USE CASE

ANOMALI

Empowering Vulnerability Analysis/ Resolution with Natural Language

Natural Language Search with Anomali Copilot

Anomali Copilot allows security analysts to perform complex queries using natural languages to analyze newly reported threats, determine vulnerabilities, and deliver insights in minutes. This use case describes the use of Copilot's cloud-native natural language processing (NLP) capabilities for:

- Simplifying and accelerating cybersecurity log analysis
- Building and retaining a cybersecurity workforce

Why cybersecurity needs natural language

Traditional query languages are designed to be precise and powerful, but they come with a steep learning curve. Cybersecurity logs are rich with data points, from IP addresses and timestamps to user activities and system errors. Crafting queries to extract meaningful insights from this data requires a deep understanding of both the query language and the underlying data structure. This complexity often leads to several challenges:

Extended training periods

Training new hires to become proficient in these query languages can take months, delaying their ability to contribute effectively.

Increased error rates

Even experienced professionals can make mistakes in crafting queries, leading to missed insights or incorrect conclusions.

Talent retention issues

The necessity of mastering these complex languages while under continuous pressure can deter potential talent and contribute to job dissatisfaction.

Anomali Copilot addresses these challenges by allowing users to interact with data using plain English, French, Spanish, Italian, Arabic, and more than 100 other global languages. Based on a large language model (LLM) trained on the world's largest threat repository, Copilot eases the learning curve for new analysts while helping professionals at all levels work more quickly and easily while avoiding errors.

Simplifying and accelerating cybersecurity log analysis

With Anomali Copilot, even those without a background in query languages can quickly and easily search and analyze logs.

Incident response

Following a suspected breach, an analyst can simply ask, “Show me all failed login attempts from external IPs in the last 24 hours.” The system quickly retrieves and displays the relevant data, allowing the analyst to act swiftly.

Threat hunting

A threat hunter looking for signs of a new malware strain might ask, “Find all instances of unusual file downloads by users in the past week.” The NLP system parses this request and highlights anomalies, enabling proactive threat identification.

Compliance audits

During an audit, a compliance officer could request, “List all access attempts to sensitive files by unauthorized users in the last month.” This natural language query simplifies the process of ensuring regulatory compliance and identifying potential violations.

Building and retaining a cybersecurity workforce

Anomali Copilot can play a crucial role in talent recruiting and retention by incorporating NLP into cybersecurity tasks and workflows.

Accelerated learning curve

New employees can start contributing sooner, as they no longer need extensive training in complex query languages. This rapid onboarding can make cybersecurity roles more appealing to a broader talent pool, including those with less technical backgrounds.

Enhanced collaboration

Natural language queries allow cross-functional teams to collaborate more easily on cybersecurity tasks. For instance, IT staff, compliance officers, and executive management can all access the same data using straightforward queries, fostering a more integrated approach to security.

Focus on strategic tasks

By reducing the time and effort spent crafting queries, cybersecurity professionals can focus more on strategic tasks such as threat mitigation, policy development, and security architecture improvement. This shift can lead to more fulfilling job roles and reduce burnout.

Ongoing professional development

NLP tools can also support continuous learning. As cybersecurity threats evolve, so must the skills of the workforce. NLP-enhanced tools can help professionals stay current with less reliance on technical query skills, allowing them to focus on understanding and addressing emerging threats.

The Anomali Security Operations Platform

Anomali ThreatStream

The world's largest threat repository, Anomali ThreatStream captures raw threat data in real time to power the LLM at the heart of the Anomali Security Operations Platform. IOCs and IOAs are immediately correlated with relevant telemetry to drive actionable insights.

Anomali CoPilot

The integrated generative AI capabilities of CoPilot makes our Security Operations Platform the fastest and most comprehensive solution in the market. Based on an LLM using the industry's largest threat repository, CoPilot mitigates hallucinations for accurate, actionable insights in plain language.

Anomali Security Analytics

Built in the cloud for massive scale and speed, Anomali Security Analytics consolidates SIEM, SOAR, UEBA, and TIP capabilities into a best-in-class, AI-driven solution at a fraction of the cost of competing offers.

Anomali ASM

Anomali Attack Surface Management provides comprehensive visibility into all your IT assets, including shadow IT, to fuel actionable security analytics. Real-time monitoring flags outdated policies, misconfigured assets, and other at-risk entities.

Anomali is headquartered in Silicon Valley and is the Leading AI-Powered Security Operations Platform that is modernizing security operations. At the center of it is an omnipresent, intelligent, and multilingual Anomali Copilot that automates important tasks and empowers your team to deliver the requisite risk insights to management and the board in seconds. The Anomali Copilot navigates a proprietary cloud-native security data lake that consolidates legacy attempts at visibility and provides first-in-market speed, scale, and performance while reducing the cost of security analytics. Anomali combines ETL, SIEM, XDR, SOAR, and the largest repository of global intelligence in one efficient platform. Protect and drive your business with better productivity and talent retention.

ANOMALI