maggio 2016

Strategie aziendali per la Cyber Security

La mia Azienda non può essere un suo obbiettivo – FALSO !!!

La mia Azienda è protetta da Firewall e Antivirus – FALSO !!!

OGNUNO
DI NOI
E' UN TARGET

Cosa fare ?

Bisogna cambiare approccio !!!

La soluzione ?....

Come cambiare ?

CONSAPEVOLEZZA

- I pericoli possono arrivare sia dall'esterno che dall'interno dell'Azienda
- Prima o poi ogni Azienda si trova nelle condizioni di gestire un incidente di sicurezza

FORMAZIONE

- Diffondere cultura nell'ambito della Sicurezza Informatica, includendo anche i rapporti con l'ecosistema fornitori e clienti

RISK ASSESSMENT

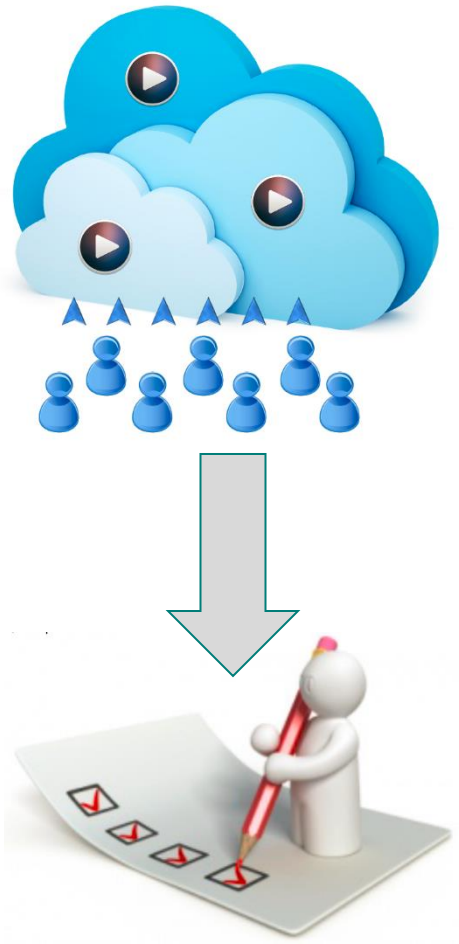
- Non tutti i dati e le informazioni aziendali hanno stesso valore e criticità
- Verificare i livelli di sicurezza implementati, rispetto a standard e modelli di riferimento
- Decidere eventuali investimenti progettuali considerando il rapporto rischio/impatto

PROGETTUALITA'

- Gli interventi progettuali devono indirizzare concetti di prevenzione, controllo e reazione
- E' necessaria l'introduzione di adeguati livelli di Security Intelligence

Formazione

- **Spesso l'anello debole è l'utente**
- **Formazione per educare gli utenti aziendali a**
  - ✓mantenere comportamenti corretti nell'utilizzo dei sistemi HW e/o SW
  - ✓utilizzare e gestire correttamente dati e informazioni
  - ✓conoscere e rispettare le policies di sicurezza aziendali
- **Indirizzare progetti di formazione che affrontino temi specifici in ambito sicurezza informatica tramite**
  - ✓seminari per Responsabili IT e/o Security
  - ✓corsi WEB e/o videoclip per gli utenti
- **Controllare lo stato di avanzamento attraverso un Portale WEB, dove**
  - ✓gli utenti possano accedere per seguire corsi/video formativi
  - ✓gli utenti possano rispondere ad un questionario per verificare i livelli di comprensione della tematica trattata
  - ✓i Responsabili IT possano tenere traccia degli accessi, delle attività svolte e del livello di formazione raggiunto



Risk Assessment

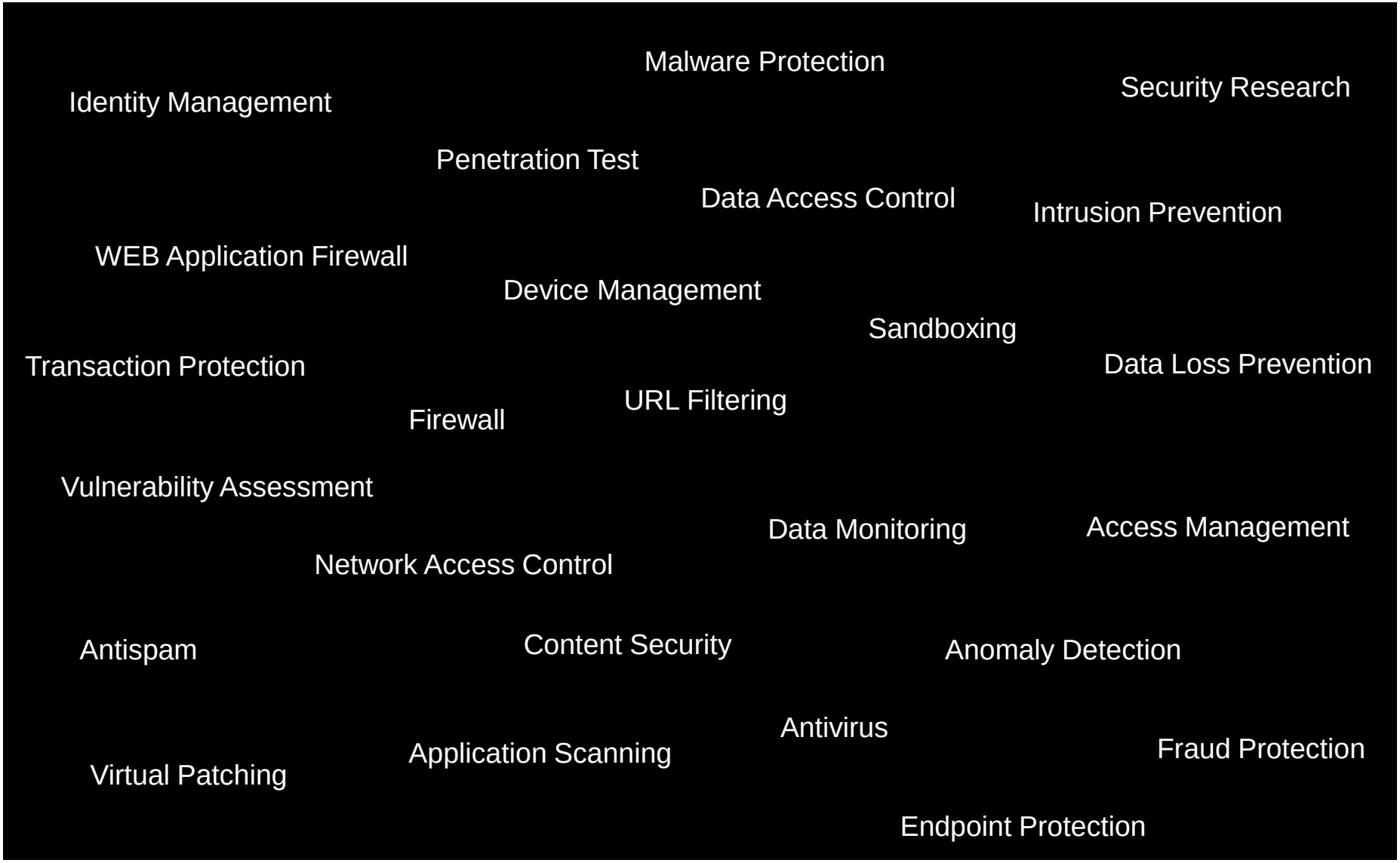
Le minacce informatiche sono un dato di fatto e sono sempre più sofisticate.

Ma quando la minaccia diventa incidente di sicurezza ? Cosa comporta questa eventualità ?

Analisi e gestione del rischio devono prevedere:

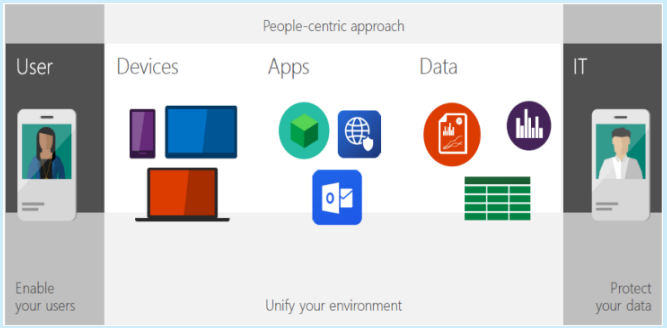
- ❑Una classificazione dei rischi che tenga presente tutte le componenti aziendali: utenti, infrastruttura, applicazioni e dati
- ❑Le possibili ripercussioni derivanti da un incidente di sicurezza in termini di:
  - ✓Perdite economiche
  - ✓Reputazione
  - ✓Vantaggio competitivo

Tipica situazione in Azienda



Progettazione

Prevenire → **Controllare** → **Rispondere**

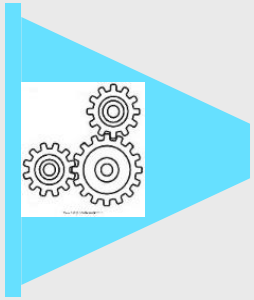


prodotti e/o soluzioni specifiche per

- Formazione
- Applicazioni/servizi
- Dati
- Network
- Endpoint

SIEM

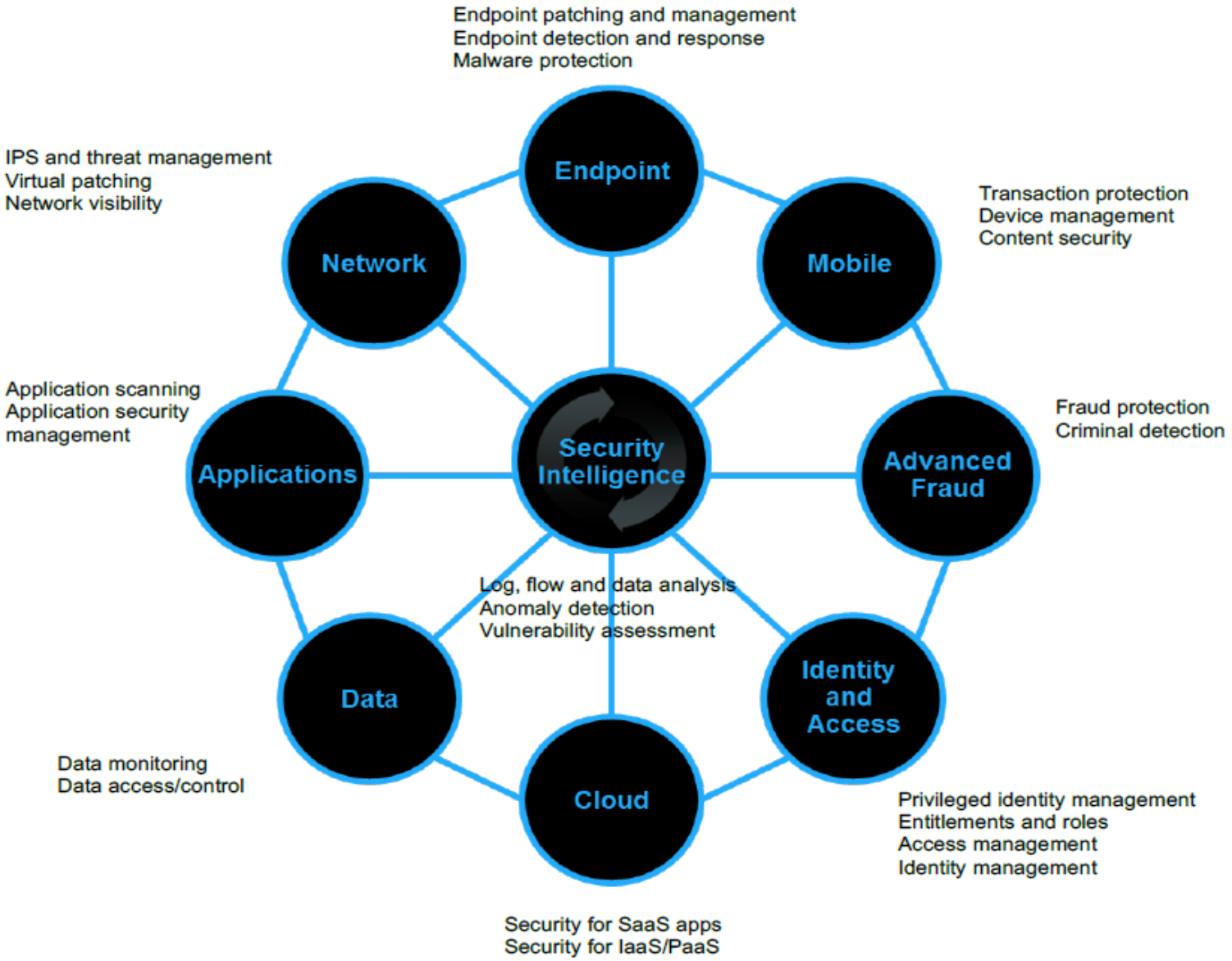
SOC – Security Operation Center



- correlazione intelligente dei log
- classificare e prioritizzare gli eventi
- monitoraggio esperto H24
- indagine forense
- supporto nella gestione degli incidenti informatici
- Servizi periodici di VA e PT

Componente fondamentale per introdurre adeguati livelli di Security Intelligence

Scenario a cui tendere



Grazie per la vostra attenzione

Paolo Baldelli
p.baldelli@vargroup.it
335.7478384