# CSO Conference *& Awards*


Produced by CSO | IDC

# Camelot Secure CMMC Module

Introducing Myrddin
a Generative AI Solution
for CMMC Compliance Support

## Sherri Thomas, Chief Revenue Officer, Camelot Secure

- Leading all revenue-generating initiatives at Camelot Secure.
- Extensive leadership experience with IBM in both regional and global roles.
- Former Vice President of IBM Federal Ecosystems and Global VP for Strategy & Transformation.
- Led IBM's Innovation Studio in Munich, focusing on customer-centric innovation.
- Proven track record in driving growth across multiple industries and regions, with a strong focus on customer success and strategic transformation.

## Jacob Birmingham, VP Product Development

- Over 25 years as an Information Systems Expert, Cybersecurity professional and ethical hacker.
- Leads the development of our CMMC Dashboard Tool and GenAI integration
- Certified as a CISM and CISSP.
- BS in Computer Engineering, University of Central Florida.
- Master Degree in Management Information Systems, University of Alabama in Huntsville.

# Who Is Camelot Secure?

**A Company with a Revolutionary and Disruptive Approach to Cyberspace & Cybersecurity Operations**

- People, Processes, Technology, and Innovation
- World-Class Workforce with a Special Operations Cyber Mindset (Seal Team 6/ Delta Force of Cyber)
- Secure360 – A Unified and Integrated Cybersecurity Platform


**Core Operational Missions**

- Adaptive Threat Intelligence (Intelligence360)
- Advanced Persistent Threat Hunt
- Security Compliance (PCI-DSS, HIPAA, NIST, CMMC)
- Training & Testing as a Service (T2aaS)

**Additional Services**

- Security Operations Center as a Service
- Cybersecurity Advisory Services

# Rise of Generative AI

**What is Generative AI & Why is it so important today?**

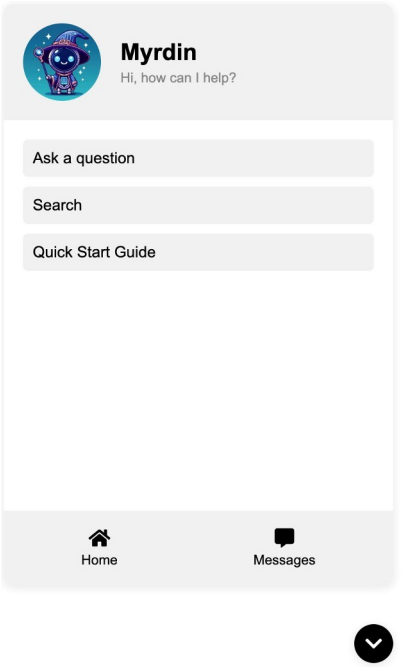
Generative artificial intelligence (generative AI) is a type of AI that can create new content, ideas and analyze lots of text data, including conversations, guidelines, instructions, processes and yes, CMMC practices.

**Generative AI is the next step in artificial intelligence.** You can train it to learn human language, programming languages, art, chemistry, and all 110 CMMC control practices, given us humans an instant CMMC subject matter expert to help answer questions about CMMC.

**Transformers**, in the context of generative AI, are a type of deep learning architecture that has revolutionized natural language processing (NLP) and other AI tasks. Introduced in the paper "Attention is All You Need" by Vaswani et al. in 2017, transformers are the backbone of many modern AI models, including GPT (Generative Pre-trained Transformer).

# Why Generative AI for CMMC?

- **Instant, Expert-Level Guidance:** Provides real-time, accurate answers to complex CMMC guidelines, processes, and rules, reducing the need for extensive manual research.
- **Context-Aware Assistance:** Offers intelligent tooltips and guidance tailored to the user's specific interactions within the dashboard, enhancing the user experience and understanding.
- **Automated Compliance Evaluation:** Assists in analyzing and evaluating user-provided implementation statements and artifacts against CMMC controls, streamlining the gap assessment process.
- **Continuous Learning & Adaptation:** Leverages AI's ability to learn from user inputs and updates, ensuring that guidance and analysis remain aligned with the latest CMMC requirements.



# Limitations of Generative AI

**Security**

- Data privacy and security concerns arise if proprietary data is used to customize generative AI models.

**Creativity**

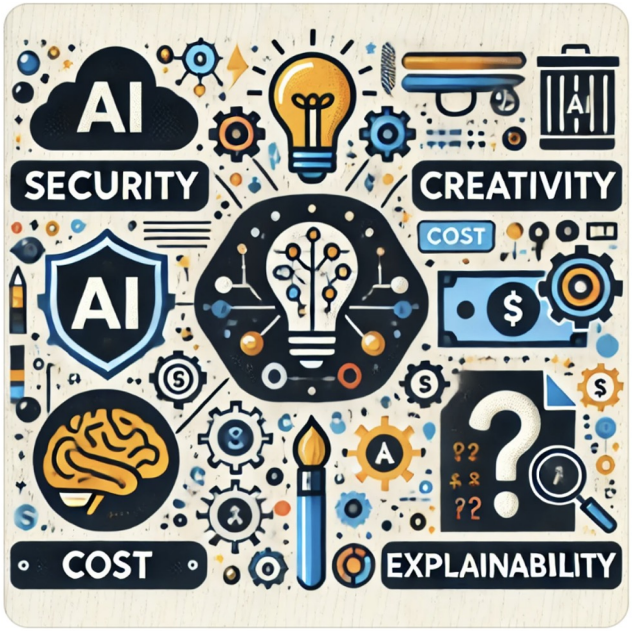
- The creativity of AI is bounded by the data it has been trained on, leading to outputs that may feel repetitive or derivative.

**Cost**

- Training and running generative AI models require substantial computational resources.

**Explainability**

- Due to their complex and opaque nature, generative AI models are often considered black boxes. Understanding how these models arrive at specific outputs is challenging.



# What about Data Security?

## Storing Data for Generative AI.
## What to know & how to do it right.

CSO Conference & Awards | Camelot Secure

Produced by CSO | IDC

# Data Security Considerations

- Store data using multiple layers of security and encryption protocols.
- Utilize managed Keys protect your data.
- Always use FIPS 140-2 compliant encryption protocols.
- Use  IEEE 802.1AE MAC Security Standards when moving data.
- Use variable network paths if crossing data over different Geo boundaries.
- Minimize privacy risk by generating pseudonymous identifiers to avoid directly identifying an individual.
- All Generative AI deployments should be in compliance with the GDPR.
- Use a cloud service that will not provide third party:
  - Direct, blanket, or unfettered access to customers' data;
  - Platform encryption keys used to secure data or the ability to break such encryption;
  - Access to data if the data is to be used for purposes other than those stated in the third party's request.

# What about Model Deployments?

## Not all Generative AI Deployments are Equal

# Generative AI Deployment Matters

**Public Deployment –** Uses existing open and available platforms such as openAI.

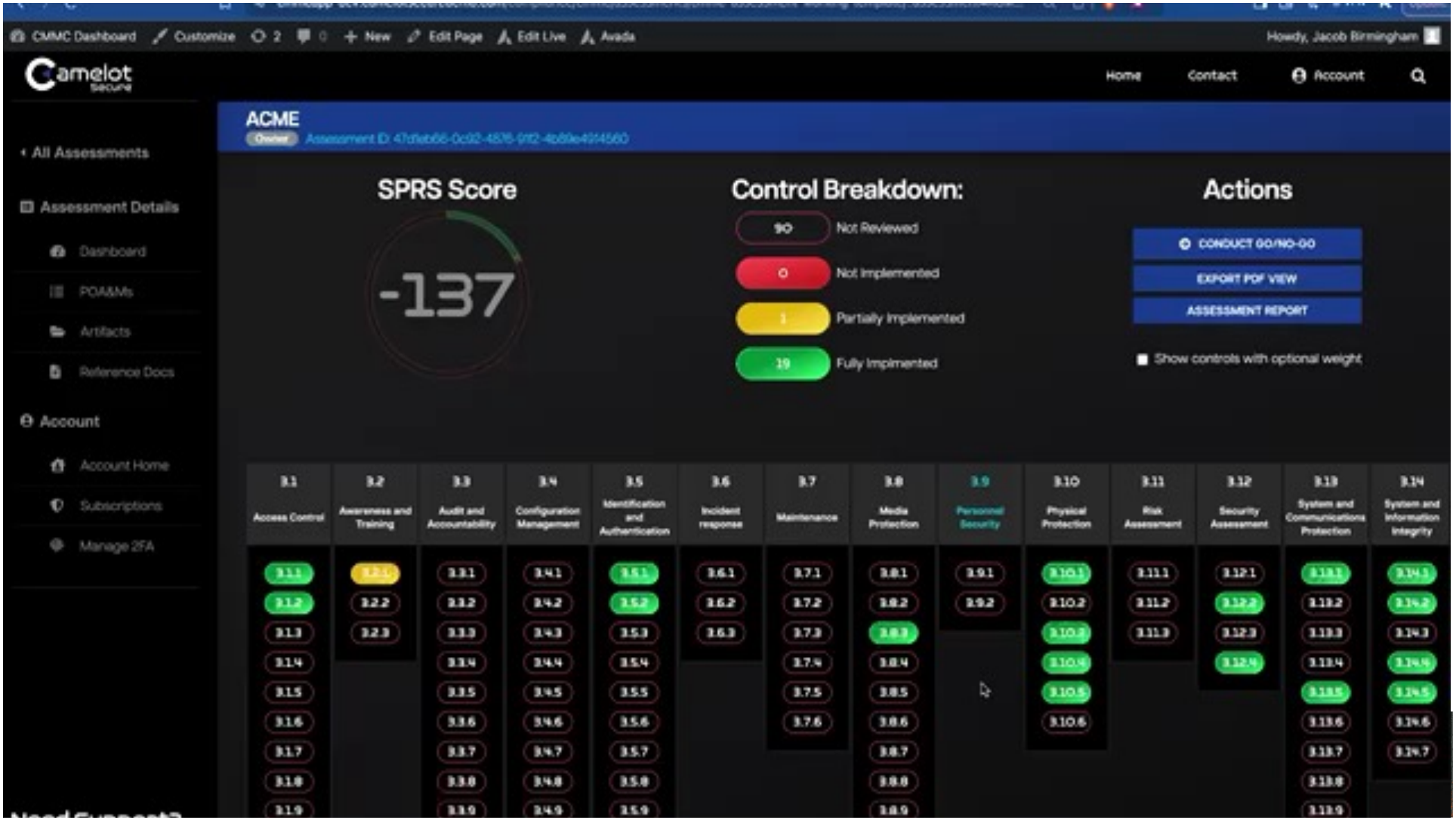
**Global Secure Deployment** - Stores data within selected region (east US), but can process prompts in different regions around the globe.

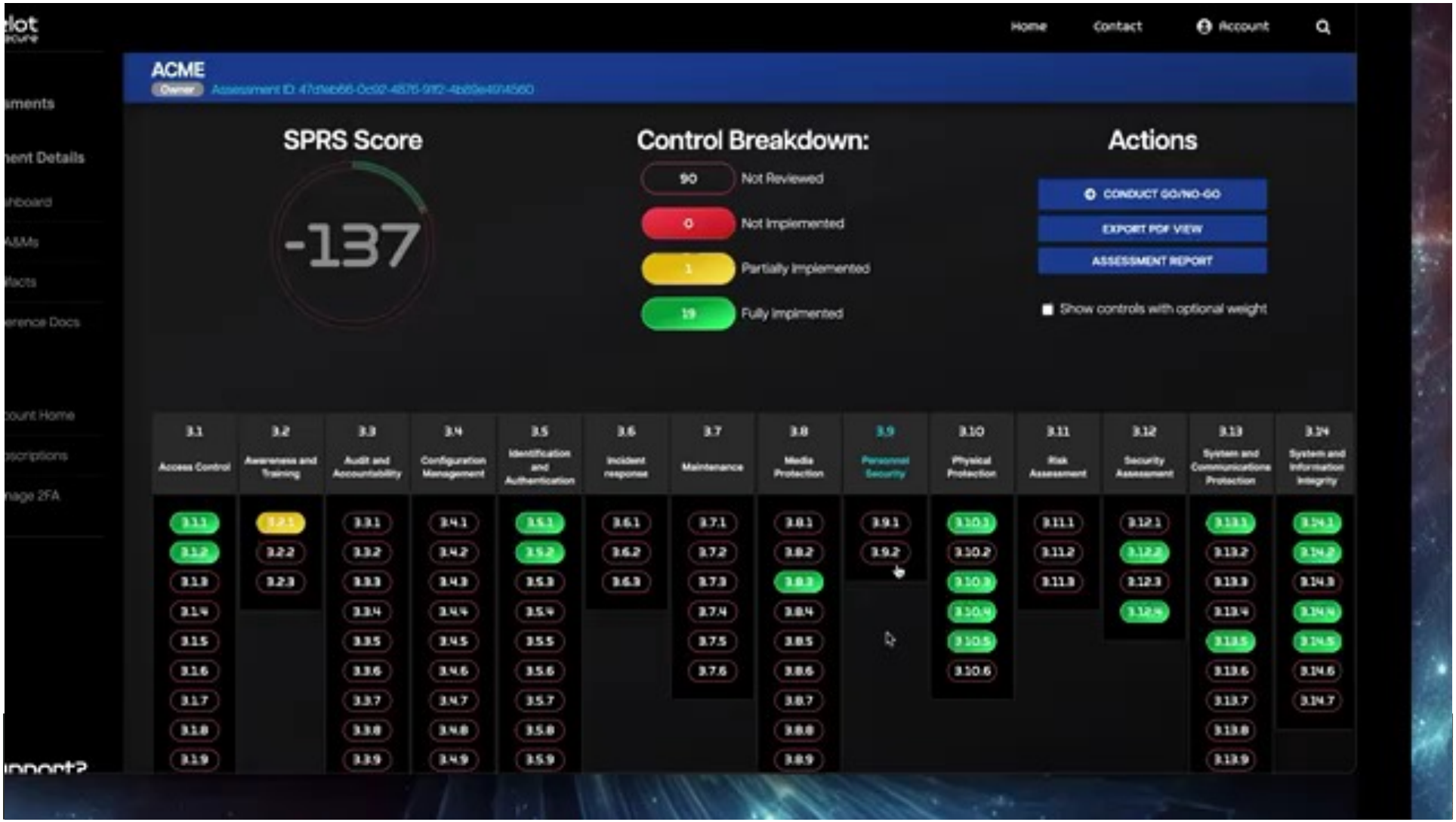
**Standard Secure Deployment** - Stores and runs prompts within selected region.

# Final Thoughts

Beyond CMMC, generative AI will drive Camelot Secure's future products and services, enabling more adaptive threat intelligence, proactive incident response, and continuous learning systems to safeguard critical infrastructures.

Generative AI's flexibility and scalability will allow Camelot Secure to deliver highly tailored cybersecurity solutions, enhancing compliance and security operations and future-proofing clients' defenses against evolving cyber threats.


CMMC Dashboard
Customize
New
Edit Page
Edit Live
Avada
Howdy, Jacob Birmingham
Camelot Secure
Home
Contact
Account
All Assessments
Assessment Details
Dashboard
POA&Ms
Artifacts
Reference Docs
Account
Account Home
Subscriptions
Manage 2FA
ACME
SPRS Score
-137
Control Breakdown:
90
Not Reviewed
0
Not Implemented
1
Partially Implemented
19
Fully Implmented
Actions
CONDUCT GO/NO-GO
EXPORT PDF VIEW
ASSESSMENT REPORT
Show controls with optional weight
3.1 Access Control
3.2 Awareness and Training
3.3 Audit and Accountability
3.4 Configuration Management
3.5 Identification and Authentication
3.6 Incident response
3.7 Maintenance
3.8 Media Protection
3.9 Personnel Security
3.10 Physical Protection
3.11 Risk Assessment
3.12 Security Assessment
3.13 System and Communications Protection
3.14 System and Information Integrity


Home
Contact
Account
ACME
Owner
SPRS Score
-137
Control Breakdown:
90
Not Reviewed
0
Not Implemented
1
Partially Implemented
19
Fully Implemented
Actions
CONDUCT GO/NO-GO
EXPORT PDF VIEW
ASSESSMENT REPORT
Show controls with optional weight
3.1 Access Control
3.2 Awareness and Training
3.3 Audit and Accountability
3.4 Configuration Management
3.5 Identification and Authentication
3.6 Incident response
3.7 Maintenance
3.8 Media Protection
3.9 Personnel Security
3.10 Physical Protection
3.11 Risk Assessment
3.12 Security Assessment
3.13 System and Communications Protection
3.14 System and Information Integrity

# Questions or Feedback?

Emails:

Stan.Oliver@camelotsecure.com

Jacob.Birmingham@camelotsecure.com