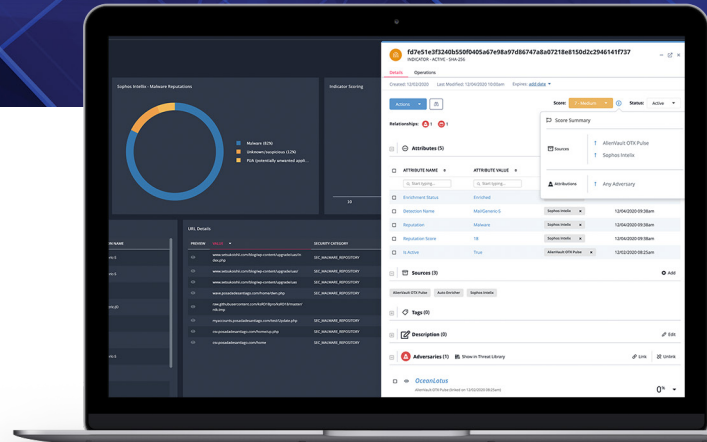


THREATQ™ AND SOPHOSLABS INTELIX

Technology Segment: Intel Feeds

By combining threat intelligence from SophosLabs Intelix and the ThreatQ Platform, organizations are able to enrich imported IOC's with the latest information SophosLabs has to offer on the global threat landscape.



THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ open and extensible platform integrates disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

SOPHOSLABS INTELIX

SophosLabs Intelix™ allows you to take advantage of curated, aggregated, and consolidated threat intelligence built and maintained by SophosLabs (a tier-1 threat research lab). Intelligence is sourced from disparate and complementary data sources with global visibility including intelligence derived from Sophos-protected networks and endpoints. Also, leverage industry-leading SophosAI research into predictive analysis and detection through deep learning artificial neural networks and advanced learning and modelling techniques.

INTEGRATION HIGHLIGHTS

Ingest actionable, relevant threat data directly from SophosLabs

Augment data for files, URLs and IP addresses

Receive detailed analysis reports for files through submission of files to SophosLabs Intelix

INTEGRATION USE CASES

The Integration supports a variety of use cases such as:

- Alert Triage**
 Add more context to the events pulled in from your infrastructure to determine maliciousness.
- Deep Threat Context**
 Add context from SophosLabs Cloud Lookups to IOC's aggregated from other feeds
- Threat Research**
 Understand behavior of files from detailed intelligence reports

Static Analysis Results

- Status: SUCCESS
- Job ID: d54d9164e41594eb31f254577571c2ae
- Request ID: e2ba3e9-c475-46bc-9c79-97de2840242a

General
General information about the submission.

NAME	VALUE
Submission Date	03/04/2021 05:09am
Analysis Type	static
Score	10
Object Type	file

Related Indicators
Indicators that identify the submitted file.

VALUE	TYPE
3395856ce81f2b7382dee72602f798b642f14140	SHA-1
275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f	SHA-256

Reputation
Analysis of the file's reputation, produced by Labs Research.

NAME	VALUE
Score	17
Score String	Malware
Prevalence	Popular
First Seen	02/18/2016 11:08pm

ABOUT THREATQUOTIENT™

ThreatQuotient’s mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization’s existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient’s solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, APAC and MENA.

For more information, visit www.threatquotient.com.

ABOUT SOPHOS

Sophos began producing antivirus and encryption products over 35 years ago. Today our products help secure the networks used by 100 million people in 150 countries and 400,000 businesses. Powered by SophosLabs, our cloud-native and AI-enhanced solutions are able to adapt and evolve to secure endpoints and networks against never-before-seen cybercriminal tactics and techniques. Our products allow you to secure every endpoint of your network, from laptops to virtual desktops and servers, to web and email traffic and mobile devices. What’s more, securing these devices is made possible through products that fit your precise needs. We ensure your network’s security by providing the one thing no one else can: Simplicity.

For more information, visit www.sophos.com.