REGISTER

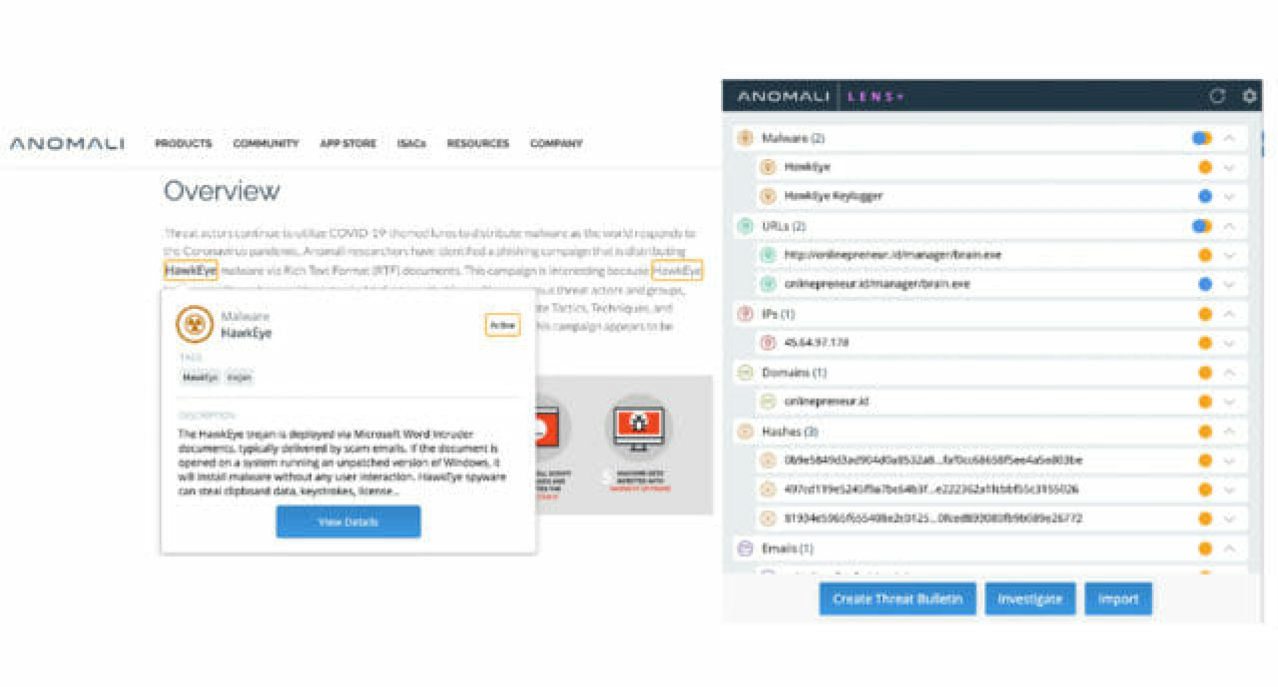
SC Media > Home > Reviews > Anomali

October 31, 2020

PRODUCT INFORMATION

Anomali

★★★★★



Overview

Threat actors continue to utilize COVID-19 themed lures to distribute malware as the world responds to the Coronavirus pandemic. Anomali researchers have identified a phishing campaign that is distributing HawkEye malware via Rich Text Format (RTF) documents. This campaign is interesting because HawkEye ... ous threat actors and groups, ... the Tactics, Techniques, and ... his campaign appears to be

Malware
HawkEye
Active

TAGS
HawkEye trojan

DESCRIPTION
The HawkEye trojan is deployed via Microsoft Word Intruder documents, typically delivered by scam emails. If the document is opened on a system running an unpatched version of Windows, it will install malware without any user interaction. HawkEye spyware can steal clipboard data, keystrokes, license...

Malware (2)
HawkEye
HawkEye Keylogger
URLs (2)
http://onlinepreneur.id/manager/brain.exe
onlinepreneur.id/manager/brain.exe
IPs (1)
45.64.97.178
Domains (1)
onlinepreneur.id
Hashes (3)
0b9e5849d3ad904d0a8532a8...faf0cc68658f5ee4a5e803be
497cd199e5240f9a7be64b3f...e222362a1fcbbf55c3155026
81934e5960f655408e2c0125...0fced89308 0fb9b089e26772
Emails (1)

Vendor: Anomali
Contact: www.anomali.com
Product: Anomali
Price: $50,000

QUICK READ

STRENGTHS: Anomali University serves as an effective knowledgebase full of helpful support documentation and a FAQ list. Lens is a powerful module and the glue of the platform, connecting Match and ThreatStream and therefore uniting the discovery, definition, and ingestion of unstructured intelligence.

WEAKNESS: None that we found.

VERDICT: Overall, security pros will find Anomali a mature, at-scale threat intelligence solution. Administrators and security teams will stop threats more effectively, improve productivity, and reduce the risk of security breaches.

RATING BREAKDOWN

SC Labs Reviews

Reviews from our expert team

Features: ★★★★★	Documentation: ★★★★★
Value for Money: ★★★★★	Performance: ★★★★★
Support: ★★★★★	Ease of Use: ★★★★★

5.00/5

SUMMARY

Anomali correlates millions of indicators of compromise against real-time network activity logs and forensic data to detect and identify adversaries early in the kill chain. This product combines automated intelligence collection, curation, and enrichment to make threat intelligence readily available to security teams. It even gives them all the details they need to detect all threats within an environment, including patient zeros buried within years of log data. Finally, it prioritizes remediations for compromised assets based on a machine learning-based risk and criticality score, empowering teams to address threats without adding to their workloads. The full platform encompasses

ThreatStream, Match, and Lens to operationalize threat intelligence and unite the tools necessary to speed threat detection and provide proactive defense measures.

Match complements ThreatStream and ingests log data from SIEM or logging technologies to automate threat detection, investigation and response with historical comparisons of log data. The comparisons highlight current and historical hosts that have been impacted within the environment. The Match dashboard displays a helpful overview of top impacts according to weighted asset-driven risk scores. Analysts may drill into such scores for additional information regarding threat impact. Security pros can use Match Explorer for proactive responses, providing analysts with the ability to search for information on specific domains and IPs to include Whois lookups and VirusTotal results. Security teams may even use Explorer to compare domain intelligence with log information to locate the patient zeros of known threats using historical data.

ThreatStream automates threat intelligence collection, curation, and distribution, driving the value and actionability of the data. There are many ways to upload data, including Twitter feeds, Anomali feeds, and ThreatStream Community Trusted Circles. The dashboard provides an insightful overview of all the ingested information. Robust data enrichments such as risk ratings and rating confidence scores are found throughout ThreatStream, providing analysts with everything they need for effective threat mitigation.

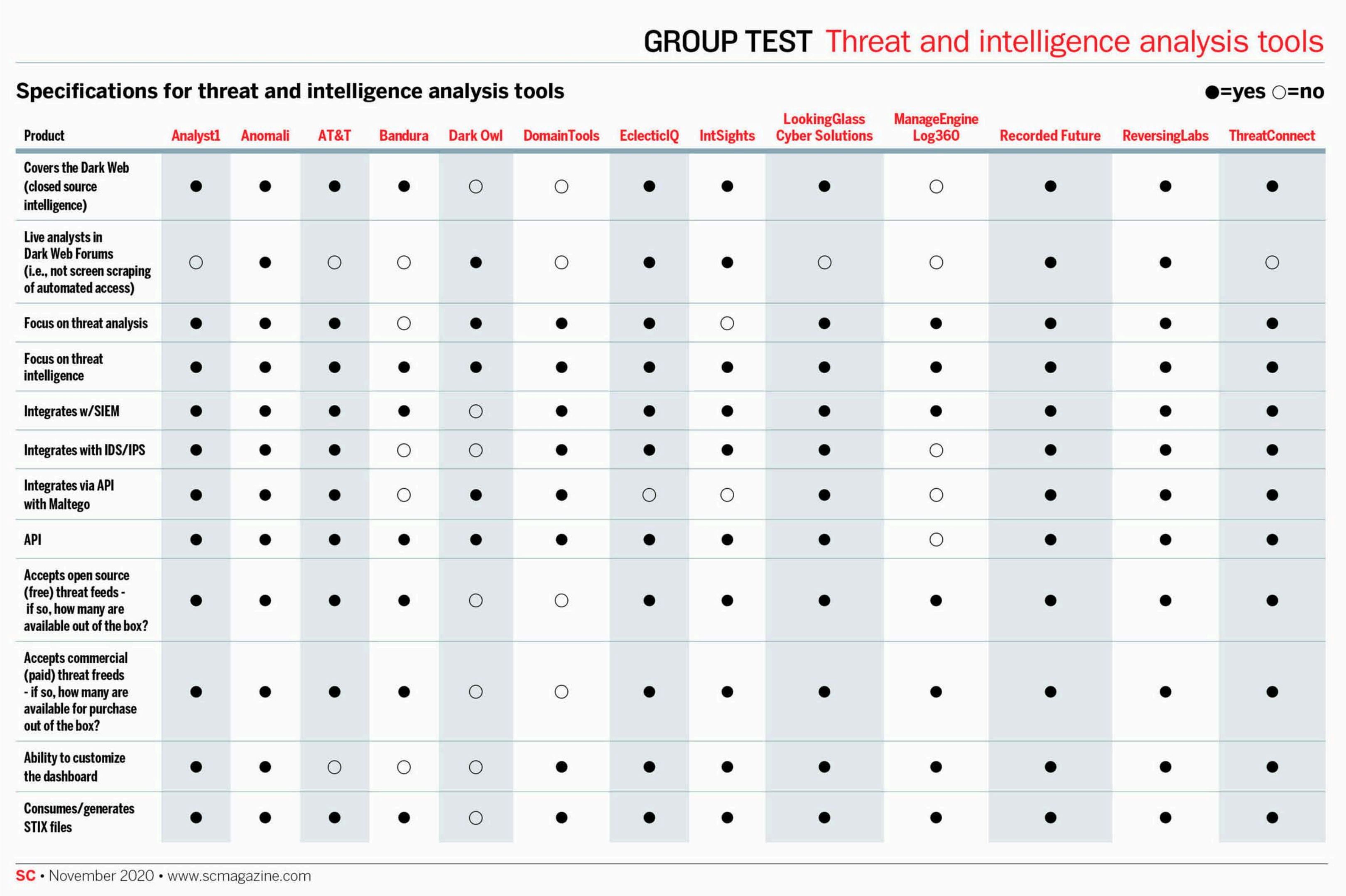
Lens serves as the glue of the platform, connecting Match and ThreatStream and therefore uniting the discovery, definition, and ingestion of unstructured intelligence. Lens is a natural language, processing-based browser plugin that focuses on actual phrasings within a page to locate possible pieces of intelligence instead of exact matches. With Lens, analysts may scan any web page for artifacts and pieces of intelligence, extract this information, compare it to ThreatStream's data repository and Match's historical data, and then differentiate correlations from other intelligence. Hovering over the highlighted information on a page reveals a detailed intelligence breakdown, including a flame icon to emphasize trending topics. Analysts may create a threat intelligence import for all intelligence information not already in the platform.

Overall, security pros will find Anomali a mature, at-scale threat intelligence product. The automation throughout the platform makes this product easy to use. Lens pulls together Match and ThreatStream to maximize efficiency and intuitive use. Match is a particularly valuable component of Anomali because it offers a unique, historical view of threat intelligence without taxing the system or the analyst. With Anomali, administrators and security teams will stop threats more effectively, improve productivity, and reduce the risk of security breaches.

Pricing starts at $50,000 and includes 24/5 phone, email, and website support for the duration of subscription. Users can get additional support for a fee. Organizations also have access to Anomali University, an effective knowledgebase full of helpful support documentation and a FAQ list.

Written by Katelyn Dunn

Tested by Tom Weil



GROUP TEST Threat and intelligence analysis tools

Specifications for threat and intelligence analysis tools

●=yes ○=no

Product	Analyst1	Anomali	AT&T	Bandura	Dark Owl	DomainTools	EclecticIQ	IntSights	LookingGlass Cyber Solutions	ManageEngine Log360	Recorded Future	ReversingLabs	ThreatConnect
Covers the Dark Web (closed source intelligence)	●	●	●	●	○	○	●	●	●	○	●	●	●
Live analysts in Dark Web Forums (i.e., not screen scraping of automated access)	○	●	○	○	●	○	●	●	○	○	●	●	○
Focus on threat analysis	●	●	●	○	●	●	●	○	●	●	●	●	●
Focus on threat intelligence	●	●	●	●	●	●	●	●	●	●	●	●	●
Integrates w/SIEM	●	●	●	●	○	●	●	●	●	●	●	●	●
Integrates with IDS/IPS	●	●	●	○	○	●	●	●	●	○	●	●	●
Integrates via API with Maltego	●	●	●	○	●	●	○	○	●	○	●	●	●
API	●	●	●	●	●	●	●	●	●	○	●	●	●
Accepts open source (free) threat feeds - if so, how many are available out of the box?	●	●	●	●	○	○	●	●	●	●	●	●	●
Accepts commercial (paid) threat freeds - if so, how many are available for purchase out of the box?	●	●	●	●	○	○	●	●	●	●	●	●	●
Ability to customize the dashboard	●	●	○	○	○	●	●	●	●	●	●	●	●
Consumes/generates STIX files	●	●	●	●	○	●	●	●	●	●	●	●	●

SC • November 2020 • www.scmagazine.com

PRODUCT REVIEW

About Product Review

Group Tests

FAQ

Licensing & Product Reviews

USER CENTER

Videos

Executive Insight Guidelines

Subscribe

Editorial Calendar

Media kit

OTHER SC SITES

RiskSec Conference

SC Resource Library

SC Online Events

SC Award