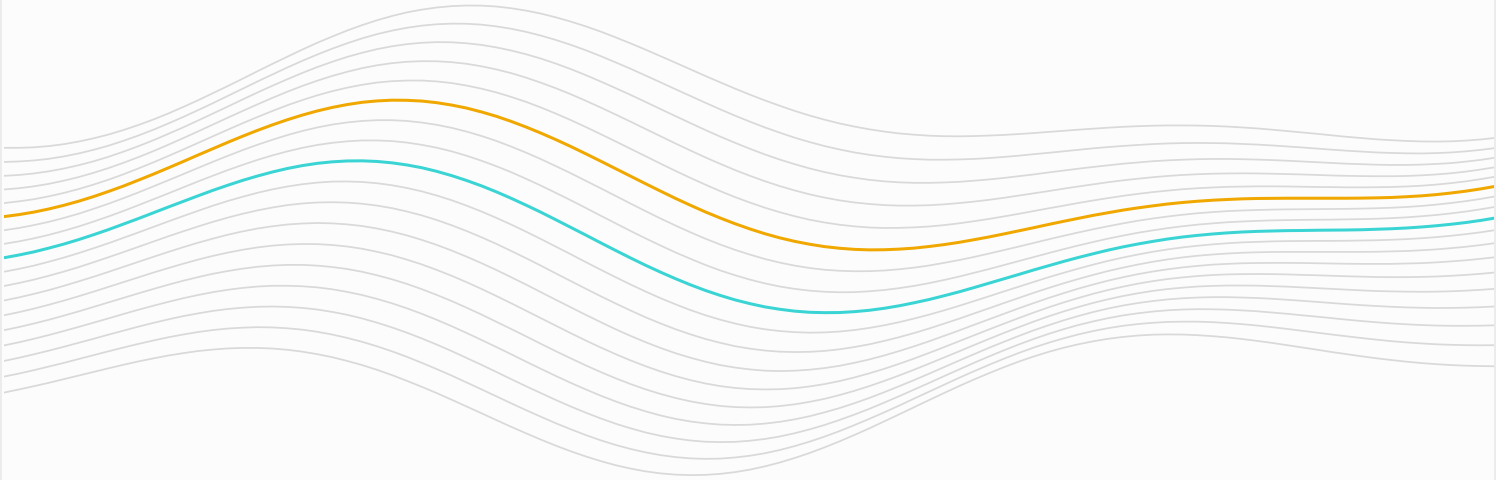
GREYNOISE



CASE STUDY

Merit Network Cuts Alerts by 25% and Gains Edge Visibility Across Its Michigan Network

Merit Network | Research and Education Network (REN), Nonprofit | Ann Arbor, Michigan

01 Company Overview

Merit Network is an independent nonprofit governed by Michigan's public universities. Founded in 1966, it operates America's longest-running regional research and education network, with more than 4,000 miles of fiber connecting hundreds of organizations across Michigan, including universities, K-12 districts, libraries, healthcare organizations, and government agencies.

Beyond connectivity, Merit provides security services through its Security Operations Center, alongside managed firewall, DDoS protection, and vulnerability scanning. Its security team protects a diverse range of member environments, each with its own equipment, resources, and security requirements. Understanding the activity targeting those environments is essential to helping members identify and respond to threats

INDUSTRY

Research and Education Network (REN), Nonprofit

LOCATION

Ann Arbor, Michigan

PRODUCTS

GreyNoise Block, GreyNoise deception sensors

USE CASES

- Alert reduction and SOC efficiency
- Network-specific threat visibility
- Threat hunting for CVEs and campaigns
- IP and ASN enrichment

02 Challenge

Merit's security team needed to deepen visibility into its member environments, assess potential threats faster, and reduce alert workload,

A Need for Direct Visibility Into Merit's Own Network.

Merit protects institutions with a diverse mix of equipment and systems. Building on GreyNoise's global threat context, the team wanted to see scanning activity directed at its own infrastructure, particularly activity targeting equipment profiles used by its members.

Time-Consuming Research Slowed Investigation Decisions.

Assessing individual IP addresses or entire autonomous systems (ASNs) required manual research into their activity and potential intent. The team needed a faster way to distinguish routine scanning from activity warranting deeper investigation and identify relevant vulnerabilities or campaigns to hunt for.

High Alert Volume Despite Existing Filtering.

Merit was already filtering its alerting pipeline and blocking benign scanners, but remaining alert volume continued to consume analyst attention and SOC processing capacity. The team needed to reduce unnecessary alerts and free staff to focus on more critical investigations.

Copyright © 2026 GreyNoise, Inc.

03 GreyNoise in Action

01

Dynamic Blocklists Wired Into the Detection Pipeline

Merit started with GreyNoise Block, building continuously updated IP lists to its firewalls. Deployment took minutes, and firewall hits dropped immediately. Merit then integrated the same lists and wired them into threat detection and alerting to filter scanning traffic before it generated alerts, further reducing noise

02

A Sensor Network Shaped Like Merit

Merit deployed more than 250 GreyNoise deception sensors across non-contiguous address blocks, on its own network, configured to match the real-world equipment profiles of its member institutions. What they attract is what actually targets Michigan research and education infrastructure. The result is primary-source observation of what is probing Merit's own network, not only what is probing the internet at large.

03

Faster Threat Hunts and Instant Indicator Context

Cross-referencing observed indicators against GreyNoise classifications is now a standing step in Merit's investigation process. When an IP or an entire ASN resolves to a known common scanner, analysts deprioritize it in seconds instead of researching it from scratch. A spike in tagged activity tied to a specific CVE or campaign tells the team what to go hunt for in their own data.

> “
>
> Block makes it easy to build dynamic, continuously updated IP lists that can be used to block, filter, or tag traffic. We were already blocking benign scanners, but integrating these lists into our threat detection and alerting pipeline reduced alert volume even further. The benefit is less alert fatigue and fewer alerts processed by our SOC infrastructure, which frees up our analysts to handle more critical investigations.
>
> SECURITY OPERATIONS TEAM, MERIT NETWORK

Copyright © 2026 GreyNoise, Inc.

04 Results

Merit reported the following outcomes across its SOC and threat hunting operations.

Up to 25%
Fewer Alerts

500 million
fewer events each month

8 hours
saved each week

250+
GreyNoise deception sensors

Up to 25% Fewer Alerts.

Merit reduced alert volume by up to 25% by integrating continuously updated IP address lists from GreyNoise Block into its detection and alerting pipeline. At Merit's scale, that means roughly 500 million fewer events each month, with monthly volume dropping from about 1.9 billion to about 1.4 billion. These efficiency gains came on top of the team's existing filtering and blocking efforts.

8 Hours Saved Each Week for Higher-Priority Investigations.

Fewer alerts reduced alert fatigue and the processing load on SOC infrastructure, freeing about 8 hours a week across Merit's security team to focus on investigations requiring more critical attention. The most noticeable gain has been how quickly analysts can now understand the intent behind activity, or confirm there is none.

Direct Visibility Into Activity Targeting Merit's Infrastructure.

GreyNoise deception sensors gave Merit firsthand visibility into scanning activity directed at its own network. Configuring sensors to match member institutions' equipment profiles helped the team uncover activity relevant to the systems it protects.

Faster Triage and More Focused Threat Hunts.

Analysts used GreyNoise classifications and tags to quickly assess IP addresses and entire ASNs, reducing manual research and helping them decide what warranted deeper investigation. Spikes in activity associated with specific vulnerabilities or exploitation campaigns gave the team early signals to guide hunts in its own network data.

05 Customer Perspectives

> "Having our own sensor network has provided insights that global threat intel data alone couldn't provide, because of our unique customer base and the industry verticals we serve. We can see who and what is actually targeting our infrastructure, and pull indicators that are more directly relevant to our environment."
>
> SECURITY OPERATIONS TEAM, MERIT NETWORK

Copyright © 2026 GreyNoise, Inc.