Data Centricity for Cloud and Application Security

OWASP FFM, 24
Where are we today?

Pressure of Digitization vs. Data Hygiene: parallel data pools & usage of external services

Application centric (redundancy of data) vs. Data centric (data != lifecycle of data)

Transition to a data centric architecture is significantly more complex for brown fields than for green fields (e.g. processes, inventory data, design, development, test, deployment, ...).
Where are we today?

- Data centricity is not a technological challenge!
- Data centricity is the necessary prerequisite for becoming technologically agnostic (IT, OT, ...)
- Data centricity is the necessary prerequisite for AA, ML, AI, ...
- Data centricity is an enabler for precise and granular risk based decision making
Where are we today?

- Legacy Systems and existing interfaces
- Identity & Access Management in hybrid environments
- Awareness and knowledge of risk foundations
- Visibility and Management of Risks
Demystifying Data Centricity

- **Gain Granular Control**: Understand the sensitivity of data and apply appropriate security measures based on its classification.
- **Enhance Visibility**: Track data movement across the entire IT landscape, including cloud environments and on-premises infrastructure.
- **Empower Real-Time Threat Detection**: Identify suspicious data activity and potential breaches with greater speed and accuracy.
Sound Risk Decisions with Data at the Core

- **Risk Prioritization:** Analyze threat intelligence, historical incidents, and potential impact to prioritize risks effectively.
- **Data-Driven Threat Analysis:** Correlate events across platforms to identify subtle attack patterns and suspicious activity.
- **Quantifying Risk:** Analyze the potential financial and reputational damage of a security breach to make informed decisions about resource allocation for mitigation strategies.
Reshaping Security and Resilience in the Digital Age

- **Move from Reactive to Proactive:** Identify and address threats before they materialize, creating a more resilient IT infrastructure.
- **Security for the Evolving Landscape:** Adapt to the dynamic nature of applications and cloud environments where traditional perimeter-based security falls short.
- **Continuous Improvement:** Analyze past security incidents and near misses to identify trends and improve security posture over time.
Conclusion:

- Data-centric security is not just a buzzword; it's a paradigm shift.
- By placing data at the core of our security strategy, we unlock a future of robust application and cloud security, informed risk decisions, and a more resilient digital foundation for our ever-evolving world.
- Let's embrace data-centricity and embark on a secure journey through the exciting landscapes of cloud, AI, and digital transformation.