SOLUTION NOTE

POWERING SOAR SOLUTIONS FROM THE FOUNDATION

OVERVIEW

As organizations seek more effective ways to combat cyberthreats, a new category of security solutions is gaining traction.

Known as security orchestration, automation and response (SOAR), these platforms are designed to make diverse security tools and systems work better together to accelerate threat response and improve security operations center (SOC) efficiency. However, getting optimal performancefrom SOAR solutions require access to contextual data. This contextual data and precise visibility can be obtained from foundational infrastructure on which all neworks depend—DNS, DHCP and IPAM.

CHALLENGES DRIVING THE EMERGENCE OF SOAR SOLUTIONS

The rise of SOAR technologies is a response to several challenges that have worsened in recent years, as cybersecurity landscapes have grown more complex. Two key challenges include:

- **Security device and alert proliferation:** Organizations have deployed hundreds of network and security devices. These tools generate a massive number of alerts that security teams must address. They also create solution silos and require manual interventions that slow response times.
- **Lack of interoperability and integration:** Today's enormous arsenals of security tools are often poorly integrated, which limits visibility, agility and the efficiency of security operations.

THE RISE OF SOAR TECHNOLOGIES

The twin obstacles of tool proliferation and lack of integration have given rise in recent years to a new category of security solutions. The term security orchestration, automation and response (SOAR) was first coined in 2017 by research firm Gartner. According to Gartner, a SOAR solution:

- Integrates disparate security tools
- Facilitates the automation of security tasks and incident response
- Combines reports and dashboards to improve the efficiency of the SOC team

As described by Gartner, the three most important capabilities a SOAR technology provides include:

- **Security incident response:** How an organization plans, manages, tracks and coordinates its response to a security incident
- **Threat and vulnerability management:** Technologies that support remediation of vulnerabilities and provide formalized workflow, reporting and collaboration capabilities
- **Security operations automation and orchestration:** Technologies that handle the automation and orchestration of workflows, processes, policy execution and reporting

KEY BENEFITS OF SOAR TECHNOLOGIES

SOAR solution enable security teams to:

Prioritize operational activities

- Consolidate data from different security tools, third-party feeds and IT databases
- Centralize visibility into security events to prioritize threat response

Formalize triage and incident response

- Review and assess incidents more quickly and begin remediation of security incidents based on best practices
- Respond to threats faster and overcome problems stemming from an overworked and undermanned cybersecurity workforce

Automate workflows

- Automate time-consuming and mundane activities so that SOC engineers can focus on proactive tasks such as threat hunting
- Centralize visibility into security events to prioritize threat response

HOW INFOBLOX POWERS SOAR SOLUTIONS

SOAR technologies represent a substantial leap forward in cybersecurity. But in order to fully deliver on their promise, SOAR solutions require access to contextual data. This contextual data and precise visibility can be obtained from foundational infrastructure on which all neworks depend—DNS, DHCP and IPAM.

They are the least common denominator that enables connectivity for traditional network topologies as well as cloud, IoT and SD-WAN. In addition, these services contain unique troves of information at the device level including device type, location in the network, owner, and audit trail such as internal and external destinations accessed/visited. Infoblox optimizes SOAR solutions by making this connective data layer available automatically and in real time to all security tools in the security stack. It does so through a highly interconnectedset of data integrations and extensive vendor APIs.

With Infoblox, security teams can enhance the performance of SOAR technologies, eliminate silos, enable automation and orchestration and improve the ROI of their entire security stack, including third-party, multi-vendor assets. Infoblox reduces the expense of responding to threats through its combination of enhanced automation and two-way data sharing of security event information.

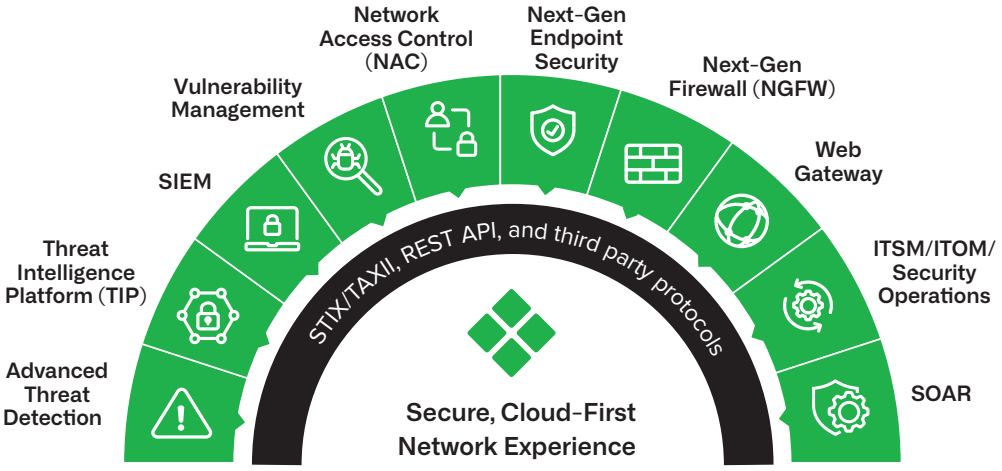

Figure 1: Infoblox makes foundational security data available automatically and in real-time to all components of the security ecosystem

INTEGRATING INFOBLOX AND SOAR

Infoblox can automatically provide a SOAR solution with crucial device and security event information automatically and in real time. On receiving data on IP addresses, network devices and malicious events from Infoblox, the SOAR platform can then use that data to block or unblock domains, check information on IP, host, network, and domains and enrich other security tools in the stack with that information.

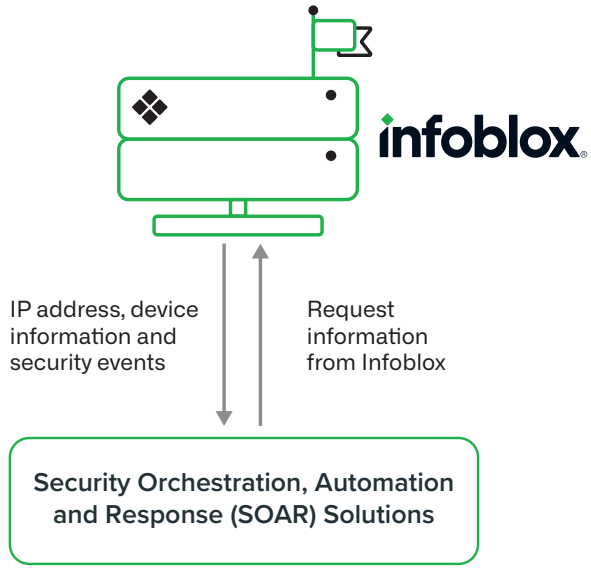

Figure 2: Infoblox data integration with SOAR

To learn more about Infoblox's security ecosystem integrations, including integration with SOAR vendors, please visit www.infoblox.com/products/bloxone-threat-defense and www.infoblox.com/solutions/cybersecurity-ecosystem/

SECURITY TEAMS CAN

- Coordinate disparate security tools and provide vendor-neutral threat intelligence for all devices
- Gain context for prioritization of threats
- Automate and respond faster to network and malicious events with a full set of threat intelligence APIs.
- Raise effectiveness and efficiency across the security ecosystem

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: 20230720v1