SOLUTION NOTE

INCREASE SOC PRODUCTIVITY WITH REAL-TIME SECURITY ALERTS ON SLACK

Automatically send Slack messages containing correlated and prioritized DNS-based security data

Today's security landscape is complex and ever-evolving. Cybercriminals are increasingly targeting DNS infrastructure to launch sophisticated attacks, such as phishing campaigns, malware distribution, and data exfiltration. Security analysts are under immense pressure to identify and respond to these threats in a timely manner and do not have the bandwidth to proactively monitor and search the multiple applications they are responsible for. This "swivel-chair" routine is highly inefficient and amplifies the need to communicate and collaborate on a single, familiar tool, speeding up both mean time to detect (MTTD) and mean time to respond (MTTR). For companies that have embraced the power of Slack, Infoblox has developed a certified integration designed to provide immediate, prioritized security notifications directly on Slack, allowing for quick SOC decision-making and action.

CHALLENGES

Security teams face numerous challenges in today's complicated threat landscape:

- **Alert Overload:** Security analysts are inundated with constant alerts from various security tools, making identifying and prioritizing the most critical threats difficult.
- **Limited Visibility:** Traditional security solutions often lack the ability to easily analyze the context and scope of threats and determine next steps.
- **Inefficient Workflows:** Investigating threats often requires jumping between different security tools, wasting valuable time and effort.

QUICK TIME-TO-VALUE THROUGH EASY INTEGRATION: INFOBLOX + SLACK

Infoblox's DNS Detection and Response (DNSDR) solution, BloxOne Threat Defense, enhanced with SOC Insights, automatically mines massive amounts of DNS Threat Intel and asset data to correlate and prioritize actionable responses to threats. The solution turns vast amounts of event, network, ecosystem, and DNS intelligence data into actionable insights to elevate SecOps efficiency. The rich security data generated by BloxOne Threat Defense with SOC Insights removes blind spots and increases the ability to fully understand DNS-based attacks.

To further elevate overall SOC efficiency, Infoblox offers a low-code integration into Slack that can uplift the benefits of each solution, reducing the total cost of ownership. This powerful combination streamlines threat detection and response capabilities, providing security teams with immediate notifications of the critical insights needed to protect your organization.

KEY BENEFITS

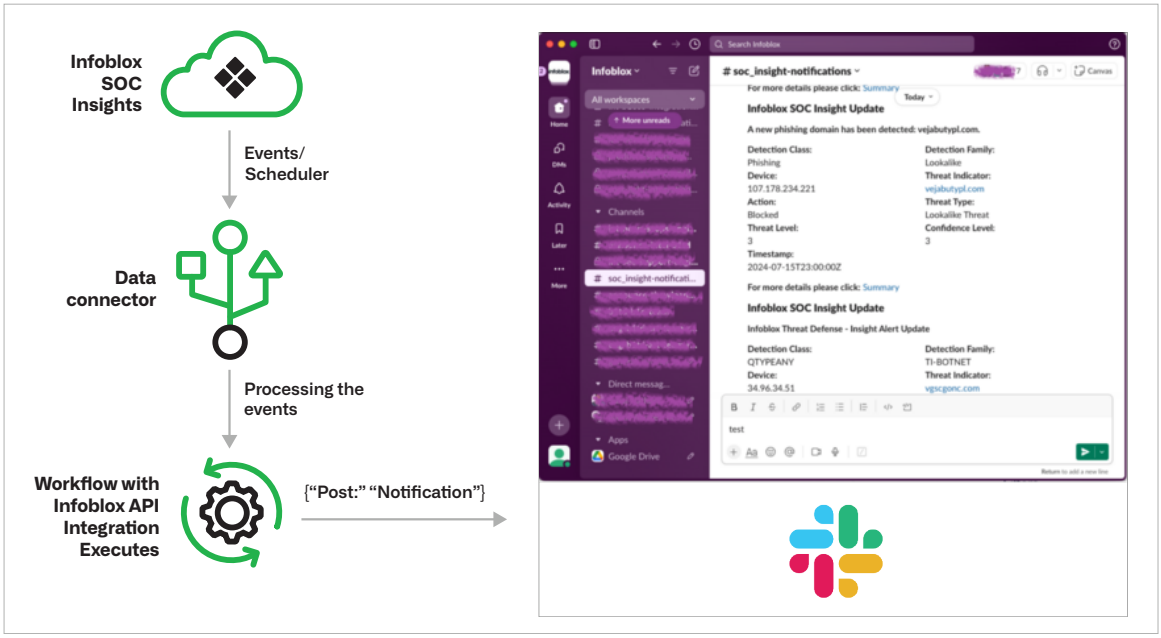
- **Centralized Communication and Collaboration:** Automatically get notified of prioritized security alerts directly within Slack and reduce the need for manual monitoring of multiple tools.
- **Accelerated Response:** Speed up incident response with direct access to threat context and details to quickly determine next steps.
- **Reduced Alert Fatigue:** Get notified of only the critical threats, reducing the noise and burden on security analysts.
- **Maximized ROI:** Amplify the value of your Slack investment by streamlining security workflows and reducing app switching.

Infoblox + Slack empowers security teams to:

- **Unify Threat Alerts:** Infoblox triggers real-time Slack messages informing security analysts of prioritized threats, immediately removing the need for manual, multi-tool monitoring tasks. Alerts are sent to a customized Slack channel providing analysts with centralized alert management, including historical documentation and tracking.
- **Simplify Investigations:** The Infoblox-driven Slack messages provide visibility into the critical content and context needed to triage and collaborate on the next steps. Simply click on the link provided in the message to be brought directly into the Infoblox Portal for further investigation.
- **Take Decisive Action:** Armed with the appropriate content and context Infoblox provides, security analysts can respond efficiently and effectively to the threats that matter most and update the status in the message thread in Slack to keep the team informed.

By implementing Infoblox for Slack, security teams can transform their security posture by gaining a centralized view of critical alerts, streamlining investigations, and accelerating their response to threats.

HOW IT WORKS



SUPERIOR SOC PERFORMANCE WITH THE INFOBLOX AND SLACK INTEGRATION

Integrating Infoblox with Slack provides a collaborative security solution that enhances your existing infrastructure. This synergy ensures:

- **SOC Efficiency:** Maintain optimal performance by immediately sending prioritized threat alerts to a centralized Slack channel. This enhances communication while providing historical tracking.
- **SOC Effectiveness:** Empower security analysts with threat content and context directly within the Slack message alert to take quick, appropriate action.
- **Operational Productivity/ROI:** Streamlining workflows and reducing app switching can improve the efficiency of your SecOps team, leading to time and cost savings.
- **Integration Simplicity:** Easy, tested, and certified low-code integration speeds up time to value.

CONCLUSION

Automating security workloads, reducing detection and response times, and maintaining effective threat response communications and collaboration are significant challenges for SecOps teams. The integration of Infoblox with Slack messaging enhances the value of your entire security stack by providing a unified platform for enriched threat intelligence communications. This combination boosts SecOps productivity, improves efficiency, and ensures a more robust and responsive security program. By leveraging Infoblox for Slack, you elevate your organization's security capabilities and maximize the return on your security investments.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240724v1