EINPRESSWIRE

Cyber Experts Foresee Widespread AI Adoption in Security Operations but Lack Clarity on Particular Use Cases

New Adarma Report Highlights the Growing Role of AI and Industry Expectations

EDINBURGH, SCOTLAND, October 17, 2023 /EINPresswire.com/ -- Adarma, an independent leader in detection and response services, has unveiled its latest groundbreaking report titled "A False Sense of Cybersecurity: How Feeling Safe Can Sabotage Your Business." The comprehensive study examines critical aspects of security operations like confidence levels, 'tool sprawl', the integration of artificial intelligence and the overall productivity and well-being of security teams.

Based on a survey* of 500 cybersecurity professionals from UK organisations with over 2000 employees, Adarma has unearthed a wealth of insights regarding the way the industry views the role of artificial intelligence (AI) in security operations. Notably, despite some SecOps leaders not anticipating a significant AI impact in the next five years, a remarkable 61% believe that AI could effectively manage up to 30% of security operations. Even more intriguingly, 17% of respondents foresee this percentage increasing to an impressive 50%. This shift in perspective underlines the growing belief in AI's potential to assist cybersecurity.

While the specific functions AI will undertake within the realm of SecOps remain uncertain, the report highlights the significant room for innovation and advancement in this field. Potentially, AI holds the promise of addressing critical cybersecurity challenges, such as reducing false positives, which in turn will bolster the industry's defence capabilities. However, security professionals are urged to remain vigilant about the source of information and must understand if AI capabilities have been trained on particular data sets and the implications this might have.

Despite an anticipation for its adoption,74% of security professionals struggled to envisage how exactly AI will help them with tasks. AI is still in its infancy, with a lack of expertise, resources and time identified as barriers to the use of both AI and automation.

The report also delves deeper into the role of automation, revealing that security teams uniformly emphasise the importance of automating tasks to improve operational efficiency. Indeed, 53% of respondents expressed a preference for eliminating the time spent on reporting – a task currently among the least automated, as 70% admitted that they don't leverage automation for this. Clearly, this gap presents an opportunity for AI to be deployed in automating reporting and other repetitive or mundane duties, thereby improving the satisfaction, efficiency, and effectiveness of security teams. Furthermore, 42% of security professionals believe that automation will provide superior contextual information, aiding in more informed decision making.

Implementing automation processes, however, is not without its challenges as outlined in the report. While most respondents reported moderate success in the implementation of their automation projects, they did acknowledge the complexity and time-consuming nature of the journey. Specifically, 42% found automation implementation to be challenging and time-intensive, with an additional 21% indicating that it was more demanding than initially anticipated. Nonetheless, an overwhelming majority (73%) attested that the effort invested in automation was worthwhile.

“Artificial intelligence possesses the capacity to enhance detections reducing instances of false positives and enhancing decision-making related to response, including isolation, quarantine and containment. Nevertheless, we must proceed with vigilance. This technology, along with our ability to employ it safely and securely in our organisations, is still in its early stages. We advocate for a watchful oversight of AI and its decision-making processes until we establish confidence and trust in its capabilities. Teams should identify specific domains where AI can provide the most significant advantages and conduct diligent investigation and monitoring to assure that desired results can be achieved. Engage with your workforce to ensure they grasp the potential risks, highlighting that the aim is not to stifle innovation but to comprehend and manage associated risks,” said John Maynard, Adarma’s CEO.

Adarma’s report underscores the transformative potential of AI and automation in the realm of SecOps. The findings provide invaluable insights into the evolving landscape of cybersecurity, particularly in how innovation and adaptability will protect organisations against emerging threats going forward.

Read the full report here: www.adarma.com/a-false-sense-of-cybersecurity

*The survey was completed between the 15th and 22nd of May 2023.

Lara Joseph
Eskenzi PR
+44 7854 841892
lara@eskenzipr.com
Visit us on social media:
Twitter
LinkedIn