Architecting the Future: Building Secure Systems in a Generative AI World

Trac Bannon
Senior Principal
Software Architect & Digital Transformation Advisor
MITRE Advanced Software Innovation Center

January 2024

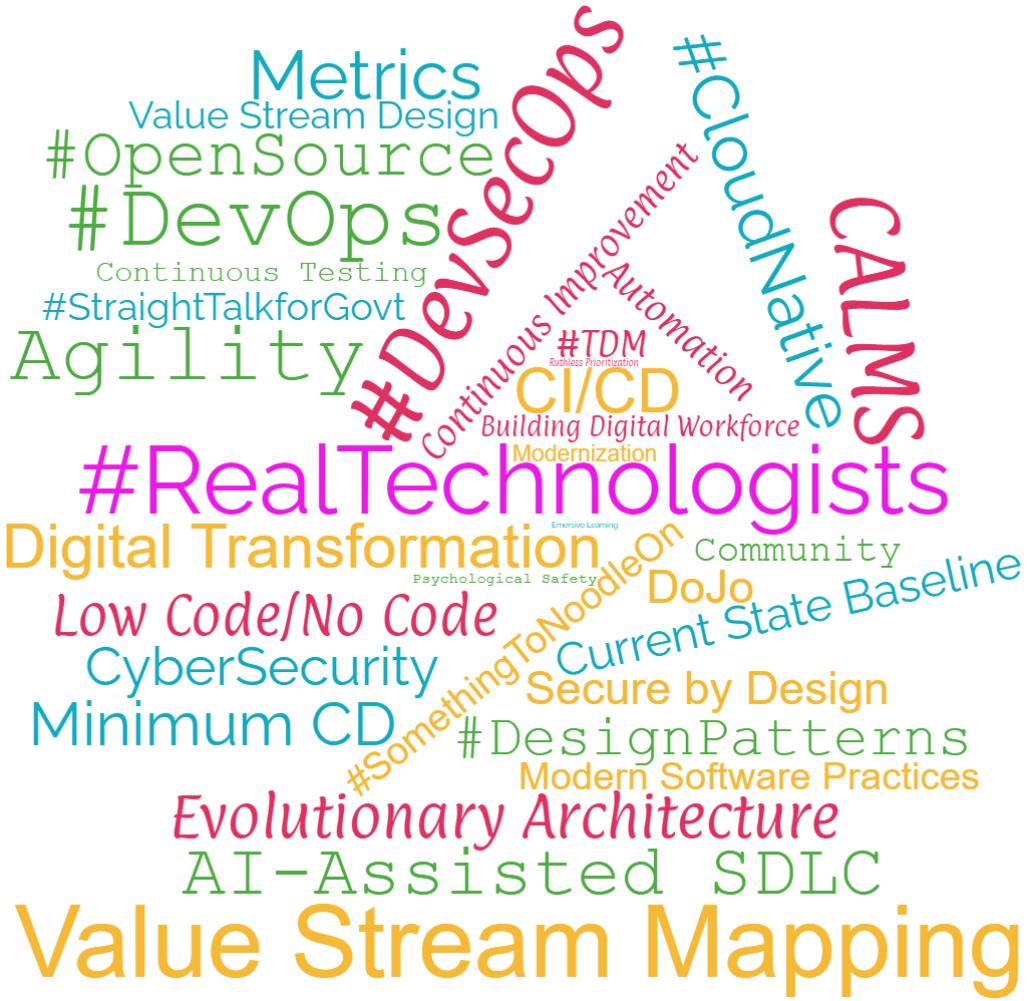
Tracy L. Bannon

"Trac"

Software architect | engineer | mentor | community leader

Who Am I?

/trās/



vsm consortium Influencer

AMBASSADOR DevOps Institute ADVANCING THE HUMANS OF DEVOPS

IEEE SENIOR MEMBER

MITRE

The Rise of Generative AI

- Growing presence across sectors
- Both boon and a security challenge
- Urgency need to addressing these cybersecurity challenges

MITRE

Urgency in understanding and addressing challenges

Organizations dashing to provide guidance:

- OWASP - Open Web Application Security Project
- CISA - Cybersecurity and Infrastructure Security Agency
- NIST - National Institute of Standards and Technology

Everyone must be GAI Savvy

Stakeholder education

Everyone grasps the potential security risks

Organization wide concern; not just IT

Beyond GAI Education…

What are the architectural considerations and principles for adopting GAI ?

MITRE

Start Secure

Secure by Design - The Foundation

- Identify Key Security Objectives
- Focus on Assets Needing Protection
- Categorize and Prioritize Resources
- Align with Specific Threats

MITRE

Defense in Depth - Layered Security

- Multi-Layered Defense
- Security Controls at Various System Layers
- Increase Difficulty for Penetration
- Redundancy in Security Measures

MITRE

Automate and Verify

- Automate Security Controls
- Reduce of Human Lag in Threat Response
- Adopt of Zero Trust Architecture (ZTA)
- Apply Least Privilege Principle

MITRE

Train Smart

Training Smart for GAI

- Data is the Foundation for GAI Models
- Risks of Compromised or Mismanaged Data
- Data Classification
- Ethical Audits for Bias Detection
- Proactive Implementation for Risk Mitigation

Keep a Strong Backbone

MITRE

GAI is increasingly sophisticated

Models are engineered to understand and respond

Generative models based on neural networks

Generated content mimics human language and decision-making

Nefarious actors are leveraging GPT models as well

Continuous Supervision!

- Understanding Normal Behavior
- Comprehensive Logging for Training and Forensics
- Determining Log Storage Duration
- Behavior Analysis and Automated Alerting

Humans in the loop

Challenges and Risks

Early Use of Code Generation for Vulnerability Injection

Complexity of GAI Models Increases Risk

MITRE

Critical Role of Human Oversight

- Humans-in-the-Loop are Essential
- Static Code Analysis (SCA)
- Code Reviews as a Security Practice

MITRE

Call to Action – Your Next Steps

- **Plan** - Educate your team, understand the risks, and plan your “Secure by Design” architecture
- **Do:** Implement your security measures, layer your defenses, and launch your Generative AI projects
- **Check:** Monitor in real-time, log comprehensively, and audit periodically
- **Act:** Adjust, improve, and evolve your strategy as you learn from the checks

MITRE

What I need from you

- Share your organization's story and lessons learned
- Continue to share out new use cases and new tools

MITRE

Tracy L. Bannon

tbannon@mitre.org | alt: Trac@tracybannon.tech

https://www.linkedin.com/in/tracylbannon

@TracyBannon

https://tracybannon.tech

Disclaimer: The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

MITRE

SOLVING PROBLEMS FOR A SAFER WORLD®