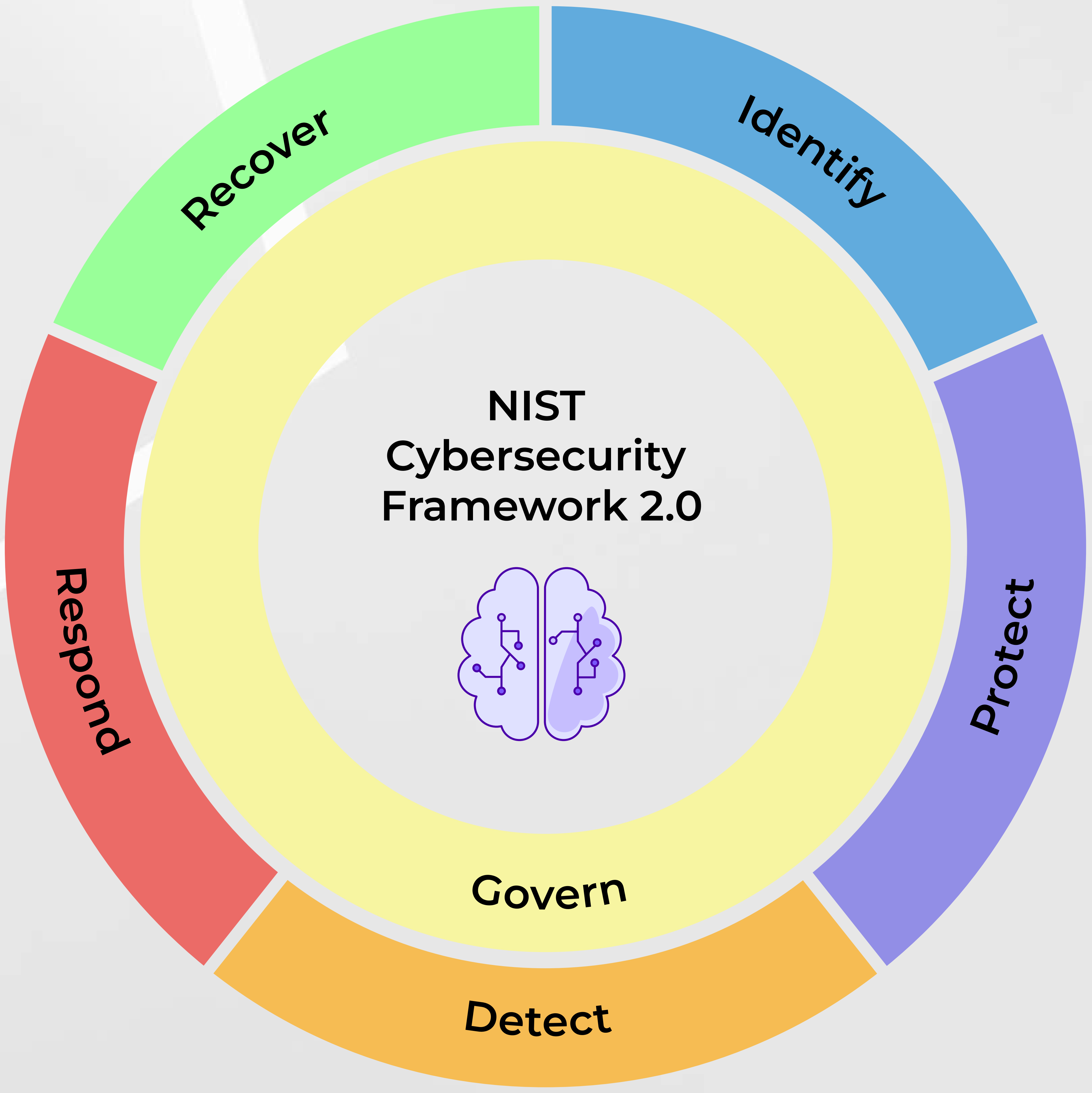
NUTANIX

6 AI Attacks and How to Protect Against Them

Malicious actors are targeting your AI assets. Are you prepared to defend them?
You need a blend of traditional security measures and focused protection for your AI assets.

Follow the NIST CSF 2.0 Framework to Secure Your AI Assets

Here's how we've applied the different components of the framework against six common threats:



Threat
Model Integrity and Recovery
Restore assets and operations impacted by a cybersecurity incident.

Solution
Deploy robust multi-location backup and recovery processes.

Threat
Model Theft
Help determine the organization's current cybersecurity risk.

Solution
Implement a zero-trust architecture (ZTA) on all your systems.

Threat
AI Manipulation Attacks
Take action regarding a detected cybersecurity incident.

Solution
Create non-digital processes for high-profile targets using check and balance threat response with gated human response and passkeys.

Threat
Model Inferencing, Prompt Injection
Use safeguards to prevent or reduce cybersecurity risk.

Solution
Perform model monitoring through a digital twin with prompt testing via AI whitehats.

Threat
Data Poisoning
Find and analyze possible cybersecurity attacks and compromises.

Solution
Check for anomalies in generated AI content through suggested model recommendations via weighted suggestions from data scientists.

Threat
Model (LLM) Outcome Manipulation
Establish and monitor cybersecurity risk management, strategy, expectations, and policy.

Solution
Conduct AI maturity assessments of trained models to identify and strengthen their vulnerabilities.

Protecting AI Assets is a Universal Concern

> A Gartner® article lists "6 reasons you need to build AI TRiSM into AI models. A comprehensive AI trust, risk, security management (TRiSM) program helps you integrate much-needed governance upfront, and proactively ensure AI systems are compliant, fair, reliable and protect data privacy."[1]

At Nutanix, we take the security, integrity, and privacy of your enterprise assets seriously.

We'd like to be your partner in securing your applications and data amid the ever-evolving threat landscape.

[1] Gartner article, AI TRiSM: Tackling Trust, Risk and Security in AI Models, 5 September 2023

NUTANIX
info@nutanix.com | www.nutanix.com | @nutanix

NutanixSecurityinfographic-FY23Q4 121223