esempi di tipologie di IoC:
  1. Anomalie nell'attività di utenti (specialmente se privilegiati)
  2. Tentativi di accesso falliti
  3. Modifiche di configurazioni inattese
  4. File di sistema corrotti o registro modificato
  5. Traffico di rete in uscita eccessivo e non correlato a richieste
  6. Localizzazione fisica (geografica) degli IP da cui provengono gli accessi e accessi contemporanei da locazioni fisiche non compatibili
  7. Picchi di volume di lettura dai data base
  8. Volume elevato delle risposte HTTP, rispetto al tipo di richiesta
  9. Numero elevato di volte in cui è richiesta una certa risorsa web (anche con URL diversi)
  10. Uso di porte TCP insolite per una certa applicazione
  11. Picco di richieste DNS da uno specifico host (può essere un DNS tunneling per comunicazione C&C)
  12. Frequenza elevata di richieste ai server
  13. Richieste provenienti da IP in black list
  14. Richieste web identificabili come Bot
  15. Patching inatteso dei sistemi
  16. File inusuali di grandi dimensioni (prima della extrafiltration di informazioni spesso i dati sono raccolti in file posizionati in cartelle inusuali)
  17. Modifiche inattese dei profili di configurazione degli smartphone aziendali
- Nel caso di adozione di un SIEM il concetto di IoC si modifica. Non è il semplice IoC a far identificare un incidente, ma la correlazione tra diversi IoC, sulla base delle regole di detection opportunamente impostate.

Approfondimento 19: OODA loop

- **Observe**. E' fondamentale il monitoraggio costante del perimetro sottoposto a controllo, attraverso tutto quello che indirettamente può evidenziare un sintomo di un'intrusione. E' necessario quindi avere una costante attenzione verso log di ogni tipo, vulnerabilità esistenti nel sistema, comportamento del traffico di rete, eventi nei sistemi, etc. Tale fase è strettamente legata al concetto di IoC visto prima. Al fine di migliorare la fase di osservazione è necessario fare un lavoro costante di tuning dei tool di monitoraggio al fine di migliorare la qualità dei log, in termini di significatività e presenza di rumore.
- **Orient**. In questa fase conta molto l'esperienza e le capacità dei SOC analyst, insieme ad attività di threat intelligence potranno orientare il team verso il tipo di attacco che si sta individuando e, quindi i successivi step da compiere. Attraverso questa fase esperienza e threat intelligence possono essere combinate per fornire contesto e contribuire quindi ad interpretare ciò che si è osservato nella fase precedente. Nella fase di Orient deve essere inclusa anche l'attività di asset management (a partire dall'asset inventory). Un corretto e asset management è necessario per il Team di gestione degli incidenti per orientarsi verso le azioni da compiere.
- **Decide**. Le decisioni sono sempre a carico degli analisti del SOC, e si raggiungono sulla base delle precedenti fasi ma anche delle policy e delle procedure predeterminate dell'organizzazione.
- **Act**. Questa fase riguarda l'adozione delle misure di Containment/Eradication& Recovery viste precedentemente.

Approfondimento 20: OODA e tool (1/2)

- **Observe**. Tutti i tool elencati per la detection sono importanti per la fase Observe. Per maggiore completezza aggiungiamo anche i sistemi **NAC** (Network Access Control) e i sistemi a supporto dell'inganno (**Honeypot**). E ancora
  - **Log analyzer** e **Log Management** – Sono strumenti a supporto della gestione (raccolta e conservazione) e dell'analisi di log dei sistemi, compresi quelli generati da strumenti della sicurezza (es. **Firewall** e **Proxy e Reverse Proxy server**).
  - **Availability monitoring** – Questi strumenti controllano se i sistemi sono attivi e reattivi. In particolare, consentono di identificare eventuali interruzioni, rilevando possibili incidenti.
  - **Net flow analyzer** – Questi strumenti esaminano i pacchetti in transito sulla rete e possono essere utilizzati per verificare comportamenti anomali in flussi di comunicazioni.
  - **Web traffic analyzer** – Questi strumenti monitorano e registrano vari tipi di traffico tra un client e un server, permettendo di analizzare pattern di traffico, specialmente nei flussi HTTP tra browser e server Web.
  - **Vulnerability scanner** – Questi strumenti identificano i sistemi vulnerabili presenti nella rete, proponendo rimedi per le vulnerabilità identificate.
- **Orient**. Strumenti per l'asset managemet che, attraverso la presenza di agent distribuiti sull'infrastruttura, permettono una gestione degli asset semi-automatica. A questi strumenti vanno aggiunti i tool di threat intelligence.
- **Decide**. Attività tipicamente umana, possono essere però adottati sistemi di supporto alla decisione

Approfondimento 20: OODA e tool 2/2

- **Act**.
  - **Antimalware** tool – Strumenti che consentono di rilevare, contenere ed estirpare malware presenti su un endpoint.
  - **Patch management** tool – Strumenti per la gestione delle patch di sicurezza dei sistemi.
  - **Forensic** tool – Questi strumenti permettono di esaminare accuratamente i media digitali utilizzando procedure tecniche che consentono di eseguire con precisione l'individuazione di importanti informazioni investigative per il backup e conservare le stesse per analisi future. Inoltre permettono di analizzare le informazioni conservate per scoprire fatti e agire sugli stessi attraverso ulteriori indagini, risposte o segnalazioni.
  - **Backup** tool – Nella maggior parte dei casi, è più sicuro ripristinare un ambiente da un backup piuttosto che tentare di ripulirlo dopo che si è verificata un'intrusione o una compromissione. Esistono troppi rischi associati a non essere certi se un dispositivo, interessato in un attacco, è stato pulito e ripristinato correttamente. Gli strumenti di backup consentono di recuperare da un incidente con un ambiente completamente ripristinato, inclusi i dati.
  - **SOAR** (Security Orchestration, Automation and Response) tool – Una particolare categoria di strumenti a supporto del workflow e dell'automazione nella gestione degli incidenti e, più in generale, nell'operato dei diversi team di un SOC.
  - **Information Management** tool – Sistemi per la condivisione delle informazioni tra i team del SOC.
  - **Anti-Phishing** – Strumenti e piattaforme a supporto del bloccaggio di campagne di phishing e di attività di awareness attraverso campagne mirate.

Approfondimento 21: Tier Levels

- È utilizzata la classica suddivisione in livelli (tier level), usata nel contesto del supporto tecnico.
- **Tier Level 1 (L1), detto SOC operator**. Monitora continuamente la coda degli avvisi di sicurezza e lo stato dei diversi *sensori di sicurezza del SOC* (primo fra tutti la console del SIEM e la altre dashboard presenti nella *control room*), occupandosi del *triage* degli avvisi e raccogliendo tutti i dati necessari al livello L2 per la prosecuzione della gestione degli avvisi. Il personale del L1 assiste anche il Team per la corretta risoluzione dell'incidente e nella comunicazione con team esterni. Il personale di livello L1 è responsabile della creazione del *ticket* nel sistema di ticketing.
- **Tier Level 2 (L2), detto SOC Analyst**. Il personale di livello L2 ha funzioni di detection più specifiche. E' compito quindi di L2 validare gli avvisi provenienti dal livello L1 per il successivo processamento, la qualificazione dell'incidente, la individuazione della procedura corrispondente. L2 opera sul SIEM e utilzzando gli altri strumenti analisi ed è di fatto responsabile, con il supporto del personale L1 delle fasi di analysis&deterction e conteinment&recovery per incidenti di complessità media e bassa. L2 è impiegato anche nelle attività di configurazione del SIEM e nell'aggiornamento delle regole di detection. E' competente anche sulle attività di notifica e reportistica.
- **Tier Level 3 (L3), detto Senior SOC Analyst**. L3 gestisce eventi più complessi, è responsabile di una generale supervisione dei processi di gestione degli incidenti, dà maggiore impulso alle attività di reverse engineering, di definizione delle detection rules, di forensics, nonché di governance del SOC. E' il punto più alto della catena di *escalation* nella gestione degli incidenti.
- **Tier Level 4 (L4), è il SOC-manager**. Gestisce le risorse umane, il budget, la pianificazione dei turni e le strategie. Comunica con il management dell'organizzazione. Funge da punto di riferimento organizzativo per incidenti critici. Fornisce una direzione generale del SOC e per le strategia di sicurezza globali dell'organizzazione.

Approfondimento 22: visione alternativa

- Il limite dell'organizzazione multi-tier è che alcune competenze non vengano valorizzate a pieno. Pertanto è possibile implementare una diversa organizzazione del personale in Team.
- **Monitoring Team**: ha il compito di monitorare la dashboard degli incidenti
- **Content Team**: sviluppa nuove regole, crea firme, ecc.
- **Threat Intelligence Team**: identifica e crea in modo proattivo nuovi indicatori specifici per l'ambiente locale anche sulla base di strumenti e metodologie di threat intelligence.
- **Incident Response Team**: esperti conoscitori del SIEM e dei servizi di detection/containment.
- **Hunting Team**: meno esperti di SIEM, ma si concentra maggiormente sui comportamenti e le principali tecniche degli attaccanti.
- **Red Team/ Blue Team/ Purple Team** : descritti precedentemente

- Ovviamente gli approcci *multi-tier* e *role-oriented* possono essere combinatim prevedendo, ad ogni tiel level, figure appartenenti ai diversi ruoli (con esclusione del livello L1 che include tipicamente solo il ruolo Monitoring Team).

Approfondimento 23: prioritizzazione

- **In base allo standard** NIST.SP.800-61r2, la prioritizzazione deve tener conto dei seguenti fattori:
  - **Impatto funzionale (IF)**. Gli incidenti che colpiscono i sistemi IT in genere incidono sulle funzionalità fornite da tali sistemi, con conseguente impatto negativo sugli utenti. La valutazione iniziale dell'incidente, infatti, deve tenere in considerazione in che modo quest'ultimo impatta sulle funzionalità dei sistemi interessati, considerando anche il probabile impatto funzionale futuro se lo stesso non è immediatamente contenuto.
  - **Impatto sulle informazioni (II)**. Gli incidenti possono influenzare la riservatezza, l'integrità e la disponibilità delle informazioni trattate dai sistemi. Ad esempio, un attaccante può esfiltrare informazioni sensibili, alterare le stesse o renderle indisponibili (es. con attacco ransomware a cifratura). La valutazione dell'incidente deve tenere in considerazione anche l'impatto di una violazione della riservatezza delle informazioni trattate, un'alterazione delle stesse nonché la loro indisponibilità momentanea o permanente sull'operatività dell'organizzazione.
  - **Recovery dall'incidente (RI)**. Le dimensioni dell'incidente e il tipo di sistema interessato determinano la quantità di tempo e risorse che devono essere impiegate per il recupero dallo stesso. In alcuni casi non è possibile riprendersi da un incidente (ad esempio se la riservatezza di informazioni sensibili è stata compromessa) e non avrebbe senso spendere risorse limitate per un ciclo di gestione degli incidenti prolungato, a meno che tale sforzo non sia diretto a garantire che un incidente simile non si possa più verificare in futuro. In altri casi, un incidente può richiedere molte più risorse da gestire rispetto a ciò che un'organizzazione ha a disposizione. Per cui, la valutazione dell'incidente deve considerare lo sforzo necessario per il recupero effettivo da un incidente e valutare attentamente il costo (in termini di risorse) e i requisiti che lo sforzo di recupero richiede per la sua gestione.

Approfondimento 24: qualificazione

La qualificazione può basarsi su standard esistenti, quali per esempio ETSI gs_isi002v010101p, per il quale sono individuate 7 macrocategorie:

- **Intrusioni e attacchi esterni** (***Intrusions and external attacks***). Racchiude tutti i tipi di incidenti di natura malevola provenienti dall'esterno. Implica azioni commesse da persone sconosciute all'organizzazione che sono al di fuori della sua cerchia di dipendenti, partner commerciali, fornitori di servizi esterni e clienti.
- **Malfunzionamenti** (***Malfunctions***). Rappresenta tutti i tipi di incidenti fortuiti (failure, guasti o calamità naturali) o involontari (errore umano). Il sistema informatico coinvolto nell'incidente può essere interno (gestito dall'organizzazione) o "esterno" (gestito da un fornitore di servizi).
- **Comportamenti interni devianti** (***Deviant internal behaviours***). Include tutti i tipi di incidenti di natura malevola o intenzionale (negligenza, incoscienza e irresponsabilità) originati all'interno del perimetro di sicurezza dell'organizzazione. Include specificamente il furto dei diritti o dell'identità. Coinvolge dipendenti, partner commerciali (compresi i fornitori), appaltatori, fornitori di servizi esterni e clienti/utenti.
- **Vulnerabilità comportamentali** (***Behavioural vulnerabilities***). Questa prima categoria di vulnerabilità copre gli eventi di sicurezza che possono essere attribuiti a un determinato utente (sviluppatore o integratore, operatore del test, amministratore di sistema o di rete, amministratore di sicurezza, utente) e per i quali è utile sottolineare l'enfasi sull'aspetto umano dell'evento, in modo da evidenziare la deviazione dal comportamento appropriato o atteso (disattenzione o malizia).
- **Vulnerabilità del software** (***Software vulnerabilities***). Questa seconda categoria di vulnerabilità copre i difetti di sicurezza che esistono nei software utilizzati dall'organizzazione (software di sistema o applicativo, acquisiti o sviluppati internamente) e che possono essere sfruttati dagli attaccanti (esterni o interni) per eseguire attacchi e innescare incidenti di sicurezza. Questo tipo di vulnerabilità sono molto difficili da risolvere durante la normale operatività, a causa della loro origine nel processo di sviluppo del software. Inoltre, queste vulnerabilità sono spesso difficili da qualificare come chiare non conformità (ad esempio, violando le regole di programmazione del software applicate all'interno dell'organizzazione).
- **Vulnerabilità di configurazione** (***Configuration vulnerabilities***). Questa terza categoria di vulnerabilità copre eventi che indicano una deviazione dallo stato dell'arte accettato nelle politiche di sicurezza o nelle migliori pratiche, in particolare descrivono errori di configurazione dell'apparecchiatura e del software (politica di sicurezza tecnica non correttamente applicata, debolezze tipiche con alcune configurazioni, etc....) che possono essere sfruttati dagli attaccanti (esterni o interni) per mettere in opera attacchi e innescare incidenti di sicurezza.
- **Vulnerabilità della sicurezza generale (tecnica o organizzativa)** (***General security, technical or organizational, vulnerabilities***). Questa quarta categoria di vulnerabilità copre le vulnerabilità di sicurezza generali che possono essere definite come aventi un effetto complessivo e significativo sul livello di sicurezza del sistema delle informazioni e posizionate su un livello equivalente a uno dei controlli dello standard ISO 27002. Riguardano principalmente errori o falle nei processi o guasti o malfunzionamenti degli strumenti tecnici di sicurezza.

Approfondimento 25: gestione

- Le procedure di gestione per i vari incidenti, individuati attraverso le tassonomie prima accennate, che in dettaglio definiscono sottocategorie a granularità molto fine, dovrà essere fatta ricalcando in maniera precisa il ciclo di vita della gestione degli incidenti dapprima descritto. La procedura, oltre alla definizione delle attività di preparation, detection, analisi, conteinment, ripristino e attività post-incidente, deve prevedere anche l'escalation ai diversi livelli L1-L4, in funzione della priorità e assegnata all'incidente.