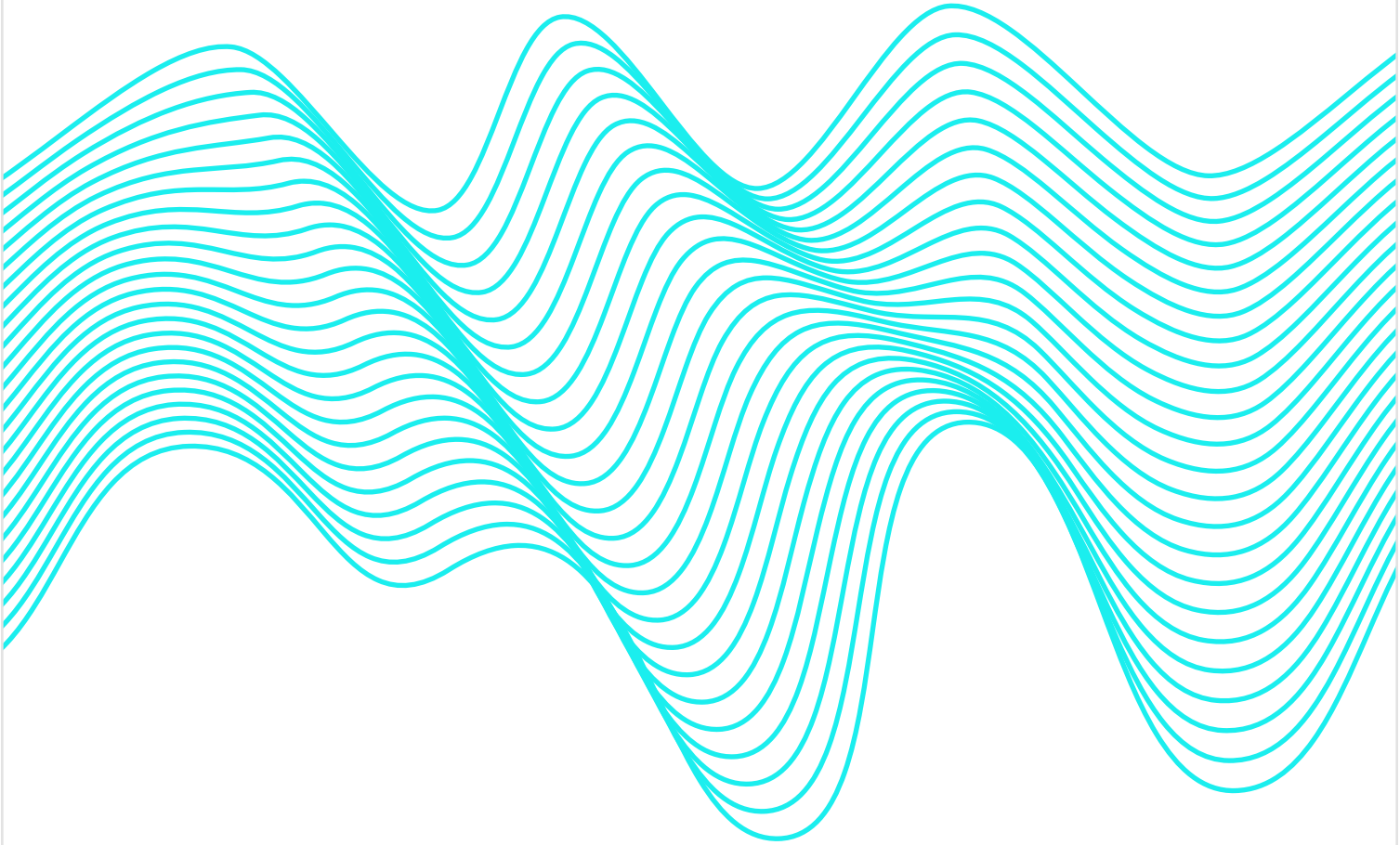
GREYNOISE

INTELLIGENCE



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.

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

How GreyNoise fits into your security operations

Traditional Threat Intelligence

- OSINT (forums, blogs, social media, news)
- Vulnerability databases and vendors (NVD, CVE)
- Threat sharing Communities (ISACs)
- Security researchers

GreyNoise Threat Intelligence

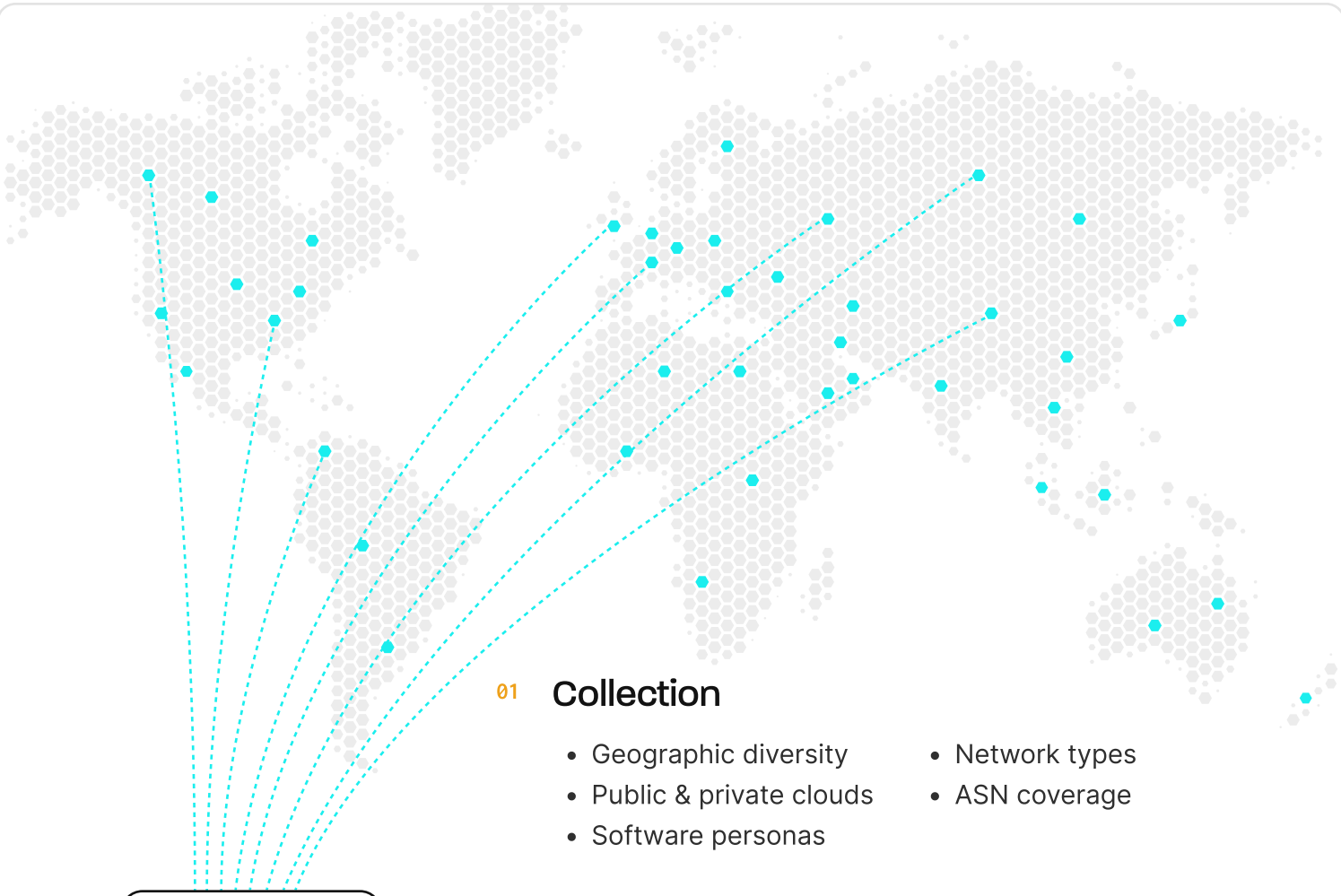
- Thousands of sensors dispersed across 50+ countries
- Mimics hundreds of cyber assets
- Deployed in thousands of POPs, ASNs, and network types

Threat intel that is immediately actionable.

- Collected and analyzed in near real-time
- Complete, verifiable receipts of the interaction
- Machine-readable to enable automation

Outcomes

- ✓ Filter false-positive & low-priority alerts
- ✓ Speed up investigation times
- ✓ Patch critical vulnerabilities with active exploitations in-the-wild
- ✓ Block malicious IPs exploiting a particular vulnerability or scanning your network



01 Collection

- Geographic diversity
- Public & private clouds
- Software personas
- Network types
- ASN coverage

02 Analysis

- Machine learning
- Metadata processor
- PCAP processor
- Data tagging
- Data indexing

03 Dissemination

- REST APIs
- Integrations
- Alerts
- Manual Search
- Raw PCAP
- Bulk Data

Microsoft Copilot for Security · Microsoft Sentinel · IBM Radar · Google SecOps · Chronicle · splunk> · paloalto NETWORKS · cisco SecureX · FORTINET · elastic · tines · ANOMALI · zscaler · RAPID7 · Recorded Future