THREATQ™ AND INFOBLOX

Technology Segment: Enrichment & Analysis

With the combination of Infoblox contextual data and the ThreatQ threat intelligence platform, your organization can categorize, manage and respond to threats with greater speed and efficacy by activating cyberintelligence in Infoblox DNS and importing Infoblox threat intelligence.

THREATQ BY THREATQUOTIENT™

ThreatQ is an open and extensible threat intelligence platform (TIP) to provide defenders the context, customization and collaboration needed for increased security effectiveness and efficient threat operations and management. ThreatQ accelerates the transformation of threat data into actionable threat intelligence by giving defenders unmatched control through a threat library, an adaptive workbench and an open exchange to ensure that intelligence is accurate, relevant and timely to their business. With ThreatQ, customers can automate much of what is manual today and get more out of existing security resources, both people and infrastructure.

SILOBREAKER

Infoblox is the leading global provider of DNS, DHCP and IP address management services. Infoblox DNS can put more than 45 million threat indicators to work in real time within the Infoblox Grid™ and BloxOne™ Threat Defense, which provides advanced DNS security as SaaS-based services from the cloud. Infoblox solutions automate network control functions to reduce costs and maximize uptime while protecting against a flood of malware and DDoS attacks. From discovery, configuration and compliance, Infoblox automates and simplifies network and security processes.

INTEGRATION HIGHLIGHTS

Enhance IP address and DNS visibility for TIP administrators.

Accelerate responses to emerging threat vectors by using Infoblox contextual data.

Integrate threat intelligence feeds from the ThreatQ platform with Infoblox DNS security solutions

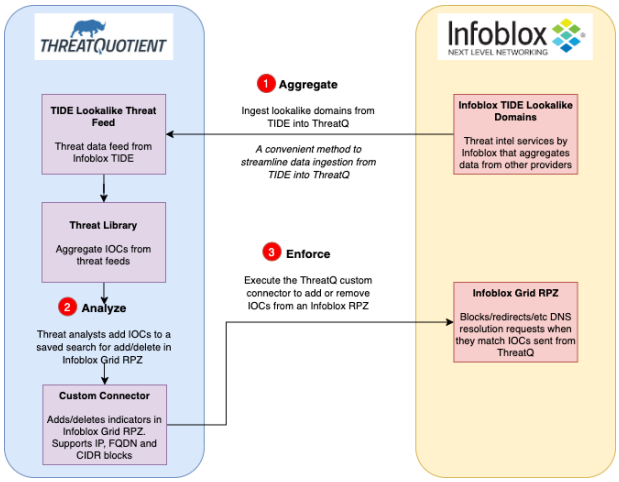
Download Infoblox threat intelligence from the Infoblox Threat Intelligence Data Exchange (TIDE) into the ThreatQ database.

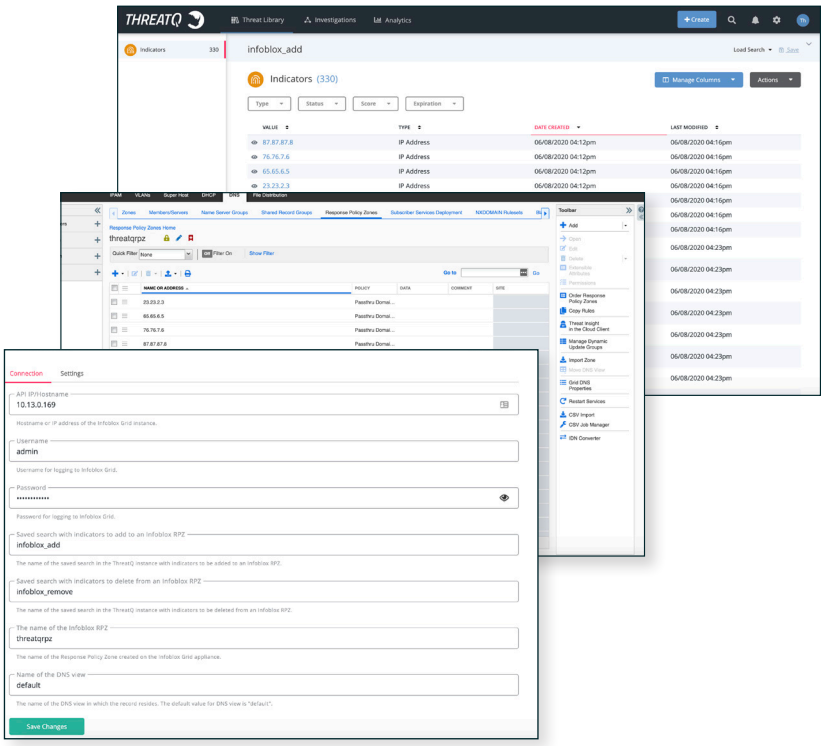
Monitor lookalike domains.

INTEGRATION USE CASES:

Integrating Infoblox IP and DNS contexts with ThreatQuotient supports a variety of use cases, such as:

- Allow joint customers to assess, categorize and manage security incidents.
- Eliminate unnecessary, duplicate and irrelevant indicators before they enter your network.
- Enforce security by blocking DNS requests to malicious resources (IP Addresses and Domains).





ABOUT THREATQUOTIENT™

ThreatQuotient™ understands that the foundation of intelligence-driven security is people. The company's open and extensible threat intelligence platform, ThreatQ™, and cybersecurity situation room solution, ThreatQ Investigations, empower security teams with the context, customization and prioritization needed to make better decisions, accelerate detection and response, and advance team collaboration. Leading global companies use ThreatQuotient solutions as the cornerstone of their security operations and threat management system. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC.

For more information, visit www.threatquotient.com.

ABOUT INFOBLOX

Infoblox enables next-level network experiences with its Secure Cloud-Managed Network Services. As the pioneer in providing the world's most reliable, secure and automated networks, we are relentless in our pursuit of network simplicity. A recognized industry leader, Infoblox has 50 percent market share for core network services comprised of 8,000 customers, including 350 of the Fortune 500.

For more information, visit www.infoblox.com.

THREATQUOTIENT™
11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQuotient.com
Sales@ThreatQuotient.com • +1 703 574-9885