

# GREYNOISE

## Real time intelligence for modern threats

Gain real-time, verifiable attack telemetry collected by a global network of sensors mimicking commonly used and exploited cyber assets.

### GreyNoise Contacts

- Kent Rounds, SVP World Wide Sales, [kent@greynoise.io](mailto:kent@greynoise.io)
- Eric Hoffman, Director of Federal Sales, [eric@greynoise.io](mailto:eric@greynoise.io)
- Mike Baker, Federal Sales Manager, [mbaker@greynoise.io](mailto:mbaker@greynoise.io)

### Why GreyNoise?

Today's attackers mass scan the internet to exploit perimeter weaknesses. The same Tactics, Techniques and Procedures are repeatedly used to exploit countless organizations. Our sensors are patient zero for these attacks, collecting valuable telemetry in the interaction. We distribute this intelligence in near real-time with verifiable proof so that our customers can act quickly. Our mission is to ensure that **no attack works twice.**

[www.greynoise.io](http://www.greynoise.io)

# GREYNOISE



## IP Alert Reduction

- Reduce IP alert volume by up to 70%
- IP enrichment on your SIEM and SOAR alerts
- Integrates with your threat intel platform



## Exploit Defense

- Block mass-scanner IPs with malicious intent
- Block IPs probing for specific CVEs
- Search specific IP addresses targeting your network



## Patch Prioritization

- Identify high-priority patches based on in-the-wild exploitation data
- Detect CVE exploitation faster than CISA-KEV
- Improve emergency response against zero-days and novel exploits



## Threat Hunting

- Speed up investigation times with IP details such as intent, scanned ports, and fingerprints
- Gain visibility into historical activity of an IP
- Detect similar IPs based on behavioral patterns

**VISIT US AT HIMSS 2025 - CARAHSOFT BOOTH - DEMO KIOSK 3**

*Day 2, Wednesday, March 5, 2025 - 9:45am – 5:30pm*

[www.greynoise.io](http://www.greynoise.io)