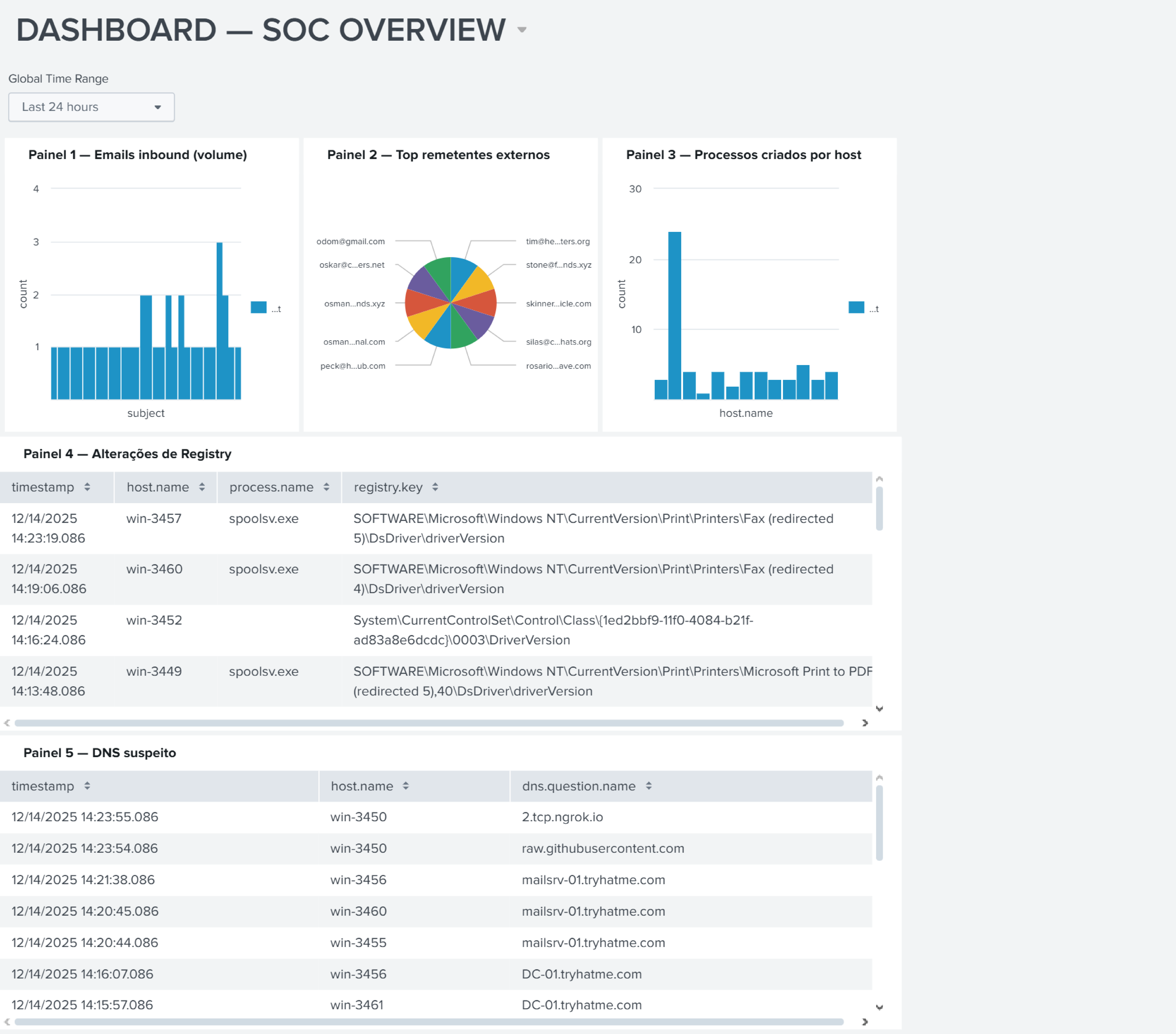

DASHBOARD — SOC OVERVIEW

Global Time Range

Last 24 hours

Painel 1 — Emails inbound (volume)

Painel 2 — Top remetentes externos

Painel 3 — Processos criados por host

Painel 4 — Alterações de Registry

timestamp	host.name	process.name	registry.key
12/14/2025 14:23:19.086	win-3457	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 5)\DsDriver\driverVersion
12/14/2025 14:19:06.086	win-3460	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Fax (redirected 4)\DsDriver\driverVersion
12/14/2025 14:16:24.086	win-3452		System\CurrentControlSet\Control\Class\{1ed2bbf9-11f0-4084-b21f-ad83a8e6dcdc}\0003\DriverVersion
12/14/2025 14:13:48.086	win-3449	spoolsv.exe	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\Microsoft Print to PDF (redirected 5),40\DsDriver\driverVersion

Painel 5 — DNS suspeito

timestamp	host.name	dns.question.name
12/14/2025 14:23:55.086	win-3450	2.tcp.ngrok.io
12/14/2025 14:23:54.086	win-3450	raw.githubusercontent.com
12/14/2025 14:21:38.086	win-3456	mailsrv-01.tryhatme.com
12/14/2025 14:20:45.086	win-3460	mailsrv-01.tryhatme.com
12/14/2025 14:20:44.086	win-3455	mailsrv-01.tryhatme.com
12/14/2025 14:16:07.086	win-3456	DC-01.tryhatme.com
12/14/2025 14:15:57.086	win-3461	DC-01.tryhatme.com