

CHECKLIST

11 Tips for Implementing GenAI into Security Operations

Generative AI (GenAI) offers unprecedented opportunities for enhancing security operations (SecOps). Integrating GenAI into your cybersecurity platform reduces the complexity of deciphering threats and helps bridge the cybersecurity skills gap. Take these steps to effectively evaluate and implement GenAI in your SecOps.

- Document GenAI Use Cases**

Create a detailed inventory of all planned GenAI applications within your organization. Identify potential vulnerabilities related to data privacy, security, and compliance. Develop a comprehensive risk-assessment document that outlines these risks and their corresponding mitigation strategies. This document provides a solid foundation for your GenAI initiatives and helps ensure a secure implementation.
- Understand AI Data Management**

Proper data management is crucial for the success of GenAI in SecOps, so document the types of data your AI systems will use. Include their sources, processing techniques, and storage methods. Understanding these aspects helps establish clear boundaries for data usage and ensure compliance with relevant security standards and data privacy regulations. Implementing strict data classifications can further enhance your ability to manage and secure AI data effectively.
- Evaluate External GenAI Risks**

Assessing external GenAI risks involves understanding how third-party AI services may impact your organization. Consider scenarios such as processing your data using external AI-powered tools and their potential dangers. Answering these questions will help you develop a comprehensive risk-management strategy, safeguarding your organization from external threats and ensuring the secure integration of GenAI technologies.
- Create a List of Approved GenAI Tools**

Selecting the right GenAI tools is essential for secure and effective implementation. Evaluate each tool based on its security features, privacy compliance, and ability to integrate with existing systems. Factors such as cost and ease of use also should be considered. Once you have identified the most suitable tools, compile a list of approved GenAI services and ensure this information is clearly communicated within your organization.
- Develop a GenAI Policy**

A comprehensive GenAI policy is critical to guiding its ethical and practical use. This policy should outline standards for the safe deployment of GenAI, including guidelines for transparency and accountability. Ensure that all employees know their responsibilities and the expectations surrounding GenAI usage. Regular updates to this policy will help you stay ahead of evolving technologies and threats.
- Integrate GenAI with Existing Infrastructure**

Seamlessly integrating GenAI capabilities into your current security tools and workflows is crucial for maximizing its benefits. To enhance overall efficiency, focus on embedding GenAI within existing central data and analytics management tools, security information and event management systems, and security orchestration, automation, and response platforms. Develop clear protocols to guide analysts in interacting with GenAI, ensuring they can leverage its capabilities effectively without disrupting existing processes.

✓ **Train Security Personnel**

Provide comprehensive training for your security team on how to use GenAI tools effectively. Ensure the training covers GenAI's capabilities and limitations and develop best practices for utilizing it in daily operations. Training helps ensure that your team is well-prepared to integrate GenAI into their workflows and can maximize its potential while minimizing risks.

✓ **Automate Routine Tasks**

Automating repetitive tasks with GenAI can significantly improve your SecOps efficiency. Identify tasks such as data correlation, report generation, and initial threat assessments that can be automated. This automation will free your analysts to focus on more complex and strategic issues, enhancing productivity and operational efficiency. It will also reduce the risk of human error in these routine tasks, further bolstering your security posture.

✓ **Enhance Threat Investigation and Response**

GenAI can revolutionize your threat investigation and response processes. Use it to analyze alerts and incidents, generate comprehensive escalation summaries, and correlate data from multiple sources. These capabilities will enable quicker and more accurate threat detection and response. With GenAI, your team can respond to incidents more efficiently and effectively, reducing the potential impact of security breaches.

✓ **Optimize Performance Metrics**

Monitoring and optimizing key performance indicators like mean time to detect and mean time to respond is essential for assessing the effectiveness of your GenAI implementation. Continuously evaluate the impact of GenAI on these metrics and adjust your strategies to improve efficiency and ensure robust security operations. Regularly reviewing these metrics will help you identify areas for improvement and ensure that your GenAI integration is delivering the expected benefits.

✓ **Maintain Transparency and Accountability**

Developing and enforcing policies for the ethical use of GenAI is crucial for maintaining trust and accountability. Ensure transparency in AI-driven decisions and actions and establish mechanisms to monitor and review AI-driven outcomes. These practices will build trust within your organization and enhance the credibility of your security operations. Regular audits and reviews will help ensure that your GenAI tools are used responsibly and effectively.

Maximize Your Security Investments

Integrating GenAI with your current security tools can enhance their capabilities without making extensive new investments. This approach optimizes your existing infrastructure's return on investment and ensures that GenAI complements and enhances your security operations for better outcomes.

For example, leveraging solutions like FortiAI can seamlessly integrate advanced AI capabilities into your existing Fortinet infrastructure, providing deeper insights and more effective threat responses without significant additional expenditures.

[Learn more about the AI integration in Fortinet FortiAnalyzer.](#)