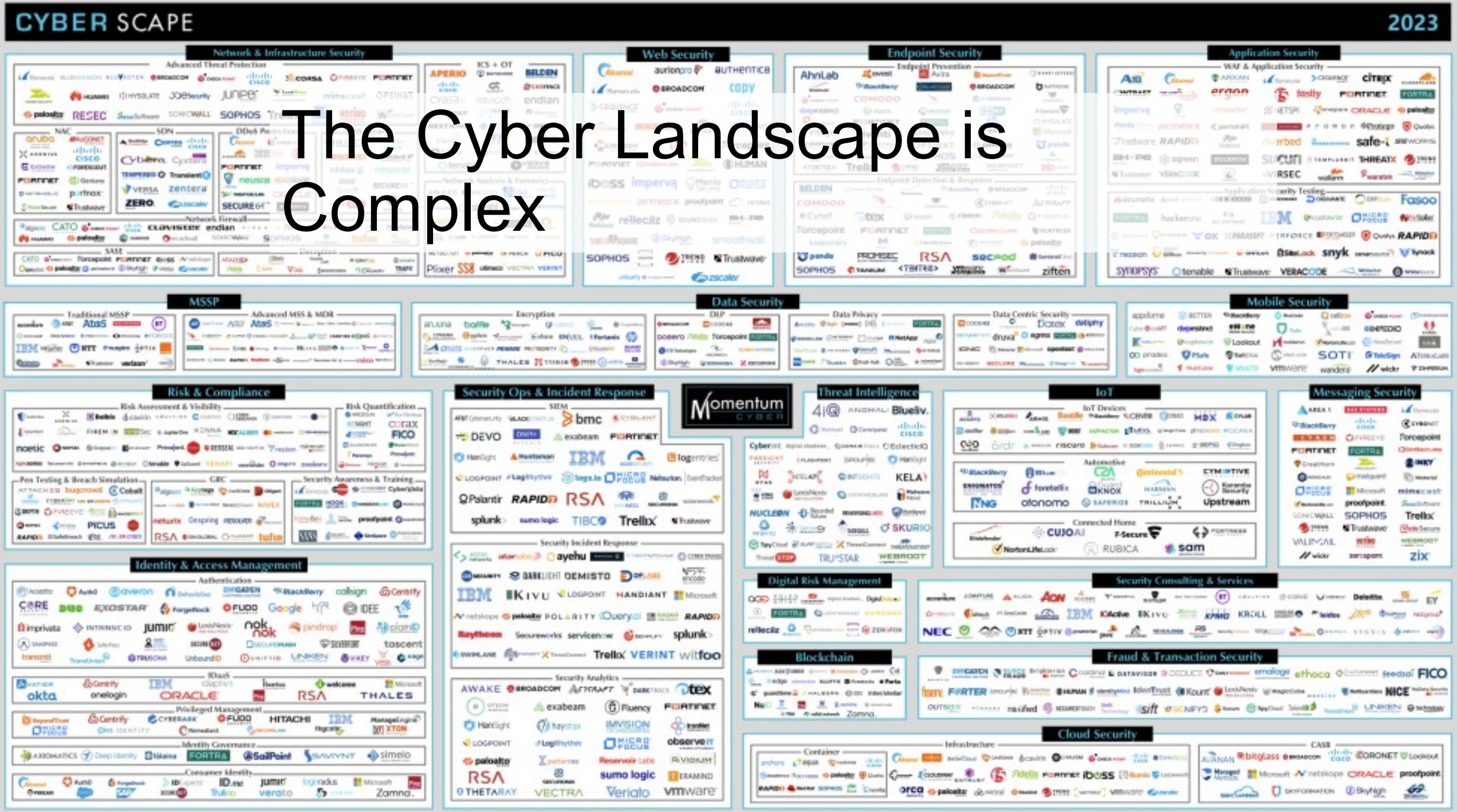
Semantic Interoperability in Cybersecurity:

Harmonizing Threat Intelligence with gist and gistCyber

Ryan E. Hohimer · Peter Winstanley · Kate Studzinski · Dalia Dahleh · Colton Glasgow · Jannes Aasman

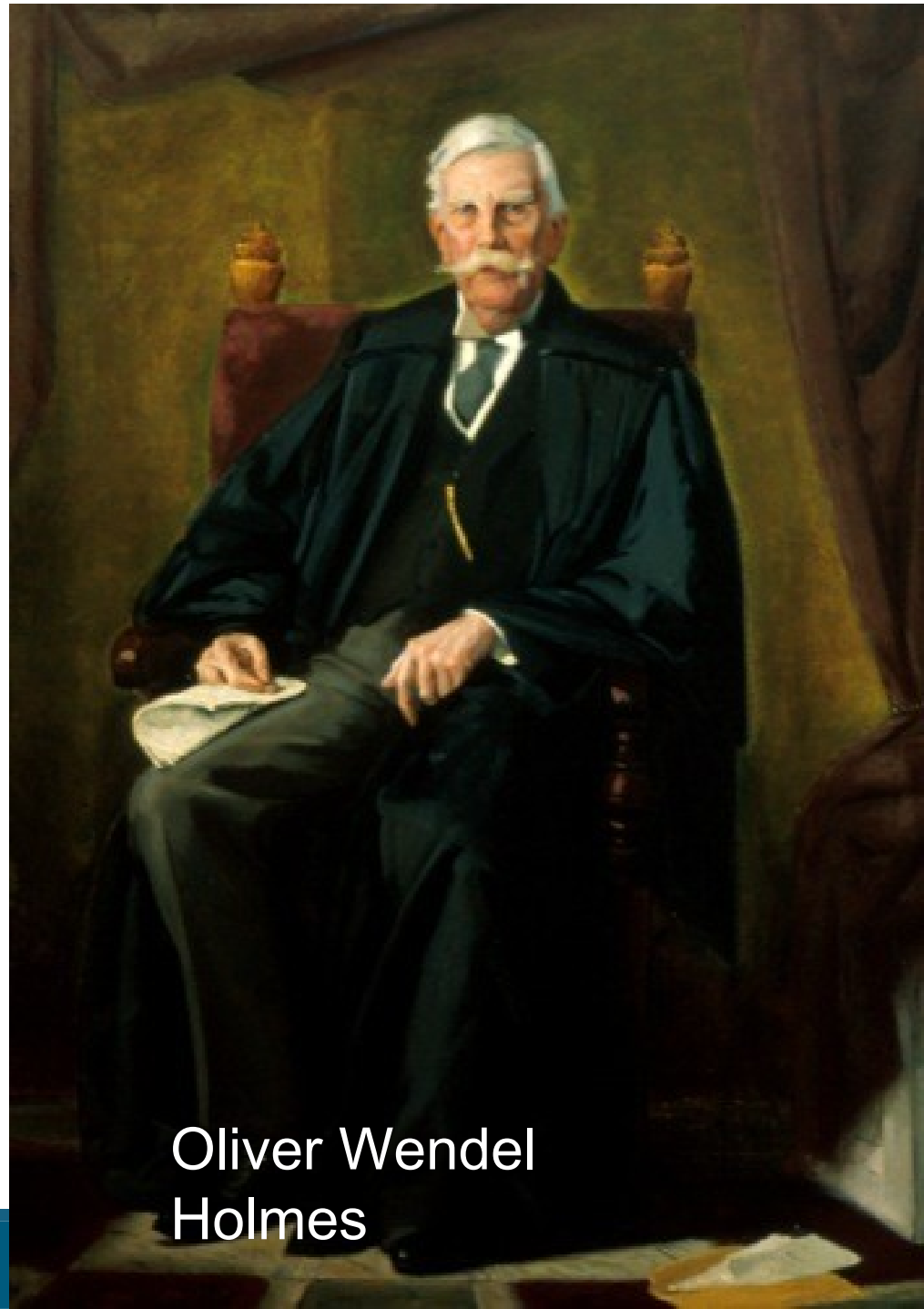
Presenters
Ryan Hohimer, Dave McComb, Jans Aasman

Sematic Technologies for Intelligence Defense, and Security
(STIDS)
May 27, 2026


CYBER SCAPE
2023
The Cyber Landscape is Complex
Network & Infrastructure Security
Advanced Threat Protection
ICS + OT
NAC
SDN
DDoS Protection
Network Firewall
SASE
Web Security
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Application Security Testing
MSSP
Traditional MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Data Centric Security
Mobile Security
Risk & Compliance
Risk Assessment & Visibility
Risk Quantification
Pen Testing & Breach Simulation
GRC
Security Awareness & Training
Security Ops & Incident Response
SIEM
Security Incident Response
Security Analytics
Momentum CYBER
Threat Intelligence
IoT
IoT Devices
Automotive
Connected Home
Messaging Security
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Digital Risk Management
Security Consulting & Services
Blockchain
Fraud & Transaction Security
Cloud Security
Container
Infrastructure
CASB

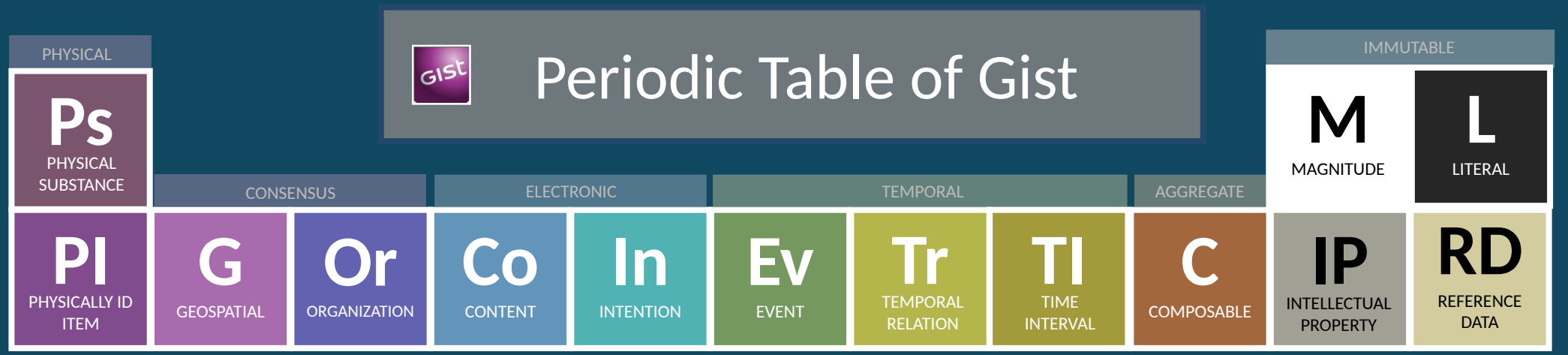
”I wouldn’t give a fig for the simplicity on this side of complexity …

but I would give anything for the simplicity on the far side of complexity”



We are on a quest

- To find the simplicity on the far side of cyber complexity
- Today we'll talk about where our quest started
- The outline of the destination
- And show you the first fruits



100 classes derived from these 14

Plus about 100 properties

https://www.semanticarts.com/gist/

Plus

https://github.com/semanticarts/gistBFO

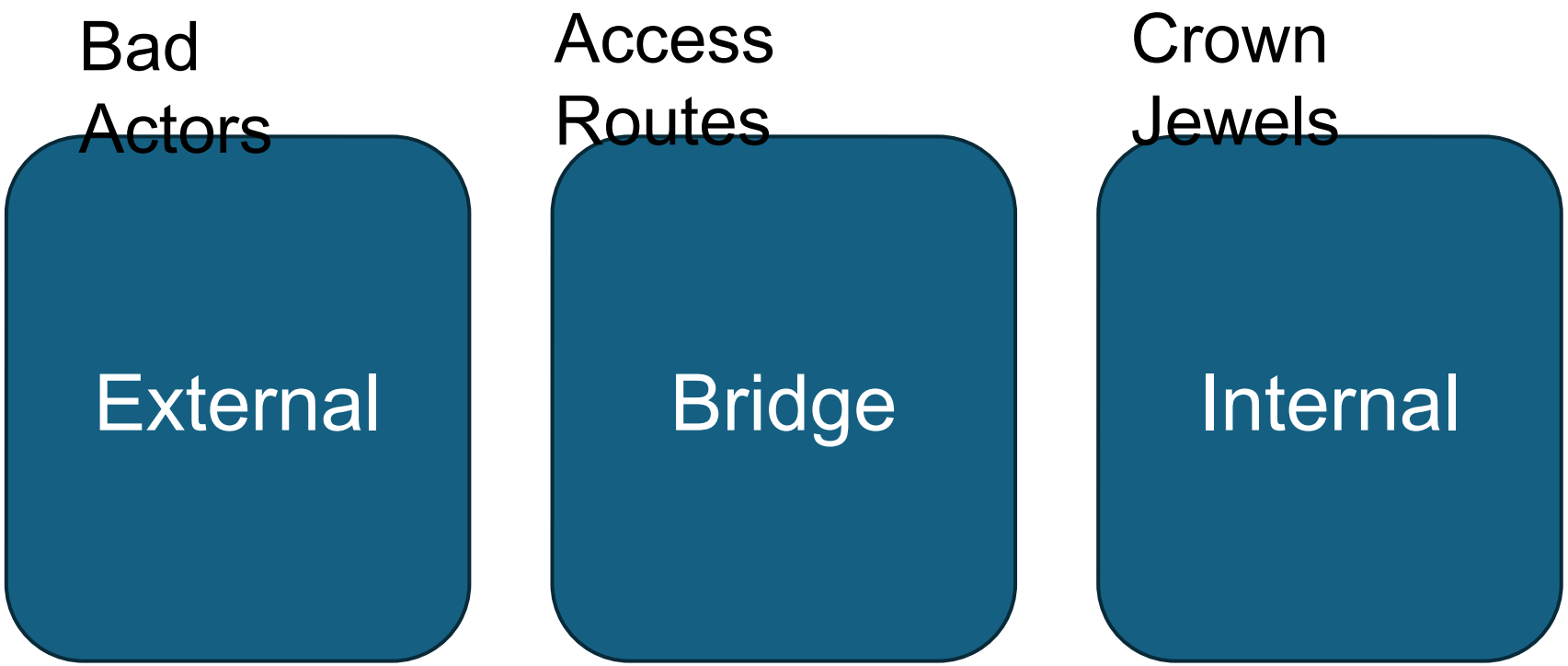
Some key initial explorations on the quest

- Morgan Stanley -- Cyber Risk Group
- Nationwide Insurance – PII in thousands of place
- Juniper Networks – firmware field upgrades, for cyber vulnerabilities
- Broadridge -- Metadata Discovery
- Center for Internet Security -- Benchmarks, Controls and Safeguards
- DarkLight – Threat Intelligence

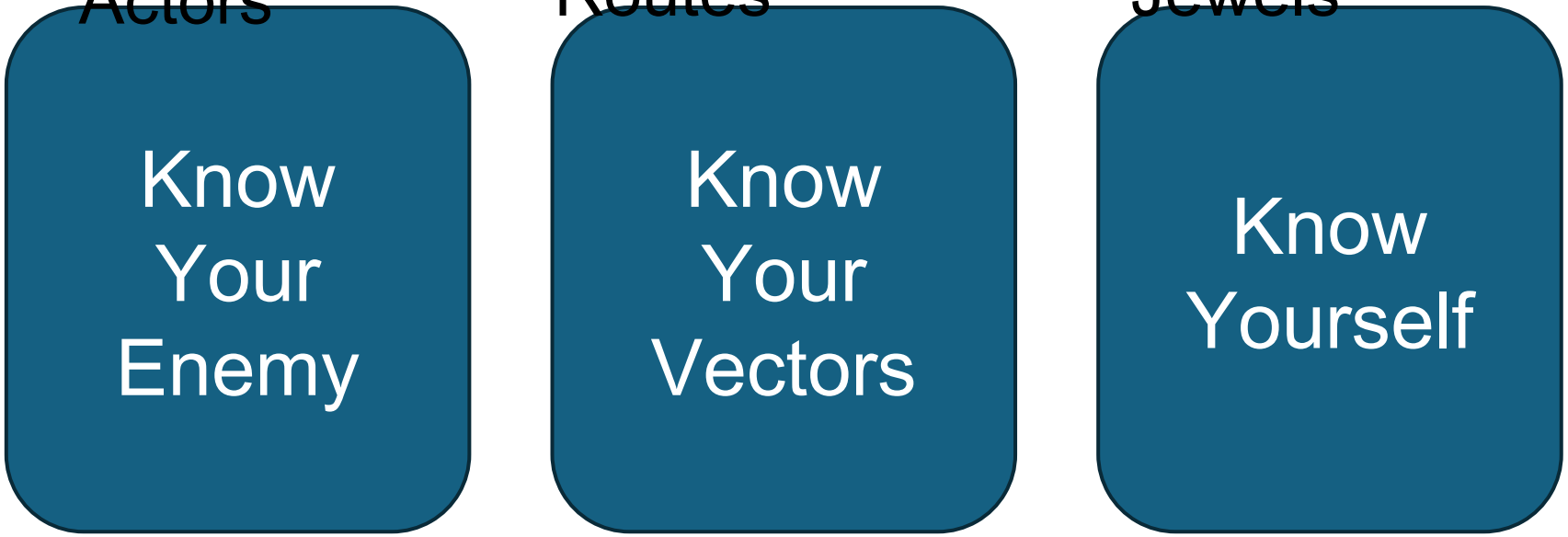
We learned …

- There are dozens of domains within cyber security
- Each with their own vocabulary
- Yet they can conform to three “universes”
- And these three universes can in turn be harmonized
- Around what we call “gistCyber”

The Three Universes …



Imploring …



- Exploitations
- Issues
- Attack Patterns

- Networks
- Software
- Configuration
- Users

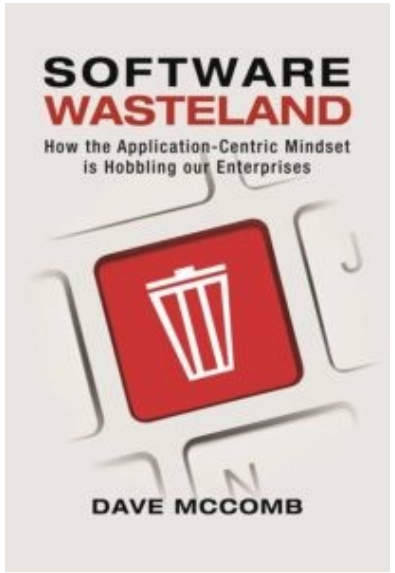
- Convertible Digital Assets
- Sensitive Information
- PII

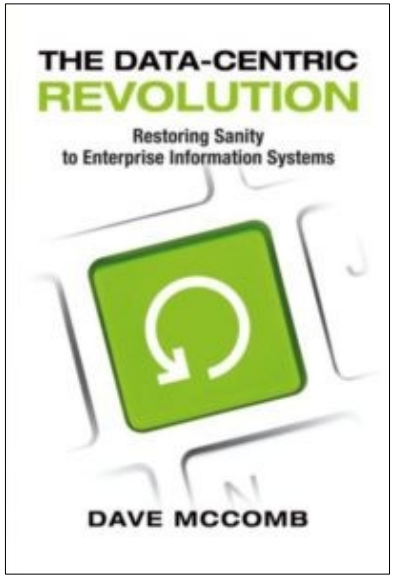
Where did these opinions come from?

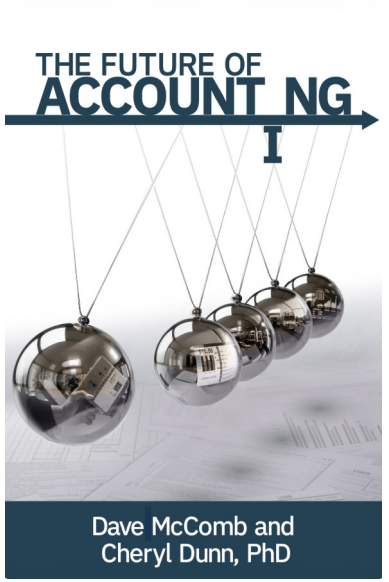
Dave McComb

- Author of ..

.







- CEO and co-founder of Semantic Arts

Semantic Arts

- Prof Services (30 employees)
- 100% focused on Knowledge Graph Implementation
- For 25 years

- Using a methodology we call the Data-Centric Approach

If you *know the enemy* and *know yourself*, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle. — Sun Tzu, The Art of War

Know Your Enemy

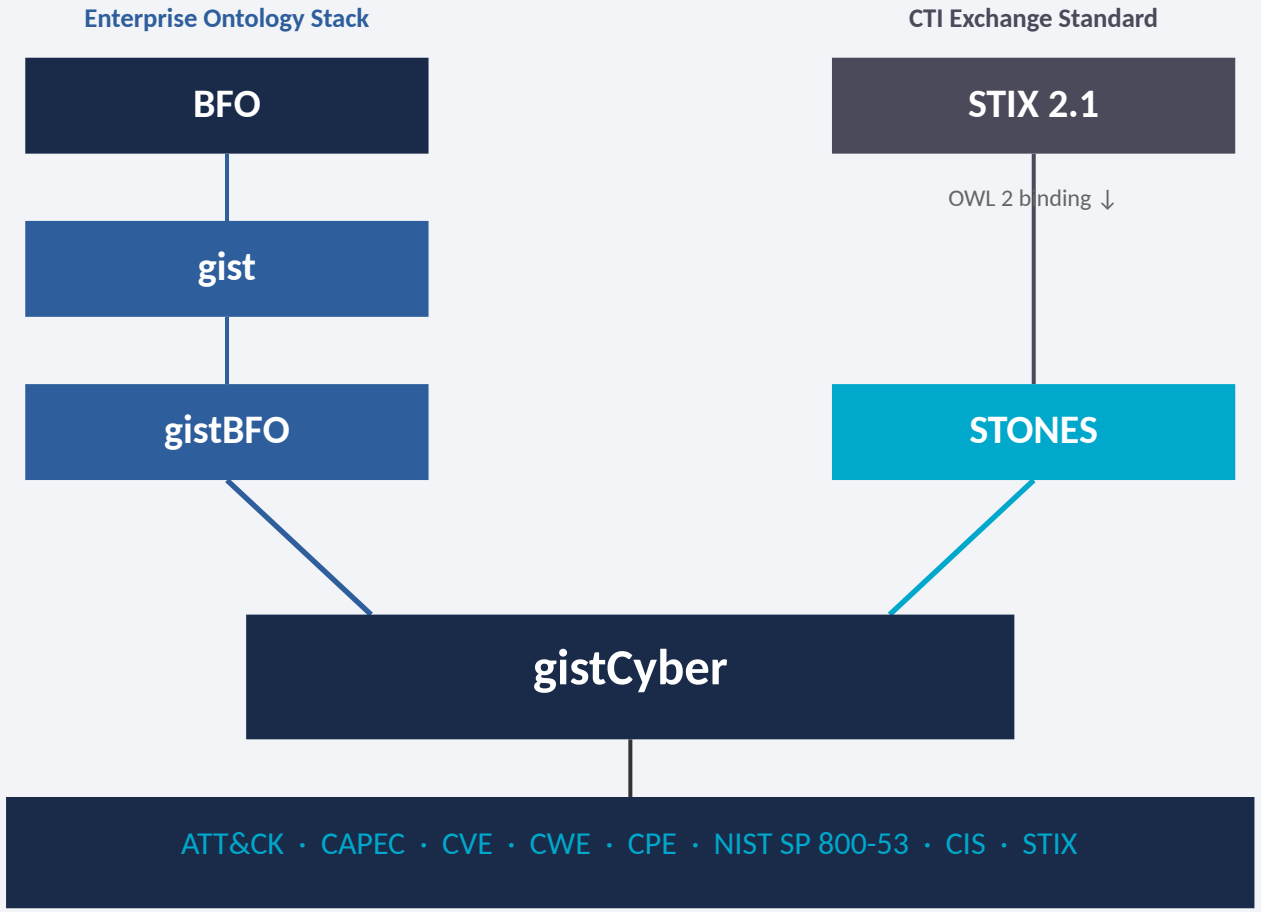
- MITRE ATT&CK — adversary tactics, techniques, and procedures (TTPs)
- CAPEC — common attack patterns and exploitation methods
- CVE — vulnerabilities actively exploited in the wild
- STIX — structured representations of threat actors, campaigns, and courses of action

Know Yourself

- MITRE ATT&CK — adversary tactics, techniques, and procedures (TTPs)
- CPE — your software assets and platform inventory
- CWE — software weaknesses present in your systems
- NIST SP 800-53 — your security and privacy control catalog
- CIS Critical Controls — your prioritized defensive posture

Fragmented standards prevent unified reasoning — gistCyber bridges both sides of the battlefield.

The gistCyber Architecture — Two Traditions, One Semantic Layer



Ontological Alignment Crosswalk

Source	Concept	gistCyber
MITRE ATT&CK	Tactics & Techniques	AttackPattern
CAPEC	Attack Pattern	AttackPattern
STIX	Intrusion Set, Course of Action	AttackPattern
CIS	Safeguard	Control
NIST SP 800-53	Control	Control

New: Semantic Arts has integrated STONES into gistCyber — connecting the STIX 2.1 exchange standard to the gist ontological foundation.

gistCyber — Designed for the Real World

Design Principles

- **Honor Subject Matter Expertise** — grounded in authoritative sources: MITRE, NIST, APL, CIS, NCOR, and countless human Security Analysts
- **Cross-Domain Applicability** — model concepts that transcend verticals: retail, healthcare, manufacturing, industrial control systems
- **Best Practices in KR&R** — Open World Assumption; captures logical relationships and inferential structure, not just data fields
- **Semantic Interoperability** – focus on integration of many excellent sources (data centric architecture)

STONES is now imported into gistCyber
bridging the STIX 2.1 exchange standard to the gist ontological foundation.

- Franz Inc
  - Jans Aasman
  - ja@franz.com
- Semantic Arts
  - Dave McComb
  - Dave.McComb@semanticarts.com
- Hohimer Intelligence Strategies
  - Ryan Hohimer
  - Ryan.Hohimer@cyberterrain.org

It's Demo Time!