SOLUTION NOTE

ENRICH YOUR SPLUNK SIEM AND SOAR WITH INFOBLOX

Get more from your Splunk Enterprise SIEM and SOAR investment with revealing DNS visibility.

CHALLENGES

Security teams rely on SIEM and SOAR tools to efficiently investigate and respond to security events. As attacks become stealthier and harder to detect, organizations have been forced to increase monitoring, which requires pulling more and more logs into their security monitoring platforms. This process increases storage requirements and the number of alerts issued and investigations undertaken, which often leads to fatigue and burnout of security analysts.

It can be difficult to access and correlate threat intelligence and relevant device and network data for investigation insights and effective automation. Playbook capabilities are limited without this valuable contextual information.

QUICK TIME TO VALUE THROUGH EASY INTEGRATION

Infoblox, a DNS infrastructure and security leader, and Splunk, a leading SIEM and SOAR solution provider, offer easy integrations that can uplift the capabilities of each solution and elevate overall SecOps efficiency.

Splunk Cloud Platform and Splunk Enterprise Security provide hybrid cloud services with proactive and reactive mechanisms for consuming external data. Based on that data they enable the security teams to search, analyze, visualize and act.

Infoblox BloxOne® Threat Defense with SOC Insights integrates with Splunk solutions to provide unique, prioritized insights and event-related data through tools like the Infoblox Threat Intelligence Data Exchange (TIDE) and Infoblox Dossier. Each feature can deliver prioritized data to Splunk to minimize storage requirements and optimize investigation, automation and other efforts by security analysts.

VISUALIZE INFOBLOX THREAT INTELLIGENCE DATA IN SPLUNK ENTERPRISE SECURITY AND CLOUD PLATFORM

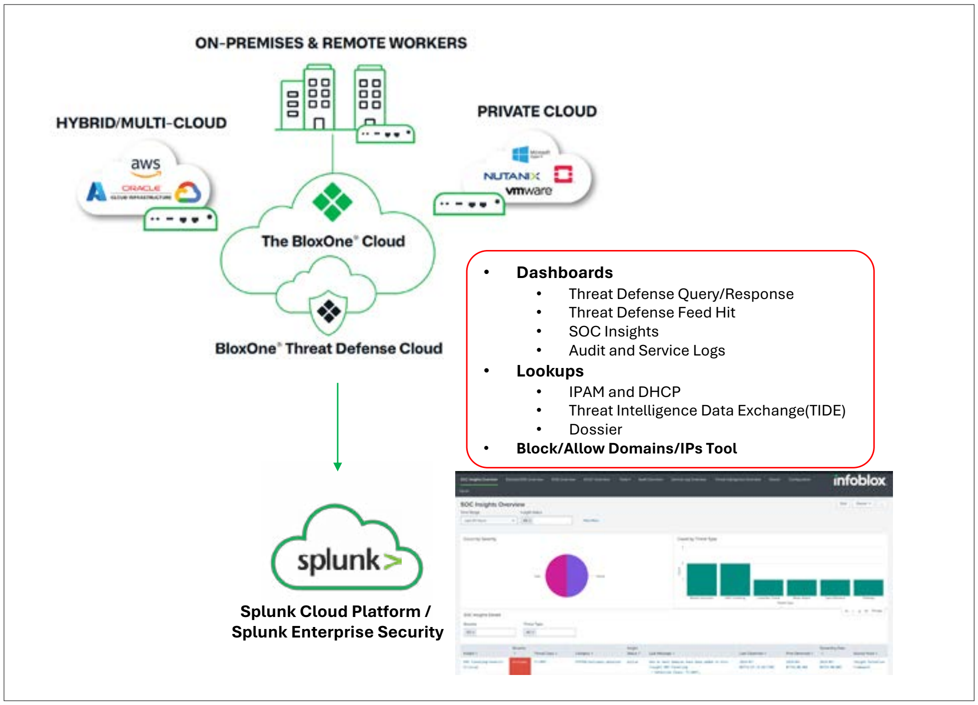
Infoblox TIDE provides highly accurate machine-readable threat intelligence to Splunk to help security teams detect threat activity and to reduce dwell time. Together, the integrated Infoblox and Splunk solution assists security teams in reducing investigation times and increasing visibility to support the modern hybrid network.

KEY CAPABILITIES

Infoblox's integration with the Splunk Cloud Platform, Splunk Enterprise Security and Splunk SOAR enhances Splunk's performance and boosts visibility into events and threat intelligence, helping to speed investigations and drive more efficient responses. The integration enables security and incident response teams to better leverage the power of SIEM and SOAR on-premises or in the Splunk Cloud Platform by pairing it with DNS security events, IP address management (IPAM) metadata and threat information from Infoblox.

Splunk SIEM capabilities, enhanced by Infoblox TIDE, enable security teams to:

- Access extensive device and network data for context
- Optimize storage requirements through intelligence filtering
- Correlate prioritized, comprehensive threat
- intelligence around events



- **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**

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 prioritized, comprehensive threat intelligence around events to provide analysts insight into malicious activity to speed investigation and response.
- Optimize storage requirements through intelligence filtering to maximize Splunk performance while ensuring analysts have all of the “right” data on demand.
- Summarize security hits by indicators of compromise (IoCs) and keep track of threat landscape hits over time based on threat severity with access to Infoblox Dossier data.
- 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.

DRIVE SOAR PRODUCTIVITY WITH INFOBLOX DOSSIER

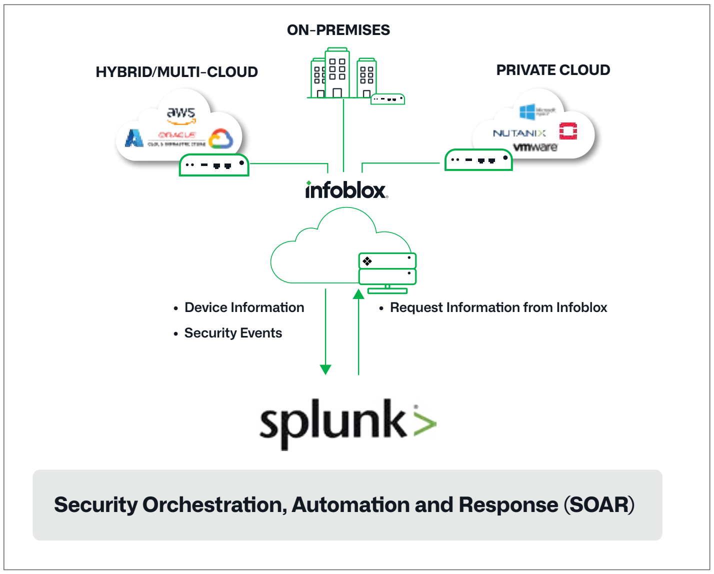
In addition to events, context, and device and network metadata, Infoblox Dossier provides access to in-depth threat intelligence. This can help analysts investigate and assess risk as well as trigger automated response and uplift playbook capabilities.

Splunk SOAR capabilities, enhanced by Infoblox Dossier, enable security analysts to:

- Gain direct access to Infoblox threat intelligence to detect threat activity
- Automate effective threat response with complete device metadata
- Empower playbooks with comprehensive threat and network insight

KEY CAPABILITIES

- Gain direct access to IoCs in Infoblox Threat Intelligence to detect and block threats and suspicious activity
- Automate effective device isolation and other threat responses with extensive visibility and device metadata
- Provide administrators with access to additional threat and network insight data to uplift your SOAR playbooks
- Automate/accelerate response with a complete set of threat intelligence APIs
- Speed response with better threat intelligence and by prioritizing higher risk security events



OVERALL SPLUNK AND INFOBLOX INTEGRATION BENEFITS

- **SIEM Efficiency**: Maintain optimal performance by accessing only the relevant threat intelligence and network data.
- **SOAR Effectiveness**: Boost your playbooks with additional access to aggregated and curated threat intelligence and device data.
- **Integration Simplicity**: Easily leverage proven Splunk apps to speed time to value.
- **SecOps Productivity:** Improve visibility and provide advanced filtering capabilities, thus improving the efficiency of SecOps.
- **Investment ROI**: Get more out of your SIEM and SOAR investment in addition to the unique security benefits of BloxOne Threat Defense.

CONCLUSION

SecOps teams struggle with managing workloads, controlling storage costs and keeping up with all the existing tools to investigate and respond to security events. Integrating Splunk Enterprise SIEM and SOAR with curated threat intelligence and device and network metadata, improves the effectiveness of these tools as well as the efficiency of your security teams. Infoblox with Splunk increases the value of your entire security stack, elevates SecOps productivity and efficiency, and makes your overall security program more robust and responsive.

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: 20240724v4