Incident Management: Significa Gestione degli Incidenti ed è composto da: Incident Response, Digital Investigation, Legal Assestment, Damage and Risk Assestment.
Digital Investigation: processo secondo il quale si hanno ipotesi da provare.
Forensic Analysis: Analisi che porta a delle ipotesi.
Politiche e Procedure: Un esempio di politica è "in questa azienda non è possibile utilizzare Skype, non è possibile scaricare mp3, …". Alle politiche devono seguire delle procedure. Un esempio di procedura è "non è possibile utilizzare Skype tranne che per gli indirizzi xxx.xxx.xxx.xxx dell'azienda, non è possibile scaricare mp3 dalle 3 alle 8, …".
Incidente di sicurezza: E' suddiviso in livelli (Top down, Bottom up). Può essere Singolo (riguarda solo un asset, ad esempio un solo pc di un'azienda), o Strutturato (riguarda più asset, ad esempio più pc della rete aziendale). Nella maggior parte dei casi dall'incidente singolo si può arrivare a quello strutturato, e in alcuni casi può essere vero anche il contrario. L'incidente di sicurezza và gestito anche dal punto di vista legale e/o giudiziario.
Framework di un incidente informatico: (non è sequenziale, ma parallelo!): Pre-incident preparation**:** Si tratta delle operazioni di tipo Preventivo che vengono effettuate per pianificare la reazione. Sono composte da: Politiche di sicurezza, Procedure da seguire in caso di intrusione, Hands On sulla log analysis e sull'esame forense. Incident Detection**:** Un incidente può essere "riconosciuto": Con l'ausilio di strumenti tecnologici (IDS, Log Correlator, Firewall, Antivirus), Segnalazione da parte di terzi coinvolti nell'incidente (anche Autorità Giudiziaria). Risposta iniziale all'incidente**:**Formazione della fonte di prova: Acquisizione delle immagini disco, Acquisizione dei logs, Elaborazione iniziale delle informazioni. Strategia di risposta all'incidente**:** Decisioni informative (Autorità Giudiziaria, coinvolgimento del management, anche di altre aziende coinvolte). Decisioni di interazione con l'opinione pubblica:Public Relations. Investigazione sull'incidente**:**Effettuazione dell'esame post-mortem, Effettuazione della parte di log analysis, Correlazione degli eventi, Il tutto rientra nella cosiddetta Artifact Analysis. Reporting: Consiste nella presentazione, a vari livelli dei cosiddetti *findings.* Comprende una serie di report e di presentazioni che devono essere inoltrate al management aziendale e all'autorità giudiziaria
Risoluzione dell'incidente**:**Riguarda le operazioni da effettuare per risolvere l'incidente informatico, comprese: Le attività di ripristino, Le attività relative alle cosiddette lessons learned che servono sia per la parte di management sia per i rapporti con i fornitori.
-Framework investigativo: Notification: notifica, quando l'incidente di sicurezza, la violazione, l'accadimento "0" si sono manifestati e/o quando l'operatore di Incident response ne è venuto a conoscenza, diretta e/o indiretta. Può essere di 2 tipologie: Human (se appunto viene fatta da un uomo) o Automatica (può essere fatta da un IDS oppure da un antivirus o firewall)**.** Preservation: quando si è chiamati a "congelare" la scena del crimine digitale, con degli accorgimenti di tipo legale/procedurale. L'obiettivo è comunque quello di garantire l'integrità delle potenziali fonti di prova, al fine di portarle, ove possibile, presso l'Autorità Giudiziaria competente, magari cercando di garantire il più possibile la compliance con il principio fondamentale del mantenimento dell'integrità al fine delle garanzie difensive. In genere si preserva il contenuto di: Media, log, supporti volatili(RAM). Se sto acquisendo un hd per esempio userò l'hardware write blocking, e i log. Esistono dei casi in cui l'acquisizione potrebbe non essere possibile: Live System Analysis , File Systems di dimensioni troppo grandi, File Systems di tipologie non riconosciute dallo strumento di clonazione, Casi contingenti di procedura penale o di eventi esogeni.
vengono sottoposti a hash per garantirne l'integrità. A volte la "qualità" dell'immagimne dipende dal tipo di file system. Survey: fase in cui si effettua un controllo generale del PC oggetto di discussione e del resto dei media eventualmente acquisiti. Questo controllo viene effettuato con metodiche particolari e con strumenti fondamentalmente automatici. Di solito ad operare sono tecnici con una conoscenza pratica dei principi di digital forensic (Forensics analisys) ma il cui skill non è paragonabile a chi si occupa del problema a basso livello e con

metodologie/ strumenti che richiedono un maggior intervento umano. Search/Analysis. È l'attività appena citata nel punto precedente. Richede una maggiore competenza negli operatori e consiste nella "scomposizione" delle fonti di prova (o meglio della loro copia identica) al fine di analizzarle in maniera estremamente approfondita, sia dal punto di vista logico ma, a volte e sempre più, sia da quello di tipo "fisico". Reconstruction. Conosciuta in italiano come "ricostruzione dell'evento" la reconstruction è quella fase in cui chi ha effettuato la perizia riproduce il possibile accaduto su un determinato PC, al fine di ricostruire un processo logico credibile ed accettabile in tribunale. I tipi di ricostruzione sono 3: Fisica (si riproduce fisicamente una macchina identica a quella in cui è successo il danno), Logica (l'immagine usa simili sistemi, utile in caso di microreti locali che hanno accesso alla lan aziendale in toto (poco frequente), può rivelarsi fuorviante, verbalizzazione interna), teorica (va fatta in extrema ratio , necessaria quando non si può accedere direttamente ai computer direttamente coinvolti come target, verbalizzazione estremamente granulare.) 6. Presentation: la presentazione multilivello (management (per i "manager", sono tralasciati gli aspetti tecnici), tecnico (molto dettagliato e con molti apsetti tecnici), legale (descrive le conseguenze legali del danno)) dei risultati dell'esame e, possibilmente anche dei possibili elementi di attribuzione di responsabilità.
Analisi Postmortem: Analisi effettuate su una macchina "staccata" dal resto del sistema.
LSA (Live System Analisys): Permette di analizzare lo stato delle macchine senza staccarle dal loro ciclo biologico aziendale.
Acquisizione e Integrità: Molto importante è verificare che le informazioni che si sta acquisendo mantengano la loro integrità, e che non siano compromesse. Questo serve per avvalere o meno la propria tesi.
Esami Limitati: Bisogna sempre fornire le motivazione sul perché non è stata eseguita un'indagine completa. Si può quindi procedere chiamando il magistero per l'estensione del mandato, dicendo che è essenziale per il proseguo delle indagini.
Investigazioni e Metodiche: Bisogna sempre innanzitutto verificare quale tipo di tenclogia utilizzare, e ciò va fatto in base al problema che si è presentato.

Standard investigativi: Bisogna trattare ogni invidente come se debba avere un responso 3 anni dopo, e debba finire in un'aula di tribunale. Per "ricordare" tutto, si utilizzano proprio gli strumenti software di case management. Gli ***Standard Investigativi*** sono: -*Criminal (penale)*: comprende il codice di procedura penale, il codice penale, polizia e autorità giudiziaria, procedibilità d'ufficio o a querela. In quella ad ufficio, nel momento in cui si conosce qualcosa, il procedimento parte automaticamente; in quella a querela invece, per le infrastrutture private c'è discrezionalità nel denunciare o no un evento (o un attacco). La differenza principale è nel fatto che la querela si può ritirare, mentre la procedibilità d'ufficio no. *–Civile:* E' meno schematico del penale e vi è preponderanza della prova. Ciò che conta principalmente quindi è la prova, e non come essa è stata ottenuta (come invece accade nel penale). *–Amministrativo:* Comprende inchieste interne, informalità, arbitrati/mediatori (figure che cercano di mediare tra 2 parti in causa, senza andare a finire in sede giudiziaria), ha potenziali incompatibilità con lo statuto dei lavoratori (ad es. l'art.5: le persone che lavorano in azienda non possono essere controllate a distanza) e con la legge sulla Privacy.
E-Discovery: è una ricerca distribuita di determinati oggetti e/o files di nostro interesse (Ricerca/Deduplicazione/Filtraggio/Presentazione). E' effettuato per esempio quando un'azienda produce prodotti pericolosi, cioè che possono provocare un incidente. L'azienda deve quindi dimostrare che il prodotto è stato realizzato con una certa attenzione.
Tainted Fruit: Fonti di prova acquisite impropriamente (abusando della propria funzione o della propria tecnologia), mediante violazione di privacy, intercettazioni abusive, violazioni della legge. Ogni fonte di prova acquisita in questa maniera non può essere utilizzata in giudizio.

Chain of Custody: (Catena della custodia): E' un inventario delle fonti di prova acquisite durante la fase post incident forensic. Le fonti di prova devono essere sigillate (fisicamente o elettronicamente) ed il tutto deve essere dotato di un Time/Operation Stamping. Molta importanza ha inoltre la sicurezza fisica della Chain of Custody, le cui fonti di prova acquisite devono avere garanzia di integrità.
Correlation: Quando si fa un indagine, non bisogna analizzare soltanto log files e file system, ma queste informazioni devono essere correlate da altre informazioni volte a sostenere la nostra tesi. Tra i suoi fini, vi è quello di analizzare in maniera correlata l'output dell'esame postmortem.
Subpoema: E' equivalente al nostro decreto del pm o all'ordine di esibizione dell'autorità giudiziaria. Può essere molto importante, in quanto input di altre aziende coinvolte nel caso. Potrebbe inoltre richiedere una deposizione da parte della persona che si è occupata del caso, come persona a conoscenza dei fatti, la quale deve scrupolosamente documentare tutto il possibile, compresi gli impedimenti tecnici incontrati.
Policy: Servono principalmente a stabilire ruoli e responsabilità (chi fa e che cosa fa), e si dividono in obbligatorie (che se violate danno luogo ad un incidente) ed informative. I ruoli e le responsabilità non si possono sempre gestire in maniera rigida, anche se devono assolutamente essere ben strutturati. Le policy vengono decise nella fase di *preparazione* dell'incidente. Devono essere inoltre continuamente testate sia con simulazioni che con casi reali, in quanto una contromisura non è efficace se prima non è testata. **Simulazione:** Si divide in: -*Statica:* fatta a tavolino, dove viene posto uno scenario e si cerca di risolverlo. *–Dinamica:* può avvenire con o senza avvertimento (non si avvisa il personale ma soltanto il responsabile dell'Incident Response Team. Nelle aziende questo può far diminuire temporaneamente la produttività, ma può essere un test anche quello.
Incident Response Team: Gruppo di persone che intervengono in caso di incidente; può essere fisso o non. L'IRT Fisso non si occupa soltanto dell'incidente, ma anche di studiare varie vulnerabilità che possono generarlo. Viene fatta una scansione sugli IP dell'azienda, e si trovano le vulnerabilità presenti per ogni macchina; i risultati si forniscono sia all'esperto di sicurezza dell'azienda, sia al gruppo di gestione degli incidenti. Questo perché loro conoscono bene la struttura della rete, e possono risalire subito alla macchina bersaglio (patchandola), e magari possono anche risolvere il "problema" sulle altre macchine della rete con la stessa vulnerabilità (macchine magari non ancora colpite).
Segnalazioni danno: Allo stato attuale la RFC 2350/3227 e la ISO 17799 richiedono la schematizzazione delle comunicazioni di incidente:Punti di raccolta(ovvero il punto di contatto interno all'azienda per la gestione della notifica,Il punto di contatto - lato investigativo - per la ricezione delle notifiche, Il punto di collection e di coordinamento tra i vari punti di raccolta), Attori del processo di segnalazione, Tracciamento della segnalazione. Il follow up opera in due direzioni: Verso l'interno(Direzione sicurezza, Direzioni HR, Legal etc , Escalation) , Verso l'esterno (Forze di Polizia, Magistratura, Altre aziende, Utenti finali per riscontro della segnalazione iniziale.)
Demage assessment: è Il conteggio dei costi relativi all'incidente di sicurezza:Costo della creazione del dato,Costo della Riproduzione del dato, Costi associati alla effettuazione dell'esame post mortem , Costi associati alla gestione legale Costo associato alla tutela del marchio e dell'immagine. Si tratta di un living cost, cioè di un processo continuo di revisione, fino alla chiusura dell'incidente. Di solito il Damage Assessment, è effettuato con tecniche e team di composizione mista. Alcuni incidenti vedono un costo anche nella gestione del team che si occupa dell'assessment medesimo
Esempio di un Organigramma Aziendale: In ordine di importanza: *-Top Mgmt/Board:* Presidenza, Amministrazione: figure aziendali che gestiscono l'incidente e a cui bisogna riferire il risultato e le conseguenze di incidenti gravi. *–Security Manager:* Cif Security Manager (o Officer CSO, conosciuto anche come GSO –Global Security Officer-), ha la

responsabilità trasversale della sicurezza, ovvero della sicurezza logica, fisica, ecc. Deve riferire tutto al Top Mgmt/Board. Vi è inoltre anche l'ISO (Information Security Officer), che ha invece la responsabilità della sicurezza dal punto di vista informativo (e non fisico). Il Security Manager è quindi a capo di: *-CSIRT (o IRT):* Team di gestione tecnica dell'incidente. Riceve i feedback (segnalazioni) dall'utente finale. Di solito vi è un numero di telefono o dei portali interni (Intranet) per segnalare delle anomalie. IRT può essere fisso (soprattutto nelle aziende di grandi dimensioni) o dinamico; in entrambi i casi si fanno simulazioni di incidenti o si aggiornano le linee guida. Al CSIRT fa riferimento l'*End User*. *–Legal:* In caso di incidente o in fase di preparazione, valuta l'impatto legale del problema (non solo quando il problema si verifica realmente). *–Organization PR:* Organizzazione delle Pubbliche Relazioni, importante sia dal punto di vista di immagine dell'azienda, che dal punto di vista legale.
Crisis Management: Disciplina che gestisce la crisi. (Incidente→Escalation→Crisi).
Gerarchia delle fonti (Norme di riferimento): -Codice penale e procedimento penale. –Codice civile e procedimento civile. –Leggi specifiche. –Legge Privacy. – Policy interne. –Normative internazionali.
Normative a latere: Sono normative internazionali (della gerarchia delle normative). Esempi: -*Basel II:* Regola i rischi nelle aziende di tipo finanziario. In questo caso vi possono essere rischi di credito o rischi operativi. *–Sox (Surbanex Oaxly):* Normativa americana che indica che le aziende devono essere organizzate per saper gestire incidenti. *–PCI (Payment Card Interface):* Insieme di passi che le aziende che effettuano pagamenti online devono seguire per porsi come tali. *–Hippa:* insieme alla PCI trova una certa corrispondenza con la nostra legge sulla Privacy. *–Legge Privacy.* Tutte queste normative possono essere oggetto di aggiornamento da parte del *DPS* (*Documento Programmatico della Sicurezza*), che è obbligatorio per tutte le aziende che trattano i dati personali. Al suo interno vi sono anche politiche di sicurezza, e contengono tutte le informazioni che l'organo accertatore (può essere la Guardia di Finanza, la Polizia Postale, il Garante della Privacy, ecc.) deve far rispettare in termini di sicurezza.
ISO 17799/ISO 27001: la ISO 17799 è detta *Normativa di indirizzo*, mentre la ISO 27001 è detta *Normativa di verifica*.**-ISO 17799: -***13.1 (Reporting):* Gli eventi e le debolezze di sicurezza (ovvero qualsiasi evento da cui si possa verificare un incidente informatico) devono essere comunicati tempestivamente per permettere delle correzioni tempestive. In azienda devono essere presenti delle procedure formali di reporting degli eventi e di escalation (cioè devono essere presenti in azienda delle procedure per riportare gli eventi in questione, e anche per "farli arrivare ai piani alti"). Tutti gli impiegati, i fornitori, e le terze parti che accedono ai sistemi dovrebbero conoscere le procedure per riportare i differenti tipi di eventi e debolezze che potrebbero avere un impatto sull'"asset organizzativo". Dovrebbe quindi essere chiesto loro di comunicare questi eventi o debolezze il più velocemente possibile agli addetti. QUINDI..: Vanno comunicati sia incidenti che vulnerabilità; Vanno coinvolti, a vario titolo, anche gli utenti finali e le terze parti; … . *-13.2 (Incident Management):* Assicurare un approccio consistente e funzionante, che possa essere applicato dai gestori degli incidenti di sicurezza informatica (…). QUINDI…: E' necessario un approccio effettivo (cioè con riscontro pratico) alla gestione dell'incidente; Continuos Improvement Process (cioè Miglioramento Continuo); Importanza della Digital Forensic.
-ISO 9001: Si occupa di certificare alcuni processi aziendali.
-ATIL: Insieme di standard di Service Delivery, che regolano cioè il modo in cui i servizi devono essere consegnati all'utente. Al suo interno sono compresi anche standard di sicurezza.

LOG:Log files: Ogni sistema/device di rete dovrebbe produrre del log files. I log vengono acquisiti per comprendere le modalità di penetrazione dell'intruso (da dove è entrato, e da dove è uscito…), per collaborare con le forze di polizia nel backtracking degli autori del reato, e per collezionare il numero più alto possibile di fonti di prova relative all'intrusione. E' molto

importante conservare il log allo stato grezzo, perché anche la sua strutturazione in database di log potrebbe essere considerata come una sorta di "manipolazione" delle informazioni. Quindi si deve cercare di conservare il Raw Log per permettere appunto l'analisi delle informazioni da parte di altri. I log si dividono principalmente in: *-Log di Sistema:* sono quelli del sistema operativo sui servizi. *–Log di Rete:* sono quelli dei router, firewall, access point, nis. *–Log di Device:* sono quelli legati ad apparecchiature particolari (ad esempio il telefono). L'*Architettura di Log* deve essere pianificata a priori (ovvero dove si trovano, come vi si accede, cosa contengono…). Nel pianificare l'attività di log, bisogna fare molta attenzione e valutare soprattutto se avviene *violazione di Privacy* (log che *non violano* la privacy sono ad esempio i log di mailserver, firewall, antivirus, backup del server di posta –questo soltanto se è specificato nelle policy, a patto che quando si fa l'analisi del file di posta, l'analista sia "attorniato" da altre persone che garantiscano e controllino il suo operato)-. **Rotation:** Quando un file di log ha occupato il 65% della coda di memoria a disposizione, avviene la rotazione, ovvero la sostituzione con un nuovo log. Rappresenta quindi il tempo totale in cui i log file debbano essere tenuti online prima dello storage. Alcune aziende (come ad esempio le banche), mantengono i *Log Life Time*. –**Retention***:* Rappresenta il tempo in i log file debbano essere tenuti online prima della loro distruzione.

Struttura dei log: Ogni log è costituito da *log entries*. Sono in pratica costituite da ciò che l'amministratore decide che deve far parte della "base loggante". In base a ciò che si sceglie di loggare, si può individuare quale può essere definito il "dato grezzo".

NetFlows (Formato log): positivo:Permette di inferire gran parte delle informazioni necessarie, Buoni risultati anche con link ad elevate velocità, Non viola la privacy degli utenti, Non soffre del fatto che le comunicazioni siano cifrate. negativo: Rappresenta un "riassunto" delle comunicazioni intercorse, Non è possibile estrarre i dati scambiati.Di solito sono generati da: router (cisco, juniper, etc),sonde con software specifico (argus, fprobe, etc),switch L2/L3 (cisco, nortel, etc).

Formato log: Syslog (RFC3164), Event Log sistemi Windows, Common Log Format e Combined Log Format per i webserver , wtmp/utmp su sistemi unix-like. **Elementi fondamentali nei log:** riferimenti temporali macchina coinvolta, dettaglio operazioni/cambiamenti effettuati . Metodi di sincronizzazione dei tempi dei log: Windows time protocol, ntp.

Log Management: E' il processo di generazione, trasmissione, analisi, storage dei log di sicurezza. Nel dettaglio: *-Generazione:* Riguarda la generazione e l'acquisizione del log file. *–Trasmissione:* Momento in cui il log acquisito viene trasmesso su un'altra macchina o dispositivo. Entrano quindi in gioco la *sicurezza* della trasmissione e l'*autenticazione* dei poli della trasmissione. *–Analisi:* Processo con cui si cerca di capire cosa è accaduto, osservando i log, che possono essere *correlati* anche con altri log presenti da altre parti. *–Storage (destinazione finale):* Metodo per determinare dove i log devono essere "salvati". In questa fase può avvenire *Storage*, oppure *Disposal*, ovvero una cancellazione dei log che non servono più.

Generazione dei Log: La generazione può essere ***continua*** (i log vengono generati di continuo; es. log di rete, syslog, ecc.), o ***schedulata*** (*batch mode*) (in cui vi è una generazione ciclica, ovvero che avviene soltanto in determinati momenti, oppure quando si verificano un tot di eventi, oppure ancora solo quando l'applicazione che logga viene avviata). I log vengono generati da: *-Security Software*. *–Packet filter:* applicano un filtraggio generale sui pacchetti in transito (generalmente operano sul router. Genera degli eventi in particolare su richiesta DENY delle ACL (Access Control List). Lavora a livello di intestazione (*header*) dei pacchetti. *–Firewalls:* La differenza dal Racket Filter è nel metodo di ispezione dei pacchetti, perché i firewalls oltre che l'header, va ad analizzare anche il contenuto del pacchetto. *–Antimalware Software:* Tutto il software in grado di contrastare o bloccare malicious code in entrata sul sistema. Può essere anche contenuto nel firewall; logga tutte le istanze in cui si presenta malicious code e logga anche quante volte viene scansionato un file infetto. Inoltre, viene

loggato anche quando e come viene fatto un update del software in questione, e se questo sia andato o no a buon fine. Altri security software che generano log sono: *- Intrusion Detection (ID) e Intrusion Prevention System (IPS):* vengono loggati record relativi ad anomalie (*Anomaly Detection*). Fanno anche il *Pattern Matching*, ovvero un incrocio tra l'evento loggato e un database di firme (ITS). IPS invece, data una violazione, procede ad una scansione su altre macchine che possono essere vulnerabili (ha quindi anche la possibilità di chiudere le connessioni relative a queste macchine). Generano quindi log file. Al loro interno solitamente si inseriscono prodotti di integrità (*Integrity Check*), come ad esempio *Tripwire*. *–Vulnerability Management System:* Software che gestisce le vulnerabilità del sistema: dipende molto dal livello di *Patching* (update) e dal livello di *Scansione*. Logga quindi il livello di aggiornamento delle patch e il livello di vulnerabilità presente. Sono sistemi che non "girano" in tempo reale, ma in maniera ciclica. *–Autentication Servers*: si occupa di gestire ogni tentativo (riuscito o meno) di autenticazione al sistema, compresa la sua provenienza. *–Network Quarantine Servers:* Sono servizi che permettono di loggare quando una macchina ha effettuato l'accesso alla rete, in maniera non conforme a determinate policy di sicurezza. Si basa sul *NAC* (*Network Access Control*), che rappresenta appunto la capacità di accedere ad una rete soltanto se vengono rispettate determinate policy di sicurezza prestabilite.

Log di audit: Log che servono per tenere sotto controllo la situazione, ovvero per "ascoltare" cosa succede. Vengono molto spesso interfacciati con gli altri log disponibili (*correlation*).

Come comportarsi in caso di incidente (con i log): *1)* Fare un *Traceback* per individuare la posizione dei log (ovvero, conoscere dove sono i log che interessano). *2)* Si contattano i sysadmin per la cautela immediata dei log files (ovvero, acquisizione e mantenimento dei log files). *3)* Contenere il danno generato (*Mitigation:* il tempo medio va dalle 2 alle 48 ore. Ai fini della completa identificazione dell'accaduto e l'identificazione delle lessons learned, e in presenza delle info necessarie, il tempo di indagine non supera i 15/20 giorni). *4)* Collezionare i log in locale (acquisizire i log di interesse sulla postazione dell'operatore (attenzione: questo non significa "generare i log"!!). Di solito i log non si "storano" in locale, perché potrebbero essere modificati da un eventuale attaccante; bisogna quindi delegare i log verso un'altra entità (*Delegation Log*, o *Remotizzazione dei Log*). *5)* Acquisire i log in una maniera *forensically sending* (riguarda l'integrità dei log files). *6)* Generare l'immagine delle macchine colpite (ovvero copia *bitstreams* del disco).

LOG: Windows LOGging: Ci sono 9 classi per raggruppare gli eventi. I log si guardano con gli *Event Viewer*, che oltre a renderne visibile il contenuto, fornisce altre opzioni, come il filtraggio ad esempio in base all'IP; consente inoltre di fare ricerche di stringhe, o di esportare i log in formati testuali "normali". Per evitare la perdita di informazioni in quest'ultimo passaggio, bisogna assolutamente conservare anche il file originale (*dato grezzo*) ed andare a fare questa analisi in *Sola Lettura* per evitare di comprometterli. Gli eventi generati da Windows si suddividono in 2 categorie: *Success Event* e *Failure Event*. .In Windows ci sono principalmente 3 tipi di log: Application Log, Security Log, System Log. **Evento (Campi Standard):** Il concetto di evento è applicato a quello della log entries. I campi standard di un evento sono: ID, Info temporali (data e ora), Username, Pc sorgente che ha generato il messaggio, Categoria, Tipo di messaggio. **Segregation of duty:** Separazione tra i vari livelli di controllo.

IDS: Introduction Detection System : Ne esistono varie tipologie, ma fondamentalmente le più importanti sono 2: *-Pattern Recognition*: è simile al sistema degli antivirus, con un database degli attacchi. Ha 3 campi: indirizzo di partenza, indirizzo di destinazione, e tipo di attacco. *– Anomaly Detection:* ha il compito di scovare le anomalie, e presuppone che gli IDS siano stati "educati" al funzionamento sicuro normale (*baseline*). Viene sviluppato anche un rank (cioè una classificazione) delle anomalie. Esistono inoltre delle soluzioni ibride intermedie, che sono parte di "architetture di retroguardia", in quanto vengono poste dietro ai firewall.

-Dove agiscono gli IDS: *-Network Intrusion Detection System (NIDS):* Sono delle "scatolette" senza IP (in questo modo non possono essere mandate offline), con una scheda di rete posta in modalità promiscua. Hanno la funzione di salvare i log e memorizzarli in un database. Agiscono sul livello 3 della scala ISO/OSI, e ciò è molto importante perché gli permettono di agire prima che i pacchetti arrivino effettivamente sulla rete. Un contro del NIDS è che su reti switchate hanno bisogno di hardware specializzati per controllare le comunicazioni. *–Host Intrusion Detection System (HIDS):* Controllano il traffico da e verso particolari sistemi, e sui loro binari presenti sul sistema. In molti casi il NIDS non "vede" qualcosa, quindi si può agire con questo HIDS. *–Application-based Intrusion Detection System (AIDS):* E' un sistema estremamente diffuso, dove le applicazioni hanno ruoli fondamentali e sono in grado di loggare. Vi è infine un'ultima tipologia, gli *Agent-based*, che hanno però l'aspetto negativo di poter essere disattivati da particolari tipo di attacco.
-Falso positivo: E' un evento effettivamente accaduto, che è effettivamente un allarme, ma che in realtà non è un problema.
-Falso negativo: Succede qualcosa di grave ma non viene segnalato come allarme. || Un sistema efficiente non deve avere troppi falsi allarmi o falsi positivi, in quanto si arriverebbe ad un punto in cui non verranno quasi più considerati (si pensi ad esempio ad una media di 150 allarmi all'ora…un po' troppo per considerarli tutti!).
-Cattura traffico: *-Full content:* possibilità data ad uno strumento di registrare tutte le comunicazioni scambiate dai poli. Si parla quindi di Payload. Pro: ogni singolo elemento dei dati è accessibile per un'analisi a posteriori da parte di altri programmi come ad esempio Tcpdump. Contro: richiede un adeguato spazio di memorizzazione, e non è molto praticabile quando le velocità dei link sono elevate. Inoltre nel 98% dei casi, il traffico cifrato non è estraibile. *–Session Oriented:* Viene visto come via di mezzo, e comprende durata, stato e dati scambiati. Si tratta però di porzioni di traffico, quindi si ha il rischio di perdita di dati. Molto spesso i dati vengono tagliati al raggiungimento di una certa grandezza del Payload quindi c'è anche la possibilità di perdere dati importanti. *–Statistico:* Si fa una statistica sui dati di utilizzo della rete.
grep è uno strumento molto potente. È usato per trovare determinate linee all'interno di un file. Ciò vi permette di trovare rapidamente file che contengono determinate cose all'interno di una directory o di un file system. Ci sono modalità che permettono di specificare i criteri di verifica da abbinare alla ricerca. Per esempio: trovate tutte le stringhe nel dizionario che cominciano con la "s" e rifiniscono con la "a" per aiutare a compilare le parole incrociate.

Iritaly: **Cancellazione dei media di destinazione:**E'possibile procedere alla cancellazione dei media di destinazione utilizzando due tecniche . La prima soluzione prevede l'azzeramento del contenuto del disco mediante la scrittura di zeri sul disco. In alternativa è possibile procedere utilizzando strumenti come bcwipe che permettono una cancellazione sicura dei dati presenti sul disco, nel caso stiamo utilizzando supporti "riciclati". Bcwipe permette di utilizzare una molteplicità di algoritmi per la cancellazione sicura dei supporti come: U.S.DoD5200.28 sette passi, 35 passate utilizzando il metodo descritto da Peter Gutmann,U.S.DoD5200.28 con un numero arbitrario definibile di passate. **Raccolta informazioni volatili**:E' possibile utilizzare i binari statici presenti nella cartella /statbinoin/win32/tool del CD per salvare alcune informazioni che si perderebbero allo spegnimento del sistema . Durante questa attività è bene fare uso di binari fidati per recuperare le informazioni di interesse. Ultimo reboot del sistema: uptime. Data e ora del sistema:A questo scopo possibile utilizzare i comandi date,time(Win32) edate(*nix). Versione del sistema:In ambienti *nix utilizzando il comando uname mentre il comando ver,psinfo sotto sistemi Microsoft.Processi attivi: Comando ps in ambienti*nix e cprocess sotto Windows. Lista delle connessioni direte attive Per Windows ricorriamo all'utilizzo di netstat,fport,cports,mentre in ambienti operativi Unix netstat, lsof. Indirizzo macchina e MAC:In ambiente Unix si utilizza il comando ifconfig per ottenere sia le

informazioni dell'indirizzo IP sia riguardo il MACAddress; in Windows si utilizza il comando ipconfig.E' possibile che sia necessario acquisire ulteriori informazioni. In linea di principio le opzioni viste coprono le informazioni minime consigliate. **Duplicazione media**: I principali strumenti rivolti alla duplicazione dei media presenti sul CD sono:dd,dcfldd,aimage,AIR(frontend). **Analisi dei media generati**: Lo strumento più intuitivo e versatile presente sul CD è indubbiamente Autopsy; questa non è altro che un front-end per le utility presenti all'interno del pacchetto Sleuthkit. Questi strumenti sono categorizzati in base al livello sul quale lavorano. Layout del disco(mmls),dettagli sul file system (fsstat), processo delle unità dati(dcat, dls, dstat, dcalc),informazioni sui metadati associati ad un file o directory (icat,ifind,ils,istat), elenco di files residenti cancellati (ffind, fls), informazioni sul journaling(jls, jcat). E' possibile generare una lista di file presenti sul supporto da esaminare e categorizzare i file presenti in base alla propria tipologia(sorter).Riduzione dello spazio di indagine mediante know-good.Si consiglia di procedere alla creazione di un elenco dei file presenti contenente per ciascuno meta informazioni (MACtime) ed hash.E' fondamentale documentare tutti questi passi in modo da poter riprodurre i medesimi risultati.(Metodo scientifico,Oggettività. Riproducibilità). **Data carving:** Strumenti per il recovery e l'estrazione di file, o framenti di questi, presenti nello spazio non allocato o marcati cancellati: lazarus, Foremost, Scalpel. **Timeline:** La creazione di una timeline avviene mediante l'esecuzione di tre passaggi:Raccolta di informazioni sui file allocati(per ogni partizione), Raccolta dei metadati dallo spazio non allocato, creazione ed ordinamento della timeline. **Cattura traffico rete:**. Il traffico sniffato può essere full content (registra tutto:dumpcap, tcpdump, wireshark, snort), session oriented(memorizza le sessioni intercorse tra i comunicanti: fprobe, argus), statistico (fa un'analisi statistica). **Analisi del traffico di rete:** Estrazione di sessioni e contenuti:tcpflow, chaosreader, driftnet. Ricerca di contenuti: ngrep. Estrazione di informazioni sui sistemi coinvolti:p0f. **Livello esposizione sistema:** composta da 4 fasi: Acquisizione di informazioni relative al bersaglio (nmap, dnsquery, arping, xprobe2, smbscan), Discovery dei servizi e delle relative versioni (nmap,amap.), Analisi delle vulnerabilità (nessus,nikto), Exploit del sistema (metasploit).

Encase: Segue tutto il processo, dall'acquisizione all'analisi, e a linee generali permette di determinare se sono presenti i file incriminati. Formato da 3 componenti principali, encase **examiner** (sw installato sul computer autorizzato nel procedere alle operazioni di investigazione forense verso un dato host sottoposto ad analis), encase **safe** (il Secure Authentication For Encase facilita l'amministrazione degli utenti, traccia le varie transazioni, gestisce e controlla i privilegi d'accesso ai diversi dispositivi di rete. Per la comunicazione fra l'Examiner e le servlet viene utilizzato un canale di comunicazione crittato a garanzia della confidenzialità dei dati scambiati), encase **servlet** (è un piccolo servizio con un impatto minimo che deve venire installato sui sistemi; permette ad EnCase Examine di vedere, importare ed acquisire dati. Solo i computer dotati di tale servizio possono essere sottoposti ad esame o venire acquisiti)