Autonomous Threat Operations Machine (ATOM)

Create an autonomous security operations center (SOC) using agentic AI

Security operations teams have long suffered from alert fatigue, inadequate capacity to handle an increasing alert volume, human bottlenecks, and shortage of skilled personnel. Traditional automation has reached the maximum limit. A paradigm shift is needed, and multi-agentic, autonomous, orchestrated AI security operations is that paradigm shift. ATOM crosses the inflection point between making humans more productive to autonomously delivering security value. SOC teams need to shift from doing tasks to governing AI systems performing the tasks.

Autonomous Threat Operations Machine (aka ATOM) orchestrates multiple AI agents to deliver improved outcomes for security operations. ATOM's alert handling skills go into action when new potential threats are detected, developing an investigation plan and forming the investigation tasks to be dispatched to individual AI agents within the Agentic framework.

ATOM completes most investigations within seconds, receiving the investigation results from the other Agents. Once investigation results are returned, ATOM makes risk decisions informed with the new information and identifies discreet actions needed to respond to the specific threat. ATOM can initiate response actions or return results for human-in-the-loop validation and response, again, all within existing security operations or service management capabilities. If your organization uses multiple languages, ATOM can provide output in the language of your choice, or multiple languages; and for multiple report personas, from a SOC analyst to a Chief Information Security Officer (CISO).

ATOM's investigation skill leverages eight additional AI agents with continued expansion planned of ATOM's skills in threat hunting via IBM's Predictive Threat Intelligence capability, offensive testing, identity management, exposure and vulnerability management.

ATOM works within your security operations tools. ATOM acts as a vendor agnostic digital operator for security analytics solutions from Palo Alto Networks, Microsoft, IBM, and Google as well as front line defense technologies from CrowdStrike, Microsoft and others. Additional Agents can be quickly developed by IBM to give Agentic access to legacy systems, as well as providing a GenAI interface to legacy machine learning AI systems

ATOM is available in multiple consumption models. The fastest way to adopt autonomous AI for your security operations is via IBM's Threat Detection and Response service. This is also the easiest adoption path because IBM delivers turn-key AI enabled security outcomes as well as AI and infrastructure operations. Other adoption options include AI-as-a-Service or on-premise deployment.

Find out more at: ibm.com/services/autonomous-threat-operations

.