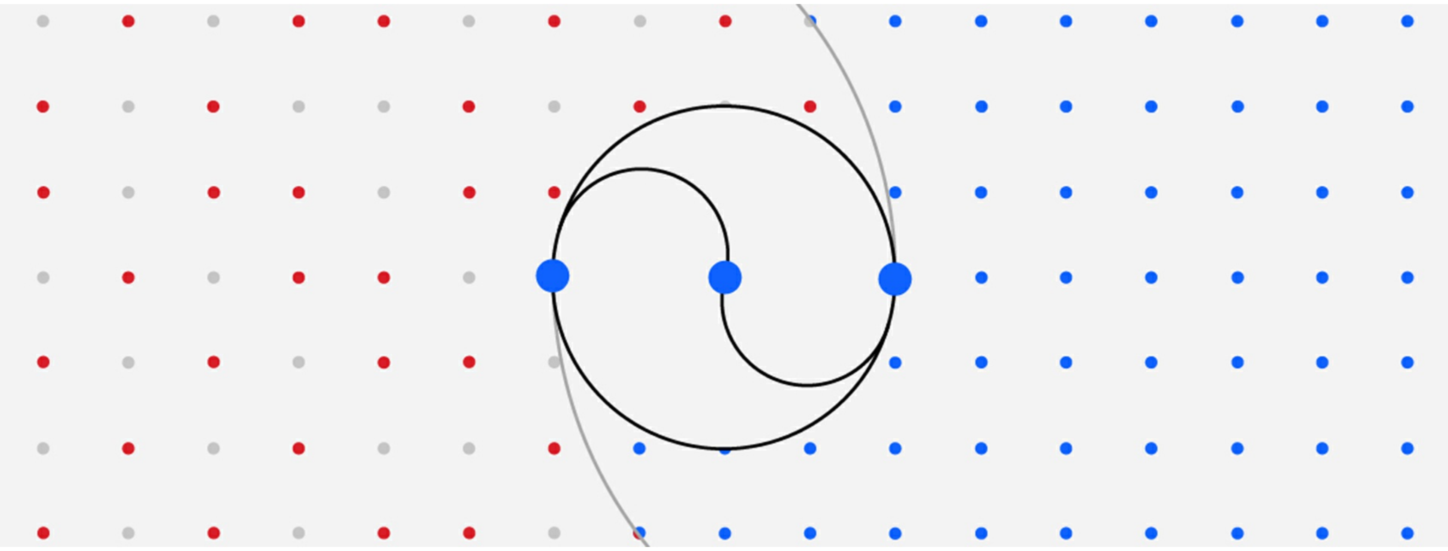
IBM Newsroom

IBM Announces New AI-Powered Threat Detection and Response Services

Ingests and analyzes security data from an extensive ecosystem of technologies and vendors

Offers 24/7 monitoring, investigation and automated remediation of security alerts



ARMONK, N.Y., Oct. 5, 2023 /PRNewswire/ -- IBM (NYSE: IBM) today unveiled the next evolution of its managed detection and response service offerings with new AI technologies, including the ability to automatically escalate or close up to 85% of alerts,[1] helping to accelerate security response timelines for clients.

The new Threat Detection and Response Services (TDR) provide 24x7 monitoring, investigation, and automated remediation of security alerts from all relevant technologies across client's hybrid cloud environments – including existing security tools and investments, as well as cloud, on-premise, and operational technologies (OT). The managed services are delivered by IBM Consulting's global team of security analysts via IBM's advanced security services platform, which applies multiple layers of AI and contextual threat intelligence from the company's vast global security network – helping automate away the noise while quickly escalating critical threats.

"Security teams today are not just outnumbered by attackers, but also by the number of vulnerabilities, alerts and security tools and systems they're tasked with managing on a day-to-day basis," said Chris McCurdy, General Manager, Worldwide IBM Consulting Cybersecurity Services. "By combining advanced analytics and real-time threat intelligence with human expertise, IBM's new Threat Detection and Response Services can augment organization's security defenses with a capability that is scalable, continuously improving and strong enough for tomorrow's threats."

Intelligently Adapting Threat Defenses

The new TDR Services are underpinned by a set of AI-powered security technologies that support thousands of clients across the world, monitoring billions of potential security events per day. It leverages AI models that continuously learn from real-world client data, including security analyst responses, engineered to automatically close low priority and false positive alerts based on a client-defined confidence level. This capability also automatically escalates high risk alerts that require immediate action by security teams and provides investigation context.

IBM's TDR Services are designed to provide:

- **Crowdsourced detection rules, Optimized alerts.** Leveraging real-time insights from IBM's threat management engagements, the new services use AI to continuously assess and auto-recommend the most effective detection rules – helping to improve alert quality, and speed response times. This capability helped reduce low-value SIEM alerts by 45% and auto escalate 79% more high-value alerts that required immediate attention[2]. Organizations can approve and update detection rules with just two clicks through its co-managed portal.
- **MITRE ATT&CK assessment.** To stay prepared for ransomware and wipe-out attacks, organizations will be able to see how their environment is covering MITRE ATT&CK framework tactics, techniques, and procedures as compared to their industry and geography peers. By applying AI, the new services are designed to reconcile the multiple detection tools and policies currently in place at an organization, providing an enterprise view into how to best detect threats and assess gaps to update within an ATT&CK framework.
- **Seamless end-to-end integration.** With its open API approach, the new services can quickly integrate with a client's enterprise-wide security assets, whether on premise or in the cloud. Organizations can continue to access their ecosystem while also having the option to connect and collaborate and define their own response playbooks through a co-managed portal. This provides a unified enterprise view, precise remediation capabilities, and consistently enforces security policies across IT & OT.
- **24x7 global support.** Organizations will have access to more than 6,000 IBM Cybersecurity Services professionals across the globe 24/7 x 365 to help augment security programs. IBM Consulting Cybersecurity Services' vast global network serves more than 3,000 clients around the world – managing more than 2 million endpoints and 150 billion security events per day.

"Security leaders today are trying to escape the vicious cycle of staff shortages, increased threats, and rising demands from the C-Suite to mature their cyber program without breaking the bank. For many organizations the old playbook of swapping out their tools for a vendor's preferred platform does not work, as they cannot afford to write off prior SOC investments," said Craig Robinson, IDC Research VP of Security Services. "A service like IBM's Threat Detection and Response offering can provide an off-ramp to these concerns, without requiring a full rip-and-replace of their prior security investments and help shift their human capital in the SOC to more of a proactive mode."

To support continuous improvement for security operations capabilities, IBM's TDR Services, which are now available, include access to IBM's X- Force Incident Response Services along with the option to include additional proactive security services from IBM X-Force, such as penetration testing, adversary simulation or vulnerability management. X-Force will also provide guidance to help clients improve their security operations over time, based on the current threat landscape, clients' evolving IT environment, and insights gleaned from engagements with thousands of IBM Cybersecurity Services clients around the world.

Additional Sources

- For more information on IBM TDR Services please visit https://www.ibm.com/services/threat-detection-response.

- Sign up for a webinar to learn more about the new TDR Services and the challenges of having a piecemeal approach to detection and response on Wednesday, November 1, 2023, at 11:00 a.m. ET here.

About IBM Security

IBM Security helps secure the world's largest enterprises and governments with an integrated portfolio of security products and services, infused with dynamic AI and automation capabilities. The portfolio, supported by world-renowned IBM Security X-Force® research, enables organizations to predict threats, protect data as it moves, and respond with speed and precision without holding back business innovation. IBM is trusted by thousands of organizations as their partner to assess, strategize, implement, and manage security transformations. IBM operates one of the world's broadest security research, development, and delivery organizations, monitors 150 billion+ security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide.

[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.

[2] Based on IBM's analysis of aggregated annual performance data observed in 2022 from engagements with 150+ Managed SIEM clients. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided.

Media Contact:
Michele Brancati
mbrancati@ibm.com

SOURCE IBM

Additional assets available online: Photos (

https://newsroom.ibm.com/2023-10-05-IBM-Announces-New-AI-Powered-Threat-Detection-and-Response-Services