GREYNOISE

CASE STUDY

Global Carrier Hunts Emerging Exploitation Campaigns Across Global Infrastructure with GreyNoise

Company Overview

A global telecommunications carrier operates one of the largest network backbones in the world, spanning 40+ countries and serving over 200 million wireless subscribers. The carrier's dedicated threat intelligence team runs custom threat hunting operations to protect core network elements — backbone routers, session border controllers, SIP gateways, and edge infrastructure — against targeted exploitation. With an in-house research capability and proprietary hunting workflows, the team operates independently from traditional SOC functions, focused entirely on identifying and preempting threats before they reach production infrastructure.

INDUSTRY:
Telecommunications
LOCATION:
Global (40+ countries)
USE CASES:
Threat hunting, proactive exploitation detection, vulnerability prioritization, edge device protection

Challenge

The carrier's threat hunting team faced three operational challenges:

- **Detecting Exploitation Before Vendor Advisories:** Edge network devices — backbone routers, SIP gateways, and session border controllers — were targeted by exploitation campaigns days before CVE disclosures. The team's custom hunting processes needed an external signal to surface emerging threats against Telco-specific infrastructure before public advisories.
- **Distinguishing Targeted Probes from Internet Background Noise:** With thousands of internet-facing IPs across 40+ countries, the team needed to quickly determine whether scanning activity targeting SIP, management interfaces, and routing protocols was directed reconnaissance or mass scanning hitting everyone. Internal telemetry alone could not answer this question.
- **Building Evidence for Emergency Change Windows:** With operations spanning 40+ countries, each with its own change advisory board, emergency patching required hard evidence of active exploitation. The team's custom threat reports needed external corroboration to justify same-day patch deployments.

GreyNoise in Action

Custom Threat Hunting with GreyNoise Data

The threat hunting team integrated GreyNoise data into their proprietary hunting workflows. By filtering GreyNoise observations by port, protocol, CVE, and ASN, the team monitors scanning trends targeting Telco-specific services — SIP (port 5060/5061), edge router management interfaces, and session border controller protocols. GreyNoise provides the external internet-wide visibility that complements the team's internal network telemetry, answering a question their own sensors cannot: is this activity targeting us specifically, or scanning everyone?

Early Warning on Edge Device Exploitation

In Q3 2025, the team's custom hunting process flagged a 400% spike in GreyNoise-observed scanning targeting a specific edge router management interface — 48 hours before the vendor issued a security advisory. IP timeline data confirmed the activity was coordinated exploitation from a cluster of IPs not previously seen in background scanning. The team issued an internal threat bulletin and initiated preemptive patching across all 40+ country networks before any exploitation attempt reached production infrastructure.

Evidence-Driven Patch Prioritization

GreyNoise data now feeds directly into the team's custom threat reports. When GreyNoise confirms active exploitation of a CVE affecting Telco infrastructure, the team packages the evidence — IP counts, geographic distribution, payload characteristics, and exploitation timelines — into a standardized brief for change advisory boards. This external corroboration transformed the patch approval process from weeks of internal debate to same-day authorization.

Results

The threat hunting team achieved four measurable outcomes in the first 12 months:

- **Early Exploitation Detection** — Identified 5 active exploitation campaigns targeting edge infrastructure before vendor advisories, including 2 against SIP gateways and 1 targeting a session border controller zero-day.
- **48-Hour Average Early Warning** — Average lead time between GreyNoise detection and public CVE disclosure or vendor advisory across all 5 campaigns.
- **Zero Compromises** — Preemptive patching prevented any successful exploitation across the carrier's 40+ country network footprint during all 5 identified campaigns.
- **Patch Approval in Hours** — Emergency change windows approved in 4–6 hours using GreyNoise exploitation evidence, down from an average of 18 days under the previous process.

Customer Perspectives

> "GreyNoise gives our hunting team eyes on the internet that we cannot build ourselves. When we see a spike in scanning against our edge infrastructure, we know within hours whether it is background noise or the start of a targeted campaign. That distinction has kept us ahead of every exploitation event this year."
>
> **Director of Threat Intelligence, Global Telecommunications Carrier**

> "Before GreyNoise, our change advisory boards wanted weeks of justification before approving emergency patches. Now we package GreyNoise data into our threat reports and get authorization the same day. The external evidence speaks for itself."
>
> **VP of Network Security Operations, Global Telecommunications Carrier**