Threat Containment and Operations

SUMMARY
With the Infoblox Threat Containment and Operations solution, your organization can eliminate silos between networking and security technologies and improve the ROI of your existing security investments. The solution improves the productivity of security operations, enhances automation, and optimizes your security, orchestration, automation and response (SOAR) solution using contextual network and threat intelligence data and ecosystem integrations. It also reduces the cost of threat feeds while improving the effectiveness of threat intelligence across the entire security portfolio.

Security Operational Challenges
If your security organization is like most, it likely has a number of operational gaps. Five key ones are silos, lack of context to prioritize and resolve threats, a cybersecurity skills shortage, manual approaches that slow resolution and fragmented threat intelligence.

Silos: Chances are, the defense strategy of your organization involves lots of security tools. These tools often work in silos between network and security teams, resulting in security gaps, slower detection of vulnerabilities and time-consuming processes to counter threats.

Lack of context: Your security operations teams are likely inundated with thousands of alerts each day, yet they have trouble prioritizing them based on actual risk. Threat intelligence combined with data contained within your network can provide a gold mine of information your teams can use to respond more effectively to security incidents. But the lack of clear visibility into network data inhibits taking the right action based on context.

Cybersecurity skills shortage: As a result of a global cybersecurity skills shortage, security teams are under pressure to do more with less.

Absence of automation: Being aware of and responding in real time to activities that network tools reveal can accelerate incident response. But without automation, your operations teams must assemble data from various sources manually. Often, security teams aren’t even notified when a vulnerability is discovered.

Fragmented threat intelligence: Most organizations are unaware that they may be using multiple sources of threat intelligence, which could lead to a higher false positive rate, conflicting information, and inefficiency. Such siloed threat intelligence adds cost, reduces effectiveness and erodes trust.

Together, these challenges lead to weak, inefficient security operations.
Key Elements of Threat Containment and Operations Solution

Infoblox’s solution to contain threats and optimize effectiveness of your organization’s existing security infrastructure provide the following benefits:

- Automate response and reduce time to remediation by two-thirds
- Optimize your SOAR solution
- Reduce the cost of threat feeds while improving the effectiveness of threat intel across entire security portfolio
- Get more value out of adjacent and complementary products through two-way data sharing
- Overcome lack of skilled resources with a 60 percent reduction in the demand on your security team to implement and operate, in terms of both skills and cost

The Infoblox solution includes the following key components:

- Optimizing SOAR solutions
- Optimizing threat intelligence
- Increasing automation for faster remediation
- Prioritizing threats and rapid triage
- Mining valuable network data for troubleshooting

Optimizing SOAR Solutions

Infoblox enables automation and optimizes your SOAR solution using contextual network and threat intelligence data, and ecosystem integrations (critical enabler of SOAR) to accelerate the speed of your threat response while reducing costs.

Optimizing Threat Intelligence

The Infoblox Threat Containment and Operations solution optimizes the use of threat intelligence. It combines policy enforcement with timely, consolidated and extensive threat intelligence drawn from multiple sources, verified and curated by an in-house threat research team. This approach eliminates conflicts between sources and distributes uniform threat intelligence across your existing security infrastructure, providing a single source of truth and orchestrating a common security policy.

Increasing Automation for Faster Remediation

Infoblox security orchestration involves using APIs to automatically share network events and indicators of compromise in real time with your existing third-party security tools. Such tools may include next-gen endpoint protection, next-gen firewalls, Network Access Control (NAC), vulnerability scanners, and security information and event management (SIEM) solutions. Infoblox API integration enables these disparate tools to work in concert to resolve security incidents faster. For example, when Infoblox detects data exfiltration or malware from an infected host, it can automatically notify an endpoint security solution to clean the infected endpoint. Likewise, it can trigger a vulnerability scan when a new device joins the network or trigger a NAC solution to prevent it from joining the network until it is brought into compliance.

In addition to sharing indicators of compromise, Infoblox also shares valuable network data, including user name, MAC address, device type, VLAN and lease history to help your teams assess risk and prioritize remediation. Security orchestration is vital to improving your security infrastructure.

Prioritizing Threats and Rapid Triage

Infoblox helps security analysts and researchers investigate threats faster by providing a single yet broad source of truth through our partners and the security marketplace. Infoblox intelligence supplies timely context, including type of malware, domain registration information and associated threat campaigns. Threat analysts and incident responders can leverage Infoblox APIs to gather information from multiple sources on an individual indicator, such as antivirus analysis, domain reputation score, passive DNS and WHOIS information. These searches occur with Infoblox masking the customer. Infoblox’s Threat Intelligence Data Exchange provides accuracy and context for each indicator, enabling security personnel to focus on the most critical indicators and ignore false positives, freeing them to handle other tasks.
Mining Valuable Network Data for Troubleshooting

DNS, DHCP and IPAM (DDI) data is a valuable resource that “crime-scene DNA” your organization can use for forensics and security operations. For example, with DDI data, your security teams can learn which device or user went to which destinations and when. DDI data can also reveal which devices are critical high-value assets that need protection. Your operations teams can determine the scope of a security incident or automate correlation of network context and data with security events. They can also access audit trails to profile device and user activity. In addition, with the Infoblox API, they can harvest historical DNS data, gaining further data mining and business intelligence to use in bolstering your security response.

Summary

With the Infoblox Threat Containment and Operations solution, your organization can bridge silos instead of creating new ones. Our solution enhances efficiency and automates security operations, enabling your teams to increase the speed and effectiveness of security solutions they already have in place. It does so by providing timely and necessary context to prioritize and remedy threats.

In addition, the solution provides your organization with access to the most extensive and updated threat intelligence, while enabling you to get the most from your existing investments in security tools and systems.