ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

COSTRUIRE E GESTIRE UN CSIRT

Computer Security Incident Response Team

Autori: Stefano Maccaglia
Raffaele “R4ff0” Addesso
Luigi “C4V” Cavucci

15 Ottobre 2009

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Cosa abbiamo in Agenda?

- **Introduzione**
- **Creare un CSIRT**
  - Requisiti per stabilire un efficace CSIRT
  - Individuazione definizione ed attuazione delle politiche e delle procedure
  - Piano strategico per l'implementazione di un CSIRT
- **L'incidente Informatico**
  - Il montaggio reattivo. Meccaniche di progettazione dell'intervento e problematiche operative
- **Introduzione sui livelli di Servizio (SLA)** che possono essere forniti da un CSIRT
- **Alcuni modelli organizzativi per un CSIRT**
- **Alcuni esempi** e alcune esperienze nazionali ed internazionali

Introduzione: il contesto

Al pari dell'Informatica (computer science), che ha dovuto combattere l'insensibilità di molta parte degli ambienti accademici prima di essere riconosciuta di diritto parte integrante delle scienze, la Sicurezza Informatica ha sofferto e continua a combattere per essere riconosciuta come una componente essenziale dell'Informatica stessa.

In questo clima parlare di Incident Response porta spesso a esagerazioni, luoghi comuni e informazioni fuorvianti…

Introduzione: il contesto

- Ma nonostante tutto, il numero di Computer Incident Response Team (CSIRT) continua a crescere con l'aumentata esigenza di protezione dei dati e degli asset da parte delle aziende.
- Questa esigenza è sfociata nella necessità di rispondere alle minacce e ai potenziali incidenti con persone preparate e capaci di gestire situazioni problematiche e prevenirne l'occorrenza.

Introduzione: Acronimi e sinonimi

- **CSIRT - C**omputer **S**ecurity **I**ncident **R**esponse **T**eam

  Organizzazione o team all'interno di una ben definita comunità, fornisce servizio e supporto al fine di **prevenire e rispondere al verificarsi di un qualsiasi incidente di sicurezza** all'infrastruttura IT.

Sinonimi

- **CERT** = **C**omputer **E**mergency **R**esponse **T**eam (marchio registrato)
- **IRT** = **I**ncident **R**esponse **T**eam
- **CIRT** = **C**omputer **I**ncident **R**esponse **T**eam;
- **CSIRT** = **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam;
- **SIRT** = **S**ecurity **I**ncident **R**esponse **T**eam;
- **SERT** = **S**ecurity **E**mergency **R**esponse **T**eam;
- **CSERT** = **C**omputer **S**ecurity **E**mergency **R**esponse **T**eam

Definizione di Incidente

La violazione o l'imminente minaccia di violazione della politica di sicurazza ICT o della prassi di sicurezza standard*

*Fonte:*NIST SP800-61*

Introduzione: Storia

- **1988** "Internet Worm". Incidente che risulta nella compromissione e nel danneggiamento di una alta percentuale di sistemi interconnessi nel network dell'epoca (circa il 10%).
- **17 novembre 1988**: primo CERT presso la Carnegie Mellon University, creato con fondi governativi.
- **1989**: viene creato il **FIRST** (Forum of Incident Response and Security Team) per facilitare la collaborazione fra i CSIRT USA
- **1992**: primi CSIRT in Europa (Olanda,Germania)

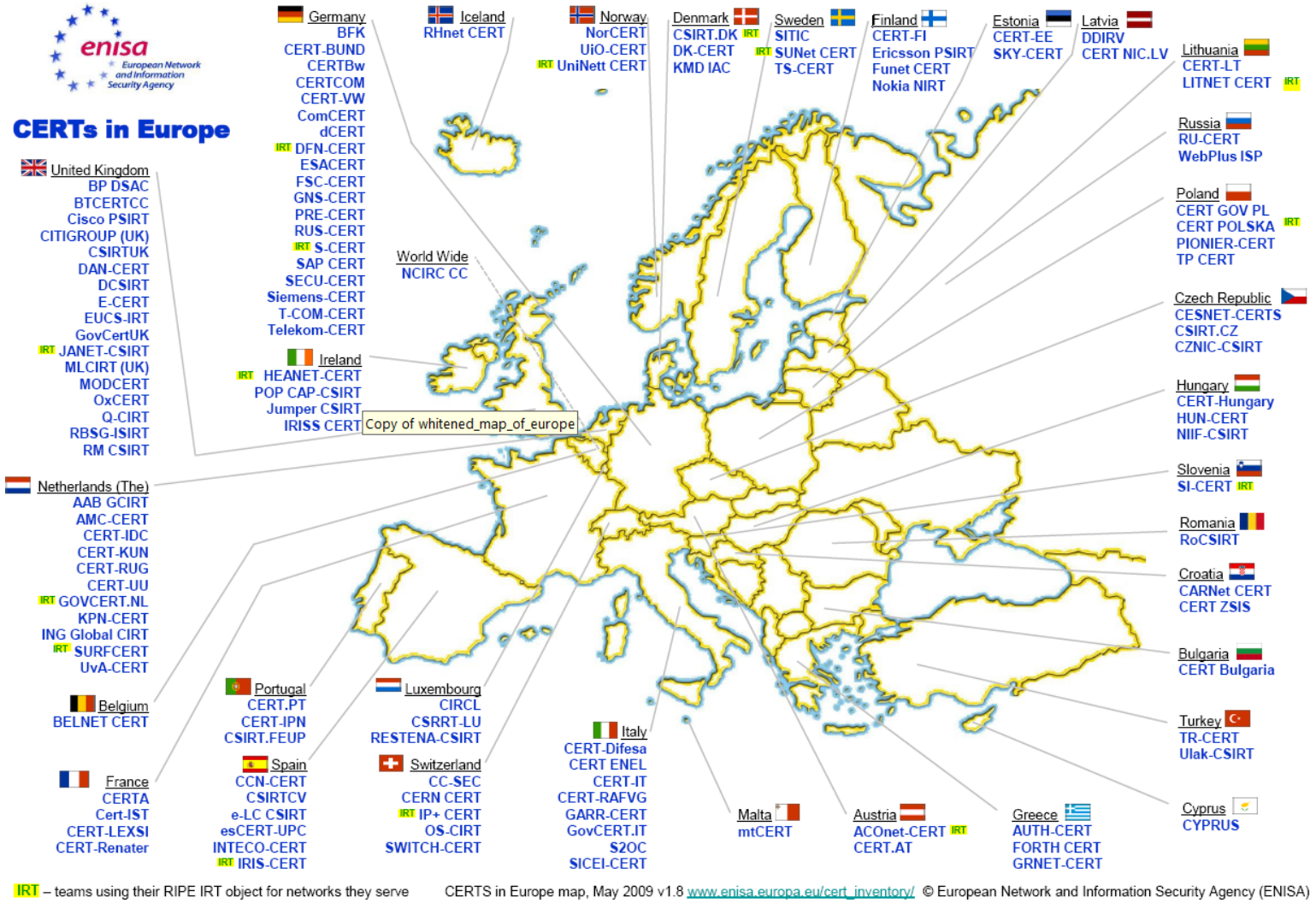
Introduzione: Storia

- Nel **Gennaio del 2003** attraverso la sua **"**Internet Domain Survey" l'ISC[1] mostra che sono circa 171.6 milioni gli host attivi in Internet . Oggi addirittura 625,2 milioni[2].
- Come si possono "gestire" e "informare dei "pericoli" una quantità così grande di utenti e sistemi?
- Chiaramente un singolo CSIRT o una sola organizzazione non è in grado di coprire efficacemente una quantità di utenti così alta.
- In particolare un singolo CSIRT non è in grado di gestire le necessità individuali di aziende e utenti diversi, diversi per cultura, posizione geografica, fuso orario e strutture organizzative.
- Così a partire dalla fine degli anni novanta si sono avviati dei progetti di costituzione di CSIRT all'interno di alcune tra le maggiori aziende private.

1 http://ftp.isc.org/www/survey/reports/2003/01/

2 http://ftp.isc.org/www/survey/reports/current/

I CERTs in Europa



E in Italia?

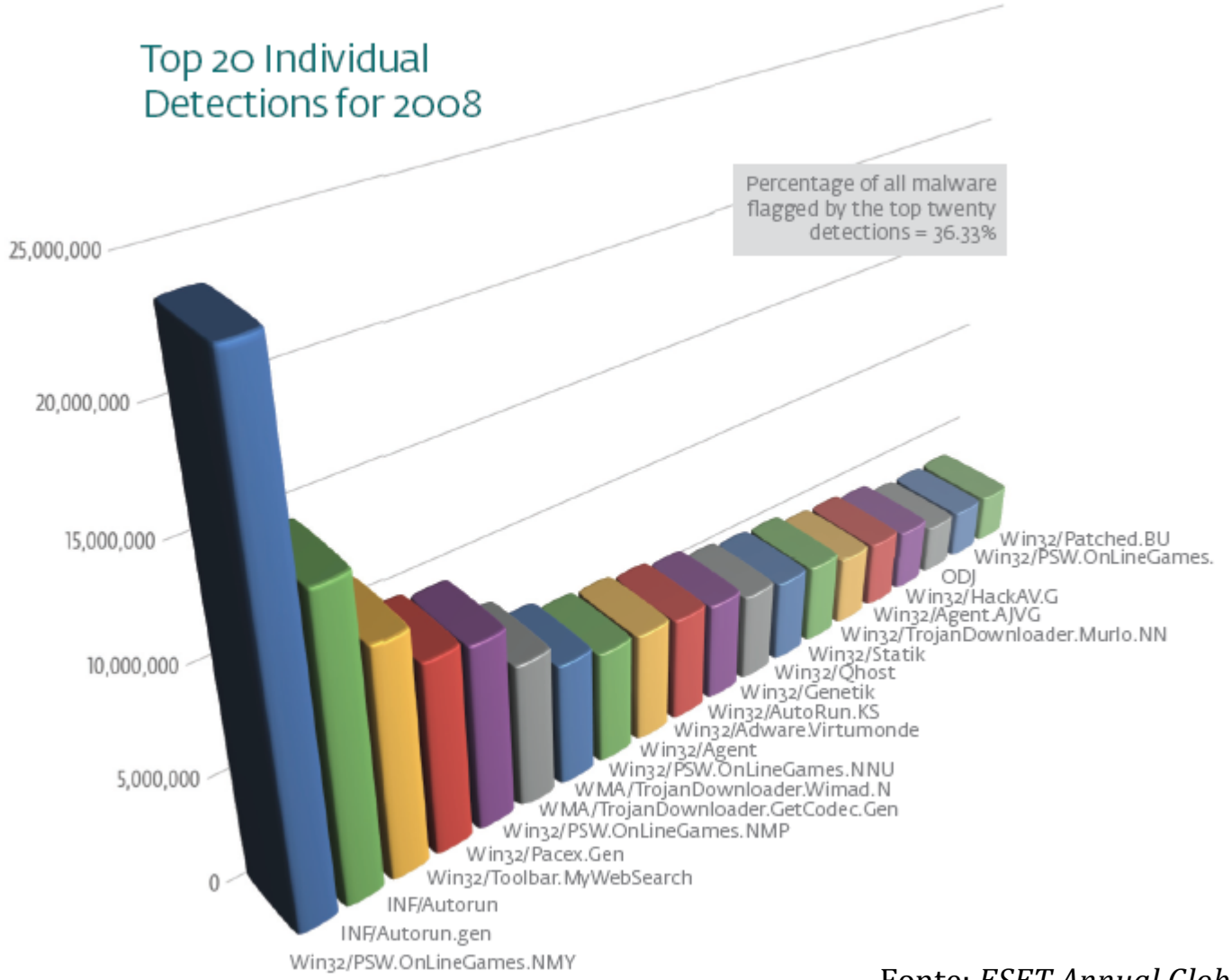
- **In Italia si parte intorno al 1995**, ma il primo vero CSIRT nazionale viene istituito all'interno del CNIPA alla fine degli anni novanta. Tale istituzione assumerà poi **nel 2005 il** nome di **GovCERT,** coerentemente con la nomenclatura utilizzata da analoghe realtà costituite in ambito europeo.
- Il GovCERT ha come obiettivo il supportare le pubbliche amministrazioni centrali nella prevenzione e gestione degli incidenti informatici, ponendosi come struttura di coordinamento dei gruppi operanti all'interno di ciascuna amministrazione centrale, previsti dalla Direttiva sulla sicurezza ICT del 16 gennaio 2002 e denominati **CERT-AM.**

E in Italia?

- **Aprile 2008**: Le Regole tecniche per il funzionamento e la sicurezza del SPC , prevedono **per la prima volta** che ogni amministrazione pubblica centrale, aderente all'SPC, si doti di una **U**nità **L**ocale di **S**icurezza, cui è affidata la responsabilità di prevenzione degli incidenti ICT sia la gestione operativa degli eventuali incedenti informatici
- ***Al CERT-SPC sono attribuite le funzioni di referente centrale nazionale per la prevenzione, il monitoraggio, il coordinamento informativo e l'analisi degli incidenti di sicurezza in SPC***.

SPC = **S**ervizio di **P**ubblica **C**onnettività

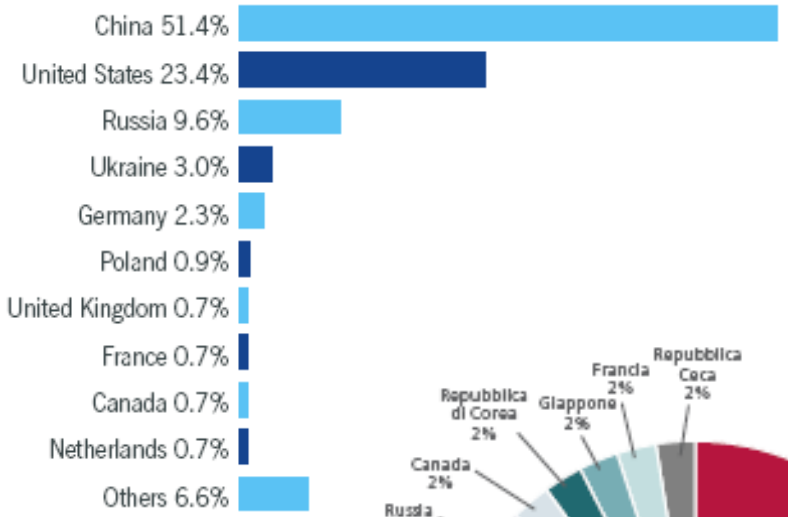
I Trend delle minacce Virali



Fonte: *ESET Annual GlobalThreat Report 2008*

Alcune minacce per provenienza

Minacce Virali per provenienza (in %)



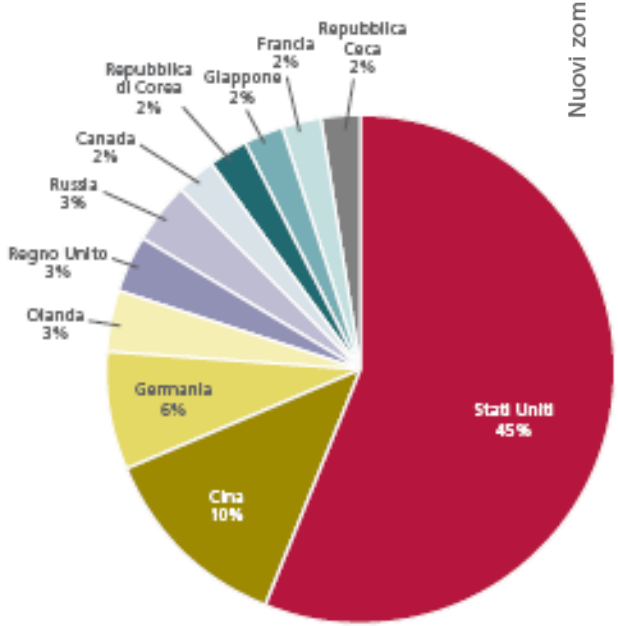
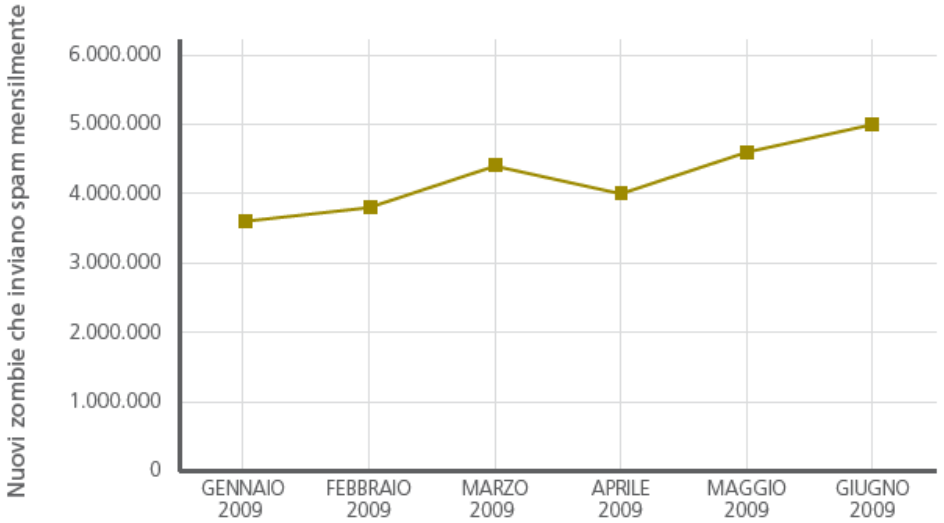


Figura 10: Distribuzione dei server web con reputazioni malevole.



Fonte: *Sophos Security Report Jan.2008*

La protezione passa per l'Incident Response

- Al giorno d'oggi uno dei problemi più importanti nel costituire un CSIRT internamente ad un'azienda (pubblica o privata che sia) è legato al grande numero di compentenze che il gruppo deve potersi garantire per operare in modo adeguato.
- Si devono infatti fronteggiare azioni e potenziali pericoli provenienti da gruppi e singoli individui, organizzazioni e semplici script-kiddies o anche più semplicemente problemi di instabilità operativa e debolezze introdotte dai nostri stessi fornitori…
- Non dimentichiamoci poi che si deve agire verso gli host interni e verso le componenti pubbliche, verso gli asset e verso i Clienti… e tutto questo in un quadro organico e specifico di ogni realta aziendale…

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Introduzione: Caratteristiche di un CSIRT

- Tipologia
- Modelli
- Costituency
- Autorità
- Modello organizzativo
- Servizi erogati
- Relazioni

Introduzione: Caratteristiche di un CSIRT

- **Tipologia**
  - **Interni**
    - Team di sicurezza Interni all'azienda stessa
  - **Nazionali**
    - Organizzazioni governative
    - Coordinamento
    - In Italia: CERT GOV, con sede presso il CNIPA
  - **Centri di analisi**
    - Servizi e centri di ricerca sulla Security (esempio lab finanziati sulla ricerca di virus e advisory)
  - **Team di supporto di fornitori**
    - Ancora, ad esempio, i team che si occupano del rilascio di aggiornamenti da parte del fornitore di piattaforme applicative
  - **Managed Security Service Provider (MSSP)**
    - Azienda esterna che fornisce servizi di Managed Security Service

Introduzione: Caratteristiche di un CSIRT

- **Modelli**
  - **Centralizzati**
  - **Distribuiti**
  - **Misti**
  - **Security Team**
  - **Coordinamento**

Ogni modello ha delle specifiche caratteristiche e delle meccaniche di attuazione differenti.

Oltre alla struttura interna a variare, tra un modello ed un altro, sono le caratteristiche dei componenti e il campo di applicazione del CSIRT.

Introduzione: Caratteristiche di un CSIRT

- **Costituency**
  - **La comunità di riferimento**
    - è costituita dagli utenti, dagli enti e dalle organizzazioni cui il CSIRT eroga i suoi servizi

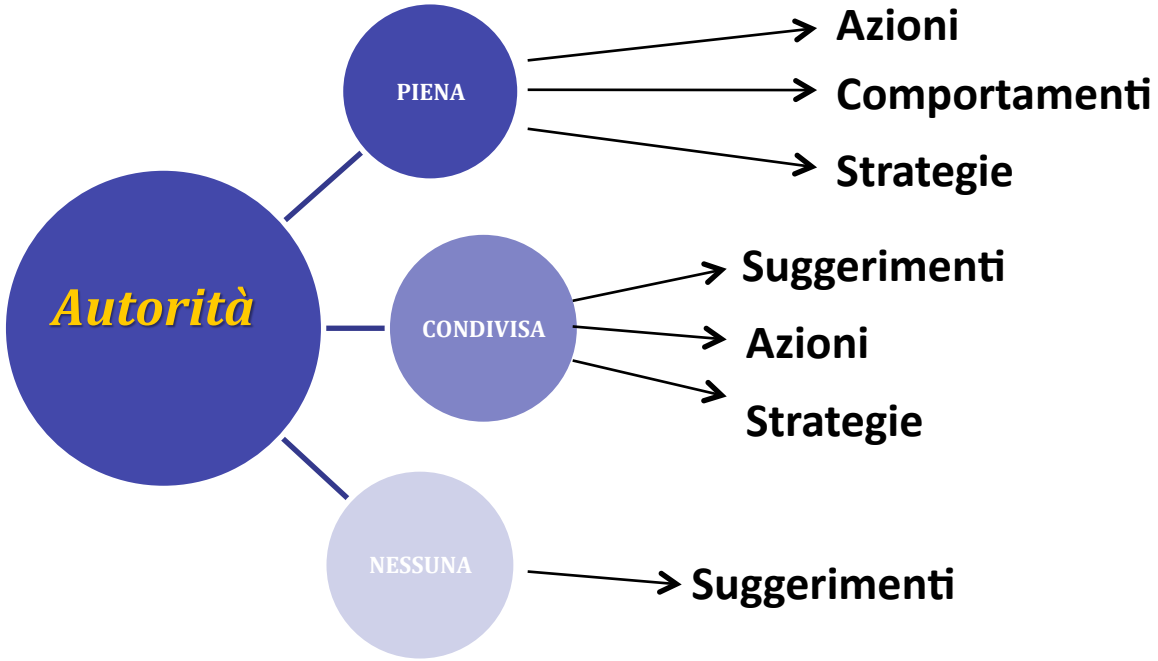
In una visione allargata, ancora non matura, la comunità di riferimento potrebbe essere costituita dall'insieme dei CSIRT che si pongono in contatto e attuano delle relazioni di mutuo scambio di informazioni.

A tendere questo approccio sembrerebbe piuttosto interessante da percorrere, è un'azione già tentata e in parte riuscita in ambito di Pubblica Amministrazione, ma essa non è stata mai tentata nel campo privato.

Introduzione: Caratteristiche di un CSIRT

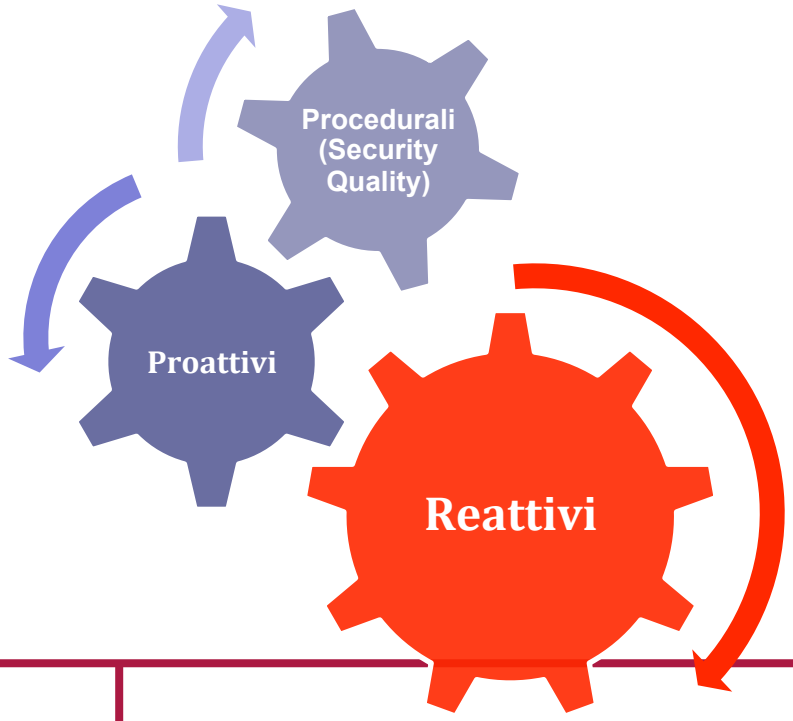
- **Autorità**
  - **PIENA:** potere di imporre azioni e comportamenti
  - **CONDIVISA:** il gruppo è in grado di influenzare azioni e comportamenti partecipando ai processi decisionali
  - **NESSUNA:** il gruppo può solo dare raccomandazioni, consigli e suggerimenti, anche se autorevoli

Introduzione: Caratteristiche di un CSIRT



Introduzione: Caratteristiche di un CSIRT

- **Servizi erogati**
  - **Reattivi**
  - **Proattivi**
  - **Procedurali (Security Quality)**



Introduzione: Caratteristiche di un CSIRT

- **Servizi erogati**
  - **Reattivi**
    - Early warning
    - Gestione Incidenti
      - Analisi
      - Response on site
      - Response Coordination
      - Response Support
    - Gestione Codici "pericolosi"
  - **Proattivi**
  - **Security Quality**

Introduzione: Caratteristiche di un CSIRT

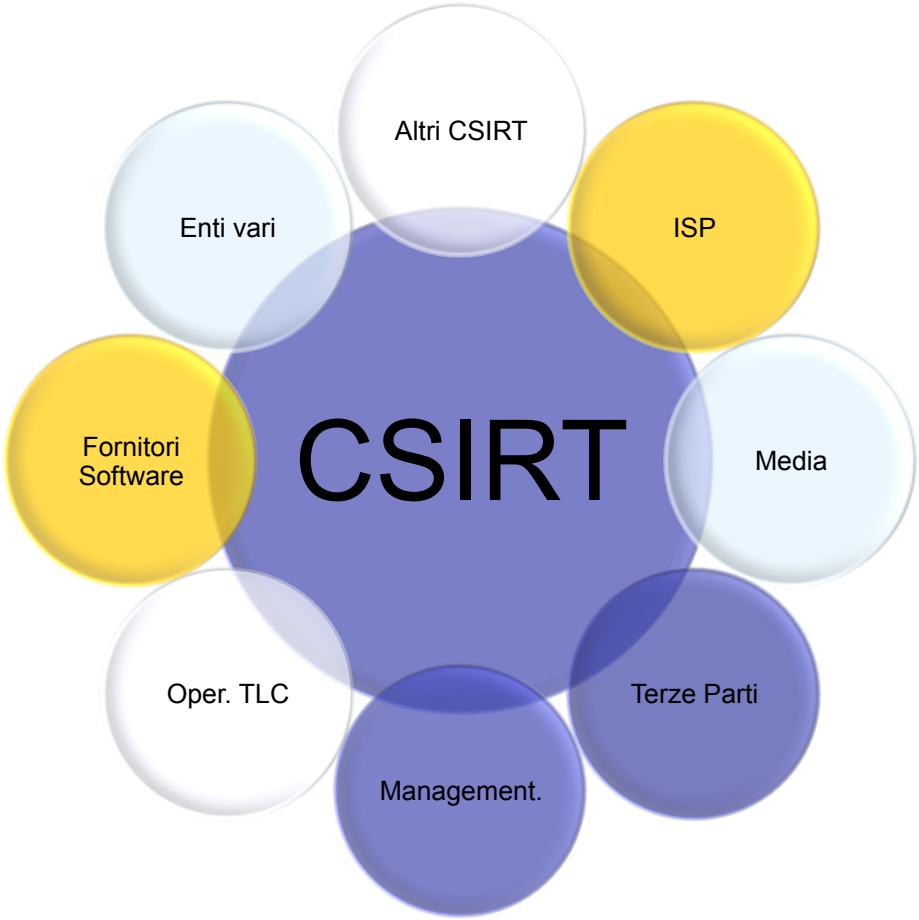
- **Servizi erogati**
  - Reattivi
  - **Proattivi**
    - Osservatori tecnologici
    - Security audit and assessments
    - Tool di sicurezza
      - Sviluppo
      - Aggiornamento
    - Intrusion Detenction Services
    - Sensibilizzazione
    - Raccolta e condivisione di informazioni
  - Security Quality

Introduzione: Caratteristiche di un CSIRT

- **Servizi erogati**
  - Reattivi
  - Proattivi
  - **Security Quality**
    - Risk Analisys
    - Business Continuty & Disaster Recovery planning
    - Consulenza
    - Formazione
    - Valutazione e Certificazione di prodotti (HW & SW)

Introduzione: Caratteristiche di un CSIRT

- **Relazioni**



ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Agenda

- **Introduzione**
- **Creare un CSIRT**
  - Requisiti per stabilire un efficace CSIRT
  - Individuazione definizione ed attuazione delle politiche e delle procedure
  - Piano strategico per l'implementazione di un CSIRT
- **L'incidente Informatico**
  - Il montaggio reattivo. Meccaniche di progettazione dell'intervento e problematiche operative
- **Introduzione sui livelli di Servizio (SLA)** che possono essere forniti da un CSIRT
- **Alcuni modelli organizzativi per un CSIRT**.
- **Alcuni esempi** e alcune esperienze nazionali ed internazionali

Creare un CSIRT

- **Qual è la migliore strategia?**
- **Importante decidere**
  - Perché dobbiamo crearlo?
  - Qual è il suo scopo?
- **Qual è il suo Target?**
- **Aziende simili come si stanno muovendo in merito?**

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Domande…

- É possibile formulare un unico set di domande ed in particolar modo di risposte, che possa essere utilizzato per definire tipologia, modello e struttura di un CSIRT?

- **RISPOSTA > Nessun Team opera esattamente nella stessa maniera.**

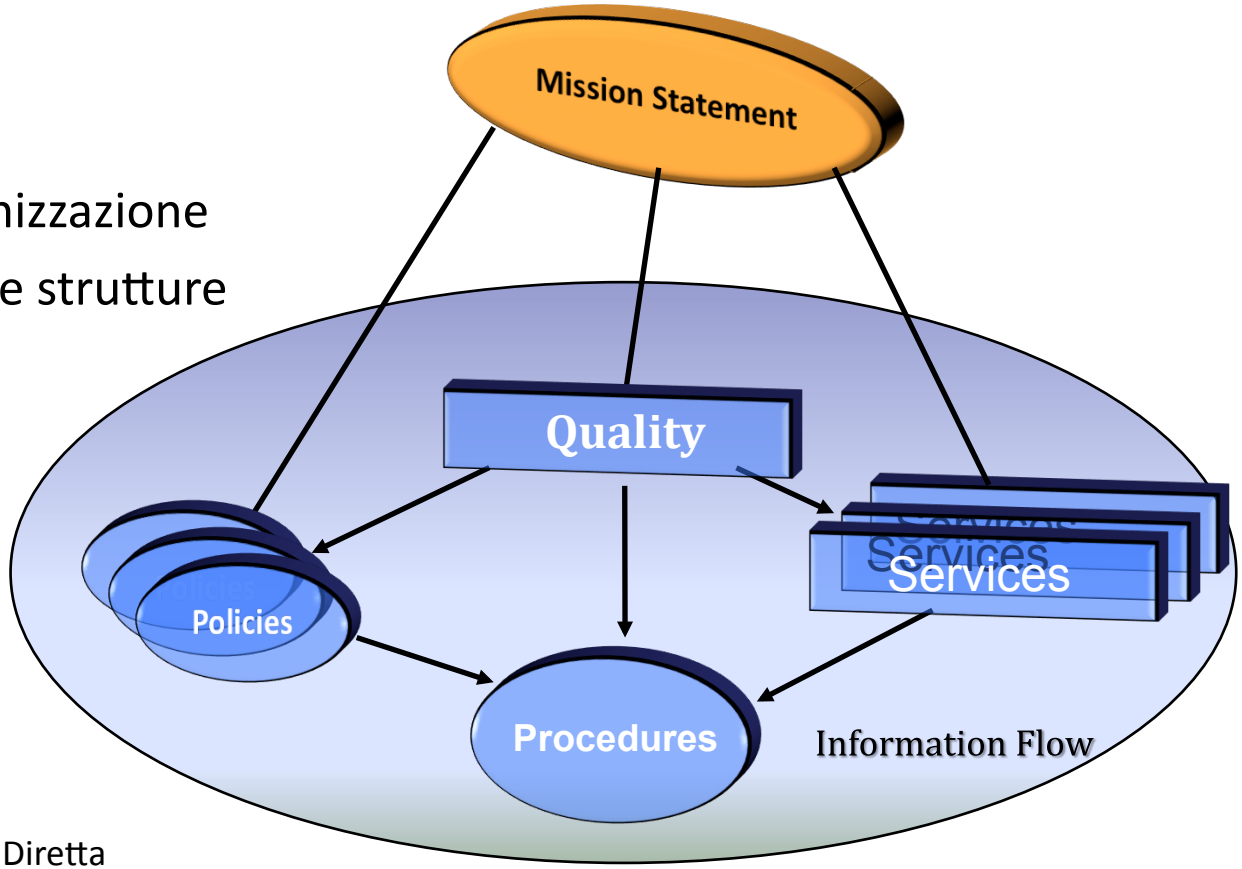
- **FATTO… >** Spesso si cercano guide ed esperienze documentate di altri CSIRT nella speranza di poter replicare le meccaniche e le procedure adottate da altri in precedenza… e allora ci si scontrerà con una quantità enorme di problemi di adattamento da parte degli operatori.

CSIRT Framework

La migliore strategia.

Partire dalle fondamenta:

- ✓ Mission Statement
- ✓ Constituency
- ✓ Posizione nell'Organizzazione
- ✓ Relazioni con le altre strutture
- ✓ Procedure



Suggerimenti per la partenza

- Ogni CSIRT opera in modo diverso in quanto diverse sono le persone, le skill, le capacità e le modalità di lavorare insieme e diversi sono anche i budget o le circostanze in cui si lavora…
- Le raccomandazioni generali per partire sono:

✓ **Step 1: Avere il supporto dal Management**

✓ **Step 2: Definire un piano strategico per il CSIRT**

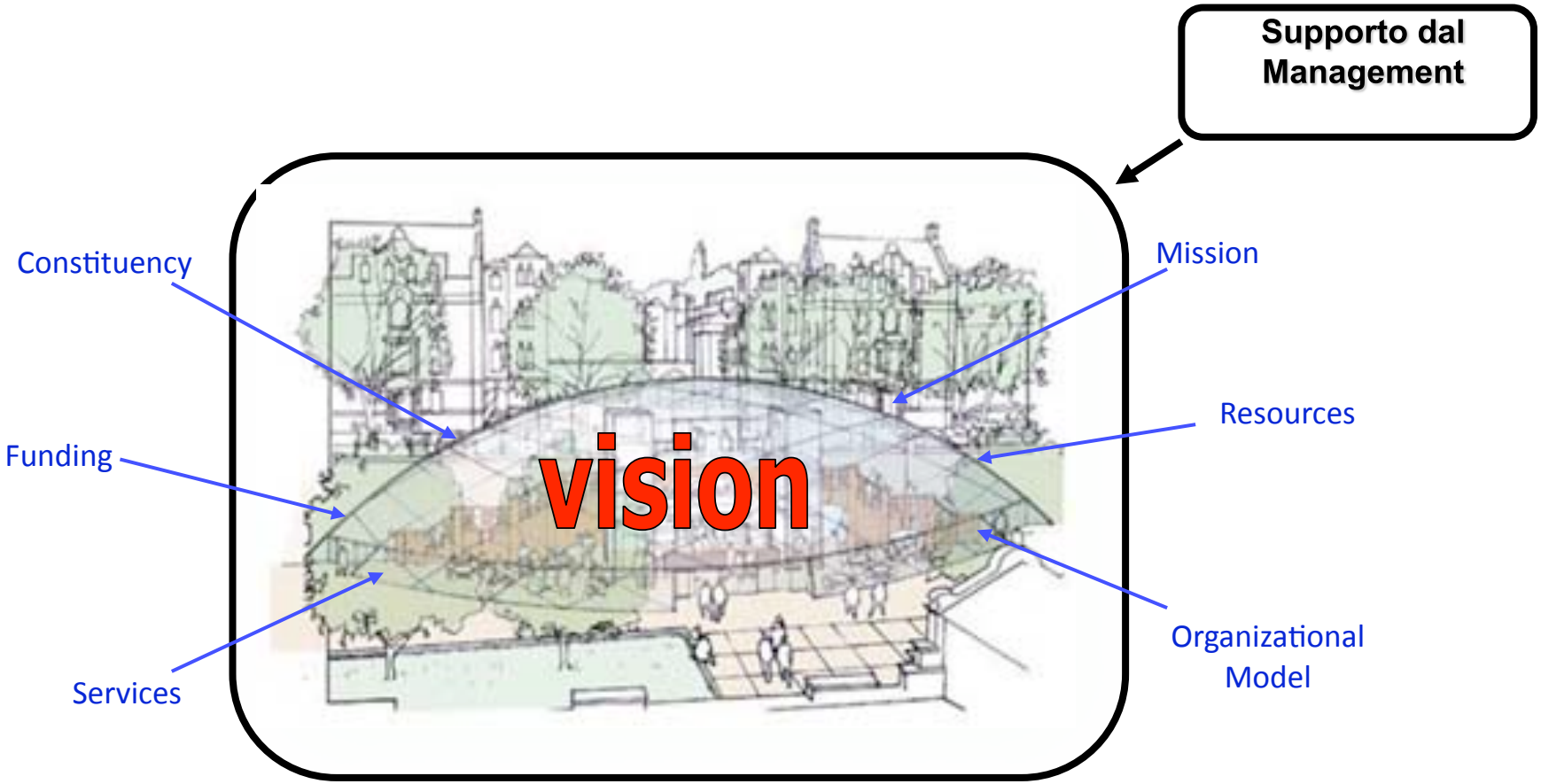
✓ **Step 3: Acquisire le informazioni più essenziali**

✓ **Step 4: Definire le modalità di attuazione del piano strategico (vision)**

Suggerimenti per la "partenza"

- ✓ **Step 5: Essere sempre impegnati nel comunicare la visione e i piani operativi del gruppo CSIRT al resto dell'Azienda**
- ✓ **Step 6: Attivare il gruppo**
- ✓ **Step 7: Misurare efficienza e difficoltà**
- ✓ **Step 8: Essere sempre in grado di "imparare" e sviluppare una knowledge base documentale**

Suggerimenti per la "partenza"



Chi dovrebbe partecipare al Team?

Personale di un CSIRT

- Manager
- Risorse Umane
- Ufficio Legale
- Dipartimento IT: Rete e Telecomunicazioni
- Sicurezza IT
- Sicurezza Fisica
- Supporto Tecnico
- Helpdesk
- Internal Audit
- Rappresentanti degli Utenti (Clienti)

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Agenda

- **Introduzione**
- **Creare un CSIRT**
  - Requisiti per stabilire un efficace CSIRT
  - Individuazione definizione ed attuazione delle politiche e delle procedure
  - Piano strategico per l'implementazione di un CSIRT
- **L'incidente Informatico**
  - Il montaggio reattivo. Meccaniche di progettazione dell'intervento e problematiche operative
- **Introduzione sui livelli di Servizio (SLA)** che possono essere forniti da un CSIRT
- **Alcuni modelli organizzativi per un CSIRT**
- **Alcuni esempi** e alcune esperienze nazionali ed internazionali

Categorizzazione degli incidenti

- Uno dei punti fermi del lavoro di un CSIRT è la **CATEGORIZZAZIONE DEGLI INCIDENTI E CLASSIFICAZIONE DEGLI STESSI**.
- Data la grande quantità di differenti "potenziali" incidenti, l'Azienda deve definire, in partenza, cosa intende per "Incidente".
- Qui illustriamo un metodo consolidato per la Categorizzazione e la Classificazione:
  - *Tipo di Evento*
  - *Impatto nell'Azienda*
  - *Aree interessate*
  - *Tipo o grado di danno*
  - *Obiettivo o sorgente dell'attacco (Evento)*

Definizione di RESPONSE

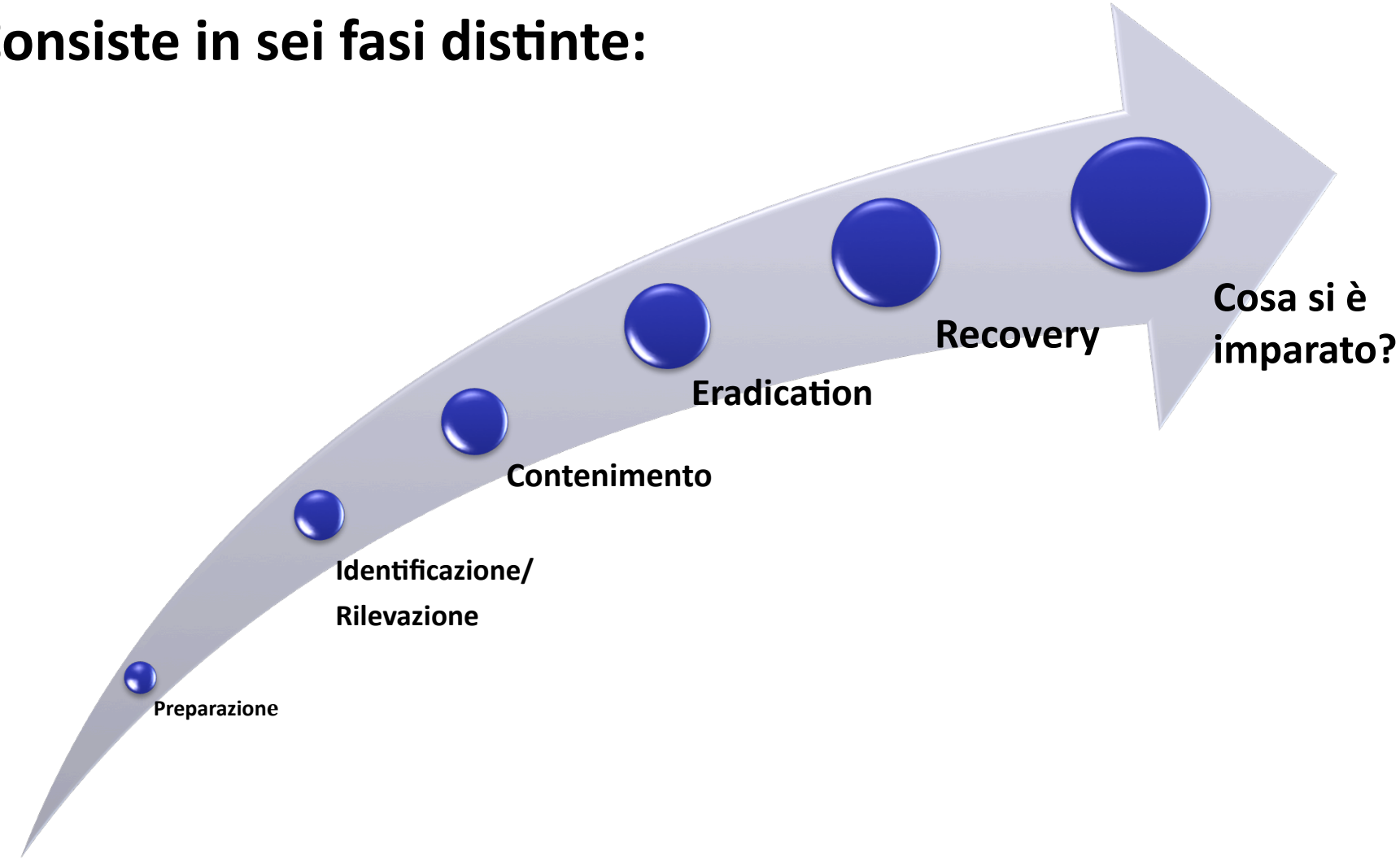
- ***L'Incident response*** **è una metodologia per la la risoluzione di eventi inattesi.**

- Eventi di tipo:
  - Naturale
  - Accidentale
  - Intenzionale

- Incidenti – *Cosa contraddistingue un incidente?*
  - **Classification** – *Che tipo di incidente è occorso?*
  - Le categorie qui sotto schematizzano i possibili casi.
    - **Perdita di confidenzialità**
    - **Perdita di integrità**
    - **Denial of Service**
    - **Violazione o Uso non consentito di Servizi o Sistemi**
    - **Danneggiamento dei Sistemi**

Incident Response

Consiste in sei fasi distinte:

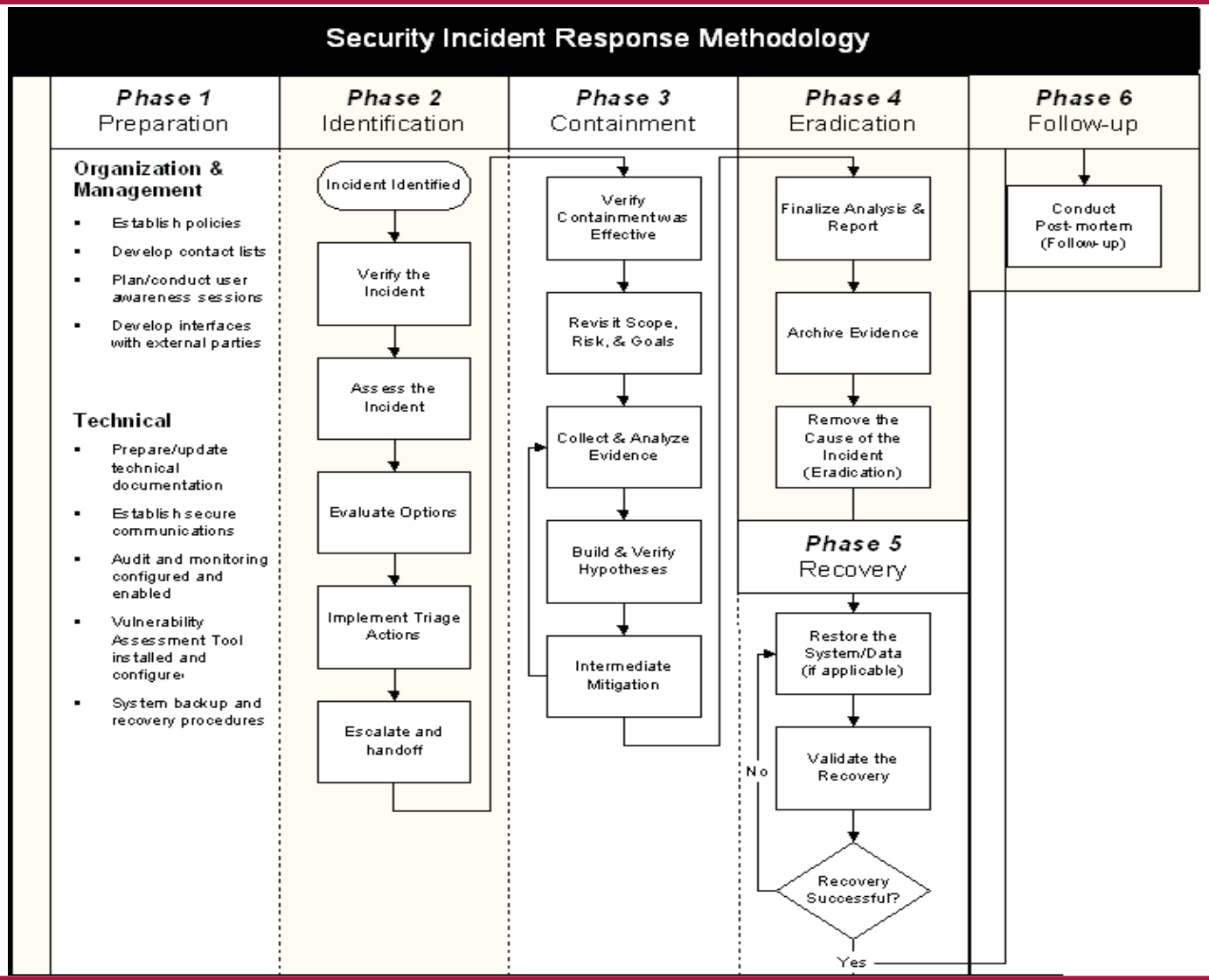


LIMITARE IL DANNO E MASSIMIZZARE LA CAPACITA' DI RIPRISTINO

Incident Response

- **Preparazione**
  - Tutto quanto precede l'attuazione di un meccanismo di Incident Response. Rientra in questo ambito il "Planning" che definisce le aree d'azione, le meccaniche di attivazione del team, nonché le Politiche e le Procedure.
- **Identificazione/Rilevazione**
  - Le misure e gli strumenti utili all'identificazione (preventiva o reattiva) e alla rilevazione di incidenti.
- **Contenimento**
  - Le misure preventive o reattive di mitigazione
- **Eradication**
  - Come eliminare della causa dell'incidente a partire dalla fonte
- **Recovery**
  - Le modalità di ripristino delle funzionalità e delle piattaforme colpite dall'incidente
- **Cosa si è imparato? (Lessons learned)**
  - Documentazione, Knowledge Base, Training.

Incident Response



Così semplice???

- Chiunque abbia avuto a che fare con un incidente ha probabilmente incontrato questa situazione, almeno una volta.
- A seguito della scoperta di una compromissione, mentre tentiamo di analizzare ciò che è accaduto abbiamo regolarmente il dirigente e /o i clienti alle nostre spalle costantemente in cerca di maggiori dettagli. Mentre elaboriamo il piano di contenimento qualcuno ha bisogno di mettersi in contatto con l'ufficio legale, il dipartimento di HR, i giornalisti, e contemporaneamente il management vuole un aggiornamento, la direzione tecnica necessita di personale o di assistenza, le squadre devono essere coordinate, tutti vogliono essere in aggiornati, un sacco di urla si susseguono, IRT esterni chiedono spiegazioni del perché la nostra rete stia attaccando la loro, nessuno trova più il backup giusto, nessuno tiene traccia delle attività e la lista potrebbe continuare…

Incident Handling & Incident Response

- Una delle cose che viene spesso è oggetto di confusione è la differenza tra l'incident handling e l'incident response.
- Molte persone vanno in "burn-out" durante gli incidenti!
- La Gestione degli incidenti: l'Incident management, non è uno sport, ma la migliore strada per rendere efficace la risposta all'incidente stesso.
- Se l'Incident Response riassume in se tutte le componenti tecniche necessarie all'analisi e al contenimento dell'incidente, l'***Incident Handling è la logistica, le comunicazioni, il coordinamento, la programmazione e le funzioni necessarie al fine di risolvere un incidente in maniera calma ed efficiente***.
- E per esperienza è bene che due figure diverse svolgano queste funzioni.

Quali misure prendere

- **Priorità e Urgenza**
  - *Identificare il livello di effort per una risposta (response level of effort) (LoE) per un determinato tipo di incidente. I vari LoE devono essere periodicamente valutati per assicurare aderenza alle necessità di protezione e alla capacità di reazione dell'Azienda.*
  - *Indichiamo nella seguente classificazione la forma più comune di scala di Priorità:*

  - Minacce per la sicurezza fisica degli esseri umani
  - Root o attacchi a livello di sistema per qualsiasi host o sistema
  - Compromissione degli account amministrativi di servizi o di software critici
  - Attacchi Denial of Service alle infrastrutture, agli account di amministrativi o a software critici
  - Attacchi o compromissioni a danno di altre strutture esterne, ma originati da sistemi interni appartenenti all'Azienda o all'Organizzazione
  - Attacchi su larga scala di qualsiasi tipo (worm, attacchi di sniffing, etc)
  - Minacce, molestie o reati penali che coinvolgono singoli account utente
  - Compromissione di singoli account utente
  - Compromissione dei sistemi desktop
  - Falsificazioni, false dichiarazioni, o furto di risorse

L'IRT

- **Incident Response Team (IRT)** – *Chi deve rispondere in caso di Incidente?*
  - **Mission Statement** - Il *perche di un team IRT e con quali compiti?*
  - **Roles and Members** – Chi dovrebbe far parte di un IRT*?*
    - **Leader** – *Coordinatore and PoC (Point of contact)*
    - **Lo Sponsor** nel Management – *Supporta lo "shift" dei ruoli in caso di Incidente e si fa carico di ridurre il peso della burocrazia ai danni dell'IRT prima, durante e dopo l'incidente.*
    - **Systems Engineer** – *Responsabile dell'analisi e della "risposta" nell'ambito dei sistemi*
    - **Network Engineer** - *Responsabile dell'analisi e della "risposta" in ambito "rete" e "connettività"*
    - **Forensic Advisor** – *Responsabile dell'analisi post-incidente e dell'identificazione dei sistemi coinvolti nell'incidente. Supporta gli altri membri del gruppo nella definizione del campo d'azione della "Response".*
    - **Public Relations Advisor** – *E' l'interfaccia nei confronti dei Clienti e della Stampa (se necessario).*
- **Ufficio Legale** – *Offre indicazioni all'IRT e al Management sui possibili scenari legali nei confronti dell'incidente e delle azioni mitigatrici e di ripristino.*

L'IRT durante un incidente

- Processo di **Incident Handling**
  - Determinare se un incidente è accaduto, *alcune attività non permettono l'azione dell'IRT se non a valle di specifici "grant" o condizioni. In altri casi l'incidente è gestibile senza l'attivazione dell'IRT (casi specifici di minore entità, documentati in modo puntuale nelle procedure d'esercizio, ad esempio, incidente di connettività causato dall'ISP).*
  - **In caso di attivazione**
  - Si contatta il Leader IRT
    Se l'IRT deve essere attivato, il Leader deve documentare l'ingaggio e circoscrivere, con l'ausilio del team, il campo d'azione.
  - **Contenimento dell'Incidente**

    La prima azione da attuare operativamente è la prevenzione della diffusione dell'incidente ad altre aree della struttura.
    Identificare e isolare l'area oggetto di indagine.
    Comunicare al personale incaricato della consulenza legale, del caso.
    Comunicare all'ufficio preposto alle pubbliche relazioni, se necessario, condividendo informazioni opportunamente censurate dall'ufficio legale.

- **Eradicate the Incident**
  - porre fine a tutto ciò che ha causato l'incidente
  - Raccogliere le prove
  - Identificare l'origine dell'incidente
  - Determinare la portata dell'incidente
    Attuare misure tampone per eliminare le minacce attive
  - Aggiornamento della documentazione con le informazioni di eradicazione

Specifiche azioni di Response

- **Valutare il danno** – *Determinare l'impatto dell'incidente nella struttura aziendale*
  - Identificare i sistemi e gli ambiti di rete affetti
  - Identificare i dati compromessi o affetti
  - Identificare le strade possibili di "remediation"
- **Minimizzare il danno** – *Minimizzare i costi, sia tangibili che intangibili associati all'incidente*
  - Recuperare i dati compromessi o potenzialmente alterati dai sistemi di backup
  - Se necessario l'Advisor per le Pubbliche Relazioni stabilirà un piano di "recupero" dell'immagine agli occhi della clientela e degli azionisti
- **Annichilire la sorgente dell'incidente** – *Prevenire il ripetersi dell'incidente*
  - Aggiornare con Patch ogni possibile vulnerabilità rimasta
  - Attuare più stringenti controlli all'accesso delle aree compromesse o affette
  - Attuare ulteriori azioni mitigatrici, se necessario

Specifiche azioni di Response

- **Analizzare l'incidente** – *Imparare dagli errori*
  - Determinare i motivi che hanno generato l'incidente
  - Determinare se misure opportune sono state individuate e attuate per prevenire il ripetersi dell'incidente
  - Determinare il livello di rischio di simili incidenti in altre aree o su altri asset aziendali
- **Revisionare il Piano di Incident Handling** - *Adattare e aumentare l'efficienza in ogni area*.
  - Valutare se l' incident handling e la risposta sono stati appropriati
  - Modificare il piano di Incident handling e Incident response a seguito delle nuove informazioni acquisite
- **Documentare** – *Mantenere aggiornati, chiari e comprensibili i record e I report di ogni incidente.*
  - Creare una documentazione finale dell'incidente con un appropriato livello di dettaglio
  - Svolgere dei debriefing tra le risorse dell' IRT, se necessario
- **Report**- *Assist others in disaster aversion*
  - Se necessario fornire un report dell'incidente e delle azioni di mitigation agli altri CSIRT e ai vari CERT nazionali.

Incident Response Planning

- Non è una semplice applicazione di derivati tecnologici, è l'attivazione di una serie di processi (legati ad un *Framework*)
- Selezionare e attivare il Team
- Sviluppare un piano di Comunicazione
- Definire Politiche e Procedure
- Piani di Incident Response efficaci includono:
  - Periodiche revisioni delle documentazioni
  - Training
  - Budget e Finanziamenti
  - Pratiche ed esercitazioni

Un esempio di "Response"

- Prima di partire:
  - Documentate tutti i passi che si condurranno durante l'attività.
- Assicurarsi il Controllo
  - Disconnettere il/i Sistema/i compromesso/i dalla rete.
  - Realizzare un dump (copia immagine) del Sistema.
- Analizzare l'attacco
  - Raccogliere dati sui software presenti nel sistema, copiare i file di configurazione, i Dati, i Log.
  - Utilizzare Tool quali gli sniffer di rete e analizzare i log in cerca di dati lasciati dall'intruso.
  - Verificare lo stato e i log di altri Sistemi nella rete compromessa.
- Contattare fonti attendibili
  - Verificare attraverso fonti accreditate le possibili modalità di introsione e documetarle nel report dell'incidente (Incident Reporting)

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Un esempio di "Response" (Cont.)

- Ripristino dall'intrusione
  - Reinstallare il Sistema Operativo, disabilitare i Servizi non necessari, allineare la macchina ad un adeguato livello di aggiornamento, verificare gli Advisories, attuare una stringente politica su Credenziali e Passwords.
- Migliorare la Sicurezza della Rete
  - Analizzare e migliorare le configurazioni degli apparati di rete, degli apparati di Sicurezza, verificare il funzionamento e la validità dei meccanismi di Logging.
- Riattivare la connessione dell'host
- Revisionare o verificare le politiche di Sicurezza
  - Documentare l'incidente, l'impatto, le fonti e le modalità di intrusione
  - Definire e validare le modifiche (se ce ne sono state) alle politiche di Sicurezza

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Agenda

- **Introduzione**
- **Creare un CSIRT**
  - Requisiti per stabilire un efficace CSIRT
  - Individuazione definizione ed attuazione delle politiche e delle procedure
  - Piano strategico per l'implementazione di un CSIRT
- **L'incidente Informatico**
  - Il montaggio reattivo. Meccaniche di progettazione dell'intervento e problematiche operative
- **Introduzione sui livelli di Servizio (SLA)** che possono essere forniti da un CSIRT
- **Alcuni modelli organizzativi per un CSIRT**
- **Alcuni esempi** e alcune esperienze nazionali ed internazionali

SLA in un CSIRT

- Introdurre il concetto di SLA in un CSIRT significa definire le **priorità di "response"**.
- **La priorità è**, in questo approccio, **la sequenza con la quale incidenti, problemi o modifiche verranno gestiti**.
- **È essenziale che la priorità venga definita sulla base dell'impatto che la problematica ha nei confronti delle attività produttive dell'Azienda**.
- **Ciò comporta che ogni CSIRT dovrebbe nascere a seguito di una Risk Analysis** utile all'ingegnerizzazione del CSIRT e all'identificazione del miglior modello funzionale per lo stesso.

Priorization Model

Impact

Rank	Guidelines
1. Extensive/ Widespread	• Business critical system and/or service are **unavailable** • Affecting more than 100 users, an entire system or service, an entire location, or entire agency
2. Significant/ Large	• Business critical system and/or service is severely **degraded** or **partial loss** of mission critical features / functionality • Non-business critical system and/or service **unavailable** • Affecting 20 to 100 users
3. Moderate/ Limited	• Any system and/or service is **degraded** or non-business critical functions or features are non-operational or unavailable to users • Affecting 5 to 20 users
4. Minor/ Localized	• Any system and/or service is experiencing minor **degradation** or non-business critical functions or features are non-operational or unavailable to customers • Affecting 1 to 5 users

Rank	Guidelines
1. Critical	• Response includes an immediate and sustained effort using any and/or all available resources as required until the Incident is resolved • Hierarchical escalation is invoked, on-call procedures are activated, and vendor support invoked • Generally customers are unable to work and no work around is available
2. High	• Assigned support team responds immediately, assesses the current situation and may interrupt other staff working lower priority Incidents / Service Requests to assist in timely restoration of services • Customers require expedited restoration of service, but can bear minimal delays • Customers may or may not have a work around available or workaround may only provide partial relief
3. Medium	• Assigned support team responds using standard procedures and operating within normal supervisory management structures • Customers may or may not have a work around available, or workaround may only provide partial relief
4. Low	• Assigned support team responds using standard procedures and operating within normal supervisory management structures • Customers may be inconvenienced, but a suitable workaround is available to allow the customer to continue working, or a delay in resolution is considered acceptable

Prioritization Model

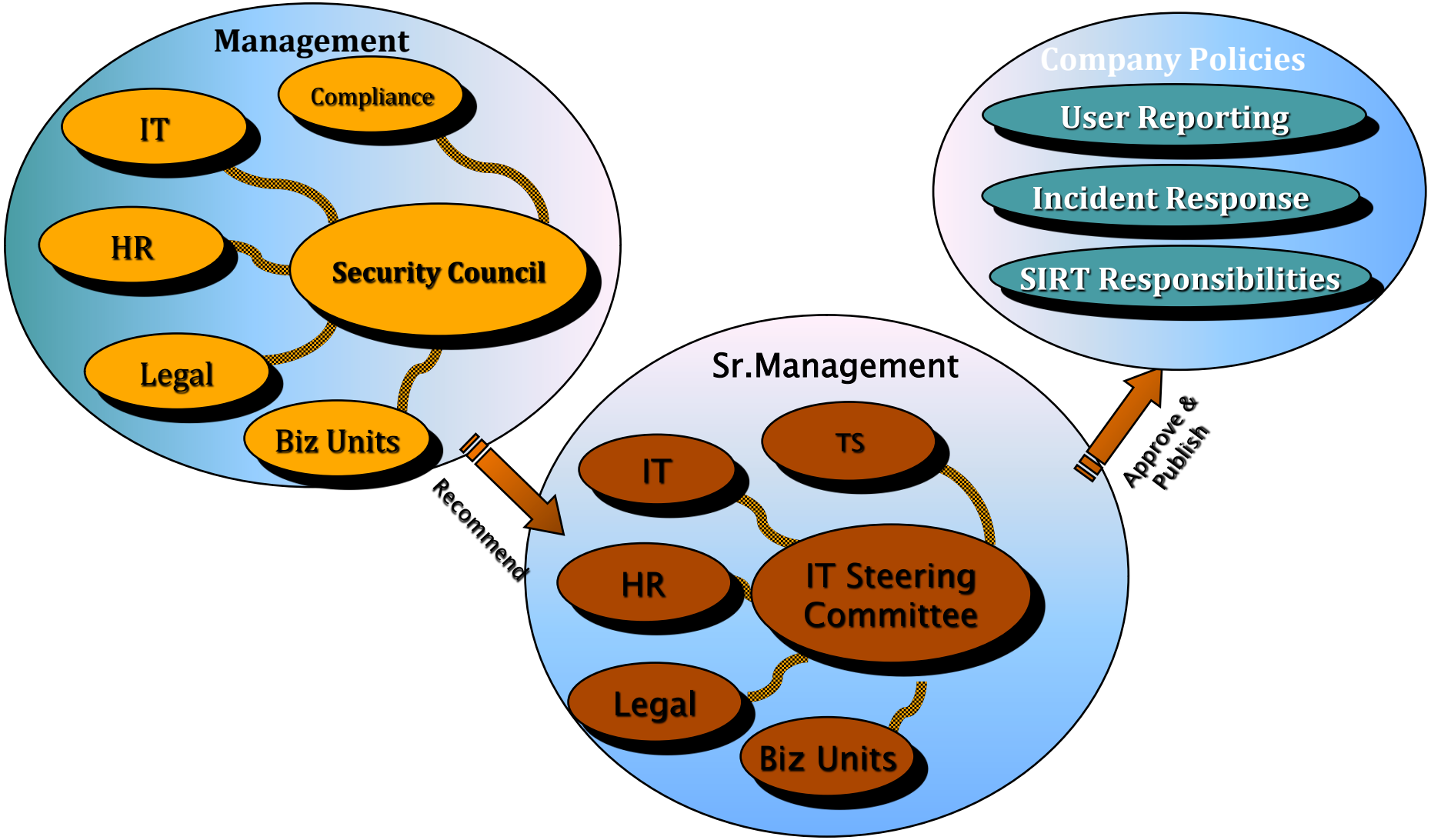
		Urgency			
		1-Critical	2-High	3-Medium	4-Low
Impact	1 - Extensive / Widespread	Critical 29	Critical 24	High 19	Low 9
	2 - Significant / Large	Critical 25	High 20	Medium 15	Low 5
	3 - Moderate / Limited	High 23	High 18	Medium 13	Low 3
	4 - Minor / Localized	High 20	Medium 15	Medium 10	Low 0

Dal Priorization Model alle Procedure

- Se identifichiamo attraverso l'analisi del Rischio le aree d'azione del CSIRT possiamo anche predisporre un impianto di processi, policy e procedure per distribuire le responsabilità in modo preventivo, strutturato e organico…

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Create policies



Create Policies

- **User incident reporting**
  - Gli utenti devono essere sensibilizzati a segnalare situazioni sospette e possibili incidenti
  - Gli utenti devono poter essere coinvolti nell'identificazione degli incidenti di Sicurezza e nella loro risoluzione.
- **Incident response**
  - Ogni incidente deve essere analizzato prontamente e gestito con l'appropriata priorità.
  - CSIRT Program.
- **Responsabilità del CSIRT**
  - Ogni componente deve avere ruoli e responsabilità e deve essere in grado di "agire" in modo coordinato con il resto del Gruppo.

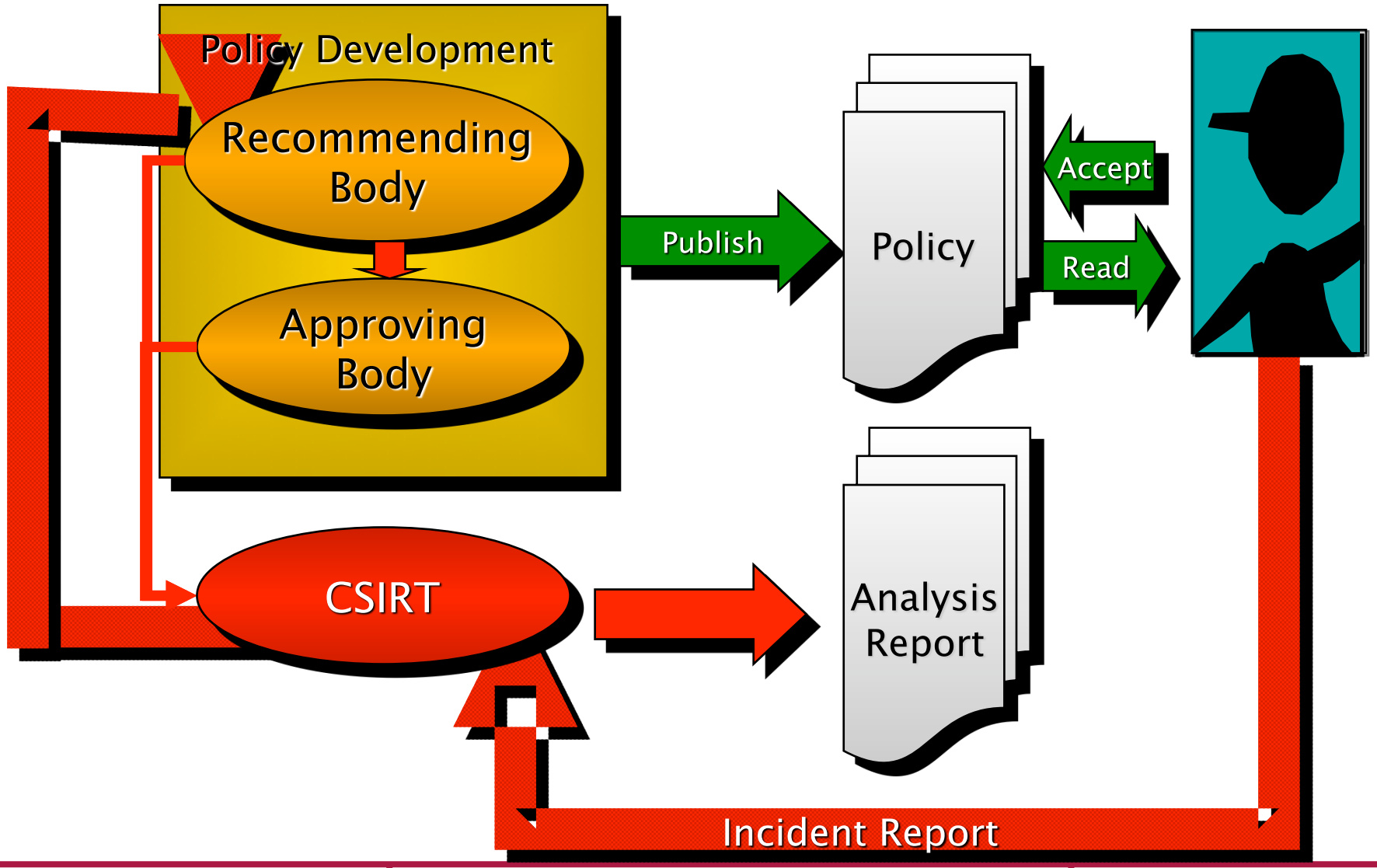
Come attuare queste Policy?

- Ci sono molte sorgenti valide:
  - NIST SP800-61
  - SANS Institute
  - CERT
  - GovCert
  - TERENA

- È essenziale “ritagliare” una soluzione su misura per l’azienda.

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Il processo “virtuoso” nell’IR



ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Agenda

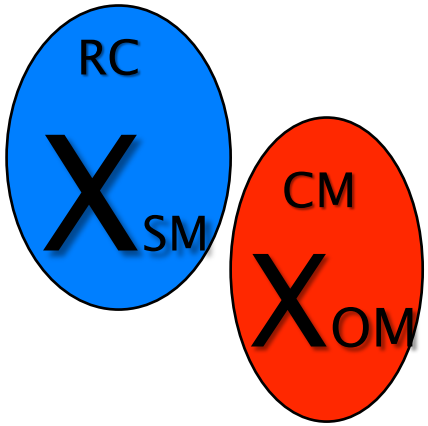
- **Introduzione**
- **Creare un CSIRT**
  - Requisiti per stabilire un efficace CSIRT
  - Individuazione definizione ed attuazione delle politiche e delle procedure
  - Piano strategico per l'implementazione di un CSIRT
- **L'incidente Informatico**
  - Il montaggio reattivo. Meccaniche di progettazione dell'intervento e problematiche operative
- **Introduzione sui livelli di Servizio (SLA)** che possono essere forniti da un CSIRT
- **Alcuni elementi organizzativi per un CSIRT**
- **Alcuni esempi** e alcune esperienze nazionali ed internazionali

Modelli Organizzativi: Linguistica

- **Evento** – occorrenza osservabile
- **Incidente/Avversità** – occorrenza con impatto negativo
- **Minaccia** – rischio potenziale che può generare un Incidente /Avversità
- **Indicatore** – sorgente dell'informazione
- **Tipologie di Incidenti** – Tipi di avversità (legate alla struttura)
- **Tracing** – tracciatura dell'incidente

CSIRT – Struttura

- **Responsabile CSIRT (RC)**
  - Solitamente un Security Officer
- **CSIRT Manager (CM)**
  - Solitamente un operativo appartenente al Dipartimento di Sicurezza (può anche essere una figura in outsourcing)

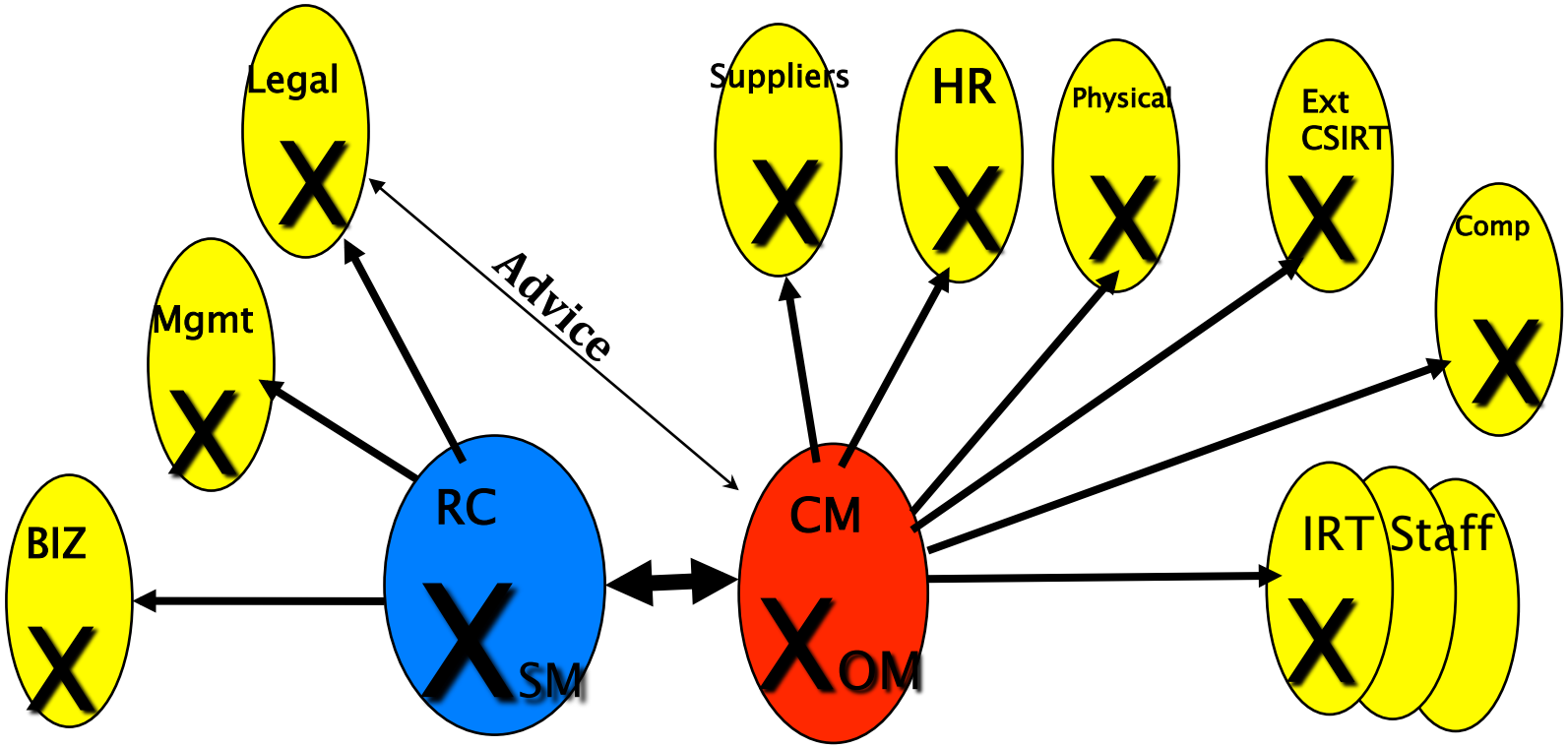


CSIRT - Struttura

- **IRT Manager (CM)**: è l'interlocutore privilegiato del Responsabile del CSIRT; è chiamato a garantire il conseguimento degli obiettivi attribuiti al CSIRT e pertanto deve:
  - guidare l'efficacia e l'efficienza del processo di gestione degli incidenti;
  - produrre informazioni per il management;
  - gestire il lavoro del personale di supporto agli incidenti;
  - monitorare l'efficacia dei processi di gestione degli incidenti e fornire raccomandazioni per il miglioramento continuo;
  - sviluppare e mantenere le procedure operative per la gestione degli incidenti.

CSIRT – Struttura Operatori

- **Skill Appropriate**
- **Gruppi organizzati in modo appropriato**
- **Comprensione del ruolo dei singoli**

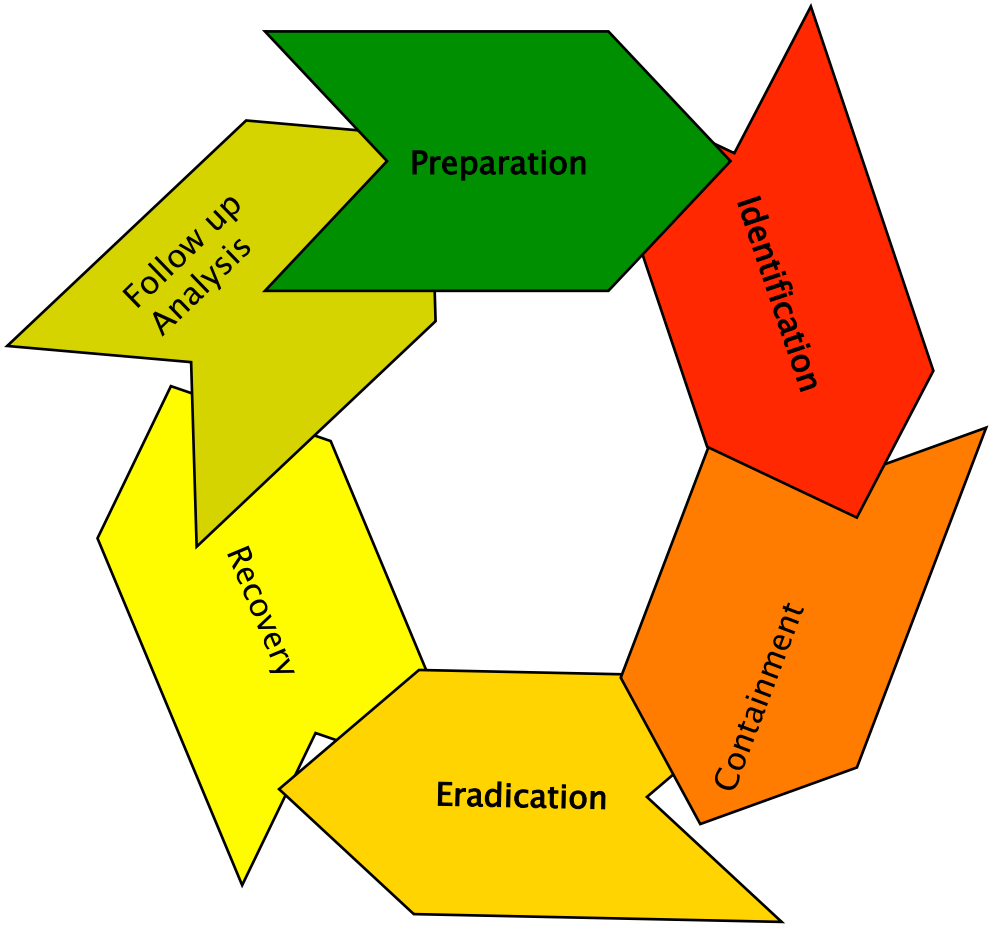


Mission – Proteggere la struttura

- **Filosofia**
  - **Bloccare immediatamente l'incidente.**
  - **Acquisire prove.**
- **Obiettivi**
  - **Immediato stop di qualsiasi minaccia attiva**
  - **Minimizzare l'impatto degli incidenti di Sicurezza nell'Azienda attraverso il contenimento e il monitoraggio delle minacce**
  - **Rispondere alle minacce di Sicurezza segnalate**
  - **Collezionare e processare i dati in modo da poterli utilizzare come prove in caso di denuncia di attività illecite**
  - **Attuare reportistica e documentazione post-incidente da poter fornire alle Autorità e al CERT nazionale**
  - **Affinare i meccanismi di risposta agli incidenti (azioni e procedure) attraverso simulazioni, test e valutazioni delle azioni svolte in precedenza**

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Hard Lessons Learned…



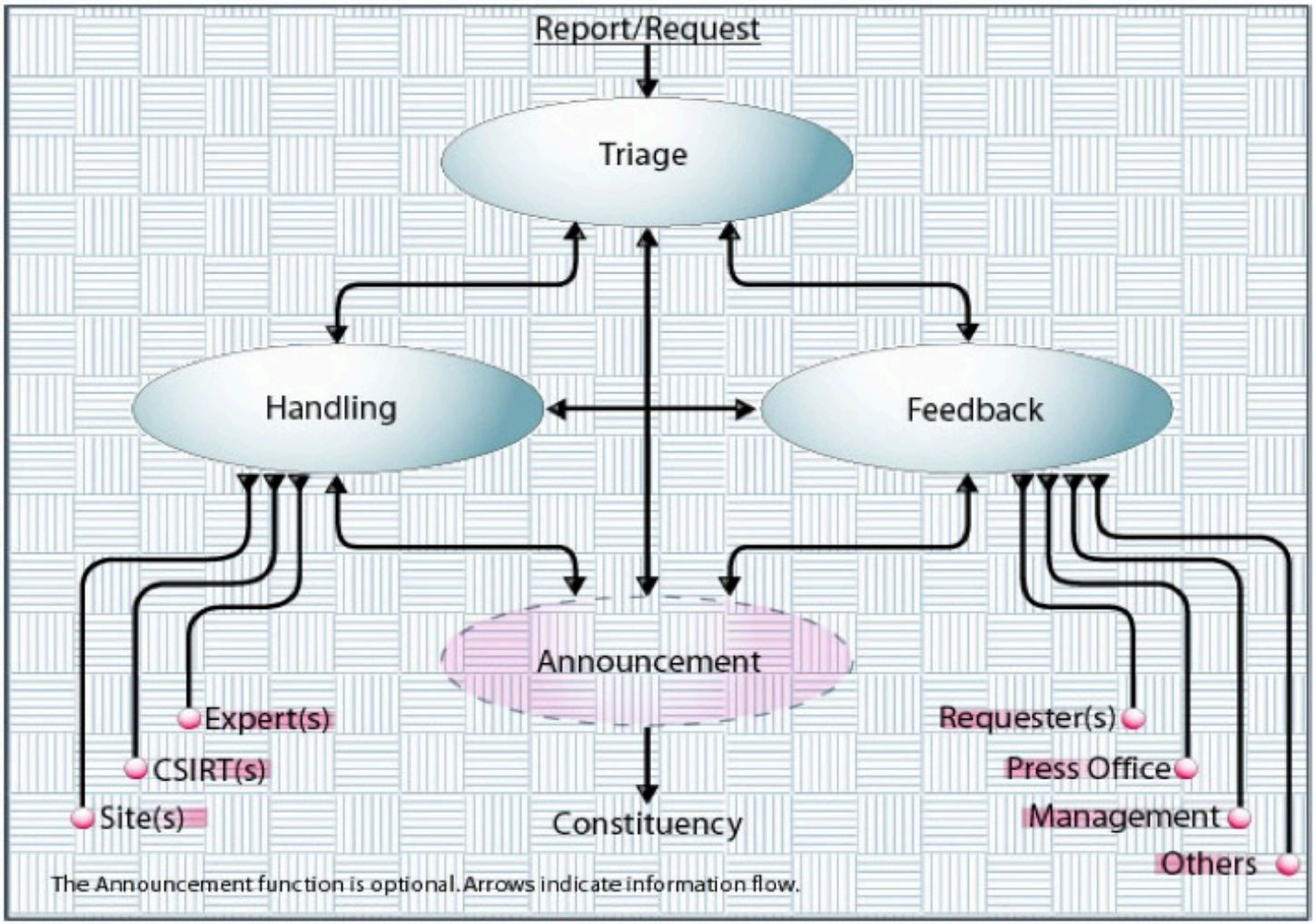
- **Documentare tutto!**
- **Presentare agli utenti differenti meccanismi di contatto con l'IRT.**
- **Avere sempre strumenti in grado di collezionare log a livello utente e sistema**
- **Mantenere aggiornate le informazioni per il contatto delle risorse del CSIRT.**
- **Centralizzare i controlli**
- **Strutturare in modo organico i rapporti con le altre strutture IT**
- **Apprendere dagli errori passati**
- **Testare e aggiornare le procedure regolarmente**

Incident Handling Service

L'**Incident Handling Service** comprende le seguenti funzioni:

- Triage
- Handling
- Announcement
- Feedback

Incident Handling Service



ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Triage Function

La Funzione Triage è il punto focale per l'accettazione, raccolta, smistamento, ordinazione e trasmissione delle informazioni.

Canale attraverso il quale tutte le informazioni vengono passate all'esterno

Supporta diversi canali di ingresso adeguati ad esigenze specifiche

Ad ogni nuovo evento viene associato un trackingnumber ed un initial priority

Sono presenti azioni aggiuntivi: Archiving, Translation o Media Conversions

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Handling Function

Guida e sostegno per presunti/confermati incidenti di sicurezza informatica, minacce e attacchi

Revisione di un Incident Report per determinare ed avere un quadro delle attività verificate

Indentificare chi è coinvolto (o ha bisogno di essere contattato)

Indentificare l'assistenza necessaria per proseguire

Individuazione di risposte adeguate (in linea con gli obiettivi e servizi della CSIRT) e conseguente notifica o follow-up

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Announcement Function

Genera informazioni su specifiche su:

- Minacce in corso
- Misure da adottare per la protezione contro queste minacce
- Varie informazioni sulla natura di attacchi recenti/ simili

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Feedback Function

Offre supporto per fornire feedback a questioni non legate direttamente all'incidente

I Feedback possono essere forniti su esplicita richiesta (es. da parte dei media), su di un timeframe constante (es. relazioni annuali) o case-driven (es. informando i media proattivamente)

Fornitura di un numero minimo di risposte a FAQ e può essere utilizzato per interfacciarsi con i media e per raccogliere informazioni generali da parte del Team

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Triage Function

Garantire che tutte le informazioni destinate all'IncidentHandling Service vengano trasmesse ad un unico punto indipendentemente dal metodo o forma in cui arriva (es. e-mail, fax, telefono, posta)

Un singolo pointofcontact è identificato dal CSIRT indipendentemente dal servizio richiesto

Informazioni e contatti dei membri di squadra non deve essere rivelata in modo che il Triage Function può essere bypassato

Per stimolare la comunicazione e la raccolta di tutte le informazioni pertinenti, il CSIRT deve fornire meccanismi efficienti per la segnalazione:

- Un point of contact ben definito
- Dettagli sulla disponibilità del point of contact
- Linee guida sul tipo di informazioni da riferire
- Documentazione di supporto (es. modulistica)

- Una volta che le informazione sono ricevute dal triage, una notifica di avvenuta ricezione dovrà essere inviata

- Le informazioni saranno quindi ordinate e trasmesse in base ad altre regole stabilite all'interno del servizio

- Inoltre laTriage Function deve decifrare messaggi criptati e verificare firme digitali, conservare queste informazioni per un utilizzo successivo, e consentire effettivamente la lettura del contenuto

- La Triage Function deve avere accesso al repository di dati utilizzati da ciascuna delle altre funzioni dell'Incident Handling Service

Se le informazioni sono insufficienti o incomplete, è probabile che la Triage Function sia lenta, imprecisa, o inefficente.

In questi casi può essere necessario richiedere informazioni più dettagliate dal mittente prima che le informazioni possano essere adeguatamente raccolte dal Triage.

Inoltre altre misure possono essere adottate per migliorare la qualità delle informazioni:

- Utilizzo di Tracking Numbers
- Utilizzo di moduli di segnalazione standard
- Pre-acquisizione di Contact Information

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Tracking Numbers

In un robusto sistema di monitoraggio, i Tracking Numbers sono i "tag" che il sistema utilizza automaticamente per ordinare le informazioni in entrata (correlate) con le altre attività connesse, senza la necessità di intervento umano.
Questo semplifica il processo e consente alla Triage Function di concentrarsi più intensamente sulla correlazione corretta delle informazioni taggate.
I numeri possono essere facilmente utilizzati nella riga dell'oggetto dei messaggi di posta elettronica, documentato su copertine di fax, e specificati in messaggi vocali.
I numeri dovrebbero essere utilizzati per il monitoraggio degli eventi nell'ambito di ciascuna funzione dell'Incident Handling Service.

Feedback, incidenti, e gli annunci dovrebbero tutti avere un proprio Tracking Number.

Tracking Numbers

Devono essere unici

Best Practice: utilizzare un prefisso unico per ognifunzione, e garantire anche che il numero di tracking che segue il prefisso è unico

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Tracking Numbers

2 tipi di Tracking Numbers

- Unique Intra-CSIRT Tracking Numbers – Tracking number utilizzato nel CSIRT

- Unique Inter-CSIRT Tracking Numbers – Tracking number utilizzato tra i vari CSIRT

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Tracking Numbers

Se un Tracking Number viene utilizzato per monitorare un evento, di solito è il caso che sia uguale dall'apertura alla chiusura del caso

Particolari casi:

• L'informazione di Triage è sbagliata: La Triage Function può identificare un evento come nuovo anche se questo stesso evento è già presente

• L'informazione è Taggata erroneamente: L'informazione può essere trasmessa con un Tracking Number sbagliato, di conseguenza viene monitorata e smistata in modo sbagliato

• Un evento è riaperto: se un evento è chiuso ma si ricevono nuove informazioni, allora l'evento sarà riaperto

•Merge di eventi: Quando si presentano nuove informazioni che collegano due o più casi, le informazioni vanno analizzate attentamente. In questicasi, archiviarele informazioni risulta molto difficile

Tracking Numbers

Le seguenti informazioni sono richieste:

- Contact information delle persone coinvolte o terzi che devono essere contattati
- Nomi ed i network address dei host coinvolti nell'incidente
- La natura dell'attività
- Descrizione delle attività edinformazioni rilevanti (es. i log, fusi orari…)
- I Tracking Numbers che potrebbe già essere assegnati (da una local security teamodaun altro CSIRT)

Incident Life Cycle

Notare che un incidente (o un evento)può percorrerela parte di analisi più volte durante ilsuo life cycle.

La chiusura di un incidente si verifica normalmente quandotutte le parti coinvolte nell'incidentenon hanno ulteriori nuove informazioni riguardante il caso e tutte le possibili azioni sono state effettuate

Incident Handling Life Cycle

Incident Life Cycle

Altri stati di transizione:

- Action required: Sono richieste azioni da parte del team riguardo l'incidente
- Waiting: La squadra è in attesa di una risposta daterze parti esterne alla squadra

Quando un CSIRT decide di chiudere un incidentedeve garantire che tutte le parti interessate siano o sarannoinformatedella chiusura

Un incidente precedentemente chiuso potrebbe essere riaperto se emergono nuove informazioni (es. un rapporto di attività ha riacceso in uno dei siti coinvolti)

In caso di necessità di riaprire un incidente, il Tracking Number originale deve essere riutilizzato se possibile.

Tuttavia, se l'attività non è considerata una continuazione del caso originale, è opportuno generare un nuovo evento per l'attività e di emettere un nuovo Tracking Number associato ad esso

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Incident Analysis

La prima analisi di un incidenti avviene durante la Triage Function, che si verifica ogni qualvolta emergano nuove informazioni.
Ci sono duetipi di analisidi un incidente da prendere in considerazione:

• Intra-Incident Analysis
Analisi delle questioni riguardanti uno specifico incidente. I tipi più comuni sono i seguenti:

- Analisi di eventuali artefatti lasciatidalle attività di intrusione (file di log, exploit, virus,trojan, toolkit, ecc)
- Analisi del ambiente software
- Analisi del web-of-trust all'interno di un incidente

• Inter-Incident Analysis
Analisi delle questioni relative ai rapportitra incidenti. Tale analisi è volta a individuare le simmetrie tra i diversi incidenti che potrebbero indicare le fontisimili o attività connesse.

Esempi ed esperienze

tunCERT
Tunisian Computer Emergency Response Team

Fermilab

eCSIRT

Cornell University
Cornell Information Technologies

Tunisian CERT presentation

Constituency	National CSIRT
Mission statementg	Defined by law : protection the Tunisian cyberspace
Offred Services	To be detailed
Funding	Gouvernement
Revenue	Free charge services
Number and quality of staff to be employed	50 for NACS 20 for cert-Tcc
Authority	Partial authority (Law N°5/2004)
Service hours	24/7

Services

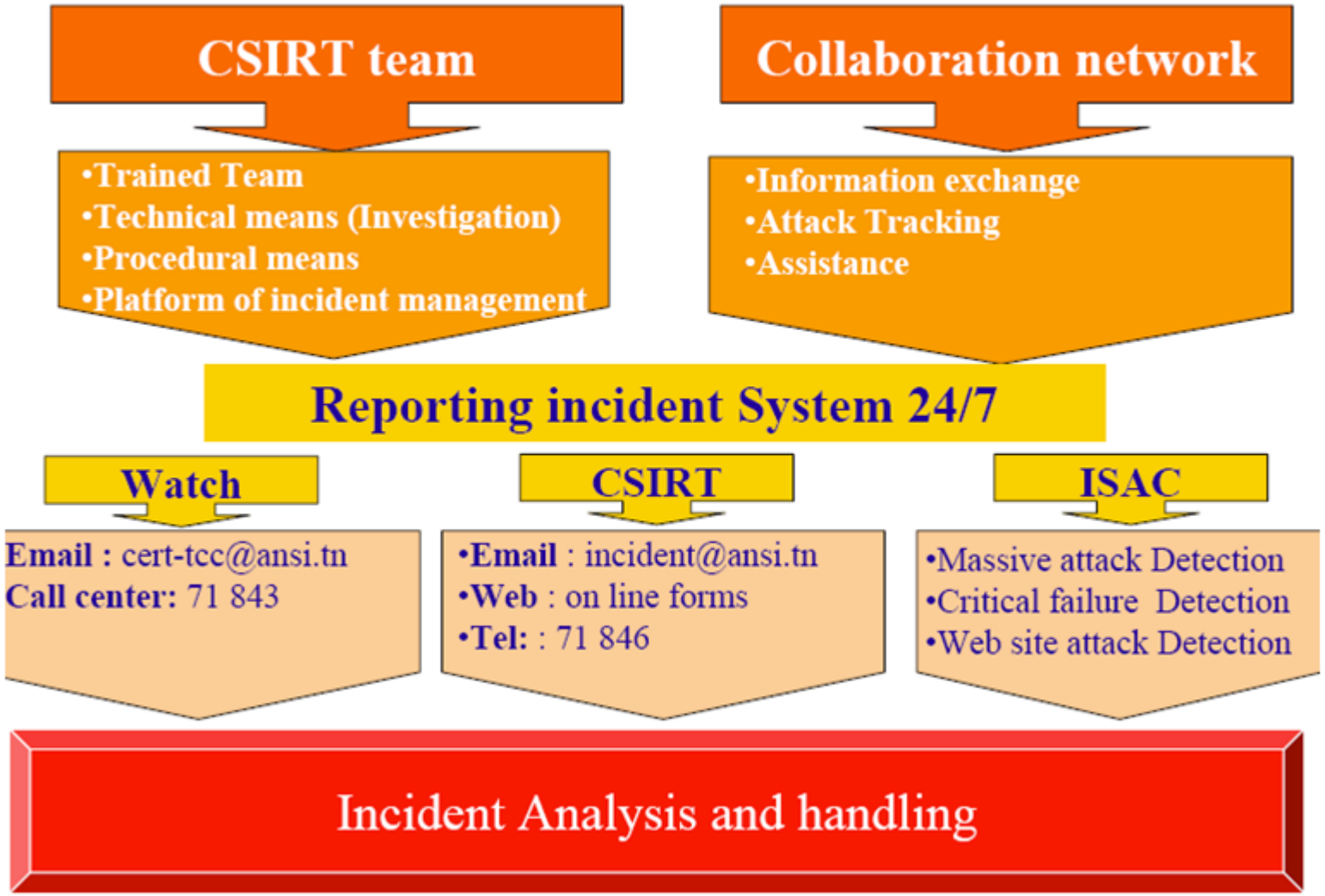
Main services

Incident analysis	Incident response on site	Incident response support
Incident response coordination	Publish advisories or alerts	Vulnerability and Virus handling
Provide and answer a hotline	Monitor IDS	Training or security awareness
Technology watch or monitoring service	Track and trace intruders	Penetration testing

Secondary services

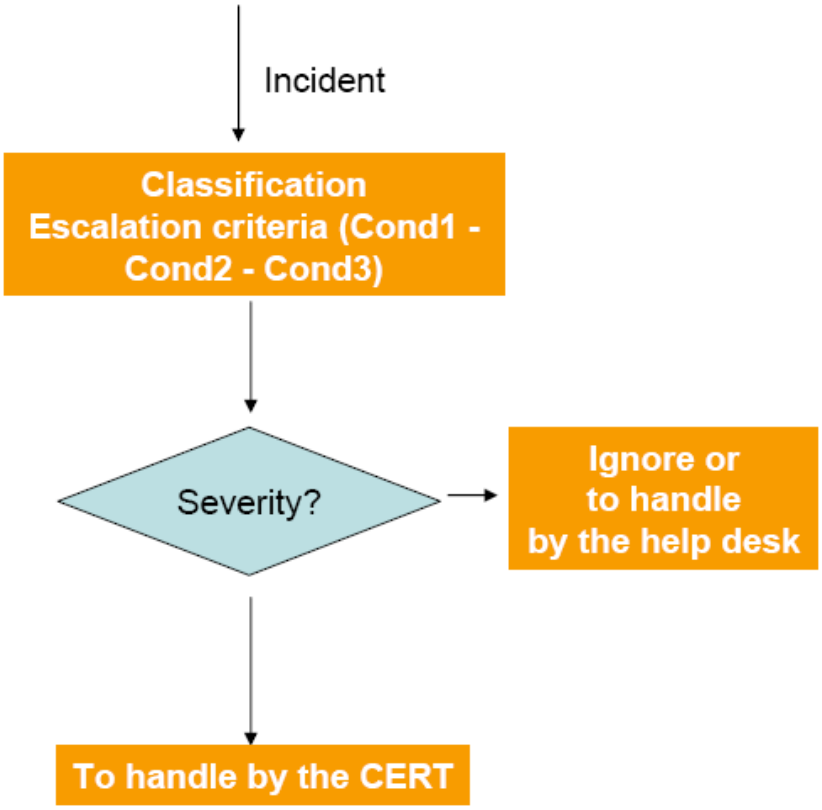
Security policy development	Produce technical documents	Vulnerability assessments
Artifact analysis	Forensics evidence collection	Pursue legal investigations
Vulnerability scanning	Security product development	Monitoring network and system logs

Services


CSIRT team
Collaboration network
•Trained Team
•Technical means (Investigation)
•Procedural means
•Platform of incident management
•Information exchange
•Attack Tracking
•Assistance
Reporting incident System 24/7
Watch
CSIRT
ISAC
Email : cert-tcc@ansi.tn
Call center: 71 843
•Email : incident@ansi.tn
•Web : on line forms
•Tel: : 71 846
•Massive attack Detection
•Critical failure Detection
•Web site attack Detection
Incident Analysis and handling

Incident Classification

Incident	Severity		
	Cond1	Cond2	Cond3
Spam	S1	S2	S2
Harassment	S2	S3	S3
Pedophilia/Pornography/Violence/..	S4	S4	S4
Malware (Virus, Warm, Trojan, Spyware, Dialer, Keylogger)	S1	S3	S4
Scan	S3	S4	S4
Sniff	S3	S4	S4
Social Engineering	S3	S3	S3
Vulnerability Exploit	S3	S4	S4
Brute Force	S3	S4	S4
Defacement	S2	S4	S5
DoS	S4	S5	S5
DDoS	S5	S5	S5
Sabotage	S3	S4	S4
Copyright	S2	S2	S2
Identity theft	S2	S3	S3
Phishing	S4	S5	S5



FCIRT

Fermilab

- L'esempio del FCIRT è interessante per il meccanismo di Incident Management attuato che lascia spazio, in caso di "incidente minore" all'autonomia del gestore della piattaforma specifica, senza ricorrere direttamente all'intervento dell'IRT, ma solo alla sua supervisione.

Modalità operative FCIRT

- A seguito dell'alert, il personale del CSIRT si attiva per identificare e classificare l'incidente che ricade in una delle seguenti tipologie:
  - **No incident**
  - **SMOKE** - Si tratta di un incidente minore che può essere gestito dal persone dell'area sotto la supervisione del personale FCIRT. *Possono essere richieste ulteriori investigazioni dal FCIRT.*
  - **FIRE** – Incidente Grave. Il personale FCIRT assume tutti i gradi di controllo del sistema coinvolto e può attuare una escalation di privilegi anche su altre piattaforme potenzialmente coinvolte.

Modalità operative FCIRT

- **SMOKE**
  - Uno “SMOKE” è dichiarato se ci sono evidenze dell’accadimento di una compromissione o di un’anomalia. Il personale FCIRT può decidere di attuare un’investigazione direttamente o può guidare il personale d’Area.
  - Se l’investigazione mostra problemi confinati ad un singolo sistema con un impatto minimo o nullo su utenti e asset si delega il “clean-up” e il “recovery” al personale che gestisce quotidianamente la piattaforma.
  - Nel caso in cui l’incidente abbia o possa avere un più ampio e critico impatto lo stato dell’incidente passa a FIRE.

SMOKE Esempio

- **SMOKE**
  - Definisce situazioni quali virus il cui vettore di propagazione sia noto.
  - In questo caso la Procedura è ordinaria:
    - Uso di un AntiVirus
    - Oppure reinstallazione del Sistema da fonte certificata.
    - Verifica del livello di patches e aggiornamenti
    - Scansione attraverso un AV aggiornato
    - Verifica dei dati hardware del sistema (NICs are registered
    - Riattivazione (Return to service)

FIRE Esempio

- **FIRE**
  - Un FIRE è dichiarato quando un incidente coinvolge sistemi critici, impatta molti utenti o in qualche modo danneggia le attività del Laboratorio.
  - Il personale FCIRT dietro segnalazione del suo responsabile, prende il completo controllo dei sistemi coinvolti
  - Questa azione può comportare varie casistiche, dal distacco dalla rete alla confisca del Sistema seguendo delle procedure prestabilite.

FIRE Esempio

- **FIRE**
  - Il primo obiettivo è il contenimento del danno. Questo obiettivo si raggiunge attraverso la disconnessione dalla rete per via logica o fisica.
  - Lo stato del sistema sarà esaminato per determinare come possa essere stato compromesso, ad esempio
    - Password debole (SQL – "SA" senza password)
    - Vulnerabilità
    - Errori di configurazione

FIRE Esempio

- **FIRE**
  - I log di rete (Network records) vengono esaminati per valutare quali e quanti sistemi sono stati coinvolti nell'evento
  - Si concerta internamente al FCIRT quali azioni devono essere intraprese per proteggere i sistemi dalla compromissione e si attivano i processi di eradication.
  - Si attiva lo specialista forense che svolgerà una copia completa dei dati delle macchine coinvolte e documenterà tutte le procedure di analisi in favore delle autorità governative.
  - I Sistemi saranno "ripristinati" e ritorneranno in Servizio

Report

- **Reporting**
  - Ogni incidente IT attiva una serie di flussi di reportistica
  - In caso di "FIRE" tutti i manager dei sistemi coinvolti, tutti i responsabili di ogni divisione e tutti i referenti saranno informati dal Leader del FCIRT (punto di contatto).
  - In alcuni casi, specificamente definiti, verranno informate anche le agenzie governative
  - Report giornalieri saranno svolti fino alla chiusura dell'incidente

Problemi

- Gestire troppi servizi
- Scarsità di tempo, risorse umane e mezzi economici
- Coordinamento
- Supporto dalla Comunità (Costituency)
- Standardizzazione della reportistica di incidente
- Il “Burnout”

Sfide

- Processo di Incident Handling automatizzato
- Processo di Gestione delle Vulnerabilità automatizzato
- Selezione efficace delle sorgenti attendibili per l'approvvigionamento delle informazioni iniziali
- Collaborazione e condivisione delle informazioni con altre realtà
- Attivare delle modalità di scambio efficaci e protette
- Maggiore integrazione con i processi Interni

Difficoltà

- ROI (Return of Investiment)
- Certificazioni in materia di CERT
- Problemi legali
- Condivisione di dati e misure
- Identificazione di strumenti adeguati alle finalità del CERT

ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

Se sospetti che il tuo sistema è compromesso cosa devi fare?

- Rimani calmo; non ti agitare.
- Notifica al tuo manager il problema.
- Apply need-to-know.
- Usa meccanismi di comunicazione out-of-band; evita le email o altri canali di comunicazione basati sulla rete IT.
- Prendi nota di ogni anomalia, potrebbe servire in caso di spiegazione e supporto all'IRT.
- Se possibile, contieni il problema, disconnetti dalla rete il dispositivo (stacca il Cavo di Rete!).
- Se possibile, fai un backup del sistema e colleziona prove.

Grazie per l’attenzione

Autori

Stefano Maccaglia
Raffaele “r4ff0” Addesso
Luigi “C4V” Cavucci