

SOLUTION BRIEF

INFOBLOX THREAT DEFENSE™ DETECTION MODE

SUMMARY

Leverage Infoblox's deep expertise in DNS intelligence to proactively detect threats.

Infoblox Threat Defense™ Detection Mode uses Infoblox Threat Intel feeds, algorithmic detections and brand protection capabilities with out-of-band query metadata/response field analysis (not live queries) to detect malicious activity such as ransomware, command and control (C2), high-risk/suspicious domains, data exfiltration, domain generation algorithms (DGAs) and more. Detected security events can then be sent as alerts to security information and event management (SIEM)/security orchestration, automation and response (SOAR) or a messaging app, for security operations center (SOC) teams to investigate and respond.

OVERVIEW & CHALLENGES

Traditional security approaches used to protect networks are reactive, relying on malware-based detection to identify threats only after they have been activated. As modern malware evolves rapidly, threat actors leverage AI to generate new variants that evade conventional security tools, making it increasingly difficult to keep up. This almost always results in patient zero and breaches. DNS is also used by threat actors for C2, data exfiltration, ransomware, zero day and phishing campaigns, and existing security tools don't monitor DNS.

Closing this gap requires preemptive threat detection to identify malicious domains before they are weaponized with malware. By monitoring DNS metadata/response fields (not live queries) associated with high-risk, attacker-controlled domains, Threat Defense helps organizations identify attacks before they start, significantly reducing the risk of ransomware, C2 activity, phishing and data exfiltration without changing DNS resolution paths.

INFOBLOX THREAT DEFENSE DETECTION MODE

Infoblox Threat Defense Detection Mode applies Infoblox's deep threat intelligence and DNS query-response metadata/response field analysis (not live queries) to provide comprehensive threat detection. It identifies malicious activity such as ransomware, phishing, C2, high-risk or suspicious domains, data exfiltration and DGAs—all without changing existing DNS resolution paths. Threat Defense Detection Mode ingests out-of-band DNS query/response metadata from supported sources (e.g., NIOS and Microsoft DNS) and analyzes it in the cloud. It then reports discovered threats and forwards alerts to existing tools for investigation and remediation. For NIOS, Detection Mode can run via DNS Forwarding Proxy (DFP) on most current NIOS versions. Microsoft DNS support uses DNS Analytic Events (not Debug Logs). A lightweight PowerShell script is deployed on each Microsoft DNS server

KEY CAPABILITIES

- Out-of-band detection (no DNS path changes, no added latency)
- Sources: NIOS or Microsoft DNS (DNS Analytic Events)
- True client IP attribution, including native Microsoft DNS client IP visibility
- SOC ready: Send detections and context to SIEM/SOAR and ticketing tools
- Side by side comparison with existing inline tools (evaluate missed threats)
- Automatic filtering of internal/authoritative domains (external focus only)

where the DNS Server role is installed. This script communicates with the Infoblox Windows Agent on a Windows Event Collector (WEC) server to collect DNS Analytic ETL files and forward normalized query-metadata events securely to the Infoblox portal.

Ecosystem integrations can then be used to send security events/alerts to SIEM/SOAR, Slack, Teams or a wide range of other messaging or ticketing apps.

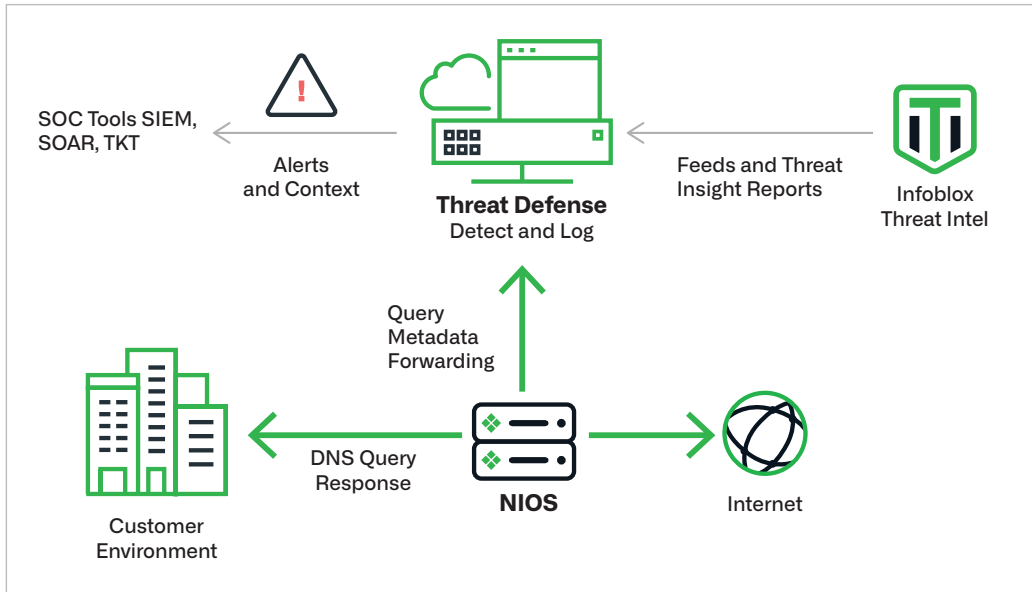


Figure 1. Threat Defense Detection Mode using Infoblox NIOS appliance to forward the query metadata to Threat Defense

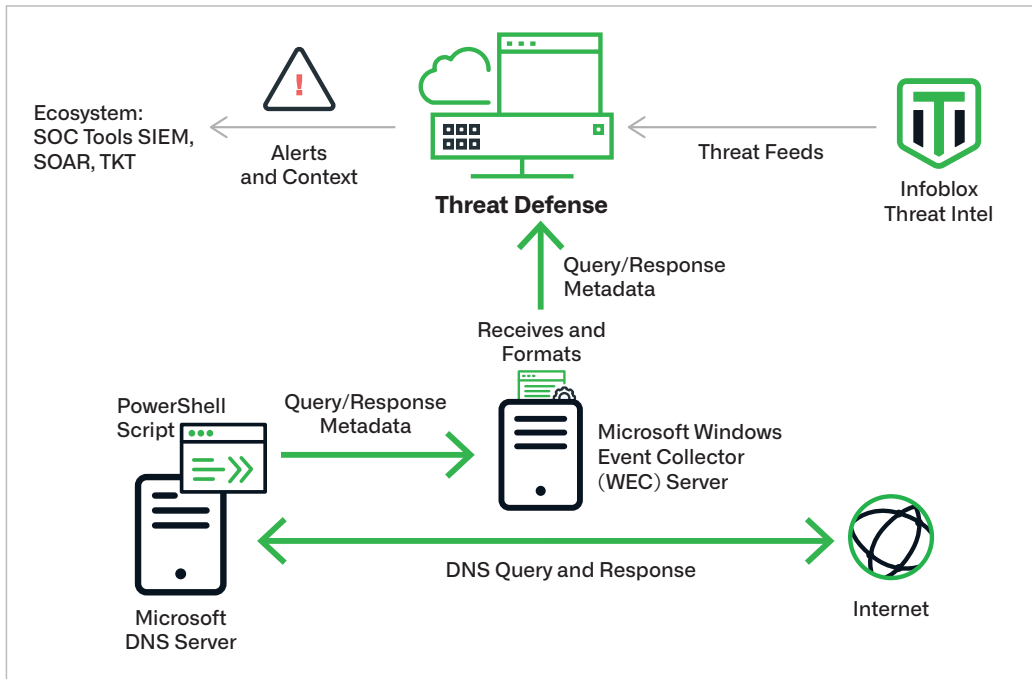


Figure 2. Threat Defense Detection Mode using Microsoft DNS to send DNS Analytic Events to the Infoblox Agent which sends query metadata to Threat Defense

BENEFITS OF DETECTION MODE

Infoblox Detects DNS Threats without Changing Resolution

Full detection capabilities are enabled out-of-band (no DNS path changes, no redirect of external queries, no added resolution latency) without needing to rearchitect resolution or point on-prem resolution to the cloud, simplifying approvals and implementation.

Use Existing Infoblox Equipment and Architecture

Use existing NIOS (DFP-based Detection Mode) or Microsoft DNS (DNS Analytic Events + Infoblox Windows Agent on a WEC server) to enable detection of threats without changing or updating resolver configuration, and to preserve true client IP attribution via Microsoft DNS ingestion for investigation and compliance with emerging protective DNS guidance.

Security Awareness and Alignment

Ensure security teams see DNS-layer risk and understand impact, driving SecOps buy-in and budget alignment beyond NetOps.