2025 CAE Community Symposium

Navigating Cloud Security and Forensics: Addressing Emerging Threats and Challenges

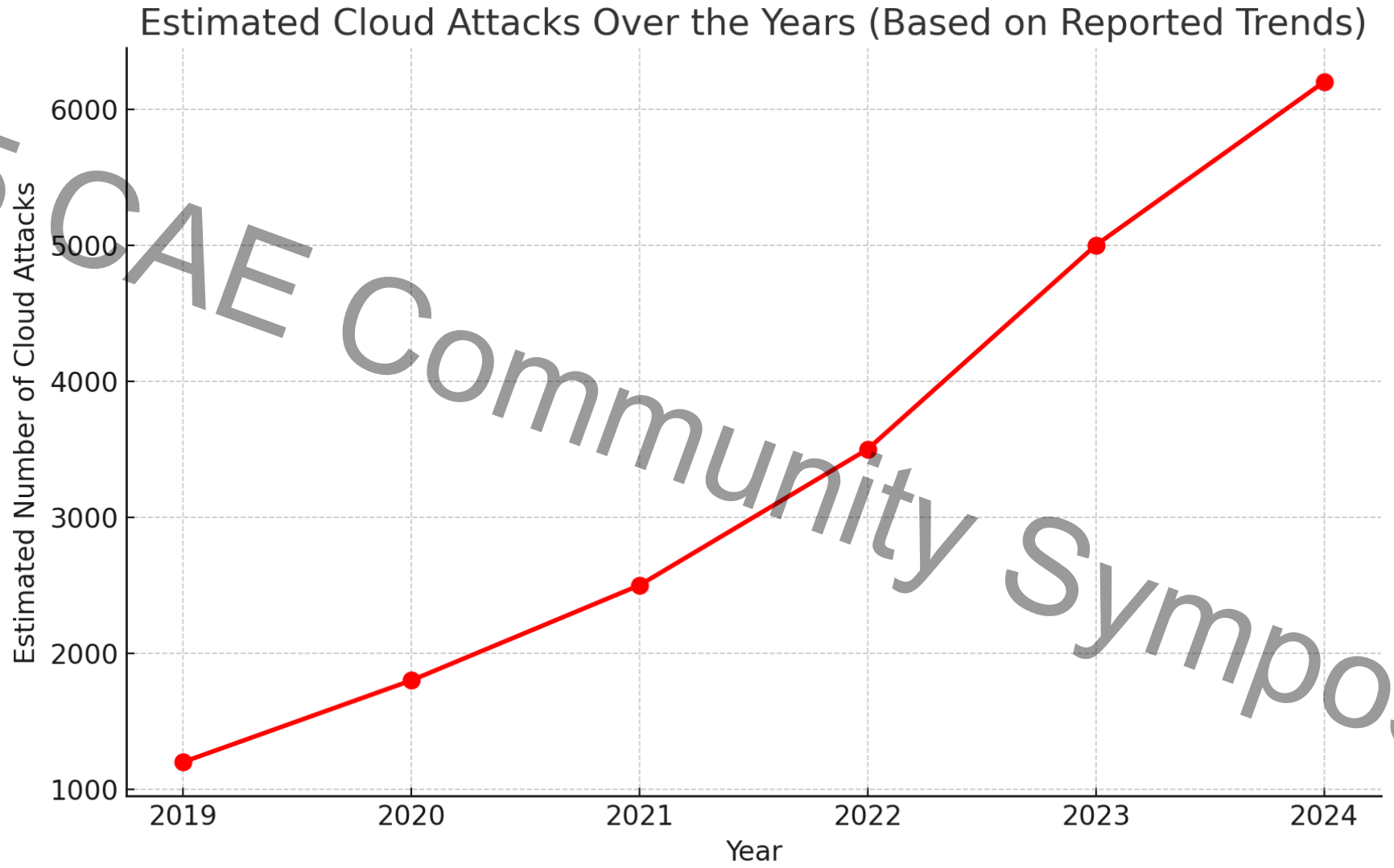
Becky Passmore, Assistant Professor Cybersecurity

Dr. Sandra Leiterman, Director of Cybersecurity Education & Outreach

University of Arkansas at Little Rock

Introduction

- Rapid Expansion of Cloud Application
- Rise of Multi-Cloud and Hybrid Environments
- Growing Attack Surface and Cybersecurity Risks



Source: StationX (2025), Statista (2024), StrongDM (2025)

The Cloud Security Landscape

Shared Responsibility Model

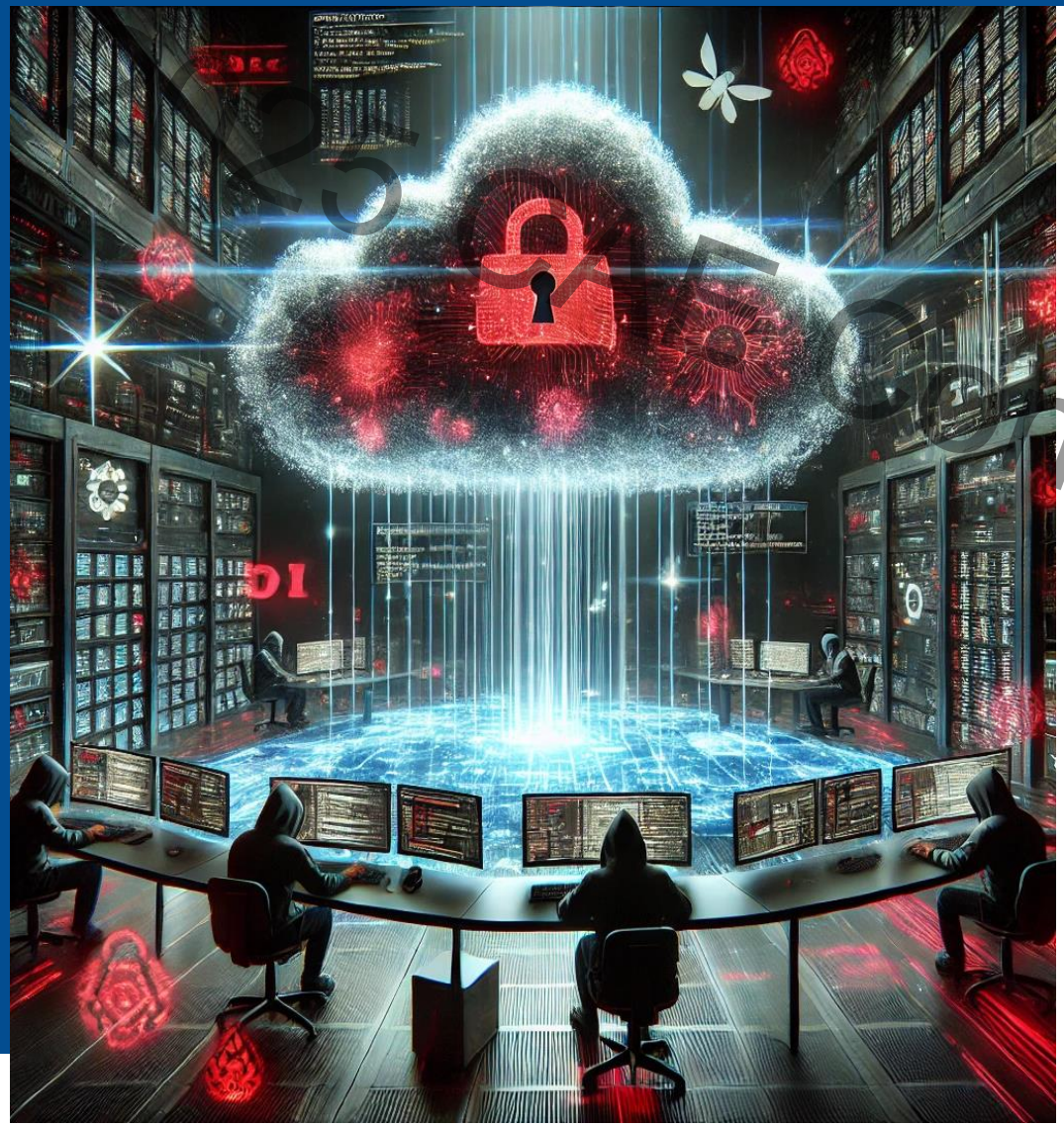
- Defining the Shared Responsibility Model
- Who is Responsible for What?
- Common Security Gaps in the Shared Responsibility Model

The Cloud Security Landscape

Key Security Challenges in the Cloud

- Visibility and Control Over Cloud Assets
- Data Security and Compliance Risks
- API Security and Supply Chain Risks
- Insider Threats and Unauthorized Access
- Evolving Threat Landscape – AI-Powered Cyber Attacks

Emerging Cloud Security Threats

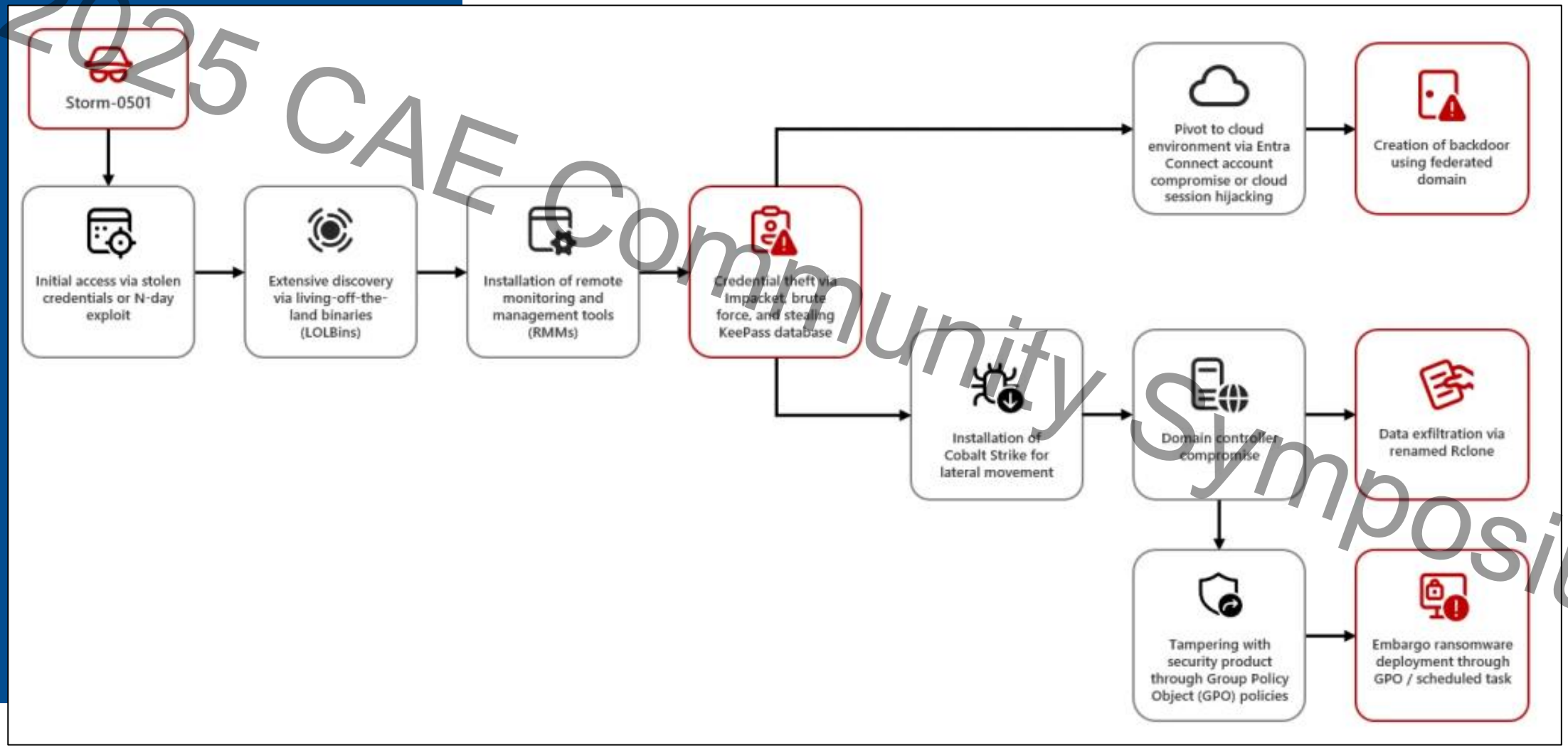


Cloud Threats

- Ransomware
- Misconfigurations
- Account Hijacking
- Data Leaks

Emerging Cloud Security Threats

Case Study – Cloud Ransomware Attack



Credit: Microsoft

Emerging Cloud Security Threats

Types of Insiders

- Malicious Insiders
- Negligent Insiders
- Compromised Insiders

Emerging Cloud Security Threats

APIs and Supply Chain Vulnerabilities

- Exploiting APIs for unauthorized access
- Third-party risks and software supply chain attacks

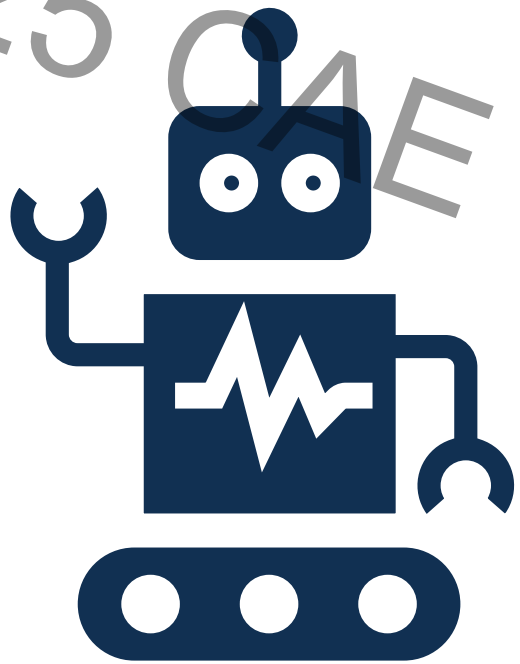
Cloud Forensics Challenges

Challenges

- Differs from traditional Digital Forensics
- Lack of direct access to data
- Legal and Compliance barriers
- Multi-Tenancy and Data Privacy concerns

Why AI is Essential for Cloud Security & Forensics

- AI for Threat Detection & Anomaly Detection
- AI for Automated Incident Response
- AI for Assisted Log Analysis & Evidence Collection
- AI Cloud Forensic Integrity

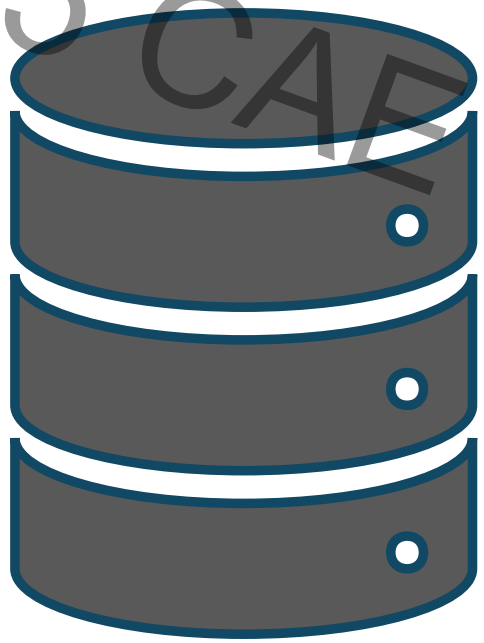


Threat and Anomaly Detection

- Machine Learning for Anomaly Detection
  - AI powered anomaly detection systems analyze large datasets in real-time to identify deviations from normal behavior.
    - Detecting insider threats
    - Detecting data exfiltration
    - Detecting unusual access patterns
- User and Entity Behavior Analytics (UEBA)
  - AI monitors user activities, flagging suspicious behavior.
    - Unauthorized access attempts
    - Abnormal data transfers

Automated Incident Response

- AI- Driven SOAR (Security Orchestration, Automation, and Response)
  - Automates threat investigation and response workflows, reducing the time required to contain cyber incidents
- Chatbots and AI Assistants
  - AI powered forensic assistants help investigators query logs and identify critical data quickly



Cloud Log Analysis for Forensic Investigations

Log Parsing and Correlation

AI automates the analysis of cloud logs from platforms.

- AWS CloudTrail Logs
- Microsoft Azure Logs
- Google Cloud Logs
  - Identify and correlate between anomalies and suspicious activity

Natural Language Processing (NLP) for Log Analysis

AI interprets vast amounts of security logs, enabling forensic analysts to quickly identify attack patterns

Ransomware Detection and Mitigation

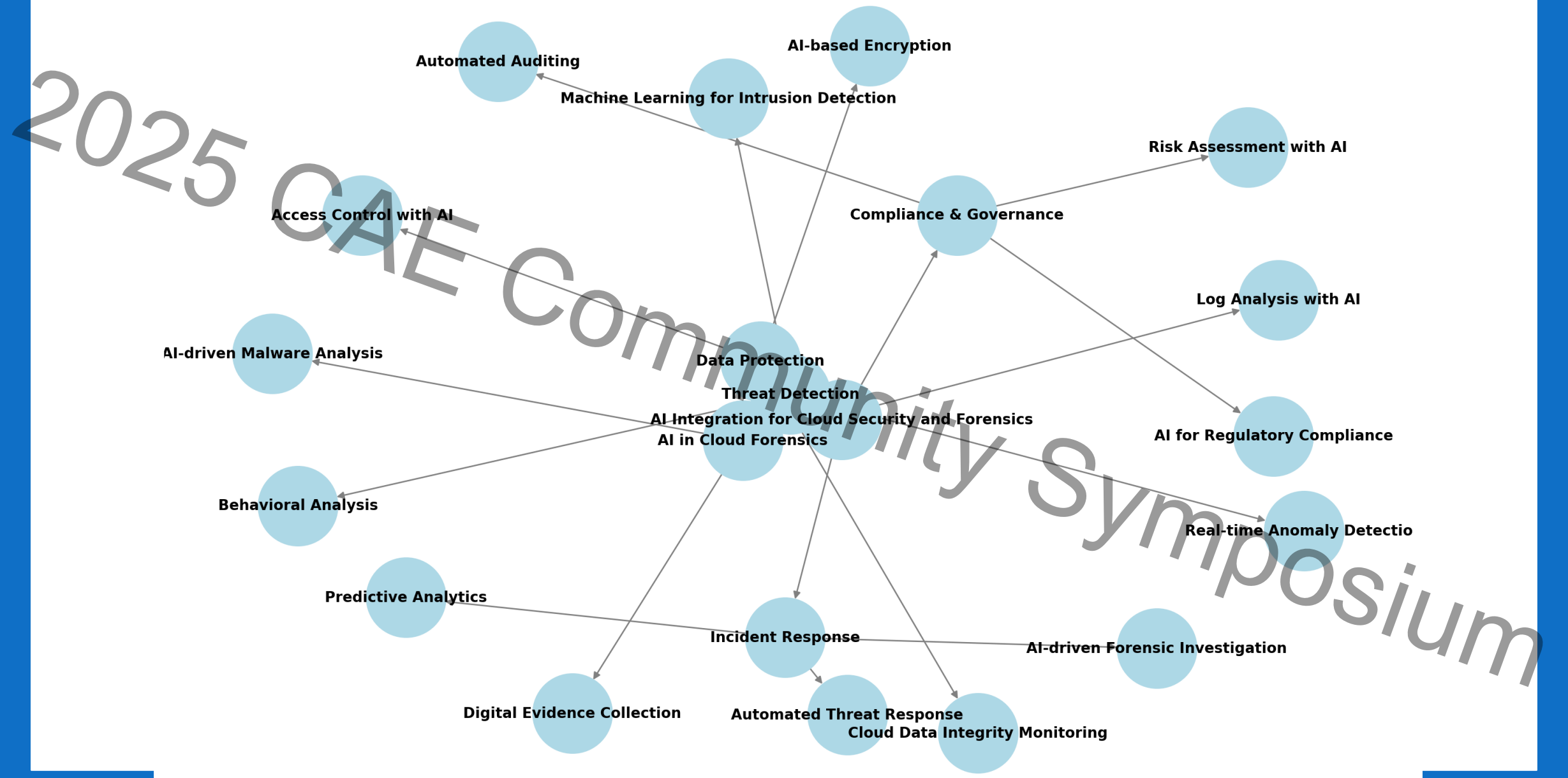
AI Based File Integrity Monitoring

AI detects abnormal file changes that indicate encryption attempts by ransomware

Automated Ransomware Response

AI driven response mechanisms isolate infected workloads and initiate recovery processes

AI Integration for Cloud Security and Forensics



Key Benefits of AI in Cloud Security and Forensics

- Faster threat detection and response
- Automated compliance and auditing
- Improved accuracy in forensic investigations
- Stronger data protection and encryption
- Reduced manual effort and operational costs

2025 CAE Community Symposium

Questions