DNSSight

USE CASE

Enhancing Threat Visibility & Response

© 2025 DNSSight. All rights reserved.

Equip financial institutions to spot and stop cybersecurity threats fast by delivering crystal-clear visibility into the sources of malicious DNS queries **—transforming uncertainty into action and risk into resolution.**

In a bustling finance hub, a leading bank struggled with a recurring problem: ***the inability to rapidly pinpoint which internal user or device was generating malicious DNS queries.***

They had a robust DNS security solution in place—one that effectively blocked suspect traffic—but the bank's security operations team still wrestled with hours of **manual correlation, searching across DHCP logs, firewall records, and AD user data.** Finding the source of malware communication felt like a treasure hunt with half the map missing.

The institution deploys, DNSSight. An on-premise DNS visibility and enrichment platform that gave the bank a profound change in perspective. DNSSight delivered both clarity and actionable intelligence.

© 2025 DNSSight. All rights reserved.

CHALLENGE

Malware Communication

Despite the bank's existing DNS security tools blocking many malicious queries, underlying infections would still ping out to suspicious domains.

The security team knew something was amiss but had difficulty tracing it to an exact device or user.

Visibility Gaps

Relying on timestamps in firewall logs was time-consuming, and the local DNS server only captured local IP addresses.

Once machines moved or addresses got reassigned, the security team's trail would run cold.

Limited ROI

Although the bank's SIEM system and DNS security solution were robust, the team expended too much effort stitching logs together by hand.

They needed automation and deeper insight to maximise return on their existing investments.

SOLUTION

Comprehensive Data Correlation

DNSSight automatically ingests and correlates DHCP, Active Directory, and DNS logs in real time, matching each DNS query to the relevant user and device MAC address.

This immediate enrichment ensures no more blind hunts across disjointed data sources.

High-Value Insights

DNSSight goes beyond standard logging by presenting enhanced statistics and alerts.

It offers metrics such as Top 10 Users generating potentially harmful traffic, an Extra Eye on priority systems, and historical trends that map out infection footprints before incidents spiral out of control.

Seamless SIEM Integration

DNSSight integrates seamlessly with the bank's SIEM solution.

Critical events and intelligence are forwarded automatically, enabling the Security Operations Centre (SOC) to zero in on the right machines at the right time—sharply reducing the window where adversaries can linger undetected.

© 2025 DNSSight. All rights reserved.

RESULTS

Pinpoint Identification

The bank's SOC team can now locate infected endpoints in seconds rather than hours.

No more sifting through mountains of firewall logs or wrestling with ephemeral IP addresses.

Mitigation Agility

Targeted response is fast and surgical.

By instantly knowing the user and device at fault, the bank can cut off harmful processes or quarantine compromised systems in near real time.

Enhanced ROI

DNSSight acts as a force multiplier, providing deeper returns on the bank's existing DNS security and SIEM investments.

With more time spent on strategic threat analysis—and less time chasing logs—the bank's security resources deliver superior value.

Streamlined Operations

Automated log correlation and enriched visibility create a calmer, more decisive Security Operations Centre.

When minutes count, clarity is invaluable.

CONCLUSION

In the high-stakes environment of modern banking, DNSSight empowers institutions to wield unmatched precision in detecting and containing DNS-based threats.

By fusing **advanced analytics, user-level detail, and streamlined SIEM integration,** DNSSight gives security teams the confidence and agility to respond to malicious DNS communications at a moment's notice **—no detective work necessary.**

With DNSSight, this leading bank is not just another firm hoping to thwart cyber-attacks; it's a fortress prepared to counter them head-on, optimising existing defences and making the most of every security pound spent. That's the power of unwavering visibility—when guided by an approach that masterfully blends persuasive influence with strategic insight.

© 2025 DNSSight. All rights reserved.