ANOMALI

Q & A

Anomali Agentic AI Q&A

1. **What is the Copilot Agentic Widget?**

   The Copilot Agentic widget is an AI-powered chat tool embedded in Anomali dashboards. It provides security analysts with insights into threat hunting, enrichment, integrators, and dashboard data analysis. It summarizes dashboard panels, explains results, and communicates its reasoning transparently using a Chain-of-Thought process.

2. **How does Copilot improve analyst productivity?**

   Copilot Agentic widget reduces the time analysts spend switching between dashboards, running manual searches, and correlating data. This allows teams to investigate and resolve threats faster with fewer resources.

3. **What impact does Copilot have on decision-making?**

   Copilot explains its reasoning and data sources, giving leaders and analysts confidence in the insights and ensuring decisions are based on transparent, validated intelligence.

4. **What types of Use Cases does Copilot support?**

   - Reports on IOCs: Generate summaries on observables like URLs, file hashes, domains, IPs, and emails.
   - Threat Intelligence Enrichment: Use Anomali ThreatStream and external sources to enrich dashboard data.
   - Trending Threat Entities: Retrieve insights into malicious actors, malware, CVEs, and attack patterns.
   - Threat Management Support: Help SOC analysts monitor and respond to threats using aggregated intelligence.
   - Internet Search: Extend knowledge to non-cybersecurity queries when required.

5. What are the key features of Copilot?

- Interactive chat inside dashboards (no context switching)
- Agentic tool selection to deliver the best answer based on query content
- Dashboard-first logic ensures context is grounded in your data before external lookups.
- Clear transparency through the Chain-of-Thought process.
- Context preservation within a session (not across sessions).
- Summarization of dashboard data and trends.
- Ability to perform advanced analysis by asking follow-up questions.

6. How does Copilot assist with Threat Intelligence?

Copilot ingests and analyzes contextual, relationship, and workflow information for entities such as actors, malware, infrastructure, observables, and vulnerabilities. It provides:

Details:

- Information on threat actors and their TTPs.
- Automated enrichment from ThreatStream and external sources.
- Identification of threats for proactive management.
- Support for centralized threat intelligence use.
- Importantly, dashboard data is always prioritized first, ensuring that enrichment and external data are only layered when necessary.

7. Can Copilot help me compare and analyze dashboard panels?

Yes. For example, if you ask how the “Top 10 Actions” panel relates to “User by Category,” Copilot can explain differences—such as one showing behavior trends while the other focuses on system interactions.

8. How does Copilot provide transparency in its answers?

Copilot employs a Chain-of-Thought process, which reveals the sources and reasoning it uses when answering questions. This ensures analysts understand how conclusions are drawn and can trust the AI’s outputs.

9. How does Copilot decide which tool or data source to use when answering my questions?

Copilot operates agentically and intelligently selects the best tool or source depending on the question.

Details:

- Highest Priority: Copilot always prioritizes the dashboard data in the current session as its main source of truth.
- ThreatStream Intelligence – for contextual threat data, IOCs, and TTPs.
- External Intelligence Sources (e.g., VirusTotal) – for enrichment and validation.
- Internet Search – for general or non-cybersecurity queries that cannot be resolved through ThreatStream.
- This adaptive approach ensures users always get the most relevant and authoritative response.

10. Can I use multiple Copilot widgets in a single dashboard?

No. Each dashboard can only contain one Copilot widget.

11. How can I add and customize Copilot in a dashboard?

You can add Copilot as a panel in the dashboard and customize it with the following options:

Details:

- Panel Title – appears at the top.
- Description – supports Markdown and links, shown as tooltips.
- Transparent Mode – display without a background.
- Show Description Toggle – control whether descriptions appear under titles.

© Copyright 2025 Anomali Incorporated®. All rights reserved. ThreatStream® is a registered trademark of Anomali Inc.
Anomali Match™ (“Match”), Anomali Lens™ (“Lens”), and Anomali Copilot are trademarks of Anomali Inc.