THREAT MANAGEMENT

DETECT, PREVENT & MANAGE VULN.

SHIFT LEFT

💲 **COST REDUCTION** ⏱️ **AUTOMATION** 🛡️ **SEC POSTURE** 💻 **QUALITY** ☕ **DEV HAPPINESS** 📊 **VISIBILITY**
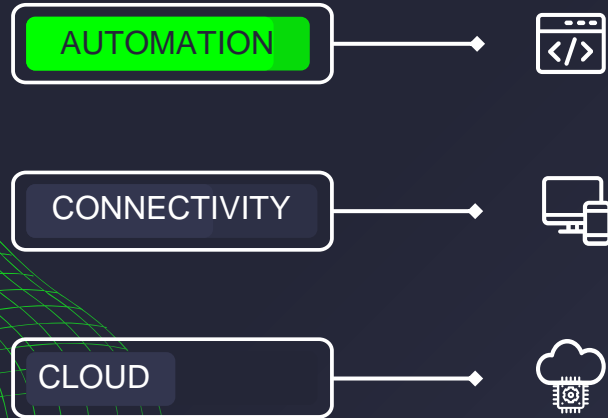
TESTING & HUNTING

ML/AI USE ↗

ATLAS Matrix

The ATLAS Matrix (ATLAS Machine Learning Threat 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 adaptation from ATT&CK. Click on links to learn more about each item, or view ATLAS tactics and techniques using the links at the top navigation bar.

Reconnaissance &	Resource Development &	Initial Access &	ML Model Access	Execution &	Persistence &	Defense Evasion &	Discovery &	Collection &	ML Attack Staging	Exfiltration &	Impact &
5 techniques	7 techniques	4 techniques	4 techniques	2 techniques	2 techniques	1 technique	3 techniques	3 techniques	4 techniques	2 techniques	7 techniques
Search for Victim's Publicly Available Research Materials	Acquire Public ML Artifacts	ML Supply Chain Compromise	ML Model Inference API Access	User Execution &	Poison Training Data	Evade ML Model	Discover ML Model Ontology	ML Artifact Collection	Create Proxy ML Model	Exfiltration via ML Inference API	Evade ML Model
Search for Publicly Available Adversarial Vulnerability Analysis	Obtain Capabilities &	Valid Accounts &	ML-Enabled Product or Service	Command and Scripting Interpreter &	Backdoor ML Model		Discover ML Model Family	Data from Information Repositories &	Backdoor ML Model	Exfiltration via Cyber Means	Denial of ML Service
Search Victim-Owned Websites	Develop Adversarial ML Attack Capabilities	Evade ML Model	Physical Environment Access				Discover ML Artifacts	Data from Local System &	Verify Attack		Spamming ML System with Chaff Data
Search Application Repositories	Acquire Infrastructure	Exploit Public-Facing Application &	Full ML Model Access						Craft Adversarial Data		Erode ML Model Integrity
Active Scanning &	Publish Poisoned Datasets										Cost Harvesting
	Poison Training Data										ML Intellectual Property Theft
	Establish Accounts &										System Misuse for External Effect

MARKET
RESEARCH
VENTURE CAP
...

· INT

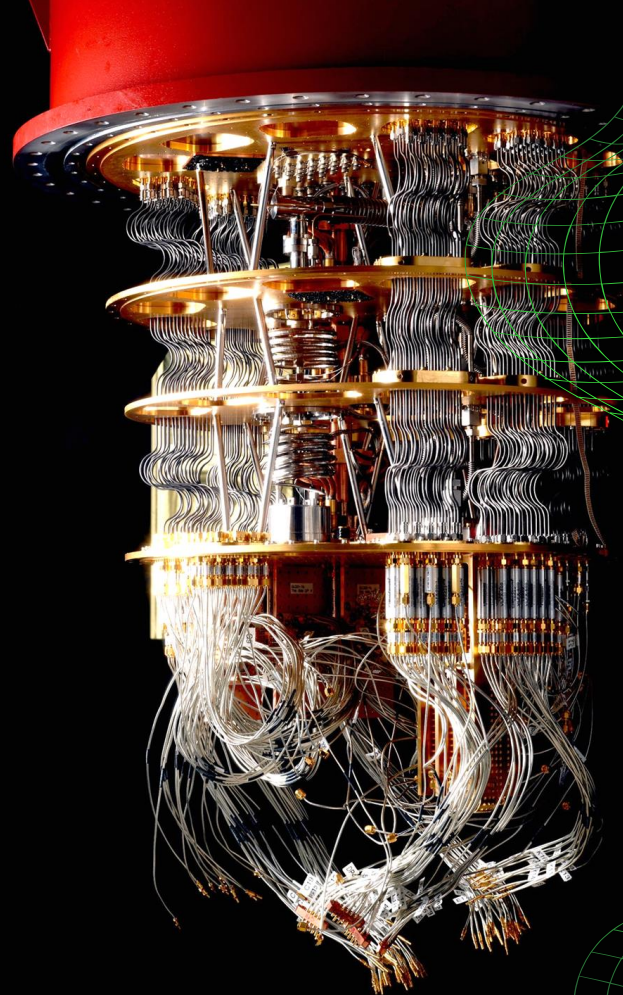ANTICIPATE RISK

FOSTER: KNOW-HOW IN HOUSE

CROSS-DISC. COLLABORATION

COMMON LANGUAGE METRICS/FRAMEWORKS

ANTICIPATE YOUR OWN RISK

THANKS!