digital system computers

Cyber Command

Piattaforma intelligente NDR di Detection & Response

Sangfor Technologies Italy

GOLD PARTNER

www.dscsrl.it

PART 1

Le minacce evolvono

Le minacce alla sicurezza evolvono rapidamente e si intensificano

La prevenzione non ferma gli attacchi

350.000 nuovi malware al giorno

- Anche se il tuo sistema di sicurezza esistente blocca il 99%.
- Oltre 3.500 nuovi malware possono passare

L'Intelligenza Artificiale rende tutto più sofisticato

- AI-Powered Concealment
- DGA Botnets
- AI Triggers

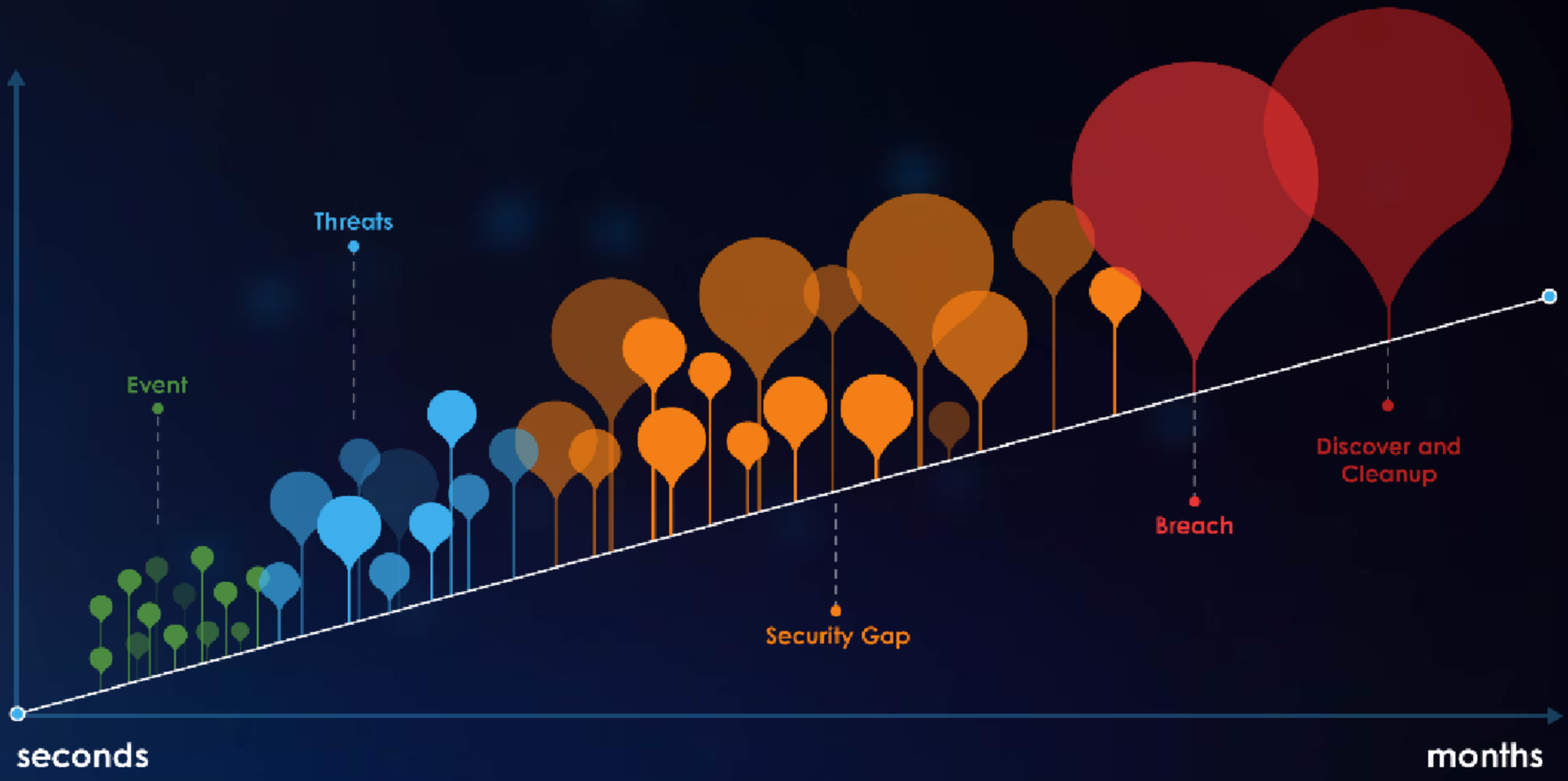
Tecniche di evasione Malware Sandbox

- Ritardare l'esecuzione
- Hardware Detection
- CPU Detection
- User Detection
- Detection dell'ambiente

Source: AV TEST

I team di security dovrebbero cambiare mindset

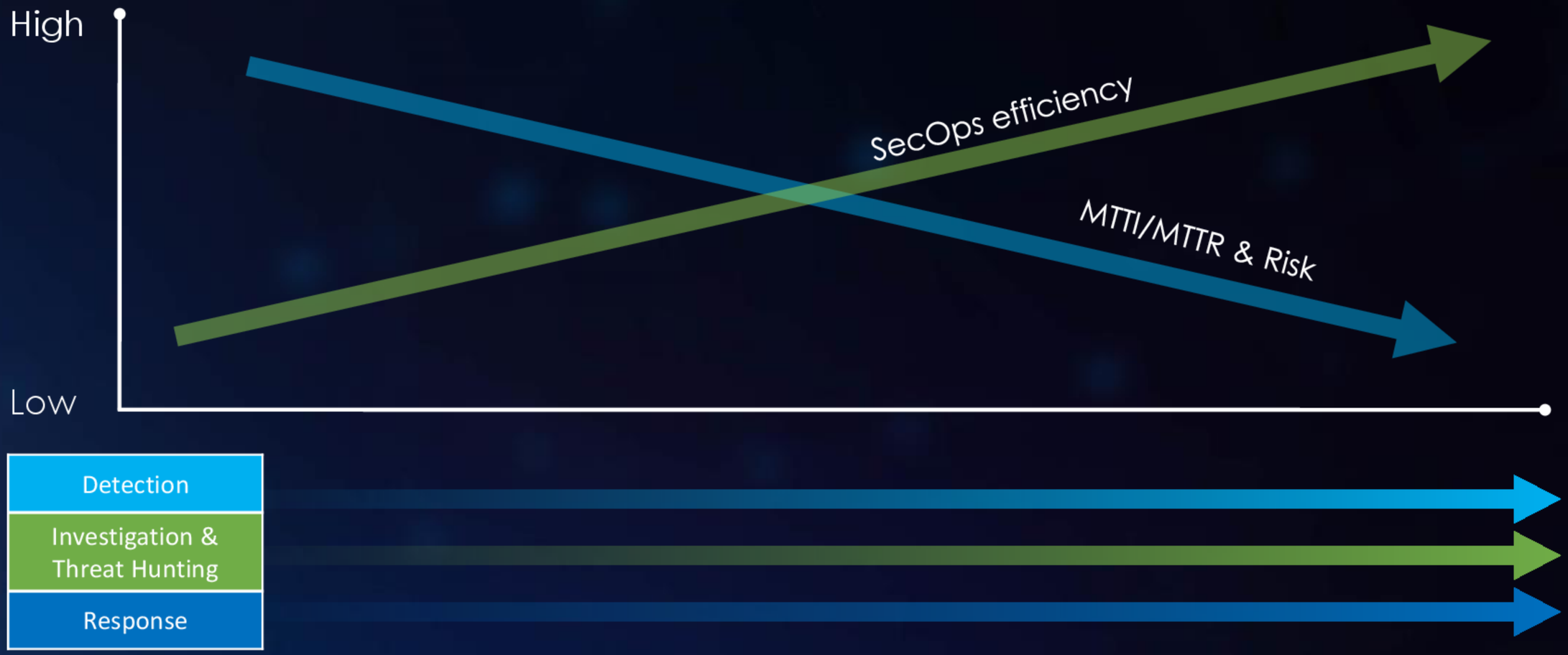
Fermare le minacce PRIMA che causino danni



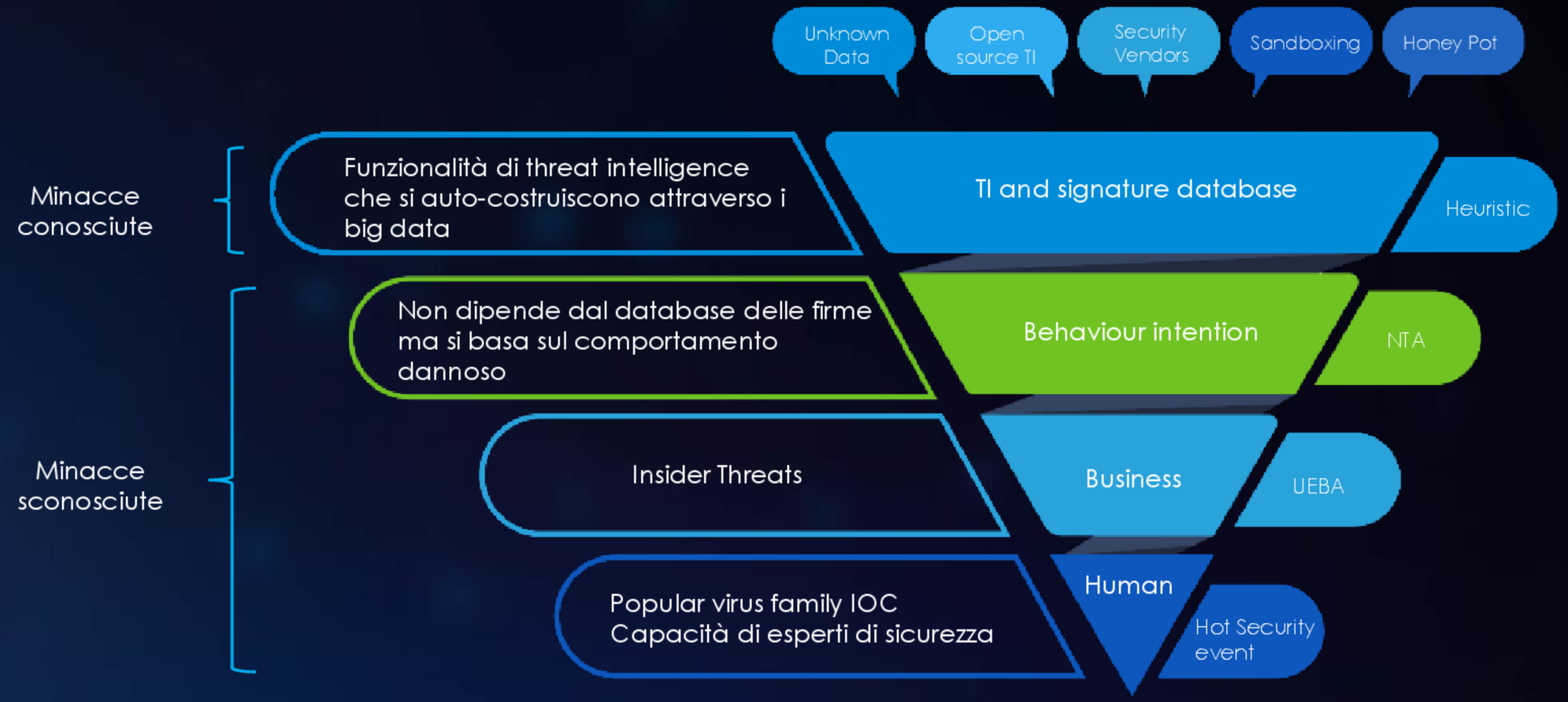
PART 2

L’approccio unico di Sangfor

Le Key Capabilities per ridurre i rischi



Coprire sia minacce conosciute che sconosciute



PART 3

Sangfor Cyber Command

Cyber Command - Introduzione

Detection delle minacce (Security posture)

- Monitora il traffico interno. Correla gli eventi di sicurezza
- Intelligenza artificiale e analisi del comportamento
- Scopri quello che non sai

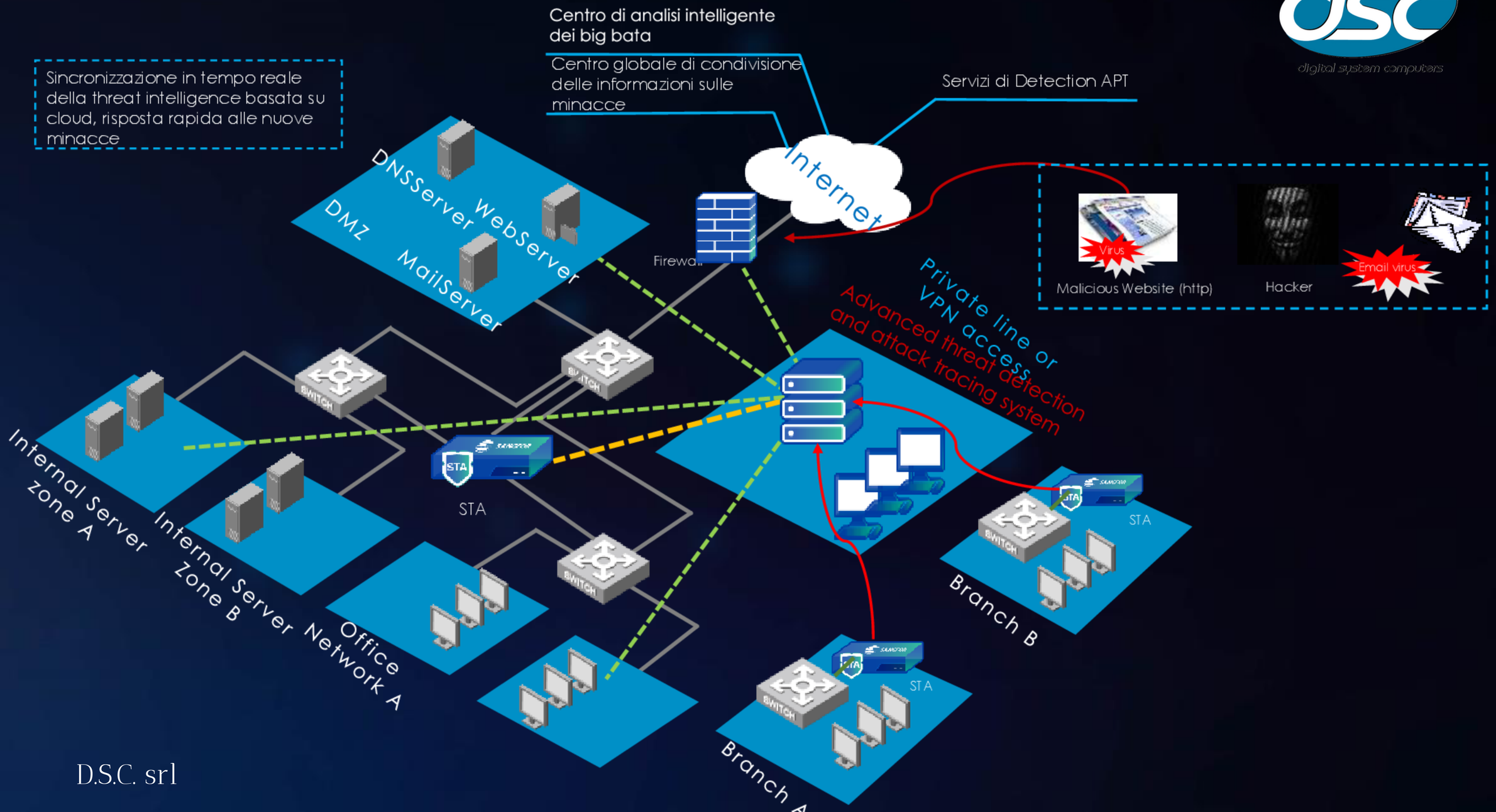
Caccia alle minacce (Incident Response)

- Scopre punto di ingresso dell'hacker
- Analizza l'impatto
- Raccoglie IOCs.

Risposta alle minacce

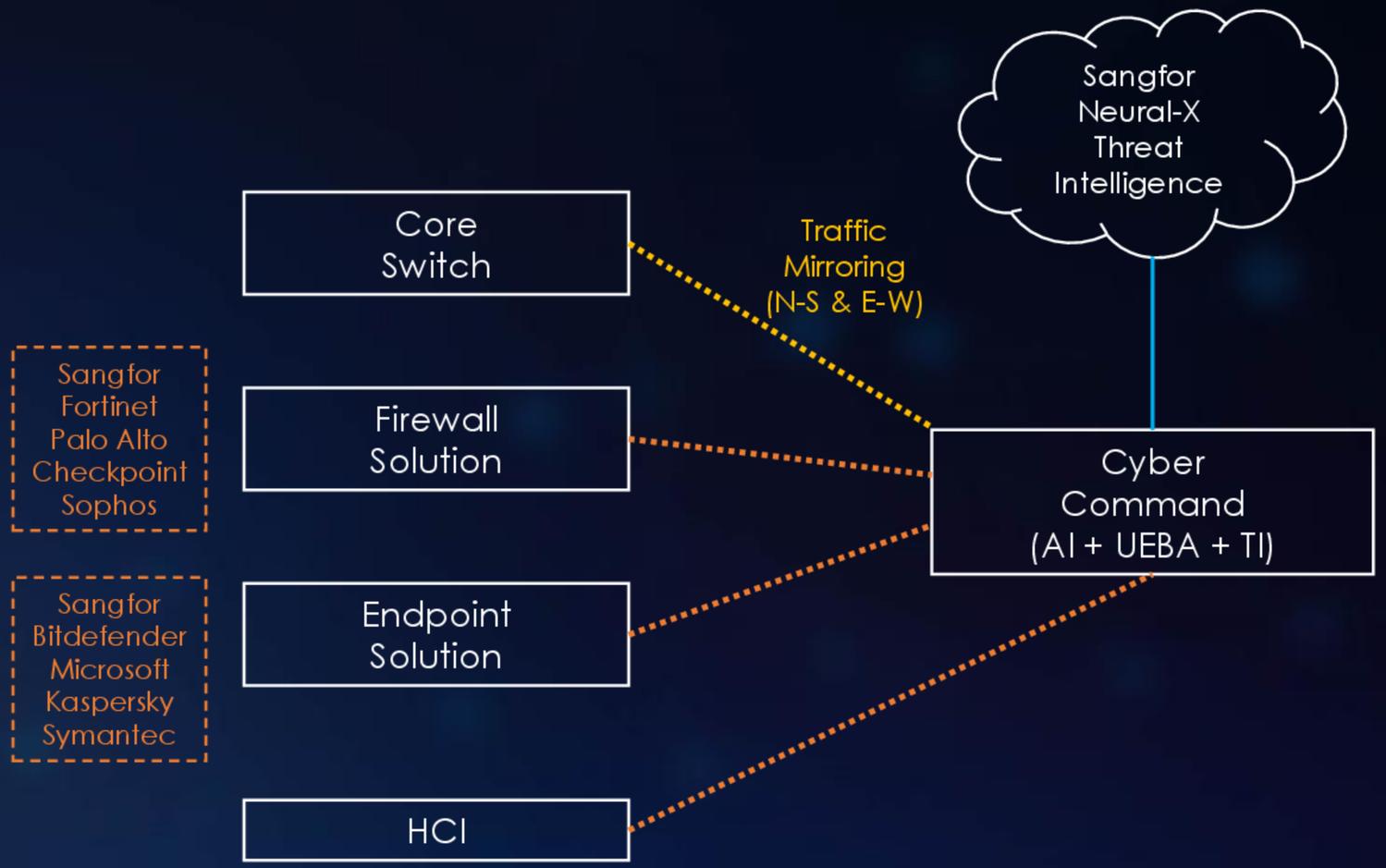
- Indaga sugli incidenti
- Correlazione con le contromisure di rete e endpoint

Deployment della soluzione



Sangfor Cyber Command - Whiteboard

- ✓ Aggiornamento delle minacce globali in tempo reale
- ✓ Identificare malware sconosciuti



Pain Points clienti:

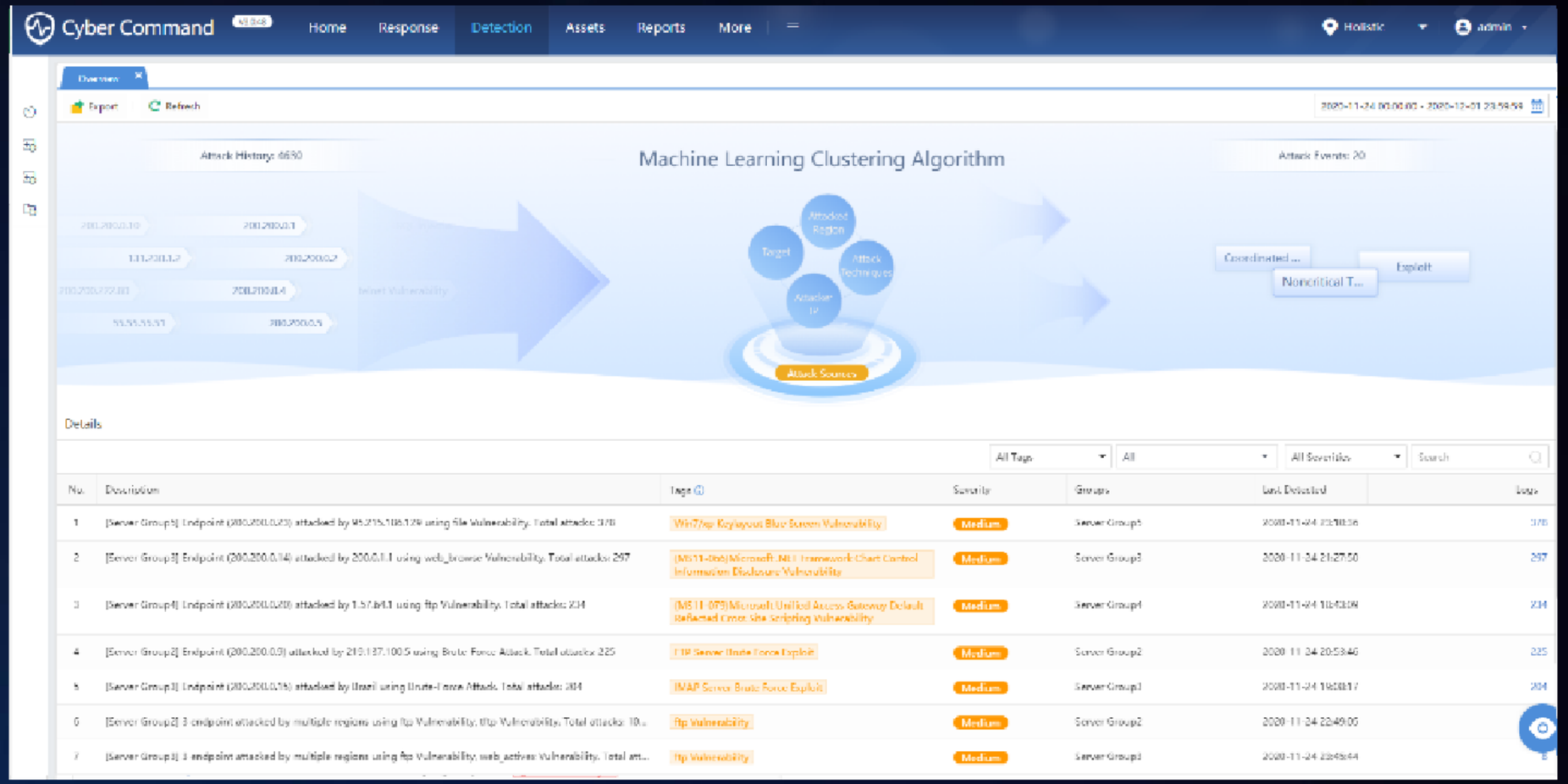
1. Ignari di attacchi che bypassano e nessuna visibilità del traffico E-W
2. Alto costo e monitoraggio umano inefficace
3. La mancanza di caccia alle minacce proattiva
4. Lunghi tempi di indagine (media 197 giorni)
5. Tempo di risposta lento (media 69 giorni)

Soluzione Sangfor

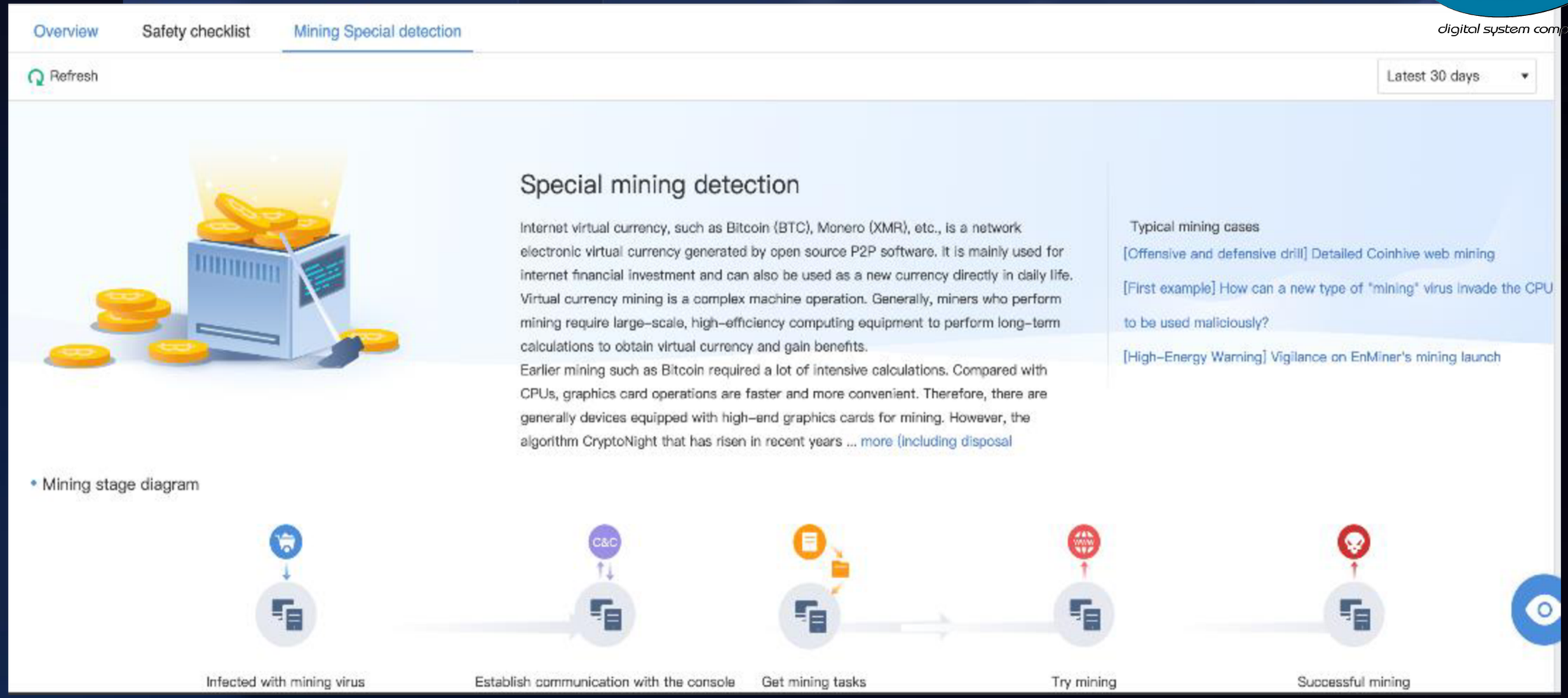
1. Visibilità di minacce sconosciute e comportamento anormale con la combinazione di AI + UEBA + TI
2. Monitoraggio continuo dell'AI 365x24x7
3. Avviso in tempo reale dei compromessi / vulnerabilità critica / attacco runtime via SMS ed e-mail
4. Analisi in tempo reale dell'impatto dei danni/ catene di attacco/ "paziente zero" per indagini post-evento
5. Risposta automatica istantanea

Indagine Semplificata

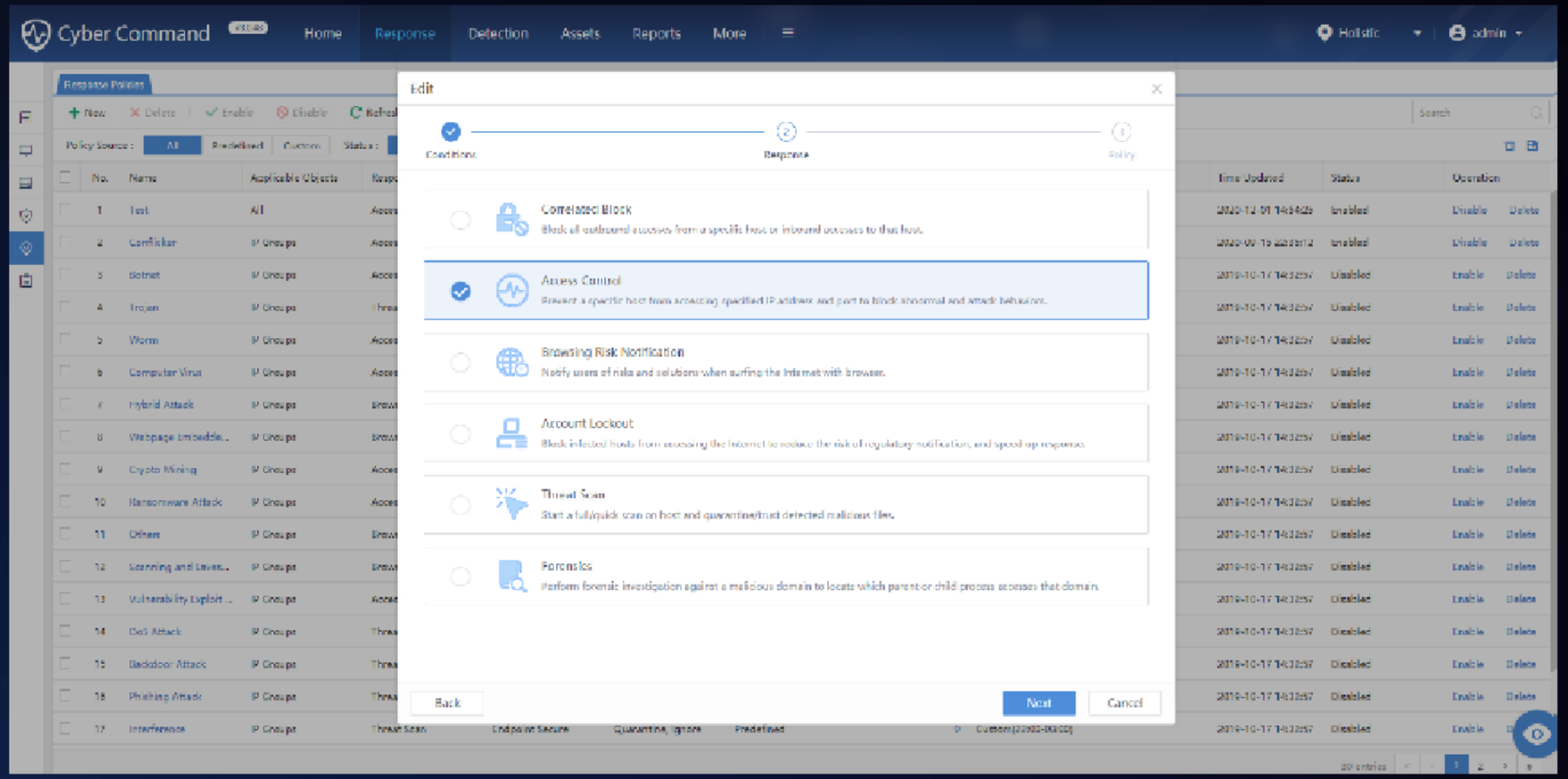
Business Perspectives → Full Visibility → Forensics Analysis → Security logs combination



Caccia alle minacce semplificata



Risposta rapida e intelligente



Visibilità completa

Overall Security Posture

Cyber Attack Posture

Asset Posture

Vulnerability Posture

PART 4

Soluzioni di Sicurezza Sangfor

Sangfor Network Security – Copertura completa

SANGFOR SECURITY

Network Solution

- ADC
- WANO
- SD-WAN
- WIFI+Switch

Security Solution

- Next Generation Firewall + NGWAF
- Endpoint Security
- IAG
- Cyber Command

Security Service

- PT and VA
- Incidence Response
- TIARA Advanced Security

digital system computers

GRAZIE

D.S.C. e Sangfor Technologies Italy

Corwww.dscsrl.ipo

GOLD PARTNER

www.dscsrl.it