RAGe Against the GRC Machine

AI-Powered Compliance

Brennan Lodge

Founder, BLodgic

April 9, 2026

Brennan.Lodge Whois Lookup

- **Role**: Co-founder and CISO
- **Experience**:
  - Over 15 years in financial services focusing on cybersecurity, data science, and leadership.
  - Previous affiliations include **JP Morgan Chase**, **Federal Reserve Bank of New York**,
  - **Bloomberg**, Goldman Sachs, and **HSBC**.
  - Led AI-centric cyber solutions at HSBC, streamlining cybersecurity processes.
  - **Professor at NYU**, Information Tech Management & Data Analytics.
  - Technical advisor roles at CounterFlow AI, Inc. and DataKind.
  - Award winning researcher
  - LinkedIn learning instructor on RAG & MCP + AI Automation

AI for Global Goals

ML x Cases Finance/ESG competition winner 2023

US Cyber Command AI RPE winner 2022

BLODGIC

All views are my own and not of my employer

Agenda

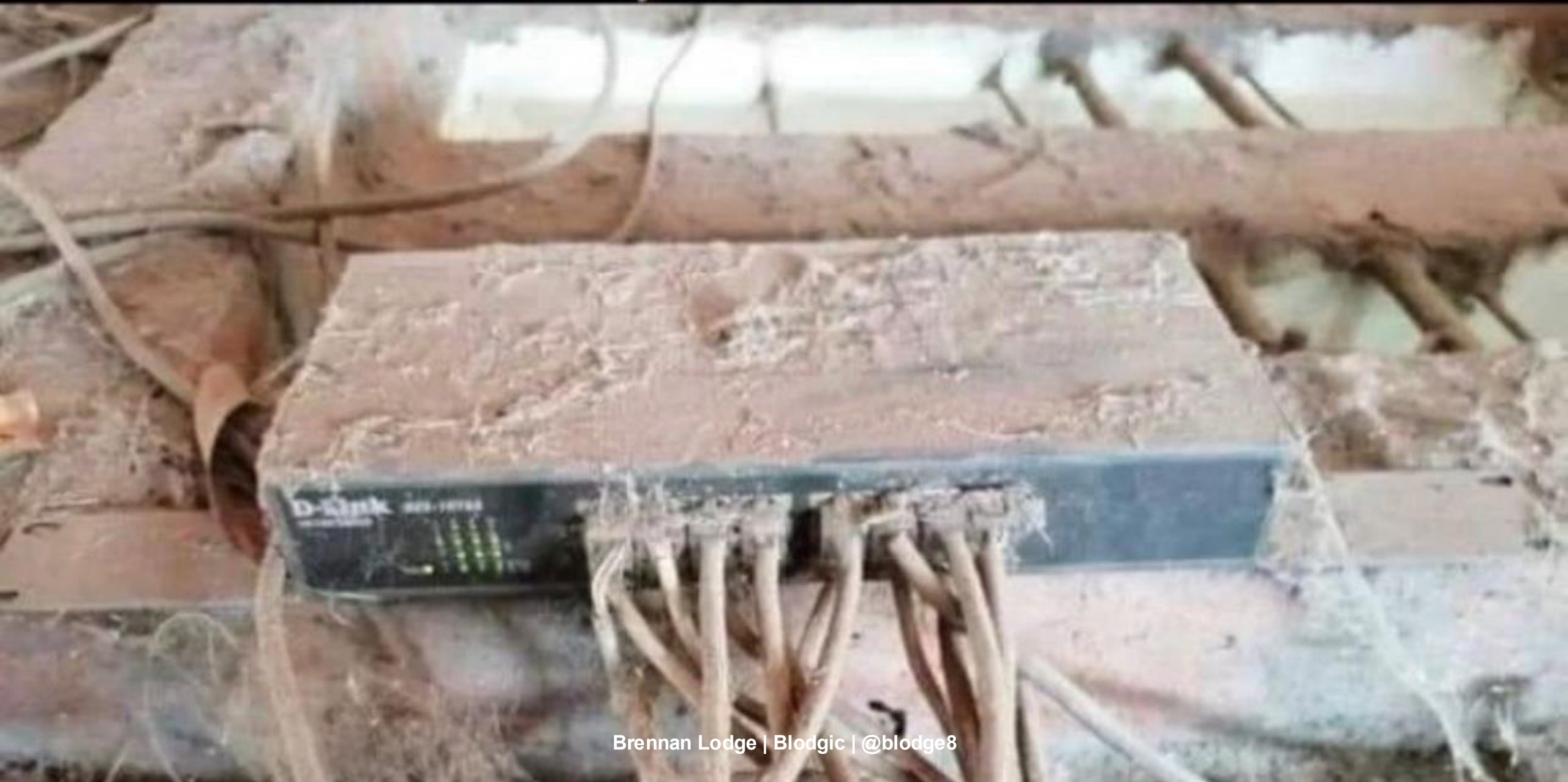
- WhoIS Brennan Lodge
- The Good, The Bad and the Ugly of AI in cybersecurity
- Introduction to Retrieval Augmented Generation (RAG) and GRC Applications
- Roll your Own RAG
- Visualize for transparency
- Data workflow
- MCP
- USE CASES + DEMOS
- Closing Remarks with links for more

BLODGIC

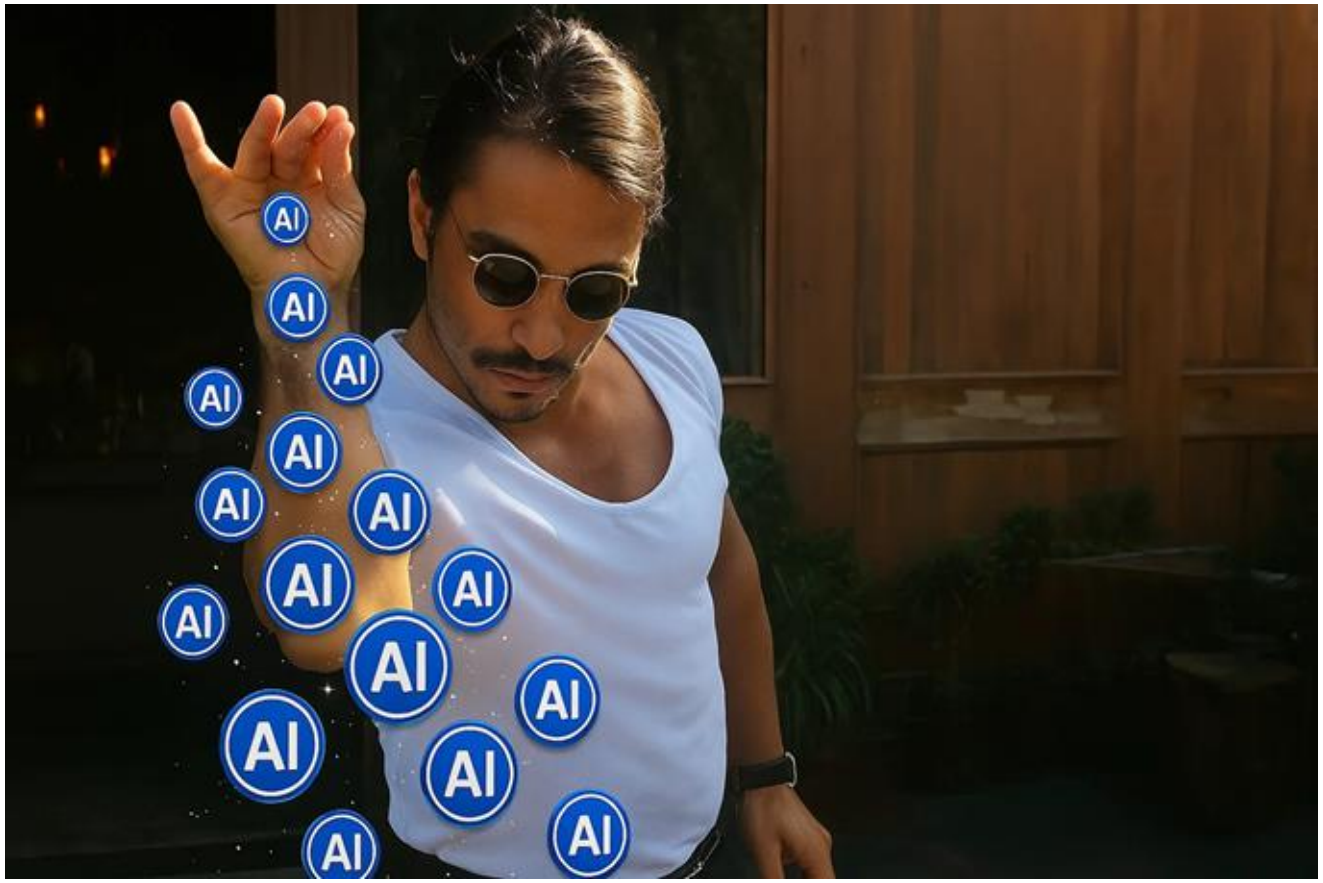
The GOOD of… AI in Cybersecurity?

- **Information Overload**
  - Cybersecurity pros face a deluge of threat data; AI can filter and prioritize this to manageable levels.
- **24/7 Defense Needs**
  - AI operates continuously, supporting human teams beyond regular work hours.
- **Talent Gap & Burnout**
  - AI mitigates the industry's talent shortage and reduces professional burnout by automating routine tasks.
- **Rising Attack Volume**
  - An estimation by Cybersecurity Ventures indicates an increase of 350% in unfilled positions from 2013 to 2023, culminating in 3.5 million unoccupied roles for this year.
- **Empowering Analysts**
  - AI provides rapid context, enhancing decision-making and easing the strain on analysts.
- **Complex Integration Challenges**
  - Tailoring AI solutions to address privacy, cost, and operational concerns in cybersecurity infrastructures.

If it works, don't touch it.



The Bad
…sprinkle a little AI on it



Siloed platforms

Cross-silo platforms

To Do What?

- SOAR 2.0
- Data co-pilot; smart automation; autonomous investigation; threat intel handling
- Detection engineering
  Easier, cover text columns, add smarter decision making; questions of scale, fidelity, model
- Answer Third party risk reviews
- Automation for the sake of Automation
- Shadow ~~IT~~ AI
  - AI ghosts in your
    - Meetings
    - Browsers

Google Launches Security AI Workbench to Rival Microsoft's Security Copilot

Introducing Charlotte AI, CrowdStrike's Generative AI Security Analyst: Ushering in the Future of AI-Powered Cybersecurity

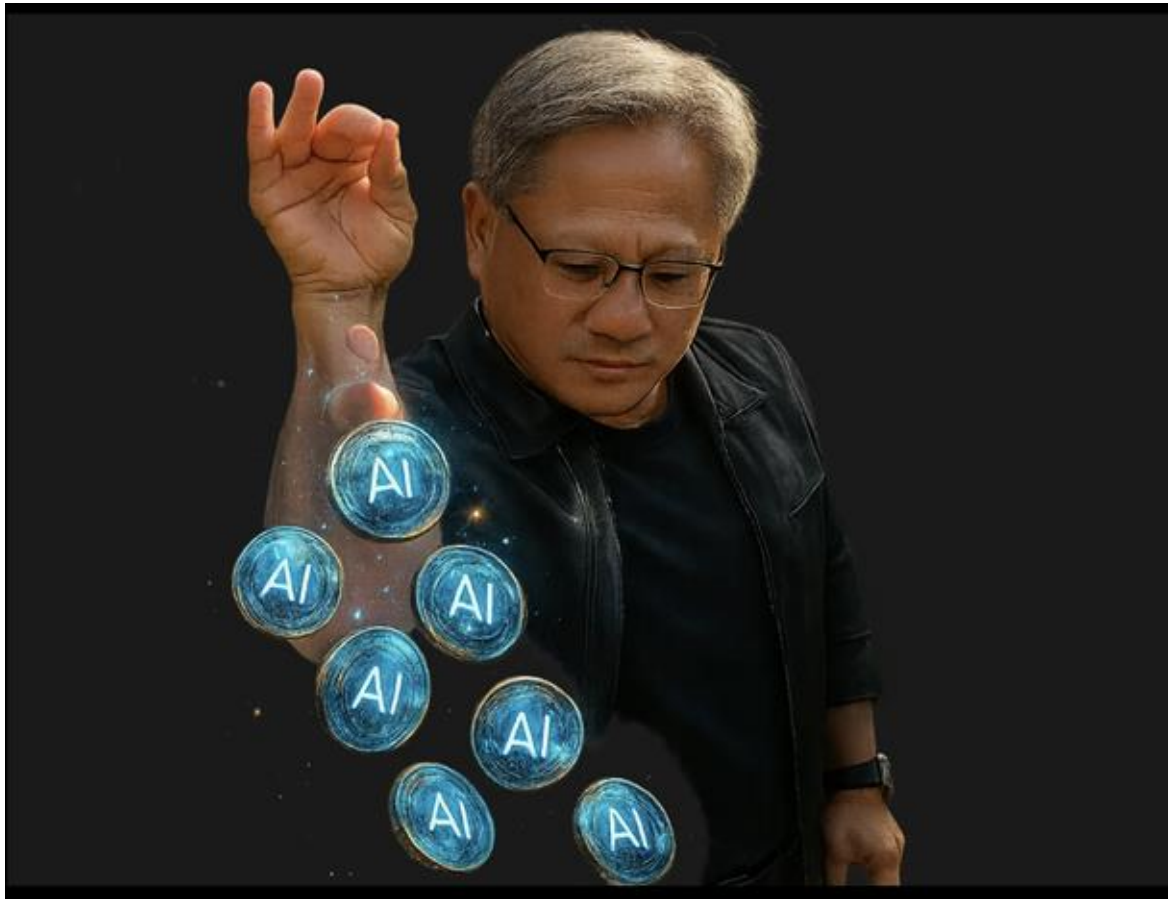
Dropzone AI

VECTRA

The Bad
…Tokens everywhere

Beware of the AI Pricing Model with tokens

- Similar to cloud and lack of transparency
- “Token” mentioned 85 times in the keynote speech’s at GTC
- Token Pricing - a ***race*** to the bottom?



This new AI industrial revolution, driven by floating point number tokens, will be as transformative and incomprehensible to many as the electricity revolution was. But within 10 years, it will become completely normal. The AI industry is going to be gigantic.” – Jensen Huang Keynote NVIDA GTC 2025

LLMs ...The UGLY.
PLEASE. NOT AGAIN!

The Ugly…
The CISO dilemma

CISO's and startups want to use AI but how?

"We have hundreds of internal genAI projects, but any new one must go through X, who is still making a policy on it"

"Unlike American regulators, we're letting banks take the lead in how AI may be used"

"We're scrambling to come up with an internal AI policy"

"We can't stop our users from using ChatGPT"

We can implement it, but how do we explain it?

"If you can't see how **AI is making decisions, you can't trust it."**
— Every modern CISO

•The *NEEDS* of AI

- **Secure**

  Transparent, auditable and no hallucinations

- **Time**

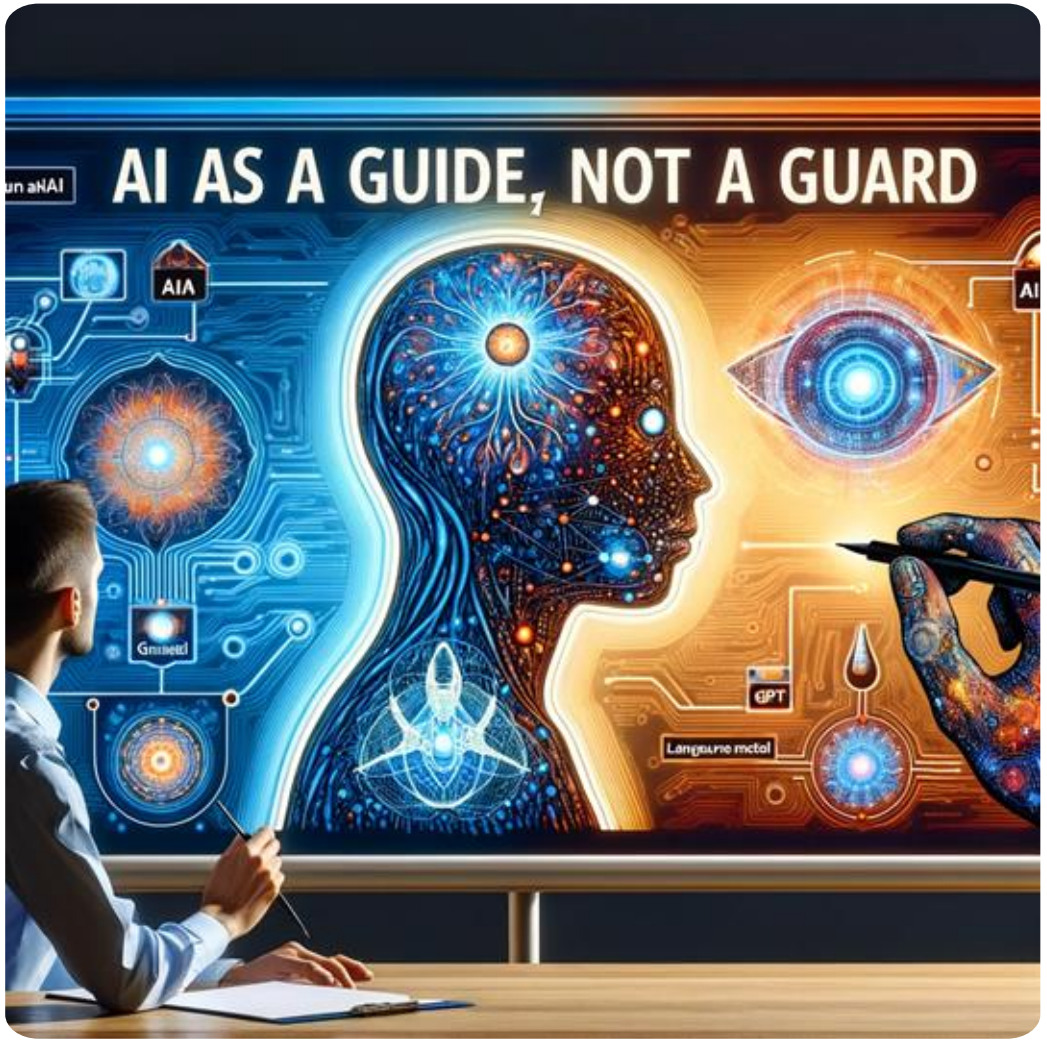
  Instant retrieval from real-time data with your own control over your own data

- **Cost**

  Lower computational and consumption costs with ability to scale

AI as a Guide, Not a Guard

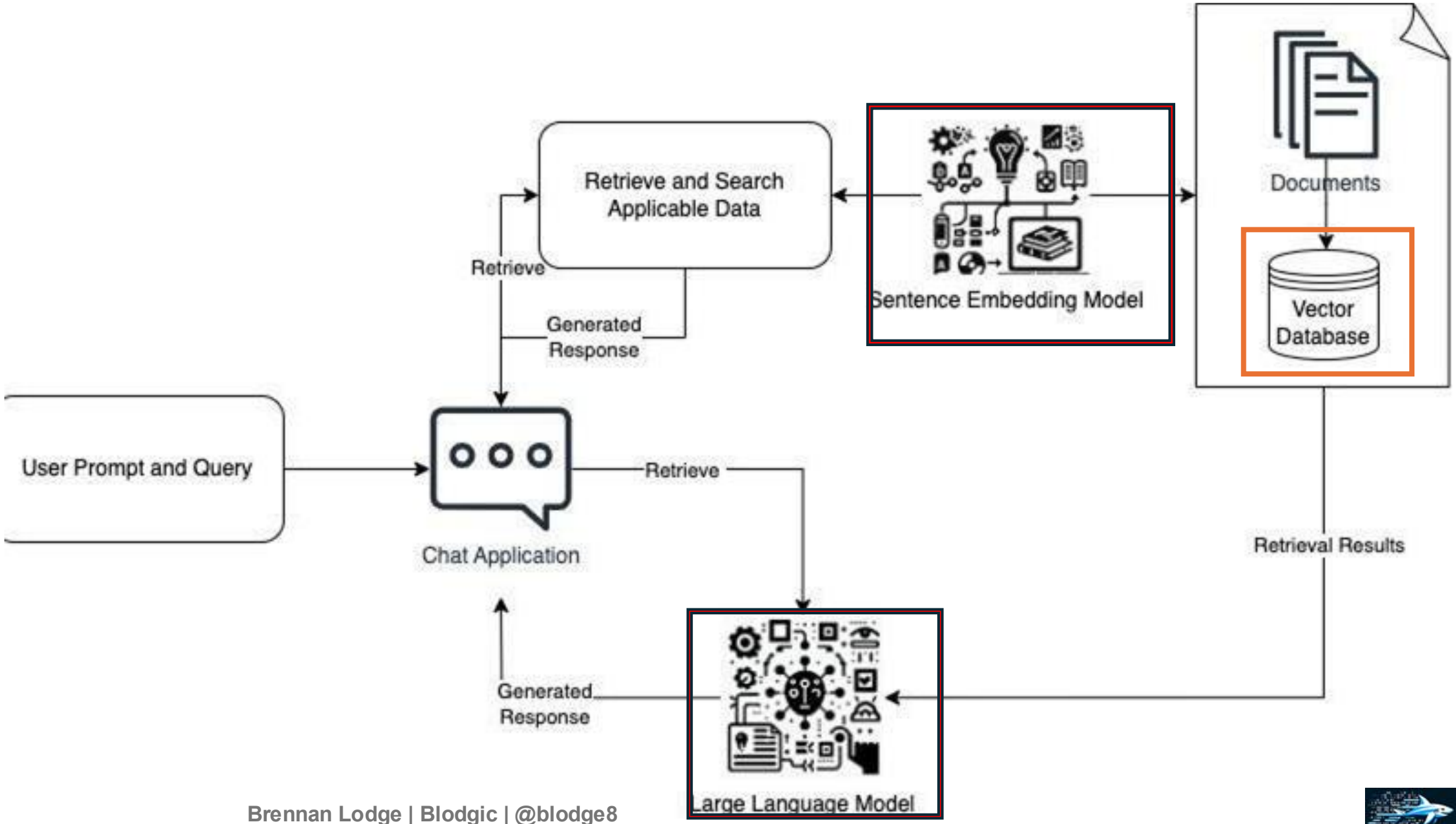
- Understanding Generative AI
- GPT & LLMs:
  - These models analyze and generate text, aiding in threat detection and alerts.
- AI as an Informative Ally:
  - AI guides cybersecurity experts through the maze of threats, risks, and data, providing them with actionable insights.
- Purpose: Democratize your cybersecurity tools
  - Real-time AI-driven cybersecurity advisory.
- Rapid Analysis:
  - Instantaneous response.
- Data-driven:
  - Leverages sources like CISA & MITRE ATT&CK, NIST, Information Security Policies, and more.
- Integration and Scale …without more headcount
  - Attack traffic can double overnight
    - **DeepTempo's** agent-free architecture elastically scales in Data Lakes without deploying new endpoints or hiring more SOC staff.
    - Just analyze my data for anomalies and don't interfere with anything else



...Enter RAG. What is it?


Brennan Lodge | Blodgic | @blodge8

Your AI Library



Why RAG?

Hallucinated answers

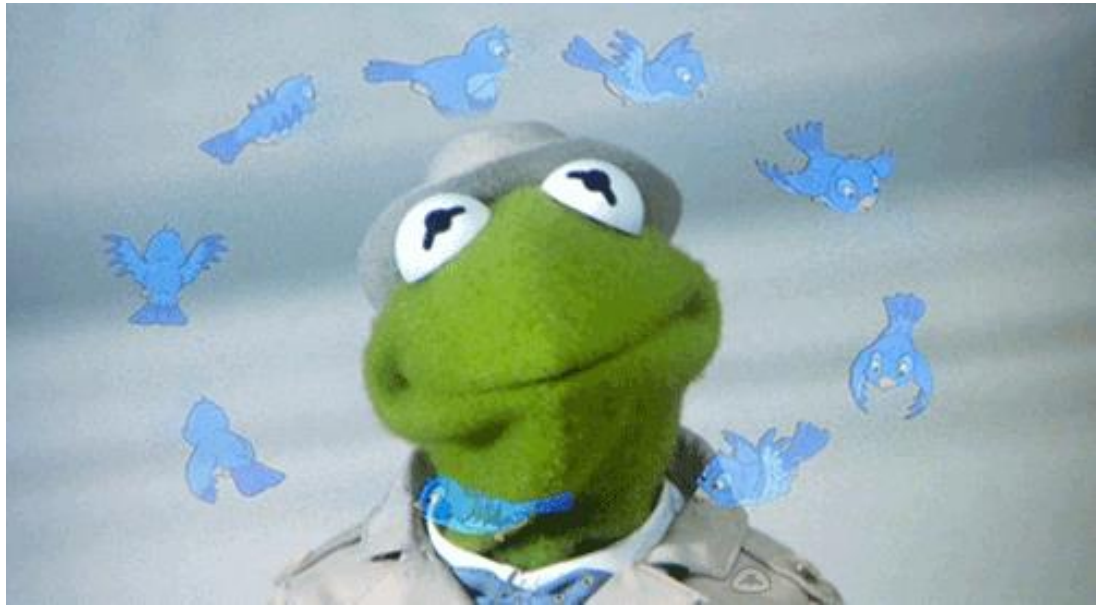
- LLMs can generate plausible but inaccurate responses.
- RAG uses source material to ensure answers are fact-based and verifiable.

Stale training data

- LLMs rely on outdated training data, missing recent information.
- RAG enables LLMs to incorporate the latest data, ensuring up-to-date responses.

Leverage Private Data

- LLMs are limited to public data, lacking personalized insights.
- RAG allows the use of private data for tailored, specific answers.



BLODGIC

Roll your own RAG

Secure

Manage your own destiny and centralize your own data

Time

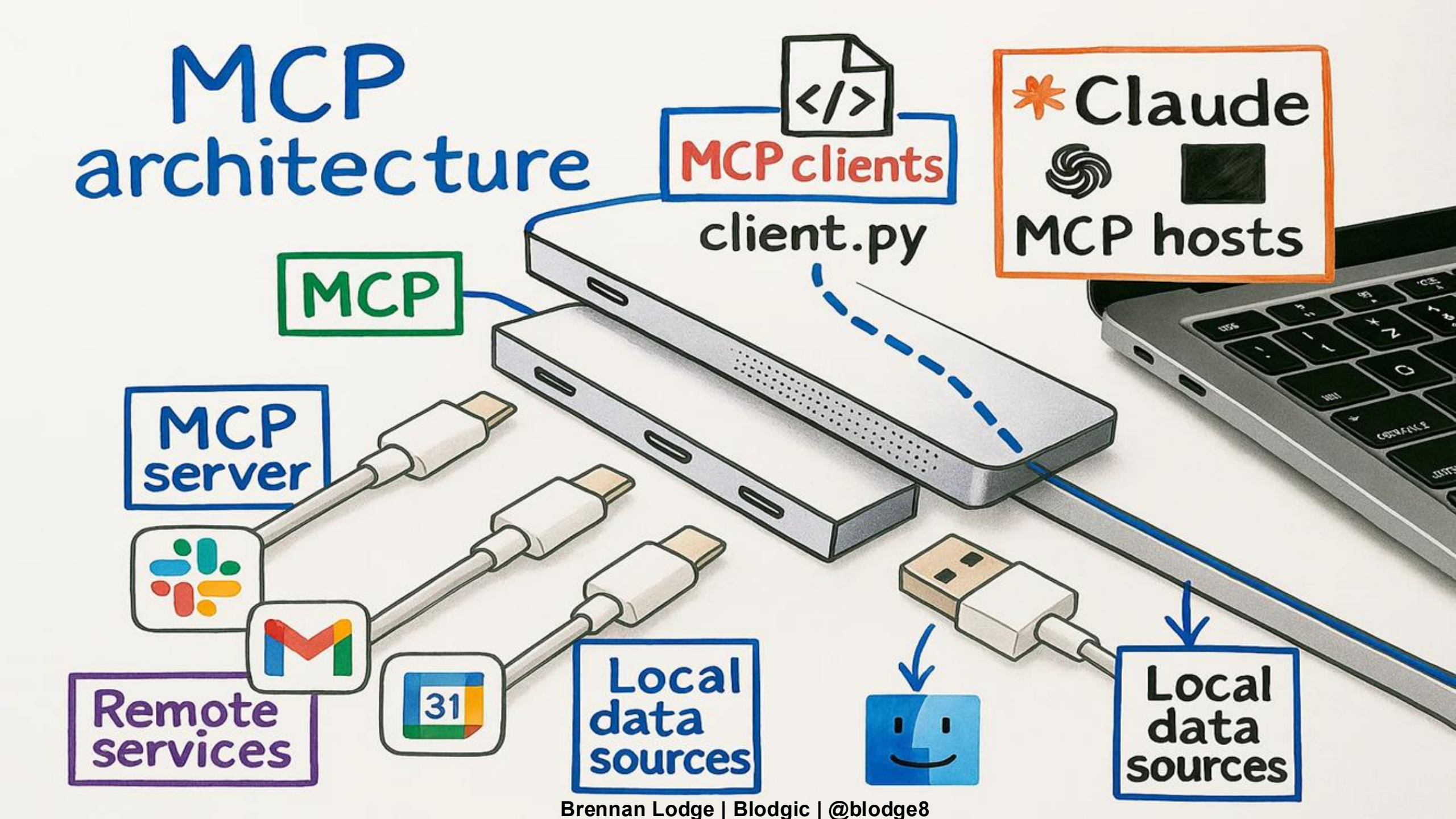
- **Quicker**:
  - Reduces the time lag in threat detection and response, moving from reactive to proactive.

Cost

- **Cost Tested and CISO Approved**:
  - Achieves response times within 10-second benchmarks, indicating robustness. Achieved a cost of < $500 per month (*milage may vary*)

Model Context Protocol

Brennan Lodge | Blodgic | @blodge8

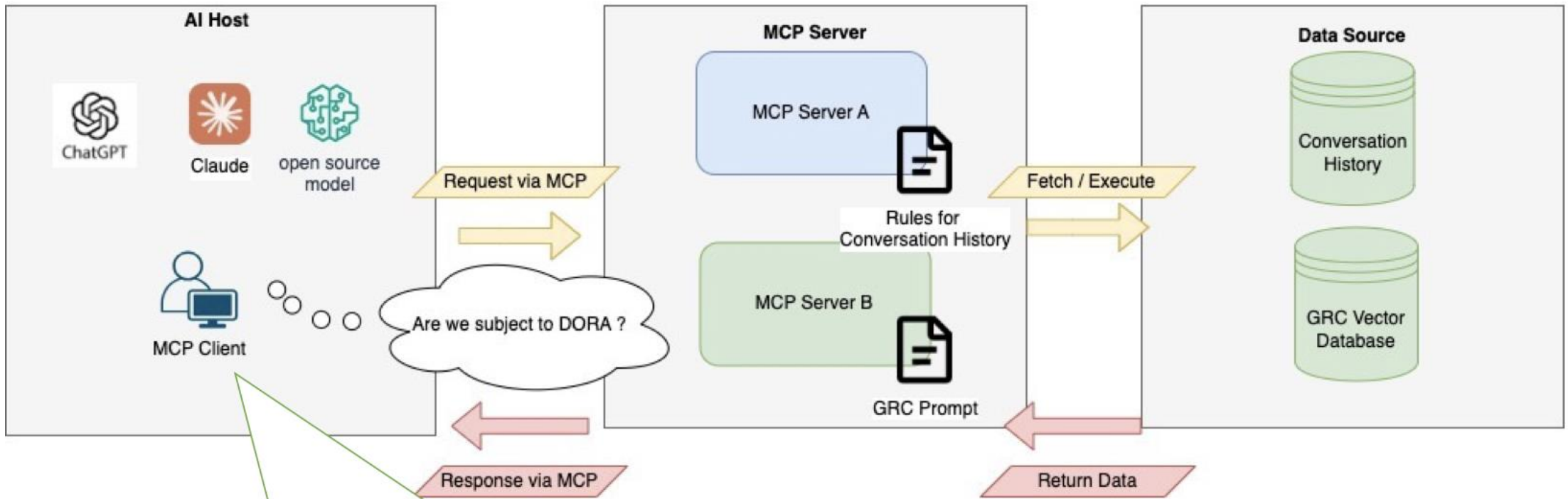

MCP architecture
MCP clients
client.py
Claude
MCP hosts
MCP
MCP server
Remote services
Local data sources
Local data sources

Architecture

Host

Client

Server



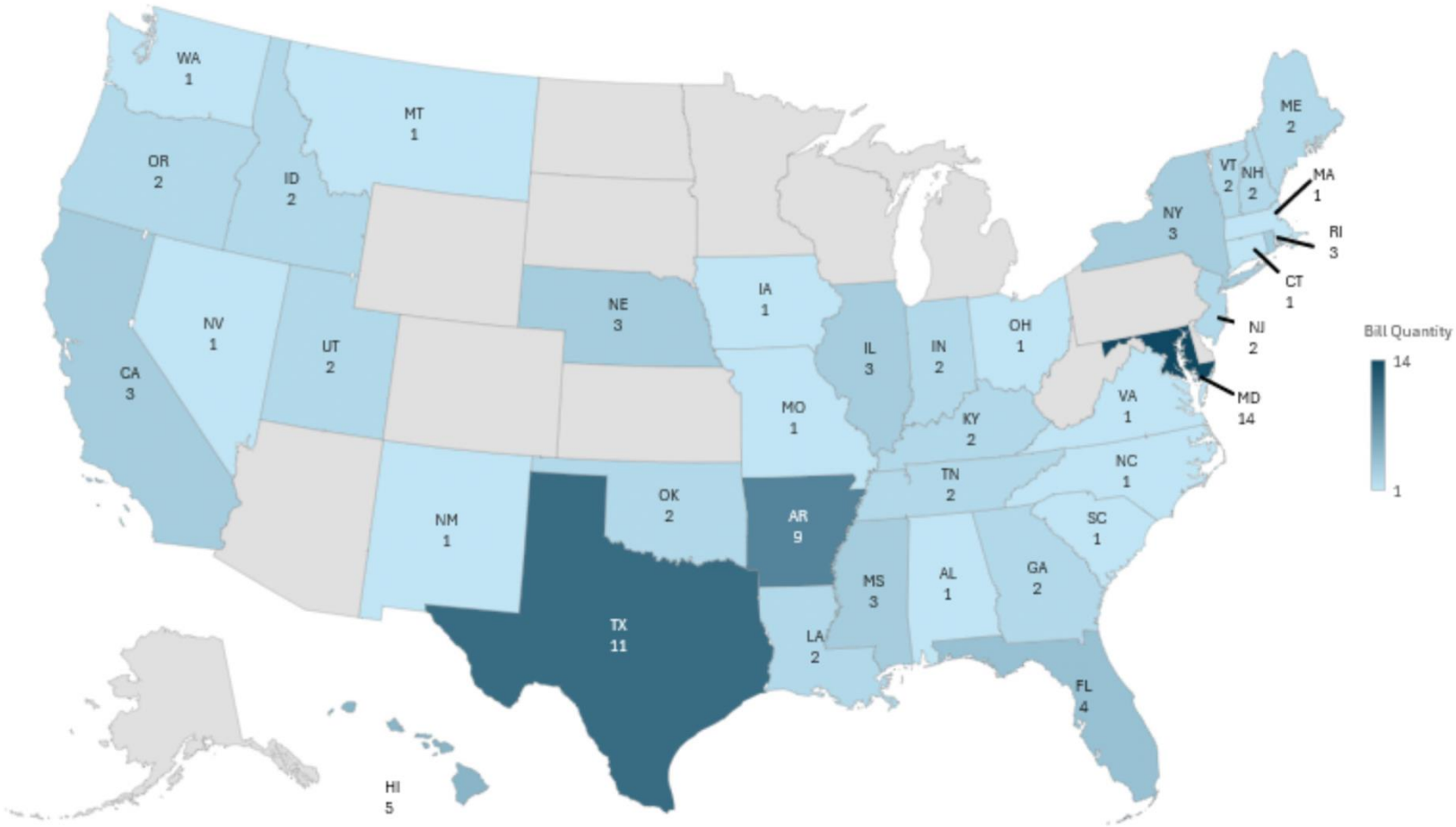
"Yes—because we provide payment and lending services to EU customers and fall under the DORA definitions of ICT third-party providers, we are subject to DORA <DORA.pdf>

A GRC Use Cases

Cybersecurity law is accelerating faster than operational security teams can adapt.

- **37 states passed 99 cybersecurity bills in 2025**

•393 new statutory cybersecurity requirements
•51% focused on governance mandates
•*Expanded incident reporting (24–72 hr windows)*
•Increased required controls
•More compliance reporting
•Sector-specific mandates (water, grid, K-12, healthcare)



Tracking Cybersecurity Policy Developments Across State Legislators. 2025 Enacted Legislation. UC Berkley

Data Privacy – UN Trade & Development

Data Protection and Privacy Legislation Worldwide

As more and more social and economic activities have place online, the importance of privacy and data protection is increasingly recognized.

Of equal concern is the collection, use and sharing of personal information to third parties without notice or consent of consumers. 137 out of 194 countries had put in place legislation to secure the protection of data and privacy.

Africa and Asia show different level of adoption with 61 and 57 per cent of countries having adopted such legislations. The share in the least developed countries in only 48 per cent.

OVERVIEW

E-TRANSACTION LAWS — 158 countries

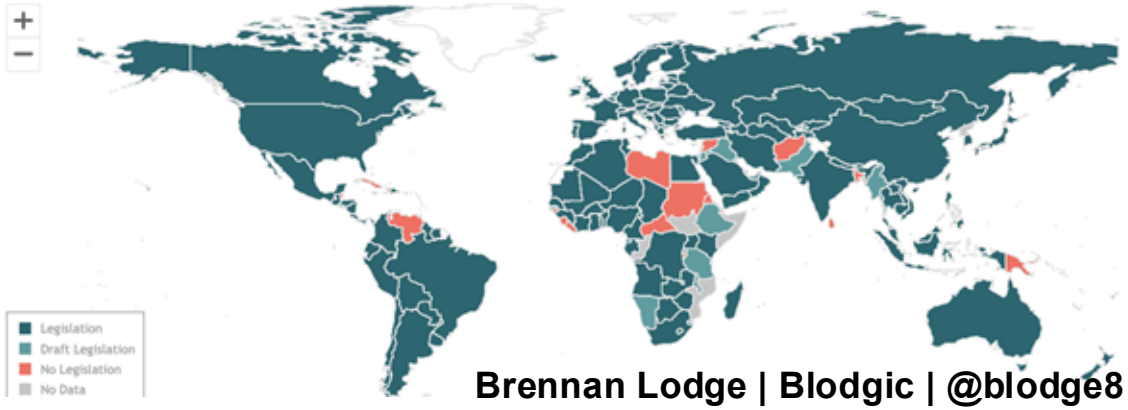
CYBERCRIME LAWS — 156 countries

CONSUMER PROTECTION LAWS — 52 countries

71%	9%	15%	5%
COUNTRIES WITH **LEGISLATION**	COUNTRIES WITH **DRAFT LEGISLATION**	COUNTRIES WITH **NO LEGISLATION**	COUNTRIES WITH **NO DATA**

Select a country ▾ Select a region ▾ DOWNLOAD FULL DATA

Data Protection and Privacy Legislation Worldwide



Brennan Lodge | Blodgic | @blodge8

BLODGIC

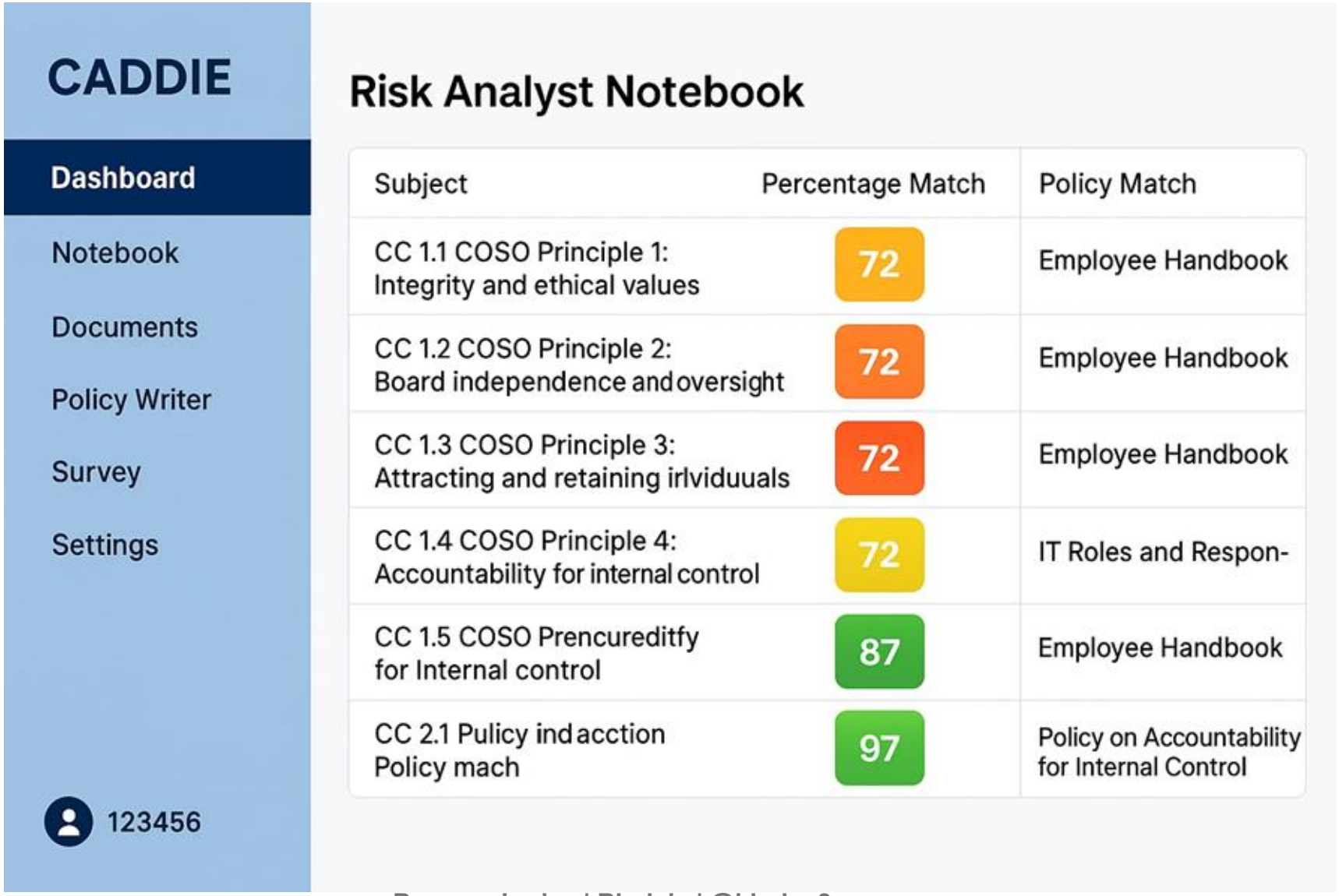
Engage, interpret, understand and stream- your Governancce Risk and Compliance

Brennan Lodge | Blodgic | @blodge8

BLODGIC

GRC BERT GAP ANALYSIS

- **Map your policies with percentage grades**



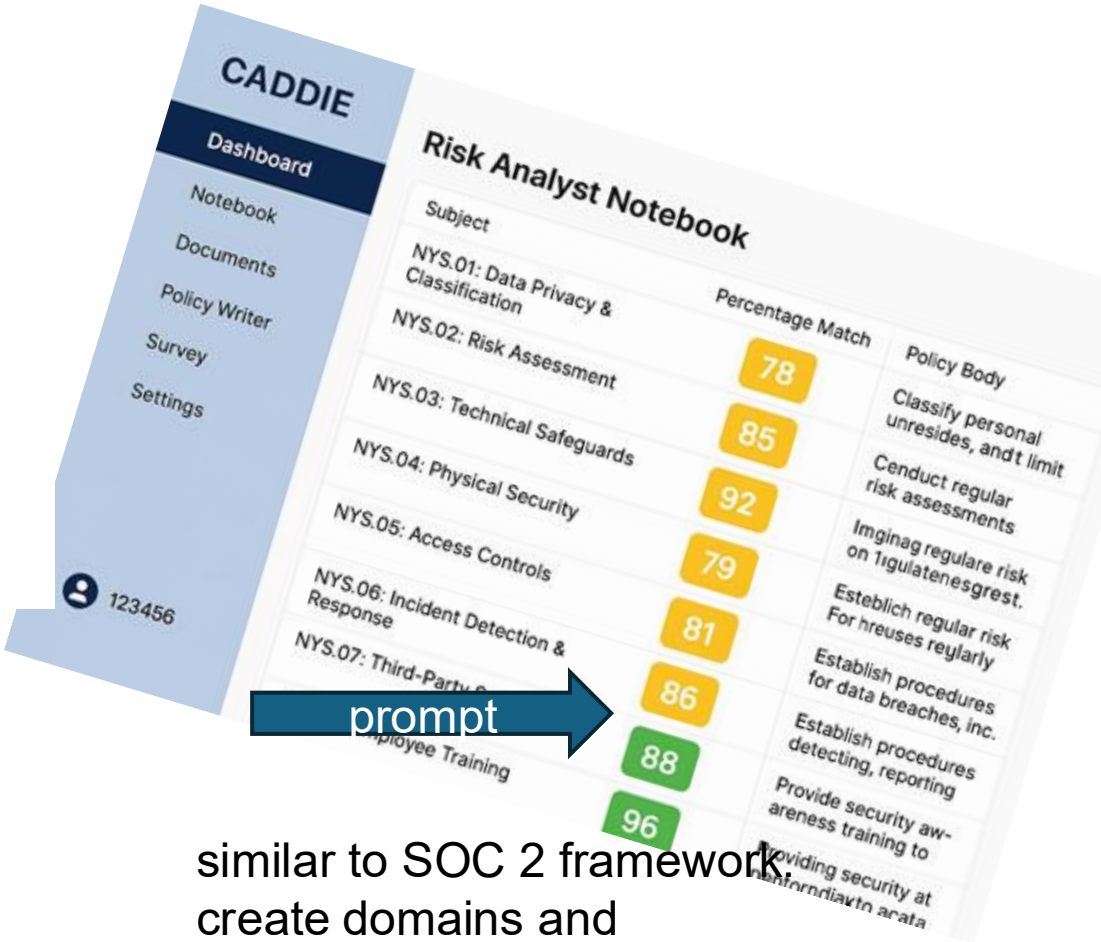
New regulation but no framework?

- **Use your RAG to create a new notebook to track compliance to the new regulation**

upload

New Regulation

Vector Database



prompt

similar to SOC 2 framework. create domains and explanations in a new framework to follow for New York SHIELD ACT

BLODGIC

github.com/Blodgic/AuditCaddie – open source project

- 50 + Policy Templates
  - Made to satisfy SOC 1
- Starter Packs
  - State Regulations
  - Data Protection Laws from 60+ Countries
- Frameworks -> Compliance Notebooks
  - FERPA
  - ISO 27001
  - NIST CSF
  - SOC 2
  - DORA
  - CMMC
- Classification Models
  - SOC 2
  - DORA
  - + more to come
- Share with us …

github.com/Blodgic/AuditCaddie/tree/main

Blodgic / AuditCaddie

Type / to search

Code Issues Pull requests Discussions Actions Projects Security Insights Settings

AuditCaddie

Public

Pin | Watch 1 | Fork 0 | Starred 3

main | 1 Branch | 0 Tags | Go to file t | Add file | Code

Blodgic Add files via upload — bd3fa69 · 2 months ago — 53 Commits

analyzers/SOC2	Create README.md	5 months ago
assets	Rename slide1 .png to slide1.png	2 months ago
docs	Create CONTRIBUTING.md	6 months ago
starter-pack	Add files via upload	2 months ago
templates	Add files via upload	5 months ago
CMMC_compliance_notebook.xlsx	Add files via upload	3 months ago
LICENSE	Create LICENSE	6 months ago
README.md	Update README.md	2 months ago
auditcaddie_launch_presentation_2025090...	Add files via upload	2 months ago

README | Contributing | License

AuditCaddie

Open Compliance Templates & AI-Powered Gap Analysis

About

No description, website, or topics provided.

Readme
View license
Contributing
Activity
3 stars
1 watching
0 forks

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

DEMO

TESTIFY: AI-DRIVEN POLICY MAPPING

RAGe AGAINST THE GRC MACHINE

AI POLICY in the NAME of...

TAKE THE POWER BACK...from the AUDITORS

Last but not least…

- **Governance for AI is crucial for the future or Cybersecurity**
- **YOU CAN DO IT!**
  - AI in cybersecurity works
- **Architecture & Cost Analysis**
  - Its cheap…for now
- **Use Cases & Integration**
  - Own your data and your own destiny
  - GRC
- **RAG + MCP for the 1st place AI Win**

LINKS TO LEARN MORE

- Brennan Lodge – blodge@blodgic.com

- Audit CADDIE
  - https://github.com/Blodgic/AuditCaddie

- LinkedIn Learning Class –
  1. “RAG for cyber security use cases”
  2. MCP Cybersecurity Course AI Security Tools and Automation

  3. !!!STICKERS!!!