Anomali for Zscaler

Customized Intelligence for Threat Detection and Response

Cyber threats against the enterprise is growing and getting more sophisticated. Malicious actors conduct campaigns using multiple techniques and are constantly finding new ways to exploit users and their data. Some attacks are targeted specifically to a company or industry and there is a need to identify and block these emerging threats.

Anomali & Zscaler

Zscaler delivers a complete security stack for all users, regardless of whether they are on or off the network. Zscaler employs multiple security techniques to protect the user and data including SSL traffic inspection, sandbox, content and URL filtering and data loss prevention. Zscaler's ThreatLabZ receives global threat intelligence from dozens of sources to investigate and eliminate threats across the Zscaler Security Cloud.

Some enterprises require additional industry specific feeds to augment their threat intelligence. The Anomali Threat Platform automates the process for collecting, managing and integrating threat intelligence from multiple premium feeds. Machine learning is applied to the threat intelligence to give more accurate results.

The Anomali Threat Platform normalizes these disparate sources and enriches it with additional threat context. By utilizing specific threat intelligence for targeted attacks, the Anomali - Zscaler integration helps prioritize and proactively mitigate threats.

Integration Overview

Anomali delivers threat intelligence in real-time to customers via its integration with Zscaler's Cloud Security Platform. Zscaler leverages this high-fidelity intelligence from Anomali to enforce security policies to protect organizations' users and devices.

JOINT SOLUTION BENEFITS

- Automatic blacklisting of Anomali threat intelligence within the Zscaler Platform
- Strengthen Zscaler policy making with integration of Anomali IOCs and threat intelligence.
- Improve visibility and protection across all users on and off network

Anomali's IOCs are enriched with factors such as risk scoring to add context and relevance for the administrator. Administrators define custom filtering policies in Zscaler based on user-defined queries in Anomali. These user-defined IOCs are ingested by the Zscaler Cloud Platform to block a compromise before it starts.
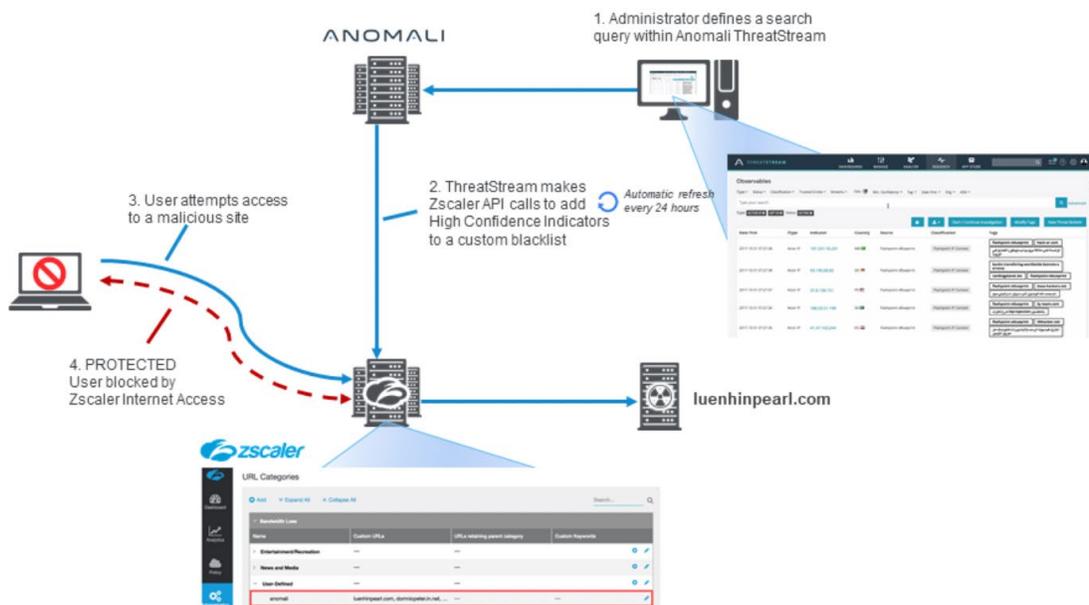
To start receiving high-confidence IOCs and enforcing them in Zscaler, administrators start with the Anomali UI to define a search query. This is followed by the creation of a user-defined URL filtering policy within Zscaler.   Zscaler will start to receive custom intelligence on suspicious domains, IP addresses and URLs, and automatically blacklist these across the Zscaler Cloud Security Platform for all the organization's users, on or off network.

About Zscaler

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100 percent cloud-delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant distributed cloud security platform, protecting thousands of customers from cyberattacks and data loss. Learn more at zscaler.com or follow us on Twitter @zscaler.

About Anomali

Anomali® detects adversaries and tells you who they are. Organizations rely on the Anomali Threat Platform to detect threats, understand adversaries, and respond effectively. Anomali arms security teams with machine learning optimized threat intelligence and identifies hidden threats targeting their environments. The platform enables organizations to collaborate and share threat information among trusted communities and is the most widely adopted platform for ISACs and leading enterprises worldwide. For more information, visit us at www.anomali.com.