SOLUTION BRIEF

Fortinet and GreyNoise Security Solution

Filter the Noise and False Positives Out of Your Security Incidents

Executive Summary

Fortinet and GreyNoise have partnered to identify and filter "noisy" security events out of alert and incident information via integration with Fortinet FortiSOAR, so security teams can focus on true threats and improve their security effectiveness.

Challenge

Every machine connected to the internet is exposed to a barrage of communications from tens of thousands of unique IP addresses per day—we call this "internet background noise." This massive volume of unsolicited traffic is a challenge for security organizations because it often triggers security tools to generate thousands of events to be analyzed, with little context. As a result, security analysts struggle to differentiate targeted cyberattacks from false positives created by internet background noise.

To address this challenge, GreyNoise and Fortinet have established a technology partnership to provide the context organizations need to filter out internet background noise from their FortiSOAR alert traffic. The partnership helps FortiSOAR security teams reduce the time they spend on harmless or irrelevant alerts by up to 25%, so they can focus on the true threats facing their organization.

Joint Solution

GreyNoise and Fortinet have partnered to deliver an industry-leading security solution to address these challenges. The integration of the GreyNoise Intelligence product and Fortinet FortiSOAR, enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, delivers context about IP addresses that generate internet background noise, so customers can more quickly filter out harmless and irrelevant events, and stay focused on the alerts that matter.

Joint Solution Components

- Fortinet FortiSOAR
- GreyNoise Intelligence

Joint Solution Benefits

- Faster triage of false-positive incidents generated by internet background noise
- Faster triage of false-positive incidents generated by common business services
- Improved security from deeper/faster insight into malicious IP addresses that scan the internet
- Reduced alert fatigue resulting from too many false positives

FORTINET FABRIC-READY

Joint Solution Components

GreyNoise is a cybersecurity platform that collects and analyzes internet-wide scan and attack traffic, classifying IPs that saturate security tools with noise. With this integration, users can contextualize existing alerts, filter false positives, identify compromised devices, and track emerging threats. This integration supports free GreyNoise Community accounts and paid GreyNoise subscriptions.

Fortinet FortiSOAR

FortiSOAR is a holistic security orchestration, automation, and response workbench, designed for security operations center (SOC) teams to efficiently respond to the ever-increasing influx of alerts, repetitive manual processes, and shortage of resources. This patented and customizable security operations platform provides automated playbooks and incident triaging, and real-time remediation for enterprises to identify, defend, and counter attacks.

Joint Solution Integration

Using the GreyNoise Connector for FortiSOAR, analysts are able to automate or perform on-demand IPv4 lookups or queries to add context to Alerts and Incidents. In addition, analysts can identify blocks of IP addresses to monitor for scanning activity, to help identify potential compromised devices.

IP Enrichment—Is It Noise?

Based on the IP lookup results, the analyst can take the following actions:

- **IP Address Found, Classified Benign**
  - ***Action: Close Alert/Incident***—This is a known benign actor scanning the internet, such as Shodan or Censys.
- **IP Address Found, Classified Malicious**
  - ***Action: Decrease Alert/Incident Severity***—This is a known malicious actor opportunistically scanning the entire internet, and not a targeted attack. However, this is confirmed malicious activity, and remediations should be validated to ensure no exploit is occurring.
- **IP Address Found, Classified Unknown**
  - ***Action: Decrease Alert/Incident Severity***—This IP is scanning internet-wide, but GreyNoise is unable to confirm if the activity is benign or malicious.
- **IP Address Not Found**
  - ***Action: Increase Alert/Incident to Highest Level Severity***—This is potentially a targeted attack on this device.

Historically, GreyNoise has seen up to 20% of alert traffic composed of internet noise (individual customer experience may vary). The playbooks and actions in this connector integration help reduce noise and common business services from your Incident Response work, freeing up time to focus on true threats.

They also help automate repetitive tasks associated with routable IPv4 addresses:

- Query an IP to determine if it is internet background noise
- Query an IP to determine if it is a common business service
- Query the GreyNoise dataset for common trends by looking for CVEs, paths, ports, or fingerprints
- Extract statistics from the GreyNoise dataset for threat hunting and identifying emerging threats
- Calculate the severity of the incident using GreyNoise IP reputation data

IP Scanning Monitoring—Is It Compromised?

If an IP address owned by your organization or that of your customers or partners is scanning the internet, this is often a tell-tale sign that the device is compromised. The GreyNoise integration with FortiSOAR allows analysts to monitor IP addresses to identify scanning activity, creating an alert in the FortiSOAR platform when activity is detected.

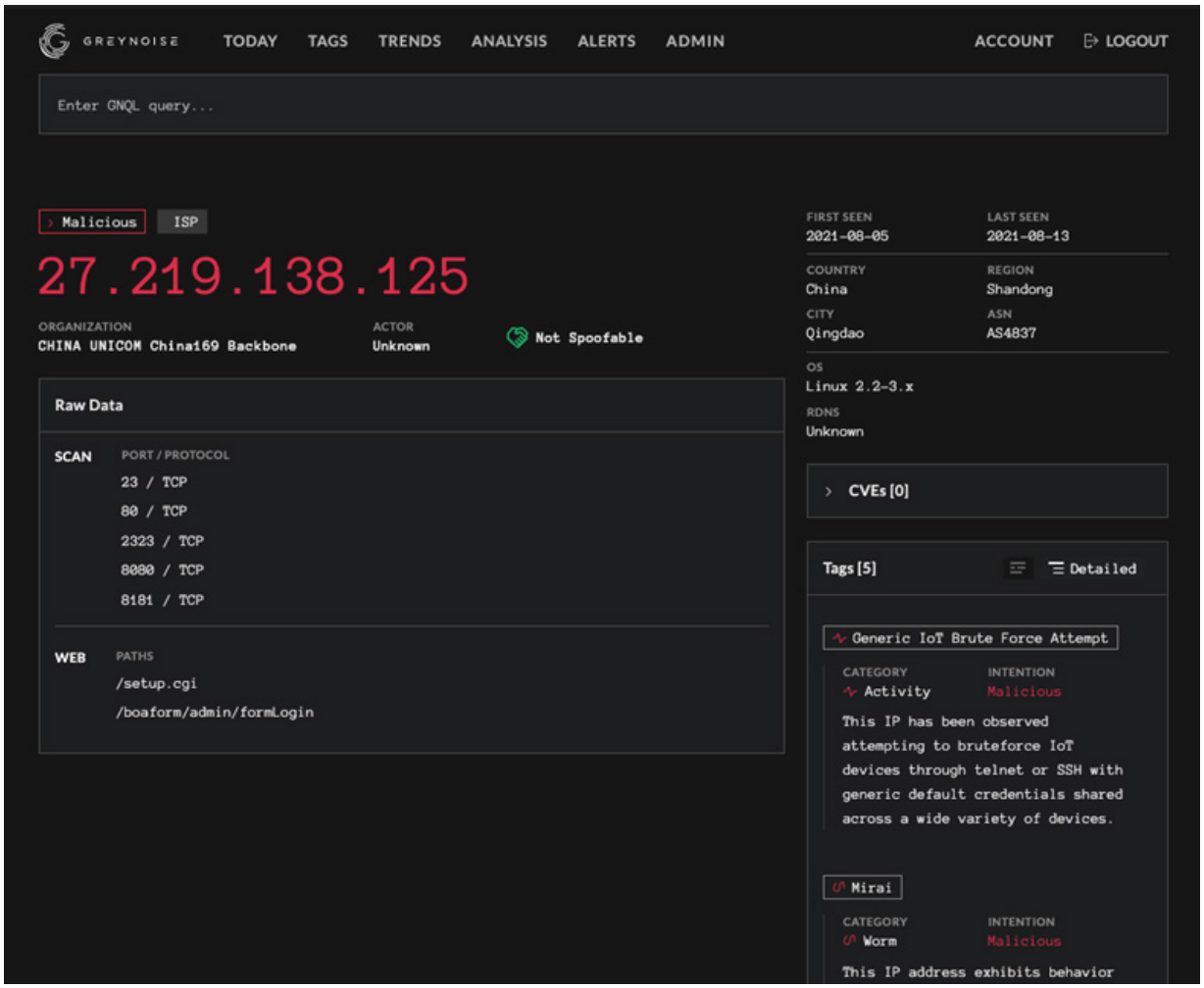

Figure 1: IP context from the GreyNoise visualizer.

Joint Use Cases

Use case 1: Alert reduction—deprioritizing alerts from inbound scanning/outbound communications

When a perimeter device detects a scan from an internet device or an outbound connection to a known scanner, the source and destination IPs are captured in the log. These log events generate alerts/incidents within FortiSOAR, and the IP address is automatically queried via the GreyNoise API using the GreyNoise IP Full Lookup playbook. The event/incident severity level is then adjusted based on the context provided by GreyNoise.

Use case 2: Alert reduction—deprioritizing alerts from inbound SSH login attempts

When an SSH login is detected from an unknown source, the IP of the login attempt is captured in the log. This log event then generates an event/incident within FortiSOAR, and the IP address is automatically queried via the GreyNoise API using the GreyNoise IP Full Lookup playbook. The alert/incident severity level is then adjusted based on the context provided by GreyNoise.

Use case 3: Compromised device detection—monitoring IP addresses for outbound scanning activity

An analyst identifies an IP address or CIDR block of addresses for GreyNoise to monitor—these can be organization-owned, customer-owned, or partner-owned IPs. If an IP address in the monitored group is detected scanning the internet, GreyNoise will generate an alert in FortiSOAR for further investigation.

About GreyNoise

GreyNoise helps security analysts save time by revealing which events and alerts they can ignore. We do this by curating data on IPs that saturate security tools with noise. This unique perspective helps analysts confidently ignore irrelevant or harmless activity, creating more time to uncover and investigate true threats. This data is delivered through our SIEM, SOAR and TIP integrations, API, command-line tool, bulk data and visualizer. GreyNoise is trusted by Fortune 500 enterprises, governments, top security vendors and thousands of threat researchers. For more information, please visit https://www.greynoise.io, and follow us on Twitter and LinkedIn.

September 15, 2021 10:34 PM
1272660-0-0-EN