Keeping Regulated Data Inbounds: Innovating with AI and Cloud Services

PRESENTED BY

Troy Leach
Chief Strategy Officer

ABOUT THE CLOUD SECURITY ALLIANCE

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

- **BUILDING SECURITY BEST PRACTICES FOR NEXT GENERATION IT**
- **GLOBAL, NOT-FOR-PROFIT ORGANIZATION**
- **RESEARCH AND EDUCATIONAL PROGRAMS**
- **CLOUD PROVIDER CERTIFICATION – CSA STAR**
- **USER CERTIFICATION – CERTIFICATE OF CLOUD SECURITY KNOWLEDGE (CCSK)**
- **THE GLOBALLY AUTHORITATIVE SOURCE FOR TRUST IN THE CLOUD**

OUR COMMUNITY

220,000+
INDIVIDUAL MEMBERS

145+
CHAPTERS

500+
CORPORATE MEMBERS

35+
ACTIVE WORKING GROUPS

60,000+
SUBSCRIBERS TO OUR WEBINAR SERIES

12,000+
RESEARCH VOLUNTEERS CONTRIBUTING

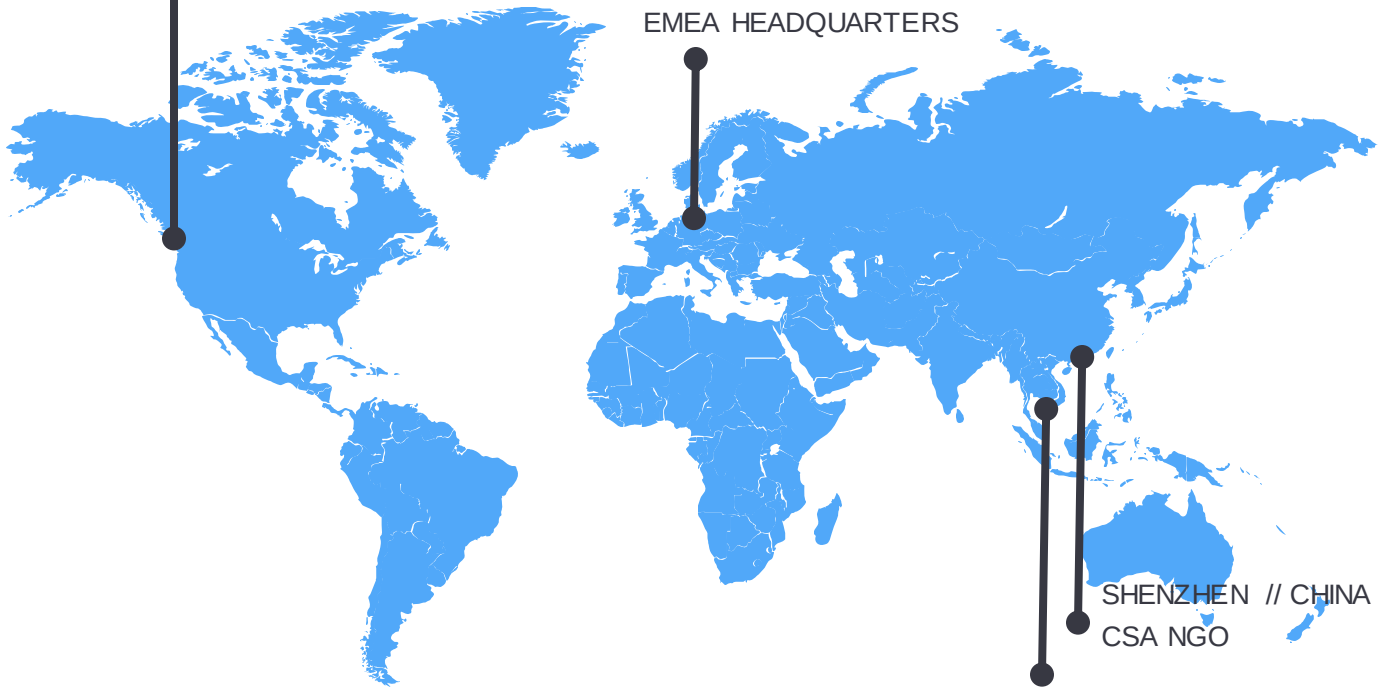
Strategic partnerships with governments, research institutions, professional associations and industry

CSA research is FREE!

2009
CSA FOUNDED

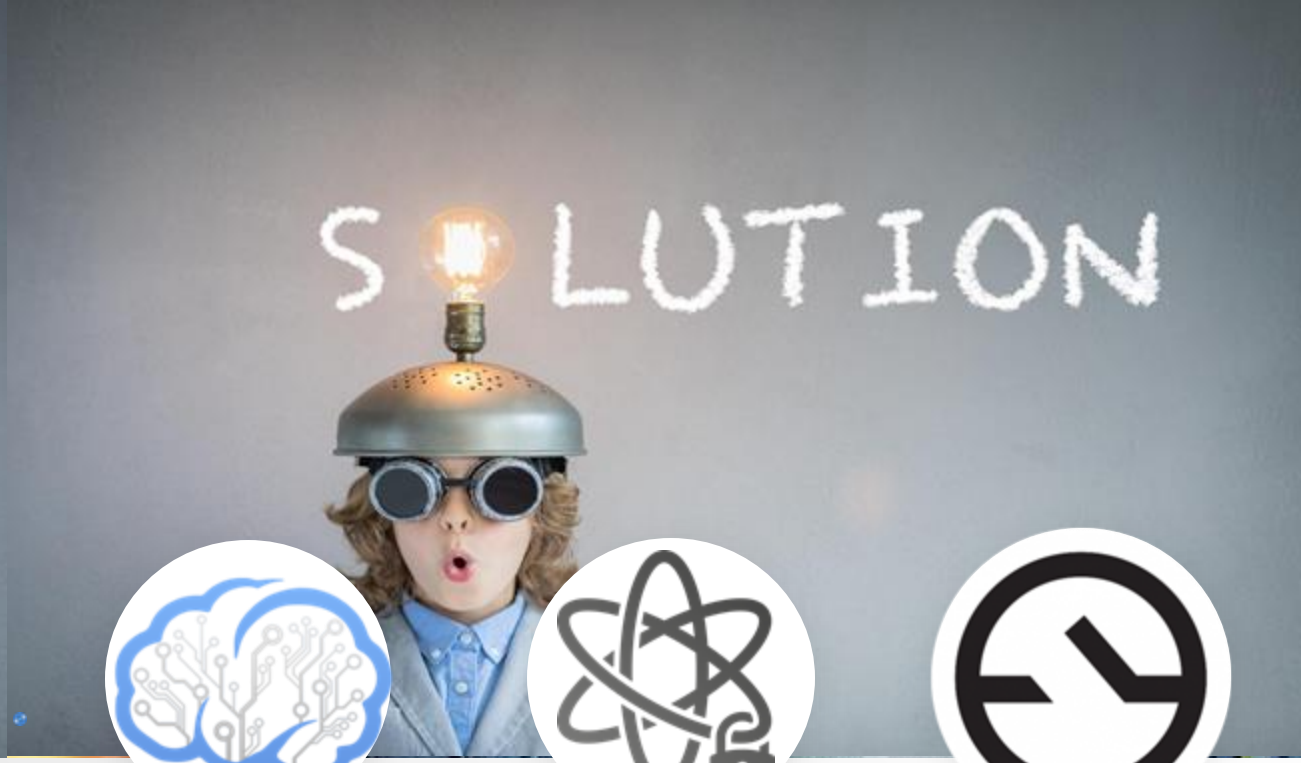
SEATTLE/BELLINGHAM, WA // US HEADQUARTERS

BERLIN // EMEA HEADQUARTERS



SHENZHEN // CHINA CSA NGO

SINGAPORE // ASIA PACIFIC HEADQUARTERS



BLOCKCHAIN

ACTED AS A DIGITAL LEDGER FOR CRYPTOCURRENCY BUT CAN NOW BE APPLIED IN NEW USE CASES.

INTERNET OF THINGS

SECURITY FOR THE MANAGEMENT, ORCHESTRATION, AND ANALYTICS OF NEW TYPES OF DEVICES, SYSTEMS, AND DATA.

DEV(SEC)OPS

STRIVES TO AUTOMATE SECURITY TASKS AND EMBED SECURITY INTO THE DEVOPS WORKFLOW.

ARTIFICIAL INTELLIGENCE

PROMISES TO TRANSFORM SOCIETY ON THE SCALE OF THE INDUSTRIAL REVOLUTION BEFORE IT.

QUANTUM COMPUTING

PREPARING FOR COMPUTE CAPABILITIES BEYOND TRADITIONAL BINARY CODE AND INTO THE QUBIT ERA.

SOFTWARE DEFINED PERIMETER

IDENTITY, ROLE BASED ACCESS CONTROL MODEL FOR A “ZERO TRUST” APPROACH IN THE CLOUD.

The Play-by-Play

1. **Knowing what's coming (Identifying Critical Risk)**
2. **Batter Heat Map (Top Threats)**
3. **Planning the Lineup (Response Planning)**
4. **Adjusting the Gameplan Pinch Hitting (Adapting)**
5. **Sharing Signs (Communicating Third-parties)**
6. **We're Talking Practice (Testing and Learning)**

Knowing what's coming

Regulation, Frameworks

DORA

EU AI ACT

AI Cybersecurity Act

SEC

US Treasury

NIST CSF v2

Also…..

PCI DSS v4, NYDFS, APRA CPS230

Technology Risks Competing for your Attention

Not just the regulatory curve you need to look for

- 40K+ IoT Devices compromised after EOL
- Changes to National Vulnerability Database (NVD)
- AI Malware Generation
- Quantum and AI influence on modern authenticatoin

Things to do today:

- Identify all likely AI use cases and Quantum Crypto Bill of Material (CBoM)
- Monitor and API protection for querying/output of LLM
- Penttestings of AI models
- AI Policy that is communicated throughout organization

State of SaaS Security 2024

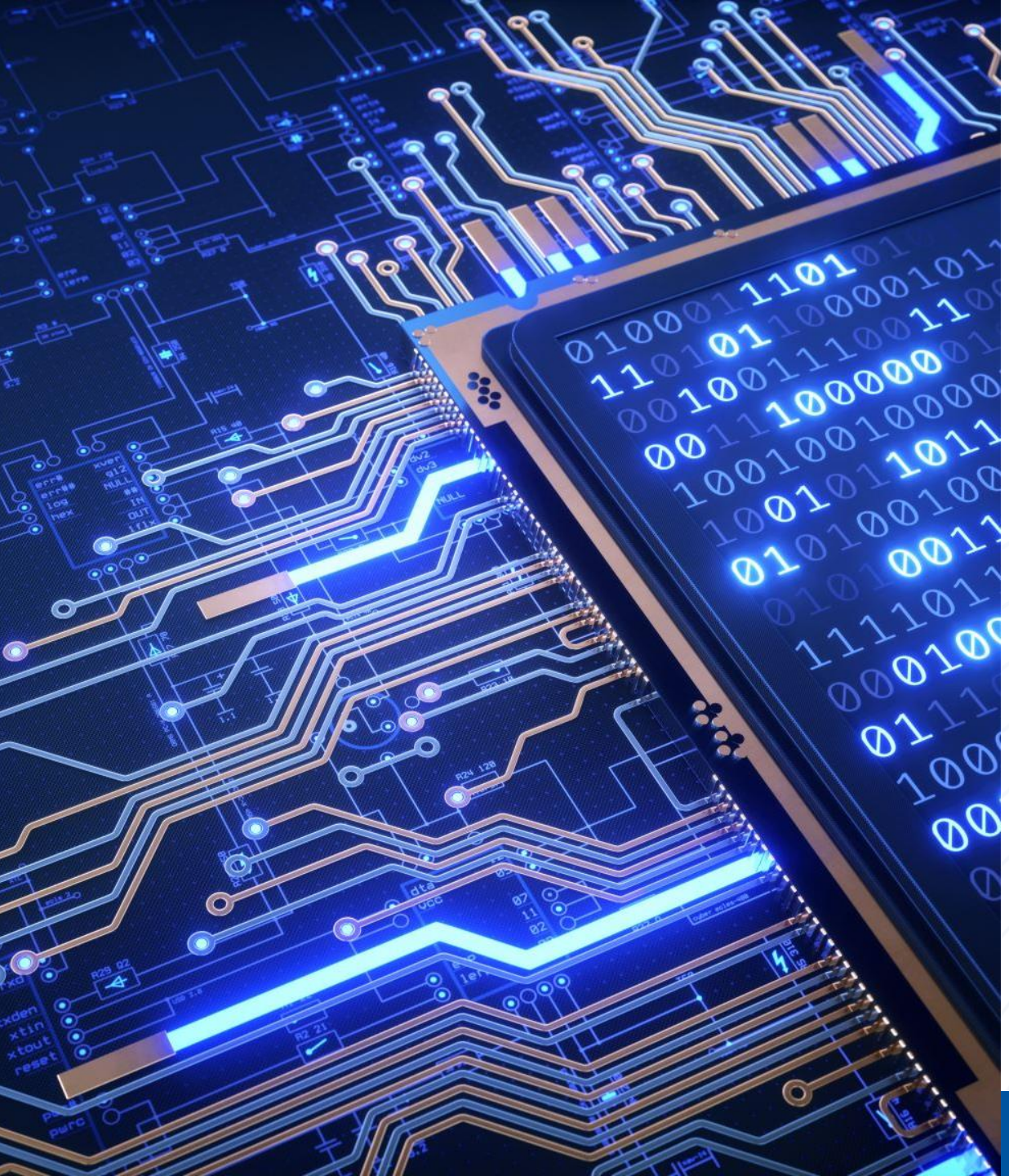
- SaaS Security is moderate to high priority for 80% of organizations
  - Many increase staff (56%) or increasing budget (39%) to support these goals

- Challenges with certain complex apps with a high volume of users (e.g., Google Workspace, Microsoft365)
  - Main challenges are gaining visibility - 73%
  - Tracking and monitoring security risks from 3rd party apps - 65%
  - Locating and fixing SaaS misconfigurations - 63%

- Might be stemming from their SaaS Security strategy

  - Most orgs are using cloud security tools -CASB, manual audits, CSPM, etc. to secure the SaaS stack
  - Variety of departments involved - decentralizing security

- Overall SaaS security improving - incidents over the past two years down from 53% in 2023 to 25% in 2024



Offensive AI

- Malware Creation
- Spear phishing
- Classify victims
- Conditional attacks
- Smart botnets

Adversarial AI

- Data poisoning
- Model Stealing
- Adversarial inputs
- Feedback weaponisation

- Deepfake

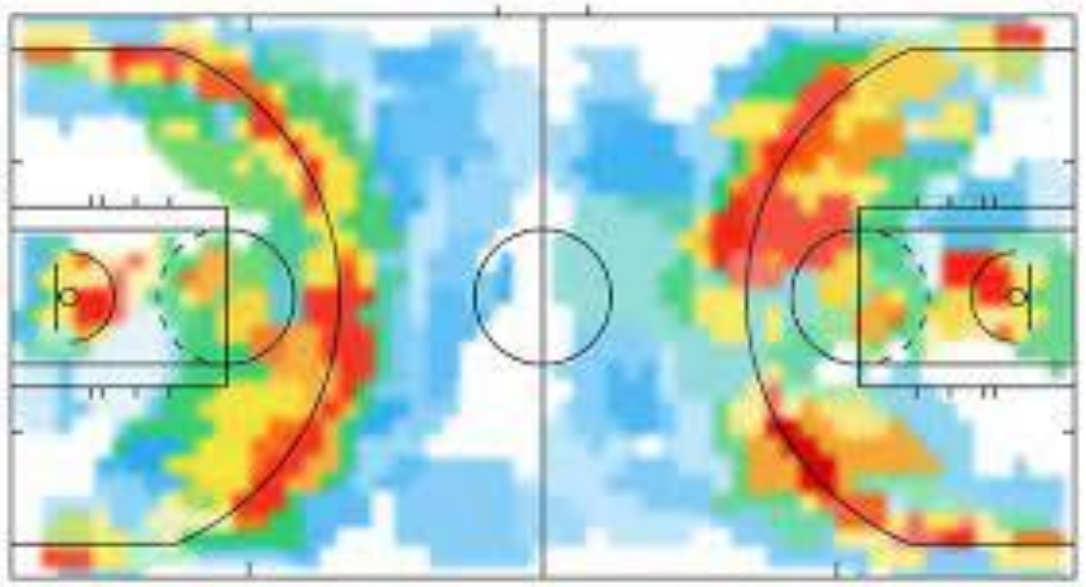
The Cyber Heat Map

Top Threats

- Identity and Access Management
- Misconfiguration and inadequate change control
- Insecure Interfaces and APIs
- Lack of Cloud Strategy

New Risks Introduced by AI

- Extraction
- Poisoning
- Inference
- Inference
- Transparency
- Degradation of Information



Setting Your Dream Team Lineup

Resource Planning and areas of growing interest

Risk Management Strategy

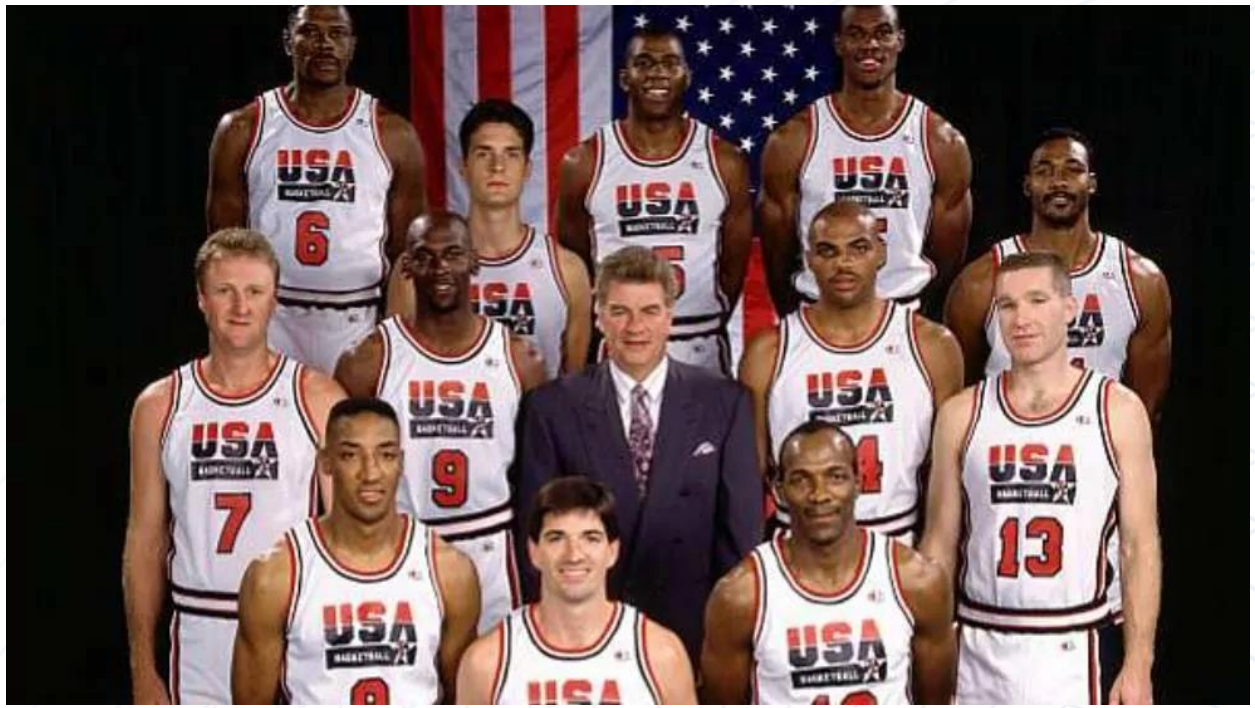
Automation for Patch Management

Tested IRP of Third Parties

Confidential Computing

Quantum Computing

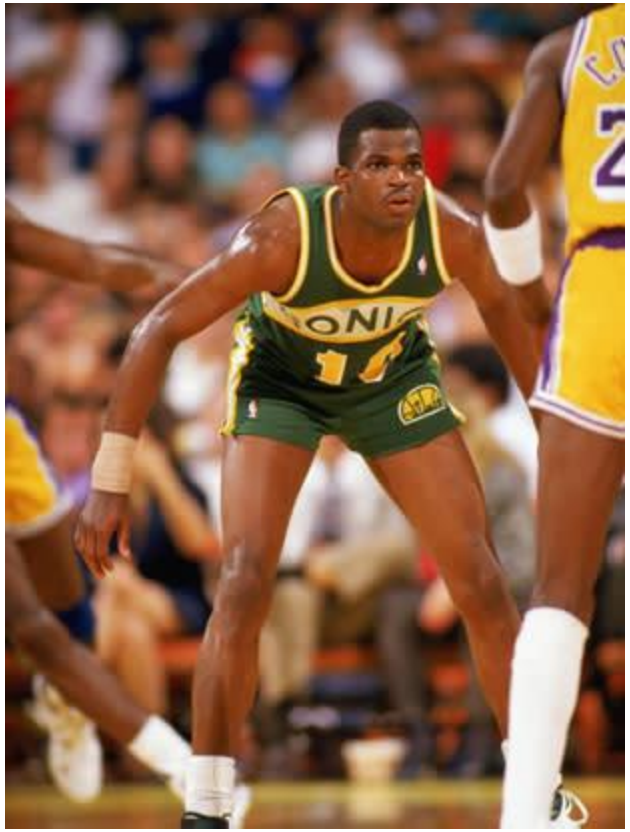
MFA



Adjusting the Defensive Lineup

Leveraging AI to enhance your security

- Malware Detection
- Vulnerability Management
- Data Classification
- Anti-spam
- SOC, IDS/IPS and Honey pots
- Threat Intelligence



Clarifying the rules

Communicating with Regulators and Service Providers

Right sport, wrong equipment

3rd-party vendors vs 3rd-party partners

Operational ~~Resiliency~~ Efficiency

We're Talking Practice

Testing and Learning Opportunities

Industry expectations for independent testing and verification is evolving quickly.

SLAs will need to accommodate expectation

AI must be verified for accuracy

CSA AI Safety Initiative

AI Research Working Groups

AI Technology and Risk

https://cloudsecurityalliance.org/research/working-groups/ai-technology-and-risk/

Mission Objective

The AI Technology and Risk Committee is focused on staying abreast of the latest technological advancements in AI while simultaneously identifying, understanding, and forecasting associated risks, threats, and vulnerabilities. This technical committee aims to act as both a knowledge hub and a proactive risk management entity, bridging the gap between innovation and security in the realm of AI.

Key Projects

- Methodology for Risk Assessment
- Educational Materials on Latest Threats
- Referenced Architecture Repository
- AI-driven Cybersecurity Solutions
- Security of AI Systems

AI Governance and Compliance

https://cloudsecurityalliance.org/research/working-groups/ai-governance-compliance/

Mission Objective

The AI Governance & Compliance Committee aspires to be the industry's cornerstone for establishing, advocating, and disseminating governance and compliance standards for artificial intelligence. The committee aims to shape policy, influence legislation, and create benchmarks that set the gold standard.

Key Projects

- Benchmark Creation
- Ethical and Responsible Use of AI
- AI Accountability and Transparency
- Public and Private Partnerships
- Periodic Industry Reviews
- Investigating methods for enhancing AI transparency and explainability.
- Analyzing the impact of transparent and explainable AI on governance.

AI Controls

https://cloudsecurityalliance.org/research/working-groups/ai-controls/

Mission Objective

The definition of a framework of controls for the governing of AI technologies from the safety, cybersecurity, privacy, accountability, and transparency perspectives.

Key Projects

- Identify an initial list of risks/threats/vulnerabilities (based on existing literature: OWASP LLM 10 ten, MITRE ATLAS Project, ENISA, research papers (e.g. https://arxiv.org/pdf/2305.15324.pdf, etc.)
- Identify possible controls to mitigate those AI-specific risks
- Identify within our existing Cloud Control Matrix (CCM) which controls are relevant (which ones are relevant as is, which ones would need to be extended/amended).
- Merge the 2 and 3

AI Organizational Responsibilities

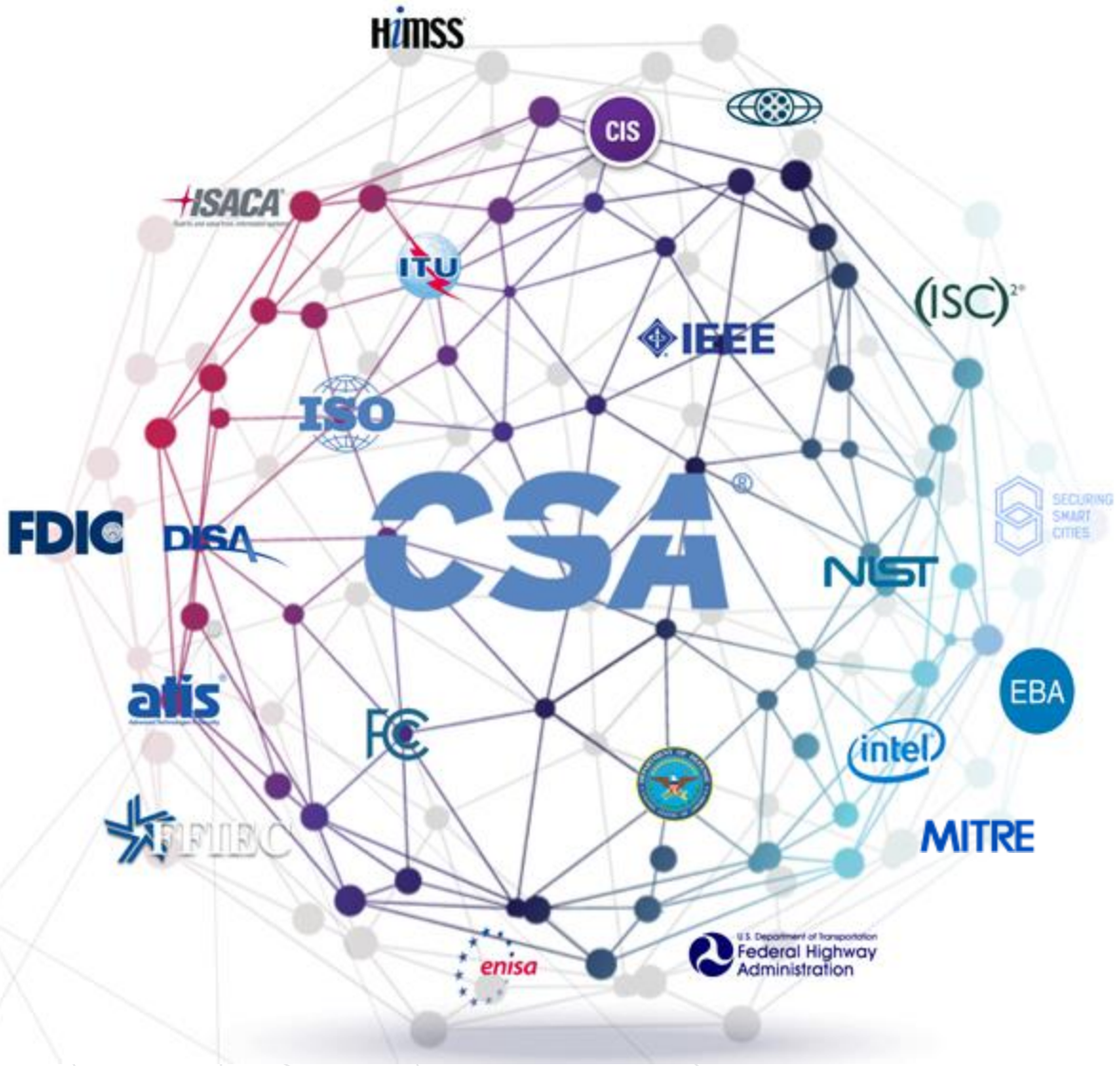
https://cloudsecurityalliance.org/research/working-groups/ai-organizational-responsibilities/

Mission Objective

The AI Organizational Responsibilities is committed to pioneering and setting industry standards for the definition of roles and responsibilities within security teams, specifically adapted to the emerging challenges and opportunities presented by AI technologies. The committee aims to identify the shifts in tasks and knowledge bases that are imperative for various security sub-teams, such as product security and detection & response teams, in the age of AI.

Key Projects

- Creating a Standardized Framework for AI Security Roles
- AI and Continuous Professional Development in Cybersecurity
- Adapting Traditional Security Roles to AI Integration
- Cross-training Needs in AI-Augmented Security Teams:
- The Evolution of Security Expertise in the Era of AI:



INDUSTRY COLLABORATION

FORMAL:

- ISO/IEC JTC 1 – IT AND CLOUD SECURITY TECHNIQUES
- ITU-T – PROCEDURES AND STANDARDS IN TELECOM
- IEEE – CYBERSECURITY AND PRIVACY STANDARDS COMMITTEE
- NIST – CLOUD SECURITY WORKING GROUP
- FCC - TECHNOLOGICAL ADVISORY COMMITTEE ON IOT
- DISA DODIN (GIG) – CLOUD COMPUTING SERVICES GUIDANCE
- DOD IC - CLOUD COMPUTING STANDARDS FOCUS GROUP
- ATIS - PACKET TECHNOLOGY AND SYSTEMS COMMITTEE ON 5G
- CIS – CLOUD SECURITY BENCHMARKS
- CLOUD SECURITY INDUSTRY SUMMIT – EXECUTIVE COUNCIL OF CLOUD
- ENISA – EU FUNDED RESEARCH ON RISK, INTEROPERABILITY, SLAS, AND MORE
- ISC2 – TRAINING AND EDUCATION PARTNER FOR CLOUD SECURITY CERTIFICATION
- ISACA – CONTINUING EDUCATION PARTNER FOR IT CERTIFICATION
- CSA CORPORATE MEMBERS – COMMISSIONED WORK TO EXPLORE TRENDING TOPICS
- AND MANY OTHERS

INFORMAL:
MPAA, SECURITY SMART CITIES, US FEDERAL HIGHWAY ADMINISTRATION,
HIMSS, HC3, FFIEC, FDIC, OCC, EBA, MITRE AND MORE

Takeaways

New regulatory requirements coming soon

Top threats continue to be misconfiguration and lack of awareness of responsibility

AI is adding daily offensive threats and defensive opportunities

Education by all stakeholders critical

cloud security alliance®

Troy Leach

Troy Leach

Cloud Security Alliance

tleach@cloudsecurityalliance.org

https://www.linkedin.com/in/troyleach/