Incident Report — Network Capture Triage

Generated: 2025-10-23T14:43:59.804120Z

Top suspicious flows:

```
src,dst,src_port,dst_port,proto,bytes,pkts,src_internal,dst_internal
172.27.91.210,224.0.0.251,5353,5353,IP,405,3,True,False
```

Top DNS queries (sample):

Enrichment (sample):

Assessment & Next steps:

Review top external flows; isolate suspicious hosts; run host-level scans; block IPs/domains; preserve evidence.