

SOLUTION NOTE

UPLIFT YOUR SIEM AND SOAR EFFICIENCY WITH MICROSOFT SENTINEL AND BLOXONE THREAT DEFENSE

CHALLENGES

Without rich contextual information, cybersecurity teams struggle to produce accurate threat intelligence and respond to security events. Context is critical for truly understanding your data. It is a challenge to not only analyze that data, but even to access it in the first place. Teams may use dozens of security tools spread over many different places, and deal with hundreds or even millions of logs per day.

Security teams need an integrated approach to total enterprise security. Implementing such an approach relies on the ability to automate manual processes, as well as a unified security stack for a faster and coordinated response to threats.

SOLUTION

Infoblox, the DNS infrastructure and security leader, and Microsoft Sentinel, a leading SIEM and SOAR, offer easy integrations that enhance the capabilities of each solution and elevate overall SecOps efficiency.

Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for attack detection, threat visibility, proactive hunting and threat response.

Infoblox BloxOne Threat Defense feeds DNS, DHCP and Threat Defense logs to Microsoft Sentinel to advance the user experience for security analysts. The integrated solution provides team members with insights and visibility into devices and user activities on the DNS level and additional network context with IPAM metadata.

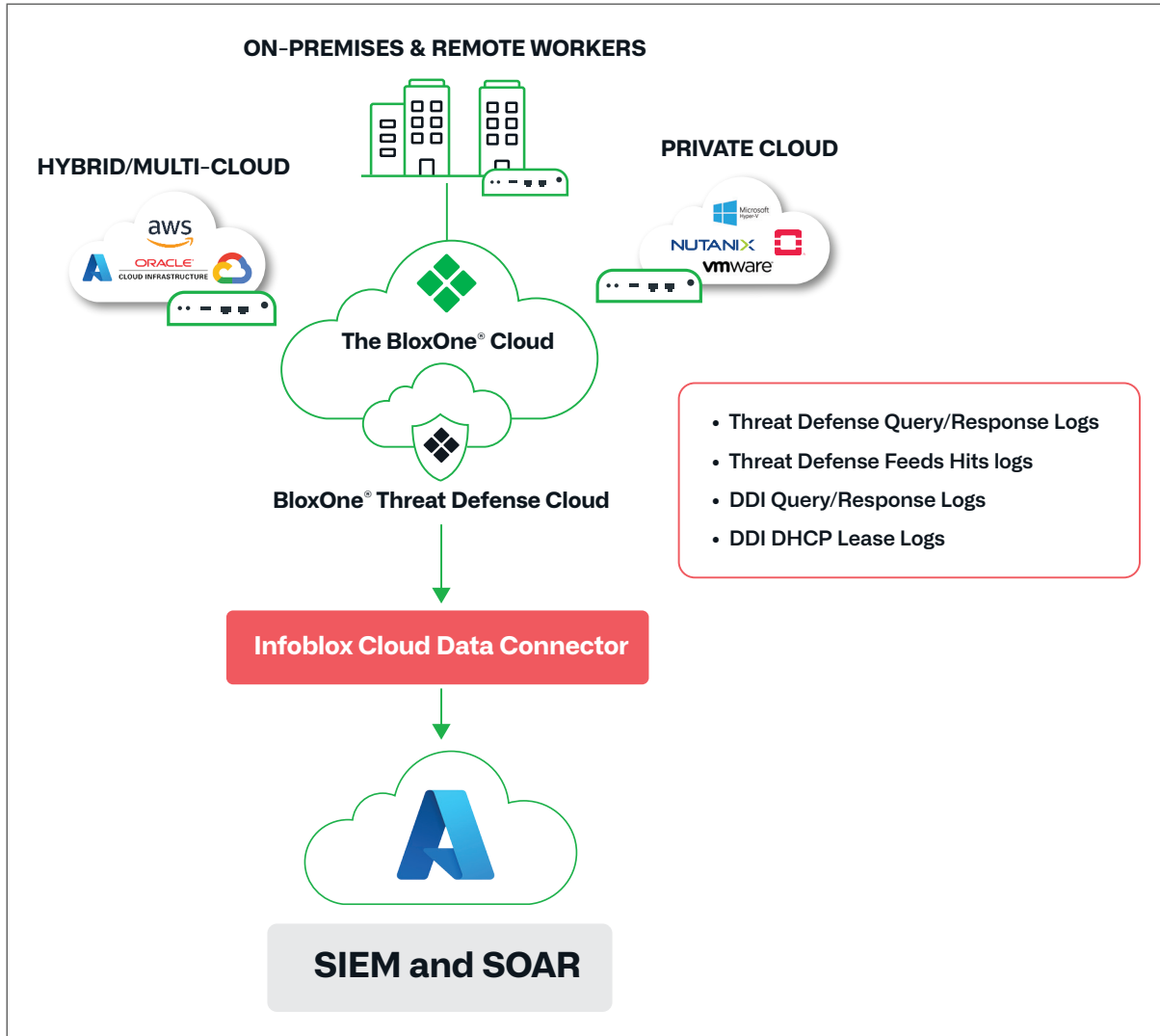
Microsoft Sentinel receives Infoblox feeds using the Infoblox Cloud Data Connector Solution that is available to download on Azure Marketplace—it can be deployed directly into customers' workspace in a single step. With the integration's data sources connected in this way, security analysts get the benefit of monitoring the data using the Microsoft Sentinel integration with Azure Monitor Workbooks, which provides integrative dashboard experiences and versatility in creating custom workbooks.

In the event of detection of a threat, security analysts can investigate the threat with rich, contextual data available in BloxOne Threat Defense. To make the best use of the data from BloxOne Threat Defense, analysts can apply custom thresholds and categorize the data based on low, medium and high severity. The analytics data can be used to create incidents in Microsoft Sentinel based on severity. Analysts also have the ability to set notifications for any user-defined anomalous activity and automate remediation as well.

KEY CAPABILITIES

BloxOne Threat Defense integrates seamlessly into Microsoft Sentinel to accelerate threat correlation and hunting, helping to reduce incident response times by two-thirds. Using Infoblox's Cloud Data Connector, a feature of BloxOne Threat Defense, users can send BloxOne data to Microsoft Sentinel to be enriched, visualized and examined. Security Analysts can then analyze the information and respond to events more efficiently while cross-correlating threat events with other security logs across Microsoft.

- Send DNS, DHCP and Threat Defense queries and responses to Sentinel
- Gain insight and visibility into devices and user activities on the DNS level with IPAM metadata
- Visualize, chart and monitor threats with fully customizable, interactive workbooks
- Investigate and detect threats automatically using thousands of analytic data points



KEY CAPABILITIES

- Access extensive device and network data (including domains, IPs and other DNS request data) that provides invaluable context around events to drive intelligent decision-making.
- Correlate comprehensive threat intelligence around events to give analysts insight into malicious activity to speed investigation and response.
- Summarize security hits by indicators of compromise (IoCs) and keep track of threat landscape hits over time with Microsoft Sentinel workbooks and security analytics.
- Speed response by prioritizing higher risk security events with access to dozens of threat intelligence feeds.
- Monitor device activity and trends across the entire platform with consolidated visibility.
- Provide administrators with access to additional threat and network insight data to maximize your Microsoft Sentinel deep investigation operations.

Microsoft Sentinel and Infoblox Integration Benefits

- **SIEM Efficiency** - Maintain optimum performance with on-demand access to only the “right” threat intelligence and network data.
- **SOAR Effectiveness** - Enhance and automate your incident remediation process by boosting your Microsoft Sentinel workbooks and playbooks with additional access to aggregated and curated threat intelligence and device data.
- **Integration Simplicity** - Download and deploy Infoblox Cloud Data Connector Solution from Azure marketplace to easily leverage proven Microsoft Sentinel solution capabilities to speed time-to-value.
- **SecOps Productivity** - Improve the efficiency of security operations using enhanced visibility, integration and automation.
- **Investment ROI** - Get more out of your SIEM and SOAR investment in addition to the unique security benefits of BloxOne Threat Defense.

CONCLUSION

Empower your SecOps experience, protect your business and mitigate risk at scale with Microsoft Sentinel and BloxOne Threat Defense. Improve your Microsoft Sentinel SIEM and SOAR efficiency by accessing comprehensive intelligence from Infoblox. Gain full visibility into threat vectors, prioritize security hits, investigate threats with artificial intelligence and respond to incidents rapidly.



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