Supercharge Zscaler with Augur Predictive Threat Intelligence

With the volume of criminal cyber-attacks faced by today's corporate networks, reacting to threats simply isn't good enough. The focus on playbooks, such as Patient Zero accepts that a threat has managed to infiltrate the organization. Time to detection becomes the key factor, resulting in a race to block attackers from spreading control in the organization. In this model, your SOC team spends its time in a losing battle buried under an avalanche of alerts. Seclytics Augur changes the playbook allowing your team to stop playing defense and taming alert overload.

Looking at Tomorrow to Protect Today

The Augur Predictive Threat Intelligence Platform uses behavioral profiling and advanced machine learning to predict where attacks will originate with high accuracy, on average, 51 days before attacks. While most Threat Intelligence Platforms (TIPs) focus on identifying current threats and alerting your security team, Augur has already predicted these threats and adjusted your security posture to block attacks before they ever get to your network. Augur lowers overall risk and solves alert overload by eliminating the need to react to alerts.

We do this by continually building and monitoring a pool of more than 10,000 adversary profiles. We identify new adversaries almost daily. Continuous surveillance means we know when they go live on day zero, and levels the playing field by removing the element of surprise. Adversary profiles also mean we can cover a much broader spectrum of potential threats from the same actor, as opposed to most TIPs which simply alert you of a specific threat when it's already knocking at your network door. Forewarned is most definitely forearmed.

Seclytics Solution

Seclytics has partnered with Zscaler to provide automated, highly-accurate and actionable, attack predictions integrated directly into the Zscaler platform.
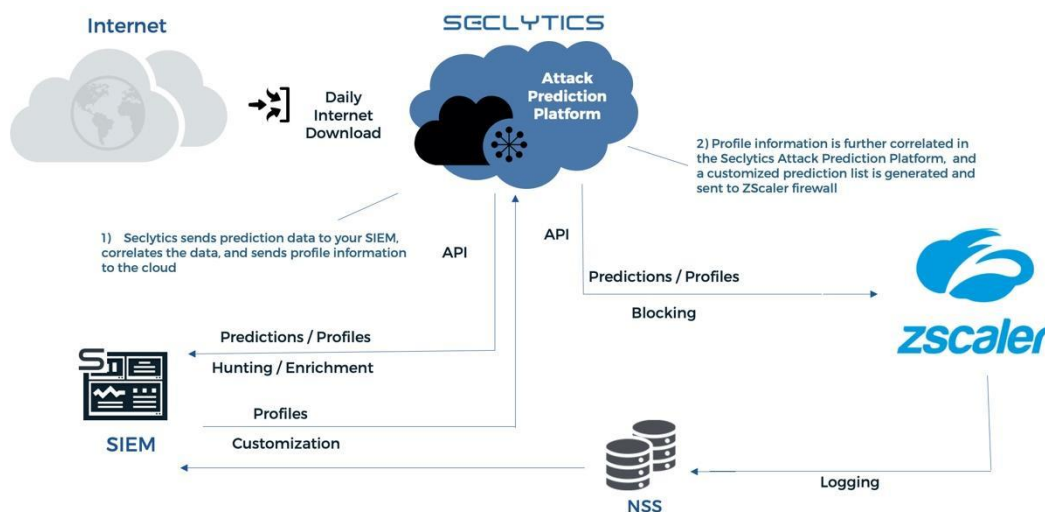
The Seclytics solution consists of two parts working together to provide full detection, reporting, and enforcement.

- Integrating with your SIEM, Augur is able to surface threats seen by Zscaler and highlight events that need to be reviewed immediately. This information is then sent to the Seclytics cloud for correlation and processing to allow us to generate Indicators of Attack associated with future threats specific to your network traffic.

- The customized prediction information, in the form of URL's or IP addresses is pushed to Zscaler via APIs, protecting you against malicious traffic before there is any risk. This data is then continually updated, adjusted based on your security posture.

Integration benefits
- Predictive intelligence protects you from attacks before they are launched
- Seamless integration with SIEM and Zscaler allowing for zero friction installation
- Automated curation of predicted intelligence and enforcement based on your network's traffic
- Threat Intelligence Platform with 160+ feeds to correlate and further research threats in your network.

Seclytics Threat Hunting Dashboard

Augur's Threat Hunting Dashboard provides a powerful and intuitive visualization of threat data and enforcement that provides customer organizations with unprecedented capabilities for viewing and assessing threat data.

In addition, Seclytics provides access to its Threat Intelligence Platform, combining predictive intelligence with data from 160+ different threat intelligence sources, associating them with traffic seen on your network. This allows for advanced investigation measures, providing the ability to further drill down into the details and threat-related context of your incidents.
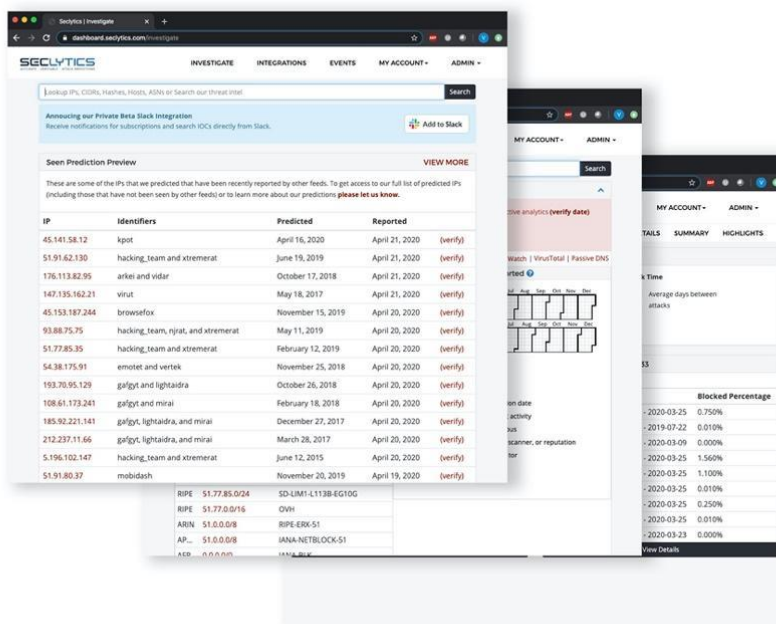
About Seclytics

Founded in 2014, and based in sunny San Diego, California, Seclytics is the leader in Predictive Threat Intelligence. The company's SaaS-based Augur platform leverages behavioral profiling and machine learning to hunt down cybercriminals in the wild. Augur predicts attacks and blocks attackers before they can get to your network. With clients worldwide across all industries, Augur provides fast, easy and reliable integrations with the security ecosystem.

About Zscaler

Zscaler enables organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler cloud-delivered services securely connect users to their applications and cloud services, regardless of device, location, or network, while providing comprehensive threat prevention and a fast user experience. All without costly, complex gateway appliances.