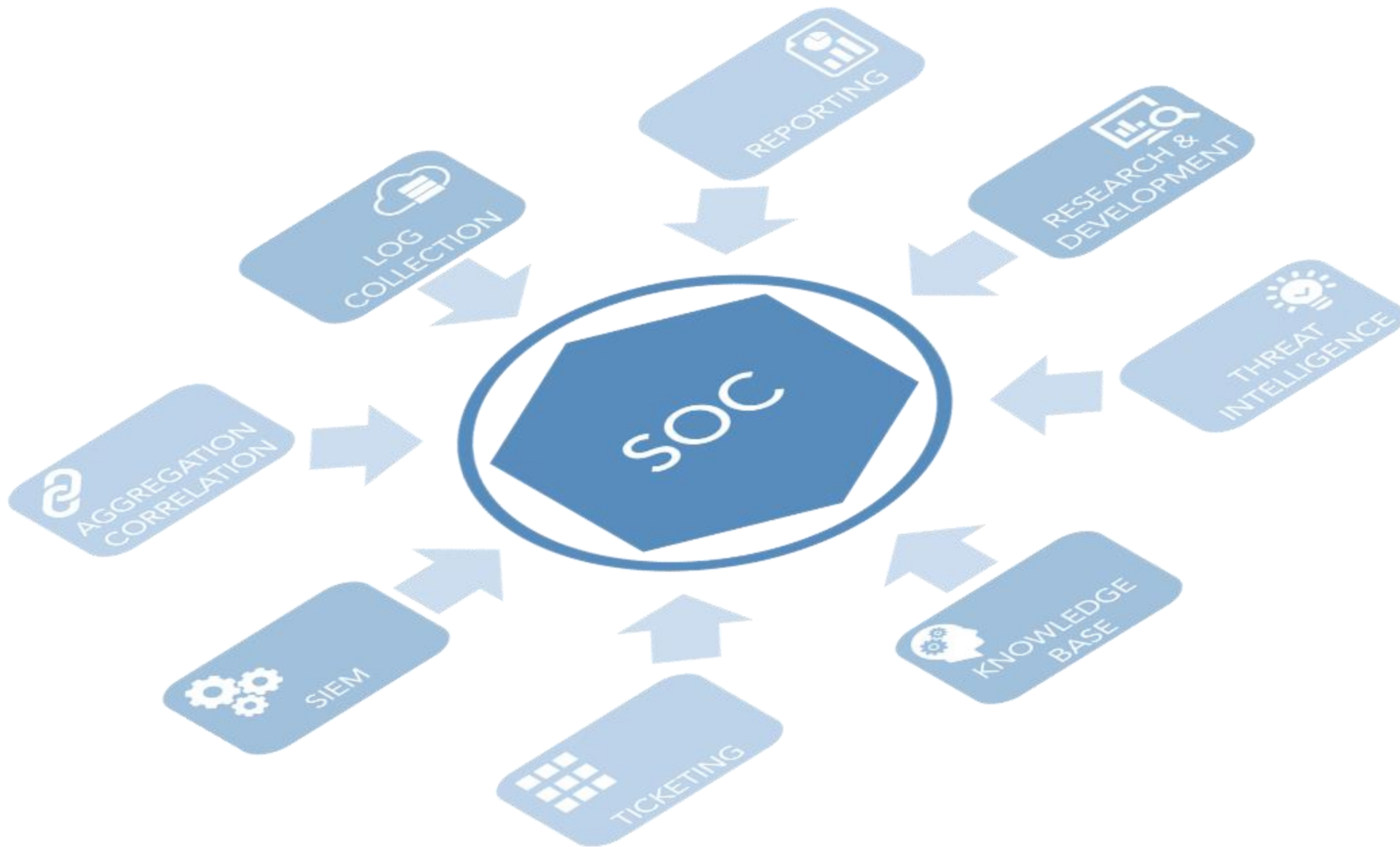




FUTURE HUNTERS

SECURITY OPERATION CENTER vs THREAT OPERATION CENTER

IL SERVIZIO SOC TRADIZIONALE



OPERATIVITA' DI UN SOC TRADIZIONALE

SAMPLE CUSTOMER	
1500 Endpoints	
Pair of Firewalls	
Active Directory	
Antivirus	
WAF	
IDS	

2 MILIARDI

DI EVENTI AL MESE COLLEZIONATI DAI SENSORI SU 1500 TARGET

900 000

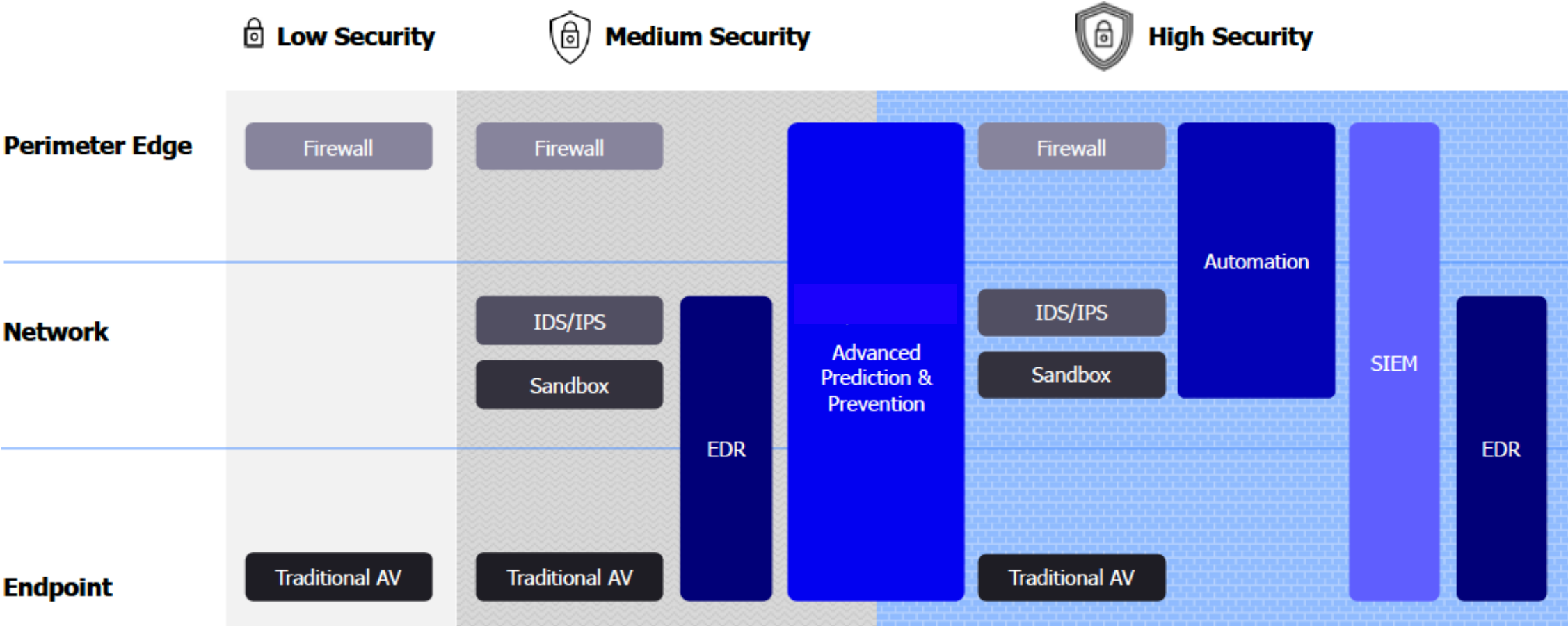
EVENTI SOSPETTI POST ANALISI DEI RAW DATA

25

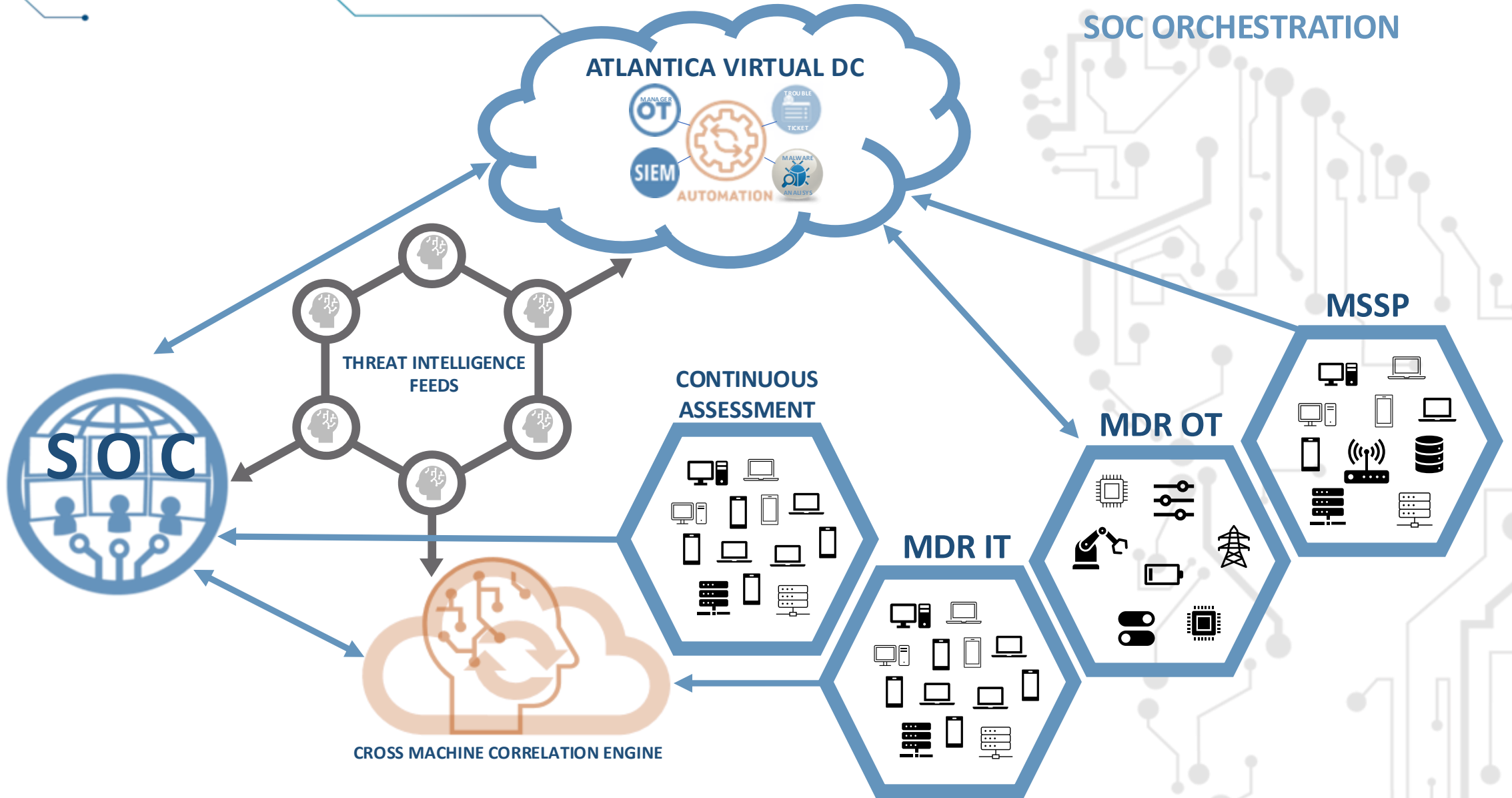
DETECTION CONFERMATE DAGLI ANALISTI E SCALATE SUL CLIENTE

15

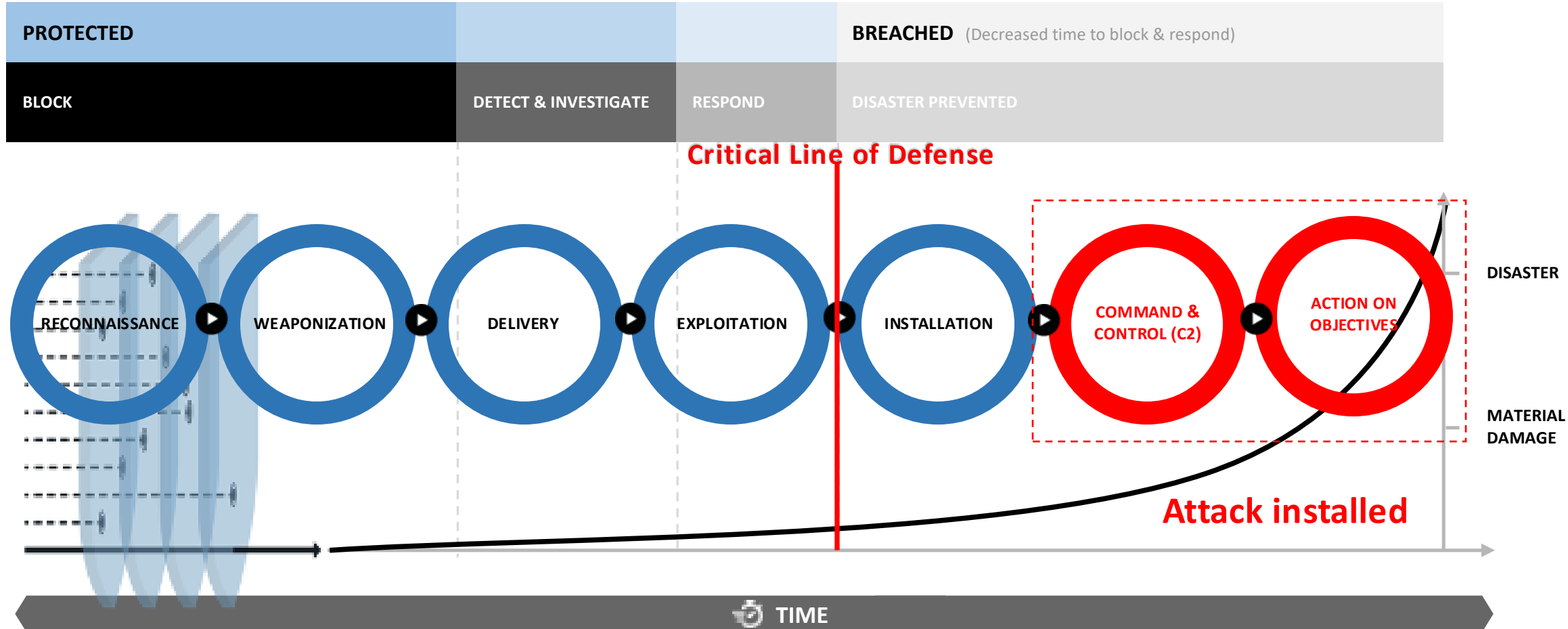
MINACCE REALI CONFERMATE DAL CLIENTE



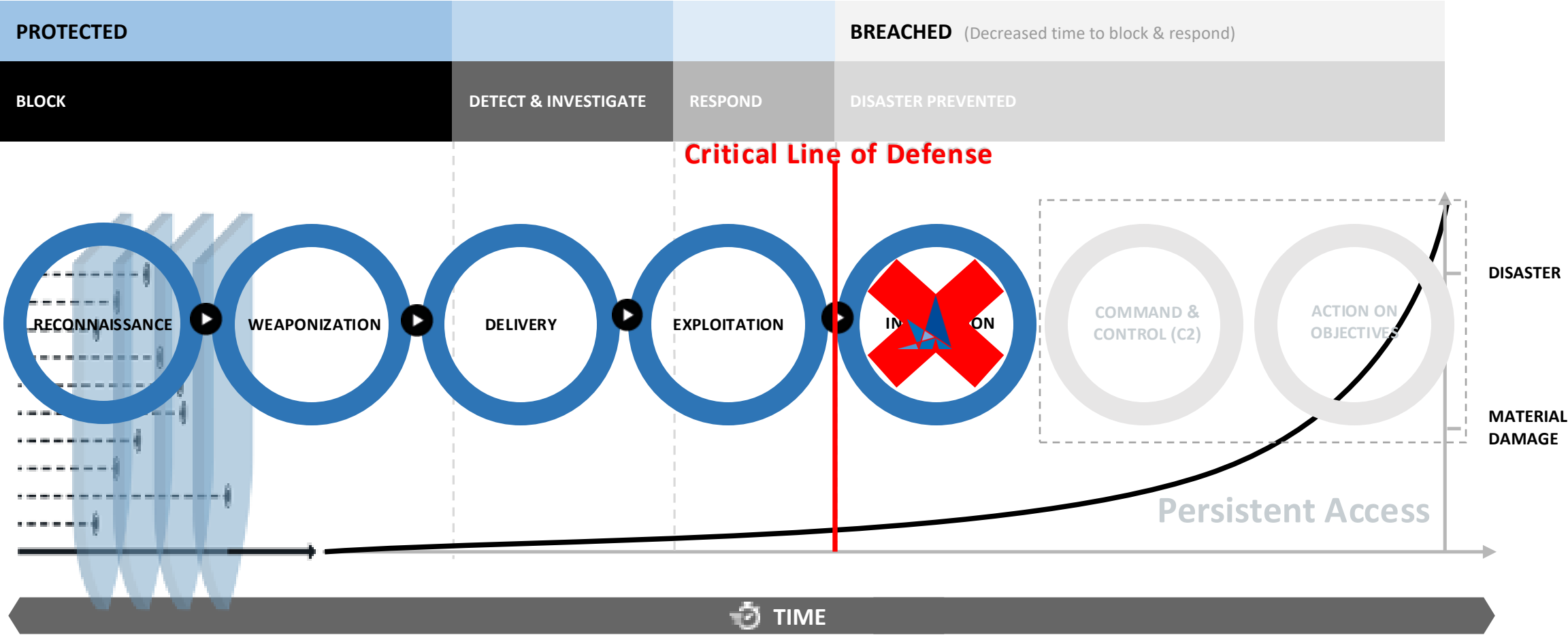
SOC ORCHESTRATION



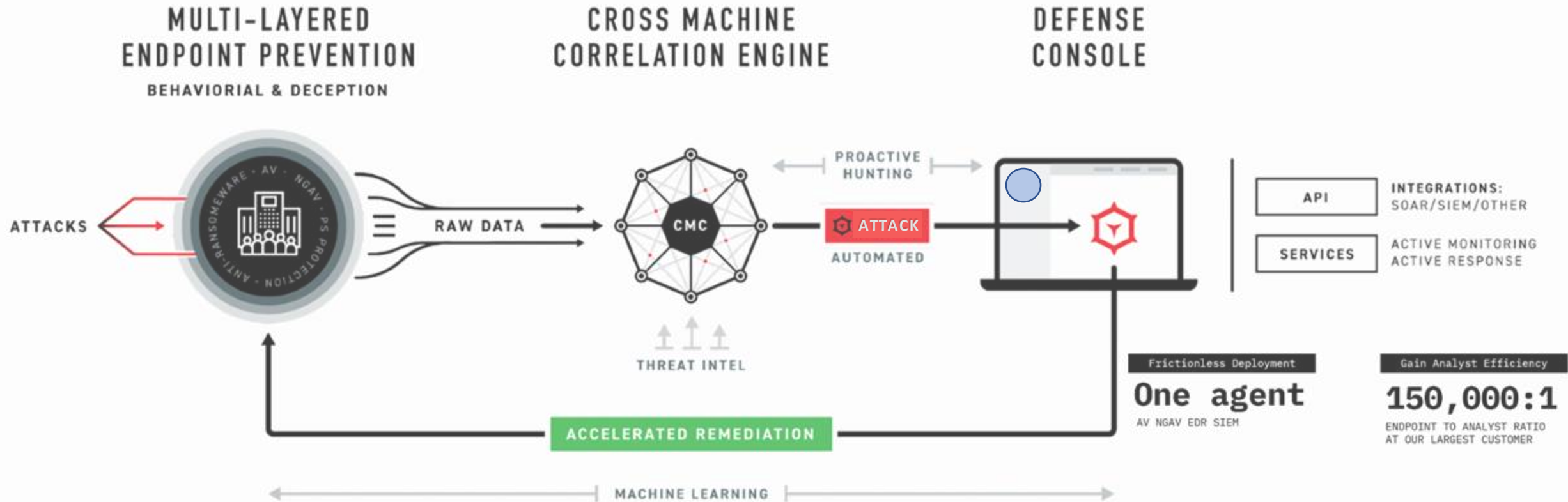
THE INTRUSION KILL-CHAIN



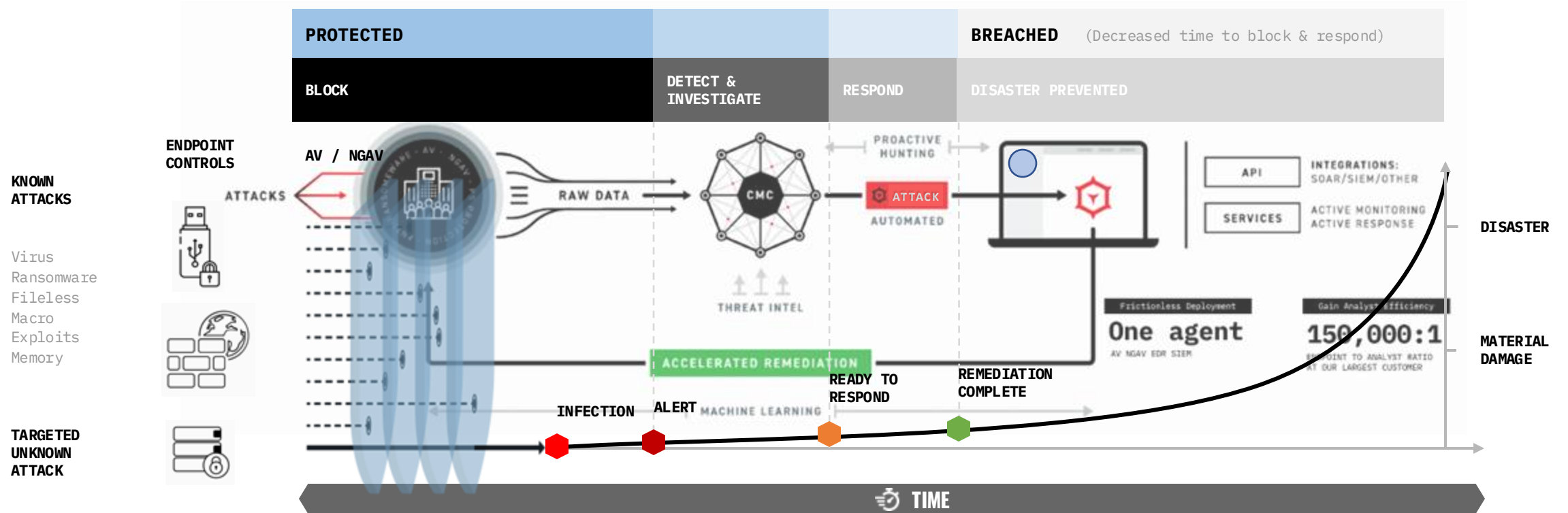
FROM SOC (Security Operation Center) TO TOC (Threat Operation Center)



ZERO-TRUST ORCHESTRATION



BLOCK-DETECT-INVESTIGATE-RESPOND



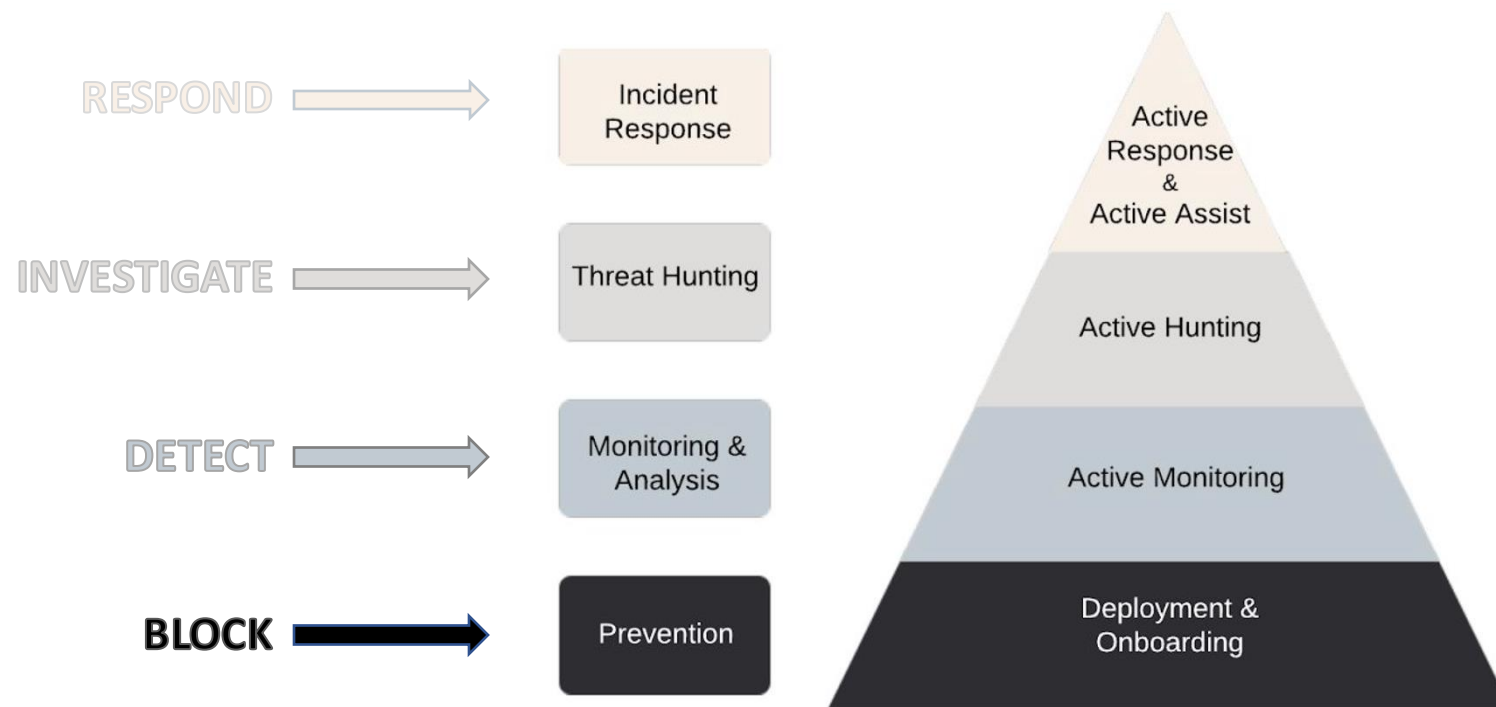
BLOCK-DETECT-INVESTIGATE-RESPOND: THE ZERO TRUST IT

PREVENTION: censimento, mappatura e validazione di tutti i processi, servizi e applicativi attivi nell'infrastruttura

MONITORING & ANALYSIS: monitoraggio e analisi di processi non censiti e validati durante la prima fase

THREAT HUNTING: ricerca attiva di minacce, compromissioni e persistenze preesistenti al nostro servizio

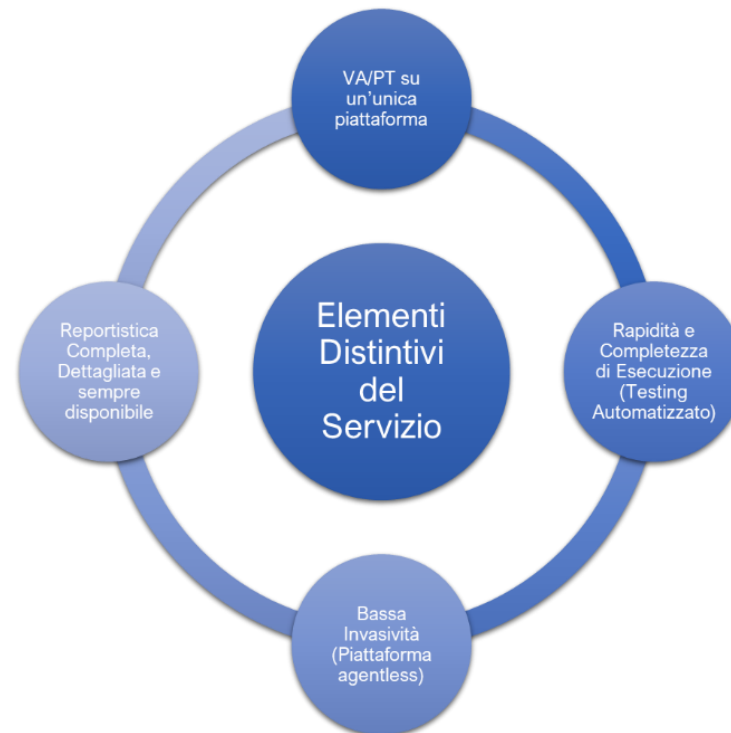
INCIDENT RESPONSE: attivazione delle policy di detection & response in modalità «prevent» per bloccare attività malevole



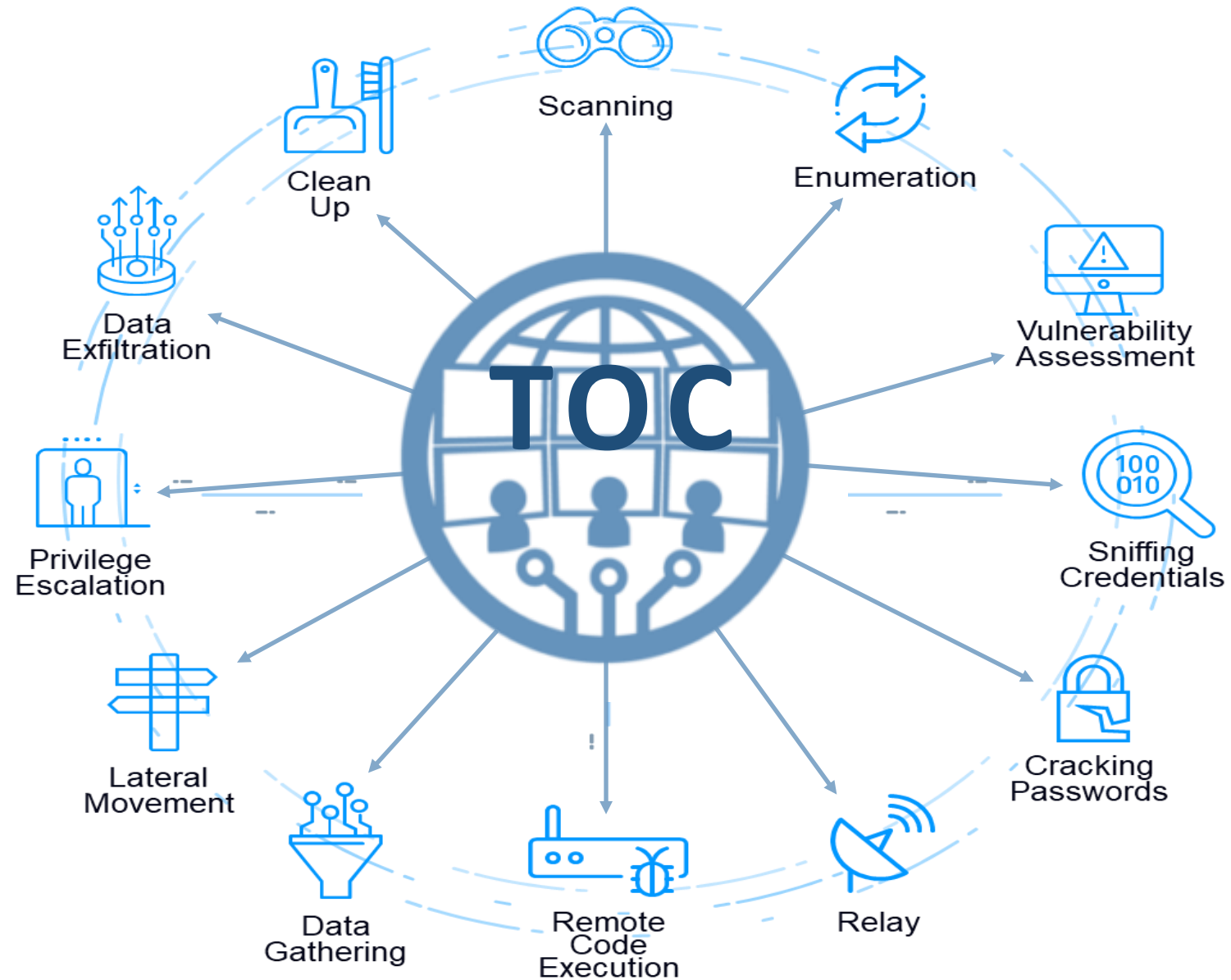
CONTINUOUS ASSESSMENT

IL TOC fornisce un servizio di Continuous Security Assessment al fine di verificare la resilienza e la postura generale della sicurezza dell'infrastruttura aziendale.

Il servizio, suddiviso in più fasi e coadiuvato da SW specializzato di Penetration Testing, si basa sulla emulazione di un attacco informatico all'infrastruttura di rete interna, simulando il comportamento di un presunto utente malevolo, al fine di testare la sicurezza della stessa.



LE FASI DEL CONTINUOUS ASSESSMENT





TOC SERVICES

- **Early Warning:** Le attività di Early Warning prevedono l'invio di comunicazioni periodiche ufficiali (bollettini di sicurezza) per allertare prontamente i referenti preposti dal Cliente su informazioni relative alle vulnerabilità (software malevoli, campagne di phishing mirate (spear phishing)).
- **Security Awareness:** Le attività di Security Awareness comprendono le azioni di formazione e di sensibilizzazione che vengono fornite al personale specialistico, e non, nel settore Informatico.
- **Threat Intelligence:** Il servizio di Threat Intelligence è volto a raccogliere, condividere e identificare le informazioni relative alle minacce, alle strategie e agli attori che si celano dietro le minacce stesse.
- **Brand Protection/Fraud Management:** Attraverso l'utilizzo del servizio di Brand Protection e Fraud Management è possibile individuare ed eventualmente contrastare l'utilizzo non legittimo del brand del cliente.
- **Malware Analysis:** Il servizio permette di analizzare malware o file sospetti in ambienti controllati e con le tecniche più avanzate di analisi dinamica e statica.
- **Forensics:** Il servizio Forensic ha lo scopo di individuare, estrarre, conservare e proteggere documenti a fini probatori senza comprometterne l'integrità (catena di custodia).