FORTINET | SECLYTICS
ACCURATE · VERIFIABLE · ATTACK PREDICTIONS

SOLUTION BRIEF

Advanced Protection with Fortinet and Seclytics Augur Predictive Threat Intelligence

True Threat Intelligence

Executive Summary

Seclytics Augur is a Predictive Threat Intelligence Platform (TIP) that uses behavioral modeling and machine learning to identify and block threats. Through our integrations with the Fortinet FortiSIEM and FortiGate next-generation firewall (NGFW), Augur can seamlessly integrate into your network and provide advanced protection, allowing your security operations center (SOC) team to stay ahead of cyber criminals and reduce alert overload.

With the volume of criminal cyberattacks 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 this model, your SOC team spends its time in a losing battle buried under alerts and remediating threats, with little true risk reduction. Seclytics Augur changes the playbook.

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 occur. While most 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 manually to alerts.

Get the most out of your Fortinet infrastructure by adding the power of predictive threat intelligence.

Joint Solution Benefits

- Predictive intelligence protects you from attacks before they are launched
- Seamless integration with Fortinet FortiGate and FortiSIEM for easy installation
- Automated curation of predicted intelligence and enforcement based on your network's traffic
- Threat intelligence feed with 160+ feeds to correlate and further research threats in your network

FORTINET
Fabric-Ready

Joint Solution Description

Augur integrates with Fortinet in two ways. Integrating with Fortinet FortiSIEM, Augur curates attack predictions that are fed to FortiSIEM via the cloud-based Augur Attack Prediction Platform. This provides the ability to report on predicted malicious traffic unseen by other security platforms and threat data providers.

Augur is also able to automate enforcement through its integration with the Fortinet FortiGate NGFW. A specifically curated dataset is created and fed into the FortiGate, allowing for seamless enforcement and blocking of predicted malicious traffic before there's any risk to your company.

Diagram of Joint Solution

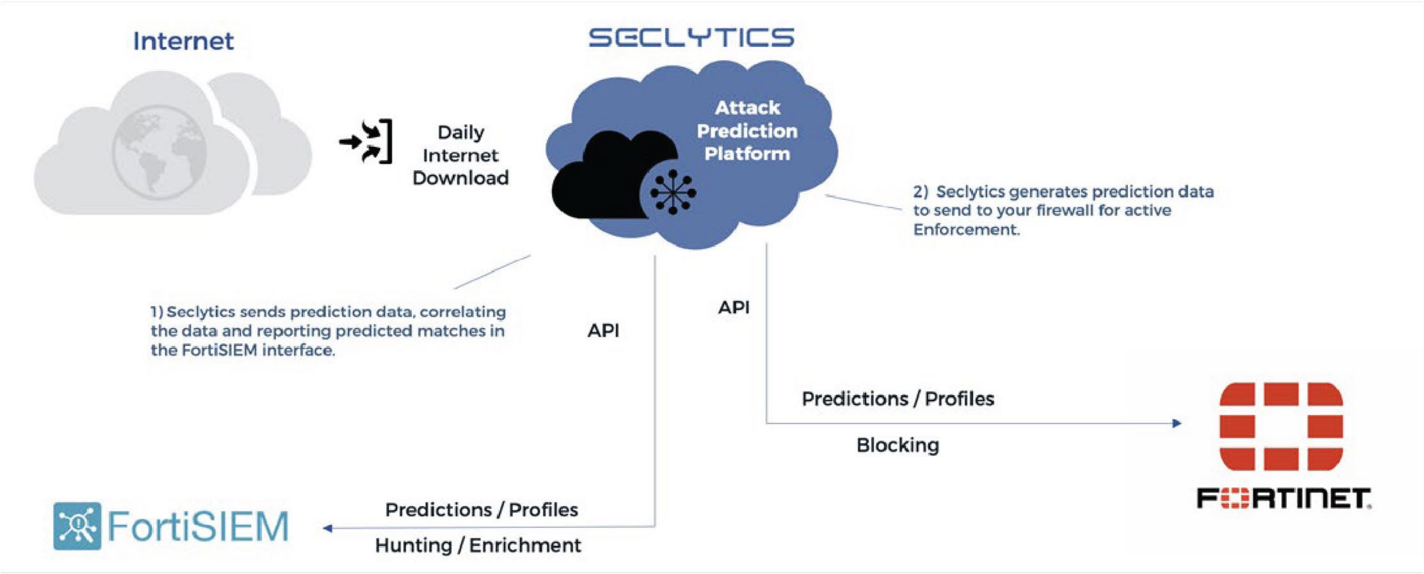

Internet
SECLYTICS
Daily Internet Download
Attack Prediction Platform
2) Seclytics generates prediction data to send to your firewall for active Enforcement.
1) Seclytics sends prediction data, correlating the data and reporting predicted matches in the FortiSIEM interface.
API
API
Predictions / Profiles
Blocking
FORTINET
FortiSIEM
Predictions / Profiles
Hunting / Enrichment

Figure 1: Seclytics / Fortinet integration.

The Augur Predictive Threat Intelligence Platform

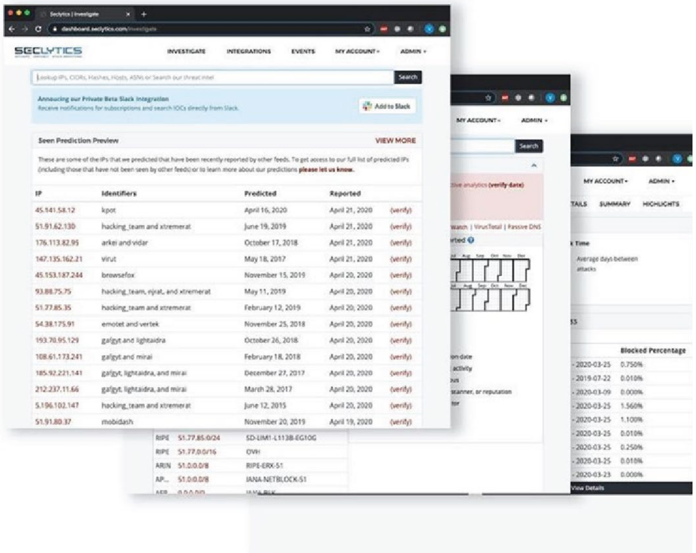
Augur uses machine learning to model the behavior of threat actors and then identify the buildup of attack infrastructure before attacks are ever launched. Making it all work with high accuracy and low false positives is serious patent-pending science.

Augur is continually building and monitoring a pool of more than 10,000 adversary profiles. It identifies new adversaries almost daily. Continuous surveillance means Augur knows when criminal infrastructure goes live on day zero, and levels the playing field by removing the element of surprise. Adversary profiles also mean Augur 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.

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 our proprietary 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.



Annoucing our Private Beta Slack Integration
Receive notifications for subscriptions and search IOCs directly from Slack.

Seen Prediction Preview

These are some of the IPs that we predicted that have been recently reported by other feeds. To get access to our full list of predicted IPs (including those that have not been seen by other feeds) or to learn more about our predictions **please let us know.**

IP	Identifiers	Predicted	Reported	
45.141.58.12	kpot	April 16, 2020	April 21, 2020	(verify)
51.91.62.130	hacking_team and xtremerat	June 19, 2019	April 21, 2020	(verify)
176.113.82.95	arkei and vidar	October 17, 2018	April 21, 2020	(verify)
147.135.162.21	virut	May 18, 2017	April 21, 2020	(verify)
45.153.187.244	browsefox	November 15, 2019	April 20, 2020	(verify)
93.88.75.75	hacking_team, njrat, and xtremerat	May 11, 2019	April 20, 2020	(verify)
51.77.85.35	hacking_team and xtremerat	February 12, 2019	April 20, 2020	(verify)
54.38.175.91	emotet and vertek	November 25, 2018	April 20, 2020	(verify)
193.70.95.129	gafgyt and lightaidra	October 26, 2018	April 20, 2020	(verify)
108.61.173.241	gafgyt and mirai	February 18, 2018	April 20, 2020	(verify)
185.92.221.141	gafgyt, lightaidra, and mirai	December 27, 2017	April 20, 2020	(verify)
212.237.11.66	gafgyt, lightaidra, and mirai	March 28, 2017	April 20, 2020	(verify)
5.196.102.147	hacking_team and xtremerat	June 12, 2015	April 20, 2020	(verify)
51.91.80.37	mobidash	November 20, 2019	April 19, 2020	(verify)

RIPE	51.77.85.0/24	SD-LIM1-L113B-EG10G
RIPE	51.77.0.0/16	OVH
ARIN	51.0.0.0/8	RIPE-ERX-51
AP...	51.0.0.0/8	IANA-NETBLOCK-51

Fortinet FortiGate Enterprise Firewalls

FortiGate NGFWs enable security-driven networking and consolidate industry-leading security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection. Fortinet NGFWs meet the performance needs of highly scalable, hybrid IT architectures, enabling organizations to reduce complexity and manage security risks.

FortiGate NGFWs are powered by artificial intelligence (AI)-driven FortiGuard Labs and deliver proactive threat protection with high-performance inspection of both clear-text and encrypted traffic (including the industry's latest encryption standard TLS 1.3) to stay ahead of the rapidly expanding threat landscape.

FortiGate NGFWs inspect traffic as it enters and leaves the network. These inspections happen at an unparalleled speed, scale, and performance and prevent everything from ransomware to distributed denial-of-service (DDoS) attacks, without degrading user experience or creating costly downtime.

Fortinet FortiSIEM

Security management can be complex for many organizations with the growth in endpoints, Internet of Things (IoT), infrastructure, security tools, applications, VMs, and cloud. FortiSIEM—the Fortinet multivendor security information and event management (SIEM) solution—brings it all together, providing visibility, correlation, automated response, and remediation in a single, scalable solution. Using a business services view, the complexity of managing network and security operations is reduced, freeing resources and improving breach detection. FortiSIEM provides cross-correlation and applies machine learning and user and entity behavior analytics (UEBA) to improve response, to stop breaches before they occur.

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 block attackers before they can get to your network. With clients worldwide across all industries, Augur provides fast, easy, and reliable integrations with many of the most important security solutions. Learn more at https://www.seclytics.com.

June 24, 2020 5:21 AM

D:\Fortinet\Solution Briefs\Grey Solution Brief\Cigent\sb-FA-seclytics-6142020