

IBM Introduces New Generative AI-Powered Cybersecurity Assistant for Threat Detection and Response Services

New advancements built on watsonx empower IBM Consulting security analysts to help clients accelerate alert investigation



ARMONK, N.Y., Aug. 5, 2024 /PRNewswire/ -- IBM (NYSE:IBM) announced today the introduction of generative AI capabilities to its [managed Threat Detection and Response Services](#) utilized by IBM Consulting analysts to advance and streamline security operations for clients. Built on IBM's watsonx data and AI platform, the new IBM Consulting Cybersecurity Assistant is designed to accelerate and improve the identification, investigation and response to critical security threats.

In addition to being included in IBM Consulting's threat detection and response practice, the Cybersecurity Assistant will be part of [IBM Consulting Advantage](#), the AI services platform with purpose-built AI assets designed to empower IBM consultants to deliver value for clients with consistency, repeatability, quality and speed.

"As cyber incidents evolve from immediate crises to multi-dimensional and months-long events, security teams are facing the enduring challenge of too many attacks and not enough time or people to defend against them," said Mark Hughes, Global Managing Partner of Cybersecurity Services, IBM Consulting. "By enhancing our Threat Detection and Response services with generative AI, we can reduce manual investigations and operational tasks for security analysts, empowering them to respond more proactively and precisely to critical threats, and helping to improve overall security posture for clients."

IBM's [Threat Detection and Response \(TDR\) Services](#) can automatically escalate or close up to 85% of alerts¹; and now, by bringing together existing AI and automation capabilities with the new generative AI technologies, IBM's global security analysts can speed the investigation of the remaining alerts requiring action. Specifically, the new capabilities helped reduce alert investigation times by 48% for one client. The new Cybersecurity Assistant delivers the following:

Accelerate threat investigations and remediation with historical correlation analysis

The Cybersecurity Assistant is designed to help speed up complex threat investigations via historical correlation analysis of similar threats. Built into IBM's TDR Services, the new capability cross-correlates alerts and enhances insights from SIEM, network, EDR, vulnerability and telemetry to provide a holistic and integrative threat management approach.

By analyzing patterns of historical, client-specific threat activity, security analysts will be equipped to be more proactive and precise. To help them better comprehend critical threats, analysts will have access to a timeline view of attack sequences, helping them to better comprehend the issue and provide more context to investigations. The assistant will also auto-recommend actions based on the historical patterns of analyzed activity and pre-set confidence levels, speeding response times for clients and helping to reduce attackers' dwell time. With the ability to continuously learn from investigations, the Cybersecurity Assistant's speed and accuracy is expected to improve over time.

Streamlined operational tasks with an advanced conversational engine

The Cybersecurity Assistant includes a generative AI conversational engine that provides real-time insights and support on operational tasks to both clients and IBM security analysts. In addition to responding to requests such as opening or summarizing tickets, the conversational feature can automatically trigger relevant actions, including running queries, pulling logs, command explanations or enriching threat intelligence. By explaining complex security events and commands, the TDR Service can help reduce noise and boost overall SOC efficiency for clients.

"With IBM's advancements to its managed security services, businesses can gain a new level of insight into critical threats and benefit from technology that continuously learns from actions taken within their specific environment. This helps drive a cycle of increasingly accurate and rapid threat investigations, which is especially crucial today as businesses face a shortage of security resources and surplus in security risks and vulnerabilities," said Craig Robinson, a Research Vice President for IDC's Security Services Research Practice.

Built in collaboration with IBM Research, the new IBM Consulting Cybersecurity Assistant takes advantage of IBM's broader generative AI capabilities – built on the company's Granite foundation models, refined for production within IBM watsonx.ai, and tapping into IBM watsonx Assistant for the conversational chat interface.

Additional Sources

- Visit [here](#) for more information on IBM TDR Services
- [Inquire](#) about a no-cost threat management workshop
- [Join our webinar](#), "Leveraging Security AI and Automation to mitigate the impact of data breaches," on Tuesday, September 17 at 11:00 a.m. ET

About IBM

IBM is a leading provider of global hybrid cloud and AI, and consulting expertise. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs, and gain the competitive edge in their industries. More than 4,000 government and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and consulting deliver open and flexible options to our clients. All of this is backed by IBM's long-standing commitment to trust, transparency, responsibility, inclusivity and service.

¹ Based on IBM's internal analysis of aggregated performance data observed from engagements with 340+ clients in July 2023. Up to 85% of alerts were handled through automation rather than human intervention, using AI capabilities that are part of IBM's Threat Detection and Response service. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided.

Media Contact:

Joel Rushing

Joel.Rushing@ibm.com

SOURCE IBM

<https://stage.mediaroom.com/ibmnewsroom/2024-08-05-ibm-introduces-new-generative-ai-powered-cybersecurity-assistant-for-threat-detection-and-response-services>