ANOMALI®

Microsoft

GET ACTIONABLE THREAT DETECTION

Enrich and accelerate your threat detection, alerting, and response capabilities with Anomali Match and Microsoft Azure Sentinel

MATCH AND SENTINEL JOINT SOLUTION FEATURES:

- Combines Sentinel's ability to aggregate data from all sources -- users, applications, servers, devices in the cloud or on-premises -- with Match's continuous correlation of all event and log data against millions of global IOCs
- Exposes previously unknown adversaries that have already penetrated your network
- Allows instantaneous retrospective analysis of your event logs and your threat intel going back years

ENHANCES YOUR AZURE SENTINEL SIEM TO:

- Correlate logs with millions of threat intelligence records imported into Anomali Match to create detection alerts
- Export the alerts created by these matches back into Azure Sentinel in the form of Common Security (CEF) logs, and then create incidents on top of them for triage by the Security Operations Center (SOC) analyst team

PUT YOUR LOGS AND YOUR INTEL TO WORK AT SCALE

Anomali Match is a high-performance threat detection and response solution that continuously correlates all collected security event and log data from Azure Sentinel and other sources against millions of globally observed indicators of compromise (IOCs) to expose previously unknown adversaries that have already penetrated your network. Match retrospective analysis looks back as far as five years.

The integration allows a powerful bi-directional flow of data between Azure Sentinel and Match. Azure Sentinel users can now export log data out of Sentinel into Anomali Match by simply registering an application in the Azure Active Directory. Once the log data is imported into Anomali Match, it is correlated against the threat intelligence also stored in Anomali Match and generates alerts as matches are identified. These alerts can then be pushed back to Azure Sentinel using a CEF over Syslog collector. This allows importation of high fidelity alerts from Anomali Match into the Common Security table of Azure Sentinel, from where customers can generate incidents using simple KQL-based scheduled rules for making them available for triage in Azure Sentinel.

FIND THREATS FASTER

Match works with Sentinel to capture and automatically, continuously correlate all of your historical event logs, asset data, and active threat intelligence to power comprehensive threat detection and response, resulting in faster Mean-Time-To-Detection (MTTD), reduced cost of security incidents, and more efficient operations.

SEE ALERTS BY PRIORITY

Triaging high volumes of alerts and prioritizing them for investigation and response is an ongoing challenge for SOC analysts. See alerts by priority, review only relevant log data, analyze a timeline of events to find "patient zero", and alert incident response systems for remediation.

INVESTIGATE BY TECHNIQUES

Identify threats in your environment based on TTPs, as well as actors, campaigns, threat bulletins, and vulnerabilities. Search for intrusions in your environment by threat actor, threat bulletins, campaign, or vulnerability, and analyze the techniques for a selected actor in the MITRE ATT&CK framework heatmap.

CASE STUDY:
HAVE WE BEEN IMPACTED?

CHALLENGE:

When a new threat is discovered in the wild, searching back through historical logs to find out if you were compromised can be a long and expensive process.

SOLUTION:

Match tells you in seconds if a threat indicator was present in your historic event data months or years in the past.

- Search historical event logs going back five years or more
- Search for threat indicators, Mitre Attack techniques, actors, vulnerabilities, or threat bulletins
- Return all threat matches in seconds
- Deliver these matches to Sentinel, or your ticketing or SOAR solution

CUSTOMER BENEFIT:

Get to answers quickly and easily identify if you've been impacted by a specific actor or campaign.

CASE STUDY:
PRIORITIZED RESPONSE BASED ON RISK SCORE

CHALLENGE:

Once you've identified malicious behavior in your network, it can be a challenge to decide which threats are the most important to deal with first.

SOLUTION:

Anomali Match integrates asset and vulnerability scan data into your threat detection results, allowing your analysts to prioritize remediation based on risk.

- Identify the top assets that show malicious activity at a glance
- Prioritize response based on risk score and asset criticality
- Track malicious activity back to the original point of intrusion and review a timeline of compromise.

CUSTOMER BENEFIT:

Instead of looking for needles in a haystack of millions of alerts, know which are the highest priority needing investigation and response first.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI®

Copyright © 2021 Anomali