Threat STOP

ThreatSTOP Operationalizes RiskIQ Threat Intelligence

Automate inbound and outbound threat mitigation at the network layer using real-time threat intelligence.

The Challenge

Organizations leverage high quality, relevant threat intelligence to investigate threats, monitor their attack surface, and mitigate online brand abuse. Security and network operations teams can recognize greater value from that threat intelligence by operationalizing it - taking rapid and appropriate action based on actionable and timely intelligence. This results in an adaptive, preventative security approach proven to reduce risk, but requires performing a complex and time-sensitive workflow requiring continual intelligence gathering, analysis, decision-making, action, and monitoring.

ThreatSTOP and RiskIQ have partnered to offer an easy to deploy, automated and affordable solution to the challenges of operationalizing threat intelligence. RiskIQ is a leader in digital threat management and a differentiated provider of high quality threat intelligence solutions, and ThreatSTOP's platform operationalizes that threat intelligence, integrating it with appliances like firewalls, routers and DNS servers to automatically harden networks against threats identified by RiskIQ.

The Threat Intelligence

RiskIQ provides world-class intelligence using vast, internet-scale data sets to provide a comprehensive understanding of the fast-moving threat landscape. To do this, advanced data reconnaissance actively captures, normalizes, correlates, and curates petabytes of internet data, RiskIQ then applies machine learning, data science, and research to yield comprehensive intelligence on active threats, issues, exploits, and adversary infrastructure across a complex, dynamic digital landscape.

The Automation Platform

MyDNS is designed to work for any users who value efficient, effective security, and it's especially well-suited for users who work remotely, travel for business, maintain highly-sensitive data on their devices, and individuals with the need to connect to the internet through gateways, such as guest networks, where they lack control over where their DNS traffic is sent, yet require substantial DNS-layer security. of blocking new domains with a manual approach, freeing those skilled resources to focus on other high priorities.

Key Benefits

1. Automatically delivers the latest actionable threat intelligence to network appliances and DNS servers as enforceable security policies.
2. Proactively prevents inbound and outbound communication with attacker infrastructure over IP and DNS at the network layer.
3. Unifies and automates network traffic policy management across multi-vendor appliance environments to enforce uniform security.
4. Provides granular reporting and analytics to visualize and alert on mitigated threats and the host machines involved.

Proactive Security

ThreatSTOP and RiskIQ empower organizations to prevent breaches by blocking inbound and outbound communication with the infrastructure attackers use to carry out attacks – the IP addresses and domains used as infection points, spoofed websites, command and control servers, and as exfiltration points for stolen data. ThreatSTOP's proactive solution to mitigating these threats means security teams can take a preventative approach to securing all users and devices in their networks, including IoT and connected devices where endpoint agents won't work, to block threats before the can become breaches.

The Complete Solution

ThreatSTOP and RiskIQ deliver a complete end-to-end solution for automating the process of blocking harmful or unwanted network connections using actionable threat intelligence data, a workflow known as Operationalizing Threat Intelligence. The ThreatSTOP platform includes customizable policies, broad compatibility with leading network appliances, and robust reporting to detail the protection received while providing visibility into affected host machines to speed remediation. The platform also includes advanced security research tools, extensible API services, and SIEM integration capabilities, offered entirely as a SaaS service.