GREYNOISE

USE CASES

5 Ways GreyNoise Drives Better Decisions in SOAR

Automation alone does not improve outcomes, better decisions do. GreyNoise delivers real-time threat context into your SOAR workflows so teams can triage faster, automate with more confidence, and ground response actions in actual attacker activity. Here are five ways SOC teams are putting it to work.

01. IP Enrichment for Faster Triage and Response Times

The Problem

Analysts manually look up IPs to understand threats, wasting time on routine enrichment and making inconsistent triage decisions.

The Solution

SOAR playbook automatically enriches every alert with GreyNoise data (classification, tags, threat level) and applies decision rules to route cases automatically.

Workflow Alert fires → /v3/ip lookup (single or bulk up to 10K) → classify → route by decision path → enrichment written to case

The Benefit

Faster response times, consistent triage regardless of shift, dramatic reduction in alert volume (40-60%).

02. Early Warning for Vendor CVE Exploitation Spikes

The Problem

Organizations don't see global exploitation spikes targeting their vendors until it's too late. Surges may signal imminent zero-day or novel exploitation activity but are invisible to individual orgs.

The Solution

GreyNoise Event Feeds send alerts to SOAR when scanning or exploitation for your vendor's CVEs surges. Playbook creates case, VM ticket, blocklist updates, and ChatOps notification automatically.

Workflow Vendor CVE Spike webhook → SOAR ingest → benign vs malicious threat assessment → CVE + IP enrichment → case, VM ticket, blocklist, ChatOps

The Benefit

Detect rising exploitation activity days before vendors announce new vulnerabilities. Patch and harden before widespread attacks. Automatically separate real threats from benign scanning activity.

Copyright © 2026 GreyNoise, Inc.

03. Detect Compromised Edge Devices

The Problem

Compromised edge devices can scan the internet or call home to attacker-controlled C2 infrastructure undetected. EDR can't run on these devices, so you typically only find out when blacklisted or reported by external parties.

The Solution

GreyNoise alerts SOAR via webhook when your IP ranges are observed conducting unsolicited scanning. A separate callback IP feed alerts SOAR whenever GreyNoise detects a new callback IP, which SOAR correlates against your outbound activity. Both trigger automatic case creation and containment tickets.

Workflow CIDR Alert webhook → SOAR ingest → device lookup → classify + tag assessment → case + containment ticket

Workflow Callback IP feed webhook → SOAR ingest → correlate with internal IP space → case + containment ticket

The Benefit

Detect compromise before reputation damage. Automated response fires in seconds. Persistent issues tracked in single case timeline.

04. Build High-Trust Blocklists

The Problem

Organizations want to automate blocklist updates, but risk blocking business-critical IPs and disrupting legitimate services.

The Solution

Use GreyNoise business services intelligence as a validation step before an IP is added to a blocklist. If the IP is tied to a business service, require manual review. If not, proceed automatically.

Workflow Analyst flags IP for blocking → SOAR checks GreyNoise Business Services Intelligence → match found: manual review → no match: automatic blocklist update

The Benefit

Automate blocklist updates with more confidence. Reduce over-blocking risk while maintaining fast response to likely malicious IPs.

05. Build Valuable Threat Intelligence into Agentic Workflows

The Problem

Agentic workflows need high-quality threat intelligence to support investigation and response. Without it, agents rely on incomplete context or low-confidence data.

The Solution

GreyNoise integrates into agentic workflows so agents can access high-quality threat intelligence through APIs, skills, or MCPs to support investigation and response actions.

Workflow Agent receives request or trigger → queries GreyNoise through APIs / skills / MCPs → analyzes threat intelligence context → returns output or triggers response workflows

The Benefit

Enable faster, more confident investigation and response by giving agents access to high-quality threat intelligence.

Copyright © 2026 GreyNoise, Inc.