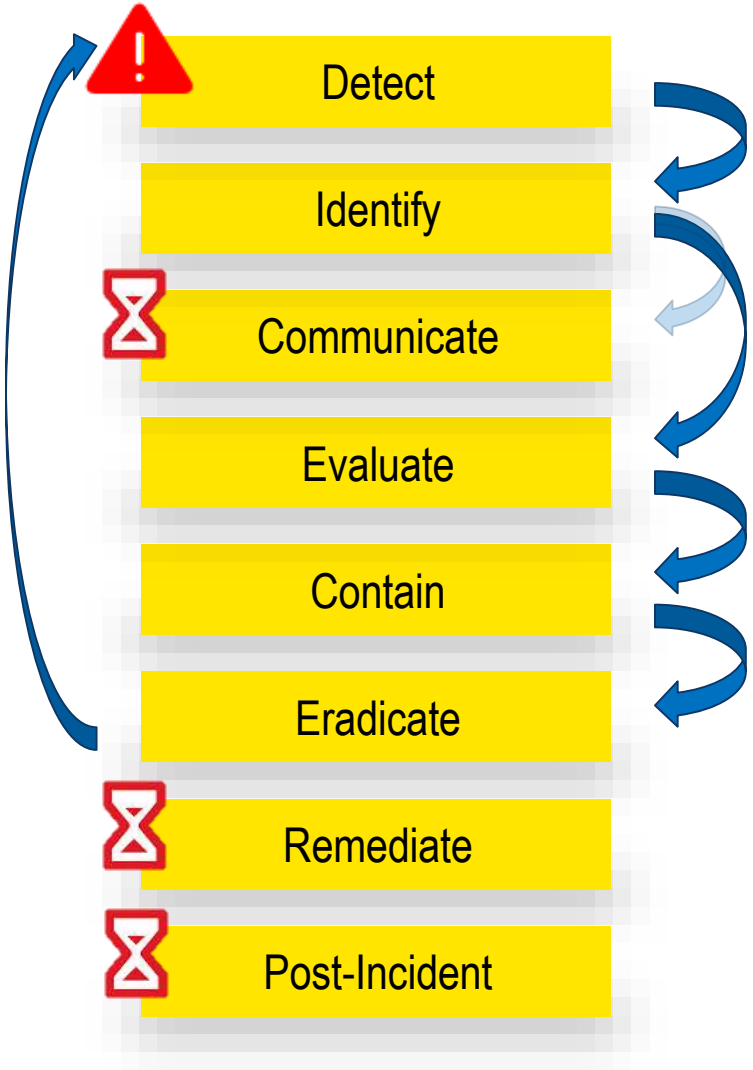
Incident response Vs. Remediation

Marco Di Leo, Consulting Technical Lead
Hewlett Packard Enterprise Security Services

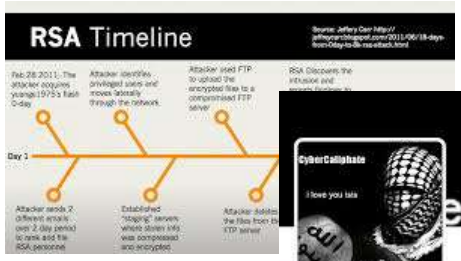
Il Processo

(nel mondo reale)

Cosa succede in realtà



Cosa sta cambiando?



1998 Lockheed Martin, DOD & NASA

2011 RSA, Google, Rackspace & Juniper Networks

2012 Iranian Centrifuges, NATO & Shell

2015 Multiple organisations across all industry

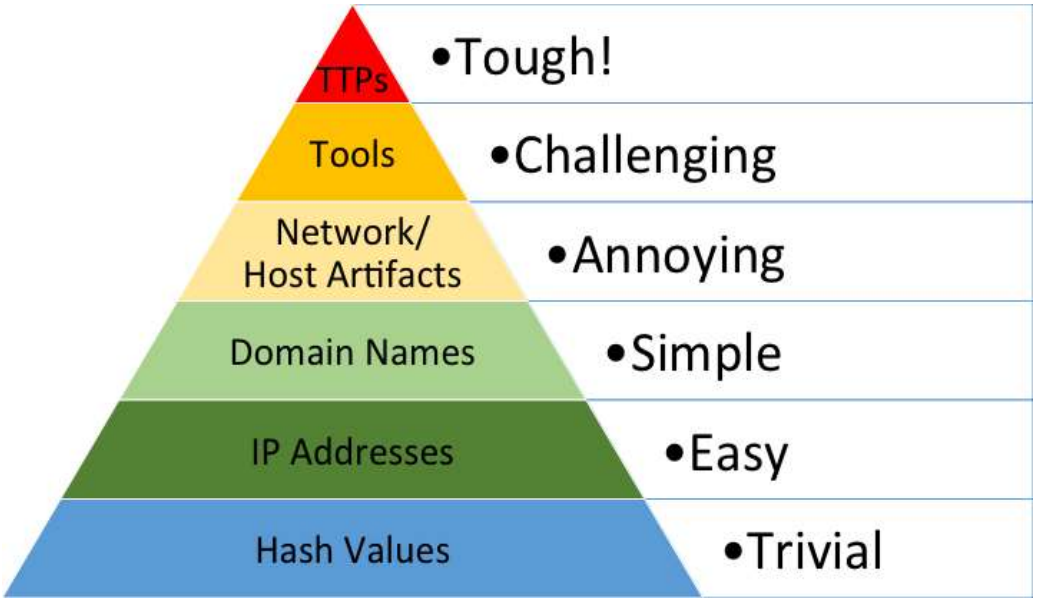
La Remediation

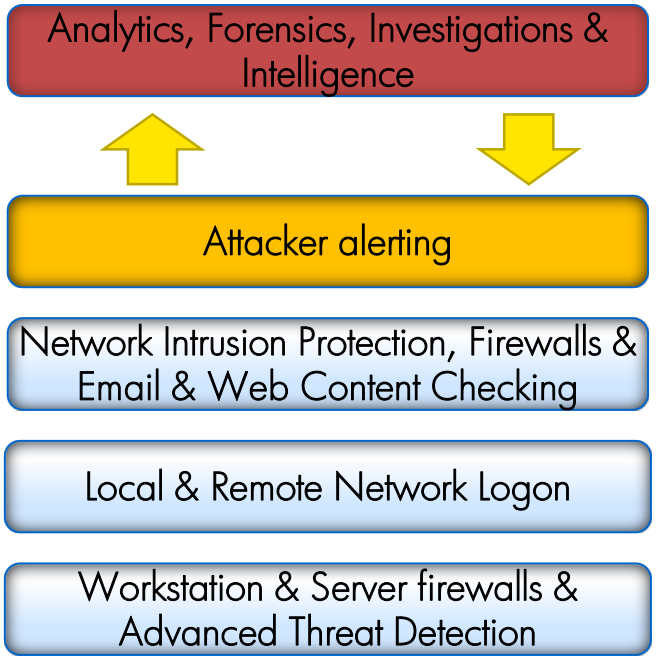
La condotta della guerra si fonda sempre sull’inganno. Quando si è in grado di attaccare, si deve apparire incapaci; quando si muovono le truppe, bisogna sembrare inattivi; quando si è vicini al nemico, bisogna fare in modo che egli creda che si è molto lontani; quando si è lontani, il nemico deve crederci vicini.

Sun Tzu

La battaglia della persistenza

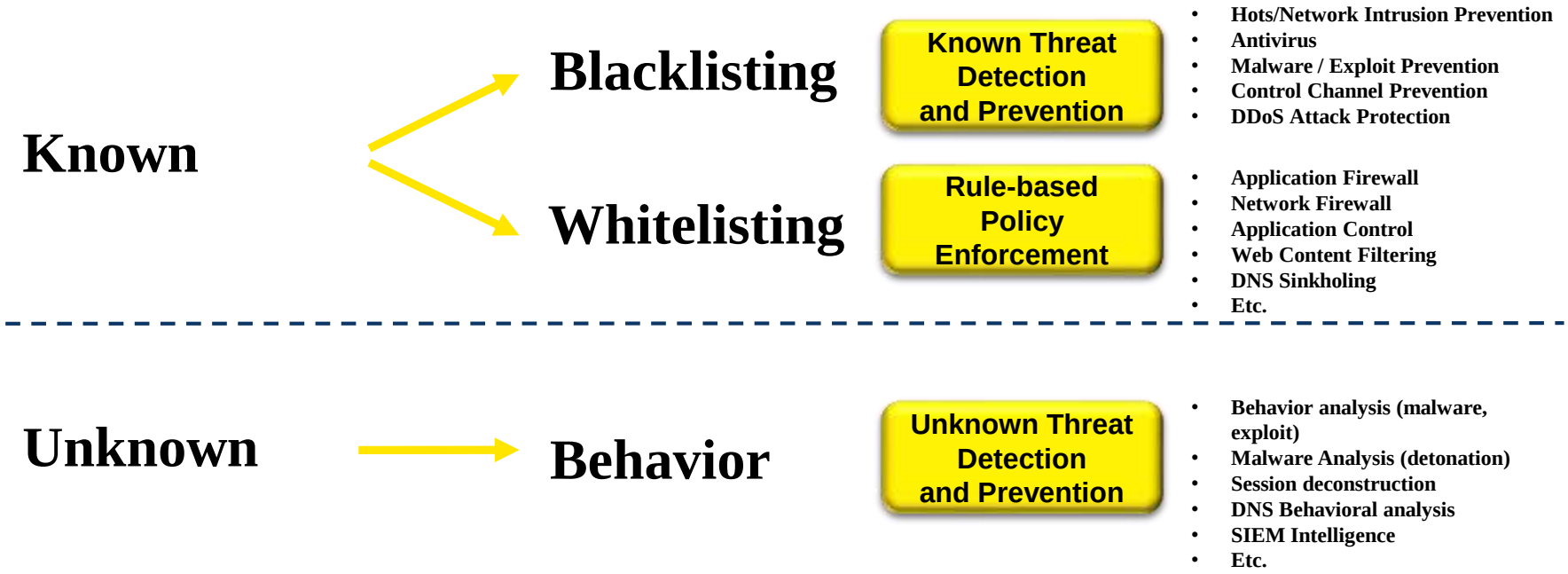
Pyramid of Pain*





* from David Bianco

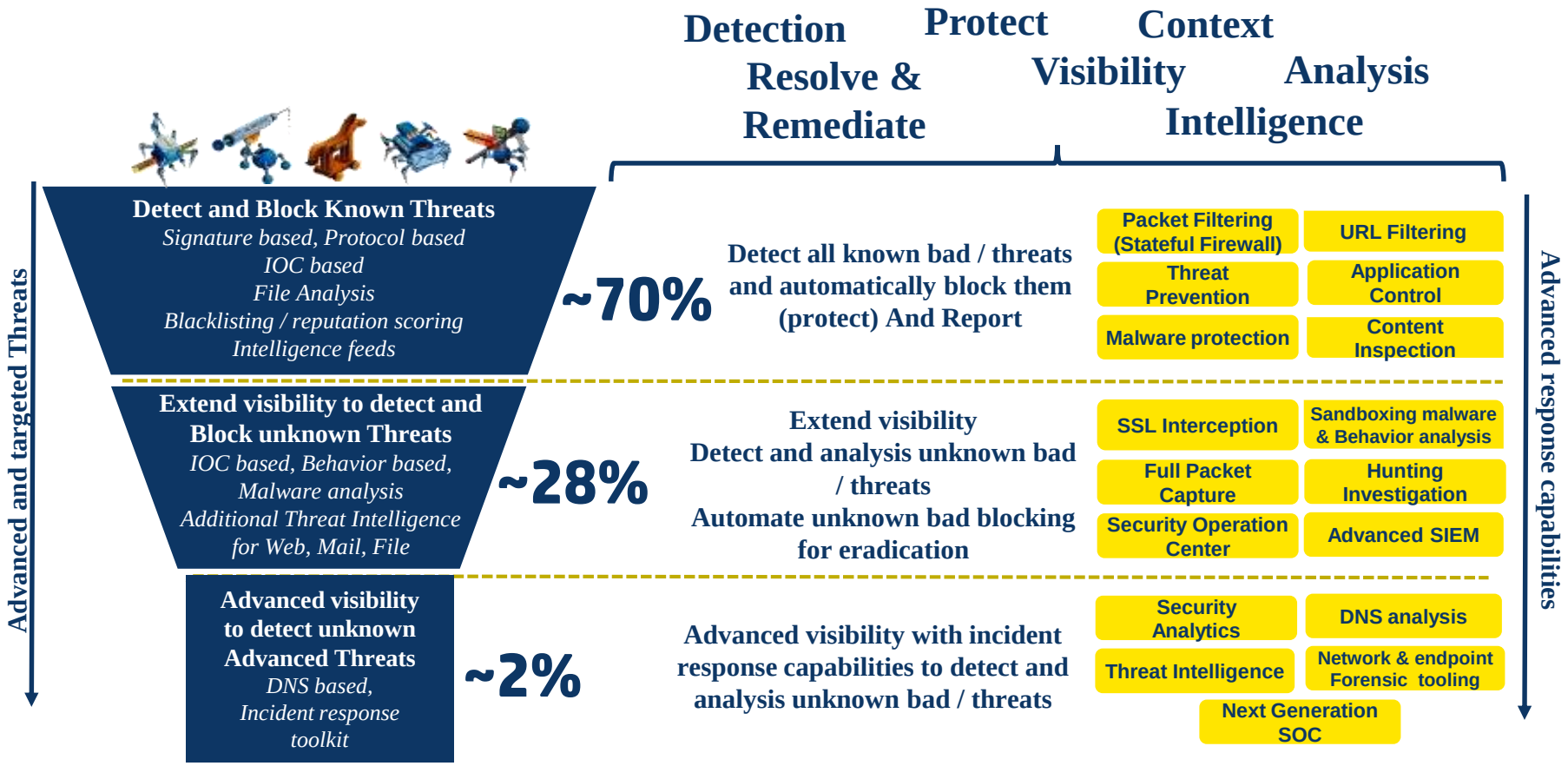
Minacce conosciute ed ignote



Eliminare gli avversari

- Per rimuovere gli attaccanti dalla rete è essenziale un attento piano strutturato in maniera tale da prevenire un cambio di tattica e una ricaduta
- Creare un punto di discontinuità più rapido possibile dove:
  - Chiudere tutte le vulnerabilità più ovvie
  - Migliorare la visibilità e la registrazione degli eventi
  - Aggiungere un livello di intelligence sulla gestione degli utenti
  - Rimuovere il controllo da parte degli attaccanti
- Dopo una prima fase di intervento, è necessario un allineamento tra il piano di remediation immediato e la strategia Aziendale sulla Cyber Security favorendo il naturale follow-up all'interno del Security Improvement Program
- Al termine del processo, si otterranno una migliore visibilità e consapevolezza complessiva, una migliore security posture e un generale miglioramento dei processi di sicurezza dell'organizzazione

Minacce, capacità, strumenti



Grazie

marco.dileo@hpe.com