TECHNOLOGY OVERVIEW

How Advanced Investigation Streamlines Your Threat Investigation Approach

Get the right information from the right sources without effort

Vectra Security AI-driven Attack Signal Intelligence™ sources comprehensive and relevant logged data from Azure AD, M365 and AWS to detect malicious events and enrich findings so analysts can make informed security decisions. When an in-depth investigation is needed, Vectra Advanced Investigation brings efficiency to forensic practices. This helps analysts get answers and evidence without pivoting between multiple tools and eliminates time-consuming tasks that require sourcing and synthesizing large disparate data, which is the case with SIEMs. In addition, Advanced Investigation empowers security teams to:

- Remove manual tasks needed to execute queries, parse data and draw relationships between adjacent incidents.
- Drive forensics across datapoints to speed investigation and hunting.
- Confidently confirm threats to determine risk and response.
- Simplify access to Azure AD, M365 and AWS CP data, formatted and searchable.

Key Benefits

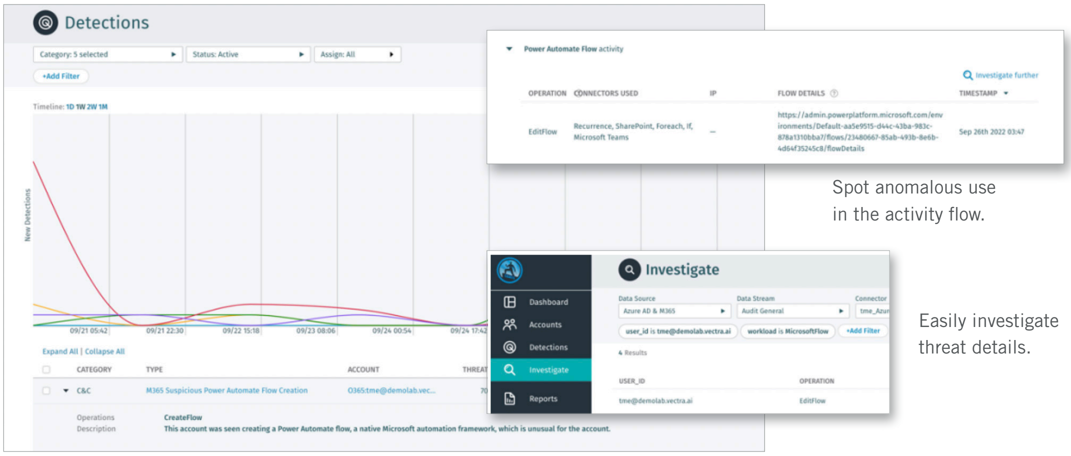
- Simplifies manual tasks
- Drives forensic processes
- Provides richer contextualization
- Reveals similar and unseen tactics
- Provides security incident details

Reduce investigator fatigue and ensure no threat is left behind

Advanced Investigation simplifies the investigator's toolset and reduces delays common to the investigation process. It allows analysts to easily contextualize broader activity surrounding detections and uncover hidden footprints. Tactical efforts to investigate flagged alerts and hunt for malicious threats are driven through Vectra's automated forensic processes that reduces the time it takes to get quality and meaningful information — even for the most critical incidents and assets.

- **Advanced Investigation draws on Attack Signal Intelligence** to pinpoint searchable logged information and meta data, freeing analysts from identifying and connecting reliable and relevant data sources.
- **Automatically translates volumes of event information** into a story so you fully understand what is currently unfolding and what happened in the past.
- **Exposes deeper related activity** without human effort or knowledge to reveal specific data that is compromised, the actions threat actors are taking and anything else that has been impacted at scale.
- **Facilitates investigation from a single interface** covering multiple indexes and quick filters with default settings, so exploring logs with depth becomes effortless.
- **Immediately surface evidence** that confirms suspicious incidents and account activity including object calls, request parameters, activities in specific periods of time, relationships between instances and the history across other M365 services and AWS entities.
- **Analysts know if exfiltration happens** and which files were impacted.

Detection events can be quickly remediated.



CATEGORY	TYPE	ACCOUNT	THREAT
C&C	M365 Suspicious Power Automate Flow Creation	O365:tme@demolab.vec...	70

Operations: CreateFlow

Description: This account was seen creating a Power Automate flow, a native Microsoft automation framework, which is unusual for the account.

OPERATION	CONNECTORS USED	IP	FLOW DETAILS	TIMESTAMP
EditFlow	Recurrence, SharePoint, Foreach, If, Microsoft Teams	–	https://admin.powerplatform.microsoft.com/environments/Default-aa5e9515-d44c-43ba-983c-878a1310bba7/flows/23480667-85ab-493b-8e6b-4d64f35245c8/flowDetails	Sep 26th 2022 03:47

USER_ID	OPERATION
tme@demolab.vectra.ai	EditFlow

Spot anomalous use in the activity flow.

Easily investigate threat details.

Cloud threat detection and response simplified

Only Vectra offers cloud detection and response with capabilities that streamline your threat investigation practice, to reduce the complexity of researching alerts, threat hunting, incident analysis and historic lookbacks. This allows analysts to gather evidence centrally, understand the threats faced, and initiate the right responses with less time and human effort involved.

Getting started is easy. See the walk through and download, the quick start guide

Vectra SaaS Advanced Investigations QuickStart Guide

Vectra SaaS Advanced Investigations QuickStart Guide

Version 1.3

Table of Contents

© 2022 Vectra AI, Inc.

About Vectra

Vectra® is the leader in hybrid cloud threat detection and response. Vectra's patented Attack Signal Intelligence detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.

For more information please contact us:
Email: info@vectra.ai | vectra.ai