Securedns Categoryget

Endpoints Summary

Method	Path	Swagger
`GET`	`/securedns_categoryget/`	Swagger ↗

> The SecureDNS Category API provides functionality to retrieve category information for SecureDNS transactions using their unique identifiers. This endpoint is essential for understanding the classification of DNS security events and can be integrated into security monitoring workflows, reporting systems, and compliance auditing processes.

Base URL: `https://control.zequenze.com/api/v1`

Authentication: All endpoints require a Bearer token:

```
Authorization: Bearer <your-api-token>
```

Overview

The SecureDNS Category API enables developers to query the categorization of SecureDNS transactions by providing a UUID-based lookup mechanism. This API is particularly valuable for security operations teams who need to understand the nature and classification of DNS security events that have been processed through the SecureDNS system.

Key Features:

- **Transaction Classification**: Retrieve detailed category information for specific SecureDNS transactions
- **UUID-based Lookups**: Use unique transaction identifiers to get precise categorization data
- **Security Integration**: Perfect for SIEM integration, security dashboards, and compliance reporting

- **Real-time Insights**: Access category data for immediate security decision-making

Common Integration Scenarios:

- Security Information and Event Management (SIEM) systems pulling DNS security classifications
- Automated incident response workflows that need to categorize DNS-related security events
- Compliance reporting systems that track DNS security categories for audit purposes
- Security dashboards displaying real-time DNS threat categorization
- Forensic analysis tools examining historical DNS security transactions

The category information returned by this API helps organizations understand the types of DNS security events they're experiencing, enabling better threat intelligence and more informed security decisions.

Endpoints

GET /securedns_categoryget/

Description: Retrieves the category classification for a specific SecureDNS transaction using its UUID. This endpoint is essential for understanding what type of DNS security event occurred, enabling security teams to properly categorize, respond to, and report on DNS-related security incidents.

Use Cases:

- SIEM systems automatically categorizing DNS security alerts for proper incident handling
- Security analysts investigating specific DNS security transactions during incident response
- Compliance reporting systems that need to classify DNS security events by category
- Automated security workflows that trigger different responses based on DNS transaction categories
- Security dashboards displaying categorized DNS threat intelligence

Full URL Example:

```
https://control.zequenze.com/api/v1/securedns_categoryget/?uuid=550e8400-e29b-41d4-a716-446655440000
```

Parameters:

Parameter	Type	In	Required	Description
uuid	string	query	Yes	The unique identifier of the SecureDNS transaction to retrieve category information for

cURL Example:

```
curl -X GET "https://control.zequenze.com/api/v1/securedns_categoryget/?uuid=550e8400-e29b-41d4-a716-446655440000" \
  -H "Authorization: Bearer YOUR_API_TOKEN" \
  -H "Content-Type: application/json"
```

Example Response:

```
[
  {
    "category": "malware"
  }
]
```

Response Codes:

Status	Description
200	Category request Ok - Returns the category information for the specified transaction
401	Category request not authorized - Invalid or missing authentication token
403	Category request forbidden / not allowed - Valid authentication but insufficient permissions
404	Provided UUID don't match any transaction - The specified UUID does not exist in the system

---

Common Use Cases

Use Case 1: SIEM Integration for DNS Security Monitoring

Security operations centers integrate this API into their SIEM platforms to automatically categorize DNS security events. When a SecureDNS transaction is flagged, the SIEM system uses the transaction UUID to retrieve the category, enabling automated rule-based responses and proper incident classification.

Use Case 2: Incident Response Investigation

During security incident investigations, analysts use this endpoint to quickly understand the nature of DNS-related security events. By querying transaction UUIDs from security logs, investigators can rapidly categorize threats and determine appropriate response procedures.

Use Case 3: Compliance Reporting and Auditing

Organizations use this API to generate compliance reports that categorize DNS security events. The category information helps demonstrate security monitoring effectiveness and provides detailed classifications required for various regulatory frameworks.

Use Case 4: Automated Threat Response Workflows

Security automation platforms integrate this endpoint to create dynamic response workflows. Different DNS security categories trigger different automated responses, from simple logging for low-risk categories to immediate blocking and alerting for high-risk classifications.

Use Case 5: Security Dashboard Visualization

Security dashboards use this API to display real-time categorized DNS threat intelligence, helping security teams visualize the types and distribution of DNS security events across their organization.

Best Practices

- **UUID Validation**: Always validate UUID format before making API calls to avoid unnecessary 404 responses and reduce API usage
- **Error Handling**: Implement comprehensive error handling for all response codes, especially 404 responses when UUIDs don't match any transactions
- **Caching Strategy**: Consider caching category responses for frequently queried UUIDs to improve performance and reduce API calls
- **Batch Processing**: When processing multiple transactions, implement appropriate rate limiting and consider batching requests to avoid overwhelming the API

- **Security Considerations**: Store and transmit UUIDs securely as they may contain sensitive information about your organization's DNS security events
- **Monitoring Integration**: Log all API interactions for audit purposes and to track usage patterns in your security monitoring workflows
- **Fallback Mechanisms**: Implement fallback procedures when the API is unavailable to ensure critical security operations can continue

---

Revision #4
Created 2026-02-04 05:11:28 UTC by ipena@zequenze.com
Updated 2026-02-11 03:09:04 UTC by ipena@zequenze.com