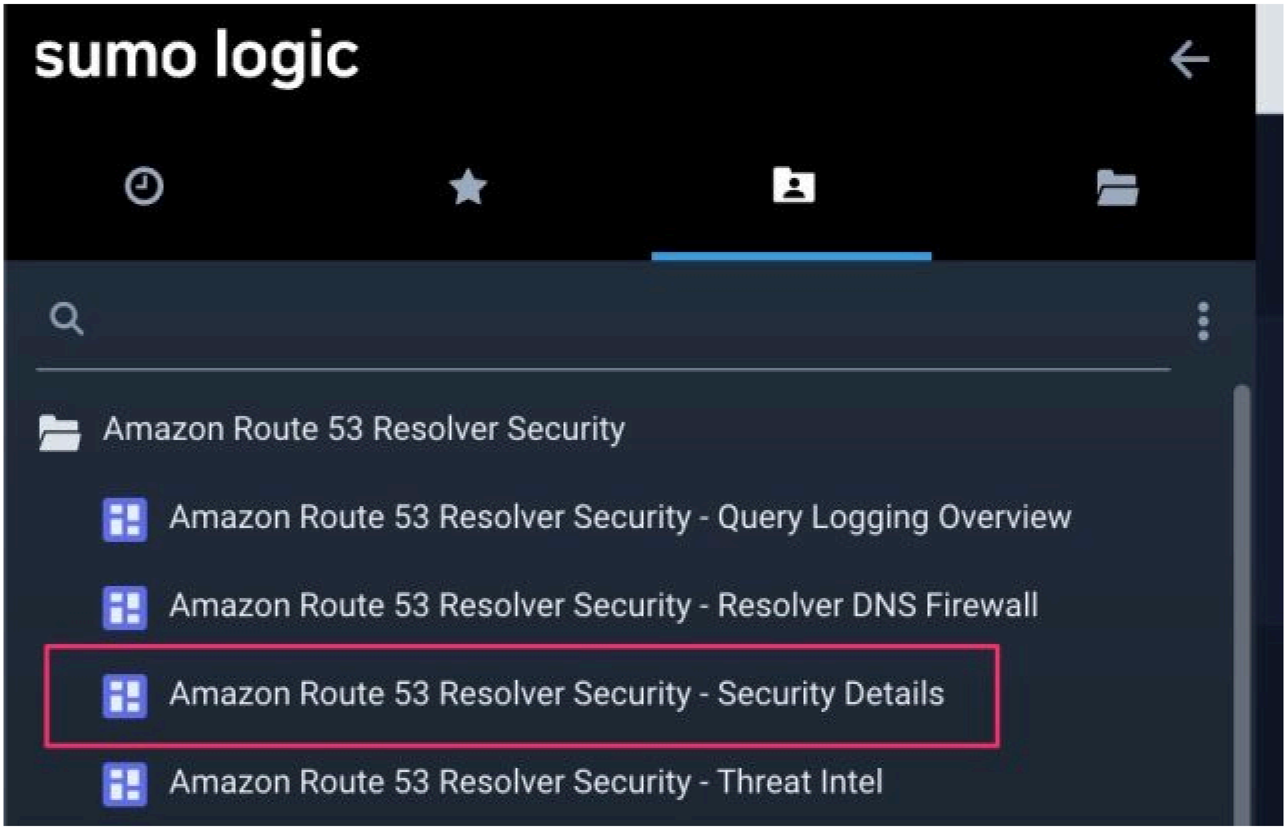
Sumo Logic で DNSクエリログ をセキュリティ分析する

dev.classmethod.jp/articles/sumo-logic-dnsquerylog-security-analysis

酒井剛

October 3, 2023


sumo logic
Amazon Route 53 Resolver Security
Amazon Route 53 Resolver Security - Query Logging Overview
Amazon Route 53 Resolver Security - Resolver DNS Firewall
Amazon Route 53 Resolver Security - Security Details
Amazon Route 53 Resolver Security - Threat Intel

DNS is an essential technology for systems to communicate over the network, and occurs at a fairly early stage of communication.
Because it occurs in almost all communications, DNS query logs are likely to be collected for security log analysis.

This time, we will collect and analyze DNS query logs using Sumo Logic, a SIEM platform.

While there are many ways to analyze security, we'd like to introduce some common areas to look at.
This time, we'll look at logs from Route53 Resolver, AWS's DNS service.
Even if you want to analyze corporate DNS logs, the analysis perspective is not much different from that of Route53 Resolver logs, so you can read the same information.

Leverage the Sumo Logic App

You can analyze Amazon Route 53 logs using Sumo Logic's pre-built dashboard (app) .

As explained below, you can install the app and create a dashboard in just a few clicks by simply setting the location of the imported logs.

Search for "Amazon Route 53 Resolver Security" in the App Catalog settings and install the app.

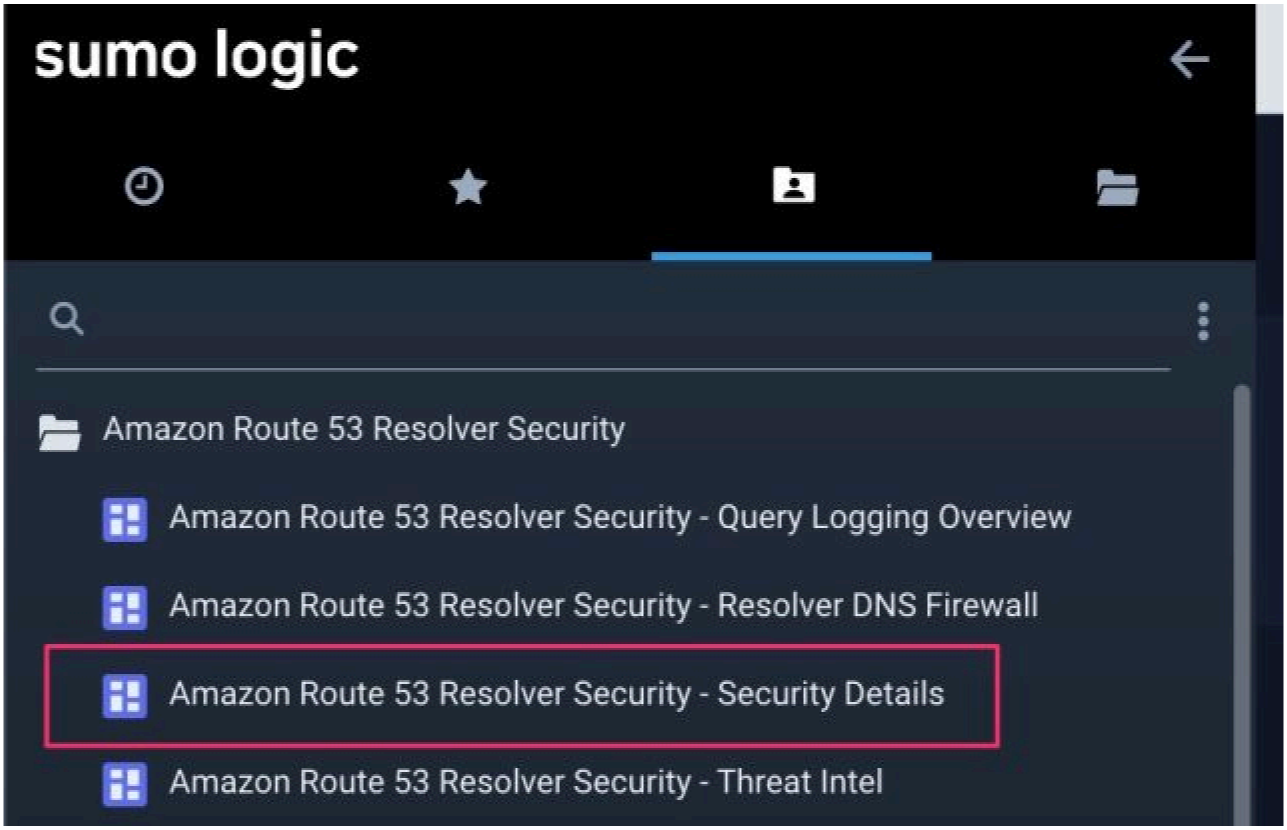
This app can visualize and analyze Route53 Resolver query logs and DNS Firewall logs .

Route53 Resolver query logs

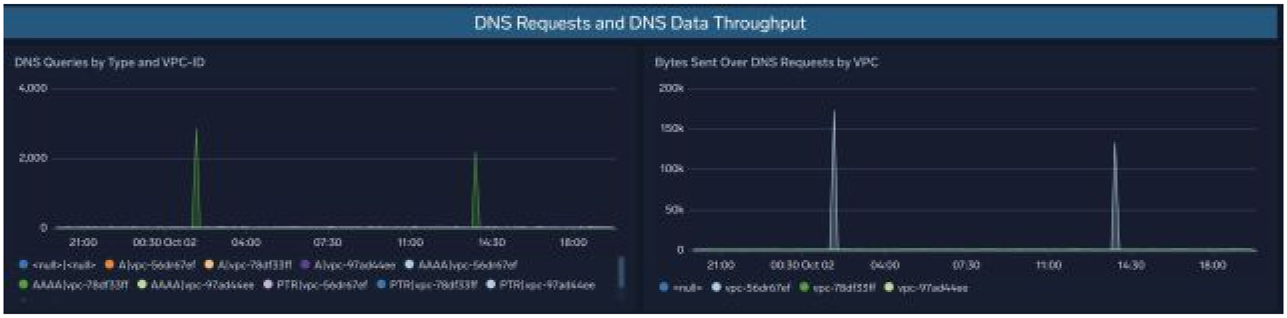
Route53 Resolver query logs are analyzed from the same perspective as general query logs such as BIND.

Amazon Route 53 Resolver Security - Security Details Dashboard

To analyze the query logs, first use the Amazon Route 53 Resolver Security - Security Details dashboard.

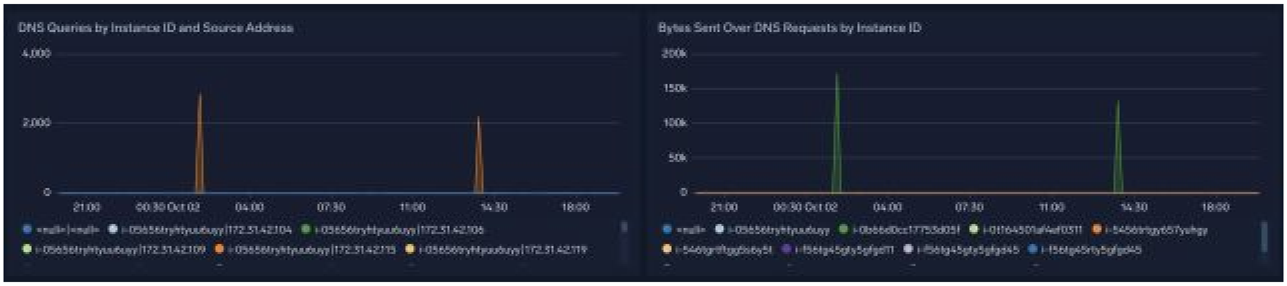

sumo logic
Amazon Route 53 Resolver Security
Amazon Route 53 Resolver Security - Query Logging Overview
Amazon Route 53 Resolver Security - Resolver DNS Firewall
Amazon Route 53 Resolver Security - Security Details
Amazon Route 53 Resolver Security - Threat Intel

It shows statistics on the number of requests by VPC ID and DNS query type (A record, AAAA record, TXT record, MX record, etc.), and the adjacent panel shows statistics on the number of bytes in DNS requests.

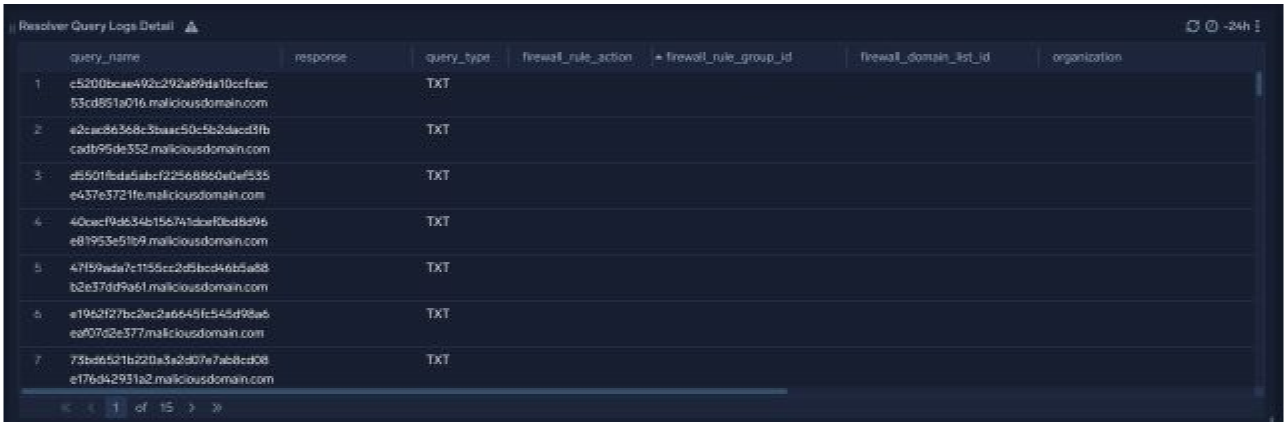


The number of bytes in DNS requests can be used to visualize whether DNS queries with suspiciously long character lengths are occurring when DNS communication with a C2 server is abused.
This security report example explains how DNS queries with abnormally long character lengths are abused, so please use it as a reference to get an idea of what to look for.

Similarly, you can check request statistics for each DNS query type based on the instance ID and source IP, allowing you to change the focus of your analysis.



Next is a table view for each query. You can see what queries are occurring and see if there are any queries worth noting.



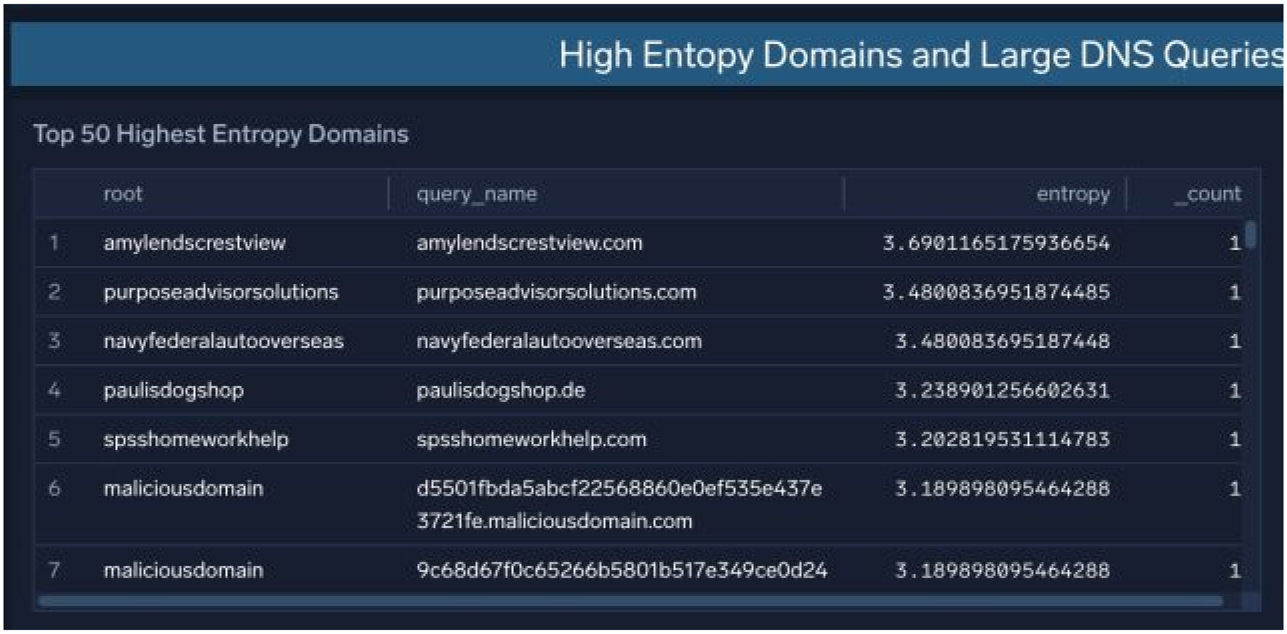
Resolver Query Logs Detail ⚠ -24h

	query_name	response	query_type	firewall_rule_action	firewall_rule_group_id	firewall_domain_list_id	organization
1	c5200bcae492c292a89da10ccfcec 53cd851a016.maliciousdomain.com		TXT				
2	e2cac86368c3baac50c5b2dacd3fb cadb95de352.maliciousdomain.com		TXT				
3	d5501fbda5abcf22568860e0ef535 e437e3721fe.maliciousdomain.com		TXT				
4	40cecf9d634b15674 1dcef0bd8d96 e81953e51b9.maliciousdomain.com		TXT				
5	47f59ada7c1155cc2d5bcd46b5a88 b2e37dd9a61.maliciousdomain.com		TXT				
6	e1962f27bc2ec2a6645fc545d98a6 eaf07d2e377.maliciousdomain.com		TXT				
7	73bd6521b220a3a2d07e7ab8cd08 e176d42931a2.maliciousdomain.com		TXT				

« ‹ 1 of 15 › »

The Top 50 Highest Entropy Domains panel allows you to analyze whether queries to highly random domains are occurring.
Security products quickly identify malicious domains and attempt to block communications to those domains, but attackers quickly switch domains to further circumvent those defenses.
Because domains must use globally unique character strings, attackers automate the

generation of domains using a domain generation algorithm called DGA (Domain Generation Algorithm). This panel allows you to analyze whether queries to such highly random domains are occurring.

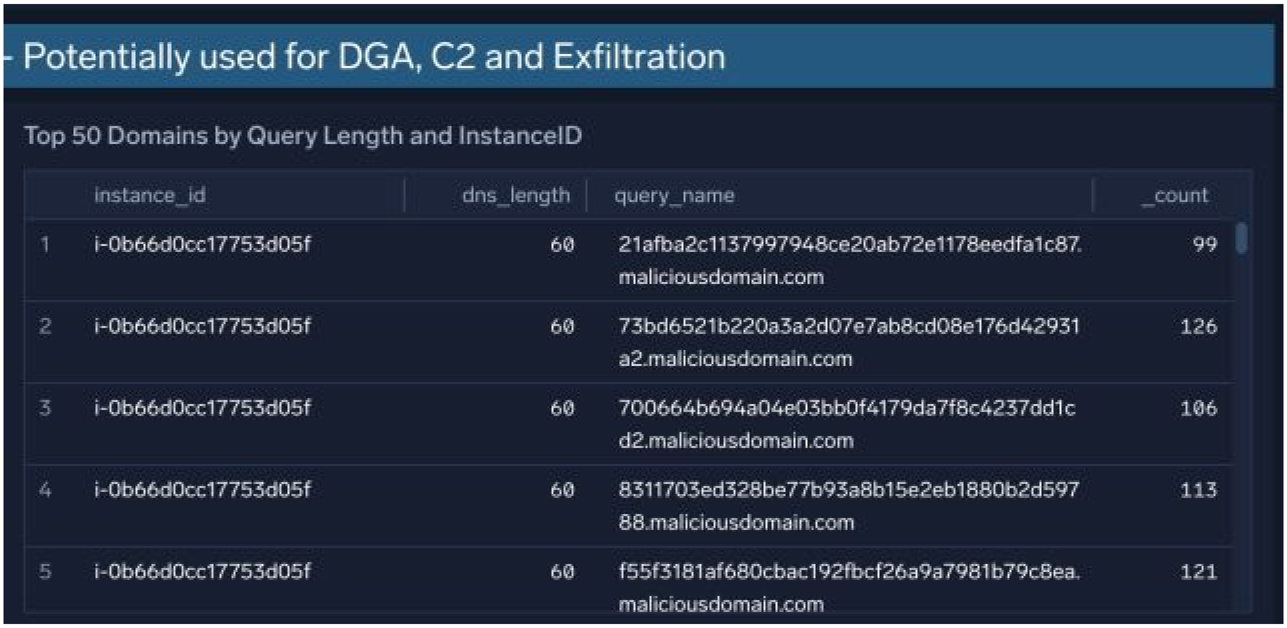


High Entopy Domains and Large DNS Queries

Top 50 Highest Entropy Domains

	root	query_name	entropy	_count
1	amylendscrestview	amylendscrestview.com	3.6901165175936654	1
2	purposeadvisorsolutions	purposeadvisorsolutions.com	3.4800836951874485	1
3	navyfederalautooverseas	navyfederalautooverseas.com	3.480083695187448	1
4	paulisdogshop	paulisdogshop.de	3.238901256602631	1
5	spsshomeworkhelp	spsshomeworkhelp.com	3.202819531114783	1
6	maliciousdomain	d5501fbda5abcf22568860e0ef535e437e3721fe.maliciousdomain.com	3.189898095464288	1
7	maliciousdomain	9c68d67f0c65266b5801b517e349ce0d24	3.189898095464288	1

The Top 50 Domains by Query Length and InstanceID panel is similar to the previous panel in that it checks for DNS queries with unusually long lengths or meaningless strings of alphanumeric characters that may contain encoded information.

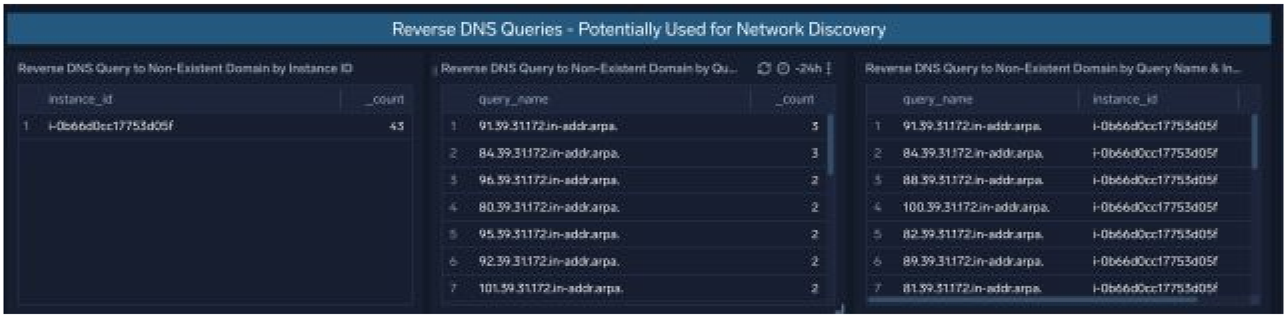


- Potentially used for DGA, C2 and Exfiltration

Top 50 Domains by Query Length and InstanceID

	instance_id	dns_length	query_name	_count
1	i-0b66d0cc17753d05f	60	21afba2c1137997948ce20ab72e1178eedfa1c87.maliciousdomain.com	99
2	i-0b66d0cc17753d05f	60	73bd6521b220a3a2d07e7ab8cd08e176d42931a2.maliciousdomain.com	126
3	i-0b66d0cc17753d05f	60	700664b694a04e03bb0f4179da7f8c4237dd1cd2.maliciousdomain.com	106
4	i-0b66d0cc17753d05f	60	8311703ed328be77b93a8b15e2eb1880b2d59788.maliciousdomain.com	113
5	i-0b66d0cc17753d05f	60	f55f3181af680cbac192fbcf26a9a7981b79c8ea.maliciousdomain.com	121

The Reverse DNS Query to Non-Existent Domain by ... panel analyzes instances of non-existent reverse lookups (searching for a domain from an IP address). Reverse lookups are sometimes used (see references) , such as in mail servers, where the server is configured to not accept email delivery unless a reverse lookup is possible. However, they can also be used for network discovery, so use these panels to check for suspicious communications.



Reverse DNS Queries - Potentially Used for Network Discovery

Reverse DNS Query to Non-Existent Domain by Instance ID

	instance_id	_count
1	i-0b66d0cc17753d05f	43

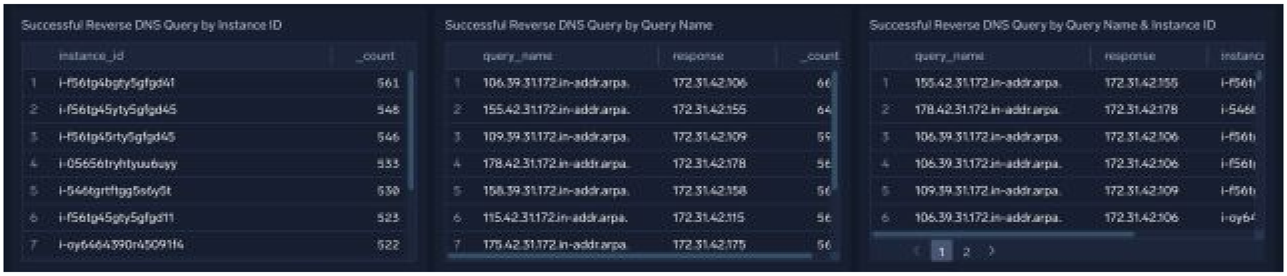
Reverse DNS Query to Non-Existent Domain by Qu...

	query_name	_count
1	91.39.31.172.in-addr.arpa.	3
2	84.39.31.172.in-addr.arpa.	3
3	96.39.31.172.in-addr.arpa.	2
4	80.39.31.172.in-addr.arpa.	2
5	95.39.31.172.in-addr.arpa.	2
6	92.39.31.172.in-addr.arpa.	2
7	101.39.31.172.in-addr.arpa.	2

Reverse DNS Query to Non-Existent Domain by Query Name & In...

	query_name	instance_id
1	91.39.31.172.in-addr.arpa.	i-0b66d0cc17753d05f
2	84.39.31.172.in-addr.arpa.	i-0b66d0cc17753d05f
3	88.39.31.172.in-addr.arpa.	i-0b66d0cc17753d05f
4	100.39.31.172.in-addr.arpa.	i-0b66d0cc17753d05f
5	82.39.31.172.in-addr.arpa.	i-0b66d0cc17753d05f
6	89.39.31.172.in-addr.arpa.	i-0b66d0cc17753d05f
7	81.39.31.172.in-addr.arpa.	i-0b66d0cc17753d05f

The Successful Reverse DNS Query by... panel analyzes reverse lookup queries to existing domains.
It analyzes whether reverse lookups should be performed, their frequency, and whether there was any attacker activity such as network reconnaissance.



Successful Reverse DNS Query by Instance ID

	instance_id	_count
1	i-f56tg4bgty5gfgd41	561
2	i-f56tg45yty5gfgd45	548
3	i-f56tg45rty5gfgd45	546
4	i-05656tryhtyuu6uyy	533
5	i-546tgrtftgg5s6y5t	530
6	i-f56tg45gty5gfgd11	523
7	i-oy6464390n45091f4	522

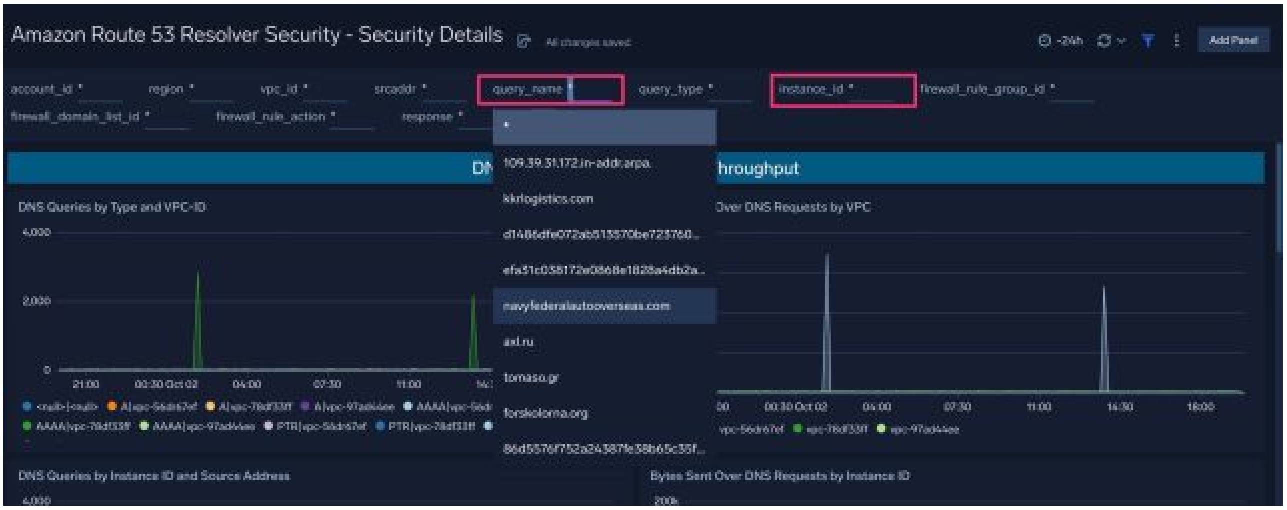
Successful Reverse DNS Query by Query Name

	query_name	response	_count
1	106.39.31.172.in-addr.arpa.	172.31.42.106	66
2	155.42.31.172.in-addr.arpa.	172.31.42.155	64
3	109.39.31.172.in-addr.arpa.	172.31.42.109	59
4	178.42.31.172.in-addr.arpa.	172.31.42.178	56
5	158.39.31.172.in-addr.arpa.	172.31.42.158	56
6	115.42.31.172.in-addr.arpa.	172.31.42.115	56
7	175.42.31.172.in-addr.arpa.	172.31.42.175	56

Successful Reverse DNS Query by Query Name & Instance ID

	query_name	response	instance
1	155.42.31.172.in-addr.arpa.	172.31.42.155	i-f56t
2	178.42.31.172.in-addr.arpa.	172.31.42.178	i-546t
3	106.39.31.172.in-addr.arpa.	172.31.42.106	i-f56t
4	106.39.31.172.in-addr.arpa.	172.31.42.106	i-f56t
5	109.39.31.172.in-addr.arpa.	172.31.42.109	i-f56t
6	106.39.31.172.in-addr.arpa.	172.31.42.106	i-oy64

Also, returning to the top of the dashboard, you can use filters to narrow down these panels to what you want to see most effectively.
Correlating information visible from logs of other systems is especially important for correlation analysis performed with SIEM.
For example, if you find access logs to a suspicious URL in proxy logs, you can narrow down your search by using a specific query name filter in DNS query logs. Once you 've identified the instance, you can filter by instance ID and correlate it to gain the security insights we've discussed so far.



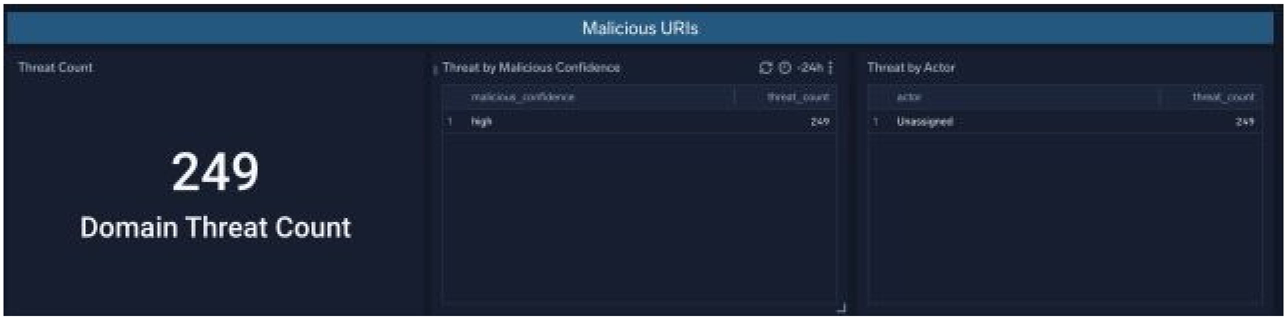
Amazon Route 53 Resolver Security - Security Details

account_id *
region *
vpc_id *
srcaddr *
query_name *
query_type *
instance_id *
firewall_rule_group_id *
firewall_domain_list_id *
firewall_rule_action *
response *

Amazon Route 53 Resolver Security - Threat Intel Dashboard

The "Amazon Route 53 Resolver Security - Threat Intel" dashboard allows you to compare CrowdStrike threat intelligence with DNS query logs to determine whether domains and IP addresses have been used by attackers in the past.

The number of times a domain has been queried for a threat determination. This shows the credibility of the threat and the attacker group identified by CrowdStrike.



Malicious URIs

Threat Count

249

Domain Threat Count

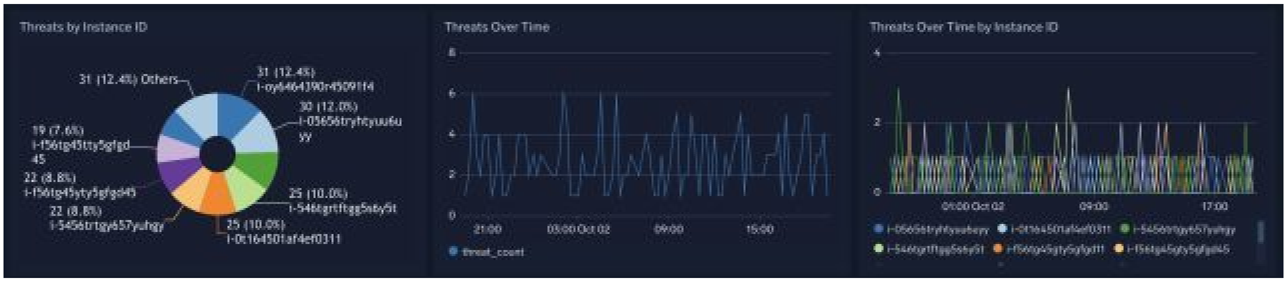
Threat by Malicious Confidence

	malicious_confidence	threat_count
1	high	249

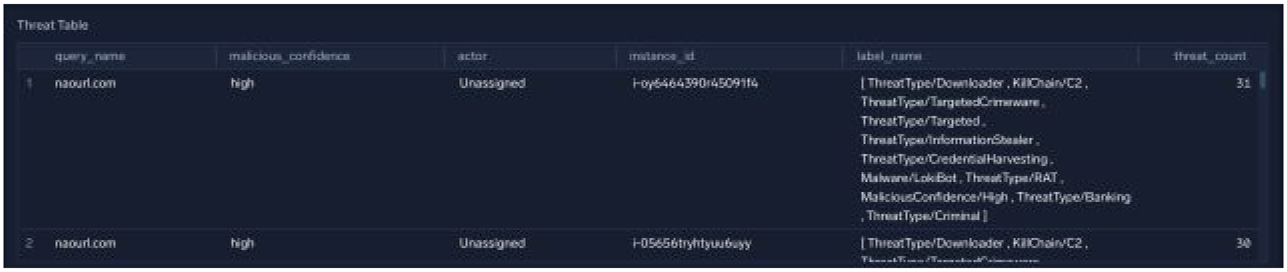
Threat by Actor

	actor	threat_count
1	Unassigned	249

You can analyze instances where DNS queries were judged to be threats, as well as statistics over time.



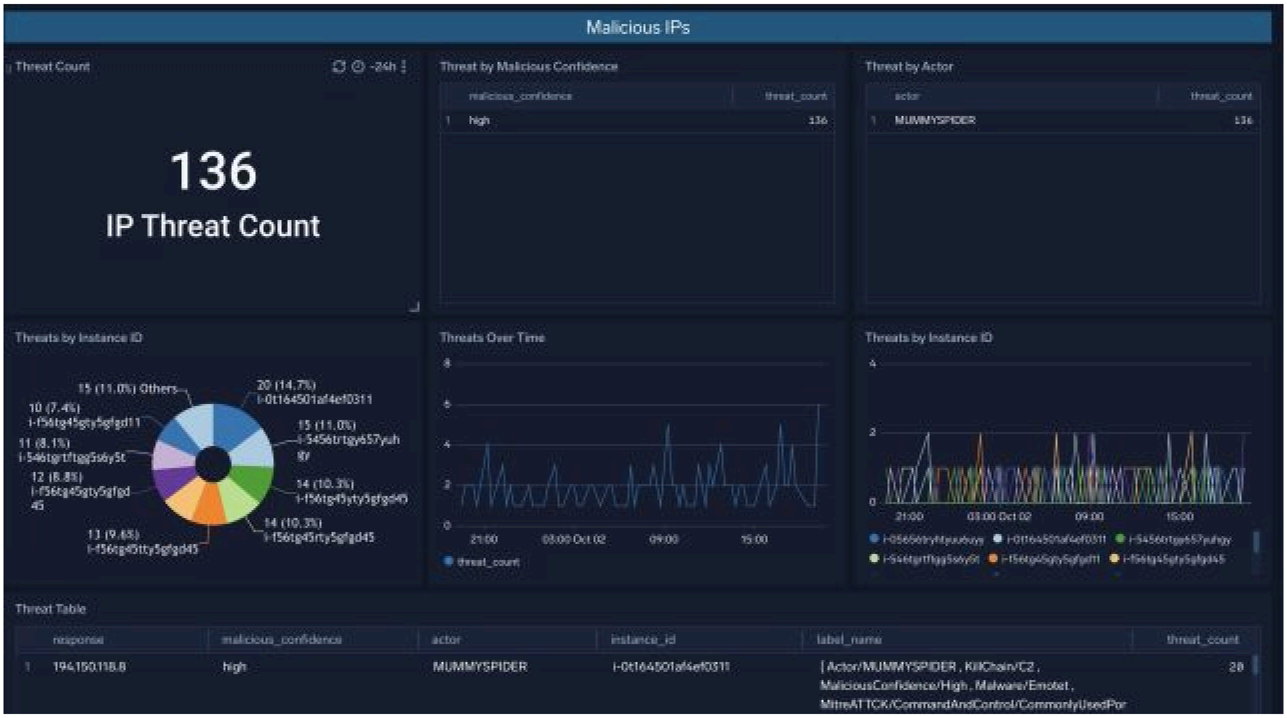
You can see the details in table format.



Threat Table

	query_name	malicious_confidence	actor	instance_id	label_name	threat_count
1	naourl.com	high	Unassigned	i-oy6464390r45091f4	[ThreatType/Downloader , KillChain/C2 , ThreatType/TargetedCrimeware , ThreatType/Targeted , ThreatType/InformationStealer , ThreatType/CredentialHarvesting , Malware/LokiBot , ThreatType/RAT , MaliciousConfidence/High , ThreatType/Banking , ThreatType/Criminal]	31
2	naourl.com	high	Unassigned	i-05656tryhtyuu6uyy	[ThreatType/Downloader , KillChain/C2 ,	30

This is the analysis result obtained by matching the IP addresses included in the DNS queries with CrowdStrike's threat intelligence. It can be analyzed from the same perspective as above.



Malicious IPs

Threat Count

136

IP Threat Count

Threat by Malicious Confidence

	malicious_confidence	threat_count
1	high	136

Threat by Actor

	actor	threat_count
1	MUMMYSPIDER	136

Threat Table

	response	malicious_confidence	actor	instance_id	label_name	threat_count
1	194.150.118.8	high	MUMMYSPIDER	i-0t164501af4ef0311	[Actor/MUMMYSPIDER , KillChain/C2 , MaliciousConfidence/High , Malware/Emotet , MitreATTCK/CommandAndControl/CommonlyUsedPor	28

This example is for a demo environment, so the results displayed are of many threats, but for normal operation, it is best to set up alerts so that you can immediately check any results that are displayed.

When you want to analyze DNS query logs such as BIND on-premises

At the time of writing, Sumo Logic does not seem to have a pre-built dashboard (app) for on-premises DNS query logs.
You can use the analysis perspective of the app "Amazon Route 53 Resolver Security" introduced here, so you can create a similar dashboard by copying the query from this dashboard and slightly modifying the data source and parsing.

summary

By importing DNS query logs into a SIEM product and visualizing them, it seems possible to continuously analyze normal conditions and determine what is abnormal.
Because there are many attacks that exploit DNS, we recommend analyzing DNS query logs using SIEM.