AI in Cyber

HNC-CY Days 2023

AUGUST 23, 2023

Clarence Worrell
Senior Data Scientist

Carnegie Mellon University
Software Engineering Institute

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM23-0880

CERT Data Science (CDS)

General Research Areas

Carnegie Mellon University Software Engineering Institute

AI for cybersecurity

- Networks (NetFlow, attestation & trust, etc.)
- Threat hunting (traditional and advanced persistent)
- Combatting disinformation (videos, images, text)

Cybersecurity for AI

- Data security (theft, poisoning)
- Model security (theft, extraction, inversion)

Quantum Computing

- Cybersecurity for quantum
- Quantum for cybersecurity

Applied Data Science for Cybersecurity Professional Certificate Program

- Fundamentals of Statistics
- Advanced Analytics: NetFlow
- Advanced Analytics: Malware
- Advanced Analytics: Digital Forensics
- Certificate Examination

Enrollment is easy:
https://www.sei.cmu.edu/education-outreach/

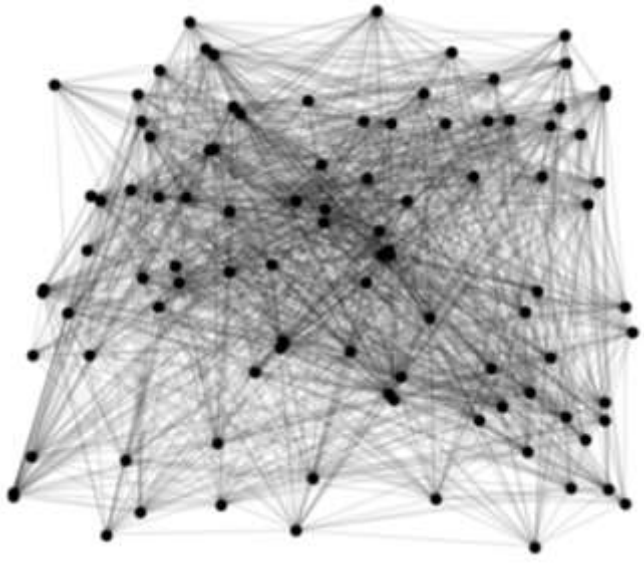
Webcast for more info:
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=976665

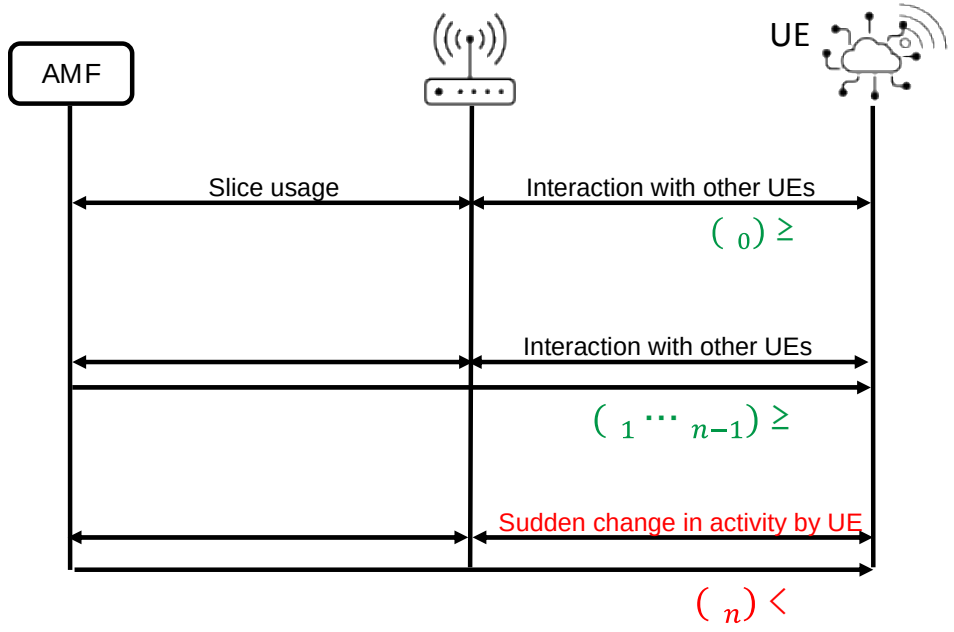
AI in Cyber: HNC-CY Days 2023

Recent CERT Data Science Research Examples

Carnegie Mellon University
Software Engineering Institute

Trust modeling in next generation networks

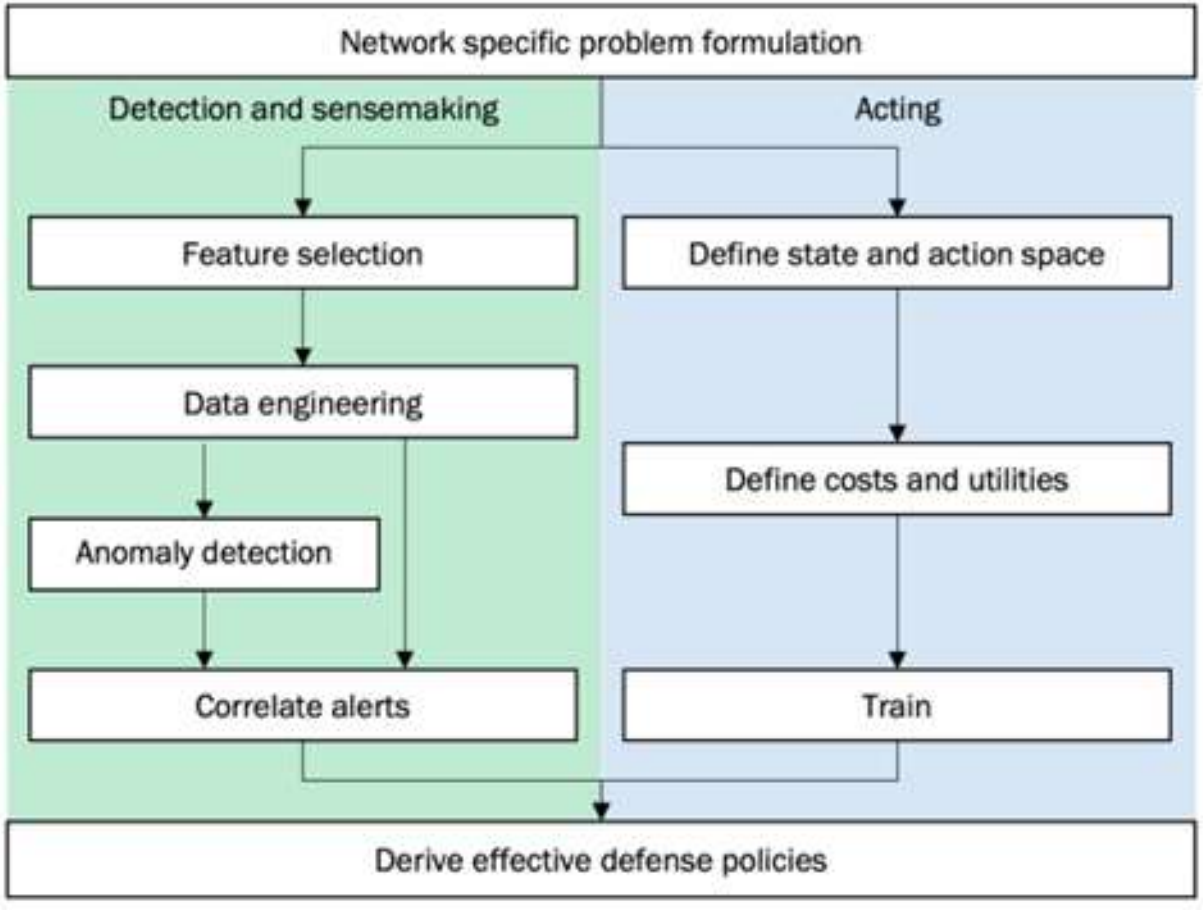




Can we assert how much each device should trust its neighbors?

Our method is risk-informed, reliable, and scalable

Advanced Persistent Threat Detection



Current state of research

- Anomaly detection
- Correlating low-level events
- Designing defenses by gamification

Can AI/ML improve upon, or complement, existing APT detection methods?

Threat Detection across Multiple Networks

- **CyberSentry**
  - CISA-managed threat detection and monitoring
  - U.S. critical infrastructure
  - Risk-informed
- **SEI**
  - Cloud visibility & threat analytics

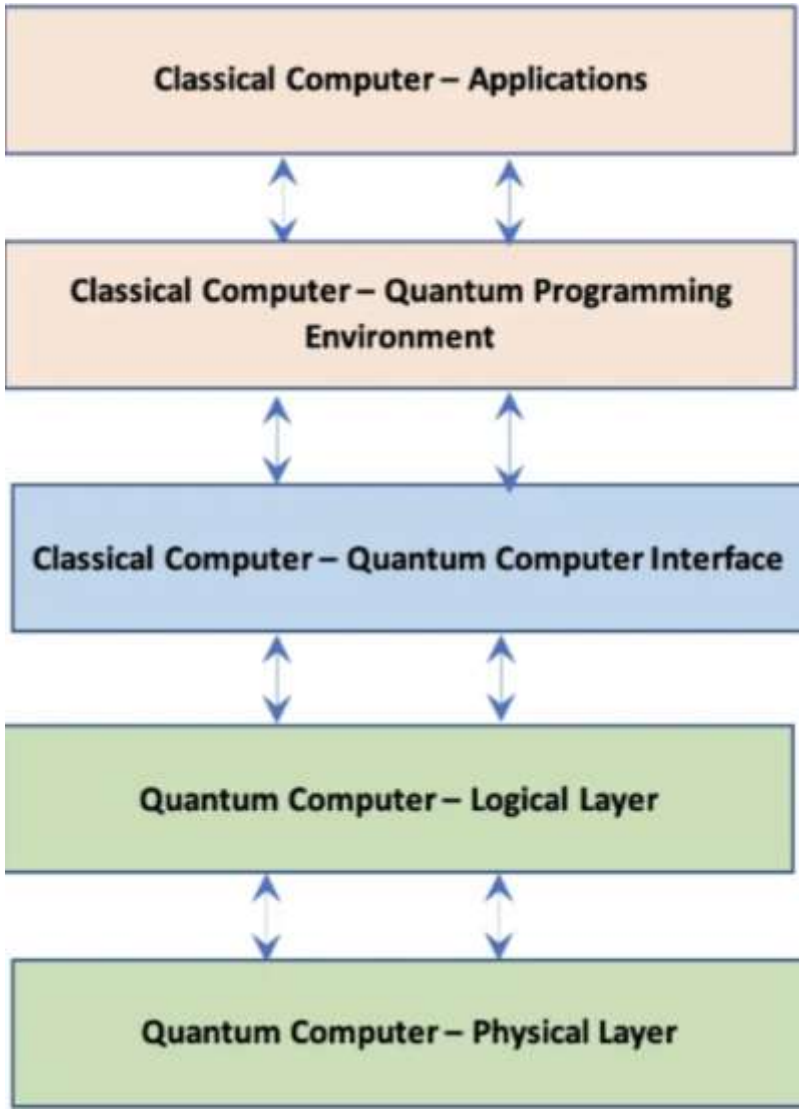
Can AI/ML methods improve threat detection when monitoring across multiple networks, vs. monitoring networks individually?

Quantum Cybersecurity

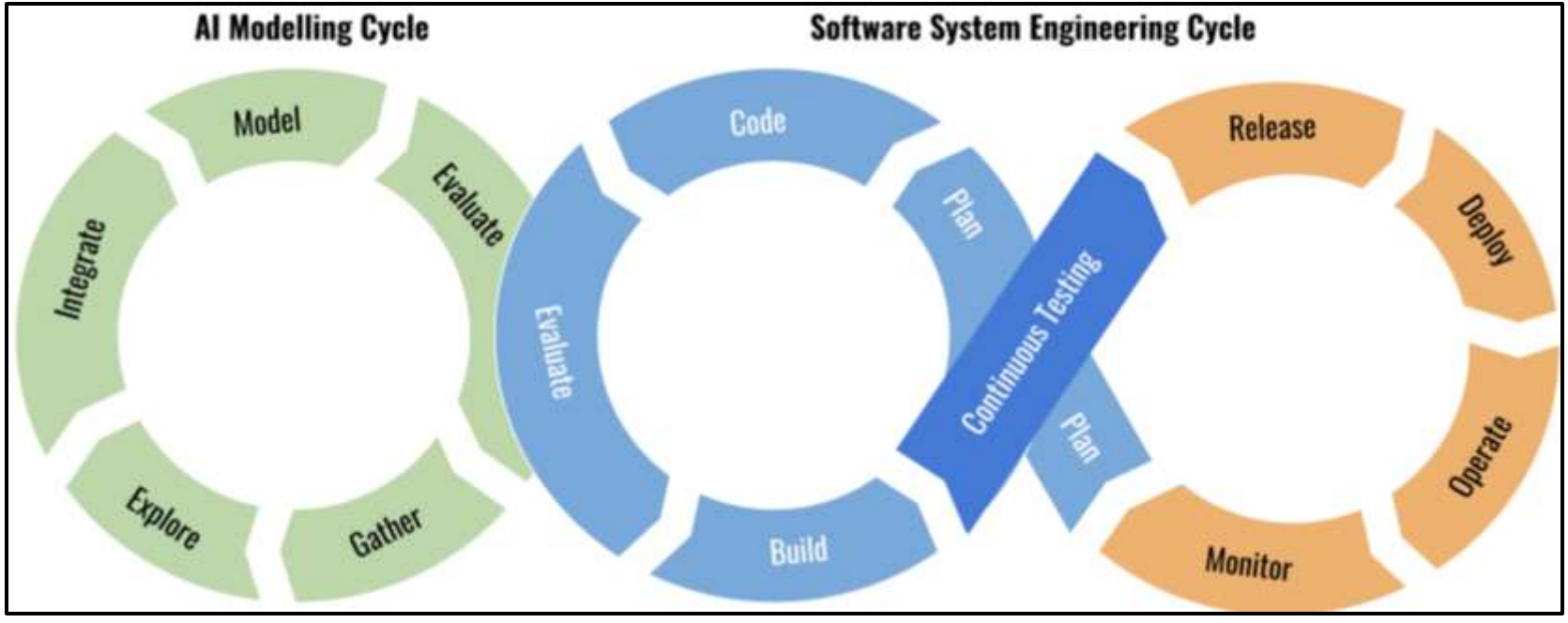
Research needs

- Secure large-scale control systems
- Distributed HP quantum computing
- Quantum computer attack vectors
- Methods for safe quantum systems
- Multi-layered instrumentation framework
- Tools to verify quantum algorithms

How can all this be done securely?



Secure, agile MLOps systems



How can we ensure effective, efficient, and secure ML-enabled software?

We present best-practices and a reference architecture that combines DevSecOps and Agile

Forensic analysis of digital media

This image cannot currently be displayed.

Generative AI allows people to manipulate content at unprecedented speed and scale

We developed a toolbox of methods to detect digital forgeries and manipulation

AI in Cyber: HNC-CY Days 2023

Open brainstorming of how SEI CDS could support HNC-CY

Carnegie Mellon University
Software Engineering Institute

Contacts

Thomas Scanlon
Technical Manager

Telephone: +1 412.268.9209
Email: scanlon@sei.cmu.edu

Matt Walsh
Senior Data Scientist

Telephone: +1 412.268.9121
Email: mmwalsh@sei.cmu.edu

Clarence Worrell
Senior Data Scientist

Telephone: +1 412.268.9059
Email: cworrell@sei.cmu.edu