

IBM 发布 SIEM 产品路线图

—— 构建下一代企业安全运营中心

2023 年 11 月 23 日 / 北京 / -- 近日，IBM 发布了其下一代 SIEM 产品路线图，旨在帮助企业构建下一代企业安全运营中心（SOC）。该路线图展示了 IBM 如何通过整合其强大的 AI 能力，特别是 watsonx，来提升 SIEM 产品的性能和效率。

IBM 表示，下一代 SIEM 产品将具备以下关键特性：1. 增强的检测能力：利用 AI 技术，能够更准确地识别和检测潜在的安全威胁。2. 简化的调查和响应：通过自动化和智能化的调查工具，缩短安全事件的响应时间。3. 可扩展性：支持大规模部署，适应企业不断增长的安全需求。4. 集成性：与现有的企业 IT 基础设施无缝集成，实现全面的安全覆盖。5. 合规性：满足日益严格的行业法规和标准，降低合规风险。

IBM QRadar SIEM 产品是这一路线图的重要组成部分。它通过整合 IBM Security 的专家知识和 watsonx 的 AI 能力，为企业提供更强大、更智能的安全运营中心解决方案。

IBM Security 高级副总裁 Kevin Skapinetz 表示：“下一代 SIEM 是 IBM 安全战略的核心。通过引入 AI，我们能够显著提升企业的安全运营效率，降低安全风险。QRadar SIEM 正是这一战略的体现，它将帮助企业更好地应对日益复杂的安全挑战。”

IBM 下一代 SIEM 产品路线图展示了 QRadar 产品的未来发展方向。QRadar 产品套件将包括 QRadar Suite 在内的多个组件，为企业提供全面的安全运营中心解决方案。

QRadar SIEM 产品将于 2023 年底作为 SaaS 产品正式推出，并于 2024 年初开始提供本地部署版本。

关于

IBM OpenShift 平台上的 QRadar SIEM 产品，将为企业提供更灵活、更易于部署和管理的解决方案。企业可以通过 OpenShift 平台快速部署和扩展 QRadar SIEM，以满足其特定的安全需求。

- 合作伙伴生态：IBM 将与全球领先的 SIEM 合作伙伴（SIGMA）合作，共同推动下一代 SIEM 产品的研发和部署。
- 客户支持：IBM 将提供全面的客户支持服务，包括培训、咨询和故障排除，确保客户能够顺利使用下一代 SIEM 产品。
- 产品路线图：QRadar 产品路线图将详细展示 QRadar 产品的未来发展方向，包括 QRadar Suite 在内的多个组件。

关于 QRadar SIEM 产品路线图，请访问 [IBM 官方网站](#) 获取更多信息。

QRadar 产品套件包括 QRadar Suite 在内的多个组件。QRadar Suite 是 QRadar 产品的核心组件，提供全面的安全运营中心功能。QRadar Suite 包括 QRadar 调查和响应（ASM）模块，用于调查和响应安全事件。QRadar Suite 还包括 QRadar 事件响应（EDR）模块，用于检测和响应安全事件。QRadar Suite 还包括 QRadar 安全运营中心（SOC）模块，用于集中管理和协调安全运营。

关于 AI 产品路线图，请访问 [IBM 官方网站](#) 获取更多信息。

QRadar SIEM 产品路线图展示了 QRadar 产品的未来发展方向。QRadar 产品套件将包括 QRadar Suite 在内的多个组件，为企业提供全面的安全运营中心解决方案。

- 安全运营中心：通过整合IBM Security QRadar SIEM和IBM Security X-Force®，实现安全运营中心（SOC）的效率提升85%，运营成本降低55%。
- 威胁情报：通过整合IBM Security QRadar SIEM和IBM Security X-Force®，实现威胁情报的实时分析和响应。
- 安全运营中心：QRadar SIEM和X-Force®的结合，为安全运营中心提供全面的安全运营能力。

IBM Security QRadar SIEM 和 IBM Security X-Force® 的结合，为安全运营中心提供全面的安全运营能力。

SOC

IBM Security 2024 年 QRadar SIEM 和 IBM Security X-Force® 的结合，为安全运营中心提供全面的安全运营能力。

- 安全运营中心：通过整合IBM Security QRadar SIEM和IBM Security X-Force®，实现安全运营中心（SOC）的效率提升85%，运营成本降低55%。
- 威胁情报：通过整合IBM Security QRadar SIEM和IBM Security X-Force®，实现威胁情报的实时分析和响应。
- 安全运营中心：QRadar SIEM和X-Force®的结合，为安全运营中心提供全面的安全运营能力。
- 安全运营中心：QRadar SIEM和X-Force®的结合，为安全运营中心提供全面的安全运营能力。

IBM Security 2024 年 QRadar SIEM 和 IBM Security X-Force® 的结合，为安全运营中心提供全面的安全运营能力。

IBM Security 2024 年 QRadar SIEM 和 IBM Security X-Force® 的结合，为安全运营中心提供全面的安全运营能力。

QRadar SIEM 产品链接：<https://www.ibm.com/products/qradar-cloud-native-siem>

AI For Security 产品链接：<https://www.ibm.com/security/artificial-intelligence>

IBM Security 产品链接：<https://www.ibm.com/security>

###

IBM Security

IBM Security 产品链接：<https://www.ibm.com/security> IBM Security X-Force® 产品链接：<https://www.ibm.com/security/x-force> 130 个安全运营中心 1500 个安全运营中心 10,000 个安全运营中心

External Communications

E-mail: kelvin.liu@ibm.com

Mobile: 86-15110254110

Address: 12F, South Tower, CP Center, Building 3, 20 Jinhe East Road, Chaoyang District, 100020, China

2020年3月12日

SOURCE IBM China

Additional assets available online:  [Photos](#) 
 

<https://china.newsroom.ibm.com/2023-11-23-IBM-SIEM>.