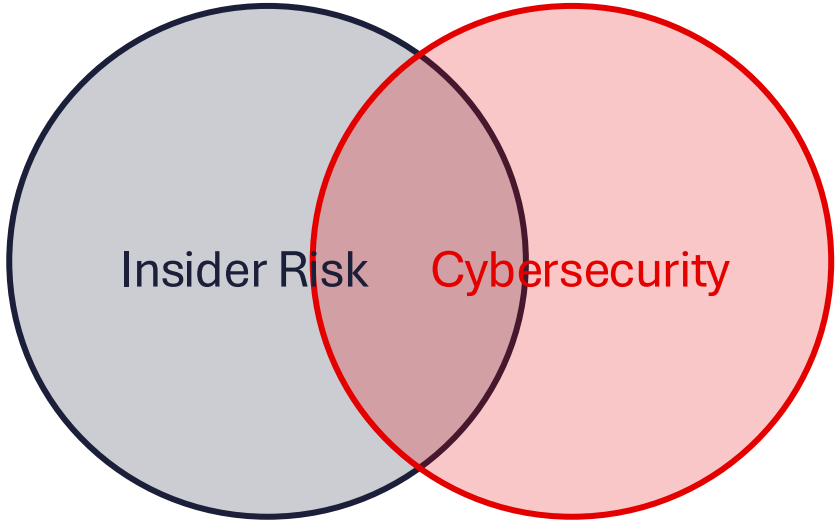
Bridging Insider Risk and Cybersecurity

Information Systems Security Association

Austin Whisnant

Nov 18, 2026





Intern,
Analyst,
Engineer,
Researcher



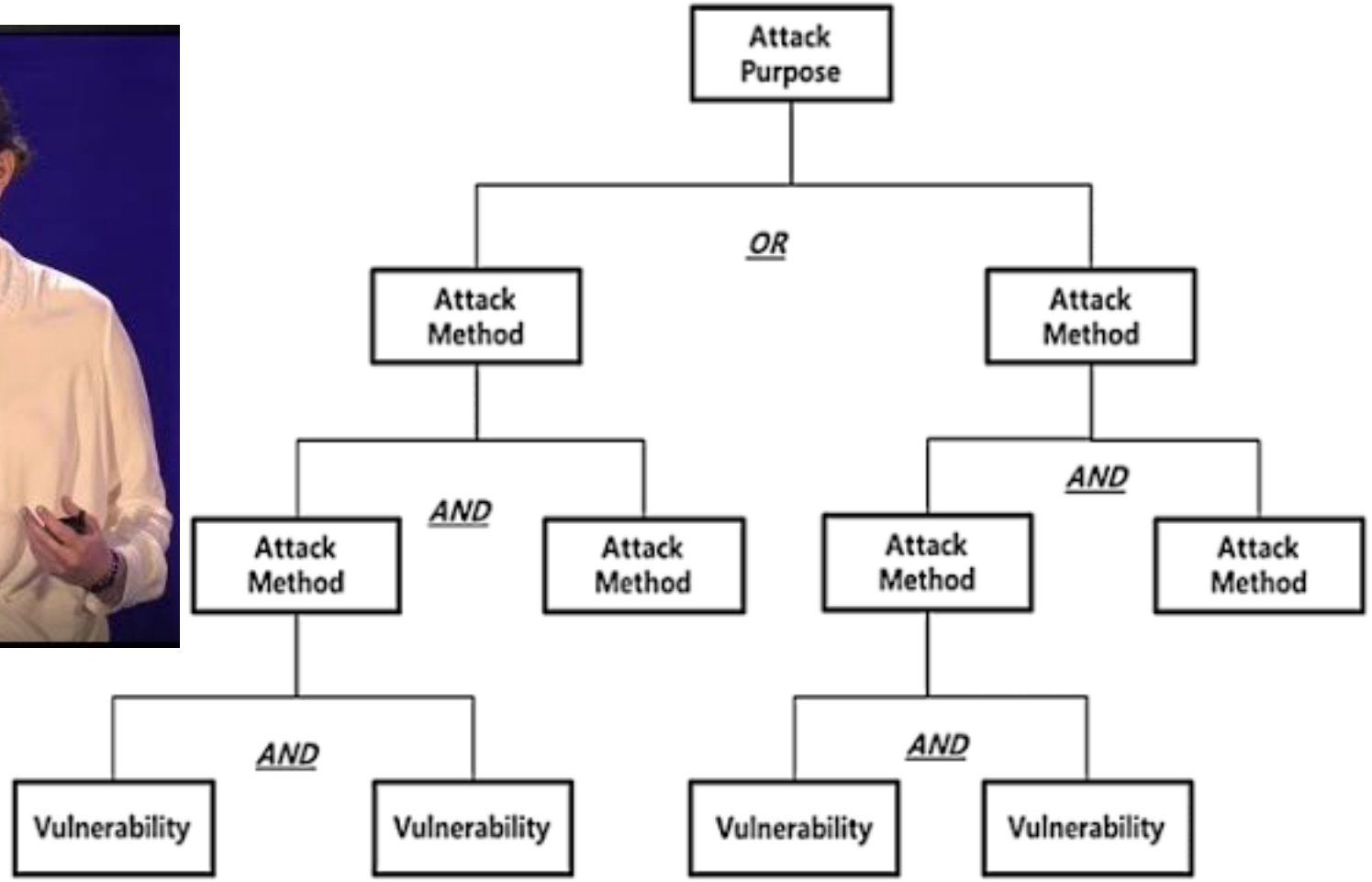


DTEX

Analyst

Network Defense Analyst





Anomaly detection & baselining

Critical asset management

Technical monitoring

Technical attack surface

Attack methods and tools

Cybersecurity Researcher - Cyberfusion

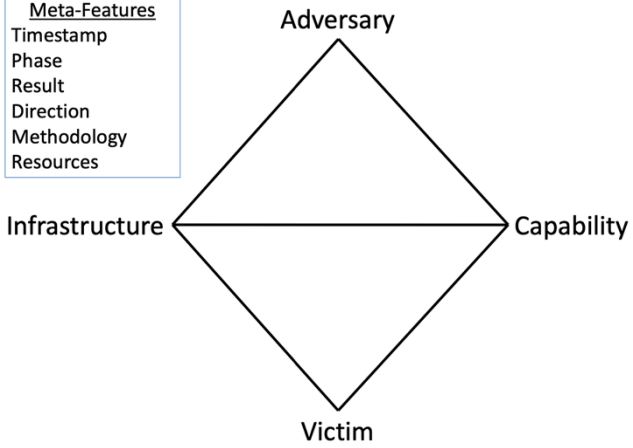
MANDIANT

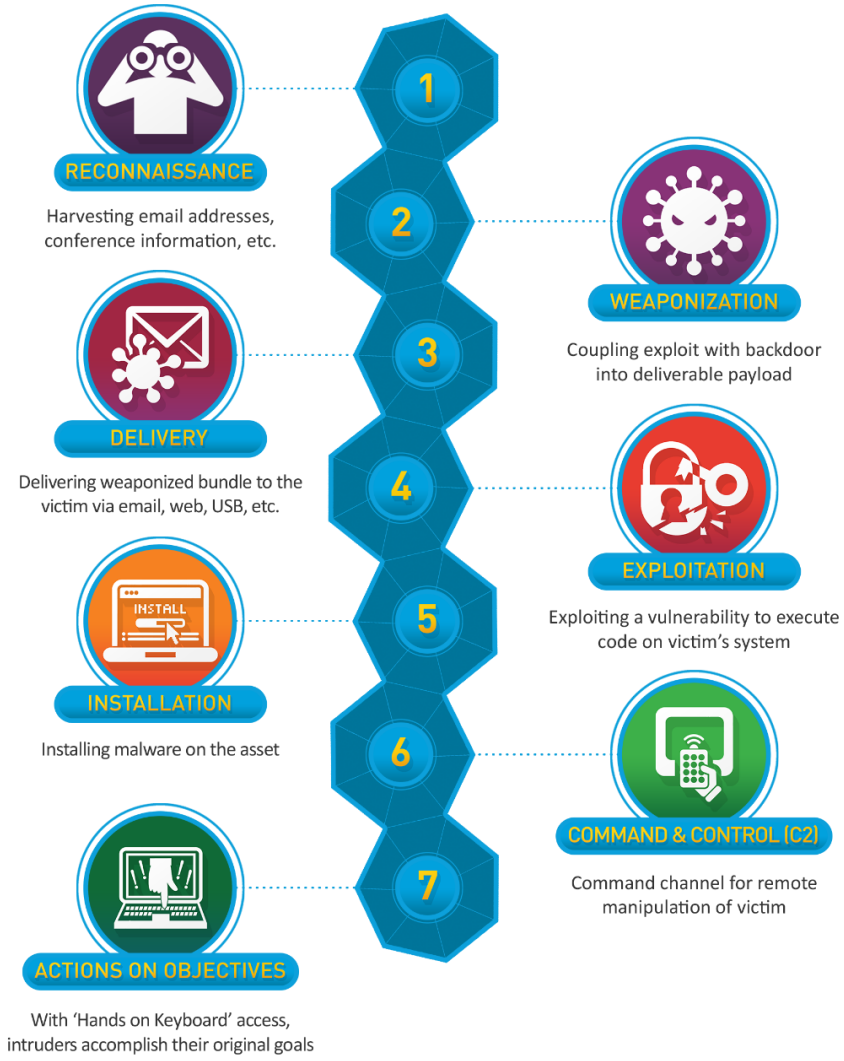
MITRE ATT&CK™

APT1

Exposing One of China's Cyber Espionage Units

Meta-Features
Timestamp
Phase
Result
Direction
Methodology
Resources





Intelligence and Indicators

Attack paths

Attacker profiles and motives

External attack infrastructure

Attribution difficulty

Limited judicial recourse

Anomaly detection
Critical asset management
Technical monitoring
Technical attack surface
Attack methods and tools

Cybersecurity Engineer – Workforce Development





Risk prioritization

Triage and validation

Technical Controls

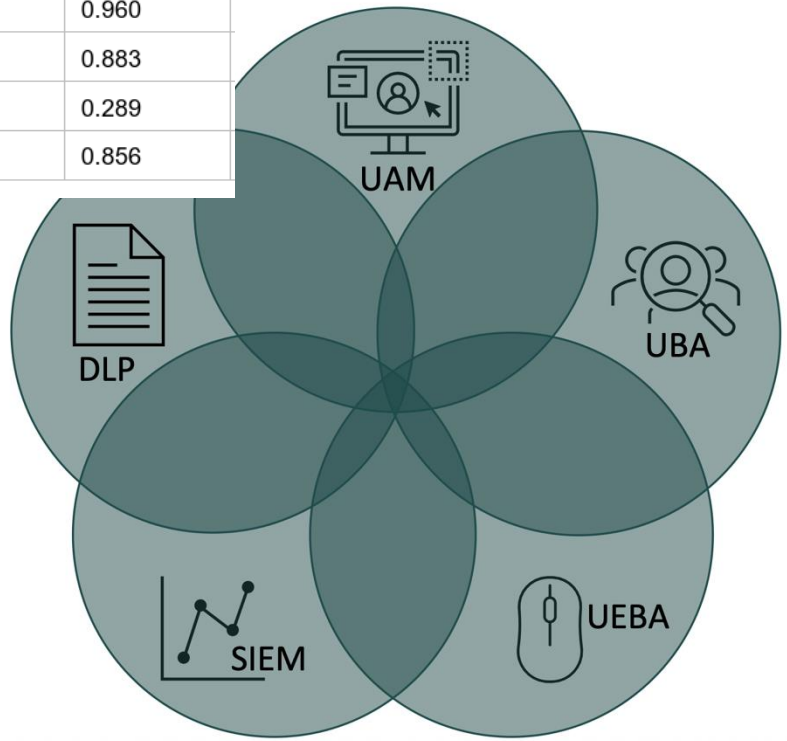
Data correlation

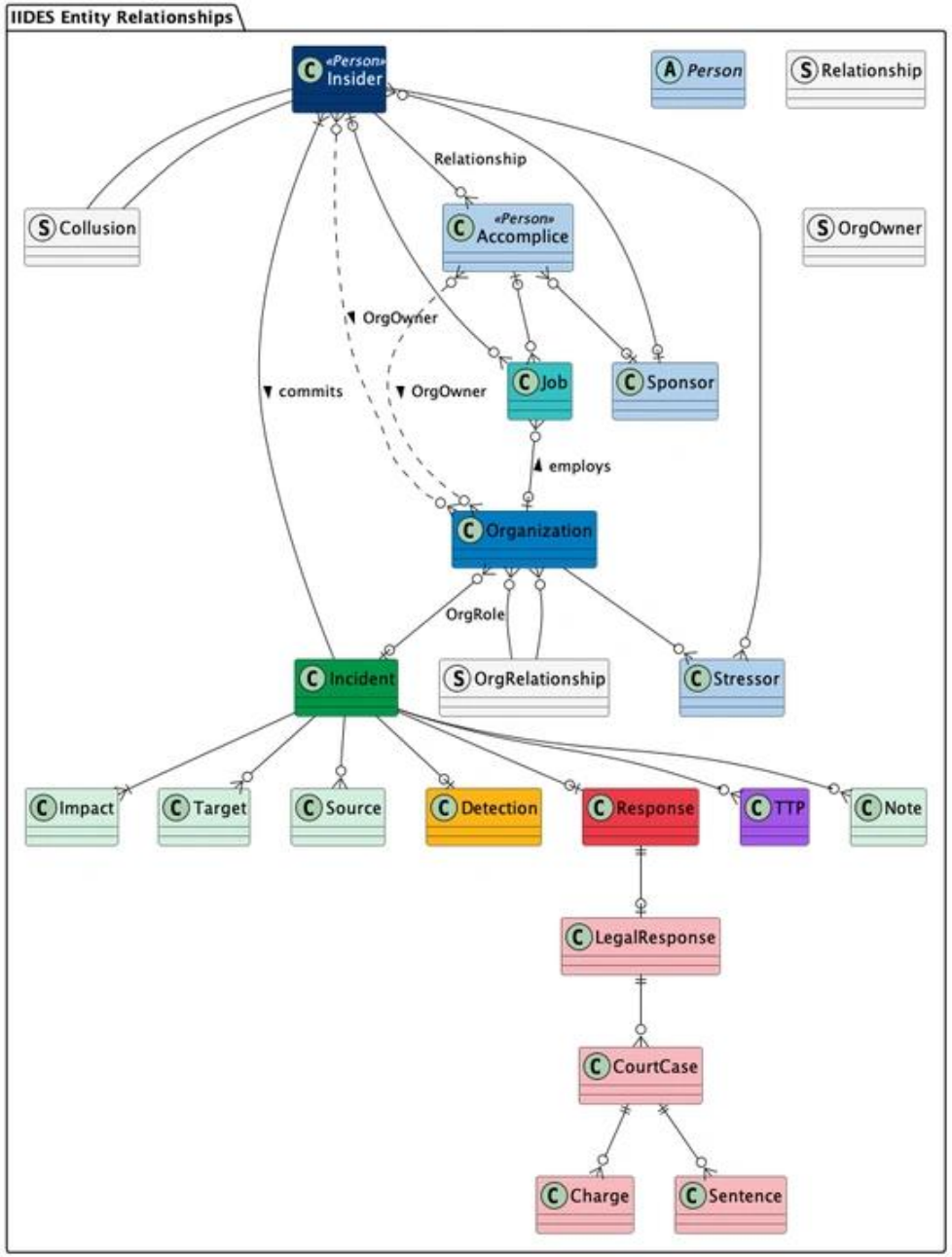
Anomaly detection
Critical asset management
Technical monitoring
Technical attack surface
Attack methods and tools
Intelligence and indicators
Attack paths
Profiles and motives
External infrastructure
Attribution difficulty
Limited judicial recourse

Senior Researcher – Insider Risk

Table 6: Classifier Results for One-Hot Encoding

	Recall	FPR	Precision	Accuracy
KNN	0.028	0.014	0.121	0.926
Random Forest	**0.902**	**0.216**	0.222	0.791
Gradient Boosting	0.500	0.007	0.837	0.960
Logistic Regression	0.837	0.114	0.345	0.883
Decision Tree	**0.982**	**0.757**	0.080	0.289
Multinomial NB	0.863	0.145	0.281	0.856





Carnegie Mellon University
Software Engineering Institute

DANGERS OF AI FOR INSIDER RISK EVALUATION (DARE)

Austin Whisnant

October 2024

Authorized access

Trusted user

Organizational context

Job role context

Investigative bias handling

Investigation sensitivity

Human-centric intervention

Privacy considerations

Psychosocial impact of monitoring

Understand intent

Involving other departments

Employee awareness & training

Intelligence

Attack paths

Anomaly detection

Critical asset management

Risk prioritization

Triage/Validation

Profiles/motivation

Technical monitoring

Data correlation

DTEX Principal Insider Risk Analyst

DTEX i3







DTEX FEDERAL

Authorized access

Trusted user

Organizational context

Job role context

Investigative bias handling

Investigation sensitivity

Human-centric intervention

Privacy considerations

Psychosocial impact of monitoring

Understand intent

Involving other departments

Employee awareness & training

Intelligence

Attack paths

Anomaly detection

Critical asset management

Risk prioritization

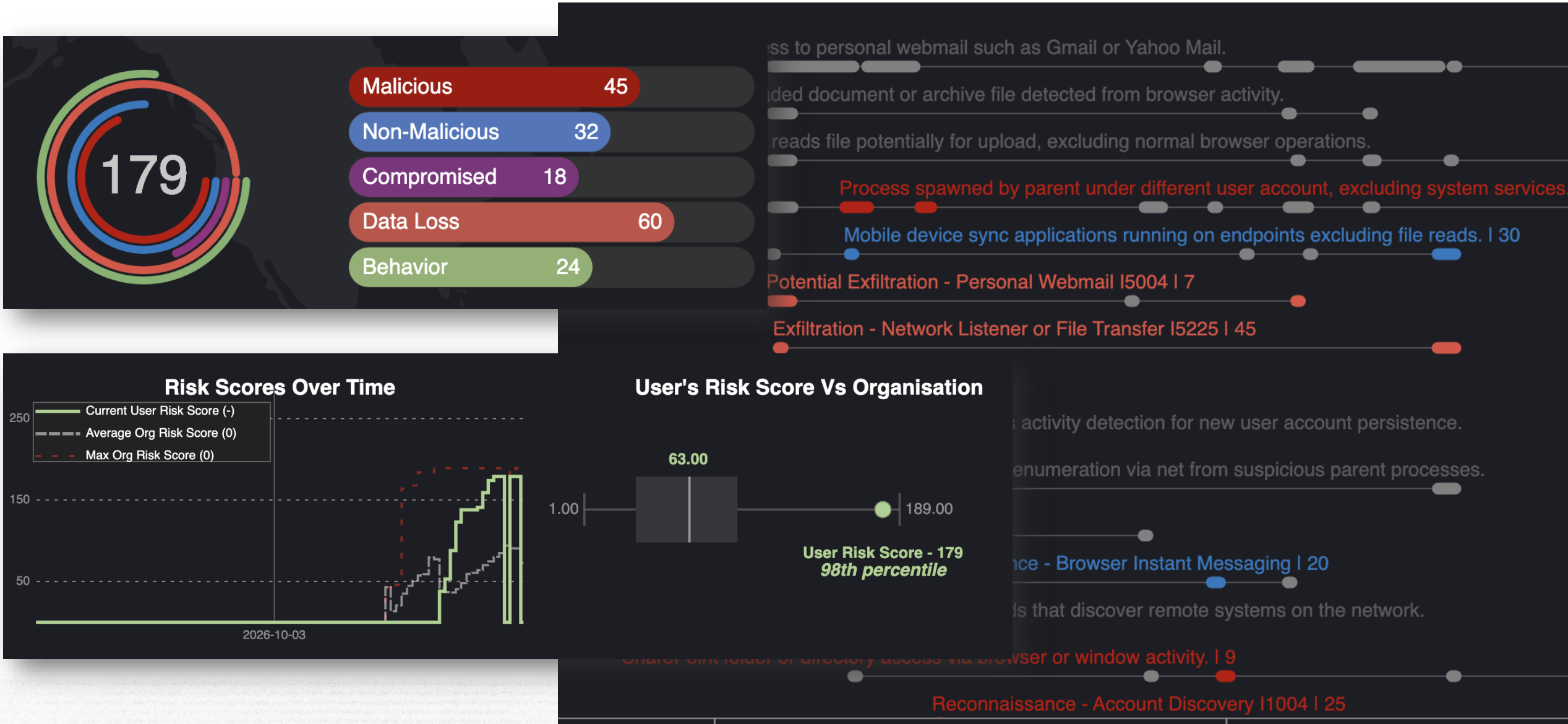
Triage/Validation

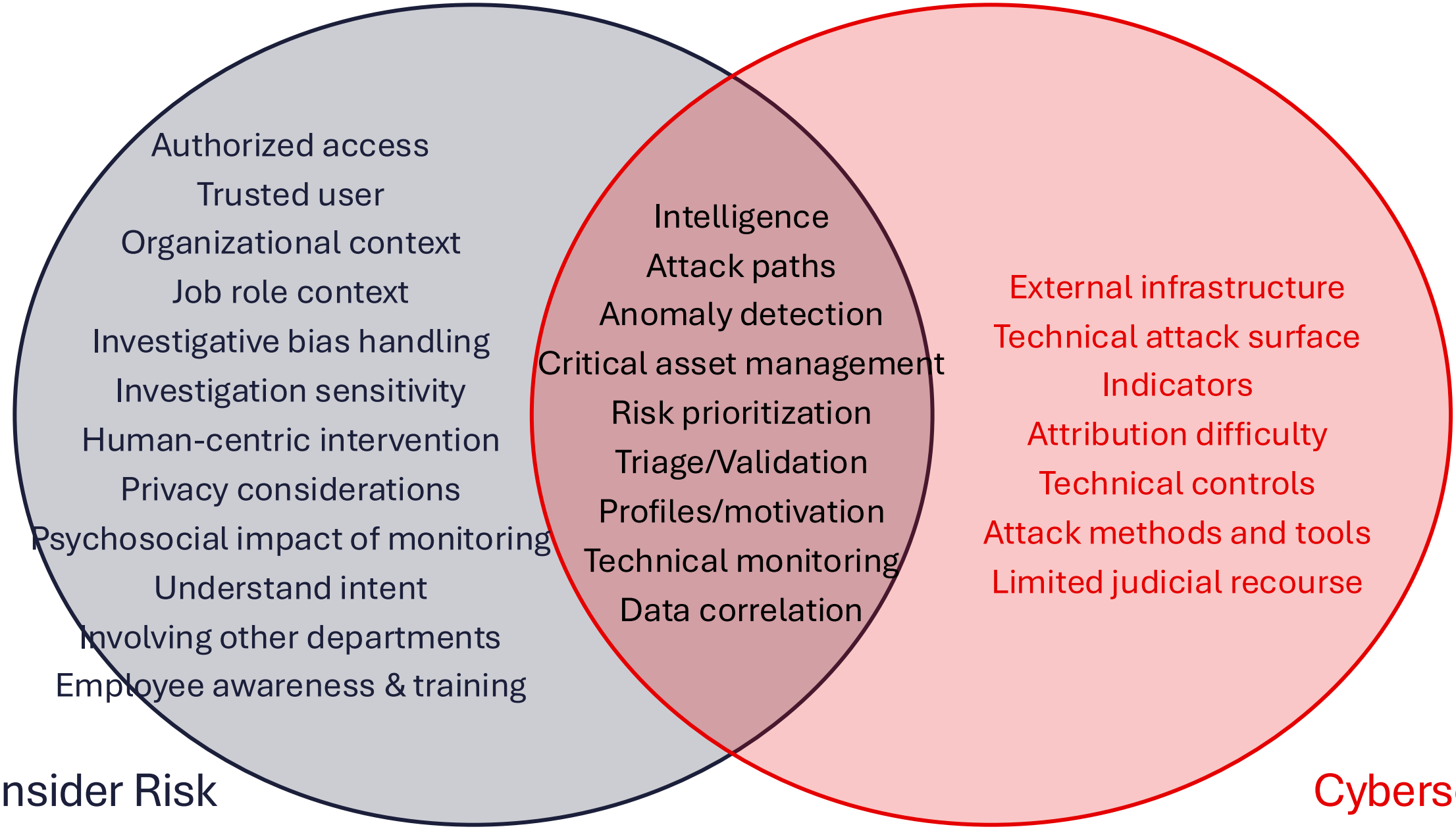
Profiles/motivation

Technical monitoring

Data correlation

DTEX Risk and Context




Authorized access
Trusted user
Organizational context
Job role context
Investigative bias handling
Investigation sensitivity
Human-centric intervention
Privacy considerations
Psychosocial impact of monitoring
Understand intent
Involving other departments
Employee awareness & training
Intelligence
Attack paths
Anomaly detection
Critical asset management
Risk prioritization
Triage/Validation
Profiles/motivation
Technical monitoring
Data correlation
External infrastructure
Technical attack surface
Indicators
Attribution difficulty
Technical controls
Attack methods and tools
Limited judicial recourse
Insider Risk
Cybersecurity

Thank You!

austin.whisnant@dtex.ai