SOLUTION NOTE

UPLIFT YOUR SIEM AND SOAR EFFICIENCY WITH MICROSOFT SENTINEL AND INFOBLOX

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 Domain Name System (DNS) infrastructure and security leader, and Microsoft Sentinel, a leading security information and event management (SIEM) and security orchestration, automation and response (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 with SOC Insights feeds DNS, Dynamic Host Configuration Protocol (DHCP) and Threat Defense logs to Microsoft Sentinel to advance the user experience for security analysts. The integrated solution provides team members with prioritized insights and visibility into devices and user activities on the DNS level and additional network context with IP address management (IPAM) metadata.

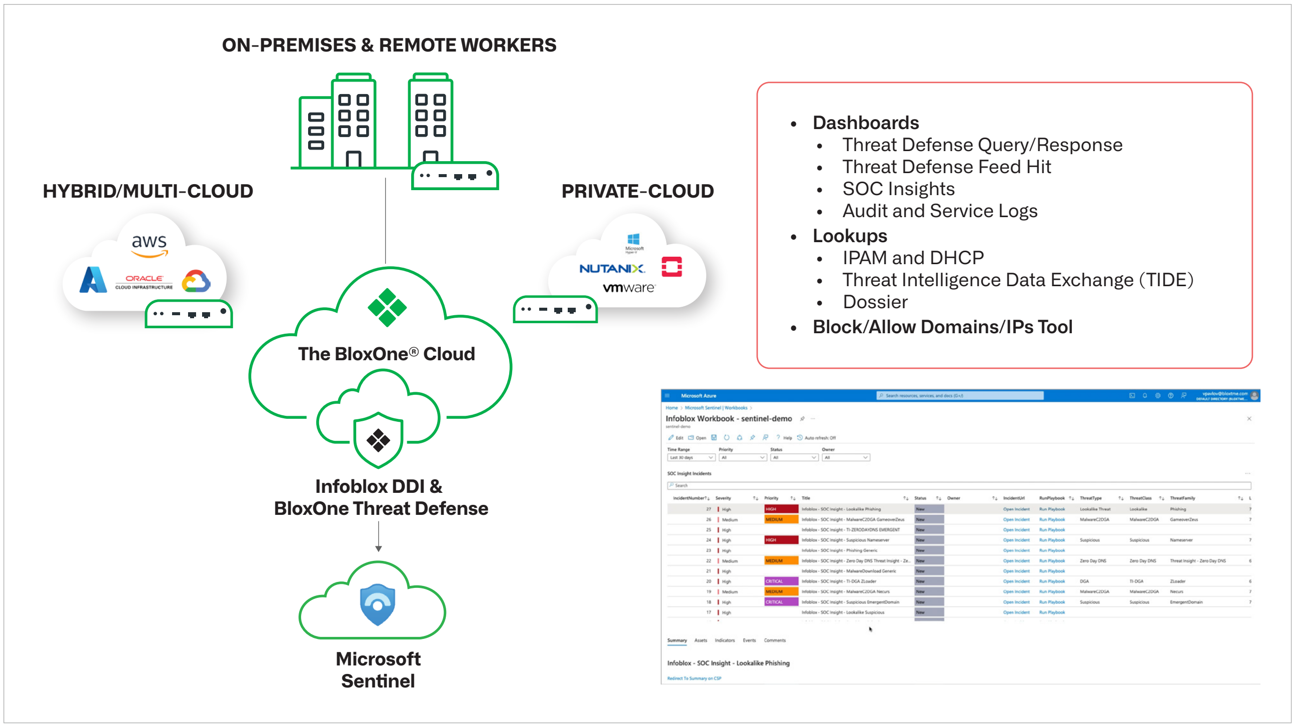
Microsoft Sentinel receives Infoblox feeds using the app—available for download on Azure Marketplace—that can be deployed directly into a customer's workspace in a single step. With the data sources connected, security analysts get the benefit of monitoring the data using the Microsoft Sentinel integration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

In the event of detection of a prioritized 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 further 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. Users can send BloxOne data to Microsoft Sentinel to be enriched, visualized, prioritized 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 Microsoft 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


ON-PREMISES & REMOTE WORKERS
HYBRID/MULTI-CLOUD
aws
ORACLE CLOUD INFRASTRUCTURE
PRIVATE-CLOUD
Microsoft Hyper-V
NUTANIX
vmware
The BloxOne® Cloud
Infoblox DDI & BloxOne Threat Defense
Microsoft Sentinel

- **Dashboards**
  - Threat Defense Query/Response
  - Threat Defense Feed Hit
  - SOC Insights
  - Audit and Service Logs
- **Lookups**
  - IPAM and DHCP
  - Threat Intelligence Data Exchange (TIDE)
  - Dossier
- **Block/Allow Domains/IPs Tool**

Microsoft Azure
Search resources, services, and docs (G+/)
vpavlov@bloxtme.com
DEFAULT DIRECTORY (BLOXTME...
Home > Microsoft Sentinel | Workbooks >
Edit
Open
Help
Auto refresh: Off
Summary
Assets
Indicators
Events
Comments

Infoblox Workbook - sentinel-demo

sentinel-demo

Time Range: Last 30 days
Priority: All
Status: All
Owner: All

SOC Insight Incidents

IncidentNumber	Severity	Priority	Title	Status	Owner	IncidentUrl	RunPlaybook	ThreatType	ThreatClass	ThreatFamily	L
27	High	HIGH	Infoblox - SOC Insight - Lookalike Phishing	New		Open Incident	Run Playbook	Lookalike Threat	Lookalike	Phishing	7
26	Medium	MEDIUM	Infoblox - SOC Insight - MalwareC2DGA GameoverZeus	New		Open Incident	Run Playbook	MalwareC2DGA	MalwareC2DGA	GameoverZeus	7
25	High		Infoblox - SOC Insight - TI-ZERODAYDNS EMERGENT	New		Open Incident	Run Playbook				
24	High	HIGH	Infoblox - SOC Insight - Suspicious Nameserver	New		Open Incident	Run Playbook	Suspicious	Suspicious	Nameserver	7
23	High		Infoblox - SOC Insight - Phishing Generic	New		Open Incident	Run Playbook				
22	Medium	MEDIUM	Infoblox - SOC Insight - Zero Day DNS Threat Insight - Ze...	New		Open Incident	Run Playbook	Zero Day DNS	Zero Day DNS	Threat Insight - Zero Day DNS	6
21	High		Infoblox - SOC Insight - MalwareDownload Generic	New		Open Incident	Run Playbook				
20	High	CRITICAL	Infoblox - SOC Insight - TI-DGA ZLoader	New		Open Incident	Run Playbook	DGA	TI-DGA	ZLoader	6
19	Medium	MEDIUM	Infoblox - SOC Insight - MalwareC2DGA Necurs	New		Open Incident	Run Playbook	MalwareC2DGA	MalwareC2DGA	Necurs	7
18	High	CRITICAL	Infoblox - SOC Insight - Suspicious EmergentDomain	New		Open Incident	Run Playbook	Suspicious	Suspicious	EmergentDomain	7
17	High		Infoblox - SOC Insight - Lookalike Suspicious	New		Open Incident	Run Playbook				

Infoblox - SOC Insight - Lookalike Phishing

Redirect To Summary on CSP

INFOBLOX AND MICROSOFT SENTINEL EMPOWER SECURITY TEAMS TO:

- 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 prioritized, comprehensive threat intelligence around events to give 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 optimal performance by accessing only the relevant 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 the Infoblox app from Azure marketplace to easily leverage proven Microsoft Sentinel solution capabilities to speed.
- **SecOps Productivity:** Improve the efficiency of SecOps 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

Version: 20240719v1