DNSCyte is a recursive DNS Service based on global cyber threat intelligence and machine learning to block threats and targeted attacks in real-time.

DNSCyte

Today's threats are evolving at an exponential rate with new methods for distribution, infection, infiltration and evasion. These new techniques are continually overcoming traditional cyber defences. Famous attacks such as WannaCry, Not-Petya were based on eternal blue. They evaded pattern and signature-based security solutions relying on DNS to communicate to external command and control servers. With DNSCyte such attacks can be stopped.

The Internet is becoming ubiquitous, and we live in a hyper-connected world. DNSCyte has indexed 99.9% of the Internet, which includes more than 1.7 billion web sites and 350 million top-level domains growing daily. With this intelligence, DNSCyte can protect global businesses and users.

DNSCyte can block zero-day attacks and identify malicious activity. DNSCyte handles the DNS requests from users and redirects malicious requests to a sinkhole providing a new layer of security with artificial
Intelligence.

Classification Within Seconds

- DNSCyte machine learning technology enables the classification of unknown traffic in seconds.

DNS Tunnelling Discovery

- Discovery of DNS tunnelling is now easy with DNSCyte.

Malicious Activity Prevention

- Protect your network against ransomware, malware, phishing, and botnet threats. Stop malicious activity before it starts communication.

Whitelisting for Internet

- Only permit categorised Internet traffic to enable strong protection for zero-day attacks.

Analysis of DNS Debug Logs

- Identify the source of malicious traffic by enabling the automatic analysis of internal DNS Server logs.

Cloud Based Realtime Reporting

- Get real-time visibility and centralised reporting without any on-premise component.

Digital Forensics

- In depth digital forensics for users, devices and processes by supporting Inline and out of band operation support.

Product Benefits

Stop Zero-Day attacks.

Pre & Post infection protection.

Define and enforce Internet usage policy.

The categorisation of Internet traffic.

Machine learning-based automatic classification engine.

DNSCyte at a Glance

- **VISIBILITY**

Monitor and control Internet access for your entire organisation.

- **PROTECTION**

Enable secure Internet browsing. Block malicious activity and zero day attacks even when users are off the premises.

- **AUTOMATION**

User behaviour analysis integrated to DNS baselining with machine learning and artificial intelligence for automated classification and blocking.

- **COMPLIANCE**

Enforce corporate compliance to acceptable use policy and enabler for external regulations.

- **RETURN ON INVESTMENT & TCO**

Frictionless access, self-service and self-enrolment increasing business productivity.

How It Works?

Deploy in minutes without making any change to your physical infrastructure. Simply enable DNS Forwarding or DNS Relay.

DNS Forwarding

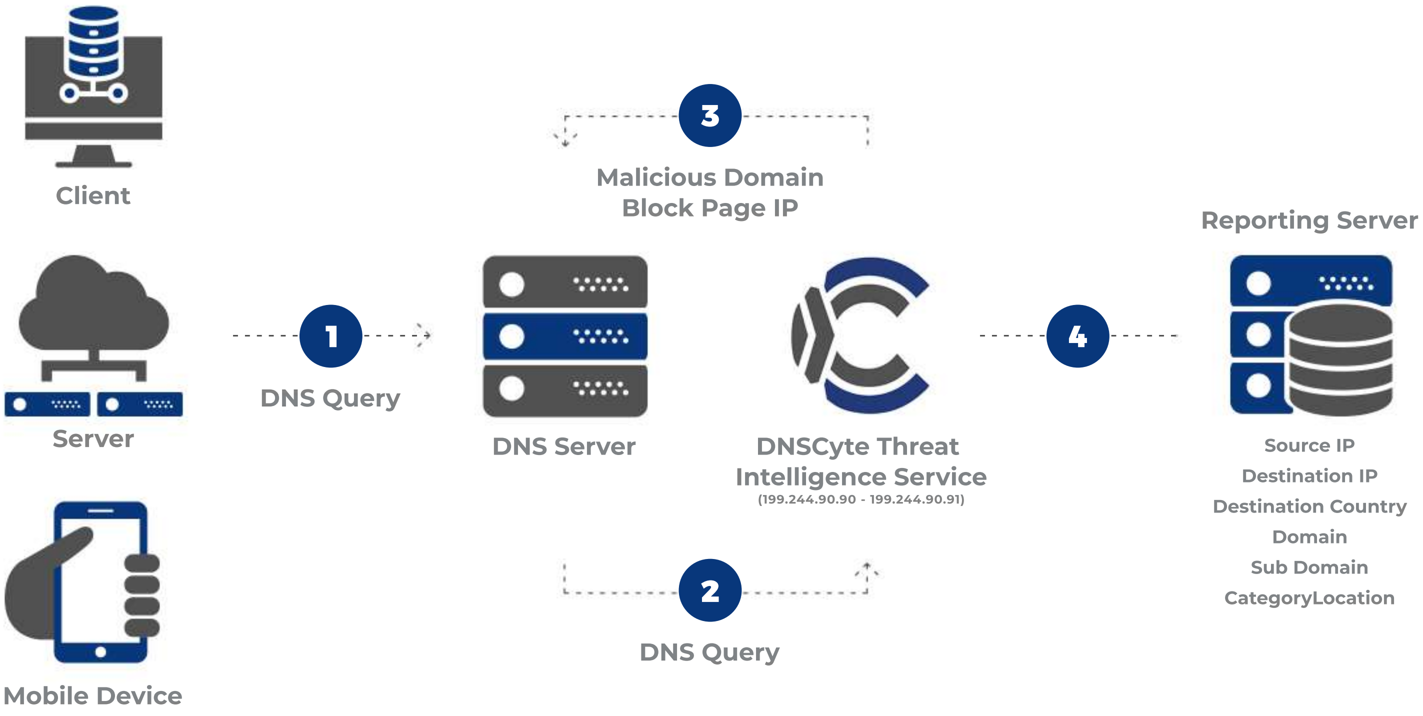
The DNSCyte Forwarding service handles all DNS requests for identification and categorisation of Internet traffic. DNSCyte redirects malicious requests to a preferred sinkhole IP Address. This enables malicious traffic to be redirected away from the internal network to a controlled destination for remediation.

1. **Every device and user accessing the Internet sends a DNS query to the DNSCyte DNS Server.**
2. **DNSCyte DNS Server forwards the request to the DNSCyte Threat Intelligence Service.**
3. **If the resolved domain is classified as malicious, the user is redirected to a secure web page for notification or access to the page is blocked.**
4. **The request history can be stored in an Elastic big data platform for detailed logging and reporting.**

✓ **Configure devices in the network to use DNSCyte DNS Servers.**

✓ **DNSCyte should be defined as the forwarder DNS on the local DNS Service if a local DNS server is active.**

✓ **When using a public DNS Service, configure the DNSCyte IP Addresses as the DNS Server**



Hardware Requirements

There is no hardware requirement for this mode of operation.

DNS Relay & Integration With Local DNS Server Platforms

DNSCyte DNS Relay is a VMWARE/Hyper-V based image provided to discover the source of malicious traffic. DNS relay is a DNS Server installed on the corporate network. This component receives DNS queries before the local DNS Server and forwards them Server after the analysis.

1. **DNSCyte on-premise module enables the analysis of DNS logs from domain name controllers, or other DNS Server's.**
2. **The system forwards the request to the DNSCyte Threat Intelligence Service for classification and security check.**
3. **The response coming from DNSCyte Threat Intelligence Service is used to permit or deny access.**
4. **The system can send the response to a SIEM with customized fields in Syslog format.**

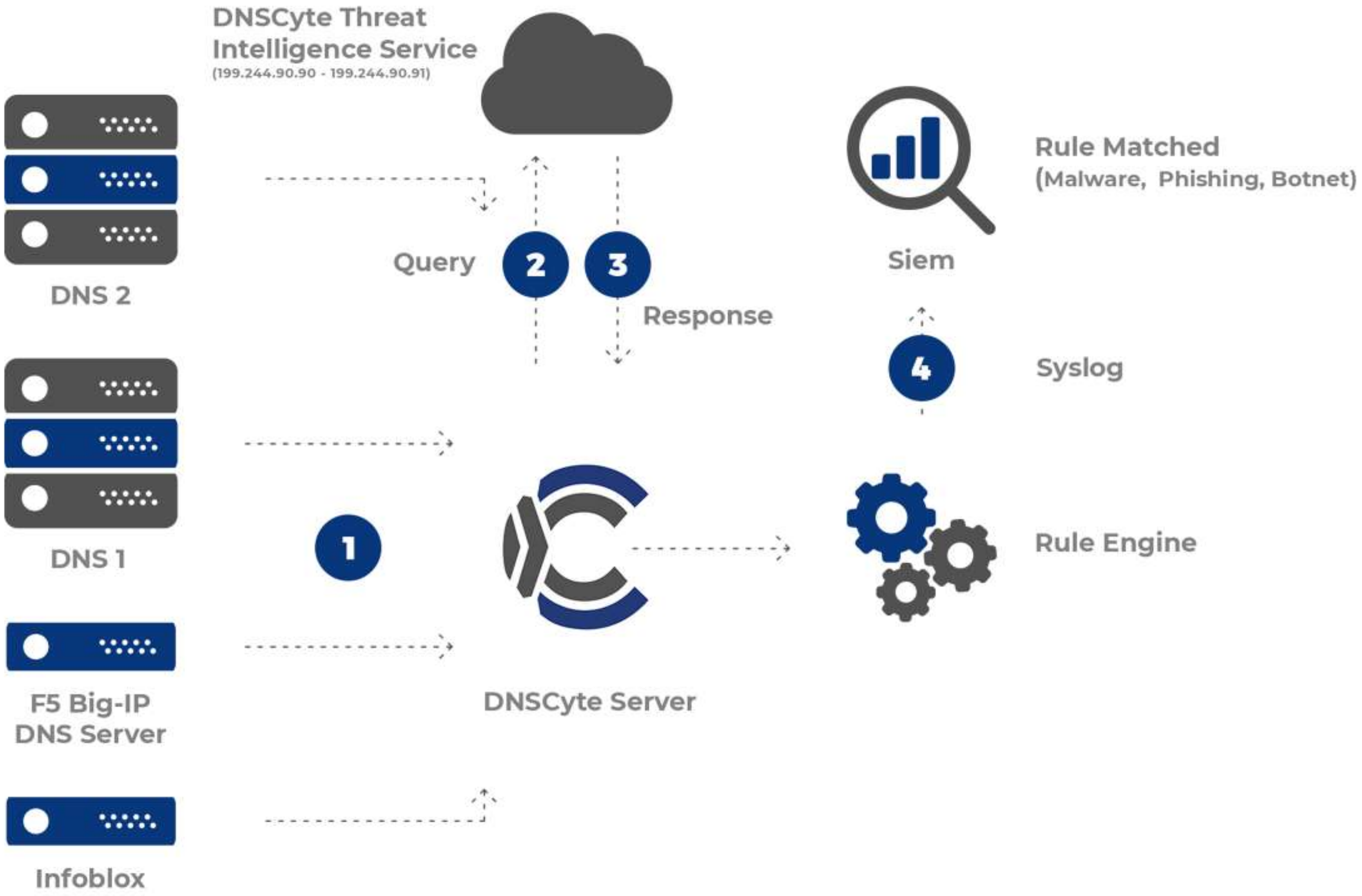
DNSCyte can also integrate with the following platforms in identifying the source of malicious traffic without relaying the DNS traffic:

- → **Windows DNS**
- → **Microsoft Active Directory**
- → **OpenDNS**
- → **F5**
- → **Infoblox**

Hardware Requirements*

A virtualised appliance with VMWARE ESX or Microsoft Hyper-V with 12 virtual cores, 24 GB RAM and 250 GB HDD for up to 10,000 users.

**Hardware required only if an on-premise DNS Server integration is required.*



About CyberCyte

CyberCyte is a UK based cyber security company that provides a framework of solutions based on Circle of Zero Trust. This includes identity management, network access control, and DNS security. Used by enterprises, governments and service providers around the World to protect their users and secure digital assets.

Davidson House, Kings Road Reading UK RG1 4EU
+44 118 900 1422
www.cybercyte.com