INFOBLOX SOC INSIGHTS: ENABLING HIGHER LEVELS OF SECURITY THROUGH DNS

EXECUTIVE SUMMARY

Security professionals face growing complexities created by multi-cloud and hybrid OT and IT infrastructure deployments. A highly disaggregated architectural approach leveraging cloud scale has proven advantages in accelerating digital transformation through gains in operational agility and flexibility. However, it also introduces many challenges – the most glaring one being a dramatically expanded threat surface that must be defended. The heterogeneous nature of cloud networking architectures also contributes to poor observability among clouds. Consequently, enterprises must embrace new security operational models that can provide higher levels of visibility to keep pace with an ever-increasing threat landscape perpetuated by bad actors that hope to leverage AI to their advantage.

Surprisingly, domain name system (DNS) is not widely utilized as a cybersecurity platform construct, but it should be. DNS is a fundamental element of network communications, serving a critical, platform agnostic function in translating domain names into IP addresses. Given the ongoing convergence of networking and security, DNS can provide valuable insights into domains that could potentially be weaponized. Infoblox recognized the value of DNS more than two decades ago, and positioned DNS to deliver new capabilities that thwart attacks, safeguard critical enterprise infrastructure and the underlying data.

Moor Insights & Strategy believes that Infoblox SOC Insights, a feature of the company's BloxOne Threat Defense solution, offers organizations of all sizes the ability to enable higher levels of security through the power of DNS. It is a complete solution, one that infuses AI to provide actionable, real-time insights, reduces mean time to incident response, mitigates downtime, and offers an additional layer of protection ensuring higher levels of business continuity.

SOC CHALLENGES

The modern security operations center (SOC) must find ways to do more with fewer resources. There continues to be a shortage of highly trained and experienced cybersecurity professionals globally. As a result, SOC analysts carry heavy workloads, often managing an intimidating amount of telemetry, alerts, signals, and cybersecurity tools. Limited visibility, manual tasks, and the generation of false positives is also compounding the challenges of managing an effective defense posture. SOC teams desperately need new ways to lower and ideally eliminate these burdens to facilitate smoother security operational models. Infoblox SOC Insights is well-suited to help address these challenges.

WHY INFOBLOX

Infoblox recently announced a new AI-infused security capability rooted in a DNS architectural approach. The solution, SOC Insights, aims to improve visibility and streamline operations to help enterprise SOC teams manage the onslaught of cybersecurity threats.

The centerpiece of the company’s cybersecurity offering continues to be BloxOne Threat Defense. Now, SOC Insights extends its capabilities as a holistic, DNS-anchored detection and response platform. Many enterprise security infrastructure providers claim that their solutions are unique, but in this case, Moor Insights & Strategy believes that Infoblox takes a unique approach to network security. Specifically, SOC Insights provides:

- ***An AI-powered SecOps capability*** that distills and analyzes the ongoing flow of threat and network data to provide actionable insights for security analysts while dramatically reducing alert fatigue.
- ***A new way to leverage the power of DNS*** to greatly reduce threat mean-time-to-respond (MTTR)***.*** This creates compelling benefits in terms of mitigating business downtime, improving security posture, and enabling a proactive versus reactive cybersecurity operational framework.
- ***The ability for organizations to reduce downtime and improve security efficacy*** by using unique DNS threat intelligence.
- ***An additional layer of protection*** realized through the cross-pollination of Infoblox AI-driven insights with other SOC security stack tools, and automated remediation capabilities facilitated through triggered API calls.

By applying AI to vast amounts of DNS and network data, Infoblox SOC Insights can provide security teams with valuable proactive threat disruption guidance, insightful analytics, and added value to other existing security tool investments. Infoblox, like many other security solution providers, is fighting AI with AI, but the difference is that the company is using it as part of a DNS defensive infrastructure to effectively thwart the growing sophistication of attacks fueled by the generative AI “gold rush.” Moor Insights & Strategy believes that Infoblox SOC Insights is yet another example of how the company is raising the bar for proactive security defense through the visibility and telemetry provided by DNS.

CALL TO ACTION

The modern SOC is under constant pressure in its defense of critical IT and OT resources, applications, and data. New approaches are required to meet the challenges that are faced by security analysts. Harnessing DNS data by using Infoblox security infrastructure can help organizations improve security posture and provide proactive approaches to prevent breaches. In doing so, enterprises can realize significant improvements in threat visibility, while also shortening time to remediation for breaches that do occur. Bad actors are becoming more sophisticated in attacks, leveraging AI to their advantage. Infoblox SOC Insights has the potential to allow defenders to stay one step ahead of attackers—even against those that use AI to perpetuate malicious activity.

Furthermore, more organizations utilize the IT distribution channel to secure cybersecurity infrastructure, while taking advantage of managed service offerings and integration services. From a route to market perspective, Infoblox is providing its channel partners and security solution providers with a new tool in SOC Insights to help organizations optimize existing security investments, streamline security operations, and ultimately drive better business outcomes. This effort has the potential to unlock incremental monetization opportunities for Infoblox partners, further the company’s sales momentum in a crowded security marketplace, and provide enterprises with an additional layer of protection and business resiliency. That is a win-win by all measures for Infoblox, its partners, and its customers.

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTOR

Will Townsend, Vice President & Principal Analyst, Networking & Security Practices at Moor Insights & Strategy

PUBLISHER

Patrick Moorhead, Founder, President, & Chief Analyst at Moor Insights & Strategy

INQUIRIES

Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

This document, including any supporting materials, is owned by Moor Insights & Strategy. This publication may not be reproduced, distributed, or shared in any form without Moor Insights & Strategy's prior written permission.

DISCLOSURES

Infoblox commissioned this paper. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.