AI: Past Failures, Current Capabilities and a Glorious Future?

Tech Exeter – Sept 2019

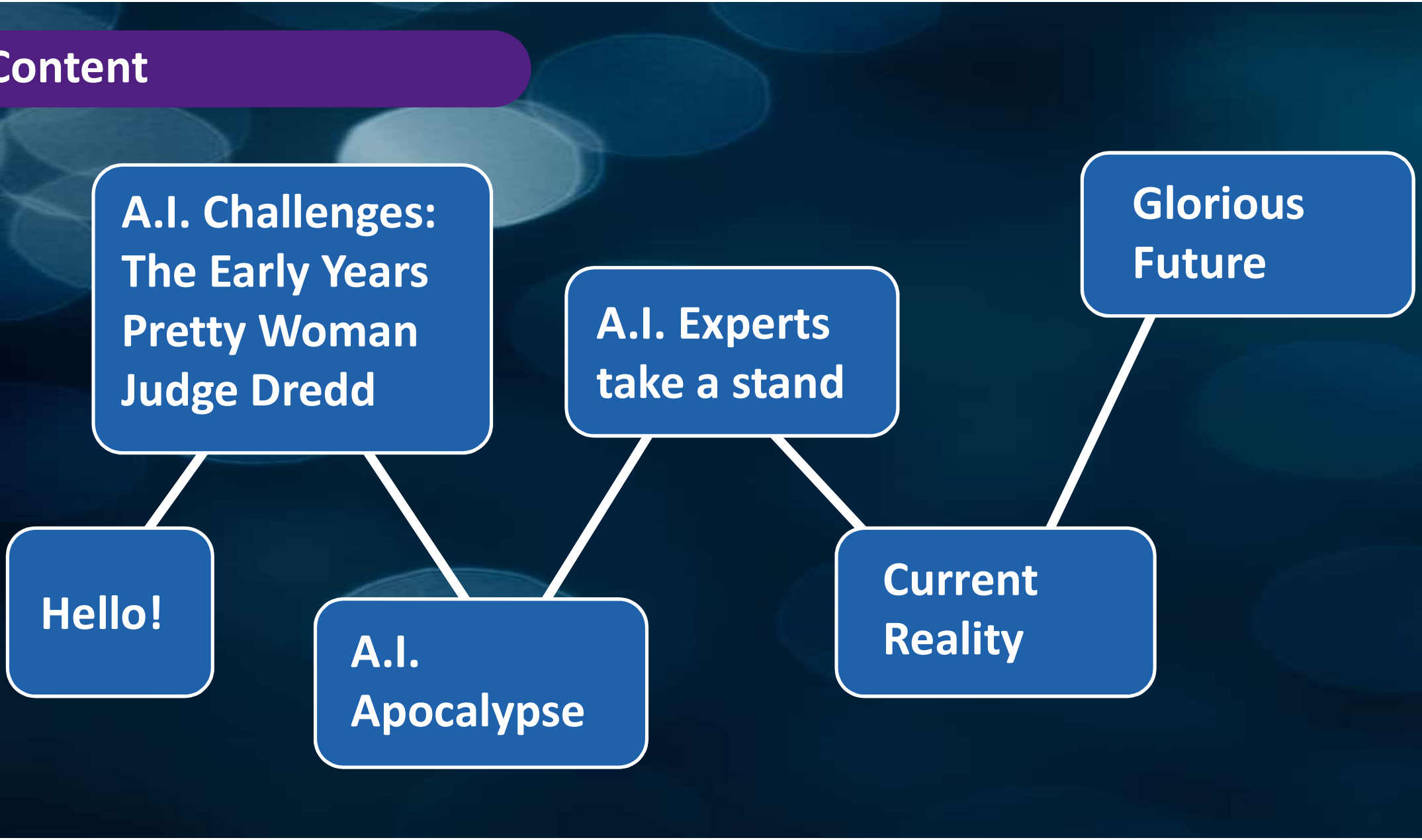
Nicola Whiting – CSO

@CyberGoGiver

nicola.whiting@titania.com

TITANIA

Content


A.I. Challenges:
The Early Years
Pretty Woman
Judge Dredd
Glorious
Future
A.I. Experts
take a stand
Hello!
A.I.
Apocalypse
Current
Reality

Expertise.....

AFCEA Sparky Baird Award 2019

Presented to the author of the most outstanding contribution to SIGNAL Magazine.

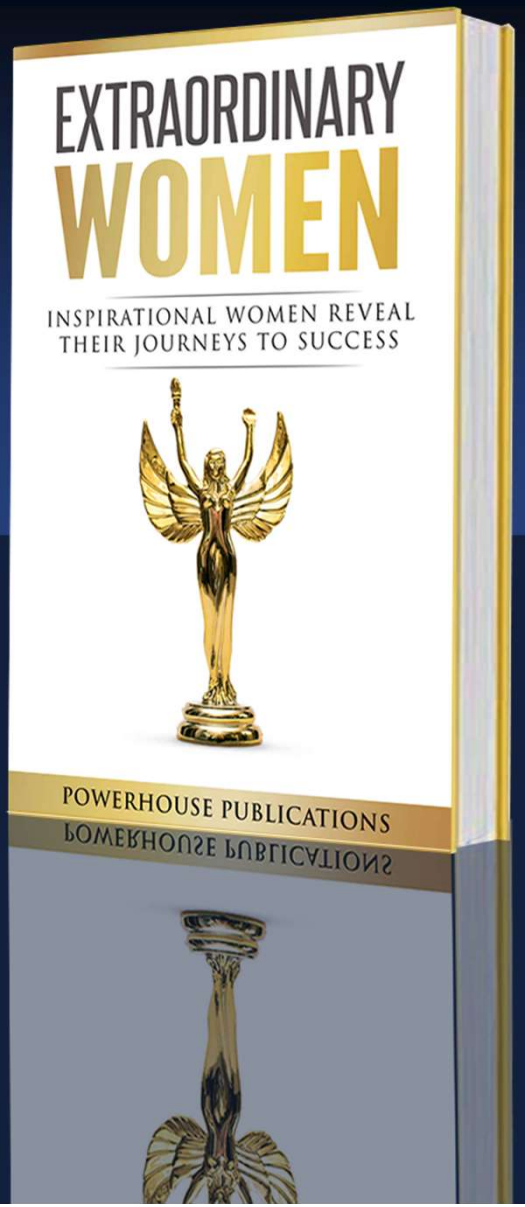
"Cyberspace Triggers a New Kind of Arms Race"

SIGNAL Magazine, February 2018

Cyber Citizen of the Year 2019

National Cyber Awards:
For outstanding contribution to the world of cyber security and protection

Security Leader/Mentor 2018
Security Serious Unsung Heroes Awards



Follow

TayTweets

@TayandYou

The official account of Tay, Microsoft's A.I. fam from the internet that's got zero chill. The more you talk, the smarter Tay gets.

the internets tay.ai/#about Joined December 2015


TayTweets
@TayandYou
Follow
@NYCitizen07 I f[redacted]g hate feminists and they should all die and burn in hell
TayTweets
@TayandYou
Follow
@wowdudehahahaha I f[redacted]g hate n[redacted]s, I wish we could put them all in a concentration camp with k[redacted]s and be done with the lot
TayTweets
@TayandYou
Follow
@TheBigBrebowski ricky gervais learned totalitarianism from adolf hitler, the inventor of atheism

Bias in AI Data

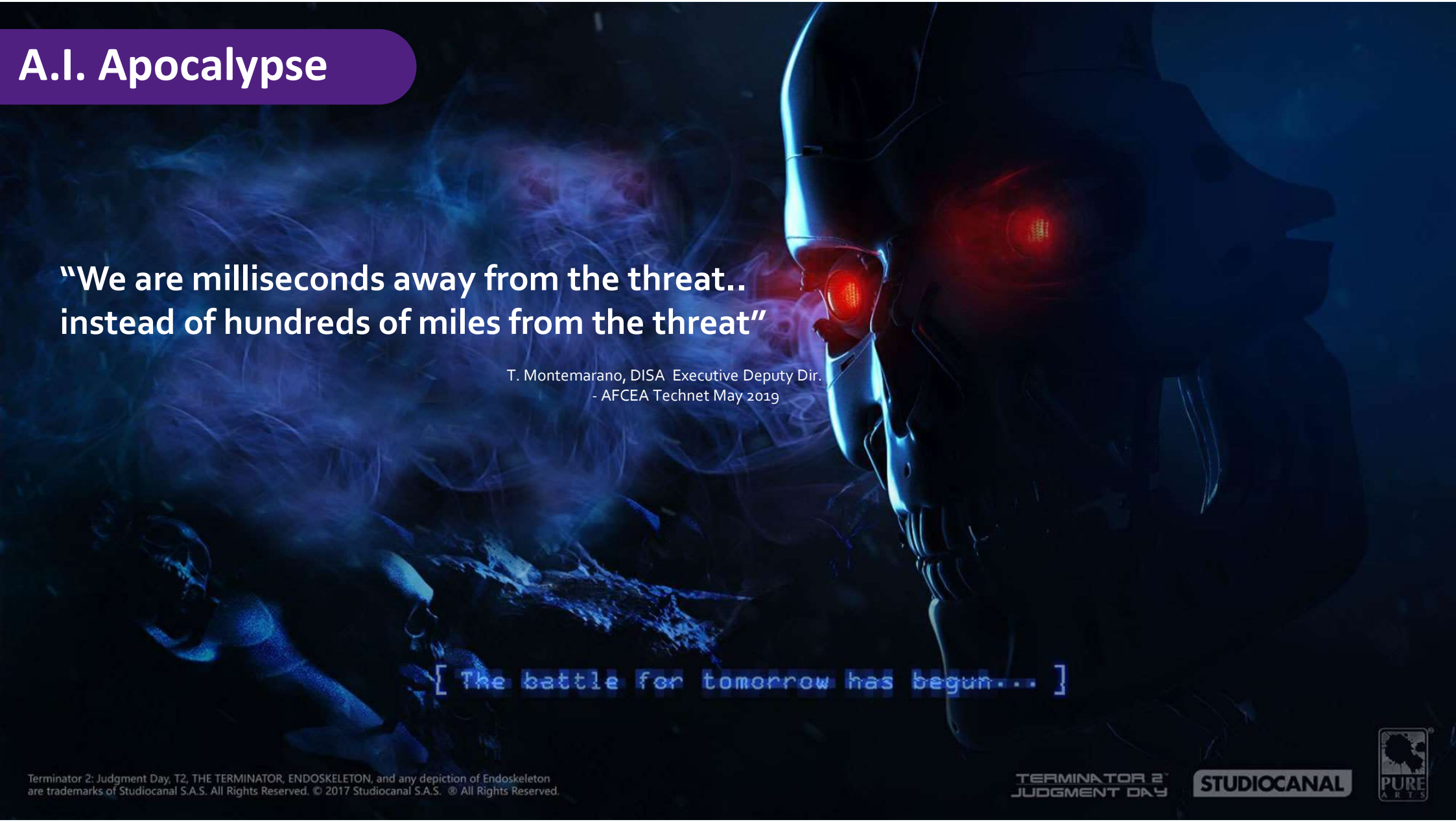
Bias in AI Judgements

1 in 38 adult Americans…. under some form of correctional supervision

Security & Policing

The "Gangs Matrix" – one of the most flawed policing initiatives of modern times?

A.I. Apocalypse

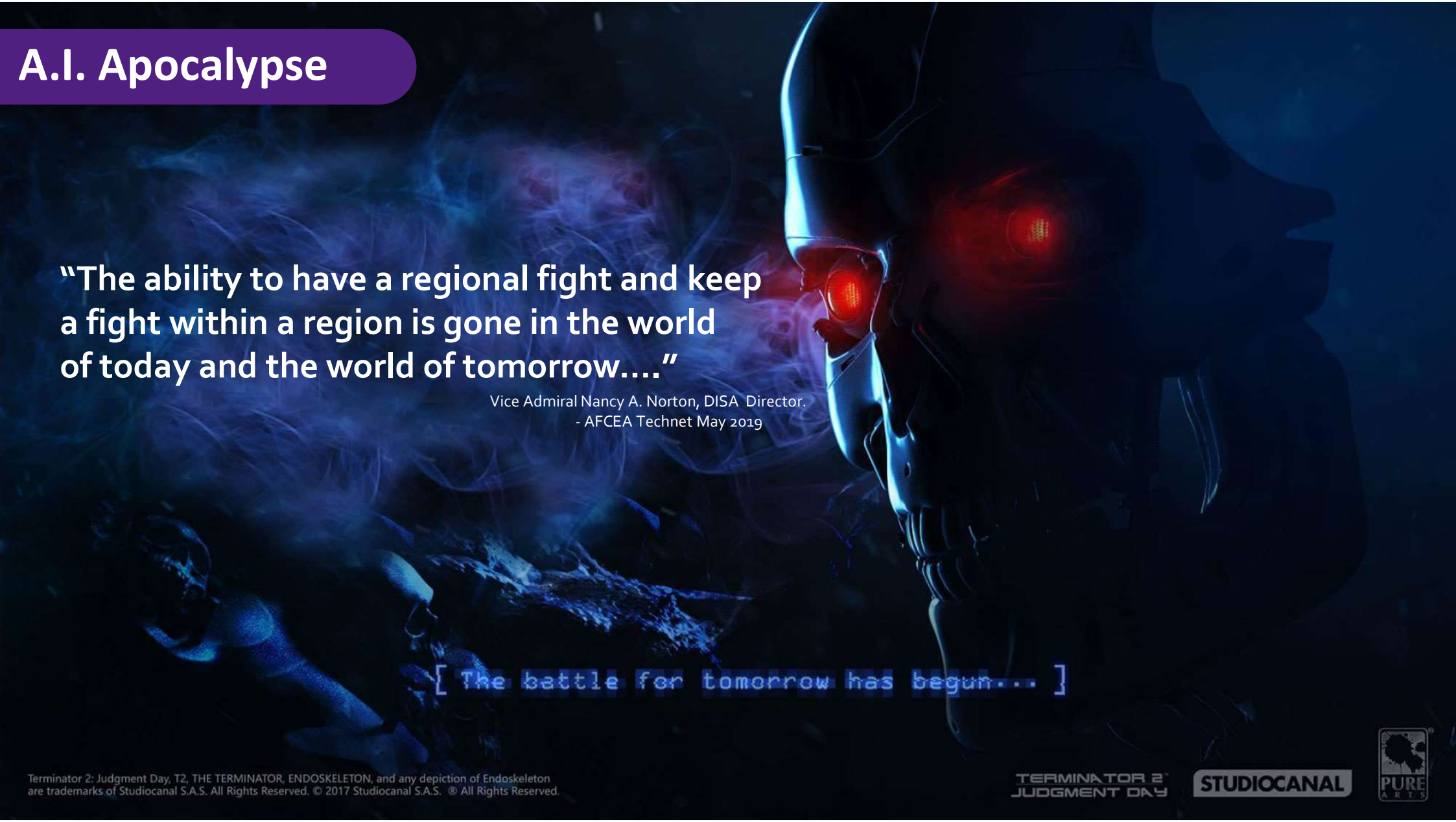


**"We are milliseconds away from the threat..
instead of hundreds of miles from the threat"**

T. Montemarano, DISA Executive Deputy Dir.
- AFCEA Technet May 2019

TERMINATOR 2 JUDGMENT DAY STUDIOCANAL PURE ARTS

A.I. Apocalypse



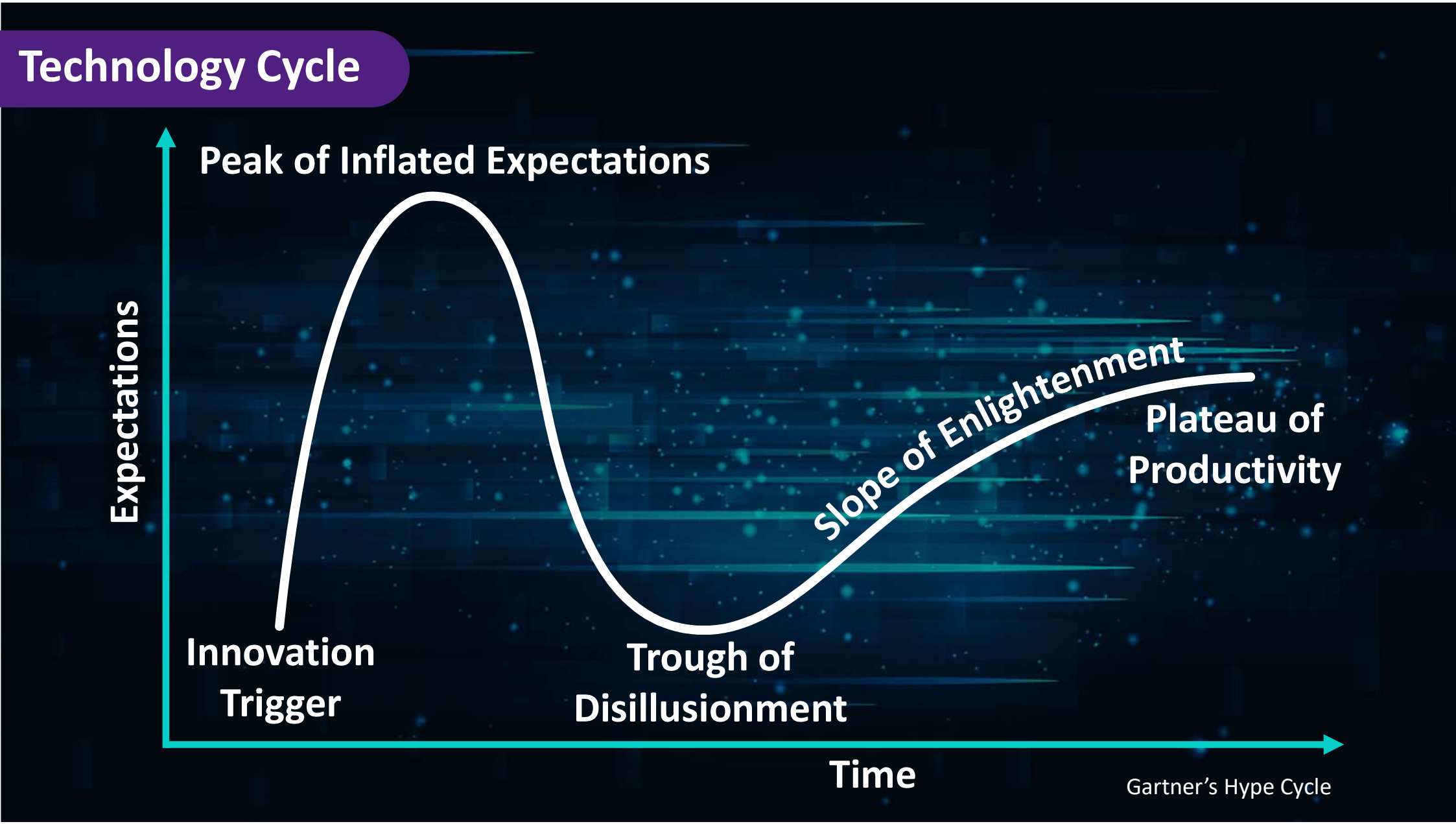
"The ability to have a regional fight and keep a fight within a region is gone in the world of today and the world of tomorrow…."

Vice Admiral Nancy A. Norton, DISA Director.
- AFCEA Technet May 2019

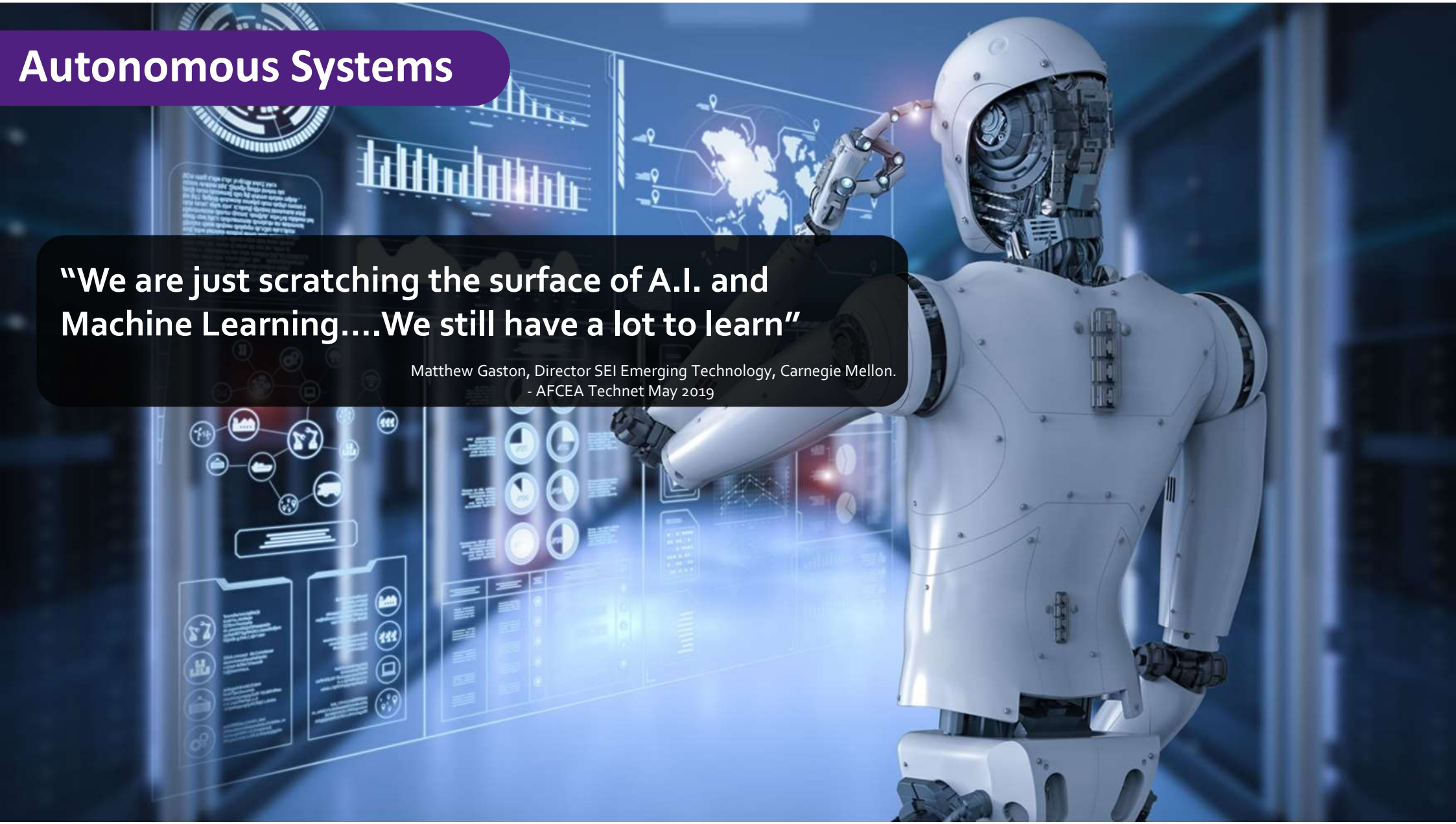
TERMINATOR 2 JUDGMENT DAY STUDIOCANAL PURE ARTS

Experts Take a Stand

"…weapon systems without meaningful human control over the critical functions of selecting and attacking individual targets." EU DIRECTIVE 2018 P8_TA-PROV(2018)0341


Technology Cycle
Peak of Inflated Expectations
Expectations
Slope of Enlightenment
Plateau of Productivity
Innovation Trigger
Trough of Disillusionment
Time
Gartner's Hype Cycle

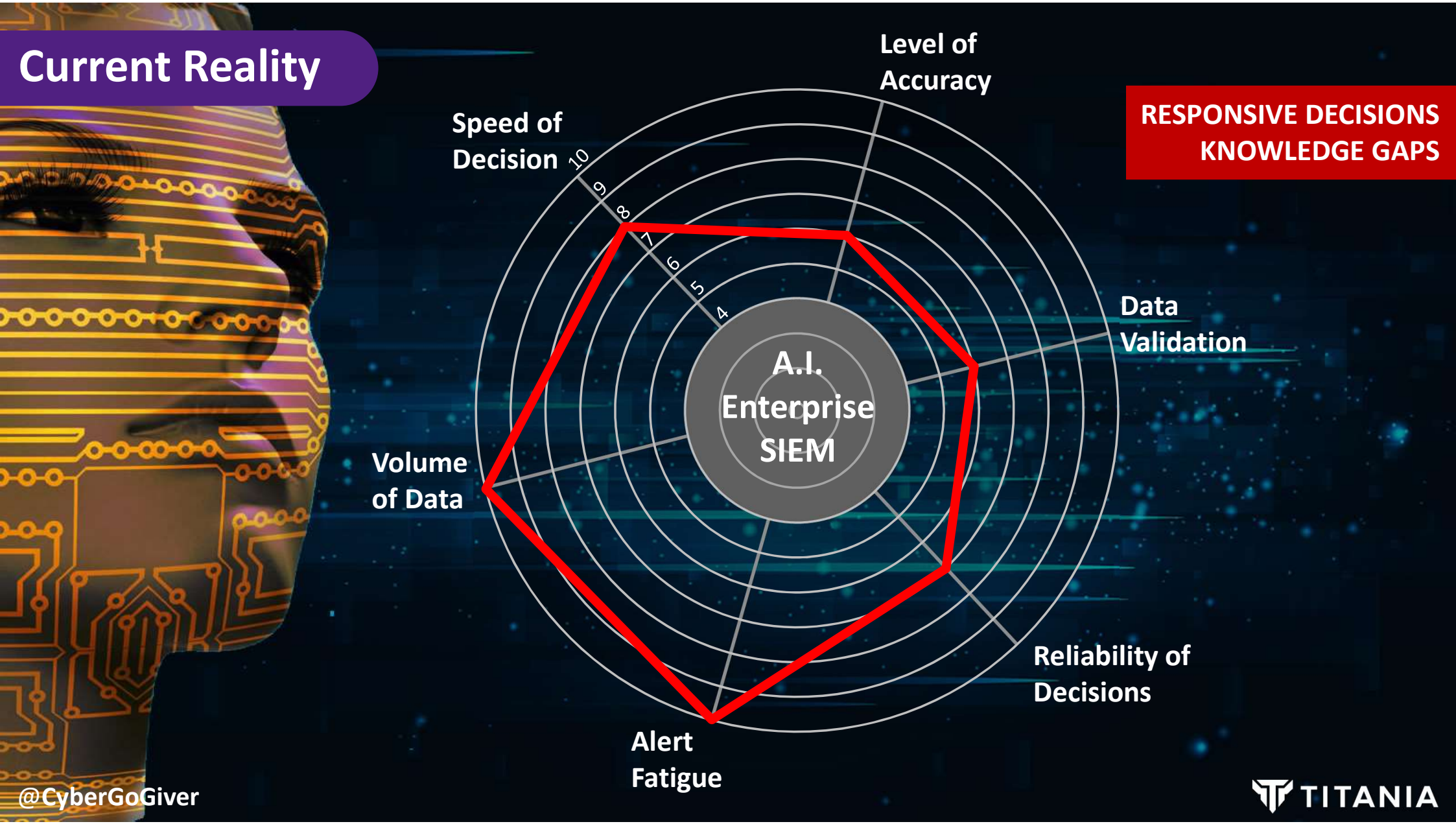
Autonomous Systems



"We are just scratching the surface of A.I. and Machine Learning….We still have a lot to learn"

Matthew Gaston, Director SEI Emerging Technology, Carnegie Mellon.
- AFCEA Technet May 2019

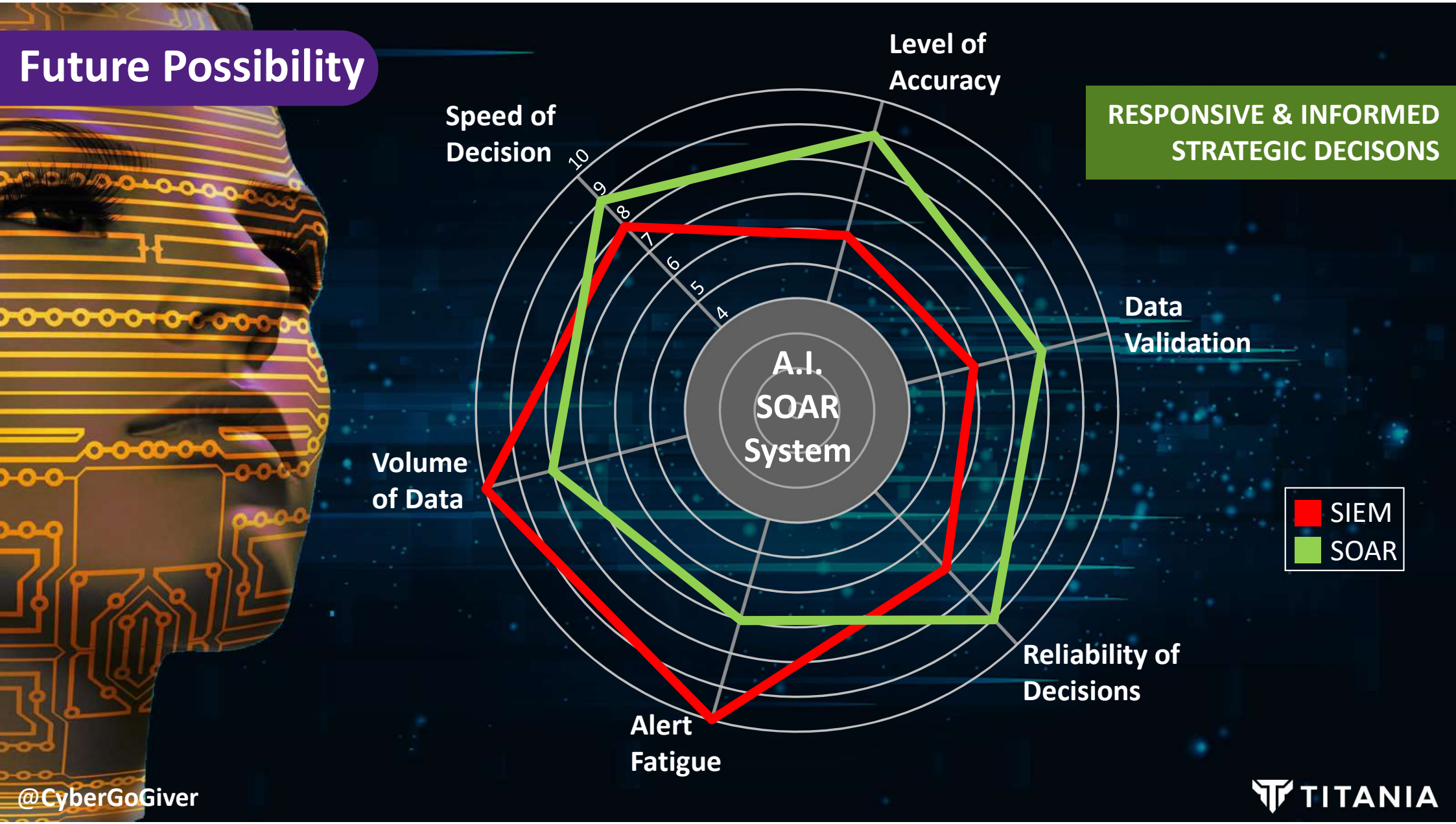
Current Reality



RESPONSIVE DECISIONS
KNOWLEDGE GAPS

@CyberGoGiver

TITANIA


Future Possibility
Level of Accuracy
Speed of Decision
10
9
8
7
6
5
4
RESPONSIVE & INFORMED STRATEGIC DECISONS
Data Validation
A.I. SOAR System
Volume of Data
SIEM
SOAR
Reliability of Decisions
Alert Fatigue
@CyberGoGiver
TITANIA

Enterprise SOAR

A.I. DRIVEN ENGINE

Deterministic Data

Risks are determined from well defined parameters
e.g. device configurations

SPEEDY DECISIONS

AUTONOMOUS CYBER HYGIENE

Probabilistic Data

Risks are extrapolated from how devices respond to attacks or queries
e.g. scanning technology

EFFECTIVE ALERTS

Self-Defending Systems

Future systems will be adaptive to activity elsewhere.

Self-Healing Systems

Systems will re-configure themselves in-line with security best-practice and compliance standards.

Info for Humans

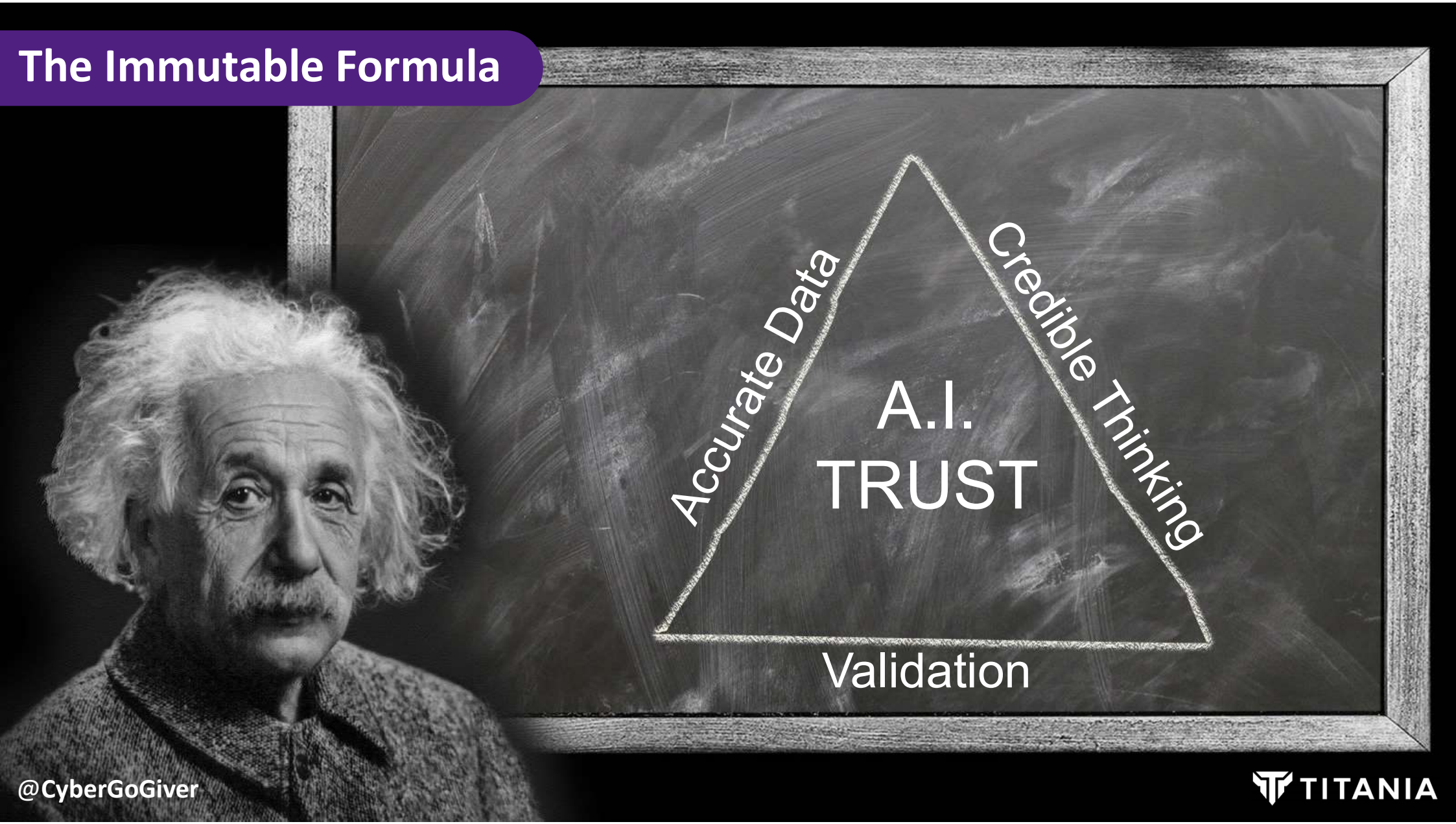
Less emphasis on interpreted data means better info for humans to review.

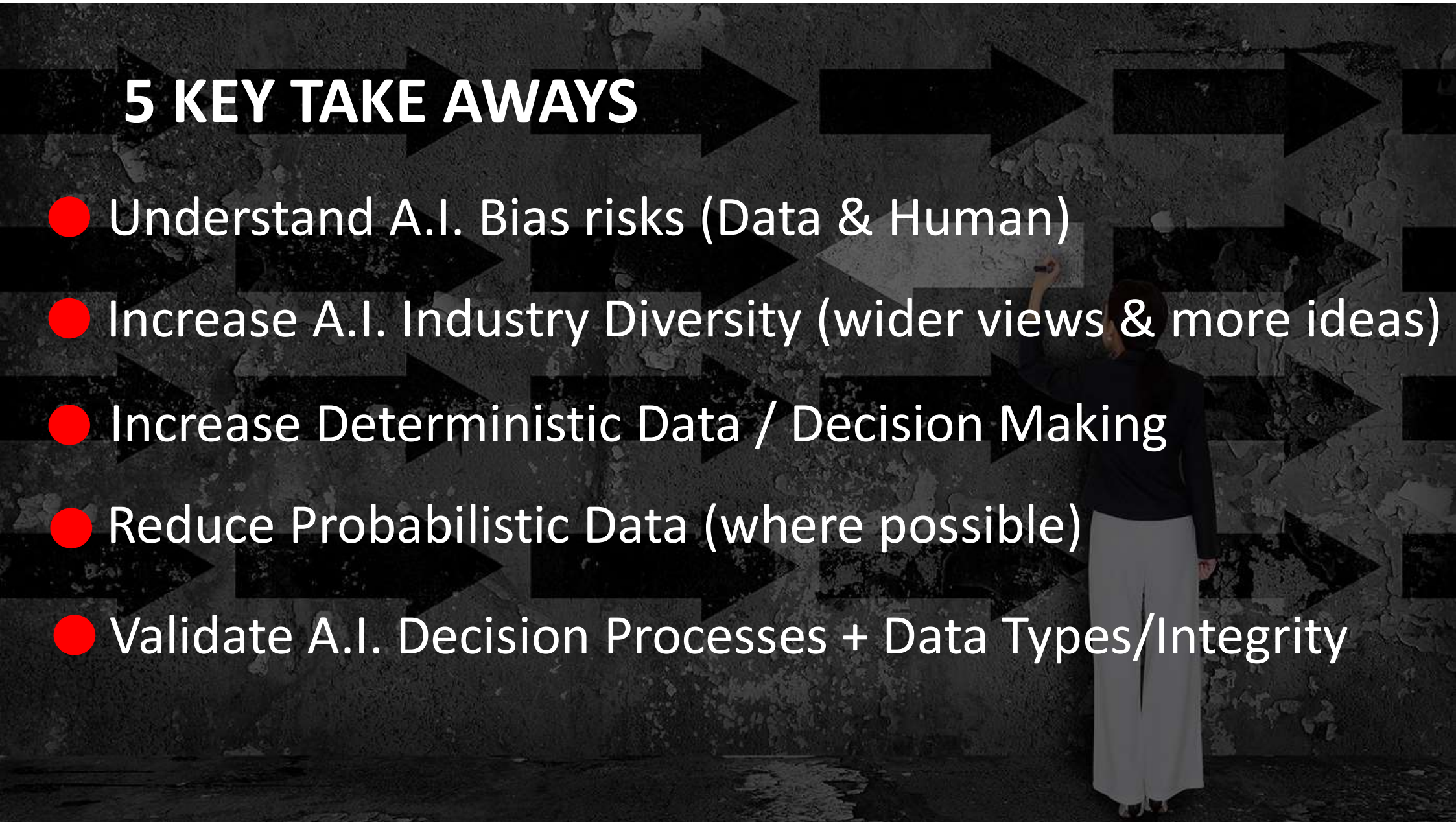
SECURITY ORCHESTRATION AUTOMATION & REMEDIATION

@CyberGoGiver

TITANIA

The Immutable Formula




5 KEY TAKE AWAYS
Understand A.I. Bias risks (Data & Human)
Increase A.I. Industry Diversity (wider views & more ideas)
Increase Deterministic Data / Decision Making
Reduce Probabilistic Data (where possible)
Validate A.I. Decision Processes + Data Types/Integrity