THREATQUOTIENT™ GREYNOISE

THREATQ™ AND GREYNOISE

Technology Segment: Intel Feeds

GREYNOISE OVERVIEW

GreyNoise collects, analyzes, and labels IPs that scan the internet and saturate security tools with noise. This unique perspective helps analysts waste less time on irrelevant or harmless activity, and spend more time focused on targeted and emerging threats.

THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ data-driven security operations platform is both open and extensible, supporting the integration of disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

GREYNOISE FOR THREAT INTELLIGENCE

GreyNoise's internet-wide sensor network passively collects packets from hundreds of thousands of IPs seen scanning the internet every day.

Companies like Shodan and Censys, as well as researchers and universities, scan in good faith to help uncover vulnerabilities for network defense. Others scan with potentially malicious intent. GreyNoise analyzes and enriches this data to identify behavior, methods, and intent, giving analysts the context they need to take action.

INTEGRATION HIGHLIGHTS

Enrich threat feeds to identify IP's used for mass scanning and exploitation

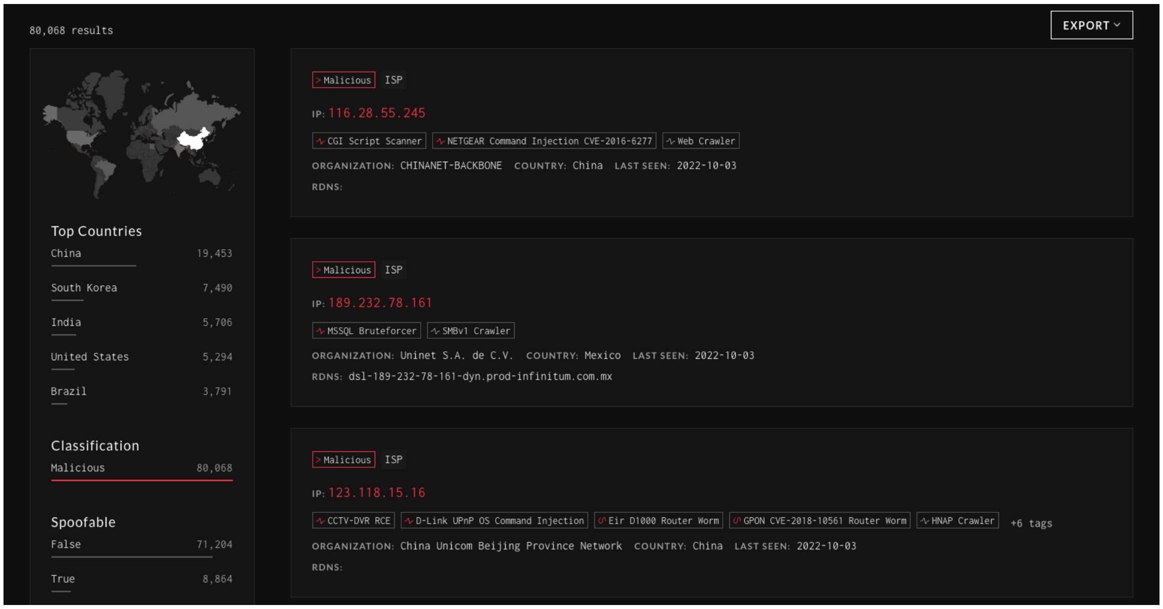
Prioritize alerts by integrating data with a SIEM

Re-score indicators in ThreatQuotient based on mass scanning activity to identify noise in data feeds

INTEGRATION USE CASES:

The Integration supports a variety of use cases such as:

- Integration with a SIEM to better prioritize alerts by understanding targeted attacks vs mass exploitation occurring across the internet
- Enriching threat intel data and better contextualizing different threat feeds
- Adding additional context when mapping infrastructure to identify scan and attack traffic from IP addresses observed by the GreyNoise sensor network



80,068 results

Top Countries

China	19,453
South Korea	7,490
India	5,706
United States	5,294
Brazil	3,791

Classification

Malicious	80,068

Spoofable

False	71,204
True	8,864

> Malicious ISP

IP: 116.28.55.245

CGI Script Scanner | NETGEAR Command Injection CVE-2016-6277 | Web Crawler

ORGANIZATION: CHINANET-BACKBONE COUNTRY: China LAST SEEN: 2022-10-03

RDNS:

> Malicious ISP

IP: 189.232.78.161

MSSQL Bruteforcer | SMBv1 Crawler

ORGANIZATION: Uninet S.A. de C.V. COUNTRY: Mexico LAST SEEN: 2022-10-03

RDNS: dsl-189-232-78-161-dyn.prod-infinitum.com.mx

> Malicious ISP

IP: 123.118.15.16

CCTV-DVR RCE | D-Link UPnP OS Command Injection | Eir D1000 Router Worm | GPON CVE-2018-10561 Router Worm | HNAP Crawler | +6 tags

ORGANIZATION: China Unicom Beijing Province Network COUNTRY: China LAST SEEN: 2022-10-03

RDNS:

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC.

For more information, visit www.threatquotient.com.

ABOUT GREYNOISE

GreyNoise is THE source for understanding internet noise. We collect, analyze and label data on IPs that saturate security tools with noise. This unique perspective helps analysts waste less time on irrelevant or harmless activity, and spend more time focused on targeted and emerging threats. GreyNoise is trusted by Global 2000 enterprises, government organizations, top security vendors and tens of thousands of threat researchers.

For more information, please visit https://www.greynoise.io/, and follow us on Twitter and LinkedIn.