Leverage AI for superior security operations efficacy

IBM Consulting Advanced Threat Disposition Scoring (ATDS) AI automates 85% of alert handling leveraging IBM's global view of millions of security incidents

The Advanced Threat Dispositioning Scoring (ATDS) by IBM is a patented security analytics solution designed to enhance cybersecurity operations through the use of artificial intelligence (AI) and machine learning (ML). ATDS is engineered to automatically handle 85% of threat alerts, significantly reducing the time and effort required by human analysts. The system is capable of analyzing vast quantities of threat alerts efficiently, leveraging sophisticated algorithms and continuous model training.

Key Features of ATDS

Observe & Learn: ATDS trains on historical actions taken by IBM security professionals to develop accurate predictive models for future threat dispositions.

Predict & Automate: ATDS recommends appropriate actions for detected threats and executes automatic measures where confidence levels are high, ensuring rapid and precise responses.

Guide & Review: With selectable levels of automation, ATDS can be used to assist analysts by highlighting crucial details and facilitating human investigation, enhancing the overall decision-making process.

Hyperawareness: Utilizing over 1.5 million historical incidents, ATDS provides precise AI insights, drawing data from nearly one thousand companies across 80 industry segments and 211 micro-regional locations.

ATDS employs Generative AI to provide superhuman analysis in human-friendly terms, ensuring transparency and explainability. The system's recommendations are enriched with explainability, confidence scoring, and actionable insights, enabling security analysts to make informed decisions.

The ATDS engine continuously improves with every disposition action, further increasing the number of alerts it can triage with high accuracy. The system's models are audited by expert security analysts, and feedback loops from human analysts enhance the quality of ML recommendations.

ATDS integrates with all major Security Information and Event Management (SIEM) systems, Extended Detection and Response (XDR) and security analytics platforms via a robust API.

ATDS can also be deployed on-premise rather than consumed as a Software as a Service (SaaS) capability.

For more information about ATDS and IBM Cyber Threat Management services, visit:

https://www.ibm.com/services/threat-detection-response