SOLUTION NOTE

ELEVATE YOUR GOOGLE SECOPS SIEM AND SOAR EFFICIENCY WITH INFOBLOX THREAT DEFENSE™ INTEGRATION

OVERVIEW

Security operations teams are under mounting pressure to reduce incident response times, eliminate alert fatigue and improve visibility across increasingly complex environments. The integration of Infoblox with Google Security Operations (SecOps) empowers these teams with actionable intelligence, automated workflows and deeper asset context, hence unlocking a new level of efficiency for modern security operations. By combining Infoblox's foundational DNS, DHCP and IP address management (DDI) context with Google's cloud-native SIEM and SOAR capabilities, organizations gain a unified, automated and highly effective defense posture.

DETECTING THREATS WITH GOOGLE SECURITY OPERATIONS

Google SecOps helps security operations teams detect and respond to modern threats with Google scale and intelligence. SecOps teams choose Google SecOps for its scalability, which allows it to ingest and search through massive amounts of data and apply Google's leading threat intelligence to detect more threats. Google SecOps also appeals to security operations teams due to its AI-powered productivity.

The Challenge: Disconnected Tools and Alert Overload

Security teams face increasing pressure to manage complex environments, rising threat volumes and siloed tools. Common challenges include:

- **Alert Fatigue:** High volumes of low-context alerts slow down response times.
- **Manual Investigations:** Analysts waste time pivoting between tools to gather context.
- **Delayed Containment:** Lack of DNS-layer enforcement delays threat mitigation.
- **Limited Visibility:** Unknown or unmanaged devices increase risk exposure.

The Solution: Infoblox + Google SecOps Integration

This joint solution delivers real-time threat intelligence, automated response and enriched visibility across your security stack.

KEY CAPABILITIES

- Real-time DNS event forwarding to Google SecOps
- Automated threat blocking via RPZ
- AI-driven alert triage with ServiceNow integration
- Vulnerability scans triggered on new device detection
- Enriched network context from DNS, DHCP and IPAM data

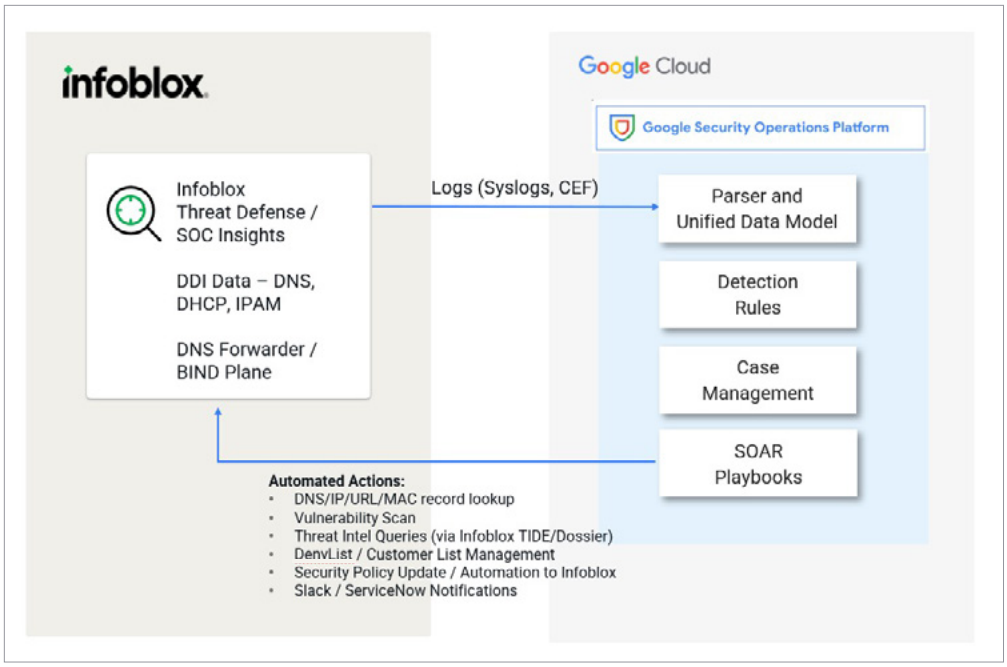

Figure 1. Infoblox integration with Google Security Operations platform

	Key Benefits
1	**Centralized Event Logging and Visibility** Infoblox Threat Defense™ sends DNS, DHCP and security event logs to Google SecOps in syslog/ CEF/LEEF formats. Google SecOps ingests and normalizes this data into its unified data model (UDM), enabling: • Deep search and correlation across DNS and network activity • Enhanced visibility into device behavior and threat indicators • Faster detection of suspicious domains and lateral movement **Benefit:** Gives analysts unified visibility and enriched context, enabling faster, more accurate threat detection across all network and security events.
2	**Automated Threat Containment via RPZ** When Google SecOps detects a malicious domain or IP: • A SOAR playbook triggers an API call to Infoblox • The threat is added to a custom response policy zone (RPZ) • DNS queries to the domain are blocked network-wide in real time **Benefit:** Immediate containment at the DNS layer, reducing dwell time and preventing command-and-control (C2) communication or data exfiltration.

3	**AI-Driven Triage and Case Management** Infoblox SOC Insights applies AI to reduce alert noise and surface high-confidence incidents. • Low-severity events trigger notifications. • Medium-/high-severity events automatically create tickets in ServiceNow. • Tickets include enriched context (device, user, threat details). **Benefit:** Streamlined incident response with reduced manual effort and faster resolution.
4	**Proactive Vulnerability Management** Infoblox detects new devices as they join the network. This event can trigger a Google SecOps playbook to: • Launch a vulnerability scan via tools like Qualys or Tenable • Prioritize scans based on device type, location and threat context from Infoblox **Benefit:** No unmanaged devices go unscanned, improving risk posture and compliance.

CONCLUSION

The integration of Infoblox Threat Defense with Google SecOps delivers a unified, automated and intelligence-driven approach to modern security operations. By combining deep network visibility with powerful analytics and orchestration, organizations can detect threats earlier, respond faster and reduce operational overhead. This joint solution enables security teams to stay ahead of evolving threats while maximizing the value of their existing investments.

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

+1.408.986.4000
www.infoblox.com

Version: 20250801v2