

— TELECOMMUNICATIONS · CRITICAL INFRASTRUCTURE

How a top telecom fought copper theft without building a GSOC

25+ arrests, powered by HiveWatch GSOC-as-a-Service and the HiveWatch OS.

72 hrs	25+	Zero	\$100K+
TO FIRST ARRESTS	ARRESTS	HITS AT REPEAT SITES	COST PER INCIDENT



2:13 AM · COVERT CAMERA CATCHES SUSPECTS MID-THEFT

FIG. 01

An industry-wide problem

Copper theft isn't a petty crime anymore. Law enforcement can treat it as domestic terrorism when it interrupts critical infrastructure — and these attacks have real implications for connectivity worldwide. In 2025, telecom networks reported 18,327 theft and vandalism incidents — 50 per day — impacting more than 11.8 million customers, according to USTelecom.

The motive is simple: copper is up roughly 52% per pound in the last year, and theft rose 59% over 2024. It's driven largely by organized criminal networks who know how to remove the material and sell it at volume. 2025 disruptions cost up to \$1.47 billion in economic gain, per Dr. Edward J. Lopez.

Downed networks affect 911 centers, critical infrastructure and public safety operations, banking, and airlines. All of it hits the economy at scale.



ARREST FOLLOWING OPERATOR ESCALATION

Multiple hits per week, six figures per hit

A large telecommunications customer was getting hammered with copper theft, resulting in outages with widespread implications. Sites in one of the hardest-hit regions in the country were struck multiple times a week. Thieves cut lines, stripped copper, and left customers without connectivity.

Here's what's often overlooked: the copper is the cheapest thing stolen. Each incident cost the customer at least \$100,000 after adding up total impact:

- The material itself, plus the labor to replace it.
- Downtime for the communications and internet services running across those lines.
- Credits and refunds owed to consumers and businesses who paid for service they didn't get.
- Fees owed to other companies that pay to use that infrastructure — when service is down, so is that revenue.
- SLA penalties for downtime, and regulatory exposure whenever critical infrastructure goes dark.

At multiple incidents per week, that math gets ugly fast.

And this wasn't smash-and-grab opportunism. The patterns pointed to organized theft rings: moving used copper at volume takes technical knowledge of what's safe to touch, a network of scrappers, and access to the limited number of facilities in any area that can process the raw material.

A full GSOC program, as a service

The customer needed a program that stopped the crime quickly — without spending a year building a SOC from scratch. With HiveWatch GSOC-as-a-Service, they got one.

- 01 **Layered monitoring, overt and covert.** Highly visible cameras at targeted sites, backed by covert sensors and alarms.
- 02 **An effective 24/7 operations center.** Operators who verify events in real time, escalate quickly, and don't let an alarm sit in a queue.
- 03 **Real-time loudspeaker intervention.** When someone approached a site, operators addressed them directly over loudspeakers as an initial deterrent.
- 04 **A rapid response network.** Off-duty law enforcement dispatched for response, plus direct escalation to on-duty police when needed.
- 05 **Evidence that builds cases.** Operators identified vehicles and suspects and fed that intelligence to law enforcement, including supporting drone deployments to follow vehicles and make arrests.

One platform behind it all

GSOCaaS isn't a room full of people watching screens — it's operators working inside the HiveWatch OS, the same platform our software customers use. Camera feeds, sensor alarms, and access events come together in one place, and a layer of AI resolves false alarms. Operators look at only real incidents, verify what's happening, and escalate what matters. Every incident log becomes a record law enforcement can use to build a case.

The service and the software aren't two products. They're one program.

How copper crime was deterred

Outcomes from the first 60 days of the program.

72 hours	First arrests made within 72 hours of starting the program.
25+ arrests	With large criminal cases now being developed against organized theft networks.
Targeted	Law enforcement acted on operator escalations, tracking suspect vehicles and making arrests.
Zero hits	Repeat-target sites went from multiple hits per week to zero. Cameras went up, loudspeaker intervention started, and the thefts stopped.
\$100K+	Saved per prevented incident. The program has paid for itself many times over.

Deterrence isn't theoretical. When thieves know a site is monitored by people who respond in seconds — not a camera someone reviews next week — they move on. And the \$100K-per-incident math makes calculating your return a no-brainer.

Every prevented incident is six figures back on your balance sheet. You don't need to build a GSOC to get results like these — you need one that already works.

Losing six figures per incident?

See how HiveWatch GSOC-as-a-Service can run yours.

hivewatch.com