Integration Brief

Enhanced Threat Detection with Infoblox Threat Intel Active Indicators and Stamus Security Platform™

Through integration of the Infoblox Threat intel into Stamus Security Platform, users gain greater threat coverage. It provides BloxOne users the ability to detect threats and unauthorized activity associated with suspicious and known-bad hosts in non-DNS communications.

EXTENDING COVERAGE FOR INFOBLOX THREAT INTEL

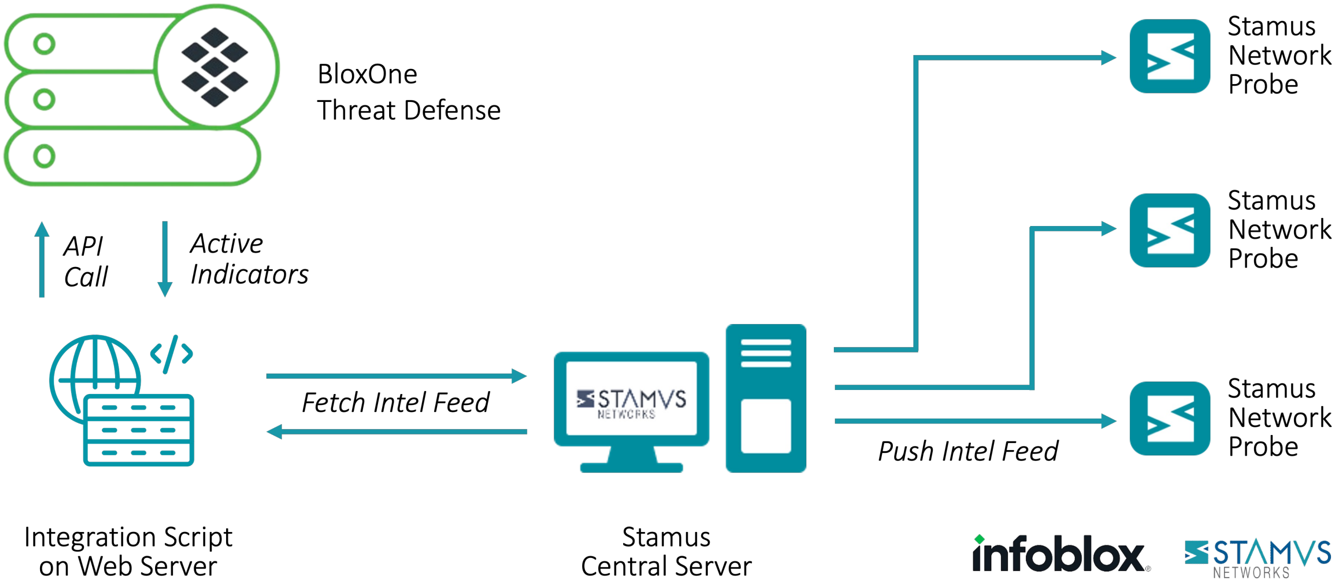
This integration incorporates Infoblox Threat Intel into Stamus Security Platform to identify network communications with dangerous hosts. The integration uses a set of periodic API calls to extract threat intelligence from the BloxOne Threat Defense and update a threat intelligence feed that can be pulled into the Stamus Security Platform.

The integration also includes an optional Declaration of Compromise™ (DoC) definition for SSP which may be used to trigger a notification or an automated response when SSP identifies devices on the network using any protocol to communicate with hosts or domains included in the BloxOne Threat Defense Threat Intelligence feed.

This integration extends the BloxOne Threat Defense user’s threat visibility to the entire network and all common protocols.

INTEGRATION OVERVIEW

This integration uses a script residing on a web server that performs API calls to download the latest Active Indicators, transforming them into a hosted threat intelligence feed for the Stamus Security Platform to ingest them as IOCs (Domain list).



This is performed as a scheduled task (cron job) on a web server on the user's network. SSP periodically retrieves these IOCs on per its configuration. The integration includes custom signatures (rules) to read the IOCs and generate alerts when a network transaction includes access to a domain in the list. These appear in the hunting interface of SSP.

As part of the download process, the indicators are formatted for ingestion into SSP as it would a standard threat intelligence feed. The periodicity of the script's execution is configured using the web server's task scheduler.

The Stamus Central Server (SCS) is configured to retrieve the Active Indicators file by making a call to the URL on the web server where the formatted file is located. Then the SCS will push those indicators to the Stamus Network Probes for use in threat detection.

This is performed as a scheduled task (cron job) on a web server on the user's network. SSP periodically retrieves these IOCs on per its configuration. The integration includes custom signatures (rules) to read the IOCs and generate alerts when a network transaction includes access to a domain in the list. These appear in the hunting interface of SSP.

INTEGRATION BENEFITS

For existing customers of the Stamus Security Platform, this integration brings a powerful new source of up-to-the-minute threat intelligence to identify malicious and unauthorized activity on the network.

For joint customers of Infoblox and Stamus Networks, this integration delivers a more complete picture of organizational engagement with malicious and suspicious hosts identified by Infoblox Threat Intel. For example, by monitoring Active Indicator domain activity on protocols such as HTTP and TLS, Stamus Security Platform can detect and alert on actual connections to a potentially bad domain which bypassed Infoblox DNS query infrastructure.

ABOUT BLOXONE THREAT DEFENSE

BloxOne Threat Defense is a hybrid cybersecurity solution that leverages DNS as the first line of defense to detect and block cyber threats. It bundles Infoblox DNS Firewall, Infoblox Threat Intelligence Data Exchange (TIDE), and Infoblox Dossier. The BloxOne Threat Defense solution combines Infoblox's on-prem and cloud-based security solutions into an integrated hybrid offering that provides enterprises scale, flexibility, and reliability.

Visit Infoblox.com to learn more

ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As defenders face an onslaught of threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. A global provider of high-performance network-based threat detection and response systems, Stamus Networks helps enterprise security teams accelerate their response to critical threats with solutions that uncover serious and imminent risk from network activity. Our advanced network detection and response (NDR) solutions expose threats to critical assets and empower rapid response.

STAMVS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com