SOLUTION NOTE

ENRICH YOUR QRADAR SIEM WITH INFOBLOX DDI AND BLOXONE THREAT DEFENSE

See more from your IBM Security QRadar with unparalleled DNS visibility from Infoblox

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. However, traditional Security Information and Event Management (SIEM) solutions often lack the depth of integration with DNS security data needed for effective investigation and response.

CHALLENGES

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

- **Alert Overload:** Security analysts are inundated with a constant stream of alerts from various security tools, making it difficult to identify and prioritize the most critical threats.
- **Limited Visibility:** Traditional SIEM solutions often lack the ability to capture and analyze the rich security data generated by Infoblox DDI infrastructure and BloxOne Threat Defense. This creates blind spots and hinders the ability to fully understand DNS-based attacks.
- **Inefficient Workflows:** Investigating threats often requires jumping between different security tools, wasting valuable time and effort.

QUICK TIME-TO-VALUE THROUGH EASY INTEGRATION

Infoblox, the leader in DNS, DHCP and IP Address Management (DDI) and DNS Security, together with IBM Security QRadar, a leading SIEM and SOAR provider, offer easy integration that can uplift the capabilities of each solution and elevate overall SecOps efficiency. This powerful combination enhances threat detection and response capabilities, providing your security team with the critical insights needed to protect your organization more effectively.

This powerful combination empowers security teams to:

- **Simplify Investigations:** Streamline your security workflows by leveraging pre-built dashboards and user actions within QRadar. These features provide quick access to critical information about DNS activity, threat intelligence, and contextual network data, reducing the time it takes to investigate and respond to incidents.
- **Unify Threat Intelligence:** Gain a comprehensive view of your network activity by correlating Infoblox data, such as DNS events, DHCP leases, audit logs, and threat intelligence feeds, with other security events collected by QRadar. This holistic view enables analysts to identify and understand the full scope of potential threats.

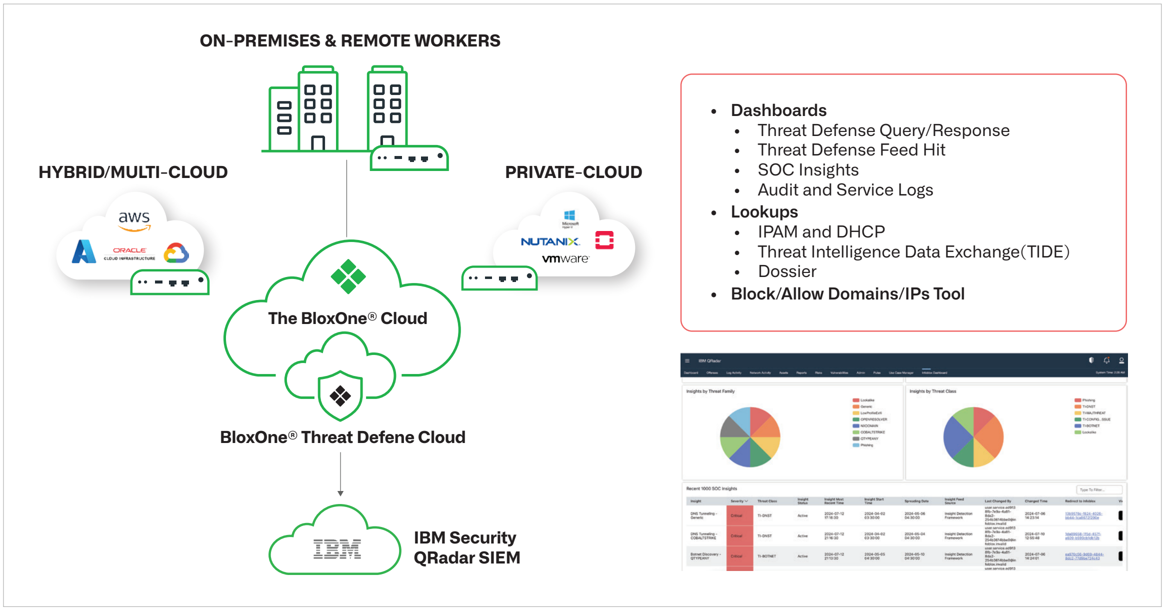
KEY BENEFITS

- **Enhanced Visibility:** Gain deep insights into your network's DNS, DHCP, and IPAM activities, ensuring comprehensive network visibility.
- **Accelerated Response:** Speed up incident response with direct access to Infoblox's threat intelligence and contextual data within QRadar.
- **Reduced Alert Fatigue:** Focus on critical threats by filtering out non-essential alerts, reducing the burden on your security analysts.
- **Maximized ROI:** Amplify the value of your QRadar investment by leveraging advanced threat intelligence from Infoblox.

- **Take Decisive Action:** Empower your security analysts with the ability to take immediate action against threats directly from QRadar. The Infoblox App allows for blocking malicious domains and IPs with a single click, minimizing the potential damage caused by an attack.

By implementing the Infoblox App for QRadar, security teams can transform their security posture by gaining a centralized view of network activity, streamlining investigations, and accelerating their response to threats.

KEY CAPABILITIES



App Configuration

- **Seamless Configuration:** Easy setup within QRadar to connect with Infoblox's advanced security services.

Dashboards

- **DNS Events Overview:** Offers a clear visualization of DNS activities, helping to identify potential threats quickly.
- **DHCP Lease Overview:** Monitors DHCP assignments to detect unusual behavior and potential security issues.
- **Audit Logs Overview:** Tracks network configuration changes, ensuring compliance and security.
- **Blocked DNS Requests Overview:** Analyzes blocked requests to prevent and respond to threats.
- **SOC Insights Overview:** Summarizes critical security insights and alerts.

User Actions

- **Dossier Lookup:** Quickly investigate domains, IPs, and other indicators of compromise with Infoblox Dossier.
- **TIDE Lookup:** Access detailed threat intelligence to make informed security decisions.
- **IPAM Lookup:** Retrieve IP address data to correlate network activities with potential threats.
- **DHCP Lease Lookup:** Trace device activities through DHCP lease records.
- **Domain/IP Blocking:** Directly block or allow domains and IPs within QRadar to streamline threat mitigation.

The Infoblox App for QRadar empowers your security operations with advanced visibility, improved response times, and enhanced efficiency, ensuring your organization is better protected against emerging threats.

OVERALL QRADAR AND INFOBLOX INTEGRATION

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

- **SIEM Efficiency:** Maintain optimal performance by accessing only the relevant threat intelligence and network data.
- **SOAR Effectiveness:** Empower your security orchestration and automation with enriched data and advanced filtering capabilities.
- **Integration Simplicity:** Quick and easy integration using proven methods speeds up time-to-value.
- **Operational Productivity:** Improve the efficiency of your security operations by providing advanced visibility and filtering capabilities.
- **Investment ROI:** Enhance the return on your SIEM and SOAR investments with the added security benefits of BloxOne Threat Defense.

CONCLUSION

Managing security workloads, controlling storage costs, and maintaining effective threat response are significant challenges for SecOps teams. The integration of Infoblox with QRadar enhances the value of your entire security stack by providing enriched threat intelligence and comprehensive network data. This combination boosts SecOps productivity, improves efficiency, and ensures a more robust and responsive security program. By leveraging the Infoblox App for QRadar, you elevate your organization's security capabilities and maximize the return on your security investments.

infoblox

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

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

+1.408.986.4000
www.infoblox.com

Version: 20240703v1