

SECURITY INTELLIGENCE

Jesus Martinez Del Rincon, Paul Miller, Ihсен Alouani, Niall McLaughlin, Vishal Sharma, Oluwafemi Olukoya



**QUEEN'S
UNIVERSITY
BELFAST**

Dr Jesus Martinez Del Rincon
SI Research Director
30 June 2023



Security Intelligence

- AI for Cybersecurity
- Cyber security for AI
- Autonomous Security
- Video Analytics for Cyber-physical security
- Security & Assurance for Finance, Insurance and RegTech

Existing Expertise

- **AI for cybersecurity**

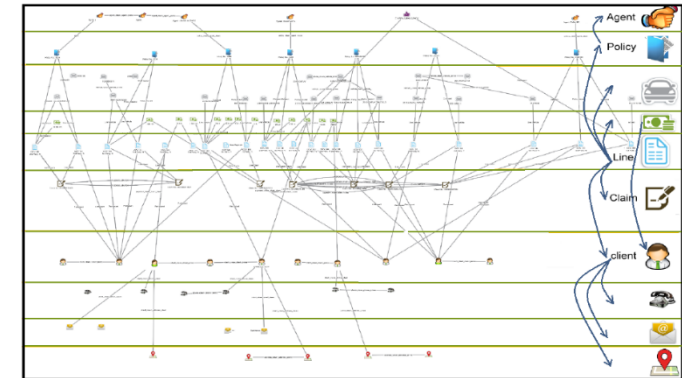
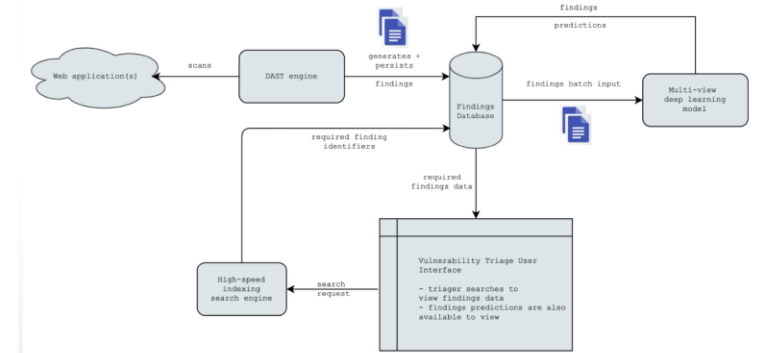
- Deep Learning for Malware Analysis and Software Vulnerability Detection [\[1\]](#) [\[2\]](#) [\[3\]](#)
- Data Analytics for Network Intrusion in Cyber-physical Systems [\[1\]](#) [\[2\]](#)
- Deep learning for Web application vulnerability analysis [\[1\]](#)
- Real time recognition of IoT attack patterns [\[1\]](#)[\[2\]](#)

- **Video analytics for cyber-physical security**

- Wide Area Tracking and Reidentification [\[1\]](#)[\[2\]](#)[\[3\]](#)
- Face Recognition and Access Control [\[1\]](#)
- Multimodal Vehicle Monitoring [\[1\]](#)[\[2\]](#)[\[3\]](#)
- 3D Pose Estimation and Activity Recognition [\[1\]](#)[\[2\]](#)
- Evidential Reasoning for Semantic Event Recognition and Decision Making [\[1\]](#)

- **Security and assurance for finance**

- Trader fraud detection
- Insurance analytics [\[1\]](#)
- Insider threat detection
- Heterogeneous graph mining



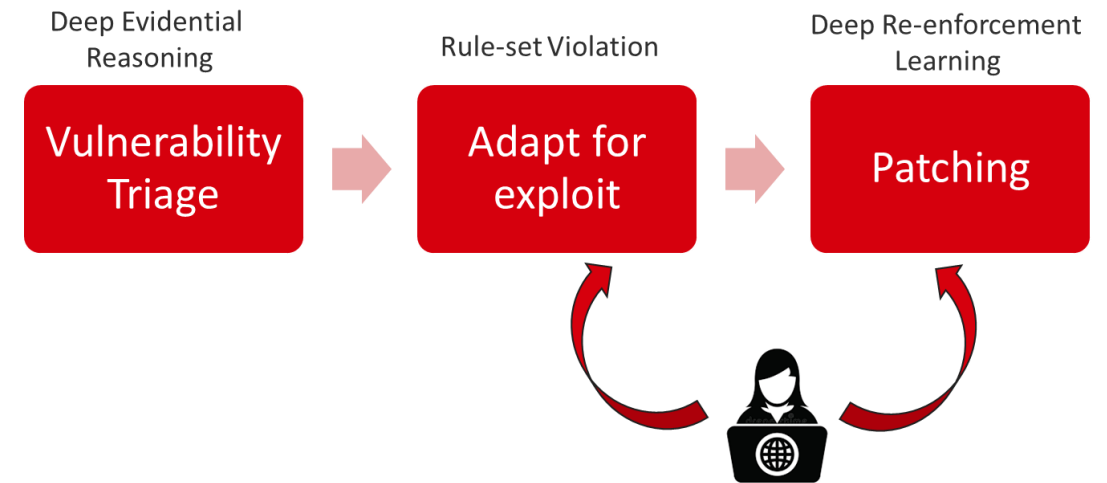
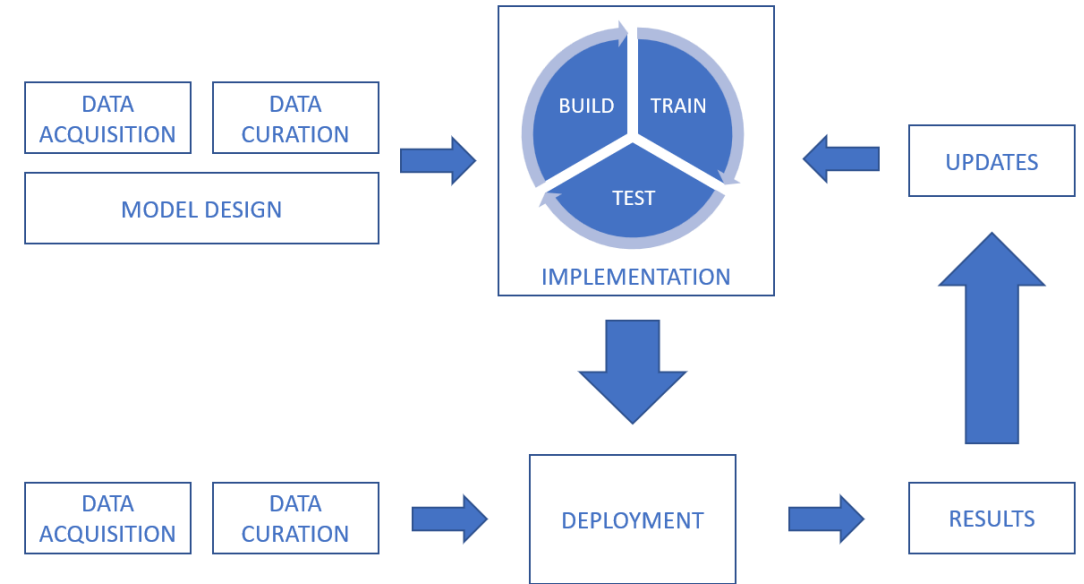
Emerging Research Areas

- **Security of AI**

- Design of adversarial attacks [\[1\]](#)
- Adversarial training [\[1\]](#) [\[2\]](#)
- Explainable AI for cybersecurity [\[1\]](#)
- Privacy Preserving Machine Learning [\[1\]](#)[\[2\]](#)
- Federated learning [\[1\]](#)
- Least privilege learning [\[1\]](#)
- Denial of features
- Securing the AI technology stack
- Trustworthy AI

- **Autonomous security**

- Learn to detect attacks
- Reason about alerts to extract semantic meaning
- Adapt to changing environment caused by attack
- Plan response and recovery



Industry Collaborators

BAE SYSTEMS

ebay

citi


Allstate®

RAPID7

 **Liberty**TM
Information
Technology

THALES

**Johnson
Controls** 

B Secur


 **National Cyber
Security Centre**


SEAGATE

salunda

 **GCHQ**

[dstl]
The Science Inside

Physical Security

Evidential Reasoning for Semantic Event Recognition and Decision Making [\[1\]](#)

Wide Area Tracking and Reidentification [\[1\]](#)[\[2\]](#)[\[3\]](#)

Multimodal Vehicle Monitoring [\[1\]](#)[\[2\]](#)[\[3\]](#)

3D Pose Estimation and Activity Recognition [\[1\]](#)[\[2\]](#)

Face Recognition and Access Control [\[1\]](#)

Fraud and Anomaly detection based on Graph Mining and Deep learning for Financial and Insurance Applications [\[1\]](#)

