



2025 GUIDE

The CISO's Guide to AI

3 Ways to Leverage AI
to Improve Your Data
Security Posture

2025 Guide The CISO's Guide to AI

2025 Guide

The CISO's Guide to AI

Artificial Intelligence (AI): a term that stirs up a blend of awe, confusion, and—in some circles—downright cynicism. If you're a Chief Information Security Officer (CISO) or in a similar role, you're right to approach the AI landscape with a dose of healthy skepticism. Why? Because it's your job to ensure that the promises of AI don't become security pitfalls.

It's frequently hailed as the magical solution to all our cybersecurity woes: automatically detect anomalies, thwart attacks, and surface vulnerabilities you didn't know you had. But like any tool, it's all about how you approach it, where you use it, and how to manage expectations. AI, like everything, has its limitations, vulnerabilities, and yes, it can be exploited.

Here's how to navigate the labyrinthine world of AI from a CISO's perspective.

Cutting Through the Noise: Reduce False Positives with AI

False positives can be the bane of a security professional's existence, diluting the focus from real threats and wasting valuable resources. This noise not only puts a strain on your Security Operations Center (SOC) but can also foster a culture of complacency.

After all, if the majority of alerts end up being false alarms, even the most vigilant teams can become desensitized to them. That's where AI/ML classification comes in. Leverage ML algorithms in your data classification to dramatically reduce the noise created by false positives, improving both the efficiency and efficacy of your cybersecurity efforts.

Use solutions like BigID that bring more depth to data classification: going beyond basic (your typical regular expressions and pattern matching), to layer in additional ML-driven classification that can validate and automatically tune models to your data.

The road to reducing false positives using machine learning isn't straightforward, and it comes with its own set of challenges. However, the effort can yield significant dividends in the form of a more focused, efficient, and responsive data security posture management. Solutions like BigID lead the market with ML-driven data classification that's accurate, tunable, and actionable. By adopting machine learning thoughtfully, you can turn a cacophony of false alarms into a symphony of meaningful, actionable alerts



Leverage ML algorithms in your data classification to dramatically reduce the noise created by false positives, improving both the efficiency and efficacy of your cybersecurity efforts.

The Hidden Risk in Unstructured Data: Harnessing AI for LLMs

You're no stranger to the challenges posed by unstructured data—those miscellaneous files, emails, and text documents that don't fit neatly into structured databases but nonetheless often contain sensitive or critical information. The rise of Language Learning Models (LLMs) like ChatGPT magnifies the importance of this issue.

These advanced models have the capability to analyze and generate human-like text based on the data they've been trained on, but herein lies a subtle yet substantial risk: if the data fed into these models hasn't been properly scrutinized, there's a potential for unintended disclosure or misuse of sensitive information.

To mitigate this risk, it is critical to have robust data handling procedures in place before employing LLMs for any task, be it customer service automation, data analytics, or threat detection. Start by flagging and tagging data that might contain personally identifiable information (PII), confidential business plans, or any other type of sensitive material.

AI-driven data classification like BigID can help - enabling you to easily and accurately tag, label, and flag critical data, while automating a stateful data inventory to drive even more value. Leveraging a solution like BigID to scan, classify, and accurately validate that the data in an LLM is fit for purpose (meaning there's no unapproved sensitive, regulated, secrets, or critical data in there) will reduce the likelihood of data breaches, data leaks, and compliance violations.

As we increasingly rely on sophisticated tools like LLMs, the data that powers them must be handled with an equal measure of sophistication and care. Prioritize flagging, tagging, and classifying unstructured data to ensure that your team is leveraging generative AI responsibly. Leverage ML algorithms in your data classification to dramatically reduce the noise created by false positives, improving both the efficiency and efficacy of your cybersecurity efforts.

Shine a Light on Dark & Shadow Data with AI: Why Visibility is Key to Improved Security Posture

Dark data and shadow data - data that you don't know about and isn't under the right security controls - exponentially amplifies your risk, vulnerabilities, unauthorized access, and potential data leaks and data breaches. After all, you can't protect what you don't know.

Dark data, owing to its sheer volume and the fact that it's often poorly inventoried, presents a rich target for cybercriminals. It may contain sensitive personal information, confidential business strategies, or intellectual property. Since it isn't actively monitored, breaches involving dark data may go unnoticed until it's too late. Similarly, shadow data bypasses your organization's security controls, making it susceptible to a myriad of threats, ranging from data corruption to phishing attacks. Employees might think they're merely being efficient by using unsanctioned apps, but the risks are not transparent to them, and that's a security blind spot.

It's critical to 'shine a light' on both dark and shadow data to improve your security posture. Use AI to automatically uncover and inventory the data that you know and the data that you don't: solutions like BigID can eliminate your blind spots. Use BigID to automatically discover data across the cloud, uncover dark data, and validate your data inventory to understand what data you have, how sensitive it is, and leverage native controls on that data to reduce risk.

In a cybersecurity landscape where visibility equates to control, letting dark and shadow data proliferate unchecked is tantamount to navigating a minefield blindfolded. By uncovering these hidden corners of your data ecosystem, you can better defend against the threats that lurk in the shadows.

How to Adopt AI Into Your Security Strategy

As with any tool, its effectiveness in cybersecurity depends on how well it is wielded. In the right hands, AI can be a formidable asset in your cybersecurity arsenal. But remember, it's just one piece of the puzzle.

Leverage solutions like BigID that take a defense-in-depth approach to automating manual processes, improving accuracy and actionability, and applying AI & ML to cut through the noise, improve risk management, and enable a robust data security strategy.

About BigID

BigID helps organizations connect the dots across data & AI: for security, privacy, compliance, and AI data management. BigID enables customers to find, understand, manage, protect, and take action on high risk & high value data, wherever it lives.

Customers use BigID to reduce their AI & data risk, automate security and privacy controls, achieve compliance, and understand their data throughout their entire data landscape: from the cloud, on-prem, and everywhere in between.

Connect the Dots Across Data & AI

Security • Compliance • Privacy • AI Data Management

Reduce risk, accelerate time to insight, and get data visibility and control across all your data - everywhere.

“**Tools like BigID are the future.**

Organizations should be leveraging these tools to remove the manual processes from data discovery, provide better visibility, and help with prioritization of controls.



Ryan O’Leary

Future of Trust: Battling Data Discovery Confusion