DNSSight
with HYAS inside

USE CASE

Empowering an International Telecom Giant with DNS Visibility

Turning Complex Network Architecture into a Launchpad for Enhanced Threat Detection and Rapid Response

BACKGROUND

A Global Telecom and a Massive Network

An international telecom company operates across multiple continents, managing a labyrinth of network segments and endpoints accumulated over years of mergers, expansions, and upgrades. Swapping out existing DNS servers or reconfiguring the entire network isn't just daunting **—it's nearly impossible without incurring astronomical costs and operational disruptions.**

Still, the company's SOC lacked a consolidated view of DNS traffic. Whenever a security event demanded deeper scrutiny, the team spent countless hours piecing together firewall logs, device logs, and local DNS records in an attempt to reconstruct a single suspicious connection.

The amount of data was staggering; correlating timestamps and packet details felt more like an archaeological dig than a streamlined process.

That all changed when the telecom deployed DNSSight.

Suddenly, previously hidden DNS insights were at their fingertips, elevating the effectiveness of existing security tools and supercharging ROI on infrastructure investments.

CHALLENGE

COMPLEX NETWORK TOPOLOGY

Legacy & Growth

After years of organic expansion and acquisitions, the telecom's network spanned numerous sites and architectures. Adapting or replacing core components posed prohibitive costs and risks to uptime.

Distributed Devices

Thousands of endpoints, routers, and servers scattered across multiple regions complicated any centralised approach to DNS security.

LIMITED DNS VISIBILITY

Manual Correlation

Identifying malicious behaviour required cross-referencing timestamps between firewall logs, DNS queries, and other devices. It was tedious, error-prone, and time-intensive.

Scalability Struggles

Given the sheer volume of DNS records, manual correlation often lagged behind real-time threats, undermining proactive defence.

UNDERUTILISED SIEM INVESTMENT

Data Overload

The telecom had a powerful SIEM in place, but critical DNS intelligence never made it into the system—choking the SOC's ability to spot suspicious patterns quickly.

Operational Gaps

Security analysts spent more time searching for missing data than acting on potential threats, reducing the efficiency of their existing solutions.

SOLUTION

DNSSight for Unified, Real-Time DNS Layer Protection

☐ SEAMLESS INTEGRATION WITH EXISTING ARCHITECTURE

No Forklift Upgrades

DNSSight overlays the telecom's existing DNS ecosystem, gathering logs from DNS, DHCP, and AIM solutions in real time. No complex re-architecture required.

Immediate ROI

By preserving hardware and network configurations, DNSSight unlocks DNS visibility without adding hidden costs or requiring prolonged migrations.

☐ AUTOMATIC DNS ENRICHMENT AND CORRELATION

Real-Time User and Device Data

Every DNS query is instantly matched with the user, machine, and timestamp—removing guesswork or manual hunting.

SOC-Ready Intelligence

High-risk activities, anomalous device behaviours, or newly flagged domains trigger automated alerts sent directly to the existing SIEM, speeding investigation and response.

☐ GRANULAR CONTROL AND INSIGHTS

Flexible Filters

DNSSight allows the SOC team to set up targeted views—focusing, for instance, on newly discovered malicious domains or high-value servers.

Comprehensive Visibility

Instead of searching logs, analysts can visualise who accessed what domain, when

RESULTS

Drastically Reduced Investigation Times

The SOC now resolves DNS-related incidents in minutes rather than hours, thanks to automated correlation and a centralised dashboard.

Analysts can quickly pinpoint the user behind suspicious DNS requests without wading through mountains of disconnected logs.

Enhanced ROI on SIEM and Infrastructure

DNSSight's enriched DNS data feeds directly into the telecom's SIEM, empowering existing threat-hunting workflows with high-fidelity intelligence.

By leveraging the current network and security tools, the telecom maximises value on investments already made in hardware, software, and personnel.

Expanded Threat Detection Capabilities

Identifying malicious domains—even if the domains are short-lived or offline—gives the SOC early indicators of potential breaches.

Complex anomalies, such as sudden changes in a critical server's DNS patterns, are flagged immediately, facilitating a proactive threat posture.

Non-Disruptive Adoption

The telecom avoided the business impact of a major infrastructure overhaul, meaning zero downtime for their global customer base.

With DNSSight's intuitive portal, analysts simply fine-tune filters and rules—"lifting a finger" just enough to harness a new frontier of network intelligence.

CONCLUSION

For an international telecom giant grappling with a sprawling network, **DNSSight delivers a game-changing level of DNS visibility** without any disruptive replacements or radical infrastructure changes. By transforming cryptic DNS queries into actionable intelligence, the SOC team gains a new battlefront in the fight against cyber threats—one they can dominate with minimal effort.

> Combining automated correlation, rich data insights, and frictionless integration, **DNSSight elevates the telecom's security operations to new heights.**
>
> With this solution in place, **the enterprise can expand its global footprint confidently,** knowing that every DNS request—no matter how small—can be traced, understood, and tackled head-on.