DIIES Dipartimento di
INGEGNERIA
dell'INFORMAZIONE, delle INFRASTRUTTURE e dell'ENERGIA SOSTENIBILE

Corso di Tecnologie per la sicurezza informatica

Incident Response

Metodologie di Difesa

Vincenzo Calabrò

Agenda

- Introduzione
  - Definizioni
  - Maturity Model
  - Metodologie
- Incident Response: la risposta agli incidenti informatici
  - Definizione di un modello
  - Scoperta e notifica degli eventi
  - Valutazione degli eventi
  - Risoluzione degli eventi

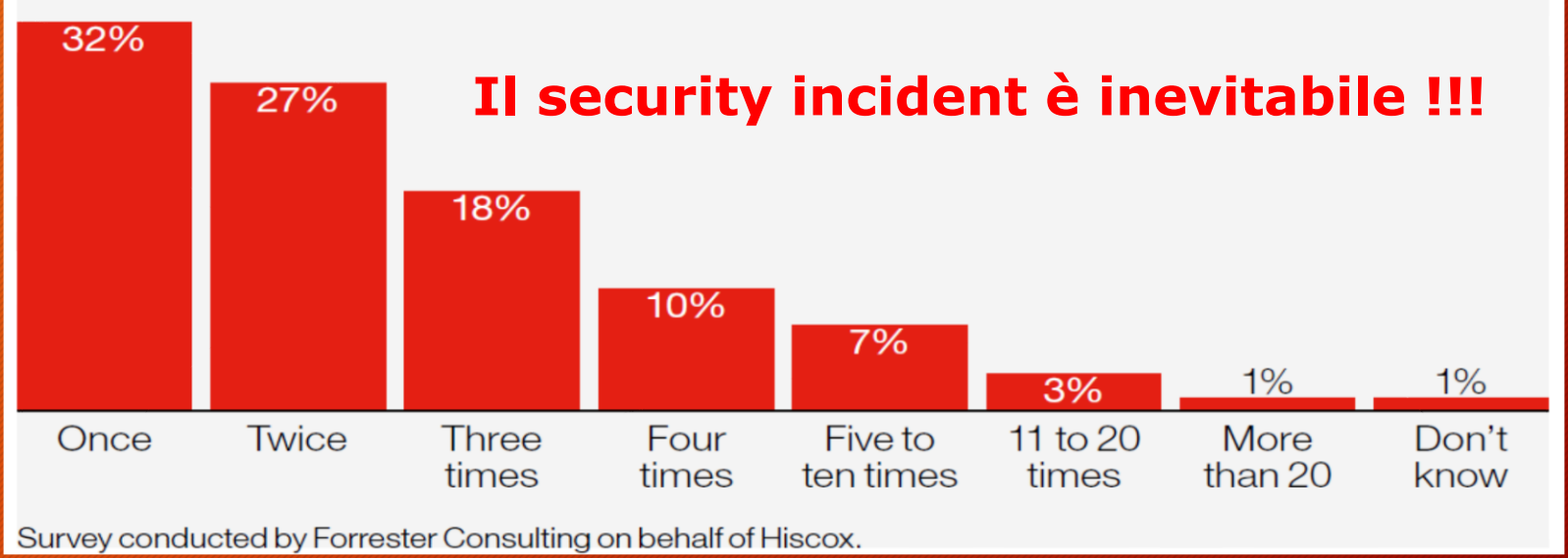
Introduzione

Definizioni

Metodologie

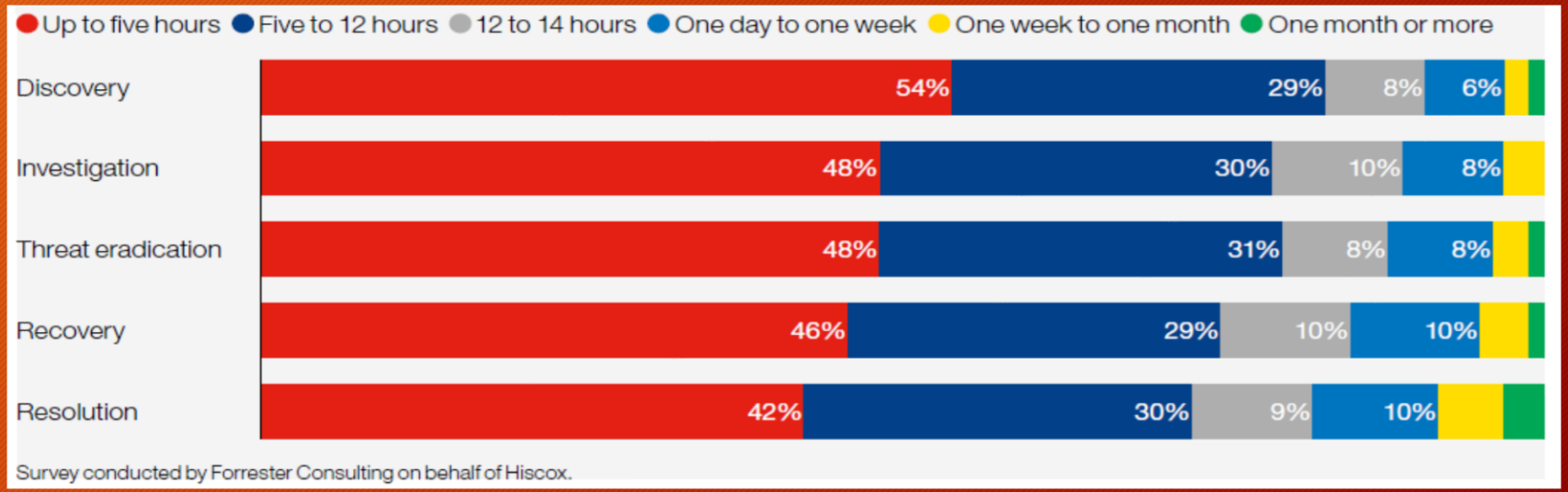
Il Security Incident è

- un evento interno o avverso che può influire sulle risorse delle organizzazioni e comprometterne gli obiettivi di sicurezza (Riservatezza, Integrità, Disponibilità, Controllo degli Accessi, ecc.)
- un evento, incidentale o accidentale, che indica che il sistema o i dati di un'organizzazione potrebbero essere stati compromessi oppure che le misure di sicurezza per proteggerli sono fallite



L'Incident Response è

- un processo coordinato per reagire alle conseguenze di un «security incident» e finalizzato al ripristino dell'operatività
- normalmente articolato in una sequenza di fasi:



Obiettivi dell'Incident Response

- Proteggere l'infrastruttura, i beni e le attività dell'organizzazione
- Limitare i danni alla reputazione o all'immagine
- Minimizzare i disservizi agli stakeholders
- Prevenire o ridurre le perdite o gli oneri
- Rispettare le normative vigenti
- Abbassare i tempi di risposta

Incident Response Maturity Model

THREAT AWARENESS

RESPONSE AGILITY

0. Non definito

Manca una visione diretta della security o la consapevolezza delle attività svolte, oppure sono fortemente decentralizzate

Response: Null
Awareness: Null

1. Consapevole

Vi è la consapevolezza che si stanno verificando incidenti informatici, ma non esiste alcuna preparazione per gestirli

Response: Pray
Awareness: Very Low

2. Reattivo

Si tenta di mitigare gli incidenti informatici in modo non strutturato, concentrandosi principalmente sulla risposta alla fase critica perché non sono ben definite le soglie di escalation

Response: Restore
Awareness: Low

3. Adattivo

Si investe e si sviluppano le risorse minime per il rilevamento e la risposta agli incidenti, sono presenti gli Incident Response Team

Response: Tool Driven
Awareness: Medium

4. Proattivo

Rappresenta un modello ottimizzato e replicabile, include attività per la risposta automatizzata agli incidenti.
L'Incident Response Program contribuisce alla strategia di sicurezza e alimenta la gestione delle crisi e dei programmi di continuità operativa

Response: Threat Driven
Awareness: High

5. Predittivo

Il modello è in grado di intraprendere azioni proattive basandosi sull'analisi delle minacce.
La sicurezza integra il rischio aziendale e diventa un processo strategico per il raggiungimento degli obiettivi

Response: Intelligence Driven
Awareness: Very High

ISO/IEC 27000-series

- La serie ISO/IEC 27000 - **Information security management systems** raggruppa un insieme di norme che hanno lo scopo di proteggere le informazioni che vengono mantenute ed elaborate da un'organizzazione.
- Attraverso questa famiglia di standard, le organizzazioni possono sviluppare ed implementare un proprio framework per la gestione della sicurezza delle proprie risorse informative.

ISO/IEC 27035-1:2016 ISO/IEC 27035-2:2016

Information security incident management

Part 1: Principles of incident management - Part 2: Guidelines to plan and prepare for incident response

ISO/IEC 27041:2015

Guidance on assuring suitability and adequacy of incident investigative method

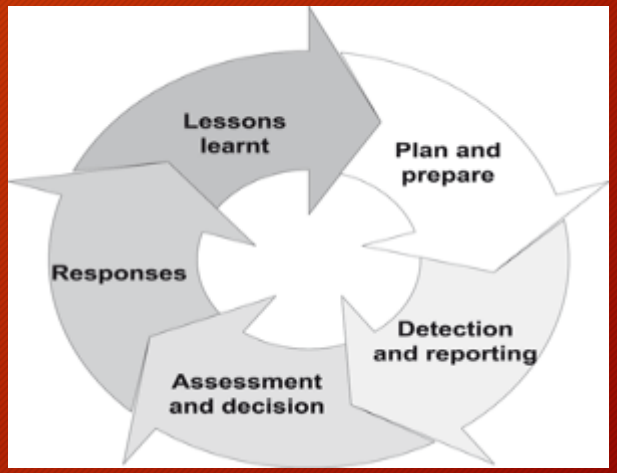
ISO/IEC 27043:2015

Incident investigation principles and processes

ISO/IEC 27035

Lo standard 27035 fornisce delle linee guida per l'implementazione di procedure e controlli al fine di creare un approccio strutturato per la gestione degli incidenti informatici. Tale standard ha come obiettivo la minimizzazione degli impatti negativi che un incidente informatico può avere sul business aziendale, attraverso il contenimento dell'incidente, la rimozione della causa scatenante, l'analisi delle conseguenze e il successivo controllo di non occorrenza.

Per poter garantire il raggiungimento degli obiettivi appena descritti il processo di gestione degli incidenti viene suddiviso in cinque fasi, ciascuna contenente determinate attività, incluse in un ciclo che dall'ultima ritorna poi alla prima.



ISO/IEC 27035-key stages

1. **Prepare** (Pianificazione e preparazione)
   (a) politiche di gestione degli incidenti di sicurezza
   (b) politiche di gestione della sicurezza e dei rischi
   (c) sistema di gestione degli incidenti di sicurezza
   (d) formazione dell'ISIRT
   (e) supporto (tecnico e di altro tipo)
   (f) formazione sulla consapevolezza nella gestione degli incidenti di sicurezza
   (g) test del sistema di gestione degli incidenti di sicurezza
2. **Identify** (Scoperta e notifica)
   scoperta di un incidente e notifica alle appropriate funzioni aziendali
3. **Assess** (Valutazione e decisione)
   valutazione dell'evento e decisione di classificarlo come evento di sicurezza

ISO/IEC 27035-key stages

4. **Respond of incident** (Risposta)
   (a) risposte agli incidenti di sicurezza informatica, ivi incluse operazioni di analisi forense
   (b) riprendersi da un incidente di sicurezza informatica
5. **Learn the lessons** (Lezioni apprese)
   (a) analisi forensi più approfondite (se necessario)
   (b) identificazione della lezione appresa
   (c) identificazione e attuazione dei miglioramenti al sistema di sicurezza
   (d) identificazione e attuazione dei miglioramenti alle valutazioni dei rischi di sicurezza
   (e) identificazione e attuazione dei miglioramenti al sistema di gestione degli incidenti di sicurezza

ISO/IEC 27041

La ISO/IEC 27041 «Guidance on assuring suitability and adequacy of incident investigative method" fornisce una guida sui meccanismi per garantire che i metodi e i processi utilizzati nelle indagini sugli incidenti di sicurezza delle informazioni siano "adatti allo scopo".

Include le migliori metodologie per:

- la definizione dei requisiti,
- la descrizione dei metodi,
- la dimostrazione che le implementazioni dei metodi sono in grado di soddisfare i requisiti,
- la verifica dei test sui fornitori esterni utilizzabili per assistere il processo di validazione.

ISO/IEC 27043

La ISO/IEC 27043 «Incident investigation principles and processes» fornisce le linee guida basate sui modelli idealizzati per processi di investigazione su incidenti comuni che coinvolgono prove digitali.

Ciò include i processi che vanno dalla preparazione pre-incidente fino alla chiusura delle indagini, nonché qualsiasi altro suggerimento generale e alert su tali processi.

Le linee guida descrivono i processi e i principi applicabili a diversi tipi di indagini, inclusi, a titolo esemplificativo ma non esaustivo:

- Accesso non autorizzato
- Alterazione/perdita dei dati
- Arresti anomali del sistema
- Violazioni della sicurezza delle informazioni aziendali

Incident Response

la risposta agli incidenti informatici

Incidente informatico

- **Nel momento in cui uno degli elementi di sicurezza previsti e in uso all'interno dell'azienda viene aggirato**, ad esempio nel caso in cui un utente riesca ad avere accesso ad un sistema a cui non è autorizzato ad accedere, **accade ciò che viene definito incidente informatico** di sicurezza: *"un singolo od una serie di eventi di sicurezza informatica inaspettati o non voluti, che hanno significativa probabilità di compromettere le attività aziendali e minacciare la sicurezza delle informazioni"*.
- L'evento di sicurezza informatica appena menzionato viene definito come *"l'identificata occorrenza di uno stato di sistema, di servizio o di rete che indica una possibile violazione della sicurezza delle informazioni, delle policy o il fallimento dei controlli previsti, o di una situazione precedentemente sconosciuta che potrebbe essere rilevante ai fini della sicurezza"*

Incident response

- **L'organizzazione, al verificarsi di eventi di sicurezza, deve essere in grado di verificare rapidamente se tale evento vada considerato un incidente informatico o meno ed eventualmente mettere in atto una serie di metodiche al fine di poter reagire efficacemente alla minaccia rilevata, attraverso le cosiddette attività di incident response.**
- Tali attività hanno l'obiettivo di garantire la tempestiva identificazione dell'evento, la sua eventuale classificazione in "incidente informatico", le conseguenti operazioni da svolgere tempestivamente nel momento in cui l'evento viene segnalato e le successive attività di investigazione atte a reperire possibili fonti di prova.

Incident response: finalità

Lo scopo dell'Incident response non si limita alla gestione dell'evento, ma interagisce anche con le altre fasi del ciclo di security assessment.

A tal fine distinguiamo:

- **Fase Predittiva / Proattiva**: finalizzata all'analisi dei rischi che possono favorire gli incidenti informatici, le cause scatenanti e le soluzioni per mitigare gli effetti.
- **Fase Reattiva:** in cui vengono definite le modalità, i ruoli e le azioni che devono portare alla **r**isoluzione degli incidenti informatici.
- **Fase Correttiva / Migliorativa**: in cui si esaminano gli incidenti subiti e si studiano le soluzioni idonee ad evitare che riaccadano.

Incident Response Life Cycle

Prima: PREPARE

- PEOPLE: INCIDENT RESPONSE TEAM
- PROCESS: INCIDENT RESPONSE PLAN
- TECH: INCIDENT RESPONSE PLATFORM
- IMPROVEMENT PROGRAM

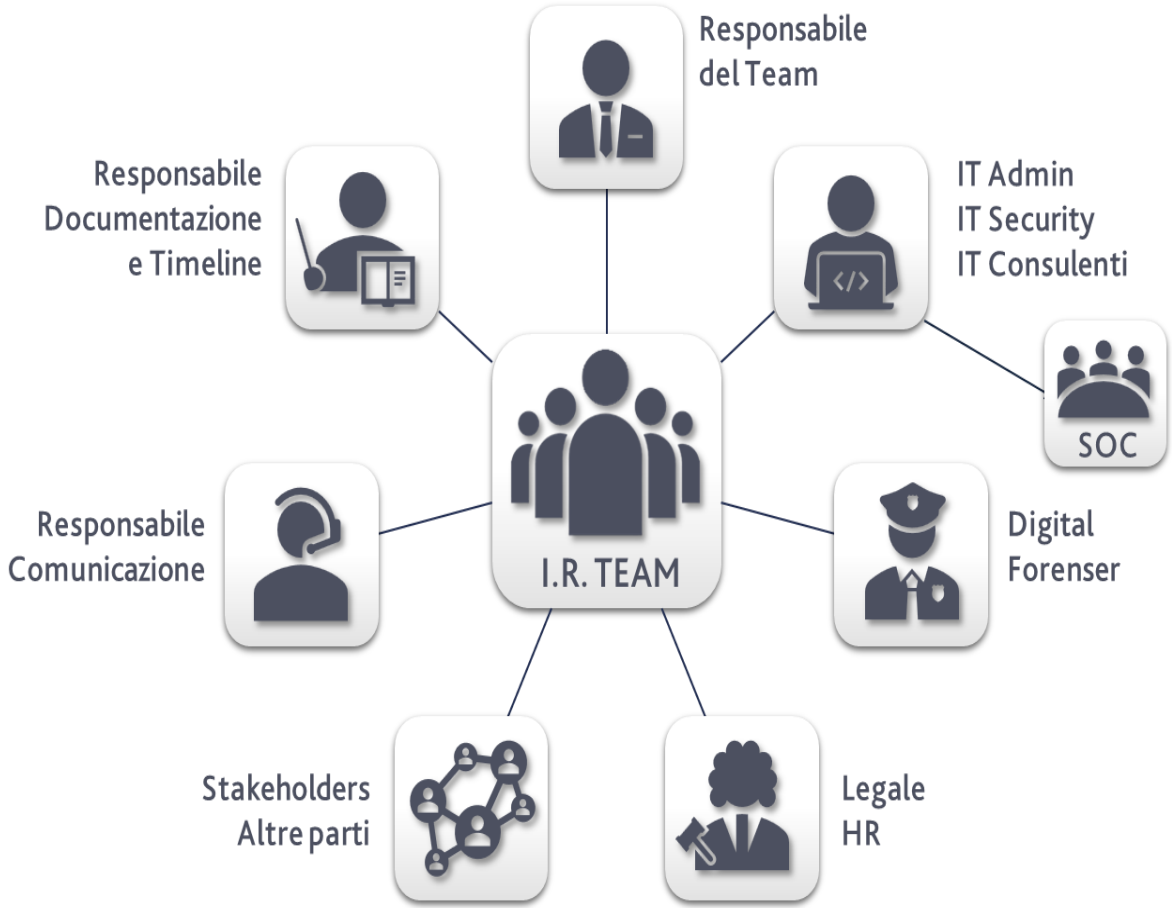
Durante: DETECT & RESPOND

- IDENTIFICAZIONE DELL'EVENTO
- CONTENIMENTO DEGLI EFFETTI
- RIMOZIONE DELLA MINACCIA
- RIPRISTINO DELL'OPERATIVITÀ

Dopo: FOLLOW UP

- DIGITAL FORENSICS
- ANALISI DELL'EVENTO
- LEZIONE DI APPRENDIMENTO
- CONDIVISIONE DEL CASO

Cosa fare prima: People
Incident Response Team



QUAL È L'OBIETTIVO DELL'I.R.TEAM?

- L'obiettivo principale consiste nel coordinare e valutare le risorse principali e i membri del team durante un incidente di sicurezza informatica per ridurre al minimo l'impatto e ripristinare l'operatività il più rapidamente possibile

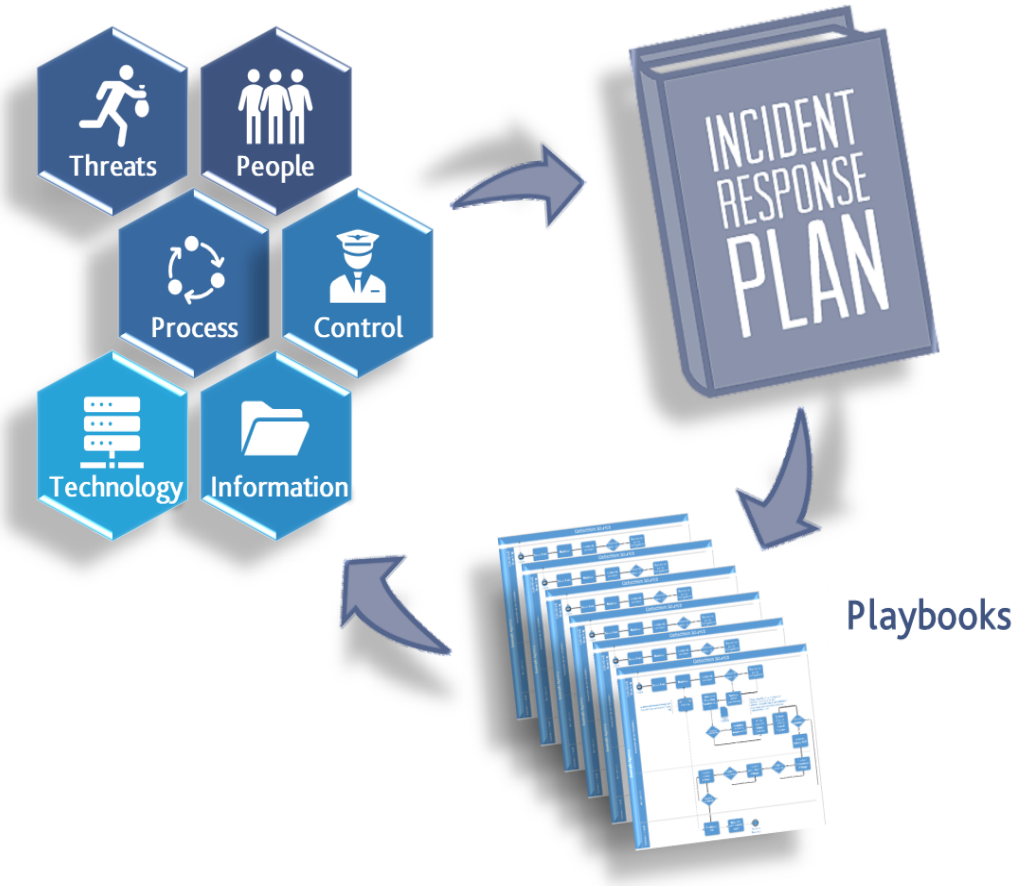
CHE COSA FA UN I.R.TEAM?

- Analizza le informazioni raccolte (regola 5 W)
- Risponde agli incidenti informatici
- Gestisce le comunicazioni interne ed esterne
- È responsabile della notifica dell'incidente alle agenzie governative
- Verifica periodicamente le procedure dell'IR

QUALI COMPETENZE SONO NECESSARIE?

- Cercare denominatori ed eccezioni comuni
- Fare affermazioni e non ipotesi
- Eliminare l'impossibile
- Cercare sempre la spiegazione più semplice
- Ragionare come un hacker

Cosa fare prima: Process
Incident Response Plan



QUAL È L'OBIETTIVO DELL'I.R.PLAN?

- Formalizzare i ruoli e le responsabilità
- Gestire una serie completa di risposte agli incidenti informatici pertinenti all'organizzazione per cui è stato elaborato

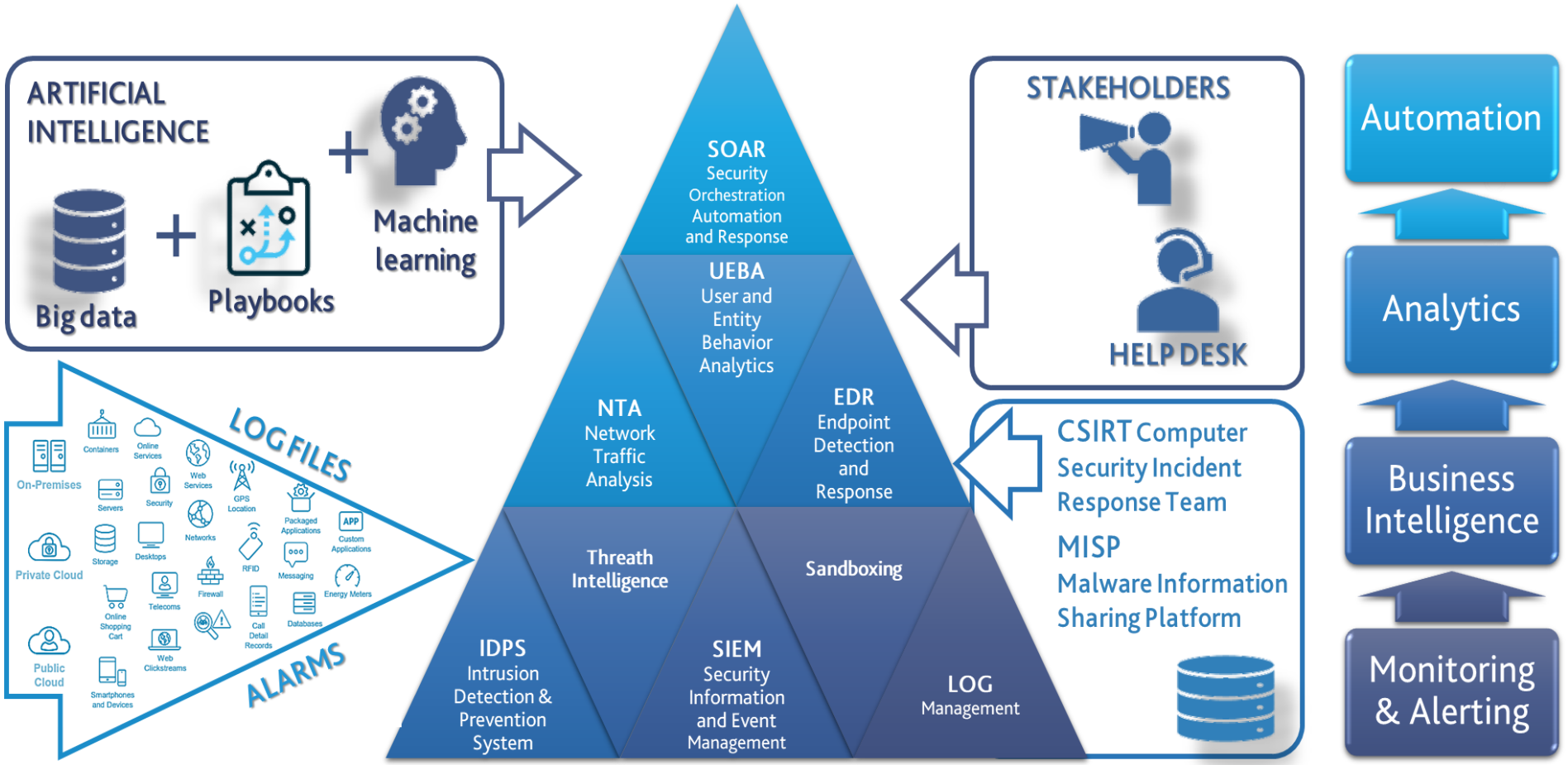
COME SI SVILUPPA UN I.R.PLAN?

- Effettuare una valutazione delle criticità
- Eseguire un'analisi realistica delle minacce
- Considerare le implicazioni sulle persone, sui processi, sulle tecnologie e sulle informazioni
- Creare modelli di risposta appropriati (Playbook)
- Rivedere periodicamente la capacità di risposta

QUALI SONO LE CRITICITÀ DI UN I.R.PLAN?

- Obsolescenza per carenza di aggiornamenti
- Complessità delle procedure da adottare
- Scarsa condivisione con gli stakeholders

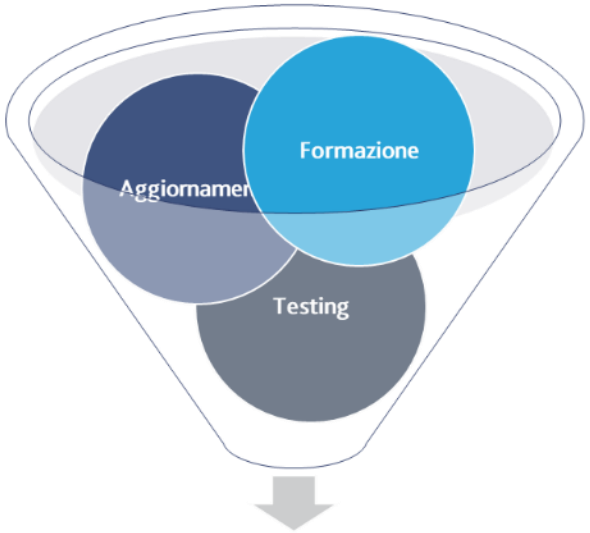
Cosa fare prima: Tech
Incident Response Platform



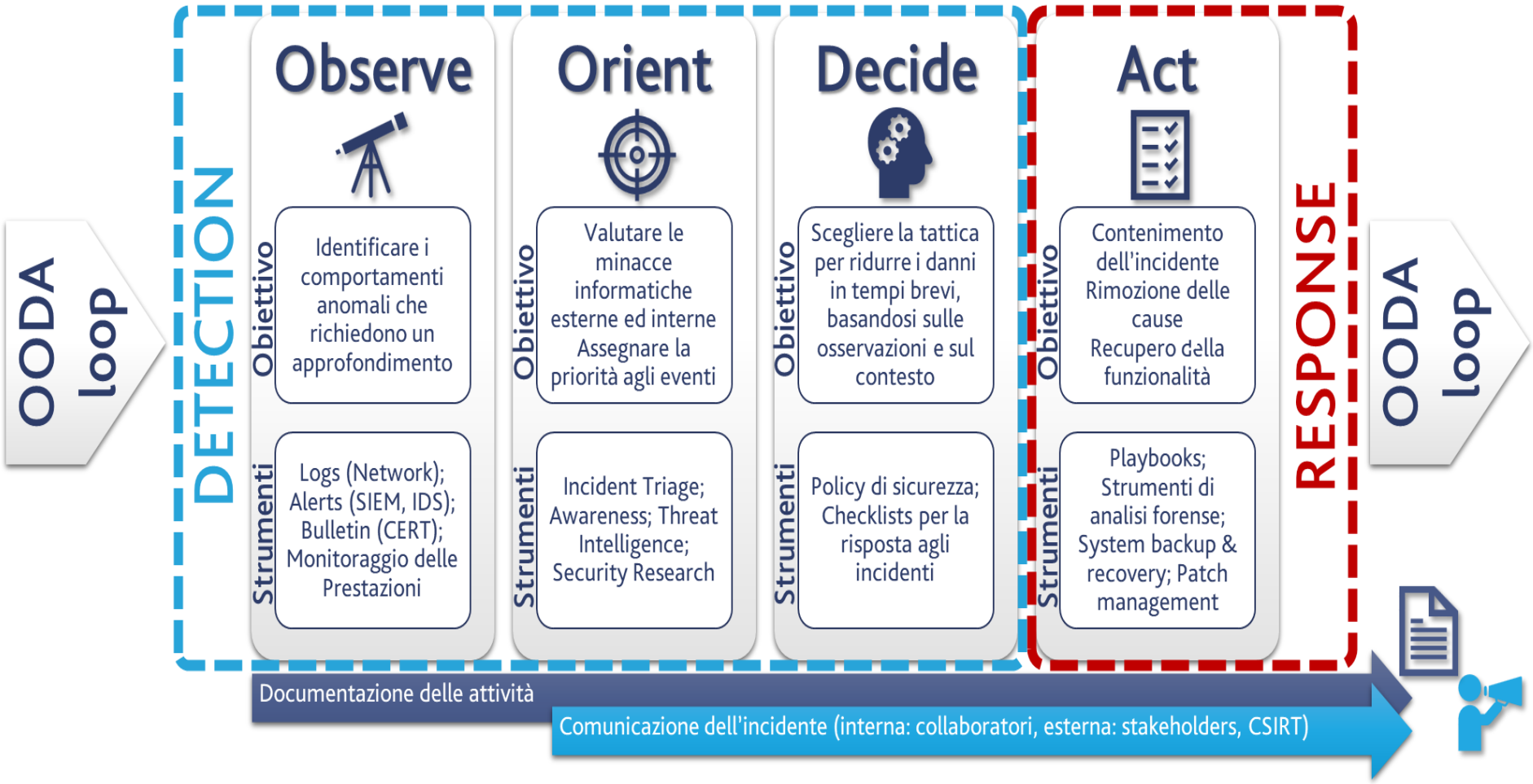
Cosa fare prima:
Improvement Program

Rivedere periodicamente il proprio stato di preparazione all'incident response

Attività	Formazione	Aggiornamento	Testing
People	✓		✓
Plan		✓	✓
Platform		✓	✓



Cosa fare durante: Detection & Response



Scoperta e notifica degli eventi

All'interno di un sistema di gestione degli incidenti di sicurezza, si entra nella fase di scoperta e notifica di un evento di sicurezza informatica nel momento in cui viene riscontrata e comunicata l'occorrenza di un evento di sicurezza o la scoperta di una vulnerabilità all'interno dei sistemi in uso.

Tale scoperta può avvenire mediante il supporto di sistemi di monitoraggio o da personale direttamente o indirettamente coinvolto nell'utilizzo dei sistemi, come ad esempio:

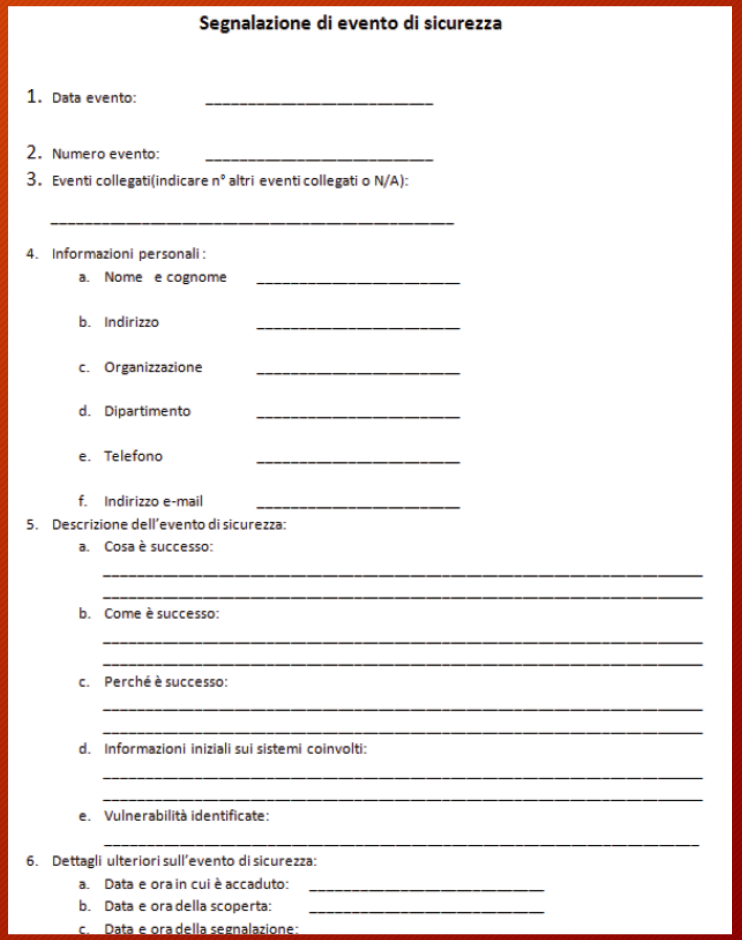
- notifiche provenienti da sistemi di monitoraggio (Es. antivirus, sistema di monitoraggio della rete, analisi di file di log di sistemi o server)
- notifiche da parte degli utilizzatori dei sistemi
- informative provenienti da enti esterni, come ISP5, fornitori o servizi che forniscono consulenza di sicurezza informatica
- responsabili della sicurezza
- dipartimento IT interno all'azienda
- clienti
- siti web di pubblica informazione (es. blog sulla sicurezza)
- mezzi di informazione di massa (tv, giornali).

Modulo di segnalazione evento

La persona (aiutata o meno dagli strumenti automatici) che nota un evento di sicurezza informatica è tenuto a segnalarlo tempestivamente al PoC (Point of Contact) oppure al ISIRT che procederà con la valutazione dell'evento.

Il modulo utilizzato per segnalare l'evento dovrebbe contenere come minimo le seguenti informazioni, indispensabili per poter effettuare l'analisi:

- data e ora della scoperta
- osservazioni
- informazioni di contatto



Segnalazione di evento di sicurezza

1. Data evento: _____
2. Numero evento: _____
3. Eventi collegati(indicare n° altri eventi collegati o N/A):

   _____
4. Informazioni personali :
   a. Nome e cognome _____
   b. Indirizzo _____
   c. Organizzazione _____
   d. Dipartimento _____
   e. Telefono _____
   f. Indirizzo e-mail _____
5. Descrizione dell'evento di sicurezza:
   a. Cosa è successo:
      _____
      _____
   b. Come è successo:
      _____
      _____
   c. Perché è successo:
      _____
      _____
   d. Informazioni iniziali sui sistemi coinvolti:
      _____
      _____
   e. Vulnerabilità identificate:
      _____
6. Dettagli ulteriori sull'evento di sicurezza:
   a. Data e ora in cui è accaduto: _____
   b. Data e ora della scoperta: _____
   c. Data e ora della segnalazione:

Valutazione degli eventi

Non appena il PoC riceve il modulo di segnalazione di evento di sicurezza, deve effettuare la sua valutazione per decidere se l'evento segnalato sia da considerare come un possibile (o già concluso) evento di sicurezza o un falso allarme.

Se viene identificato come un falso allarme, deve comunque completare il modulo ed inviarne una copia al l'ISIRT e alla persona che ha effettuato la segnalazione.

Se, invece, valuta che l'evento è un incidente di sicurezza e possiede delle competenze adeguate, lui stesso potrebbe svolgere ulteriori azioni di analisi e approfondimento per individuare, ad esempio, ulteriori misure di controllo immediate.

In ogni caso, l'incidente va segnalato all'ISIRT così che si possa procedere ad ulteriori valutazioni e decisioni da parte del team preposto allo svolgimento di tali attività.

Durante la valutazione il PoC deve reperire il maggior numero di informazioni possibile. In particolare, dovrebbe essere in grado di fornire le seguenti informazioni:

- informazioni generali sull'incidente: che tipo di incidente è, da chi o da che cosa è stato causato, su cosa potrebbe influire e cosa è stato fatto fin'ora per gestire tale incidente;
- conseguenze dell'incidente: bisogna valutare quale dei pilastri della sicurezza informatica è stato violato, quindi identificare se come conseguenza si sia ottenuto il rilascio o la modifica di informazioni senza autorizzazione, il ripudio di informazioni, la non disponibilità di informazioni o servizi o la distruzione di informazioni o servizi.

Valutazione degli eventi

Se l'incidente di sicurezza informatica venisse risolto in questa fase, il PoC dovrebbe completare il modulo inserendo tutte le azioni effettuate ed eventuali "lesson learned" ed inviare il modulo all'ISIRT per la revisione e l'archiviazione.

Sebbene, in generale, la maggior parte delle situazioni normalmente implichi il passaggio di testimone all'ISIRT per la valutazione finale, vi possono essere dei casi in cui il PoC ritenga l'incidente particolarmente grave, per cui debba contattare direttamente la persona a capo dell'ISIRT e scalare la segnalazione all'unità di crisi, che si occuperà del caso.

L'ISIRT ha la responsabilità di prendere la decisione finale in merito all'occorrenza o meno di un possibile incidente di sicurezza. Una volta ricevuto da parte del PoC il modulo, compilato in modo più o meno dettagliato, la persona contattata deve rivederne il contenuto e raccogliere più informazioni utili a valutare l'incidente, che può essere ridotto a falso allarme o essere confermato.

Risoluzione degli eventi

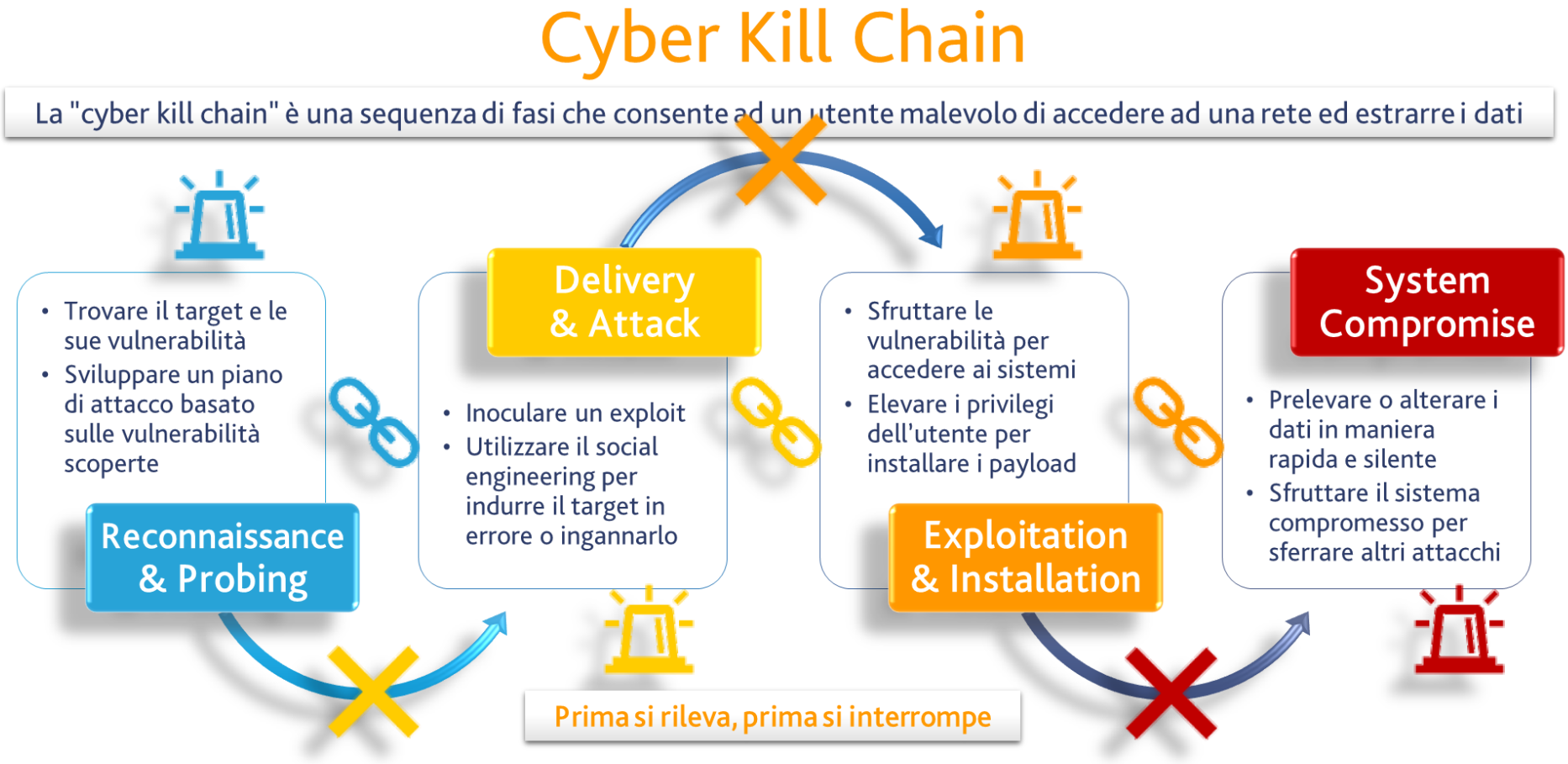
Una volta effettuata l'analisi dell'evento, la gestione dell'incidente, inclusa la risposta immediata ed eventuali azioni aggiuntive, va prioritizzata a seconda della criticità e degli impatti sull'azienda.

L'unità di crisi, che prende in carico la gestione dell'evento, deve conoscere e applicare le modalità operative codificate e idonee a mitigare i danni e rimuovere il problema, in caso contrario, in collaborazione con il responsabile dell'ISIRT dovrà individuare le soluzioni più opportune.

Quest'ultima opzione presuppone che:

- Non è stata eseguita una corretta valutazione dei rischi
- Non sono state previste adeguate misure di contenimento/risoluzione
- Non è stata sviluppata un'idonea fase di formazione/informazione

Criticità: Incident Triage



Alcuni esempi di Incident Triage

Evento	Kill Chain Stage	Priorità	Azione Consigliata
Port-scannig activity	Reconnaissance & Probing	Low	Ignorare la maggior parte di questi eventi tranne se l'IP di origine non abbia una cattiva reputazione o ci siano più eventi dallo stesso IP in un breve lasso di tempo
Malware Infection	Delivery & Attack	High	Correggere le eventuali infezioni da malware il più rapidamente possibile prima che progrediscano. Analizzare il resto della rete per individuare eventuali apparati compromessi
Distribuited Denial of Service	Exploitation & Installation	High	Configurare i server Web per la protezione dalle richieste di HTTP e SYN FLOOD. Filtrare le richieste durante un attacco per bloccare gli IP di origine
Distribuited Denial of Service (diversivo)	Exploitation & Installation	High	A volte un DDOS viene utilizzato per distogliere l'attenzione da un altro tentativo di attacco più serio. Aumentare il monitoraggio e indagare su tutte le attività correlate
Unauthorized access	Exploitation & Installation	Medium	Abilitare il monitoraggio sui tentativi di accesso non autorizzati, con priorità su quelli critici e / o contenenti dati sensibili

Alcuni esempi di Incident Triage

Incidente	Kill Chain Stage	Priorità	Azione consigliata
Insider Breach	System Compromise	High	Identificare gli account utente privilegiati per tutti i domini, server, app e dispositivi critici. Assicurarsi che il monitoraggio sia abilitato per tutti i sistemi e per tutti gli eventi di sistema e assicurarsi che stiano alimentando la tua infrastruttura di logs
Unauthorized Privilege Exclalaion	Exploitation and Installation	High	Configurare i sistemi critici per registrare tutti gli eventi di escalation dei privilegi e impostare gli allarmi per i tentativi di escalation dei privilegi non autorizzati
Destructive attack (data, system, etc)	System Compromise	High	Eseguire il backup di tutti i dati e i sistemi critici. Testare, documentare e aggiornare le procedure di ripristino del sistema. Durante una compromissione: acquisire le prove con attenzione e documentare tutte le fasi e tutti i dati probatori raccolti
Advanced Persistent Threat (APT) or Multistage Attack	All Stages	High	Considerare ciascun evento in un contesto più ampio, che includa le informazioni sulle minacce più recenti
False Allarms	All Stages	Low	Configurare la piattaforma di Incident Response per ottenere la giusta quantità di segnale-rumore

MITRE ATT&CK https://attack.mitre.org/

MITRE ATT&CK (***Adversarial Tactics, Techniques and Common Knowledge***) è una risorsa di conoscenze di tattiche e tecniche di attacco basate su osservazioni del mondo reale.

- una **Tattica** è una descrizione di alto livello del comportamento di un attaccante
- una **Tecnica** rappresenta una descrizione dettagliata di una determinata Tattica.

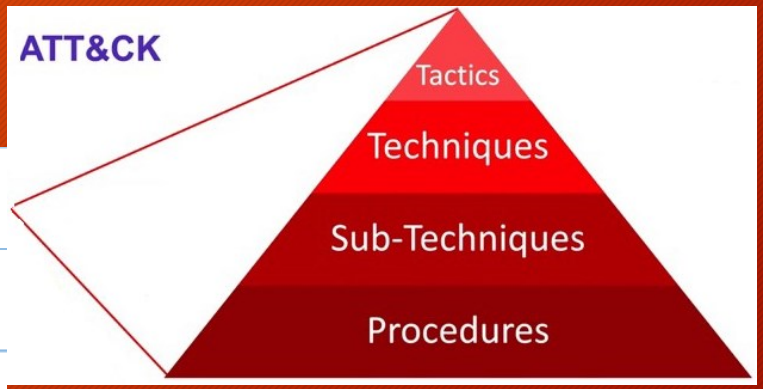
Le informazioni contenute nel ATT&CK vengono utilizzate come base per lo sviluppo di modelli e metodologie di minacce specifici nel settore privato, nel governo e nella comunità di prodotti e servizi della sicurezza informatica.

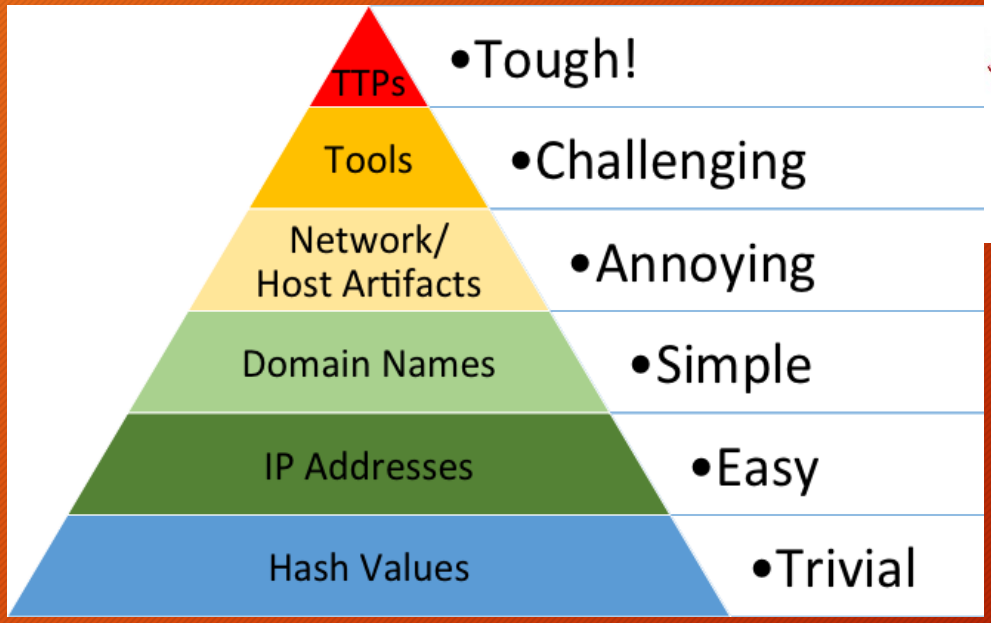
È free, open e accessibile a livello globale.

Chiunque può contribuire allo suo sviluppo.

David Bianco's Pyramid of Pain

- Un efficace sistema di Threat Intelligence deve essere in grado di negare gli indicatori di compromissione
- La piramide evidenzia che non tutti gli indicatori di compromissione sono uguali
- Gli indicatori in alto sono più efficaci



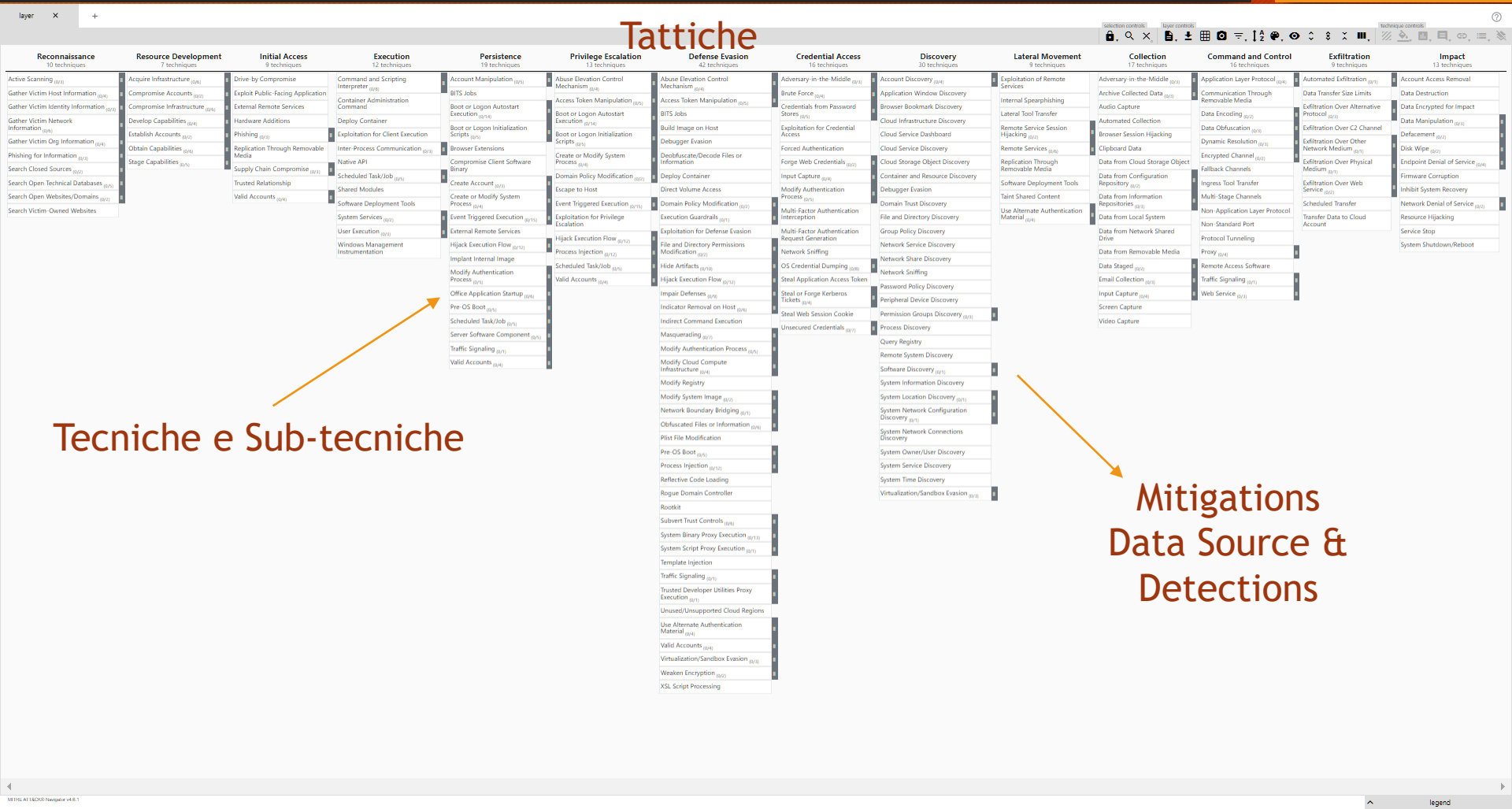


ATT&CK Matrices

- MITRE ATT&CK può essere usato come simulatore di scenari di rischio per valutare la risposta dell'organizzazione, ma ovviamente anche come checklist di cose da fare è cioè in senso proattivo.
- MITRE v.11 mette a disposizione 3 differenti matrici:
  - **Enterprise** (PRE, Windows, macOS, Linux, Cloud, Network, Containers)
  - **Mobile** (android, ios)
  - **ICS** (industrial control systems)

ATT&CK Navigator

Tattiche

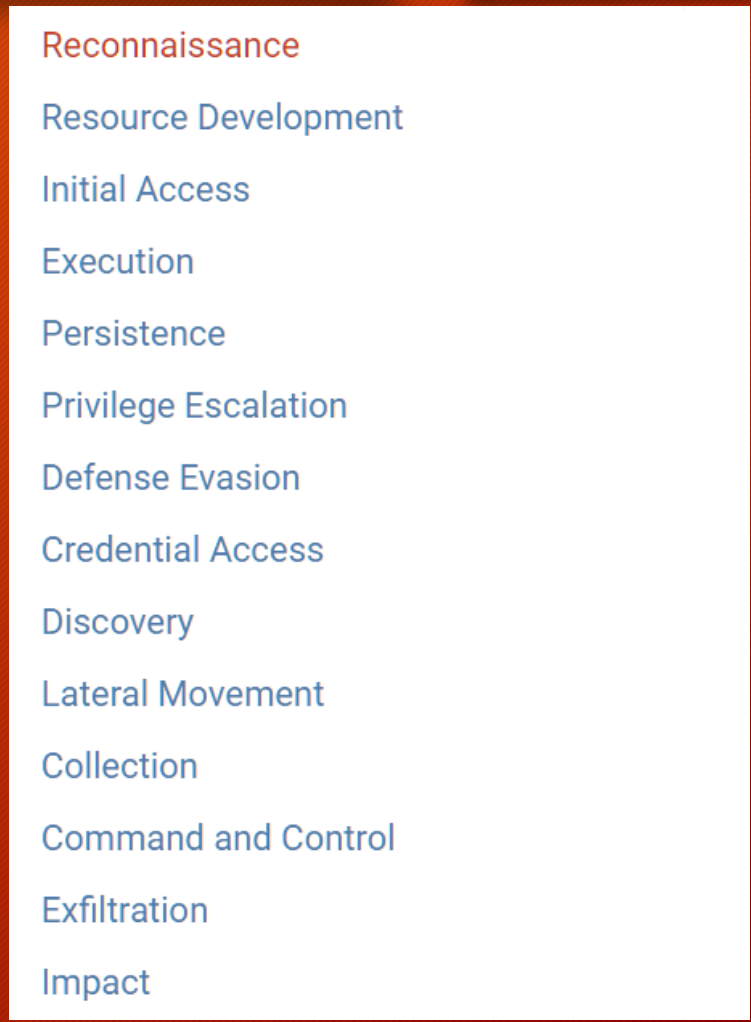


Tecniche e Sub-tecniche

Mitigations
Data Source &
Detections

ATT&CK Tactics

- Una **Tattica** è una descrizione di alto livello del comportamento di un attaccante
- È l'obiettivo intermedio dell'avversario durante un attacco
- Spiega il «***perché***» di ogni azione dell'attaccante
- Ogni tecnologia ha una lista di tattiche
- Ad ogni tattica è assegnato un ID univoco e può prevedere più specifiche tecniche



ATT&CK Technique

- Una **Tecnica** rappresenta una descrizione dettagliata di una determinata Tattica
- Si suddividono in **tecniche** e **sub-tecniche**
- Identificano «***come***» l'avversario effettuerà ogni azione con diversi livelli di dettaglio
- Ogni tecnologia ha una lista di tecniche
- Oltre ad indicare la tecnica o il codice utilizzato, possono altre informazioni quali:
  - Informazioni
  - Azioni per Mitigare l'attacco
  - Azioni per Rilevare l'attacco
  - Reference

ATT&CK Mitigations

- Identificano le configurazione, gli strumenti o i processi che possono «prevenire» una tecnica di attacco
- Suggeriscono le attività cambiare una regola di sicurezza o lo sviluppo di un tool
- Sono raccomandati per prevenire l'esecuzione di specifici attività degli avversari
- Le azioni di mitigation sono mappate per ogni specifica tecnica e sono visualizzate nella stessa pagina

ATT&CK data sources & detections

- Identificano come vengono utilizzati i dati e la detection per ogni specifica tecnica di attacco
- I dati sono le informazioni raccolte dai sensori o dai logs
- I dati sono fondamentali per identificare le attività dell'attacante
- La detection può rappresentare un processo di alto livello, un sensore, i dati e le strategie di detection
- L'interpretazione dei dati aiuta ad identificare la tecnica utilizzata dall'avversario

ATT&CK Groups and Software

- Identificano i gruppi e i tools che hanno utilizzato per prima la tattica di attacco
- Le tecniche di attacco si modificano nel tempo per cui il framework deve essere aggiornato frequentemente ed è in continua evoluzione
- Chiunque può contribuire allo sviluppo o correzione

Cosa fare dopo: Follow up

l'incidente va affrontato prima che si verifichi

prima — PREPARE

- Effettuare una risk analysis
- Eseguire una cyber security threat analysis
- Considerare le implicazione delle persone, dei processi, delle tecnologie e delle informazioni
- Creare un framework adeguato

durante — RESPOND

- Identificare un incidente di cyber security
- Valutare le minacce informatiche
  Assegnare la priorità agli eventi
- Scegliere la tattica migliore per rispondere rapidamente
- Contenere l'incidente
  Rimuovere le cause
  Recuperare la funzionalità

dopo — FOLLOW UP

- Indagare sull'incidente in maniera approfondita
- Segnalare l'incidente agli stakeholder e agenzie
- Realizzare una revisione del piano di incident response
- Condividere e approfondire la lezione appresa

Esercitazione

- Installare OSSIM e gli Agent HDIS su Windows e Linux
- Provare gli attacchi di Penetration Testing sulle macchine Windows e Linux
- Analizzare i risultati ottenuti su OSSIM
- Implementare le regole di incident response

Malware

Il termine malware (Malicious Software) indica un programma (un eseguibile, una libreria dinamica, uno script, una pagina html, un documento con macro, ecc.) avente effetti indesiderati e potenzialmente pericolosi per l'utente, come il furto di identità, la criptazione dell'hard disk, ecc.

Il ciclo di vita di un malware è composto di quattro fasi:

1. A-day: malware creato
2. 0-day: il malware viene rilasciato in pubblico ed è in grado di infettare i sistemi vulnerabili
3. D-day: prima opportunità per la rilevazione (detection)
4. R-day: scoperta della risoluzione (remediation)

Malware - analisi

Esistono sostanzialmente due tecniche per l'analisi del malware:

- **Analisi statica**: l'analisi è effettuata senza eseguire il malware, ma studiando il codice, qualora non sia offuscato.
  - **Base**: con questa metodologia l'esame è condotto senza guardare il codice, ma si effettua la scansione con i software antivirus (p.e. VirusTotal)
  - **Avanzata**: si utilizzano strumenti appositi di disassembling per capire la struttura di flusso e i dati del programma, analizzare le chiamate a sistema/API
- **Analisi dinamica:** in questo caso il malware viene eseguito in ambiente virtuale o in un sistema emulato allo scopo di monitorare il comportamento e, in particolare, le chiamate a sistema/API e l'attività di rete
  - **Base**: si esegue il malware in un ambiente sandbox e si monitorano i processi, le connessioni di rete, filesystem, voci di registro, ecc.
  - **Avanzata**: si sfruttano strumenti di debugging per l'esecuzione controllata riga per riga

Malware - comportamento

Generalmente un malware prima infetta un sistema e poi si propaga su altri sistemi. Per questo, l'architettura di un malware si basa su 4 aspetti:

- Meccanismo di infezione (*come trova una nuova vittima*)
  - Random scanning
  - Permutation scanning
  - Localized scanning
  - Hit-list scanning
  - Topological scanning
  - Meta server scanning
  - Passive scanning
- Meccanismo di propagazione/diffusione (*come di diffonde su altri host*)
  - Self-carried propagation
  - Embedded propagation
  - Secondary channel propagation
- Meccanismo di attivazione (*come verrà attivato*)
  - Attivazione umana
  - Attivato in base all'attività umana
  - Attivato da processi schedulati
  - Auto-attivazione
- Natura dell'attacco (*quando realizza gli effetti*)

Malware - condivizione

Per migliorare la capacità di risposta ai malware e più in generale agli attacchi informatici è necessario condividere le informazioni sugli attacchi.

Si condividono:

- **Indicatori di Compromissione (IoC)**: artefatti osservati in una rete o all'interno di un sistema che con un'alta probabilità è correlabile, o indica, un'intrusione;
- **Indicatori di Compromissione (IoA):** artefatti che consentono ai team di sicurezza di sviluppare un approccio più proattivo alle investigazioni, aiutandoli ad identificare e comprendere in modo rapido quali sono le azioni più comuni che un criminale informatico deve condurre se desidera avere successo.

Protocolli più noti:

- STIX (Structured Threat Information eXpression): linguaggio
- TAXII (Trusted Automated eXchange of Intelligence Information): protocollo
- OpenIOC (Open Indicators of Compromise): linguaggio
- TLP (Traffic Light)Protocol: protocollo di condivisione

Fine

vincenzo.calabro@unirc.it

linkedin.com/in/vincenzocalabro