DESAFIO 2 — CADEIA DE ATAQUE

Global Time Range: Last 24 hours

Identificar EMAIL com ANEXO

1.5
1
0.5
:00 AM
un Dec 14
025
8:10 AM
8:20 AM
_time
attachment
datasource
host
index
linecount
source
sourcetype
splunk_server

Ver se houve EXECUÇÃO DE PROCESSO

timestamp	host.name	process.name	process.command_line	process.parent.name
12/14/2025 08:13:12.524	win-3450	rdpclip.exe	rdpclip	svchost.exe
12/14/2025 08:13:18.524	win-3460	iexplore.exe	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:2832 CREDAT:9474 /prefetch:2	iexplore.exe
12/14/2025 08:06:29.524	win-3450	rundll32.exe	C:\Windows\system32\rundll32.exe C:\Windows\system32\inetcpl.cpl,ClearMyTracksByProcess Flags:8388616 WinX:0 WinY:0 IEFrame:0000000000000000	iexplore.exe

Filtrar execução suspeita

Investigar DNS suspeito

timestamp	host.name	process.name	dns.question.name	dns.resolved_ip
12/14/2025 08:21:47.524	win-3451	OUTLOOK.EXE	DC-01.tryhatme.com	172.16.1.10
12/14/2025 08:20:59.524	win-3451	OUTLOOK.EXE	mailsrv-01.tryhatme.com	172.16.1.15
12/14/2025 08:17:58.524	win-3454	OUTLOOK.EXE	autodiscover.tryhatme.finance	34.244.197.202
12/14/2025 08:15:41.524	win-3449	OUTLOOK.EXE	autodiscover.tryhatme.finance	34.244.197.202
12/14/2025 08:12:01.524	win-3456	OUTLOOK.EXE	mailsrv-01.tryhatme.com	172.16.1.15
12/14/2025 08:07:22.524	win-3458	OUTLOOK.EXE	autodiscover.tryhatme.finance	34.244.197.202
12/14/2025 08:05:33.524	win-3455	OUTLOOK.EXE	autodiscover.tryhatme.finance	34.244.197.202

Correlacionar TUDO por HOST