KNOW MORE NOISE

GREYNOISE

REN-ISAC Techburst

Tracking Internet Noise to Reduce Alerts and Focus on Trending Exploits

Andrew Morris, Founder & CEO, Greynoise

February, 2022

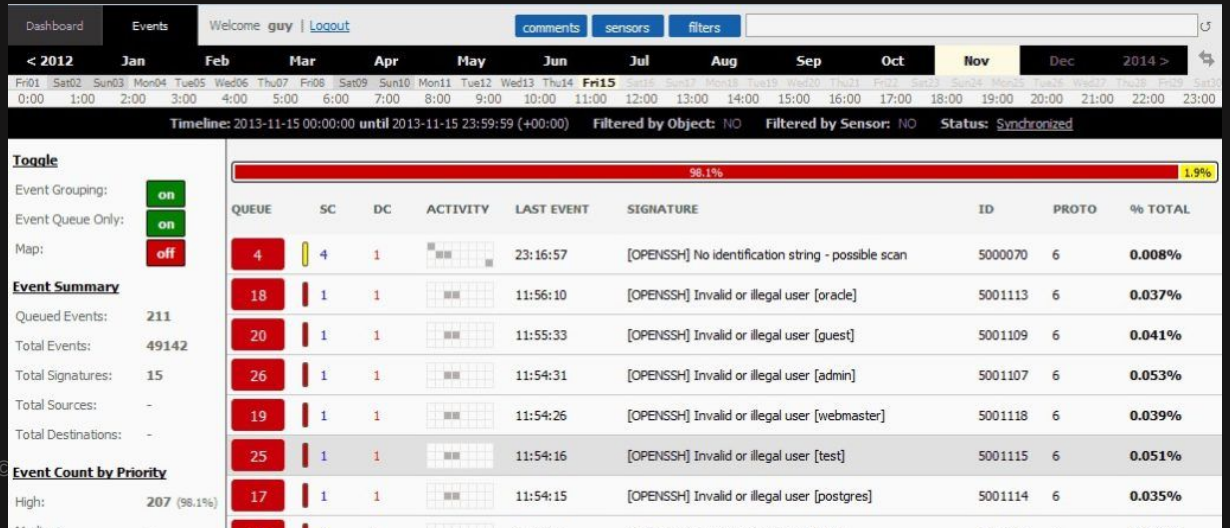
Meet the Speaker

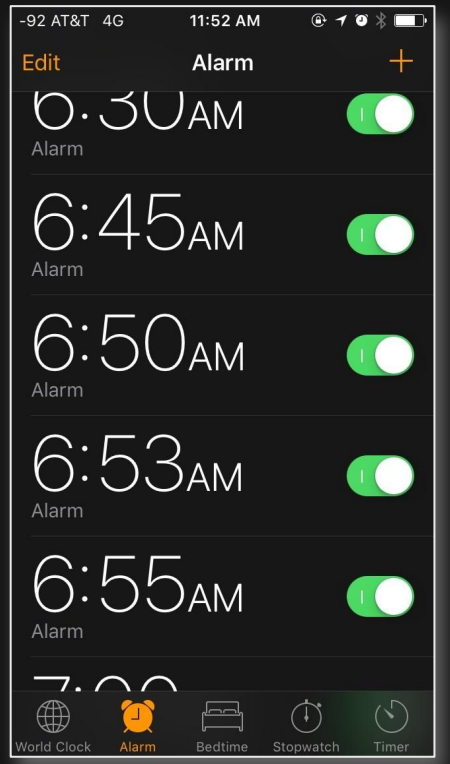
Andrew Morris

Founder and CEO
GreyNoise Intelligence
@Andrew___Morris
andrew@greynoise.io

EVERYONE IN THE SOC IS TOO BUSY

- Everything feels on fire all the time
- Every alert is critical, but lacking context
- There is not enough time to do meaningful work
- If every alert is urgent, then nothing is urgent





Is this what your IDS feels like?

INTERNET NOISE IS PART OF THE PROBLEM

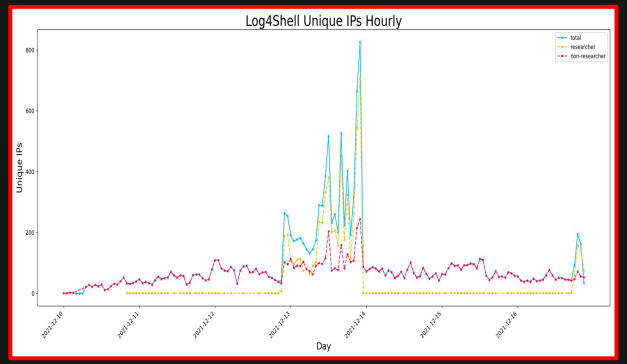
The internet is super noisy

“Internet Noise” is spam targeting the SOC

- Every machine connected to the internet is exposed to scans and attacks from 1000’s of unique IP addresses per day.
- This triggers thousands of events to be analyzed, many from benign sources.

Source: GreyNoise analysis, 2021

Opportunistic attacks are now the #1 attack vector



Every new CVE is a race against time

- The time delay is getting shorter between a CVE being disclosed and internet-wide exploitation starting.
- It’s a race against time to see who can find vulnerable servers first.

Source: IBM X-Force Threat intelligence Index for 2021

False positives are driving alert fatigue

38%

of security alerts are “noise”

Alert fatigue is making us less secure

- 45% of alerts are false positives
- 49% of analysts ignore alerts if the queue is full
- 10-50% analyst churn in the past year

Source: IDC, CriticalStart, HelpNet Security

PROBLEM: The internet is super noisy

- No seriously, it's insanely noisy
- Have you ever used Shodan?
  - Censys?
  - BinaryEdge?
  - RiskIQ?
  - SecurityTrails?
  - BitSight?
  - Security Scorecard?
  - GOOGLE SEARCH?

The way that these technologies work has an unintended consequence...

Suricata + Emerging Threats ruleset on some empty IPs (4 days)

signature	hits	ips
ET POLICY RDP connection request	707029	1450
ET SCAN NMAP -sS window 1024	352324	6048
ET DOS Microsoft Remote Desktop (RDP) Syn then Reset 30 Second DoS Attempt	101793	698
ET POLICY MS Remote Desktop Administrator Login Request	40519	66
ET TROJAN MS Terminal Server Single Character Login possible Morto inbound	25285	156
ET DROP Spamhaus DROP Listed Traffic Inbound group 14	17800	302
ET SCAN Suspicious inbound to MSSQL port 1433	15350	4684
ET POLICY RDP disconnect request	13354	19
ET DROP Dshield Block Listed Source group 1	13100	264
ET POLICY Reserved Internal IP Traffic	12678	1
ET POLICY SSH session in progress on Expected Port	10533	383
ET SCAN Sipvicious Scan	8982	99
ET SCAN Sipvicious User-Agent Detected (friendly-scanner)	8143	91
ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infection (Inbound)	5650	67
ET SCAN Suspicious inbound to mySQL port 3306	3879	646
ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03	3261	113
ET SCAN Suspicious inbound to PostgreSQL port 5432	3234	683
ET POLICY Lets Encrypt Free SSL Cert Observed	2761	6
ET SCAN Suspicious inbound to Oracle SQL port 1521	1928	424
ET POLICY Inbound RDP Connection with Minimal Security Protocol Requested	1585	113
ET POLICY SSH session in progress on Unusual Port	903	108
ET POLICY MS Terminal Server Root login	818	248
ET INFO Potentially unsafe SMBv1 protocol in use	805	554
ET EXPLOIT [NCC GROUP] Possible Inbound RDP Exploitation Attempt (CVE-2019-0708)	674	22
ET POLICY DNS Update From External net	479	1
ET SCAN Suspicious inbound to mSQL port 4333	378	64
ET DROP Spamhaus DROP Listed Traffic Inbound group 2	304	14
ET POLICY Inbound RDP Connection with TLS Security Protocol Requested	175	48
ET DROP Spamhaus DROP Listed Traffic Inbound group 33	150	2
ET VOIP Modified Sipvicious Asterisk PBX User-Agent	122	5
ET SCAN HID VertX and Edge door controllers discover	118	26
ET SCAN NMAP -sS window 4096	71	35
ET SCAN Malformed Packet SYN RST	70	8
ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	48	30
ET POLICY SSH Client Banner Detected on Unusual Port	46	5
ET SCAN Potential SSH Scan	45	13
ET EXPLOIT Eir D1000 Modem CWMP Exploit RCE	43	30
ET DROP Spamhaus DROP Listed Traffic Inbound group 3	39	4
ET SCAN Potential VNC Scan 5900-5920	36	17
ET DROP Spamhaus DROP Listed Traffic Inbound group 21	33	2
ET SCAN Potential VNC Scan 5800-5820	32	3
ET INFO Cisco Smart Install Protocol Observed	32	17
ET POLICY Inbound HTTP CONNECT Attempt on Off-Port	30	12
ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x02	23	1
ET DROP Spamhaus DROP Listed Traffic Inbound group 9	20	13
ET SCAN NMAP -f -sV	19	9

How noisy?

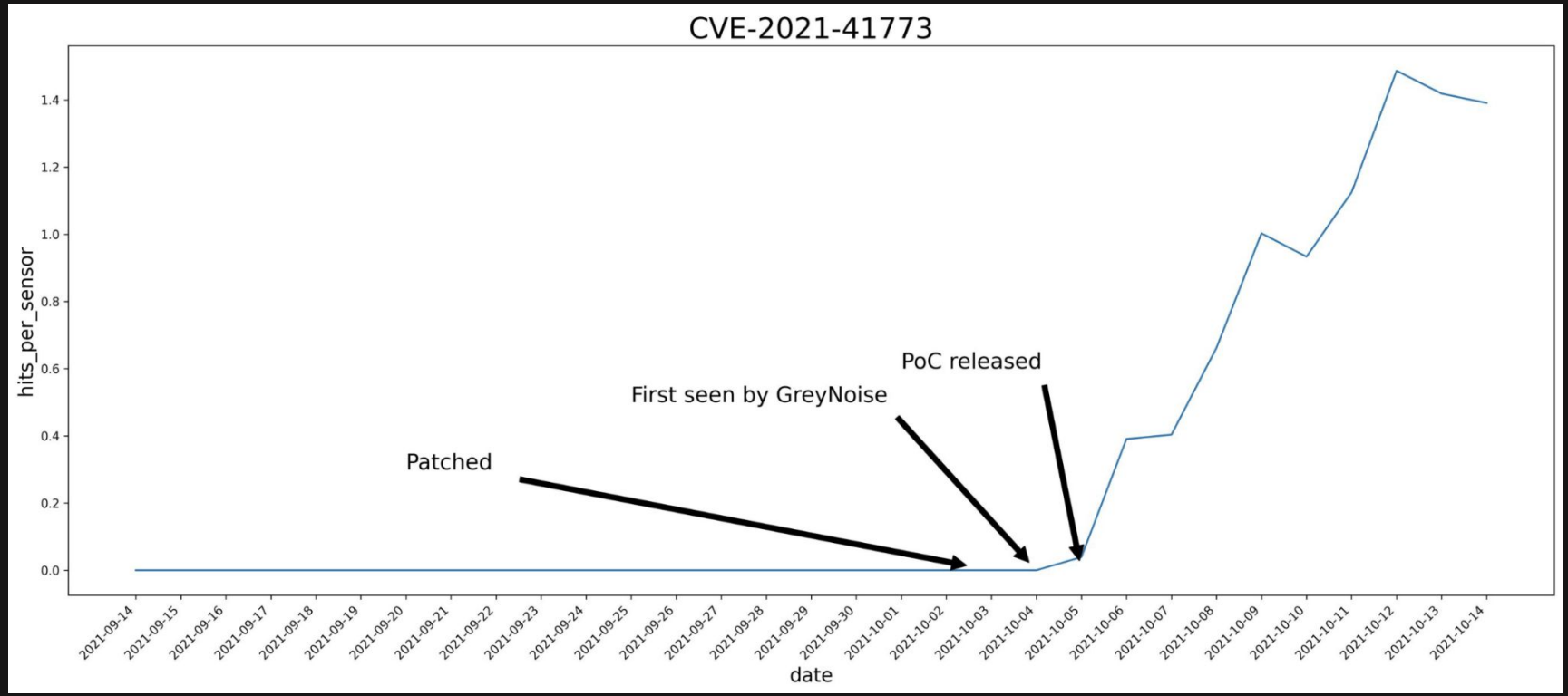
- This gets really REALLY bad on large networks
- On a daily basis, every individual routable IP on the Internet sees:
    - ~3,000 unsolicited SYNs from...
    - ~1,000 distinct IP addresses
- Each /24 receives about 46mb of unsolicited network data from ~200,000 IP addresses **from SYNs alone**
- Why?
    - BAD: To do BAD STUFF to you, from the same place or somewhere else: Credential stuffing, proxy checking, brute forces, exploit vulnerabilities, etc
    - GOOD: Web search, asset discovery, third party risk, security research

This creates a huge noise problem.

PROBLEM: Newly disclosed vulnerabilities are quickly weaponized

- There is always some time delay between a vulnerability being disclosed and internet-wide exploitation starting
- This time delay is getting shorter and shorter
- Good guys, bad guys, and those somewhere in between know this and want to scan the internet to find vulnerable servers first
- Case study: Apache CVE-2021-41773
  - Sept 29, 2021: Patch submitted
  - Oct 03, 2021: GreyNoise observes first internet-wide vuln scan
  - Oct 04, 2021: Apache version update, patch is GA
  - Oct 05, 2021: Apache discloses vulnerability to CVE

Apache CVE-2021-41773 vuln checks + exploitation



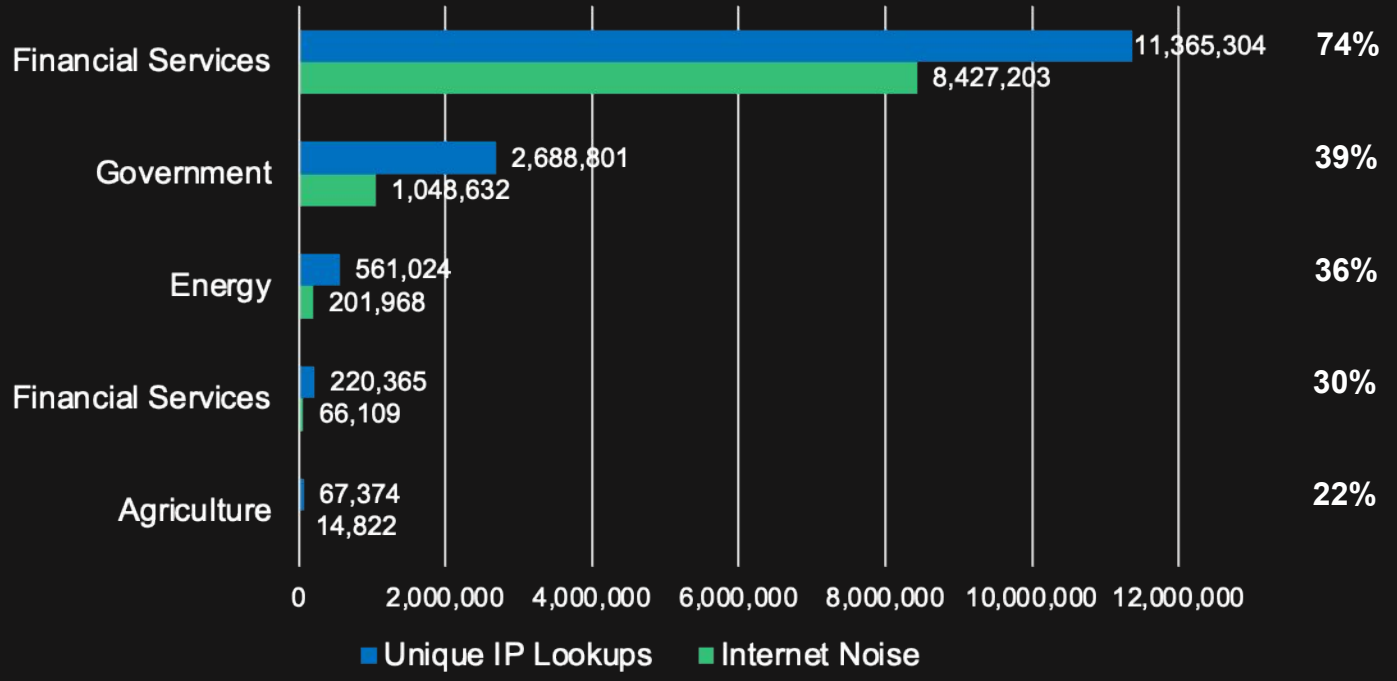
Many SOC teams have no idea which “bad” to focus on

- There used to be ***some*** bad on the internet
- There is now an absolutely insane amount of bad on the internet
- Machine hours are cheap, human hours are expensive
  - More and more attacks are automated
- **Old way**: Bad guy starts with a target organization, identifies vulnerabilities, exploits them.
- **New way**: Bad guy starts with new vulnerabilities/exploits, finds targets on the Internet who are susceptible to them.
- Which bad should you focus on?

PROBLEM: Internet Noise is a significant percentage of security alerts

Aggregate Noise %:

38%



Source: GreyNoise analysis: GreyNoise POV results for Q3 '2021, percentage of noise in SIEM/SOAR IP lookups

Vision for solving the problem of “internet noise”

What if we enumerate and classify internet traffic,

filter out the “everywhere”,

and investigate the outliers?

“Good or Bad, Everywhere or Only You” Paradigm

The IPs that hit your network can be roughly separated into these quadrants:

Categorizing the IPs that Hit your Network

	Everywhere	Only You
Bad	• Mirai • Bots • Worms • Credential bruteforcing • Unsophisticated ransomware gangs	• Targeted bad guys • APTs • Sophisticated ransomware gangs
Good	• Google Search Engine • Shodan / Censys • ASR Companies (BitSight, Security Scorecard)	• Your users • Your employees • Your customers • Your partners

GreyNoise provides the ground truth on internet noise, so your security team can

- Reduce noisy alerts in the SOC
- Defend against opportunistic attacks

GreyNoise is like noise-canceling headphones for the internet…

… or a spam filter for your SIEM.

GREYNOISE INTELLIGENCE COLLECTION

Data set:	**NOISE** *(Internet-wide scanners and attackers)*	**RIOT** *(Common internet business services)*
Context provided:	Internet-wide scanners with benign, malicious, and unknown intent.	IPs of common business services that are almost certainly not attacking you.
Examples:	Benign IPs ● Shodan, Censys, researchers, and universities who scan in good faith Malicious IPs ● Opportunistic attackers scanning for vulnerable systems	SaaS APIs ● Microsoft O365, Google Workspace, Slack Business services ● CDNs, update servers, cloud security products Internet infrastructure ● Public DNS servers, NTP services
Data source:	GreyNoise's internet-wide sensor network passively collects packets from hundreds of thousands of IPs seen scanning the internet every day.	GreyNoise's RIOT data collection includes over 70 million IPs, leveraging a number of tactics and methods to acquire, track, curate and age-off data over time.

Our data is delivered through our API, integrations and web-based visualizer.

What can you use GreyNoise to do?

BEFORE GREYNOISE

- Show me failed login attempts and brute force attacks 😐
- Show me IPs attempting to exploit hosts on my perimeter 😐
- Show me IPs that are conducting recon on my network 😐

AFTER GREYNOISE

– I see failed login attempts and brute force attacks ***that are specifically hitting my network*** 😎

– I see IPs attempting to exploit hosts on my perimeter ***and not the rest of the internet*** 😎

– I see IPs that are conducting recon on my network ***and nobody else's network*** 😎

“Good or Bad, Everywhere or Only You” Paradigm

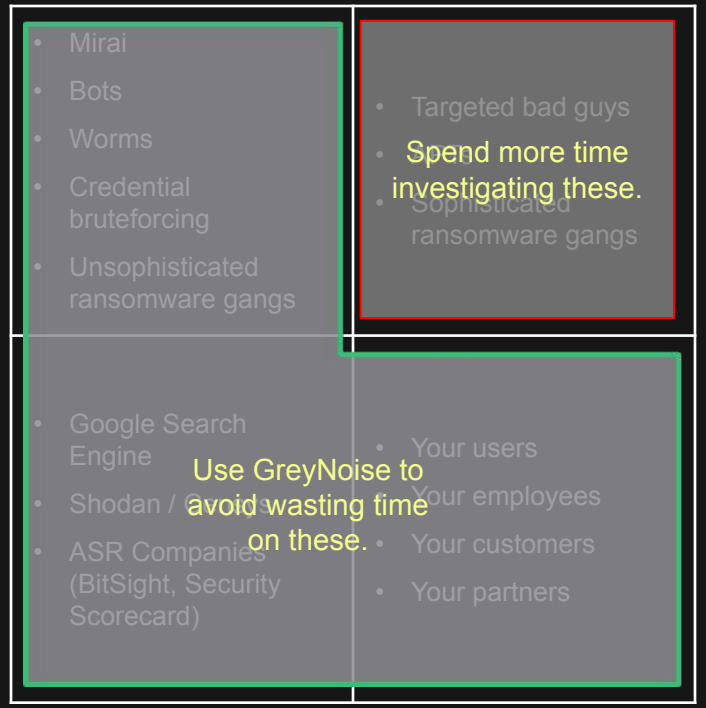
If you could focus on the threats that matter to YOU

You could spend LESS time chasing ghosts

- IP addresses that turn out to be Shodan or Googlebot…

And MORE time defending against the most dangerous targeted threats.

Categorizing the IPs that Hit your Network

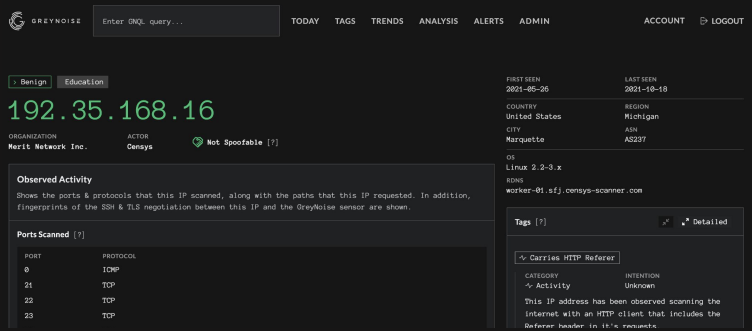


GreyNoise Stuff You Can Use Right Now

Stuff you can use right now

Free web interface:

https://greynoise.io



Unauthenticated Community API:

```
[andrew] ~ $ curl -s https://api.greynoise.io/v3/community/192.35.168.16
{
  "ip": "192.35.168.16",
  "noise": true,
  "riot": false,
  "classification": "benign",
  "name": "Censys",
  "link": "https://viz.greynoise.io/ip/192.35.168.16",
  "last_seen": "2021-10-18",
  "message": "Success"
}
```

How it works

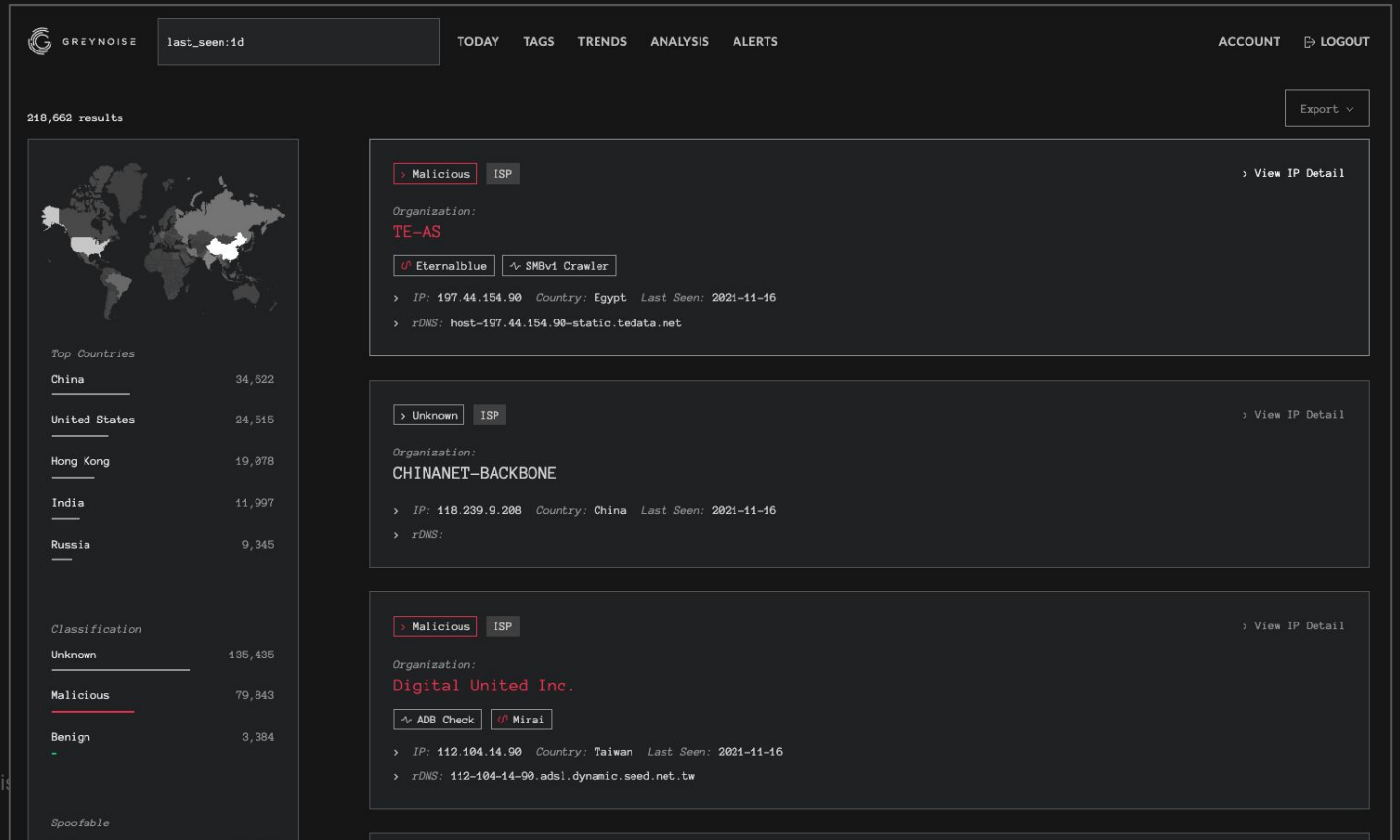
- We operate a huge network of collector sensors located in hundreds of data centers across the globe
- They sniff “internet background noise”
- Our research team tags it with useful analytics
- Those analytics are displayed to our users in their SIEM, SOAR, TIP, CLI, etc.

How you can use GreyNoise right now

Grab a list of IPs hitting your network and deploy it against our Analysis Page:

https://greynoise.io/viz/analysis

DEMO



What other cool stuff can you use GreyNoise for soon?

- What IPs are exclusively scanning/attacking a particular country?
- How many gigabytes of very low-value logs am I storing in $SIEM?
- How many other organizations in my vertical are being attacked by this IP?
- How many other analysts are investigating this IP or have had an alert raised from this IP?

What products support GreyNoise?

Operationalize **GreyNoise** Intelligence into your research tools and security automation

- SIEM
- SOAR
- TIP
- Security controls
- Analyst tools

Questions?

Thank You!

Even after filtering and blocking, most networks see at least a 25% reduction in alert volume using GreyNoise

Create your free GreyNoise account today at https://greynoise.io

Andrew Morris
Founder, CEO
@andrew___morris
andrew@greynoise.io
https://greynoise.io

Follow us on Twitter for product updates and urgent public security announcements of internet-wide exploitation:

@GreyNoiseIO