# The evolution of AI and automation in security management



The landscape of artificial intelligence and automation within business practices is rapidly evolving, particularly in the realm of security information and event management (SIEM) and security orchestration automation and response (SOAR) technologies. Major players in the market, including IBM, Microsoft, and Palo Alto Networks, are expanding their offerings, utilising AI to enhance functionality and efficiency.

In early 2024, IBM made a significant move by selling its QRadar Software as a Service (SaaS) version to Palo Alto Networks while retaining its on-premises QRadar SOAR solution. This on-premises system boasts support for over 300 third-party integrations visible in its marketplace and provides connectors for IBM's own Guardium and Verify product lines. Notably, QRadar is integrated with IBM's Watson AI-based app development studio, which, when paired with the Playbook Designer, enables the creation of bespoke playbooks and workflows. The application of QRadar has now extended beyond security purposes; it is being utilized in non-security contexts such as employee onboarding and management. IBM's approach to pricing tends to be transparent, with estimations based on the number of authorised users, starting at around £10,000 per year.

In parallel, Microsoft has developed its own dual SIEM and SOAR service known as Microsoft Sentinel. This cloud-native service leverages Azure's analytic capabilities to aggregate data from a broad range of cloud and on-premises sources through various connectors. These include pre-built connectors for Microsoft’s own Defender products and third-party tools such as AWS S3, Google Cloud services, Jira Audit, and Okta, available on the Azure Marketplace. Microsoft offers comprehensive migration guides from other platforms like Splunk and QRadar SOAR, demonstrating a keen interest in attracting users from competitor services. Their automation strategies are enhanced through AI, particularly within Azure's Logic Apps—but perhaps most notably, Microsoft Sentinel is available as a preview version with tier-based pricing structures, allowing clients to sample its capabilities cost-free for the first month under certain conditions.

Palo Alto Networks has been making strides with its Cortex XSOAR platform, which features over 1,000 third-party integrations across security and non-security tools. This diverse integration portfolio covers security, networking, and cloud services originating from the vendor. The XSOAR system utilises AI not only to streamline incident responses but also to intelligently filter out duplicate alerts and reduce false positives. Furthermore, it has expanded its repertoire by incorporating various large language models, such as ChatGPT and others, to adeptly analyse and process incident data.

The advancements in AI automation signal a transformative shift in how businesses operate, particularly within the domains of security and operational efficiency. With these emerging technologies shaping industry standards, the future of automation in business practices continues to evolve dynamically, driven by the innovations of companies like IBM, Microsoft, and Palo Alto Networks.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.channelfutures.com/mergers-acquisitions/palo-alto-networks-completes-ibm-qradar-purchase> - Corroborates the acquisition of IBM's QRadar SaaS assets by Palo Alto Networks and the integration with Cortex XSIAM.
2. <https://www.paloaltonetworks.com/company/press/2024/palo-alto-networks--closes-acquisition-of-ibm-s-qradar-saas-assets> - Provides details on the acquisition of IBM's QRadar SaaS assets by Palo Alto Networks and the partnership for AI-powered security solutions.
3. <https://www.paloaltonetworks.com/company/press/2024/palo-alto-networks--closes-acquisition-of-ibm-s-qradar-saas-assets> - Mentions the retention of IBM's on-premises QRadar SOAR solution and its integrations.
4. <https://www.ibm.com/security/security-intelligence/qradar> - Details IBM's QRadar system, including its support for over 300 third-party integrations and integration with IBM's Watson AI.
5. <https://docs.microsoft.com/en-us/azure/sentinel/> - Describes Microsoft Sentinel, its cloud-native SIEM and SOAR service, and its integration capabilities with various cloud and on-premises sources.
6. <https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources> - Lists the pre-built connectors available for Microsoft Sentinel, including those for Microsoft Defender products and third-party tools.
7. <https://docs.microsoft.com/en-us/azure/sentinel/migrate-from-splunk> - Provides migration guides from other platforms like Splunk to Microsoft Sentinel.
8. <https://www.paloaltonetworks.com/products/cortex/cortex-xsoar> - Details Palo Alto Networks' Cortex XSOAR platform, including its third-party integrations and AI-driven incident response capabilities.
9. <https://www.paloaltonetworks.com/products/cortex/cortex-xsoar/features> - Explains the use of AI in Cortex XSOAR to streamline incident responses and filter out duplicate alerts and false positives.
10. <https://dev.to/td_inc/automation-trends-that-will-impact-your-business-in-2025-1jnb> - Discusses the broader impact of AI automation on business practices, including operational efficiency and innovation.
11. <https://blog.whitehat-seo.co.uk/ai-automation-in-2025> - Provides insights into the strategic implementation and scaling of AI automation in businesses, reflecting the transformative shift in operations.
12. <https://www.csoonline.com/article/3622920/soar-buyers-guide-11-security-orchestration-automation-and-response-products-and-how-to-choose.html> - Please view link - unable to able to access data