SOLUTION BRIEF

SIEM/SOAR + BLOXONE® THREAT DEFENSE — A POTENT COMBINATION

Enhance the effectiveness and coverage of these solutions through seamless integration

THE CHALLENGE

Security teams rely on SIEM and SOAR platforms to monitor, coordinate and automate responses to security alerts generated by security tools, applications and network assets. As attacks become stealthier and harder to detect, organizations have been forced to increase monitoring, which requires pulling more and more logs into these orchestration platforms. At the same time, fast-rising numbers of alerts and investigations often lead to fatigue and burnout of security analysts. In addition, the security tools and hardware that feed into SIEM and SOAR are not designed to detect the presence of widespread threats that exploit DNS pathways.

ENHANCE SECURITY COVERAGE OF SIEM/SOAR WITH INTEGRATED DNS DETECTION AND RESPONSE

The DNS protocol plays a central role in all network communications. It is also inherently insecure, which is why it is the vector for more than 90 percent of malware and is also invoked in pervasive ransomware, data exfiltration and distributed denial of service attacks. DNS Detection and Response (DNSDR) expands the defense-in-depth of SIEM/SOAR solutions by identifying and remediating DNS threats that elude other security measures.

The industry's leading DNSDR solution, Infoblox BloxOne® Threat Defense, integrates with top-tier SIEM/SOAR platforms and eases burdens for SecOps teams. It does so by accelerating SIEM/SOAR analysis and correlation and by reducing mean time to respond (MTTR). In addition, the solution gives security organizations:

- Comprehensive device and user context to understand potential risk, efficiently prioritize alerts and enrich SOAR playbooks
- A structured view of network and threat intelligence data to help SecOps make appropriate decisions faster
- DNS-centric threat intelligence to detect threats, such as lookalike domains, connections to malicious and suspicious domains and data exfiltration, while automatically sharing incident information with SIEM/SOAR

TOP SIEM/SOAR PLATFORMS INTEGRATE WITH INFOBLOX

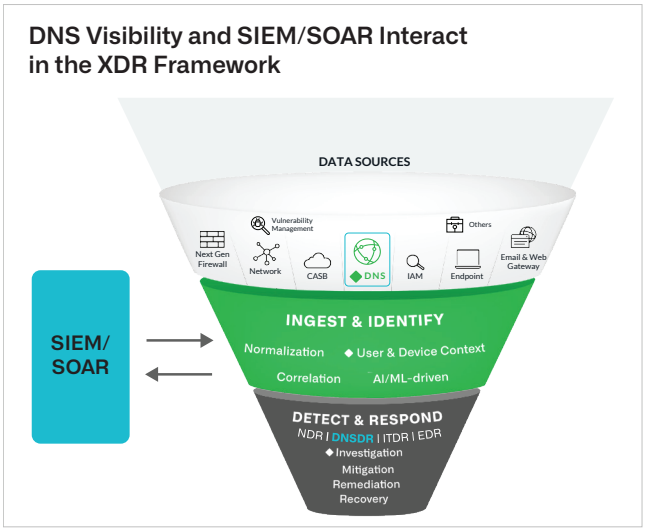
Microsoft Sentinel

IBM QRadar

splunk>

LogRhythm The Security Intelligence Company

DNSDR ELEVATES SIEM/SOAR AND THE ENTIRE XDR ECOSYSTEM



DNSDR and SIEM/SOAR platforms are essential components of extended detection and response (XDR) solutions. Through APIs and pervasive automation, DNSDR implementations like BloxOne Threat Defense improve the performance and efficiency of not only SIEM/SOAR, but of core XDR capabilities across the security ecosystem.

"Infoblox's Cybersecurity Ecosystem integration with [SIEM vendor] and robust API calls was the perfect complement. Not only did the integration deliver immediate time to value, but it also extended its ROI and added the flexibility to integrate with a broad array of future security and orchestration tools."

- **Global Weather Service Customer**

SHARING DNS VISIBILITY AND CONTEXT WITH SIEM/SOAR

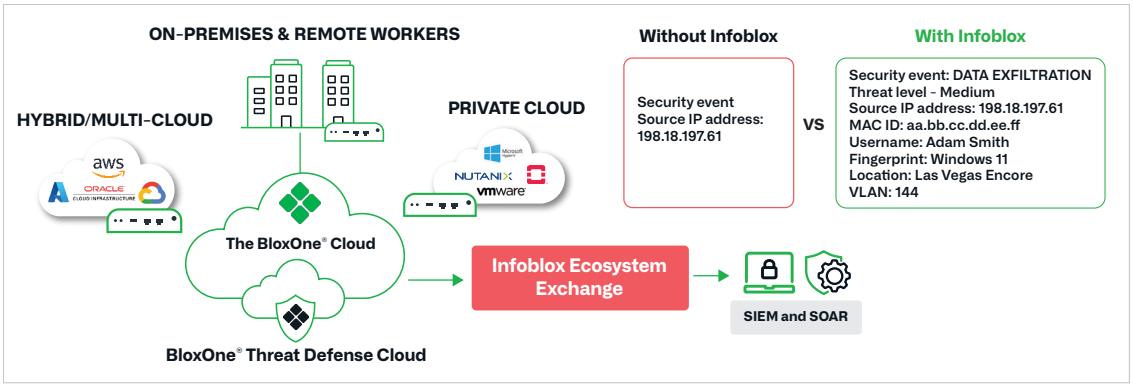
In the event of a threat detection, security analysts can investigate the threat with rich, contextual data provided in real time by BloxOne Threat Defense. Using that data, analysts can:

- Create incidents in the SIEM/SOAR based on severity
- Apply custom thresholds and categorize the data based on low, medium and high severity
- Set notifications for any user-defined anomalous activity and automate remediation

TOP 10 REASONS CUSTOMERS CHOOSE BLOXONE THREAT DEFENSE

1. Accelerate Time to Value
2. Detect Threats Other Solutions Miss
3. Achieve Anywhere, Hybrid Visibility and Control
4. Stop Attacks Earlier in the Attack Chain
5. Boost SecOps Efficiency
6. Speed Investigation and Response by 3X
7. Unlock the power of DNS Threat Intel
8. Optimize the Security Ecosystem
9. Get More from Security Investments
10. Gain Greater Context by Merging IPAM with DNS

HOW INFOBLOX AND SIEM/SOAR INTERACT



To learn more about the benefits of our Cybersecurity Ecosystem visit https://www.infoblox.com/products/cybersecurity-ecosystem/

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