

Technical Insights: 5 Ways GenAI Can Help Build Better Security Architecture

Richard Bartley

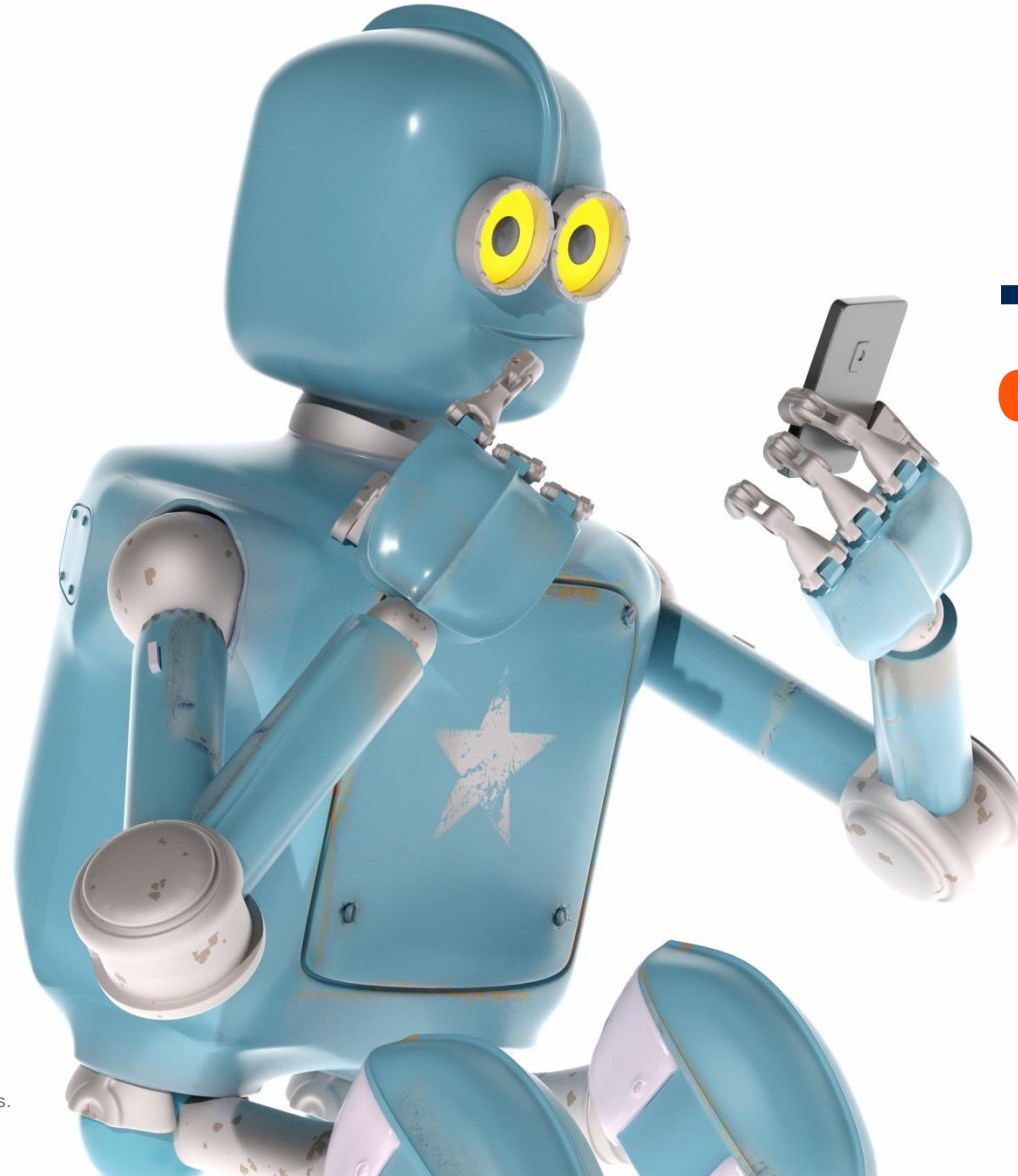
© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."

Gartner®

Need Support With Security Architecture?



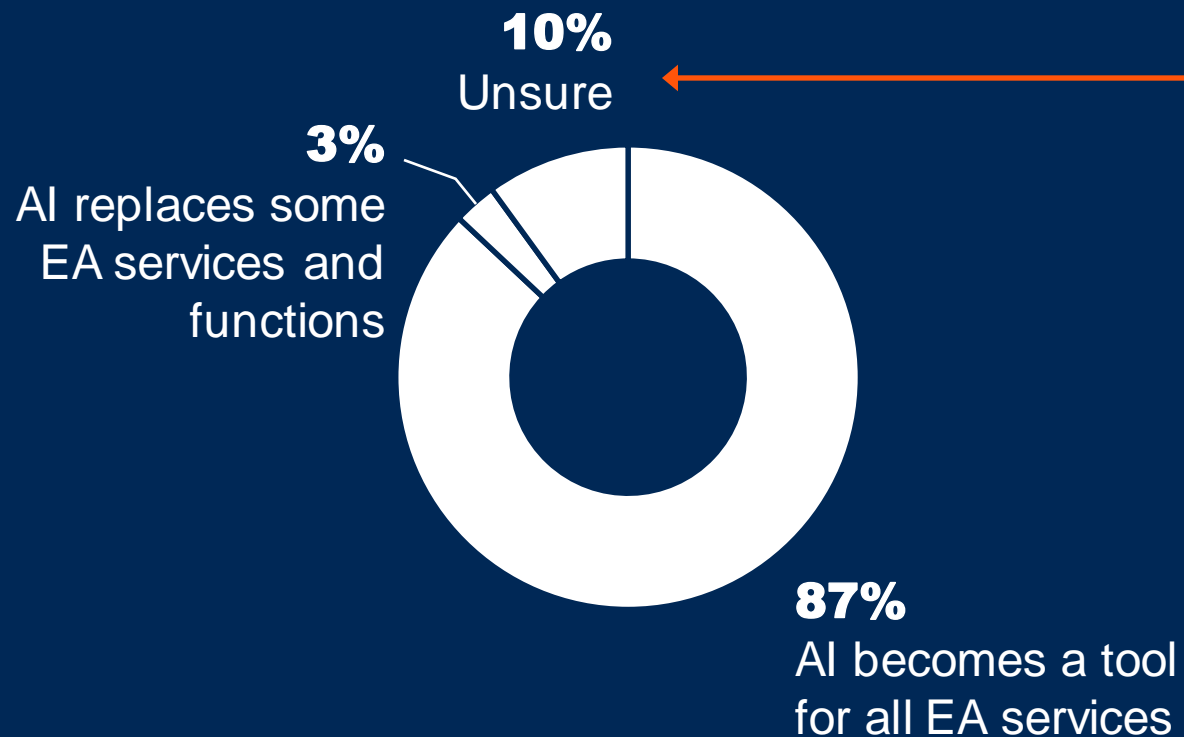
Generative AI Can Help ...



**... but it won't
do it for you.**

Gartner Surveyed Enterprise Architect's View of AI's Impact ...

AI in EA role



0%

AI replaces enterprise architects —

Developments in AI will lead to organizations not needing enterprise architects.

n = 28* Gartner EA clients, excludes unsure

Q: In your view, how will AI impact the EA role?

Source: 2023 Gartner Assessing Enterprise Architecture Survey

* Caution: Base size less than 30; interpret with caution.

Key Issues

1. Warnings and caveats.

2. Five ways:

- Contextualize and enhance
- Analysis uplift and explain
- Identify relationships and validation
- Create and optimize
- Manage

3. Recommendations for action.



Key Issues

1. Warnings and caveats.

2. Five ways:

- Contextualize and enhance
- Analysis uplift and explain
- Identify relationships and validation
- Create and optimize
- Manage

3. Recommendations for action.



Warnings and Caveats!



**Hallucination/
inaccuracy**



Bias



**Incomplete
data**



**Lack of
transparency**

Need for Checks and Balances



Treat outputs
as first drafts



Testing



Output
validation



Explainability



Versioning
and rollback



Observability



Prompt
engineering

Key Issues

1. Warnings and caveats.

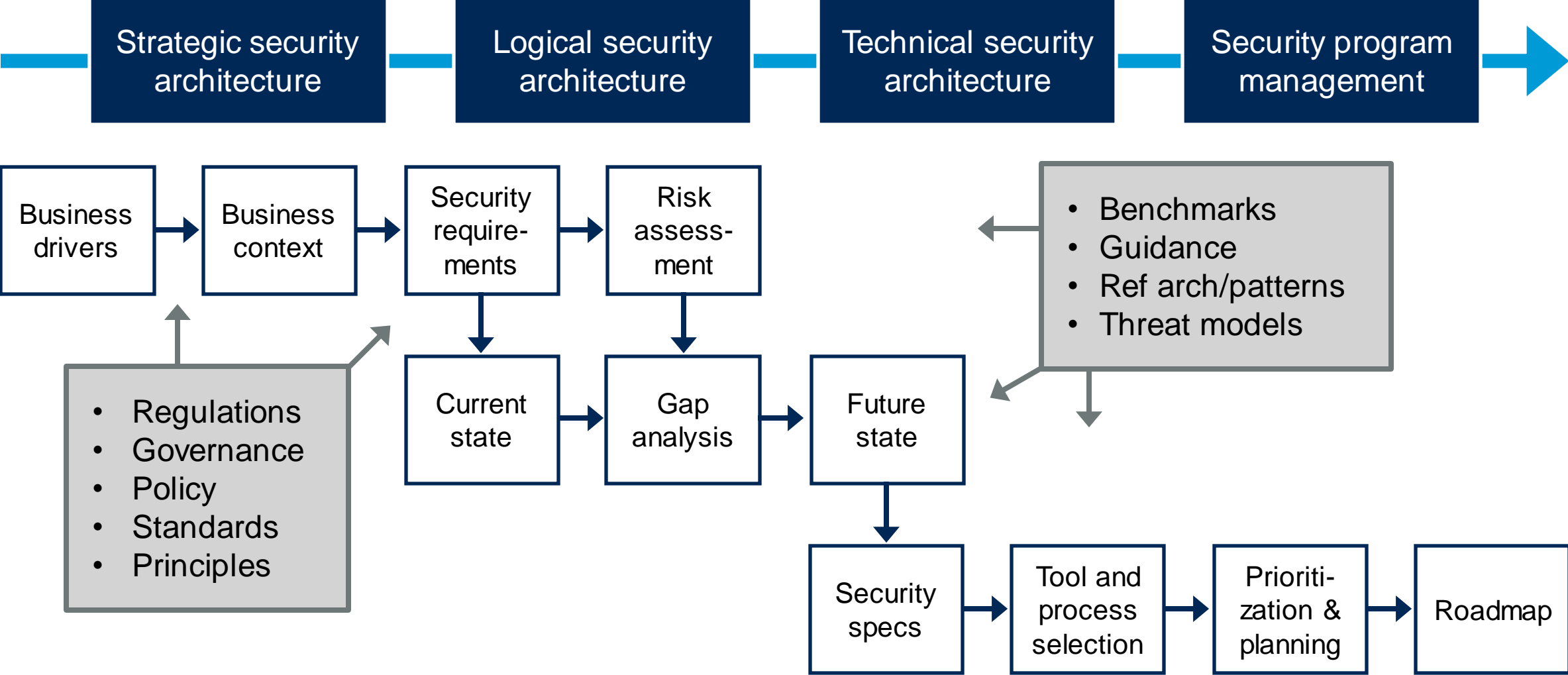
2. Five ways:

- Contextualize and enhance
- Analysis uplift and explain
- Identify relationships and validation
- Create and optimize
- Manage

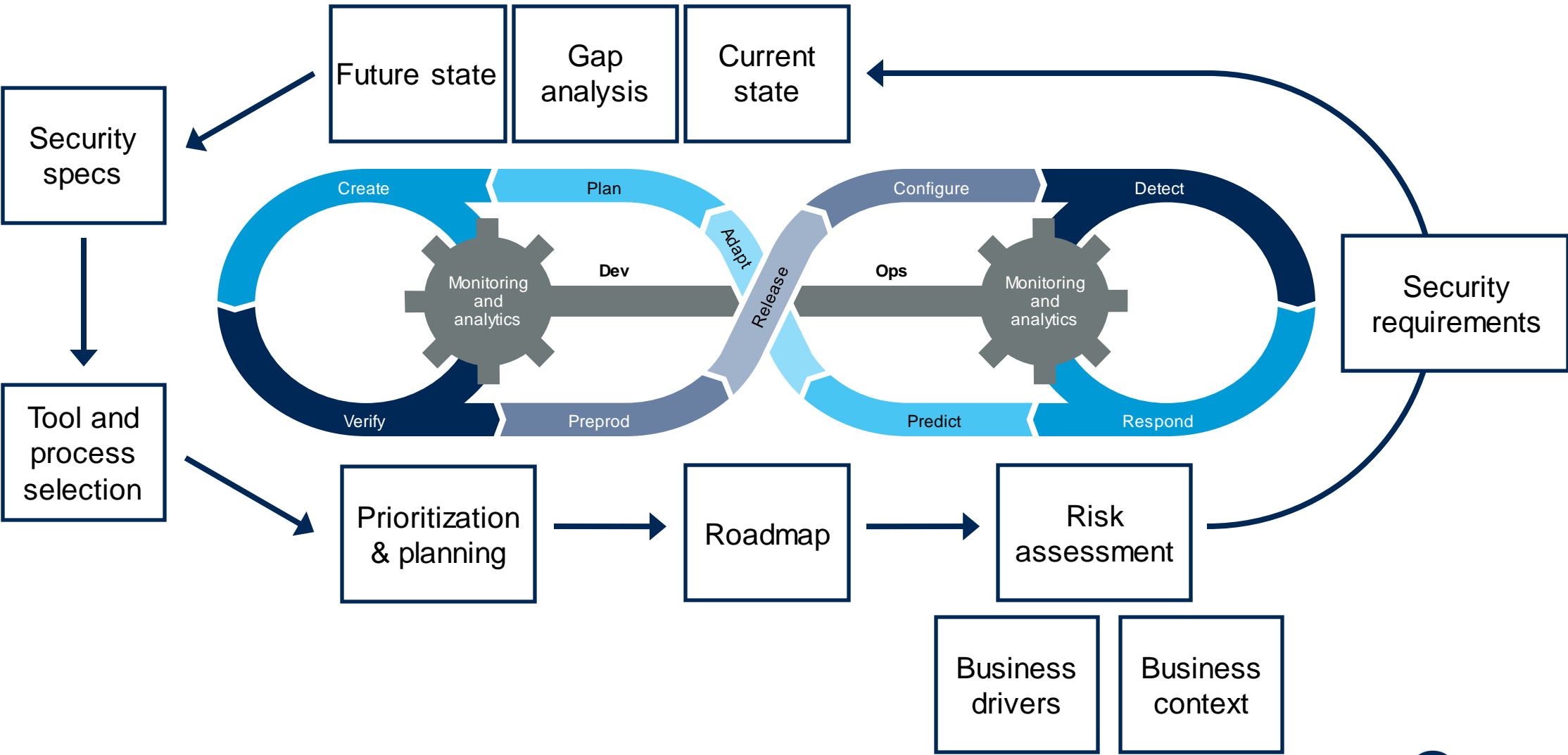
3. Recommendations for action.



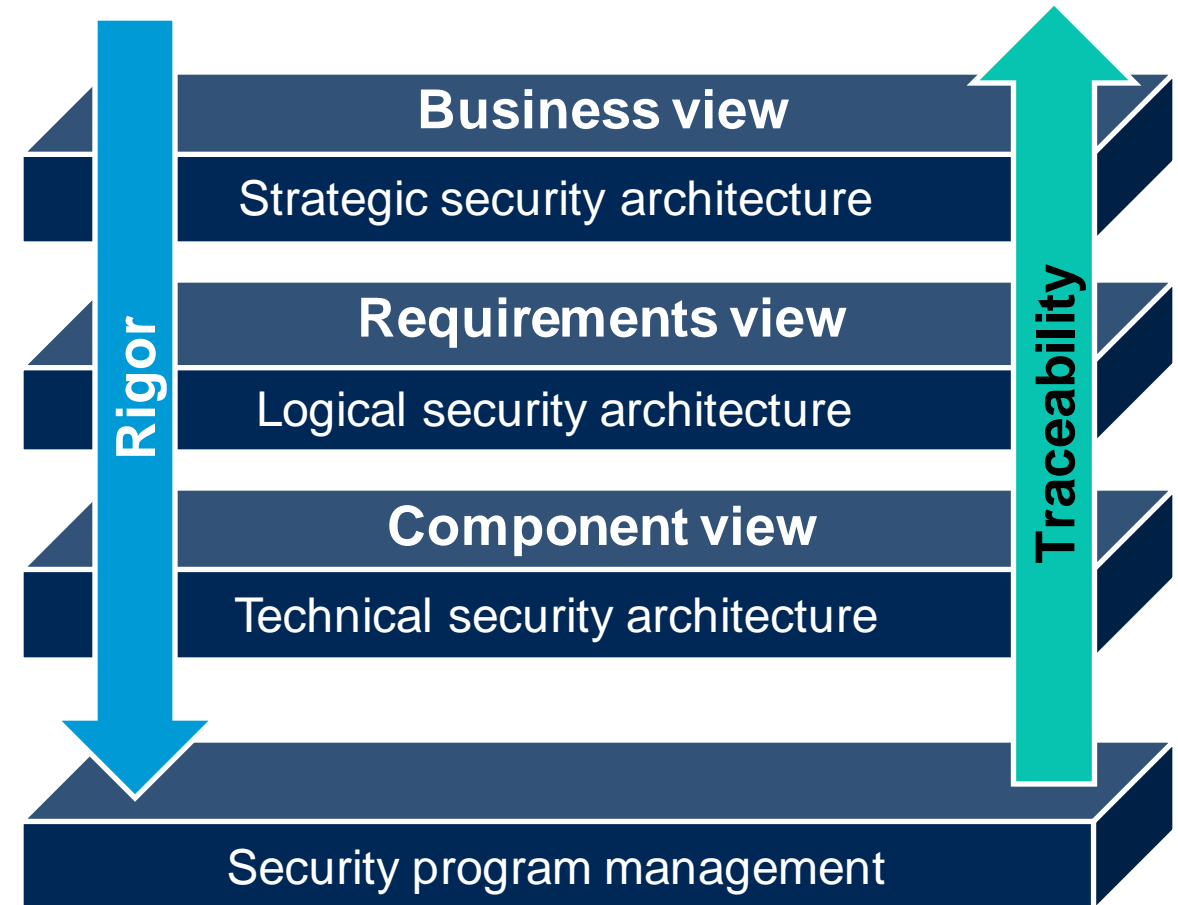
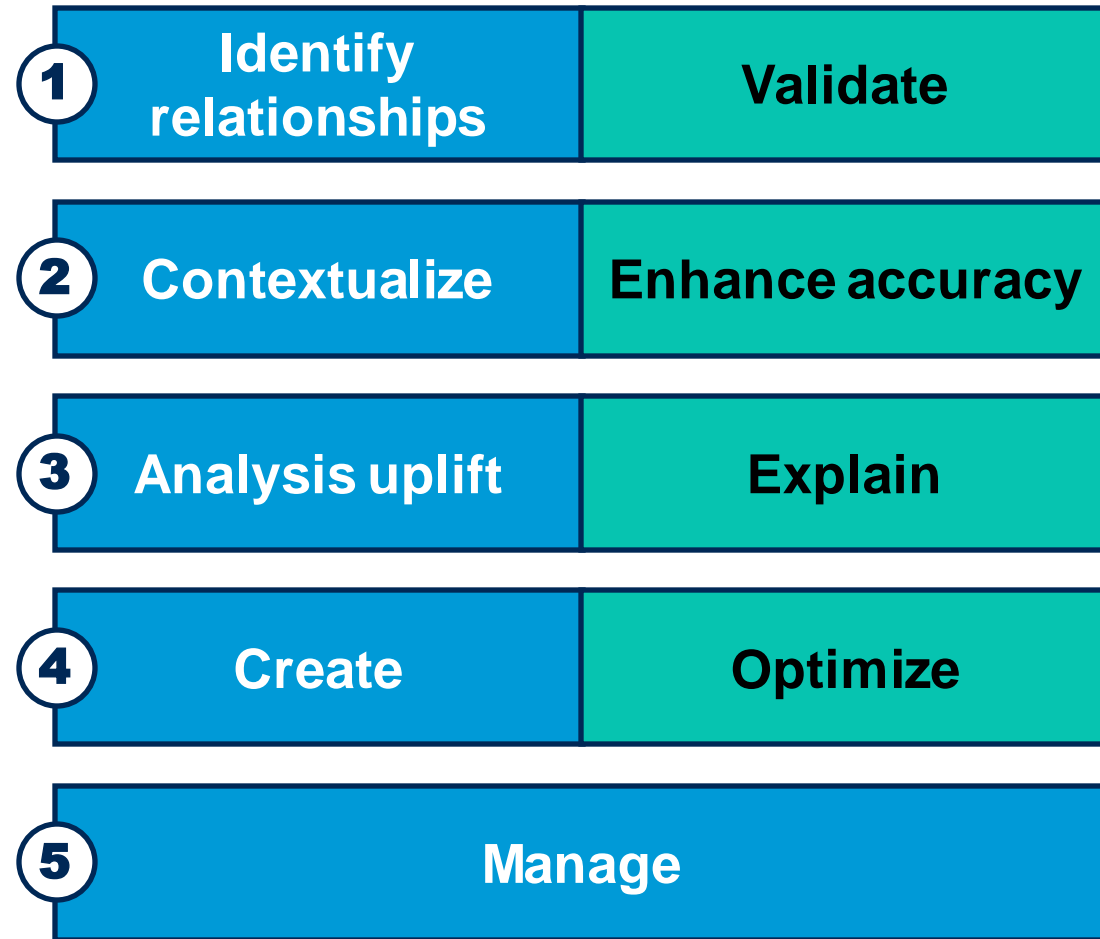
First: General Security Architecture Steps



Of Course, Applies in Agile/DevOps Too ...



5 Ways ...



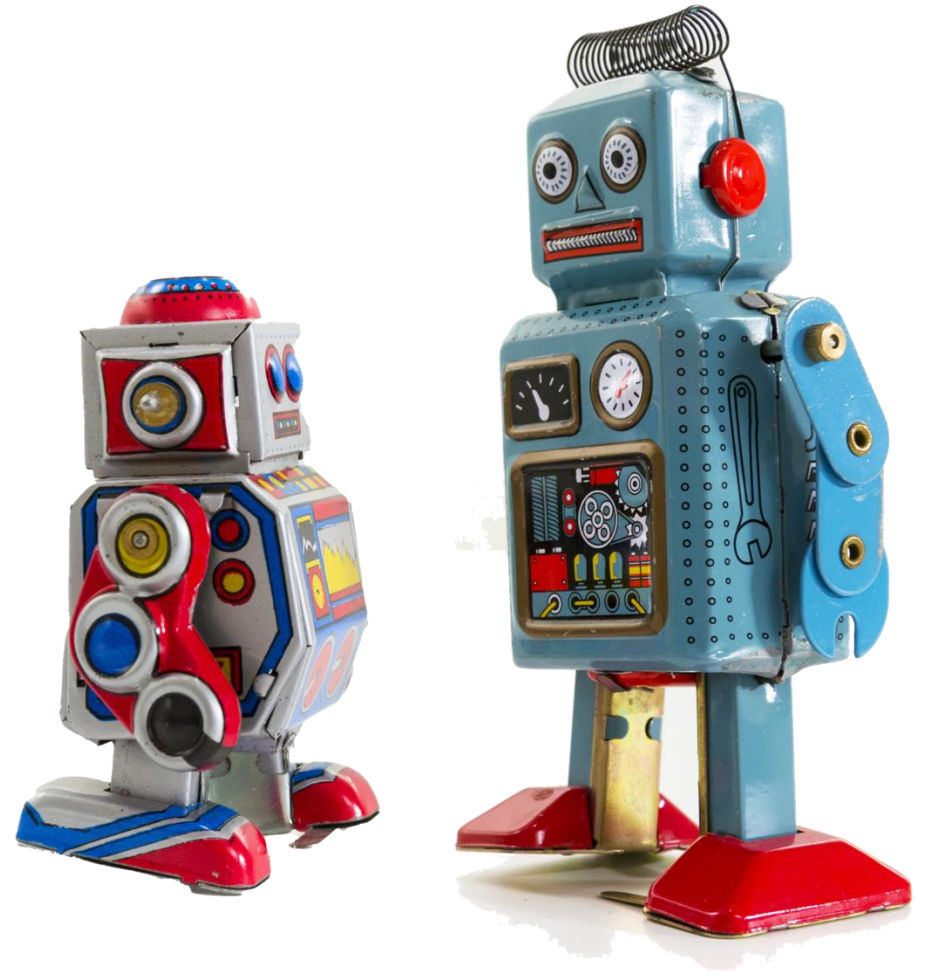
① Identify Relationships and Validation

- Identify the context for security needs.
- Develop and validate the conceptual architecture with business stakeholders.
- Lock down the scope.
- Map the drivers to strategic risks.



Ways generative AI (GenAI) could help

- Map drivers to the security frameworks to ensure consistency.
- Map drivers to threat models and MITRE ATT&CK.
- Identify the relationships between entities based on risk and security policies.



① Identify Relationships and Validation

Identify the industry contextual security drivers and map them to a security framework of choice.

Prompt: Provide a list of cybersecurity drivers based on financial services regulations in the U.S.A. ...



How can I help you today?

Plan a trip

to see the northern lights in Norway

Help me pick

a birthday gift for my mom who likes gardening

Suggest fun activities

to help me make friends in a new city

Plan an itinerary

to experience the wildlife in the Australian outback

Message ChatGPT...



ChatGPT can make mistakes. Consider checking important information.

① Identify Relationships and Validation

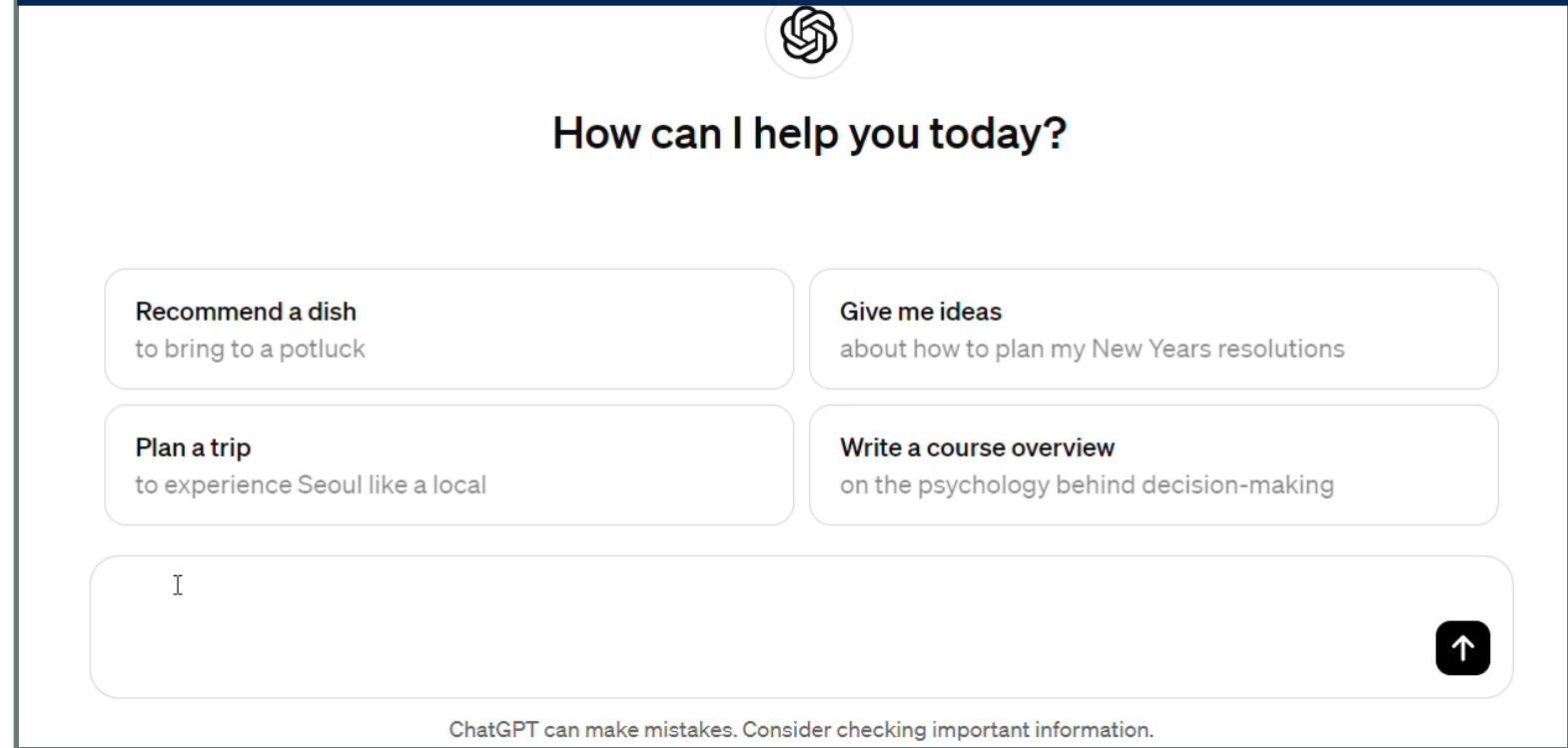
Identify industry contextual security drivers and map them to a security framework of choice

Drivers	Identify	Protect	Detect	Respond	Recover	Govern
Legal compliance	Y	Y				Y
Data protection		Y				
Risk management	Y	Y	Y	Y	Y	
Consumer trust and reputation		Y			Y	
Business continuity					Y	
Regulatory oversight	Y					Y
Interconnected systems		Y				
Industry standards and best practices		Y	Y	Y		
Incident response preparedness				Y		
Information sharing and collaboration			Y	Y		

① Identify Relationships and Validation

Suggest logical controls to address specific security attributes.

Prompt: Given the following list of security attributes, what security controls do you recommend to address them?



The screenshot shows the ChatGPT interface. At the top, the OpenAI logo is centered. Below it, the text "How can I help you today?" is displayed. There are four suggested prompts in rounded rectangular buttons: "Recommend a dish to bring to a potluck", "Give me ideas about how to plan my New Years resolutions", "Plan a trip to experience Seoul like a local", and "Write a course overview on the psychology behind decision-making". At the bottom, there is a text input field with a cursor and a send button (an upward arrow). A disclaimer at the very bottom reads: "ChatGPT can make mistakes. Consider checking important information."

① Identify Relationships and Validation

Suggest logical controls to address specific security attributes

Security attribute	Recommended security controls
Continuous	<ul style="list-style-type: none">• Implement continuous monitoring solutions for real-time threat detection and response.• Utilize continuous integration/continuous deployment (CI/CD) pipelines with automated security testing.
Protected	<ul style="list-style-type: none">• Employ encryption mechanisms to protect sensitive data at rest and in transit.• Implement access controls to restrict unauthorized access to resources.
Reliable	<ul style="list-style-type: none">• Implement redundancy and failover mechanisms to ensure system availability.• Regularly test and update backup and disaster recovery plans.
Automated	<ul style="list-style-type: none">• Utilize automated vulnerability scanning and patch management tools.• Implement automated incident response processes.
Change-managed	<ul style="list-style-type: none">• Implement change management processes to track and approve modifications to systems and configurations.• Utilize version control systems for code and configuration management.

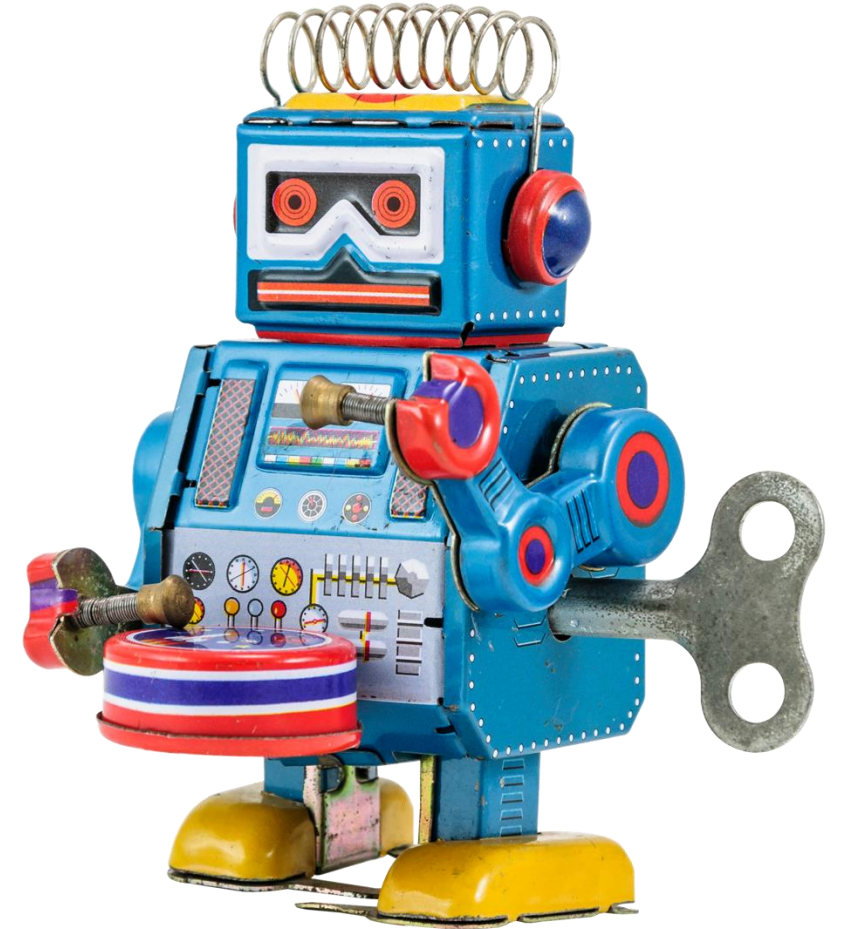
② Contextualize and Enhance

- Define trust relationships and domain mappings.
- Map assets.
- Generate clear requirements.
- Identify data assets.
- Support current state identification.



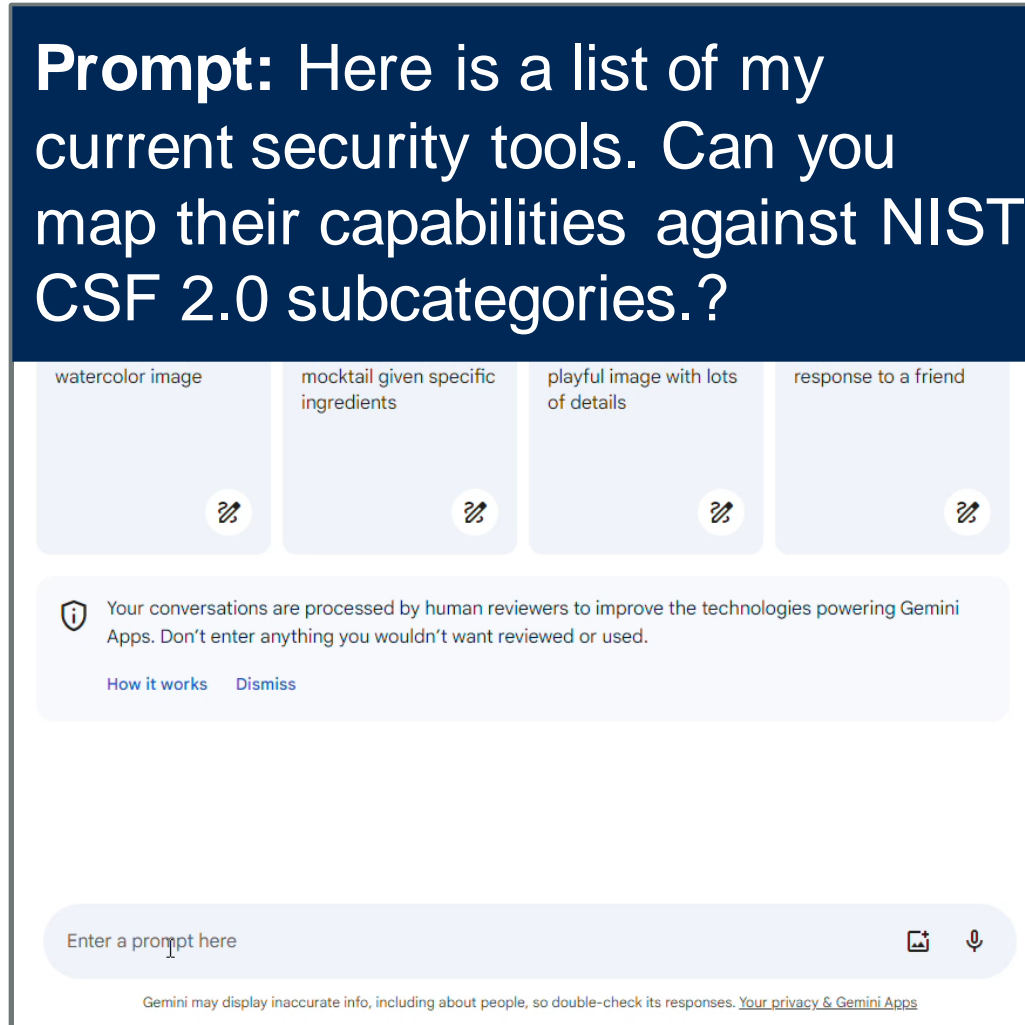
Ways GenAI could help

- Define controls needed to protect against a particular threat actor.
- Map MITRE ATT&CK TTPs to National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF).



② Contextualize and Enhance — Example

Identify NIST CSF subcategories addressed by current state capabilities.



② Contextualize and Enhance — Example

Identify NIST CSF subcategories addressed by the current state capabilities

NIST CSF subcategory	AWS S3	AWS KMS	TLS 1.2	Amazon Macie	AWS IAM	AWS Secrets Manager	CrowdStrike Falcon	AWS Inspector	AWS Security Hub	Amazon GuardDuty	AWS WAF	AWS Network Firewall	Amazon Detective	Snyk	Wiz
Identify (security state)									Y						Y
Identify (user, devices & applications)					Y										
Identify (data discovery)				Y											
Identify (system vulnerabilities)								Y						Y	
Identify (software vulnerabilities)														Y	
Identify (security misconfigurations)															Y
Protect (data at rest)	Y														
Protect (key management)		Y				Y									
Protect (data in transit)			Y												
Protect (access control)					Y										
Protect (secrets management)						Y									
Protect (preventative controls)										Y	Y				
Protect (patching)								Y							
Detect (anomalies & events)					Y		Y		Y	Y			Y		
Detect (threats & incidents)										Y				Y	
Respond (analysis & containment)							Y						Y		
Recover (recovery)							Y								

AWS = Amazon Web Services

② Contextualize and Enhance — Example

Identify NIST CSF subcategories addressed by the current state capabilities

NIST CSF subcategories	AWS IAM	AWS Secrets Manager	AWS S3	AWS Macie (for S3)	AWS Inspector	AWS Security Hub	AWS GuardDuty	AWS WAF	AWS Network Firewall	Amazon Detective	CrowdStrike Falcon	Snyk	Wiz	TLS 1.2
DE.AE.1 — asset management					Partial	Partial							?	
DE.AE.2 — security configuration management					Partial	Partial								
DE.CM.2 — security continuous monitoring				Partial	Partial	Partial	Partial	Partial	Partial	Partial				
PR.AC.1 — access control	X		Partial											
PR.AC.2 — data at rest protection		X												
PR.AC.3 — data in transit protection								Potential						
PR.AT.1 — detection capabilities				Partial	Partial	Partial	Partial	Partial	Partial	Partial	Partial			
DE.CM.4 — anomalies and events				Partial	Partial	Partial	Partial				Potential			
RS.AC.1 — security incident response						Partial	Partial							
RS.AC.5 — analysis						Partial	Partial							
RC.RP.5 — impact analysis														
RC.RP.10 — recovery plan testing and revision														

③ Analysis Uplift and Explain

- Synthesize logical architecture from concepts and other inputs.
- Identify policy relationships and define the domain framework.
- Identify the current state architecture.
- Perform gap analysis.



Ways GenAI could help

- Build requirements based on incident findings or identified threats.
- Provide root-cause summaries for findings and events with explanations.
- Increase accuracy by training your GenAI models with past findings, successful protection approaches and patterns.



③ Analysis Uplift and Explain — Example

Build requirements based on an identified threat.

Prompt: What security controls should I select to protect me against data poisoning attacks?

Create a splashy
watercolor image



Brainstorm ideas for a
mocktail given specific
ingredients



Create vibrant &
playful image with lots
of details



Help me craft a text
response to a friend



Your conversations are processed by human reviewers to improve the technologies powering Gemini Apps. Don't enter anything you wouldn't want reviewed or used.

[How it works](#)

[Dismiss](#)

Enter a prompt here



Gemini may display inaccurate info, including about people, so double-check its responses. [Your privacy & Gemini Apps](#)

③ Analysis Uplift and Explain — Example

Build requirements based on an identified threat

Control	Description	Example tools
Data validation & sanitization	Clean and validate data before training. Ensure data adheres to expected formats and identify outliers.	OpenRefine , Pandas (Python library)
Data provenance	Track the origin of your data. Identify sources and maintain an audit trail.	Apache Atlas, OpenLineage
Data monitoring	Continuously monitor data for statistical anomalies. Track metrics like distribution and correlations.	TensorBoard, scikit-learn (Python library)
Anomaly detection	Use algorithms to identify suspicious data patterns that deviate from the norm.	Isolation Forest (scikit-learn library), LSTMs (neural network architecture)
Model explainability	Use interpretable AI models to understand decision making and identify potential biases.	LIME (interpretable machine learning technique), SHapley Additive exPlanations (SHAP)
Multimodel approach	Train multiple models with different data and algorithms to avoid single point of failure.	TensorFlow, PyTorch (machine learning frameworks)
Security awareness	Train the staff on data hygiene and identifying suspicious patterns.	Security awareness training programs, workshops

④ Create and Optimize

- Create technical specifications.
- Define infrastructure security.
- Include external guidance and influences.
- Support component selection.
- Define future state architecture.



Ways GenAI could help

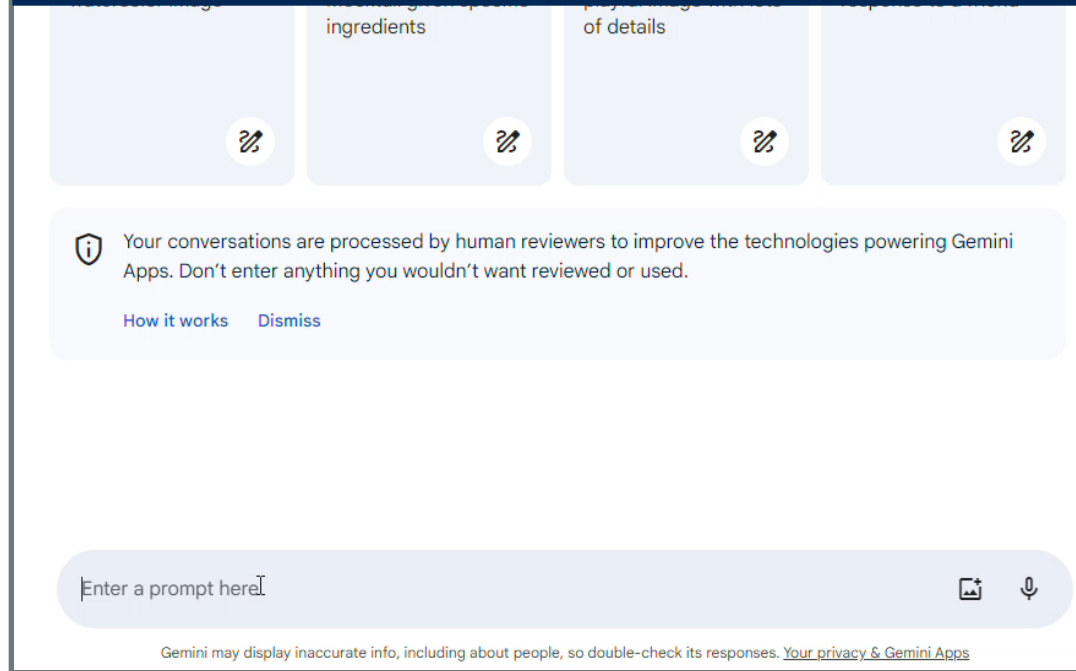
- Define security policy needed using Open Policy Agent (OPA).
- Identity the potential components for a given IT solution.



④ Create and Optimize — Example 1

Define the security policy needed using OPA in REGO for any S3 bucket deployment.

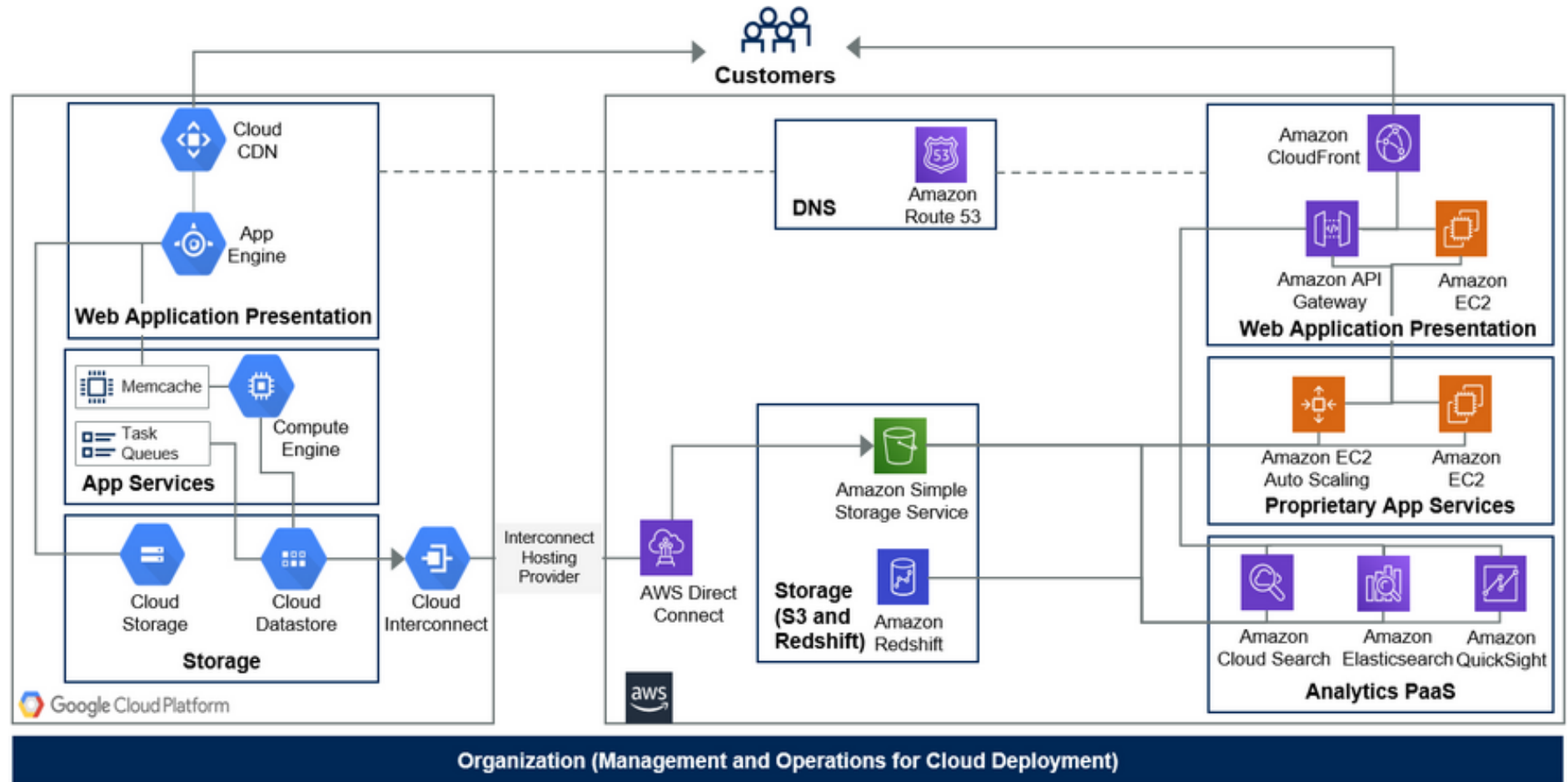
Prompt: Can you define an OPA policy that enforces encryption and prevents default routes on all AWS S3 buckets to be deployed?



④ Create and Optimize — Example 2

Identify detective security controls needed for a given logical diagram

Deployment
logical diagram
for case study



④ Create and Optimize — Example 2

Identify detective security controls needed for a given logical diagram.



④ Create and Optimize — Example 2

Identify detective security controls needed for a given logical diagram

Category	GCP	AWS
Log management & analysis	Cloud logging, cloud monitoring	Amazon CloudWatch
Security information & event management (SIEM)	Integrates with cloud logging (external tool needed)	Integrates with CloudWatch (external tool needed)
Security posture management (SPM)	Cloud security command center (SCC)	Amazon Security Hub, AWS Config, Amazon Inspector
Threat detection & investigation	* Cloud SCC with features like: * event threat detection (premium) * security health analytics (SHA) * Amazon GuardDuty	* Amazon GuardDuty * Amazon Detective (for forensic analysis)
Vulnerability scanning	Cloud security scanner (integrated with SCC)	Amazon Inspector (integrated with Security Hub)
Anomaly detection	Cloud monitoring can be configured for anomaly detection	Amazon CloudWatch can be configured for anomaly detection

⑤ Manage

- Generate management summaries.
- Create stakeholder communications.
- Support roadmap construction.
- Identify risk-based priorities.



Ways GenAI could help

- Provide a short summary of a large architectural description for leadership.
- Map future state architecture components to a roadmap based on perceived risk.



⑤ Manage — Example

Leadership asks whether our current security controls will address DHS CISA's list of small business cybersecurity risks.



⑤ Manage — Example

Leadership asks whether our current security controls will address DHS CISA's list of small business cybersecurity risks

Security tool	Ransomware/ malicious code/ destructive malware	Spyware	DDoS	Phishing/email imposters	Network infrastructure threats	Website threats	Wireless network threats	Mobile application threats
AWS IAM & Secrets Manager	Reduces attack surface	Limits data access	—	—	Limits access to resources	Limits access to web applications	Limits access to resources	—
CrowdStrike Falcon	Detects and responds to deployment	Potential detection	—	—	—	—	—	—
Snyk	Scans for vulnerabilities	—	—	—	—	—	—	Scans mobile app code (if applicable)
Amazon Inspector	Identifies vulnerabilities	—	—	—	Identifies vulnerabilities	Identifies vulnerabilities	Identifies vulnerabilities	—
AWS GuardDuty & Amazon Detective	Detects suspicious activity	—	—	—	—	—	—	—
AWS WAF	—	—	Mitigates DDoS attacks	—	—	Protects web applications	—	—
AWS Shield (assumed)	—	—	Protects against DDoS attacks	—	—	—	—	—
User education & awareness training	—	—	—	Helps prevent phishing	—	—	—	—
DMARC (implemented with email provider)	—	—	—	Helps prevent email spoofing	—	—	—	—
AWS Network Firewall	—	Limits unauthorized communication	—	—	Limits access to resources	Protects web applications	Limits access to resources	—
AWS Config	Monitors for misconfigurations	—	—	—	Identifies configuration drift	Identifies configuration drift	Identifies configuration drift	—
AWS CloudTrail	Aids in threat detection	—	—	—	—	—	—	—
Wiz (if applicable)	—	Protects against data exfiltration	—	—	—	—	—	—

Key Issues

1. Warnings and caveats.

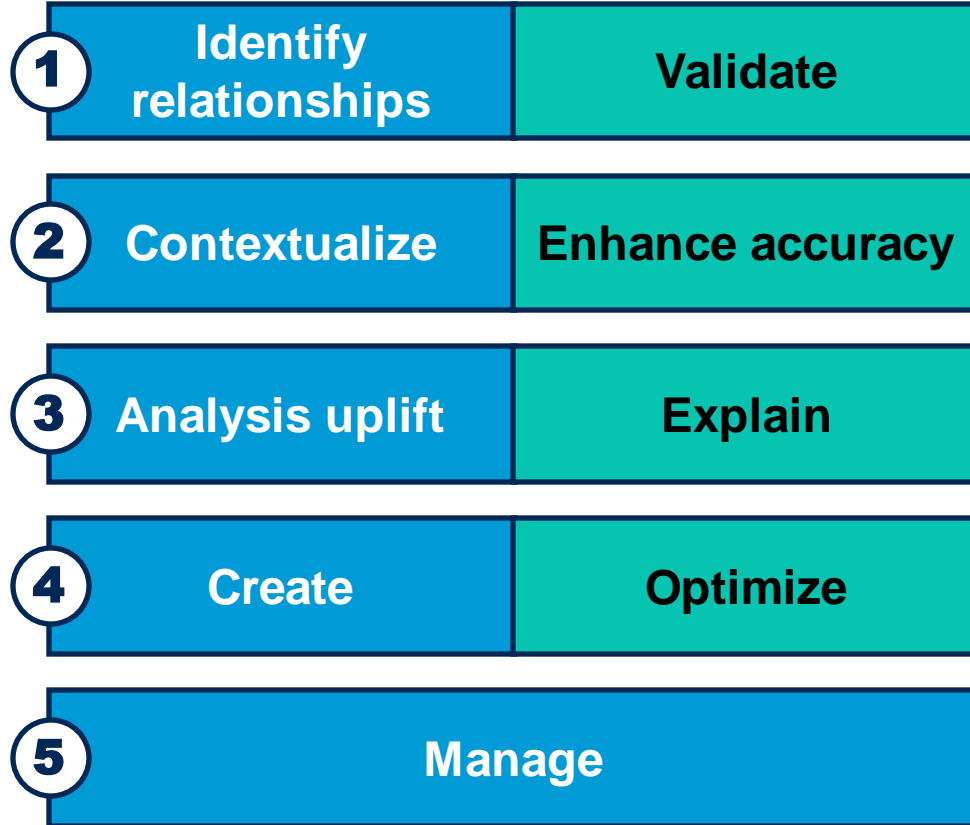
2. Five ways:

- Contextualize and enhance
- Analysis uplift and explain
- Identify relationships and validation
- Create and optimize
- Manage

3. Recommendations for action.



Recommendations for Action

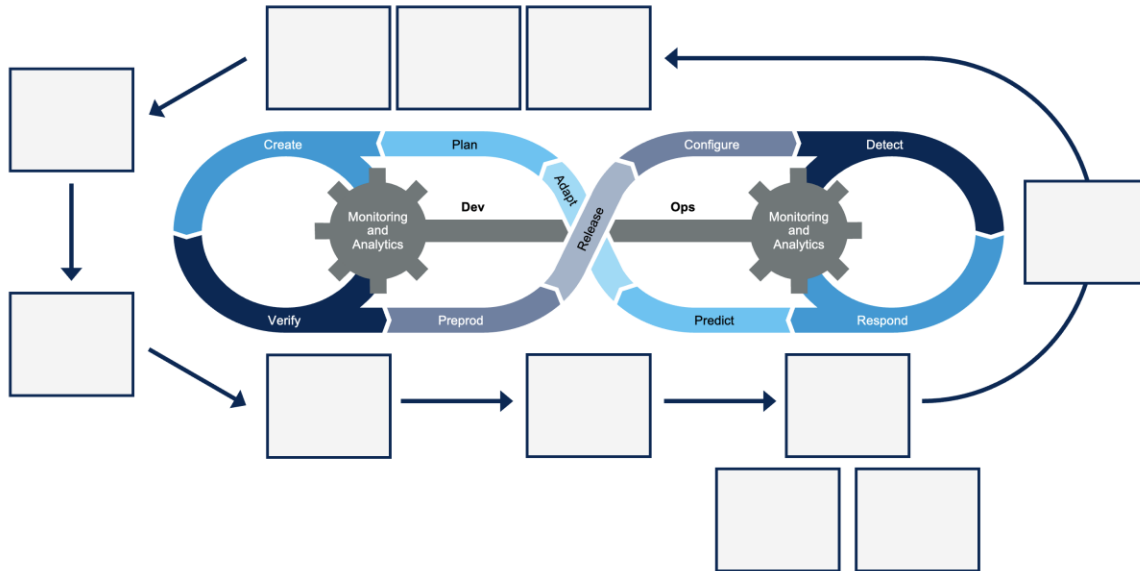


- ✓ Build your own dedicated **private** security GenAI chatbot.
- ✓ Fine-tune it with the widest set of security relevant material:
 - **Strategic** — company policies, strategies, plans, reports, strategic risk and filings.
 - **Logical** — required frameworks, security risks.
 - **Technical** — current state architecture, technical plans, roadmaps, BOMs/SBOMs.
- ✓ Define and enhance prompt engineering for security architecture.
- ✓ Train your architects.
- ✓ (Warnings and caveats still apply!)

Into the Future ...

Self-fulfilling, proactive and threat-responsive architecture:

- Security drivers and goals are codified.
- Security policy is specified based on risk appetite.
- Self-fulfilling architecture would select aligning controls.



Seek to implement automation to:

- Identify deviations from security policy.
- Design remediation.
- Return to secure posture.
- Identify risks and specific threats.
- Proactively realign architecture to counter.

Recommendations

- ④ Utilize GenAI to help accelerate security architecture processes and ensure it remains central and relevant even in fast-moving agile development.
- ④ Use public GenAI services to get general insights and support. Remember to be cautious. Do not input sensitive information here, and use results judiciously.
- ④ Research and develop private GenAI tools and services. Look to build your own so that internal data can be used to improve architectural decisions.

Recommended Research

To learn more about access to Gartner research, expert analyst insight, and peer communities, contact your Gartner representative or click on “Become A Client” on gartner.com to speak with one of our specialists.

- 🔍 [Use Security Architecture to Enable “Security by Design”](#)
Richard Bartley
- 🔍 [2024 Planning Guide for Security](#)
Richard Bartley, Patrick Hevesi and Others
- 🔍 [The Future of Security Architecture: Cybersecurity Mesh Architecture \(CSMA\)](#)
Patrick Hevesi and Mary Ruddy
- 🔍 [Innovation Guide for Generative AI in Trust, Risk and Security Management](#)
Avivah Litan, Jeremy D’Hoinne and Gabriele Rigon
- 🔍 [Generative AI Adoption: Top Security Threats, Risks and Mitigations](#)
Dennis Xu and Kevin Schmidt
- 🔍 [Reference Architecture Resource Center](#)

Access to Gartner research is subject to individual subscription type and product entitlements.