



Cloud Security Alliance

The State of Cloud and AI Security

February 2025

Building security best practices
for next generation IT

220k+

INDIVIDUAL MEMBERS

140+

CHAPTERS

500+

CORPORATE MEMBERS

30+

ACTIVE WORKING GROUPS

3,400+

STAR REGISTRY
ENTRIES (provider
certification)

12,000+

CONTRIBUTING RESEARCH
VOLUNTEERS



Research, Best
Practices, Education
and Certification



Strategic partnerships with
governments, research
institutions, professional
associations and industry

2009

CSA FOUNDED: 501(c)6 non-profit

SEATTLE/BELLINGHAM// GLOBAL
HEADQUARTERS



BERLIN //
EMEA HEADQUARTERS

SHANGHAI // GREATER
CHINA REGION

SINGAPORE // ASIA PACIFIC
HEADQUARTERS

*World's most vital
cybersecurity
community*

CSA's 3 Pillars



Key priorities from large enterprises

- Robust Generative AI strategy
- State of the art cloud security: cloud-native, multi-cloud
- Security at scale: automation, orchestration, continuous controls monitoring
- Securing DevOps and “shifting left”
- Zero Trust as broad guiding principles beyond identity and network layer
- Data: Governance, Sovereignty, Security
- Supply Chain, Third Party Risk Management and Vendor Procurement
- Global optimization & standardization VS regional & nation-state priorities
- Cybersecurity workforce readiness

The Cloud and
AI had a baby
and they
named it
ChatGPT



Cloud history by version number

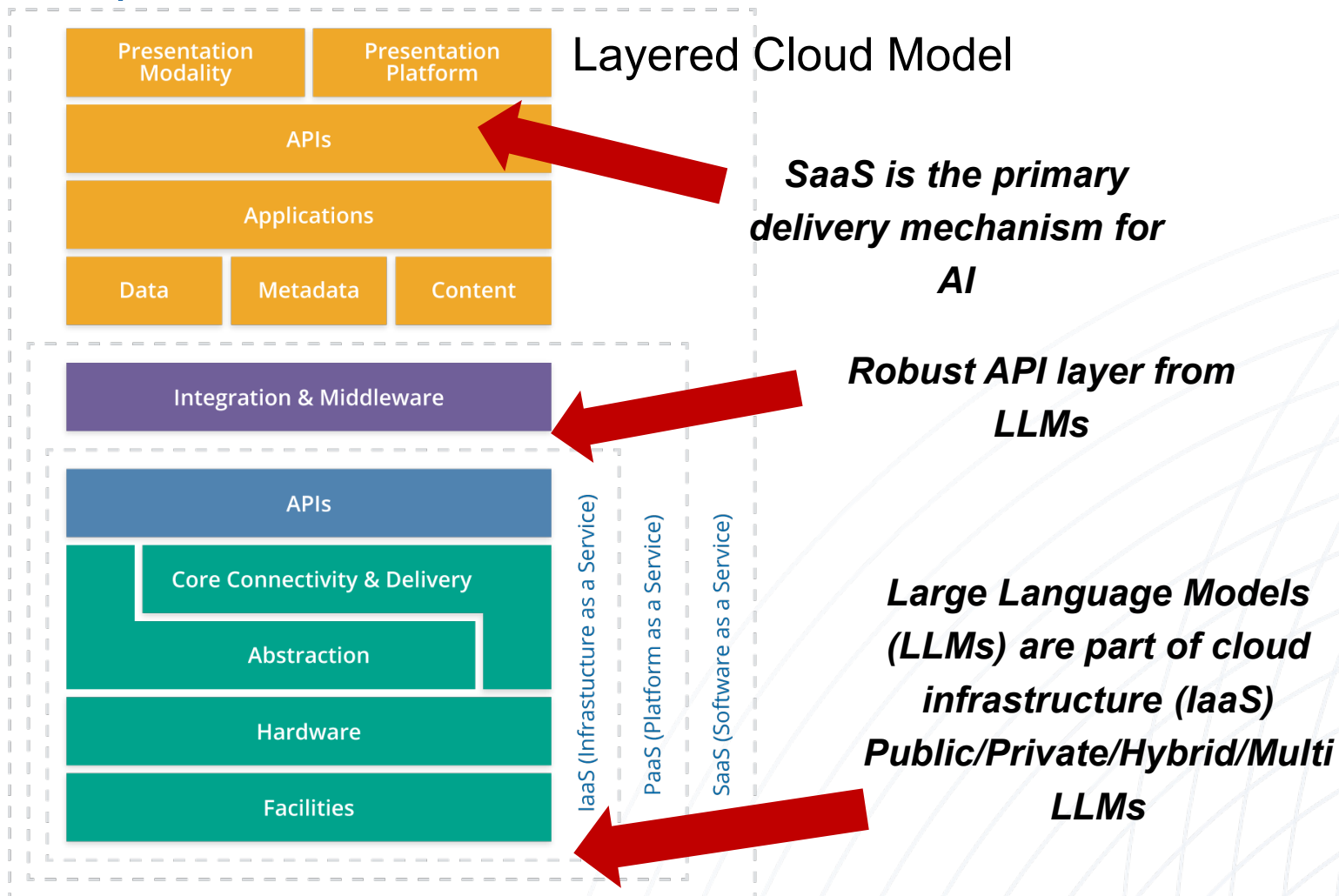
Cloud 1.0 – Cloud delivers traditional IT services (e.g. Virtual Machines) in new business model (2008-2016)

Cloud 2.0 – Cloud Native Technologies & Frameworks: DevOps, Containers, Serverless, CNAPP, etc. Pandemic accelerates move to cloud and rise of Zero Trust as the strategy for securing cloud sprawl (2016-mid 2022)

Cloud 3.0 – Tech economic downturn, Rise of Generative AI and its merger with Cloud 2.0 (mid 2022-)

Context: AI emergence echoes Cloud emergence

Layered Cloud Model From the 2009 CSA archives



- Enterprises will vary in adoption pace
- Curious innovators turn prototypes into new mission critical systems
- GenAI becoming pervasive in SaaS, App stores
- Industries are transformed
- Shared responsibility
- Remember your cloud journey, it will echo with AI

Top Threats to Cloud Computing



1. Misconfiguration and inadequate change control
2. Identity and Access Management
3. Insecure interfaces and APIs
4. Inadequate selection/implementation of cloud security strategy
5. Insecure third-party resources
6. Insecure software development
7. Accidental cloud disclosure
8. System vulnerabilities
9. Limited cloud visibility/observability
10. Unauthenticated resource sharing
11. Advanced Persistent Threats

<https://cloudsecurityalliance.org/research/working-groups/top-threats>

Top Threats of Large Language Models

LLM01: Prompt Injection

LLM02: Sensitive Information Disclosure

LLM03: Supply Chain Vulnerabilities

LLM04: Data and Model Poisoning

LLM05: Improper Output Handling

LLM06: Excessive Agency

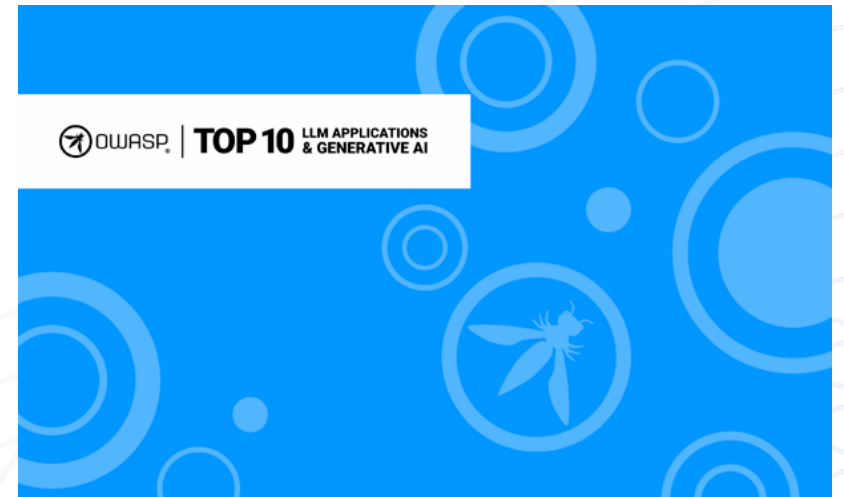
LLM07: System Prompt Leakage

LLM08: Vector and Embedding Weaknesses

LLM09: Misinformation

LLM10: Unbounded Consumption

www.owasp.org



OWASP Top 10 for LLM Applications 2025

Version 2025
November 18, 2024

OWASP PDF v4.2.0a 20241114-202703

ChatGPT's correlation

OWASP Top 10 (LLM)	CSA Top Threats to Cloud Computing
LLM01: Prompt Injection	Insecure Interfaces & APIs
LLM02: Sensitive Information Disclosure	Accidental Cloud Data Disclosure
LLM02: Sensitive Information Disclosure	Insecure Interfaces & APIs
LLM03: Supply Chain	Insecure Third-Party Resources
LLM03: Supply Chain	Insecure Software Development
LLM04: Data and Model Poisoning	Insecure Software Development
LLM04: Data and Model Poisoning	Advanced Persistent Threats
LLM05: Improper Output Handling	Insecure Interfaces & APIs
LLM06: Excessive Agency	Identity & Access Management (IAM)
LLM06: Excessive Agency	Unauthenticated Resource Sharing
LLM07: System Prompt Leakage	Misconfiguration & Inadequate Change Control
LLM07: System Prompt Leakage	Accidental Cloud Data Disclosure
LLM08: Vector and Embedding Weaknesses	System Vulnerabilities
LLM09: Misinformation	Limited Cloud Visibility/Observability
LLM10: Unbounded Consumption	Misconfiguration & Inadequate Change Control

The CSA Security, Trust, Assurance & Risk (STAR) program

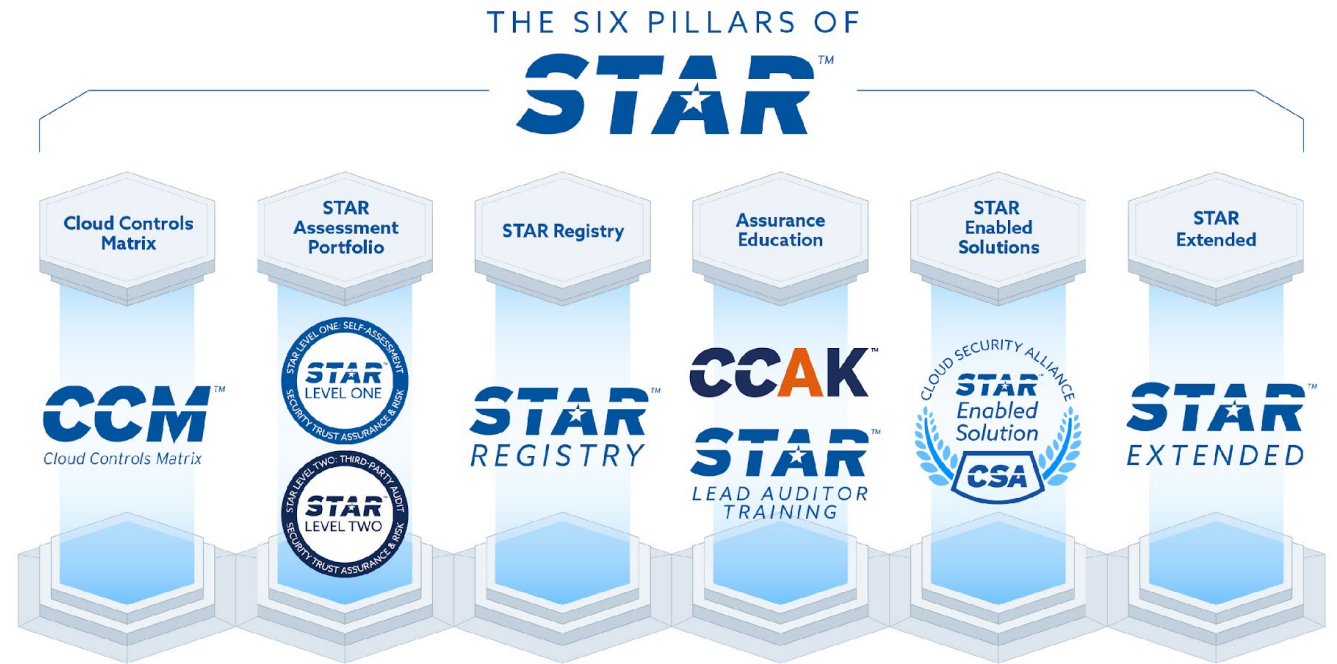
STAR = Security, Trust, Assurance & Risk

Launched in 2011, over 3,400 registered provider entries

Adopted by nations, industries and enterprises

Comprehensive program pillars

All major audit firms & ISO certification bodies perform STAR assessments



The Cloud Security Standard: Cloud Controls Matrix (CCM) v4

- A&A** Audit and Assurance
- AIS** Application & Interface Security
- BCR** Business Continuity Mgmt & Op Resilience
- CCC** Change Control and Configuration Management
- CEK** Cryptography, Encryption and Key Management
- DCS** Datacenter Security
- DSP** Data Security and Privacy
- GRC** Governance, Risk Management and Compliance
- HRS** Human Resources Security

- IAM** Identity & Access Management
- IPY** Interoperability & Portability
- IVS** Infrastructure & Virtualization Security
- LOG** Logging and Monitoring
- SEF** Sec. Incident Mgmt, E-Disc & Cloud Forensics
- STA** Supply Chain Mgmt, Transparency & Accountability
- TVM** Threat & Vulnerability Management
- UEM** Universal EndPoint Management

Composed of:

- 17 security domains
- 197 Controls
- CAIQ Questionnaire

Encompasses

- Control Applicability and Ownership
- Architectural Relevance – Cloud Stack Components
- Organizational Relevance

Transparency in CSA STAR

Cloud providers are **REQUIRED** to also have a STAR Level I Self Assessment even if they are audited – you have the ability to **review detailed cloud security control implementation** information yourself

CAIQ [™] CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.							
Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification
CEK-03.I	Are data at-rest and in-transit cryptographically protected using cryptographic libraries certified to approved standards?	Yes	Shared CSP and CSC	Data at-rest and in-transit are encrypted in the core infrastructure of ABC Cloud Co using cryptographic libraries certified to approved standards	Customers of ABC Cloud Co are responsible for encryption and key management within their environment. ABC Cloud Co provides cryptographic services which can be availed by customer.	CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.
				CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)		
				Data at-rest and in-transit are encrypted in the core infrastructure of ABC Cloud Co using cryptographic libraries certified to approved standards	Customers of ABC Cloud Co are responsible for encryption and key management within their environment. ABC Cloud Co provides cryptographic services which can be availed by customer.		

Shared Security Responsibility

Now available, the Cloud Controls Matrix (CCM) Implementation Guidelines allow you to **compare the cloud provider control assertions with CSA's Shared Security Responsibility Model** to assure that controls are implemented correctly by both the provider and user and **eliminate the gaps**

Control Title	Control ID	Control Specification
Data Encryption	CEK-03	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards.
Control Ownership by Service Model		
IaaS	PaaS	SaaS
Shared (Dependent)	Shared (Dependent)	Shared (Dependent)
SSRM Guidelines		
CSP	CSC	
<p>Control Ownership Rationale. In the context of the service delivery models, IaaS, PaaS, and SaaS, the CSP has the primary responsibility of managing and providing cryptographic protection for data at rest and in transit, using certified cryptographic libraries, but the control's implementation is also dependent on the CSC, making it a shared but dependent responsibility.</p> <p>Implementation Guidelines. This measure enhances the security posture by safeguarding sensitive information from unauthorized access during storage and transmission. Using cryptographic libraries certified to approved standards adds an extra layer of assurance, meeting industry benchmarks for encryption, and instilling confidence in both the CSP and CSCs regarding the confidentiality and integrity of their data</p>	<p>Control Ownership Rationale. The control ownership for the encryption of both at-rest and in-transit data is shared with a dependency between the CSP and CSC. While the CSP provides the cryptographic tools and libraries, the CSC is responsible for correctly implementing and using these tools to ensure the appropriate level of data protection.</p> <p>Implementation Guidelines. From the CSC perspective, the cryptographic protection of data at-rest and in-transit using certified libraries ensures the confidentiality and integrity of their sensitive information within the cloud environment. This control provides reassurance to CSCs in the security measures implemented by the CSP and safeguarding their data against potential security threats.</p>	

Download CCM Implementation Guidelines here: <https://cloudsecurityalliance.org/research/cloud-controls-matrix/>

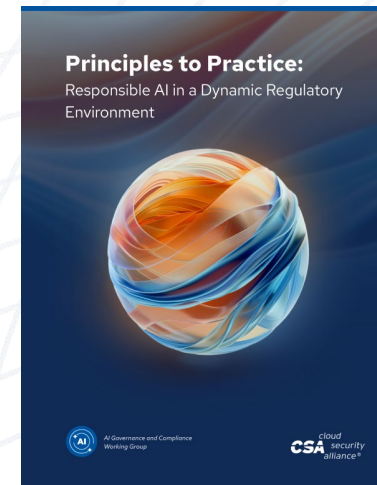
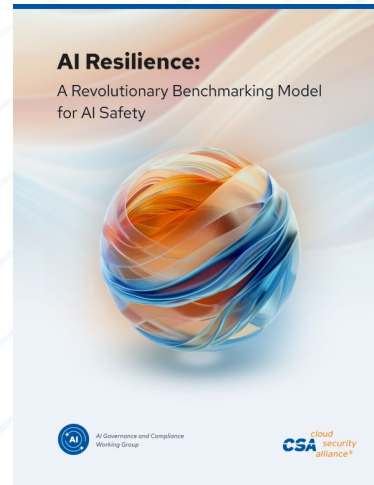
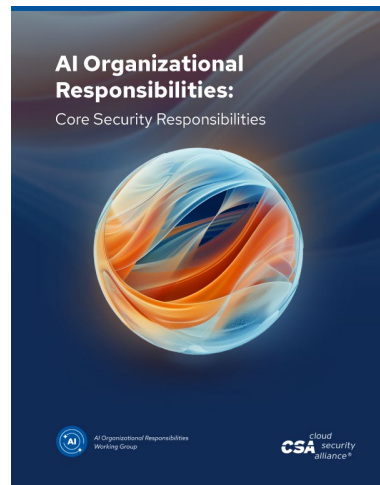
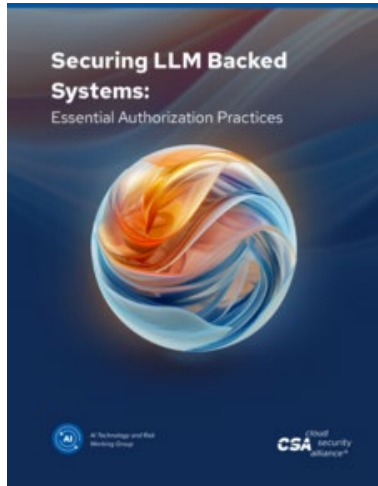
What about AI Security?



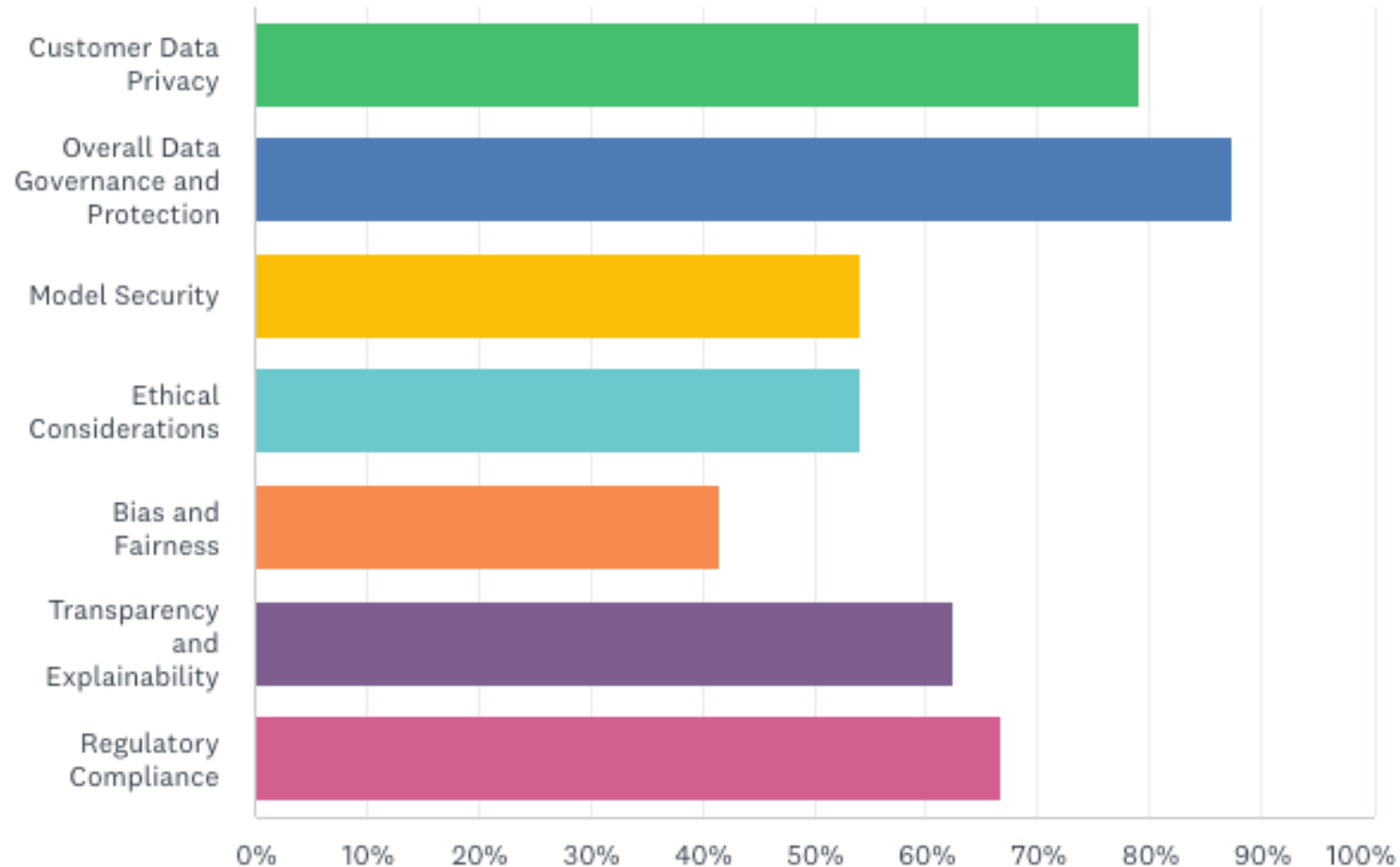
AI Controls Matrix in peer review, available in Q2

Leading portfolio of AI best practices

AI Safety Initiative



Current Enterprise AI Safety & Security Priorities *



*Survey of CSA community, September 2024

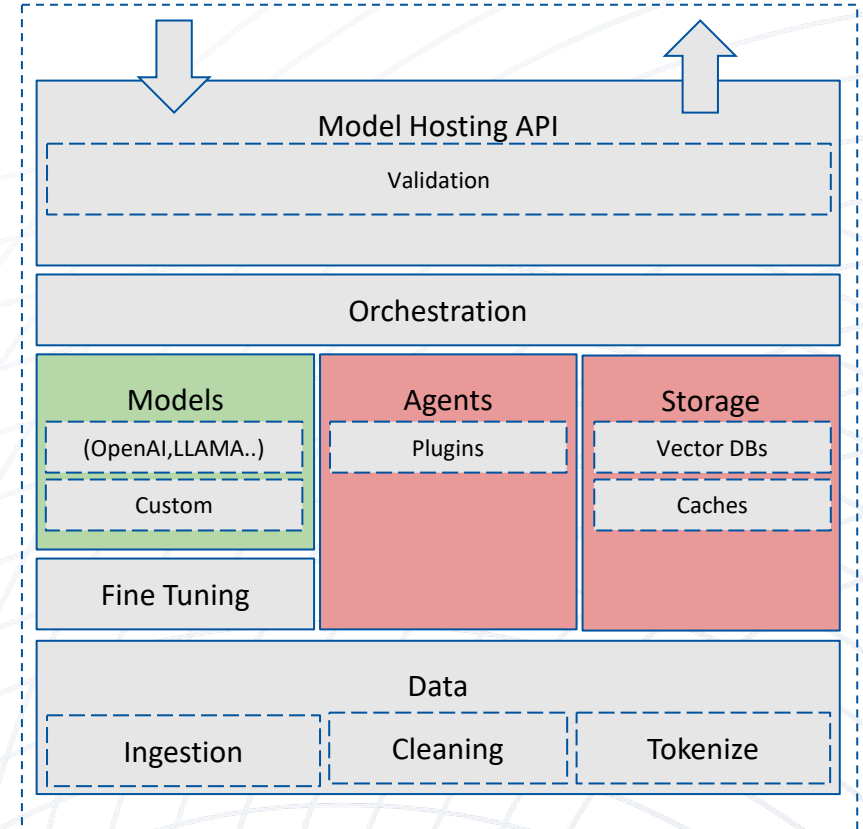
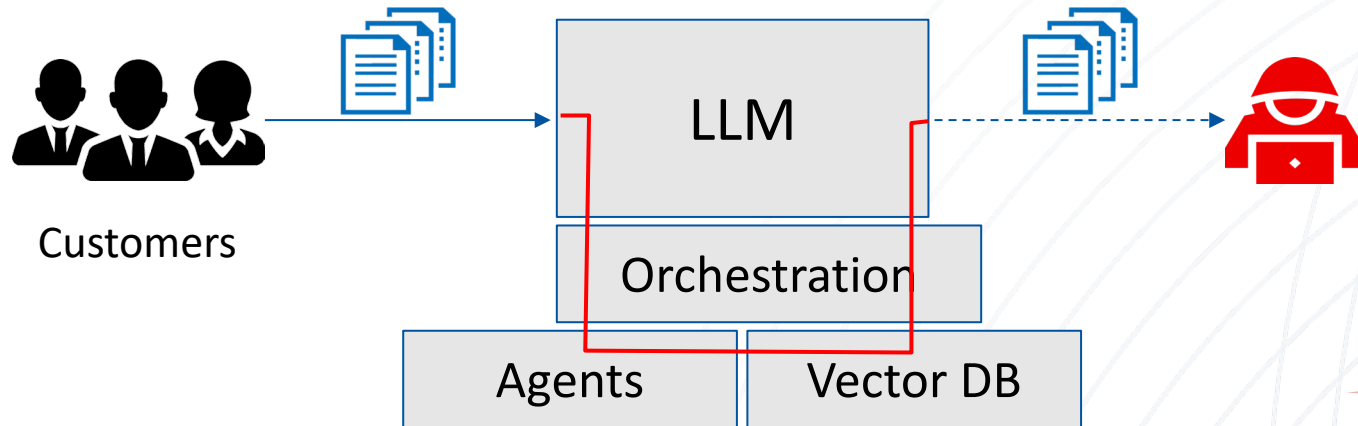
LLM Data leakage is traditional data security

Scenario 1



Data Leakage Risk is Low

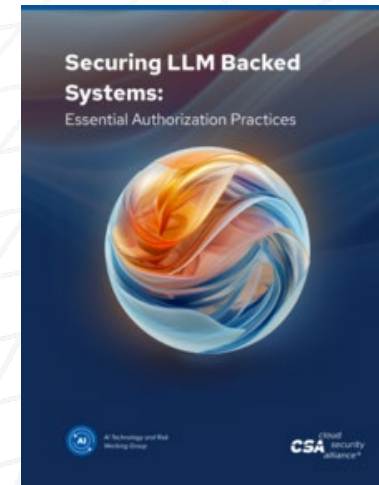
Scenario 2



Data Leakage becomes a real threat. ACL is critical

How organizations are implementing GenAI

- Organization-wide, Top down, Bottom up
 - Dimensions: Security, Trust, Data Privacy, Ethics, Compliance
- Risk Management
- Data Governance
- Model Governance
- Zero Trust Philosophy
- Training & Awareness
- Understanding Shared Security Responsibility (Internally, Third Parties, Supply Chain)



AI Organizational Responsibilities

Comprehensive Security Framework

Explores core security responsibilities essential for the development and deployment of AI and ML systems, focusing on data security, model security, and vulnerability management to ensure the security, privacy, and integrity throughout their lifecycle.

Data Security and Privacy

Emphasizes measures such as data authenticity, anonymization, pseudonymization, data minimization, access control, and secure storage and transmission to protect sensitive information and comply with data protection regulations.

Model Security

Discusses the importance of robust access controls, secure runtime environments, and MLOps pipeline security to mitigate risks associated with AI models and ensure their reliable operation.

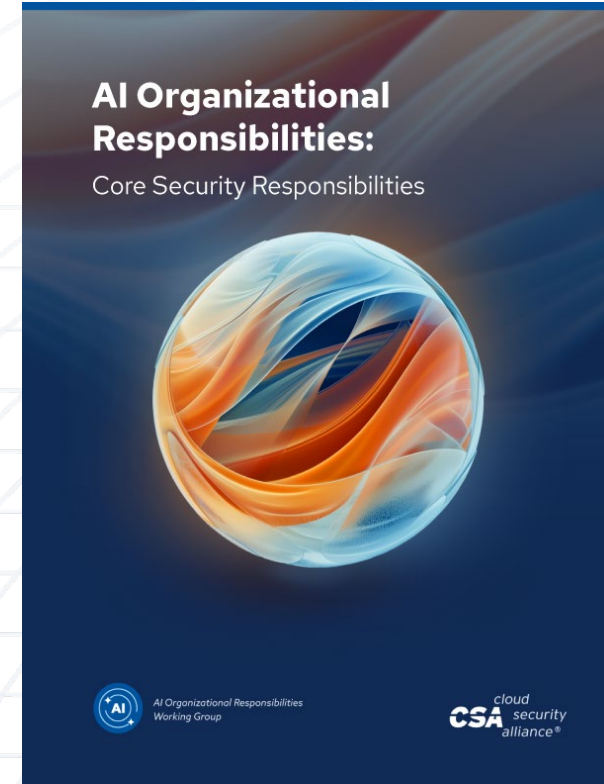
Vulnerability Management

Highlights the necessity for an AI/ML asset inventory, continuous vulnerability scanning, risk prioritization, remediation tracking, and exception handling to proactively manage vulnerabilities and minimize security breaches.

Evaluation and Governance

Utilizes quantifiable evaluation criteria and the RACI model for clear role definitions, supplemented by high-level implementation strategies and continuous monitoring to ensure robust governance.

www.cloudsecurityalliance.ai



AI Model Risk Management Framework

The Four Pillars of AI MRM Framework

Model Cards: Provide transparency about the model.

- Model's details and purpose, training data, performance metrics, known limitations.

Data Sheets: Document the training data.

- Data source and acquisition methods, data composition and characteristics, potential biases and limitations, ethical considerations.

Risk Cards: Identify and categorize potential risks.

- Risk category, risk description, potential impact, severity level, likelihood, mitigation strategies.

Scenario Planning: Explore hypothetical situations to identify risks.

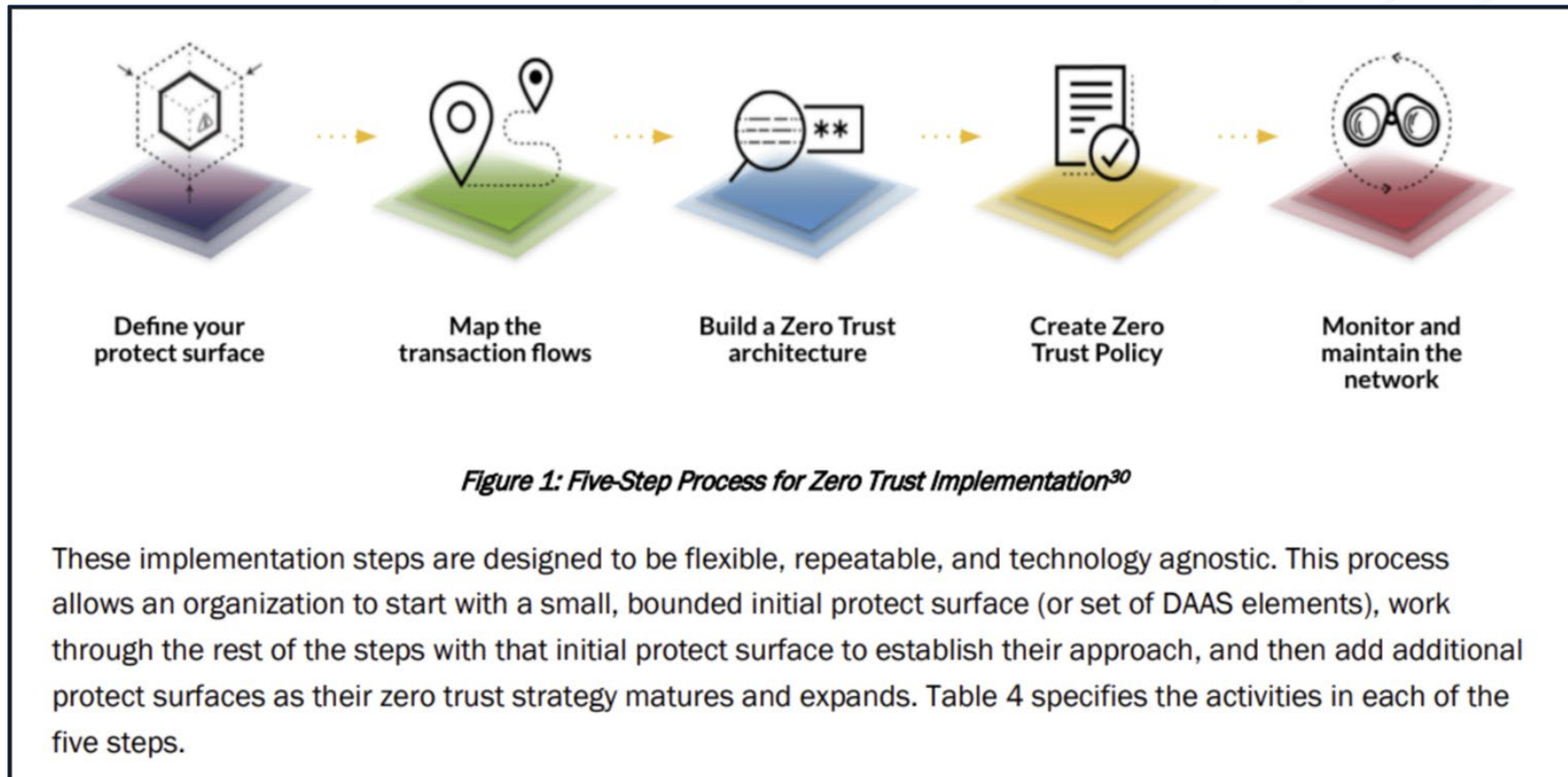


www.cloudsecurityalliance.ai

Zero Trust to protect the Cloud 3.0 merger with AI

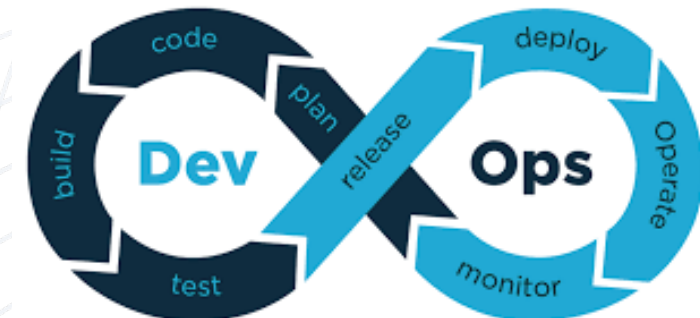
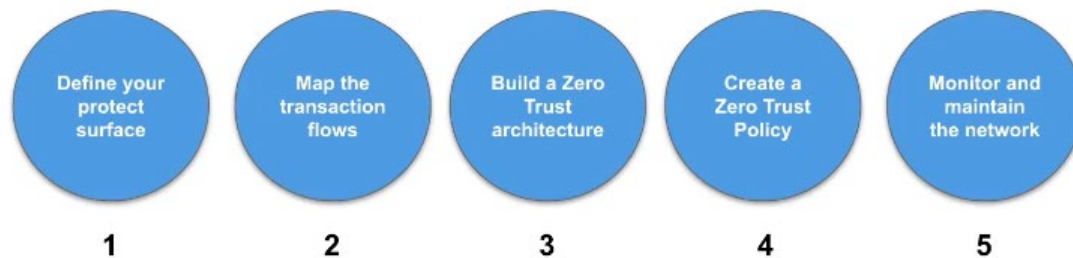


www.cloudsecurityalliance.org/zt

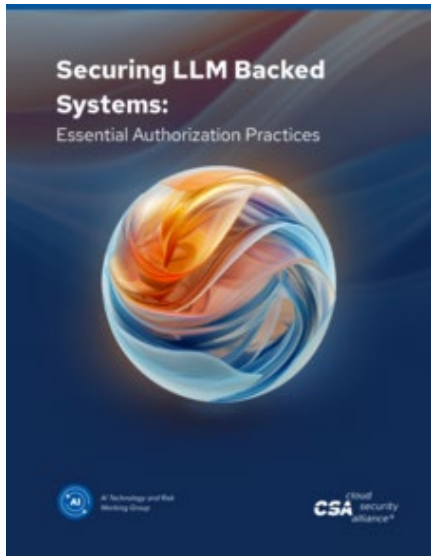


Cloud Native Zero Trust implementation is immature

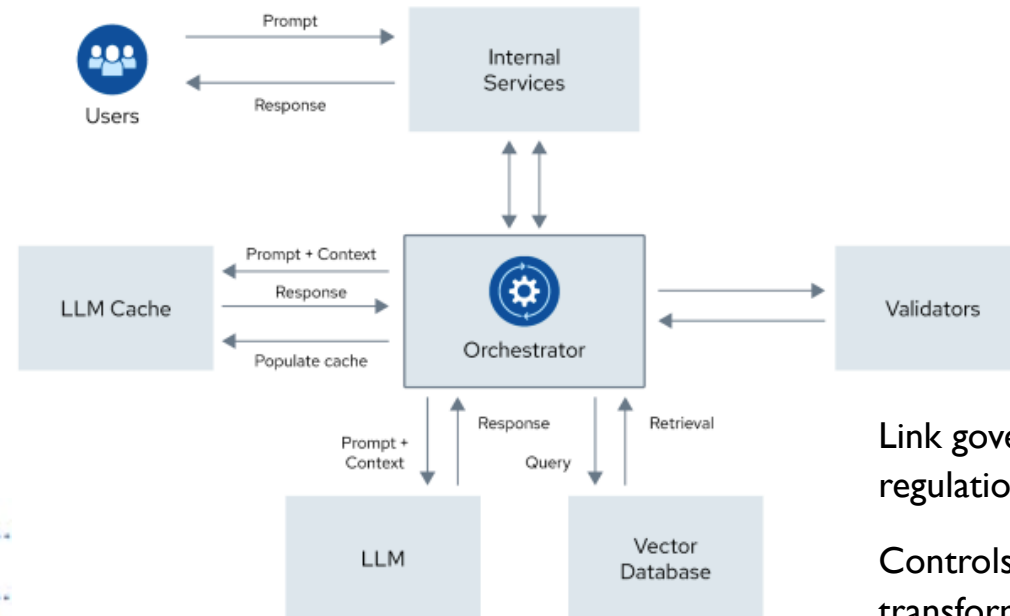
- Cloud Native Infrastructure Insecurities
 - Shadow Access endemic
 - 72% of containers live less than 5 minutes
 - 90% of granted permissions are not used
 - 87% of container images have high or critical vulnerabilities
 - 15% of high or critical vulnerabilities are in use
 - *Source: Sysdig Cloud Native Security & Usage Report 2023*
- Priority to apply ZT to DevOps & Microservices
 - Extend 5 Pillars to “Cloud Native”
 - Container and Serverless deployment
 - Focus on Automation, Tooling & Granularity
 - Layer 7 Access Control
 - Infrastructure as Code
 - Policy as Code
 - Use 5 Step process in Cloud Native Process



Early CSA work intersecting AI & Zero Trust – Data Governance



Components of LLM-backed Systems



Optimize Authorization for

- RAG access using a vector database.....
- RAG access using a relational database.....
- RAG via API calls to external system.....
- LLM systems writing and executing code.....
- LLM-Backed Autonomous Agents.....

Link governance to existing privacy standards and regulations

Controls may be stripped during data transformation

Need access control for multimodal data & vector embeddings

Data classification schema for LLMs

www.cloudsecurityalliance.ai

The letters 'AI' are rendered in a large, glowing, blue, serif font. They are surrounded by a complex network of glowing blue lines and nodes, resembling a neural network or data flow. The background is a futuristic cityscape at night, with lights and a grid overlay.

What's Next?

Major areas we are focused on

System 2 / Reasoning / Chain of Thought Models

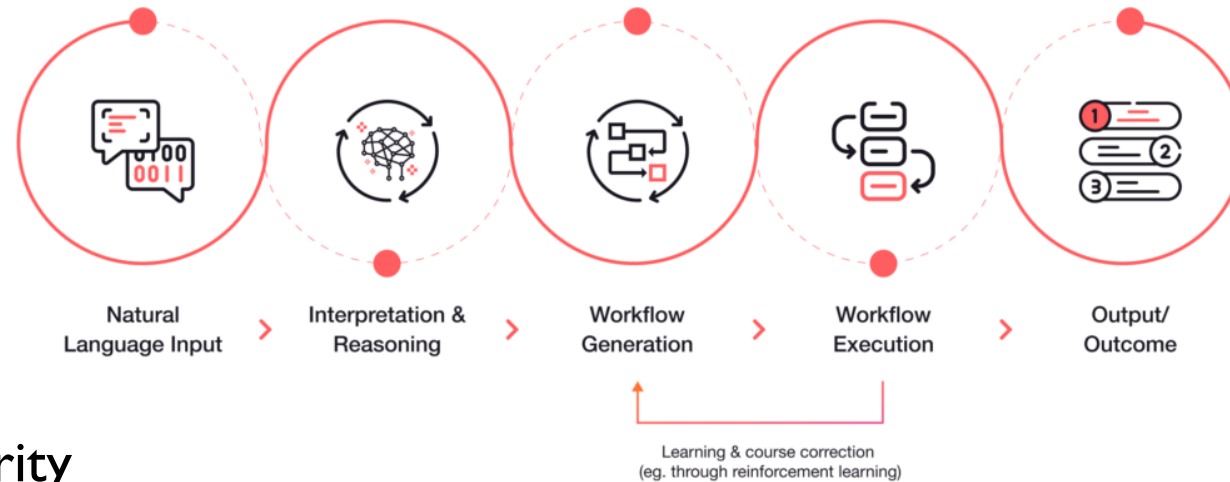
 Llama

Open Weight Models

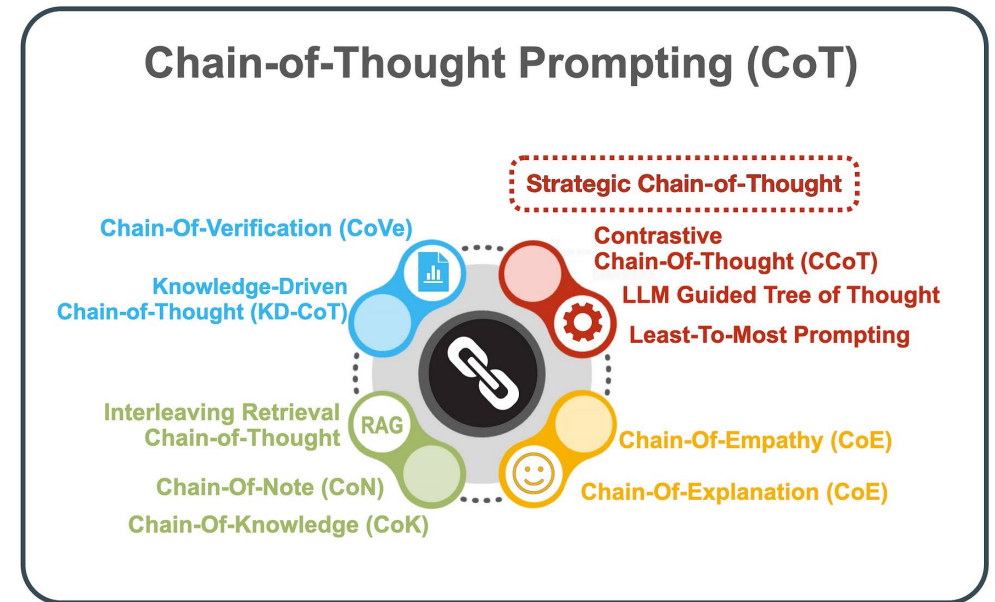
VS

 deepseek

Agentic AI

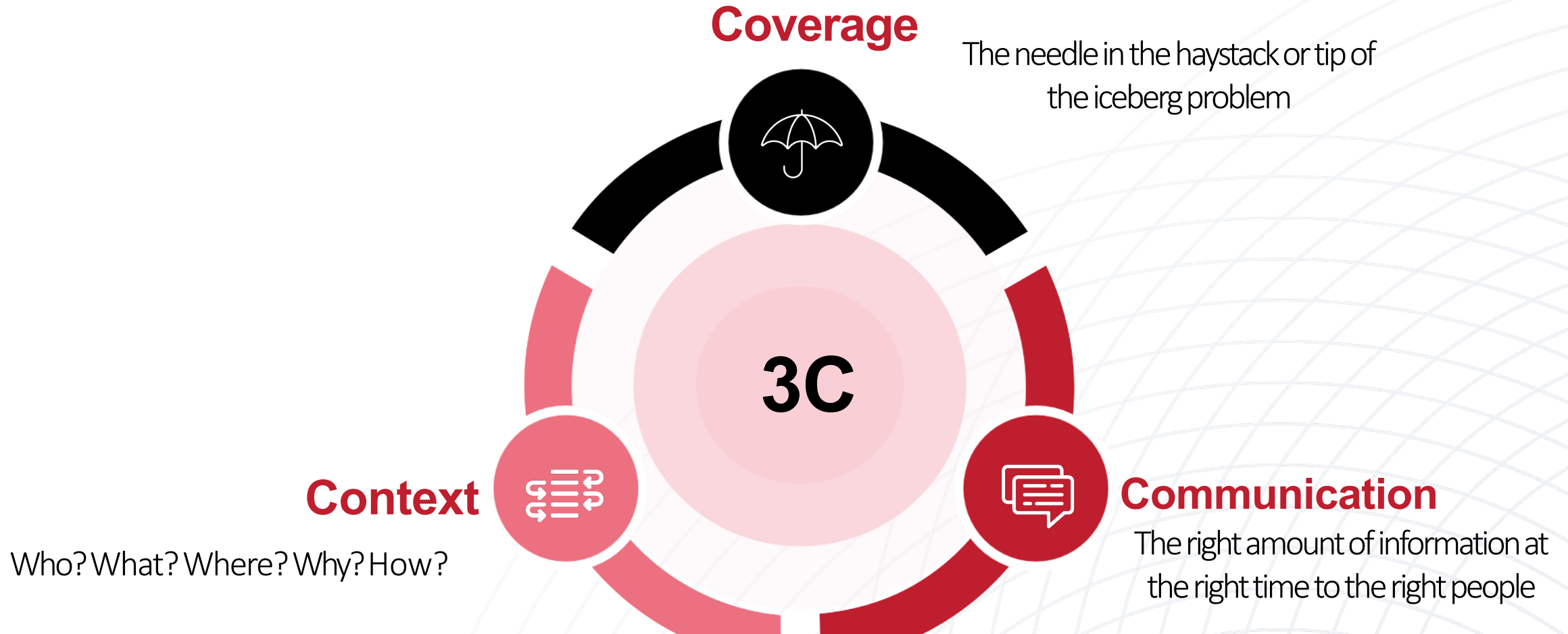


AI-Centric Cybersecurity



www.cobusgreyling.com

AI-Centric Cybersecurity: The three C's



Source: Caleb Sima, CSA AI Summit at RSA Conference 2024

AI excels in the three C's

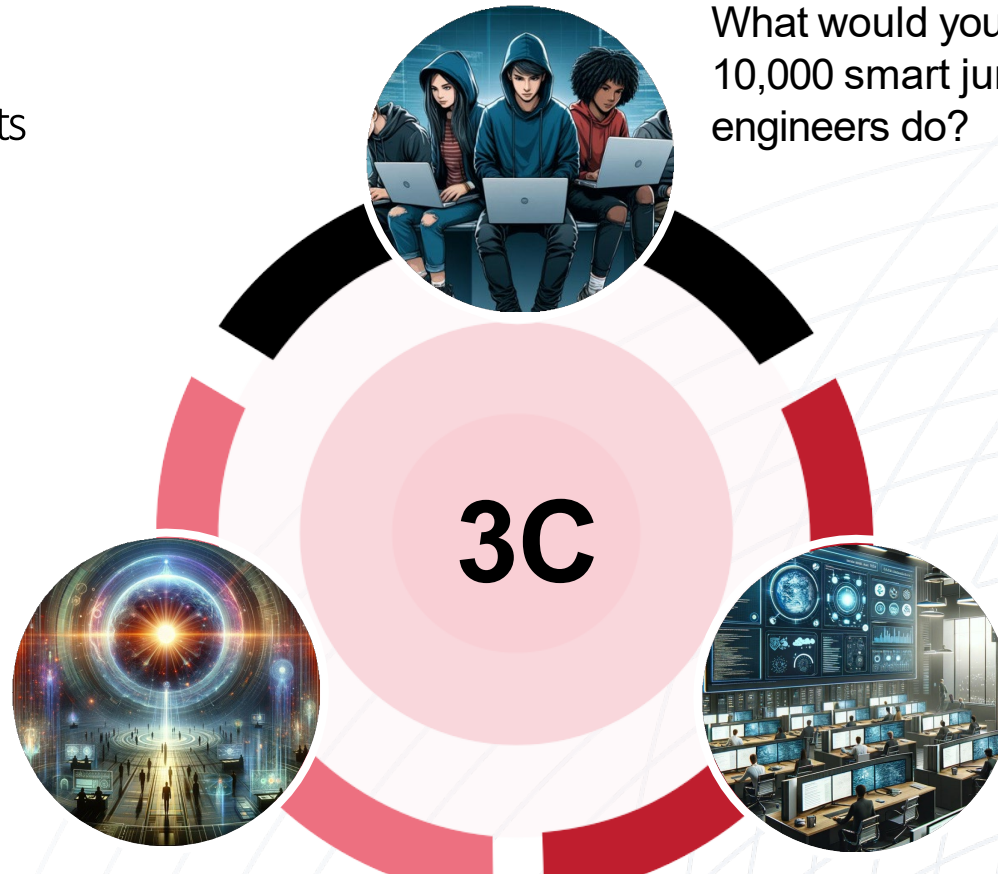
GenAI connects the dots:
Syslog meets Slack channel meets
Zoom meeting summary

Coverage

What would you have
10,000 smart junior security
engineers do?

Context

Oracles &
Synthesization of the
state of the organization



Communication

Communication is a
translation challenge:
ChatOps is back!

Source: Caleb Sima, CSA AI Summit at RSA Conference 2024

A Path Forward

- Cloud is the foundation for IT, AI and Cybersecurity
- Cybersecurity professionals should be the top experts of AI in their organizations
- The high level principles cybersecurity professionals have been taught are relevant
- Understand generative AI, its inner workings and how it is evolving
- Zero Trust is a key philosophy for hardening both cloud and AI
- Good AI is necessary to defeat malicious AI



Thank You



Jim Reavis, CEO: jreavis@cloudsecurityalliance.org

