



digital system computers

Cyber Command

Piattaforma intelligente NDR di Detection & Response

Sangfor Technologies Italy



■ www.dscsrl.it



PART 1

Le minacce evolvono

Le minacce alla sicurezza evolvono rapidamente e si intensificano

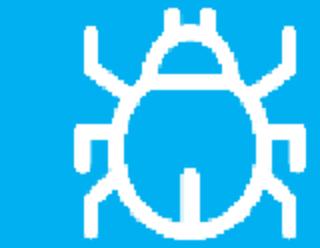


La prevenzione non ferma gli attacchi



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



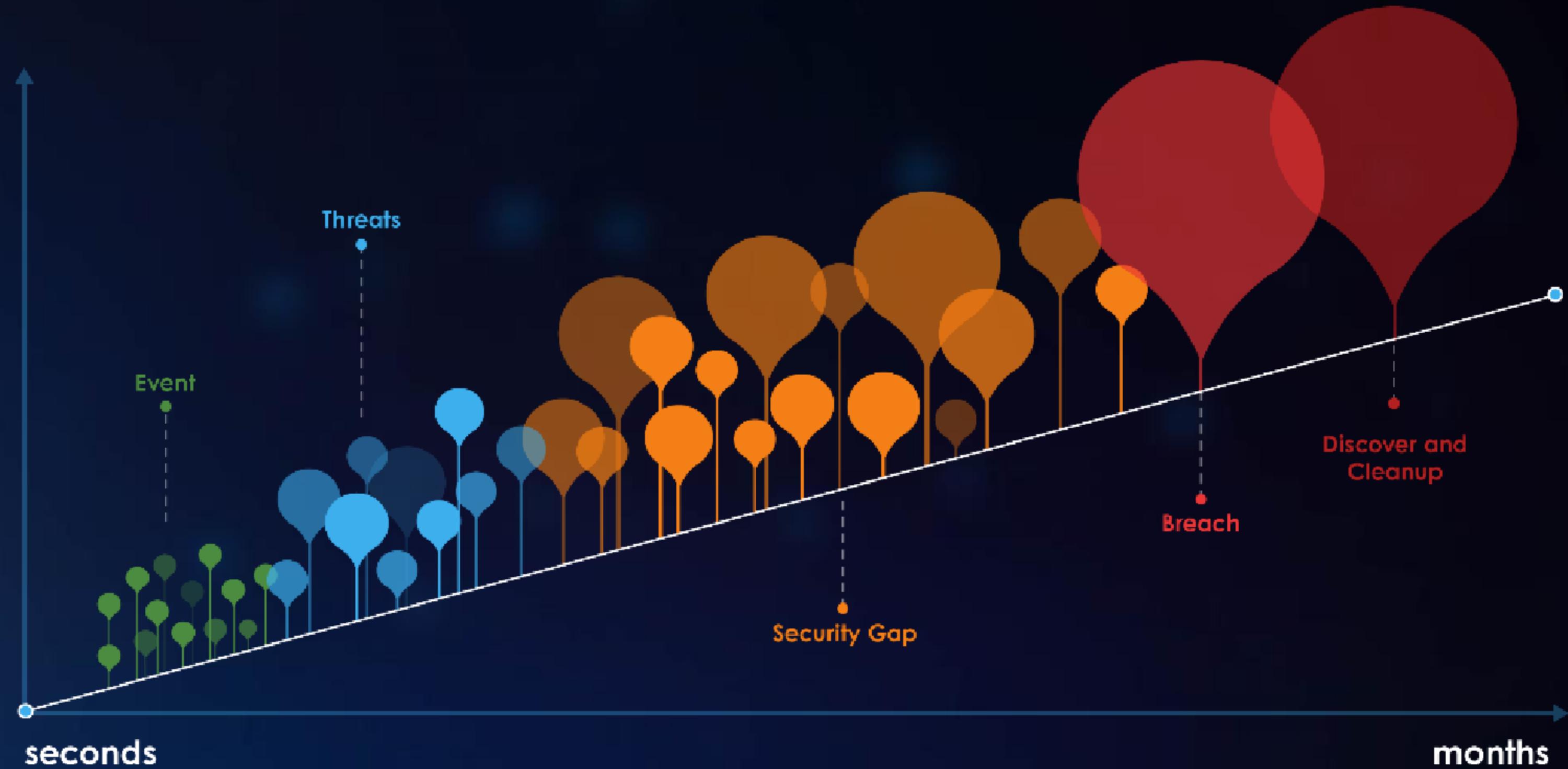
Tecniche di evasione Malware Sandbox

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

Source: AV TEST

I team di security dovrebbero cambiare mindset

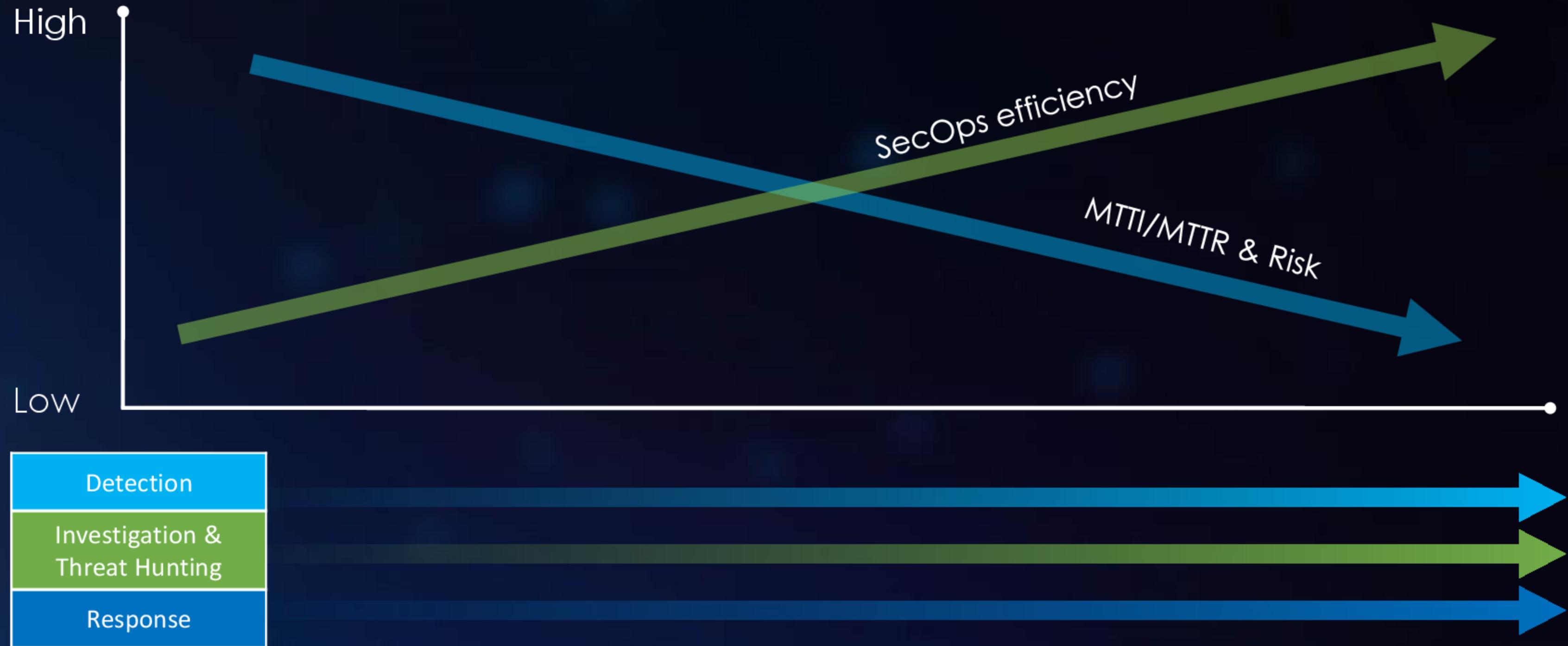
Fermare le minacce PRIMA che causino danni



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.

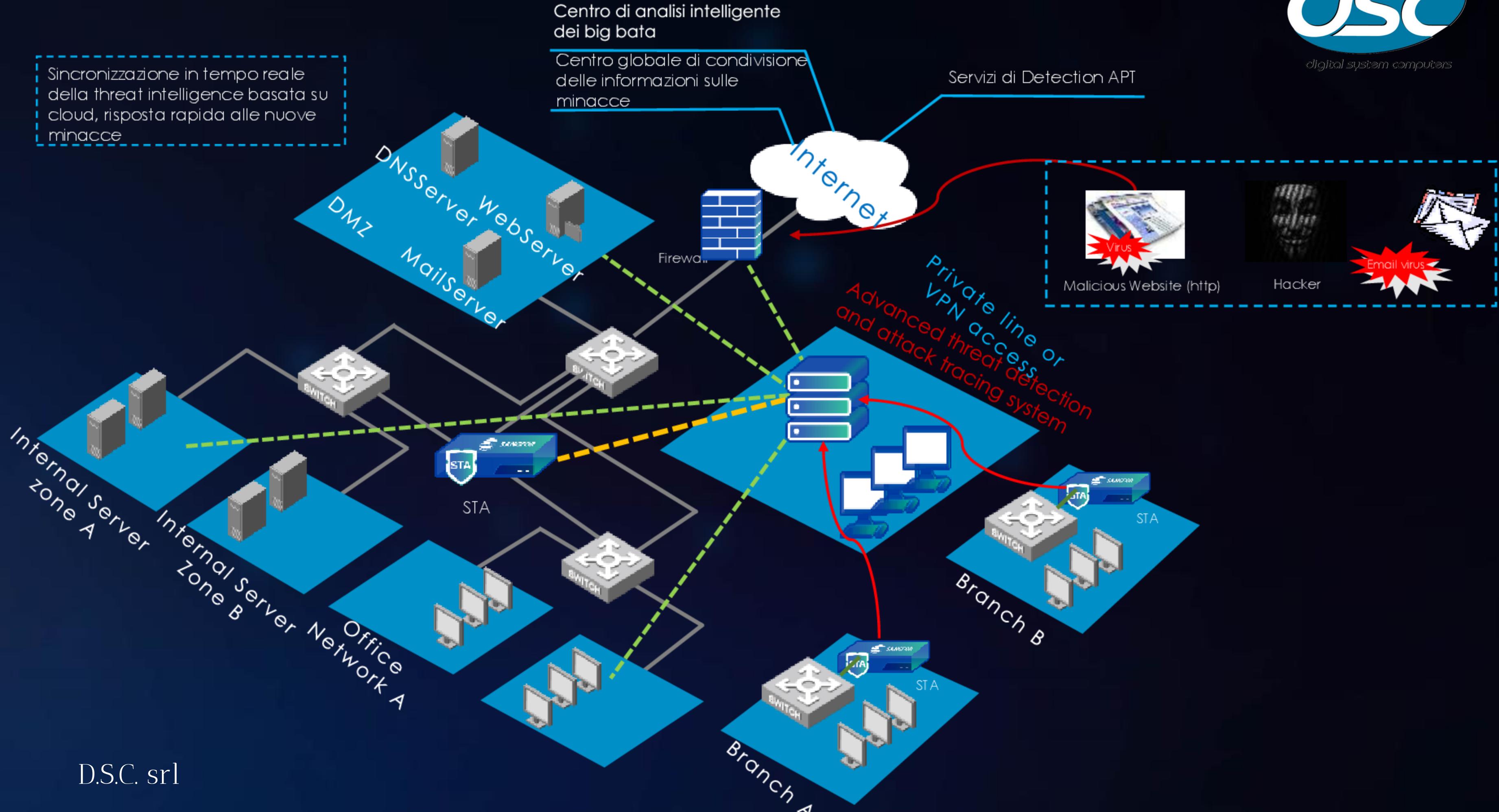
Risposta alle minacce

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

Deployment della soluzione



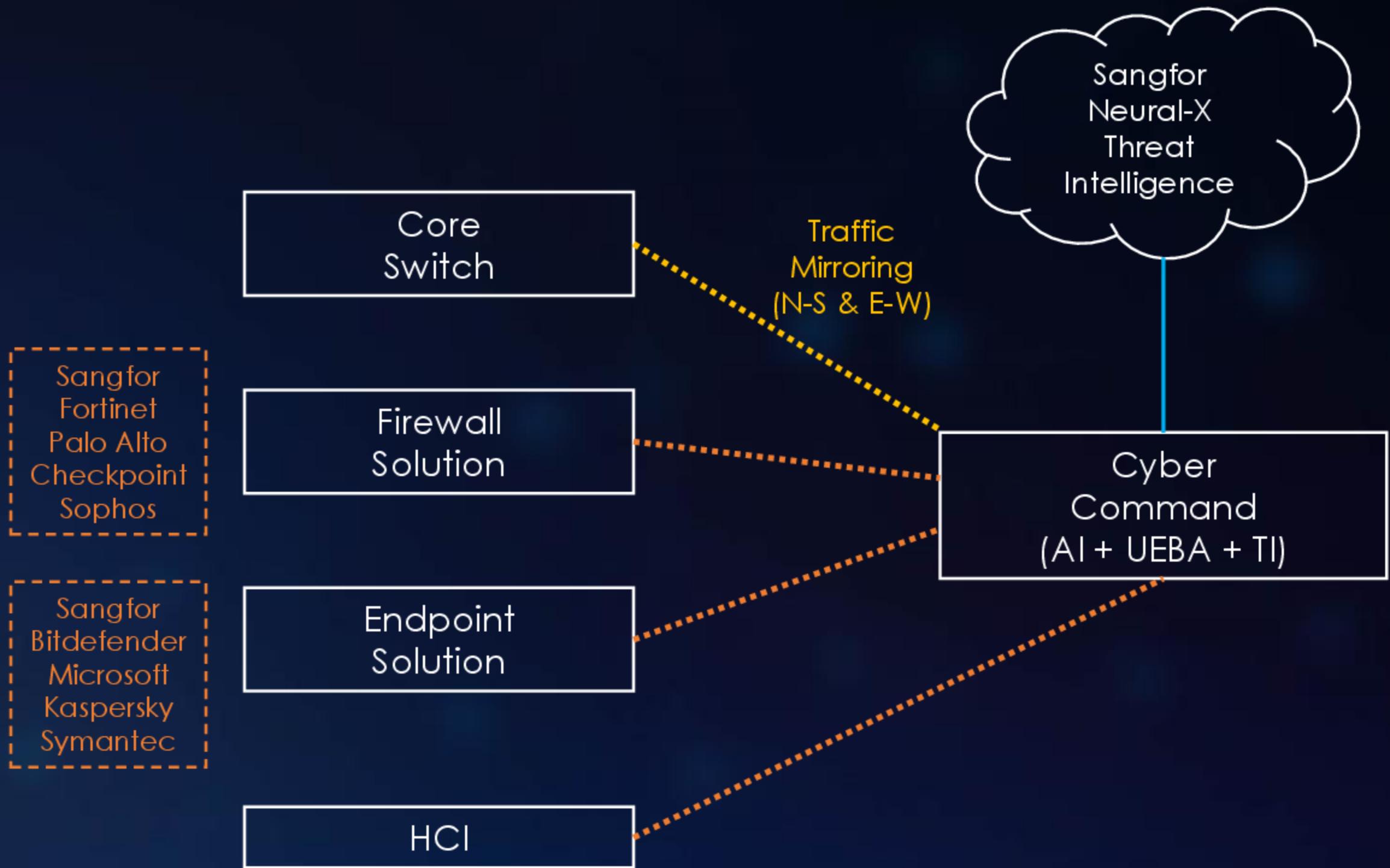
digital system computers



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 inefficiente
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



digital system computers



The screenshot displays the Cyber Command interface. At the top, there's a navigation bar with tabs: Home, Response, Detection (which is selected), Assets, Reports, and More. Below the navigation is a search bar with the date range "2020-11-24 00:00:00 - 2020-12-01 23:59:59".

The main area features a "Machine Learning Clustering Algorithm" diagram. It shows a central circle labeled "Attack Sources" connected to several other circles: "Target", "Attacked Region", "Attack Techniques", and "Attack IP". Arrows point from various IP addresses listed on the left ("200.200.0.10", "200.200.0.11", "111.200.1.2", "200.200.0.2", "200.200.22.88", "200.200.0.14", "99.99.99.99", "200.200.0.5") to these central nodes.

On the right, there are sections for "Attack History: 6690" and "Attack Events: 20". The "Attack Events" section includes buttons for "Coordinated ...", "Noncritical T...", and "Exploit".

At the bottom, a table titled "Details" lists seven attack entries:

No.	Description	Tags	Severity	Groups	Last Detected	Count
1	[Server Group 5] Endpoint (200.200.0.20) attacked by 95.215.196.129 using file Vulnerability. Total attacks: 378	Win7sp1, Keylogger, Blue Screen Vulnerability	Medium	Server Group 5	2020-11-24 22:51:56	378
2	[Server Group 5] Endpoint (200.200.0.14) attacked by 200.0.1.1 using web_browser Vulnerability. Total attacks: 297	MS11-061, Microsoft .NET Framework Chart Control Information Disclosure Vulnerability	Medium	Server Group 5	2020-11-24 21:27:50	297
3	[Server Group 4] Endpoint (200.200.0.20) attacked by 1.57.64.1 using ftp Vulnerability. Total attacks: 234	MS11-073, Microsoft Unified Access Gateway Default Reflected Cross Site Scripting Vulnerability	Medium	Server Group 4	2020-11-24 21:04:08	234
4	[Server Group 2] Endpoint (200.200.0.9) attacked by 219.137.100.5 using Brute Force Attack. Total attacks: 225	FTP Server Brute Force Exploit	Medium	Server Group 2	2020-11-24 20:53:46	225
5	[Server Group 3] Endpoint (200.200.0.15) attacked by 192.1 using Brute-Force Attack. Total attacks: 204	IMAP Server Brute Force Exploit	Medium	Server Group 3	2020-11-24 19:08:17	204
6	[Server Group 2] 3 endpoint attacked by multiple regions using IIS Vulnerability, IISp Vulnerability. Total attacks: 104	IIS Vulnerability	Medium	Server Group 2	2020-11-24 22:49:00	104
7	[Server Group 3] 3 endpoint attacked by multiple regions using IIS Vulnerability, web_activescanner Vulnerability. Total att...	IIS Vulnerability	Medium	Server Group 3	2020-11-24 22:49:44	8

Caccia alle minacce semplificata



Overview Safety checklist Mining Special detection

Refresh Latest 30 days

Special mining detection



Internet virtual currency, such as Bitcoin (BTC), Monero (XMR), etc., is a network electronic virtual currency generated by open source P2P software. It is mainly used for internet financial investment and can also be used as a new currency directly in daily life. Virtual currency mining is a complex machine operation. Generally, miners who perform mining require large-scale, high-efficiency computing equipment to perform long-term calculations to obtain virtual currency and gain benefits.

Earlier mining such as Bitcoin required a lot of intensive calculations. Compared with CPUs, graphics card operations are faster and more convenient. Therefore, there are generally devices equipped with high-end graphics cards for mining. However, the algorithm CryptoNight that has risen in recent years ... [more \(including disposal\)](#)

• Mining stage diagram



Infected with mining virus Establish communication with the console Get mining tasks Try mining Successful mining

Typical mining cases

[Offensive and defensive drill] Detailed Coinhive web mining

[First example] How can a new type of "mining" virus invade the CPU to be used maliciously?

[High-Energy Warning] Vigilance on EnMiner's mining launch

Risposta rapida e intelligente



Screenshot of the Cyber Command software interface showing the 'Edit' dialog for a Response Policy.

The dialog is divided into 'Conditions' and 'Responses' tabs. The 'Responses' tab is active, displaying a list of available actions:

- Correlated Block
- Access Control (selected)
- Browsing Risk Notification
- Account Lockout
- Threat Scan
- Forensics

Below the responses, there are buttons for Back, Next, and Cancel, along with tabs for Threat Scan, Endpoint Secure, Quarantine, Ignore, and Predefined.

The background shows a list of existing response policies in a table format.

Time Updated	Status	Operation
2020-12-01 14:04:09	Enabled	Disable Delete
2020-09-19 22:00:14	Enabled	Disable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete
2019-10-17 14:02:57	Disabled	Enable Delete

Visibilità completa



Overall Security Posture



Cyber Attack Posture



Asset Posture



Vulnerability Posture

PART 4

Soluzioni di Sicurezza Sangfor

Sangfor Network Security – Copertura completa



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.it

■ www.dscsrl.it

