Incident Response

Cosa fare prima, durante e dopo un cyber attacco

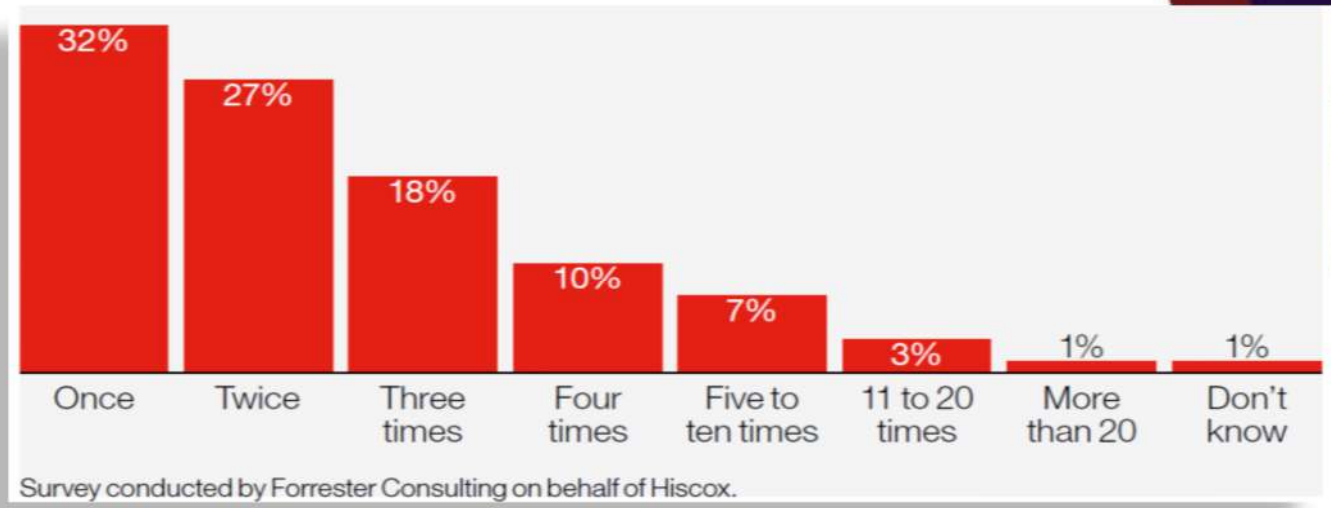
Vincenzo Calabrò
Referente Informatico e Funzionario alla Sicurezza CIS,
Professore a contratto di Tecnologie per la Sicurezza Informatica

Forum ICT Security, Roma, 16 ottobre 2019

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**

Negli ultimi 12 mesi, quante volte la vostra organizzazione ha subito un **«security incident»**?



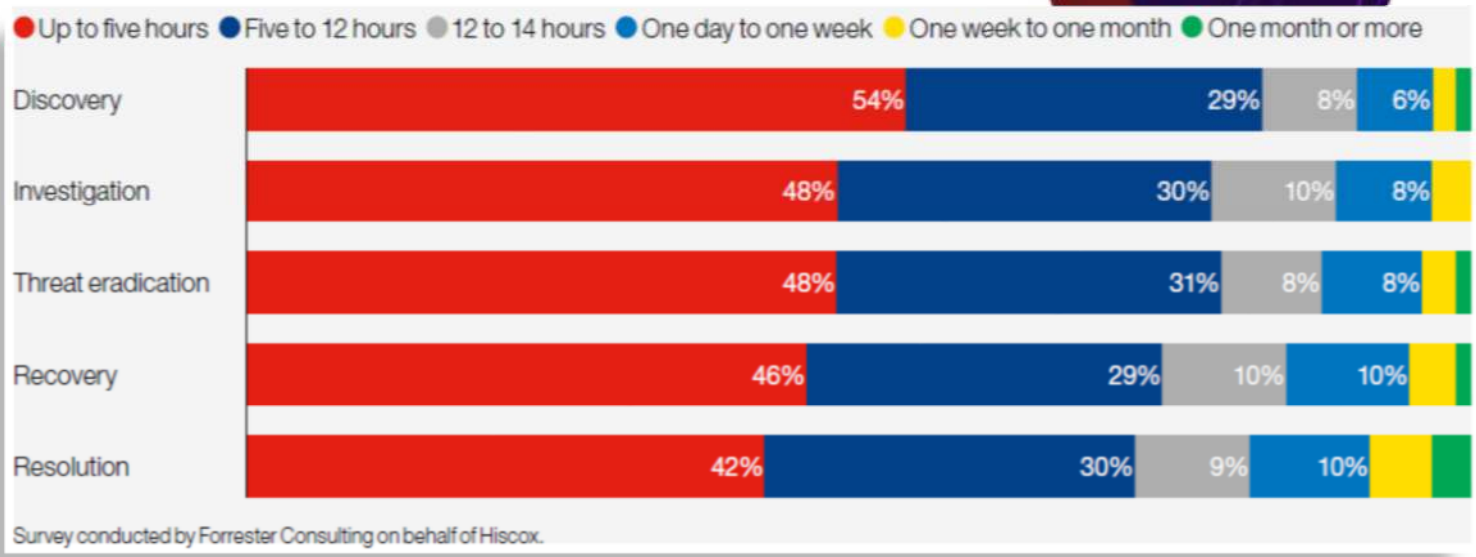
Il security incident è inevitabile !!!

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:**

Quanto tempo è stato speso per risolvere un **«security incident»?**

Il tempo è prezioso



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

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

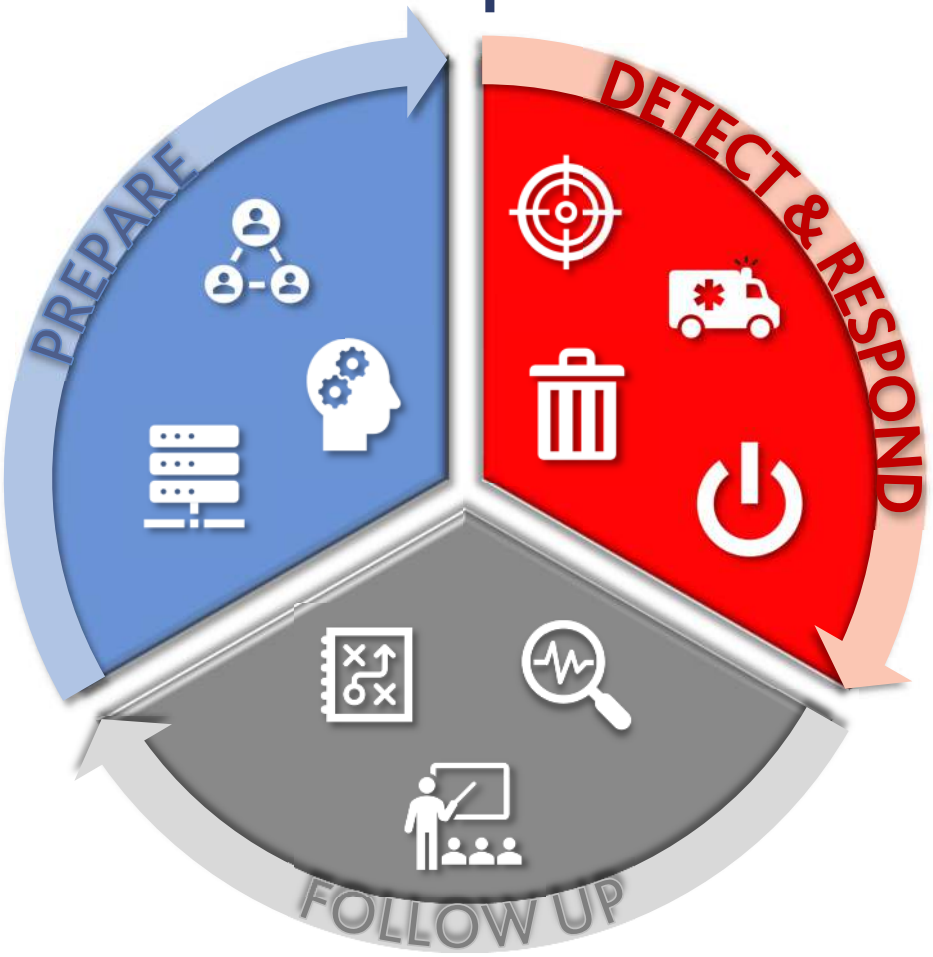
5. Predittivo

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

RESPONSE AGILITY

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

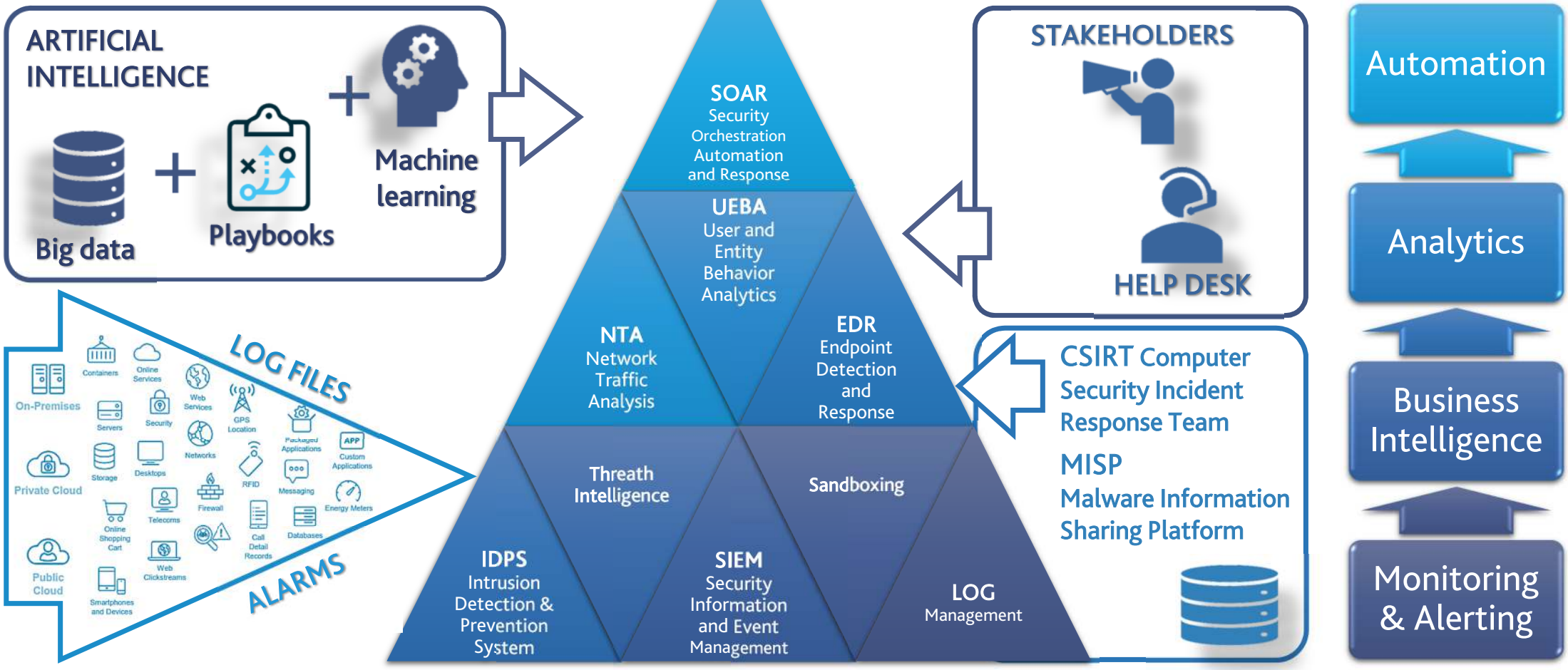
COME SI SVILUPPA UN I.R.PLAN?

- 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

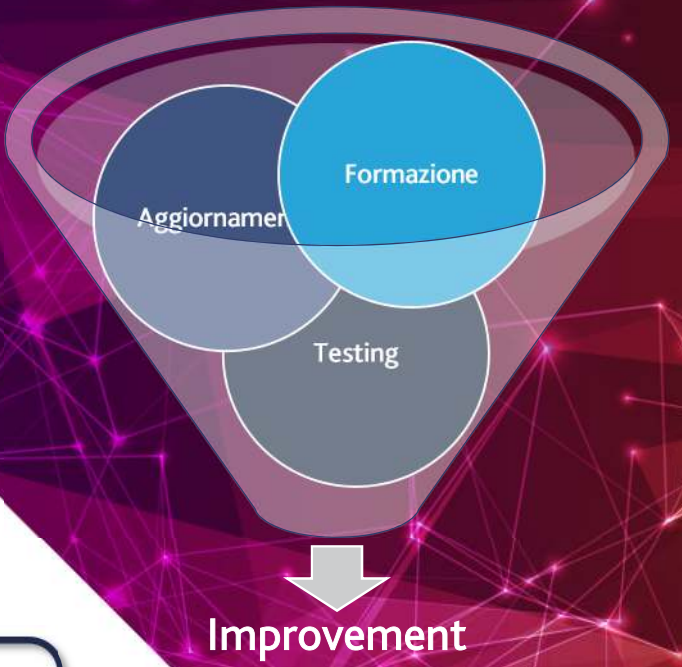
Cosa fare prima: Tech → Incident Response Platform



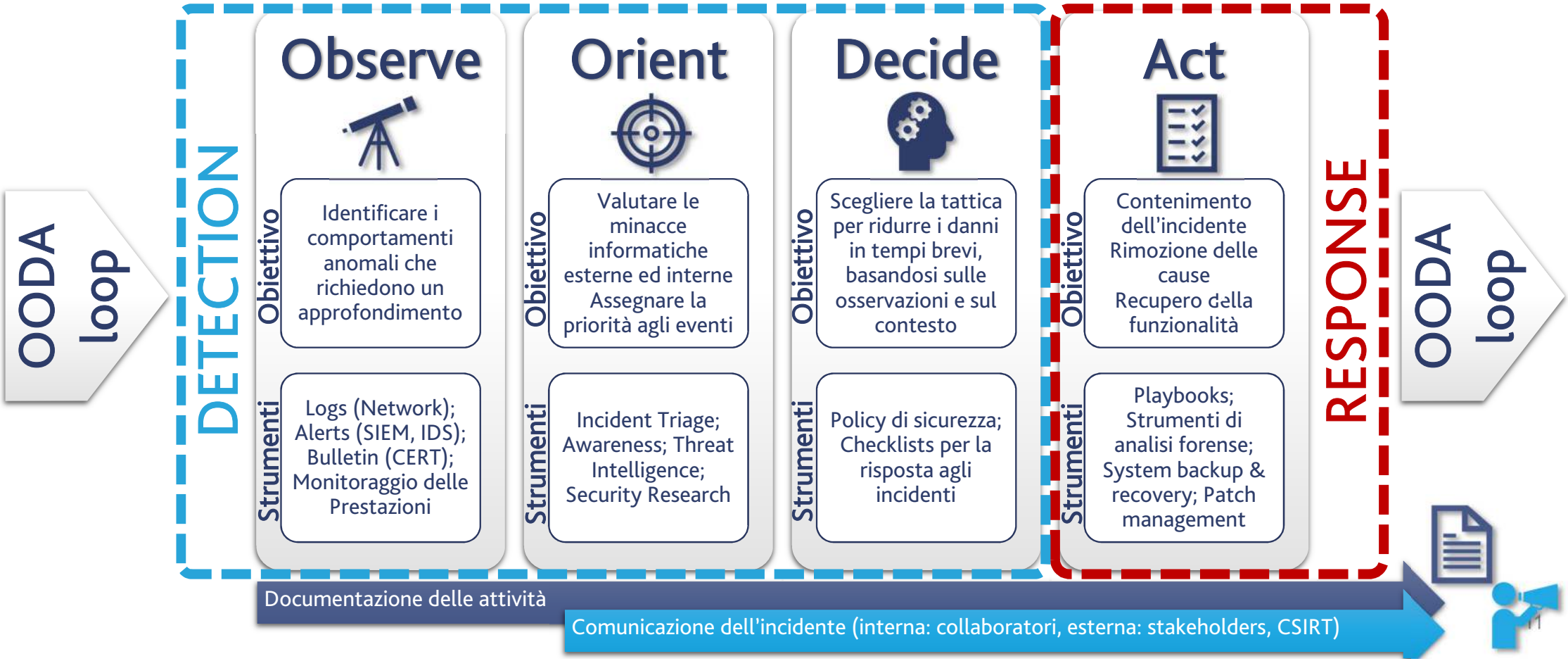
Cosa fare prima:
Improvement Program

Rivedere periodicamente il proprio stato di preparazione all'incident response

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



Cosa fare durante: Detection & Response



Criticità: Incident Triage → Cyber Kill Chain

La "cyber kill chain" è una sequenza di fasi che consente ad un utente malevolo di accedere ad una rete ed estrarre i dati

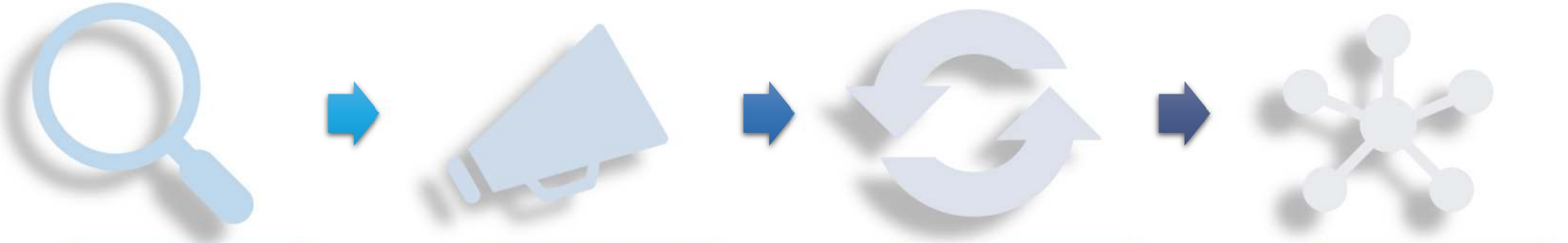
Prima si rileva, prima si interrompe

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

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

Cosa fare dopo: Follow up



Indagare sull'incidente in maniera approfondita

Segnalare l'incidente agli stakeholder e alle agenzie governative

Realizzare una revisione del piano di incident response

Condividere e approfondire la lezione appresa

In sintesi: 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

Reference

- A. Shostack, A. Stewart, The New School of Information Security, 2008
- D. Murdoch, Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02), 2019
- E.C. Thompson, Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents, 2019
- NIST Computer Security Incident Handling Guide
  https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
- NIST Guide to Integrating Forensic Techniques into Incident Response
  https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response
- NIST Security and Privacy Controls for Federal Information Systems and Organizations
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- SANS Incident Response Checklists – https://www.sans.org/score/incident-forms
- The Cyber Kill Chain - https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- OODA loop – https://en.wikipedia.org/wiki/OODA_loop

***Bruce Schneier**, The Future of Incident Response (2014):*

> “Incident Response needs people, because successful Incident Response requires thinking”

Vincenzo Calabrò

LinkedIn vincenzocalabro