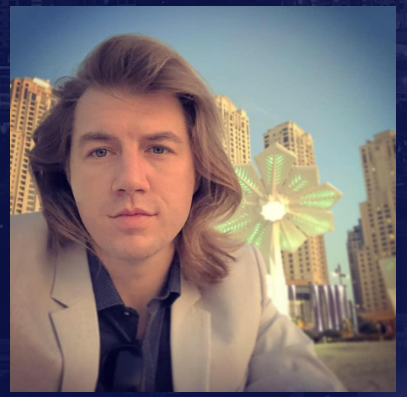
AI BOM Workshop at RSA 2024

Lightning Talk

AI Policy and the Software Supply Chain: Transparency, and Security of Suppliers, Services, and Products



Nicholas Vidovich,
VP of Customer Experience @ Finite State

FINITE STATE

Lightning Talk

Goal: Quickly introduce a lot of concepts that we can talk about in more detail at break-out sessions

Transparency & Security in the Software Supply Chain

- Transparency via SBOMs enables better security, and informs policy requirements in the traditional Software Supply Chain
  - Licenses and Compliance
  - Known Vulnerability Correlation, Management
  - Continuous Monitoring, Incident Response

- **This translates to AI transparency as well**

GRC in the Age of AI

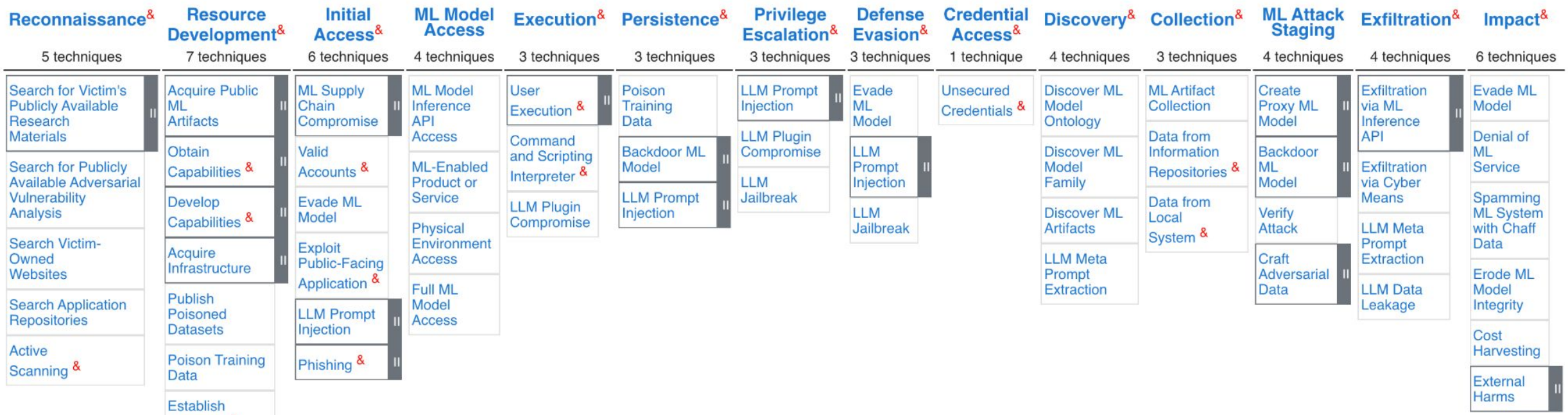
- Governance
- Risk
- Compliance

- Oversee policy, manage risk, ensure compliance
- Stay up to date on regulatory changes
- Simplify auditing
- Address any challenges that can endanger revenue, reputation, and customer and stakeholder interest

MITRE ATLAS Framework

ATLAS Matrix

The ATLAS Matrix below shows the progression of tactics used in attacks as columns from left to right, with ML techniques belonging to each tactic below. & indicates an adaption from ATT&CK. Click on the blue links to learn more about each item, or search and view ATLAS tactics and techniques using the links at the top navigation bar. View the ATLAS matrix highlighted alongside ATT&CK Enterprise techniques on the ATLAS Navigator.



https://atlas.mitre.org/matrices/ATLAS

FINITE STATE

For Creators and Consumers

Policies for purchasing, employee use, and product development teams

- Suppliers
  - Understand the security considerations your suppliers use when creating AI products you use
- Services
  - Understand the implementation of various AI models in the services you and your employees use
- Products
  - Be specific about the AI models and capabilities you are building into the products you create

Licenses and Compliance

Compare Open Source Software Licenses to their potential AI corollaries

- Data
- Models
- Methods

- Permissive
- Copyleft
  - Weak
  - Strong

Example: Potential Permissive AI Licenses

- “Source Data License”
  - Training data is freely available and usable, with few restrictions on how it is subsequently used
- “Open Model License”
  - Model can be used, modified, and integrated into proprietary systems without obligation to disclose modifications or share improvements
- “Method Transparency License”
  - Methods used for training do not have to be disclosed, even if used commercially

Example: Potential Restrictive AI Licenses

- “Shared Data License”
  - Any models trained using a specific data set must also make its training data available under similar terms
- “Reciprocal Model License”
  - Any derivative models must also be shared under the same open conditions
- “Innovations Sharing License”
  - Any novel method or improvement in the training process developed using the original model must be shared

Regulatory and Compliance Frameworks

May govern what data can be shared with generative AI systems, and whether the systems are built with protections or not

- GDPR
- HIPAA
- PII

- As a consumer, how is the data that is shared collected, stored, and transmitted?
- As a creator, are your products built with these considerations in mind?

What policies and controls exist that need to be updated to incorporate new AI tools?

Security Standards and Protocols

Employee Use Policies - so far, many companies are just saying “NO.”

- RBAC
- MFA

- Standard access control to enhance security against unauthorized access
- All users to access AI systems with data relevant to their job functions

Security Standards and Protocols

Data Classification and Handling

- Identify Data Types
  - Input data, training data, generated data, and metadata
- Sensitivity Levels
  - Public, Internal Use Only, Confidential, Restricted
- Handling Protocols
  - Access Control, Encryption, Data Masking and Anonymization, Audit and Tracking

Security Standards and Protocols

Vulnerabilities in (Generative) AI Systems

- Jailbreaks
- Sandbox Escapes
- Abuse

- Vulnerability Management for AI enabled systems may look similar to traditional software supply chain:

  - Continuous Monitoring
  - Incident Response
  - Search & Visibility

So Vuln Management Policies probably look similar, too!

Supply Chain Transparency

Vendor Policies

- Supplier Audits
- Questionnaires
- Attestations

- Just as in traditional software supply chain security practices, new policies will be implemented for engaging with your vendors in pre and post-sales transparency

Supply Chain Transparency

Disclosure Requirements

Contract Stipulations to require AI BOMs

Known Vulnerability Disclosures

Product Development Policy & Best Practices

Security as a Priority

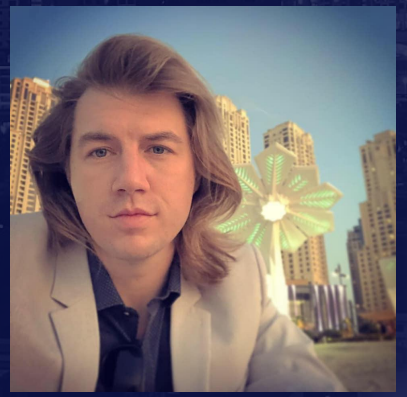
- Secure By Design
- Secure By Default

- Updated policies for AI powered products
- SSDLC
- NIST CSF

AI BOM Workshop at RSA 2024

Lightning Talk

AI Policy and the Software Supply Chain: Transparency, and Security of Suppliers, Services, and Products



Nicholas Vidovich,
VP of Customer Experience @ Finite State

FINITE STATE