

## SOLUTION BRIEF

# SIEM/SOAR + INFOBLOX THREAT DEFENSE™—A POTENT COMBINATION

Enhance the effectiveness and coverage of these solutions through seamless integration

### THE CHALLENGE

Security teams rely on security information and event management (SIEM) and security orchestration, automation and response (SOAR) platforms to monitor, coordinate and automate responses to security alerts generated by security tools, applications and network assets. As attackers are increasingly using AI to generate unique, single-use exploits, 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 built to see what is happening at the DNS layer, the earliest, most universal control point for nearly every attack.

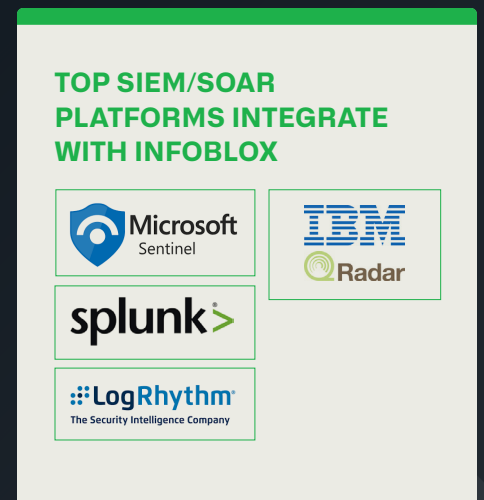
### ENHANCE SECURITY COVERAGE OF SIEM/SOAR WITH PREEMPTIVE DNS-LAYER SECURITY

The DNS protocol plays a central role in all network communications. It is also inherently insecure, which is why it is the vector of choice for malware and is also invoked in pervasive ransomware, data exfiltration and distributed denial-of-service attacks. Protective DNS security from Infoblox extends the defense-in-depth of SIEM/SOAR solutions with a preemptive, DNS-first control point. It identifies and blocks DNS-based threats and attacker infrastructure before they are weaponized, closing gaps that traditional “detect and respond” tools cannot see.

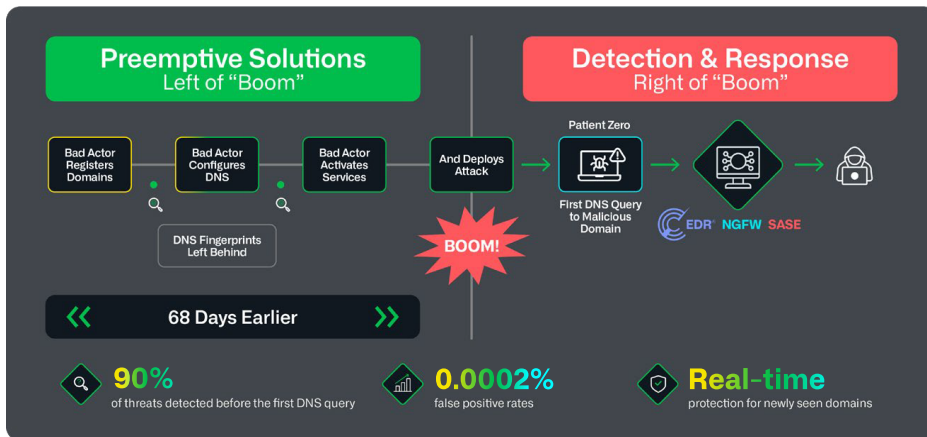
Infoblox Threat Defense™ is powered by predictive threat intelligence. It integrates with top SIEM/SOAR platforms to enhance each solution’s capabilities and preemptively reduces the burden on SecOps teams by accelerating SIEM/SOAR analysis and correlation, reducing mean time to respond (MTTR). In addition, 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



## PROTECTIVE DNS DELIVERS PREEMPTIVE SECURITY



Preemptive security is an advanced approach that focuses on anticipating, predicting and stopping cyberthreats before they can cause harm. A Protective DNS approach is preemptive because it does not rely on patient zero. It uses a combination of predictive threat intelligence that blocks threat actor infrastructure before it is weaponized, and algorithmic/ML-based analysis of DNS queries in customer networks to provide protection before impact. Organizations can use DNS to protect their entire environment—infrastructure on-premises, cloud workloads, remote users and IoT/OT devices—from today's sophisticated, modern AI-driven attacks.

## SHARING DNS VISIBILITY AND CONTEXT WITH SIEM/SOAR

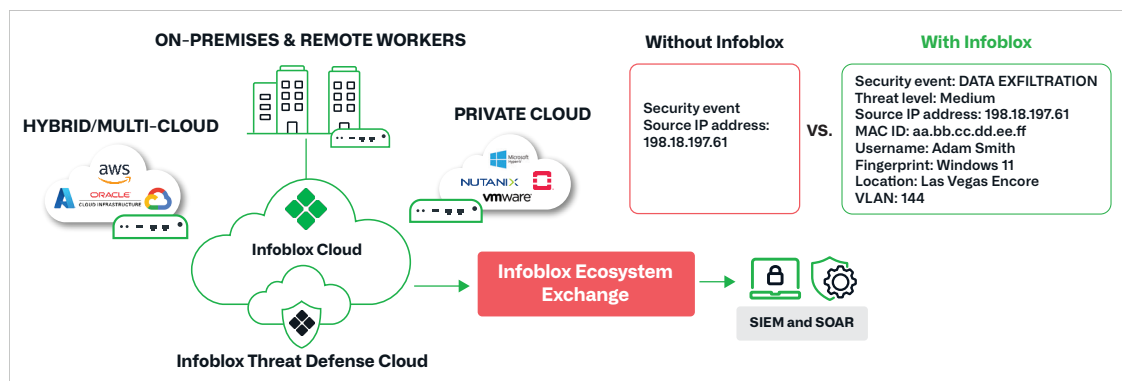
In the event of a threat detection, security analysts can investigate the threat with rich, contextual data provided in real time by Threat Defense. Using that data, analysts can:

- 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 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 three times
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 IP address management (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/>