ThreatHole

ThreatHole provides AI-assisted DNS security monitoring and response by integrating Pi-hole with Splunk. It visualizes DNS activity across clients, highlights suspicious and malicious domains based on threat intelligence feeds (PhishTank, URLhaus), and tracks query trends over time. The dashboard supports active response actions (block/unblock domains, enable/disable Pi-hole) and integrates with a local assistant to generate explanations, SOC-style reports, and recommendations. This creates a complete detection → triage → response workflow for a home-network SOC.

Global Time Range: 15:00 – 23:54:23.22... | Types: All (1) | Actions: All (1) | Statuses: All (1) | Client IP: * | Domain: * | Reply types: All (1) | TI Statuses: All (1)

Statistical visualisations:

Total queries in last 24h
1,265 ↓ -92%
Total queries

Blocked queries in last 24h
37 ↓ -96%
Blocked queries

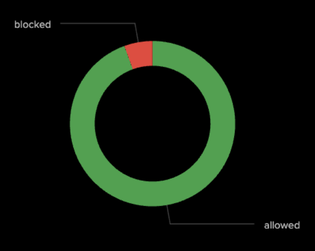
Allowed queries in last 24h
1,228 ↓ -92%
Allowed queries

Malicious queries in last 24h
0 ↓ -100%
Malicious queries

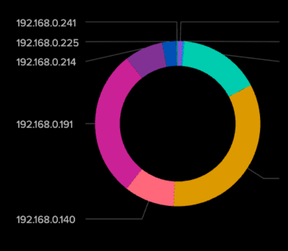
Suspicious queries in last 24h
17 ↓ -87%
Suspicious queries

Clean queries in last 24h
1,248 ↓ -92%
Clean queries

Allowed vs Blocked
Pie chart showing proportion of DNS queries that were allowed vs blocked by Pi-hole

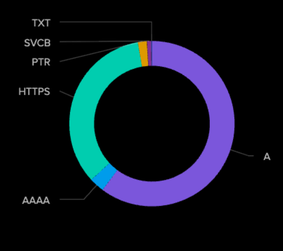


Active Clients
Pie chart showing which clients generated the most DNS queries

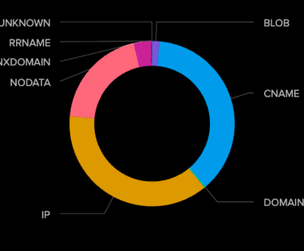


TI Statuses
Pie chart showing distribution of Malicious, Suspicious, and Clean DNS queries based on TI

Types
Pie chart showing the distribution of DNS query types

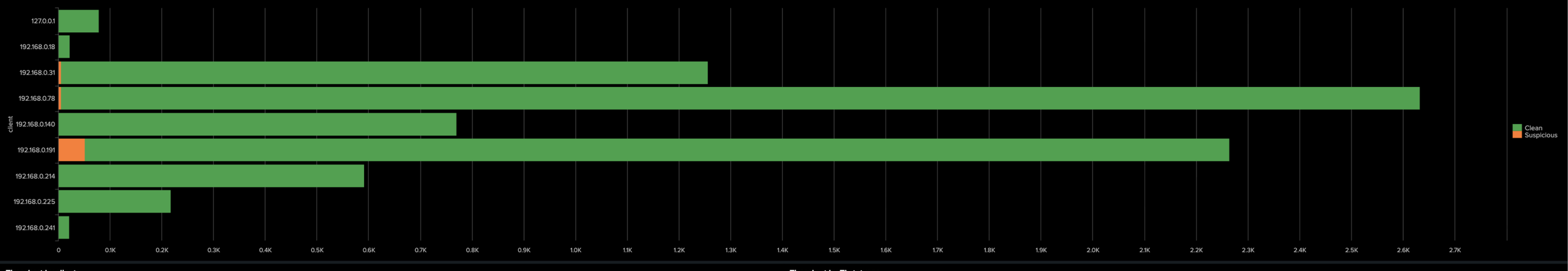


Reply Types
Pie chart representing how Pi-hole responded to DNS queries

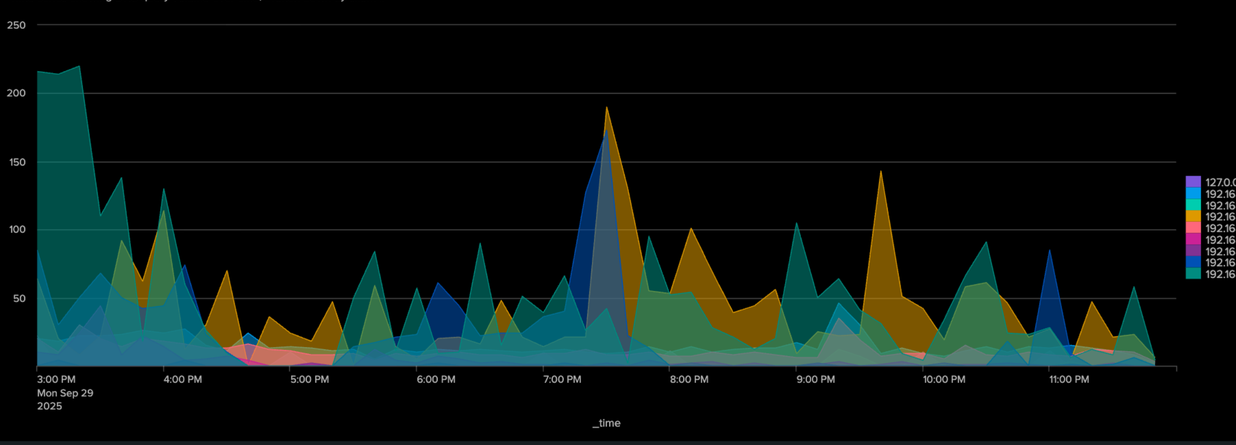


Anomaly Detection in number of DNS queries
Line chart identifying statistical anomalies in DNS query volume using a 5-minute time bin and 2 standard deviation bounds. Data points outside the upper or lower bounds are marked as anomalies. Interactive Feature: Clicking an anomaly triggers a drill-down search that displays related client and domain information for that timestamp.

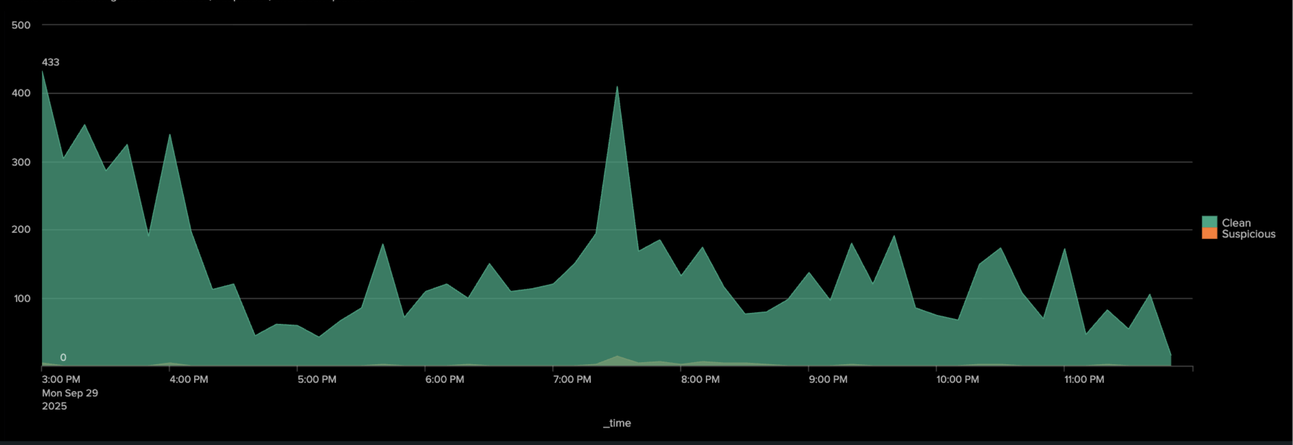
TI statuses per client
Stacked bar chart displaying how many Malicious, Suspicious, and Clean queries each client made



Timechart by clients
Time series showing DNS query volume over time, broken down by client IP



Timechart by TI statuses
Time series showing trend of Malicious, Suspicious, and Clean queries over time



Interestings domains by client
Table listing clients with the highest number of DNS queries, along with associated blocked, malicious, suspicious, and suspicious TLDs.

#	client	count	suspicious_TLDs	malicious_domains	suspicious_domains	blocked_domains
1	192.168.0.191	2264	one.top		github.com www.adsensecustomsearchads.com www.googletagmanager.com	_dns.resolver.arpa analytics.google.com api.segment.io api.sprig.com b.6sc.co bat.bing.com browser-intake-datadoghq.com cdn.bttrack.com mask-h2.icloud.com mask.icloud.com munchkin.marketo.net pagead2.googlesyndication.com snap.licdn.com static.cloudflareinsights.com stats.g.doubleclick.net tracking.intentsify.io www.adsensecustomsearchads.com www.google-analytics.com www.googletagmanager.com
2	192.168.0.78	2633	NULL		googleads.g.doubleclick.net	_dns.resolver.arpa

Prev 1 2 Next

Detailed table
Full table of DNS queries with enriched fields.

#	Time	Type	Action	Status	Client IP	Domain	Forward	Reply type	TI status	suspicious_TLD
51	2025-09-29 18:25:06	A	allowed	Replied from stale cache	192.168.0.31	cl4.g.aaplimg.com	1.0.0.1#53	IP	Clean	
52	2025-09-29 18:25:06	HTTPS	allowed	Replied from stale cache	192.168.0.31	cl4.g.aaplimg.com	1.0.0.1#53	NODATA	Clean	
53	2025-09-29 18:25:05	AAAA	allowed	Forwarded	192.168.0.191	release-assets.githubusercontent.com	1.0.0.1#53	NODATA	Clean	
54	2025-09-29 18:25:05	A	allowed	Forwarded	192.168.0.191	release-assets.githubusercontent.com	1.0.0.1#53	IP	Clean	
55	2025-09-29 18:25:04	AAAA	allowed	Forwarded	192.168.0.191	github.com	1.0.0.1#53	NODATA	Suspicious	
56	2025-09-29 18:25:04	A	allowed	Forwarded	192.168.0.191	github.com	1.0.0.1#53	IP	Suspicious	
57	2025-09-29 18:25:04	AAAA	allowed	Forwarded	192.168.0.191	ollama.com	1.0.0.1#53	NODATA	Clean	
58	2025-09-29 18:25:04	A	allowed	Forwarded	192.168.0.191	ollama.com	1.0.0.1#53	IP	Clean	
59	2025-09-29 18:24:42	A	allowed	Replied from stale cache	192.168.0.191	eu-mobile.events.data.microsoft.c	1.0.0.1#53	CNAME	Clean	

Prev 1 … 5 6 7 8 … Next

Ask AI:

Question (Only for Advise action): * | Action: Explain | Searches: Anomaly Detection in number of DNS queries | Custom search: `pihole_ftl` | Events limit: 25 | Submit

Reply from AI
Displays the AI assistant's explanation, report, or recommendation based on selected search results

Instructions

Select an action, an existing search, or select \"Custom search\" and specify your own. If the action is \"Advise\", add a question to the message for AI. Specify the event limit from 1 to 50 and click the \"Submit\" button.

Active responce:

Domain / RegEx: | Action: Block exact domain | Submit

Action: Check Pi-hole status | Minutes: 5 | Submit

Pi-hole responce
Shows API response from Pi-hole after executing block/unblock domain actions

Instructions

Enter the domain or regex and choose action. Then click Submit button to send request to Pi-hole API

Pi-hole responce
Shows API response when Pi-hole is enabled, disabled, or status is checked

Instructions

Choose action (if Disabling Pi-hole blocking, enter number of minutes). Then click Submit button to send request to Pi-hole API