INL/CON-21-64781-Revision-0

CCE and Resilience Strategies

October 2021

Samuel Douglas Chanoski

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-21-64781-Revision-0

CCE and Resilience Strategies

Samuel Douglas Chanoski

October 2021

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Southeast Tri-Regional
2021 Joint Engineer
Training Symposium

Sam Chanoski
Technical Relationship
Manager, INL

CCE and Resilience Strategies

U.S. Department of Energy | Idaho National Lab | National & Homeland Security

Idaho National Laboratory

The Realities of Cyberspace

INL's technical doctrine is based on the following assumptions:

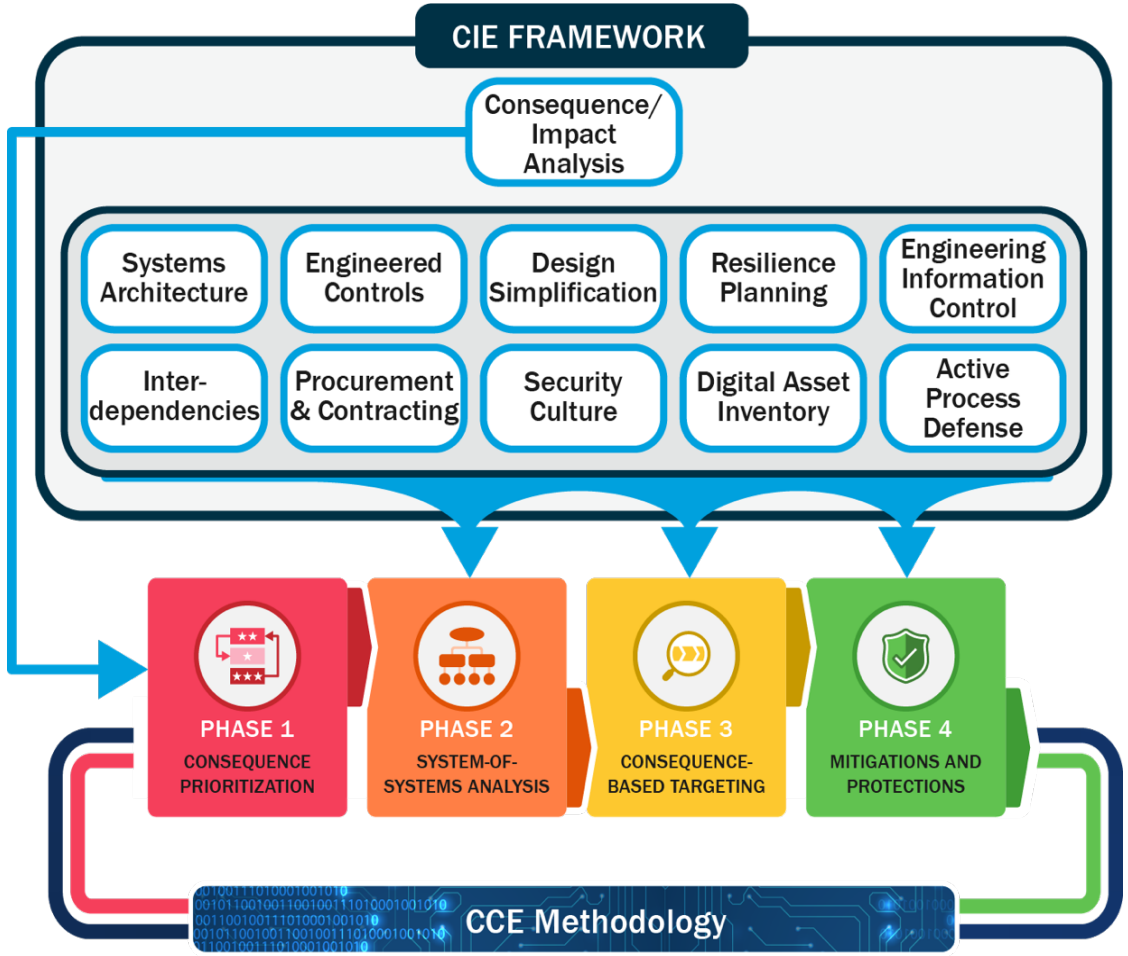
- **Existing security efforts are insufficient** to protect control systems and the infrastructure they support against catastrophic technical attacks.
- **A determined, well-resourced and patient adversary *WILL* succeed** in penetrating and exploiting a critical infrastructure network**.**

Given time and resources, cyber attackers* WILL *have success

CCE vs CIE

- **Cyber-Informed Engineering (CIE)** framework that drives the inclusion of cybersecurity as a principal element of risk management.

- **Consequence-driven Cyber-informed Engineering (CCE)** implements CIE concepts through a thorough process of identifying and mitigating potential catastrophic effects of cyber-enabled sabotage.



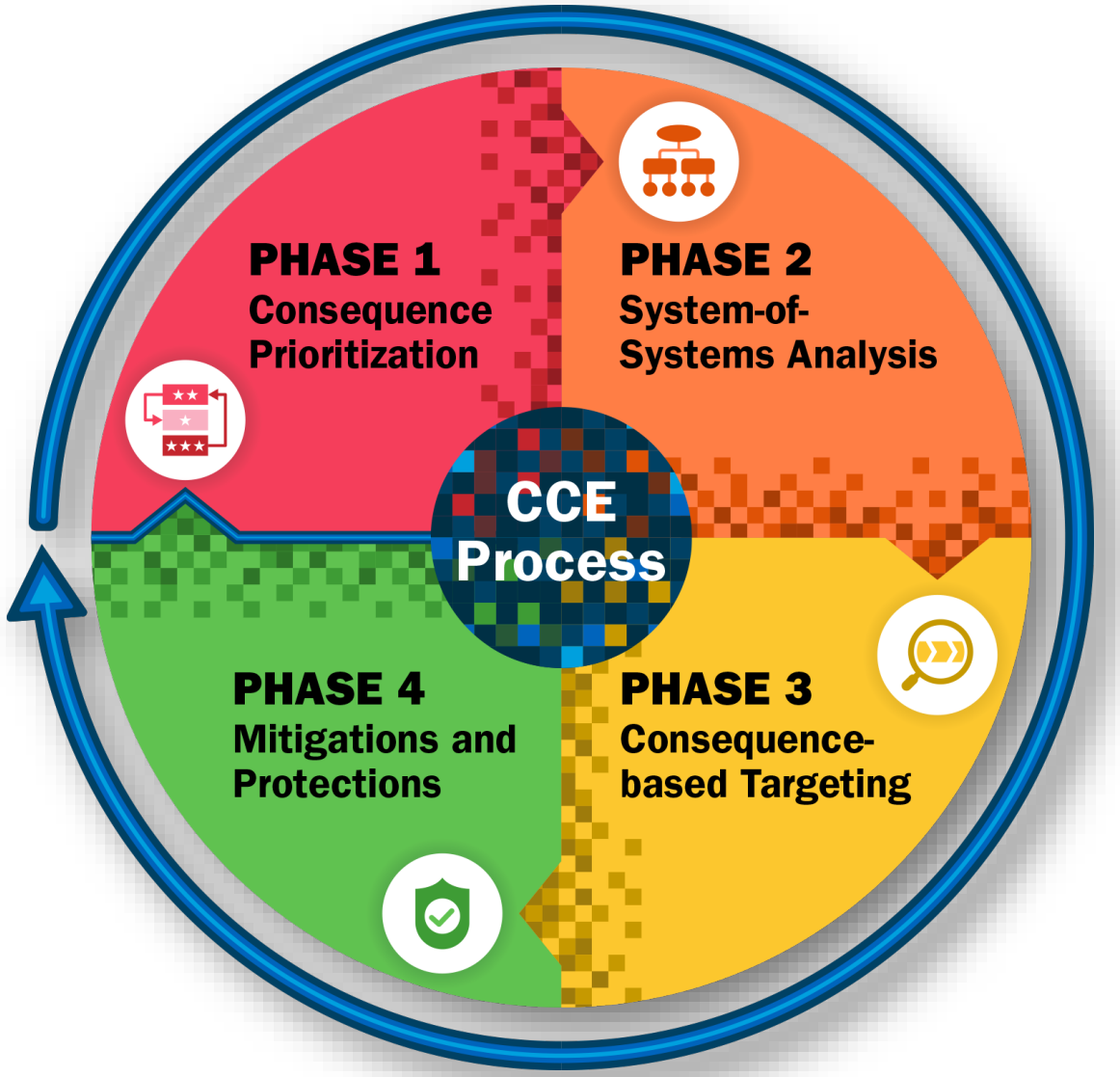
Critical Functions

Not Just OT or IT

Colonial Pipeline

Maersk

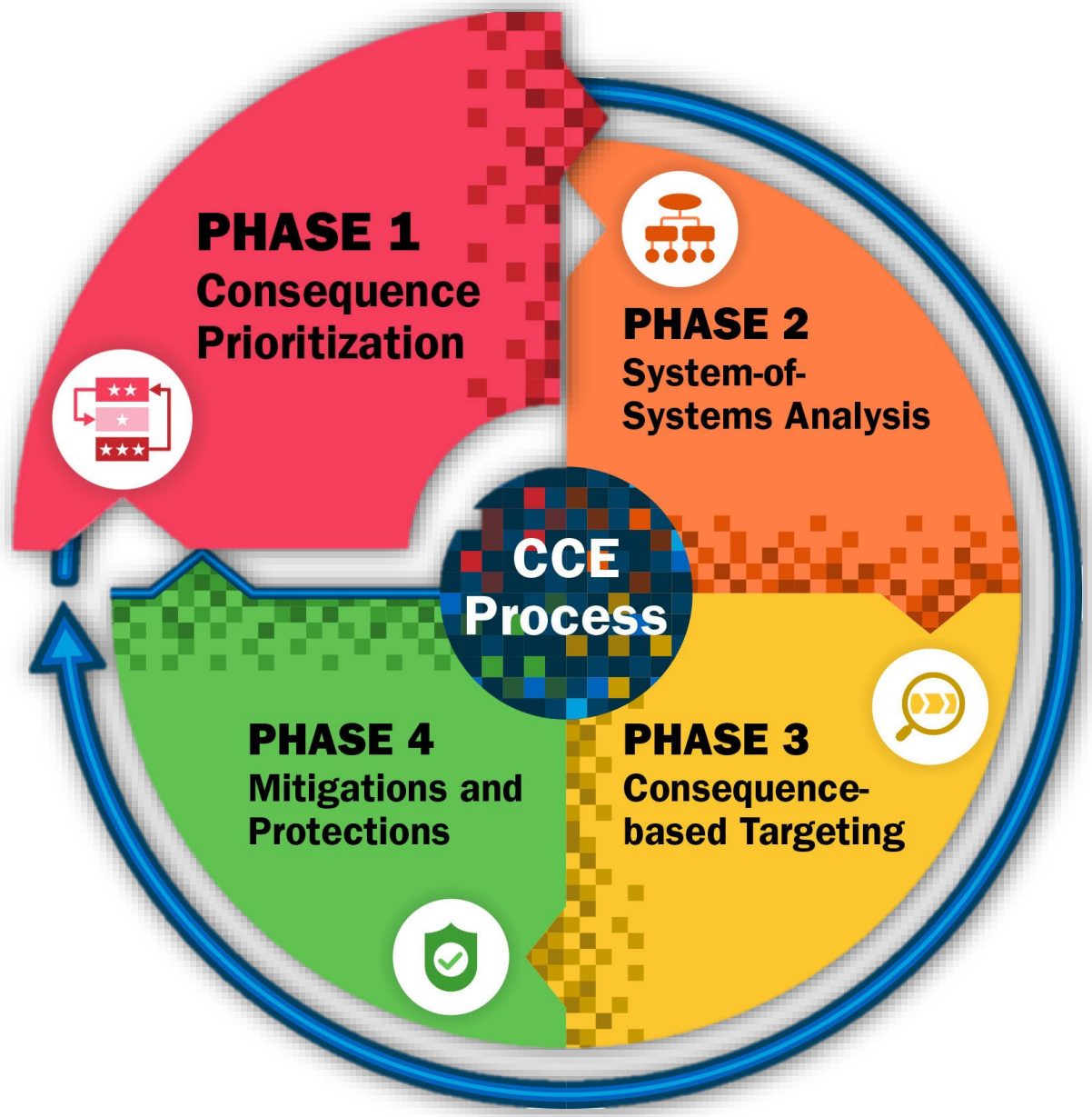
Consequence-driven Cyber-informed Engineering



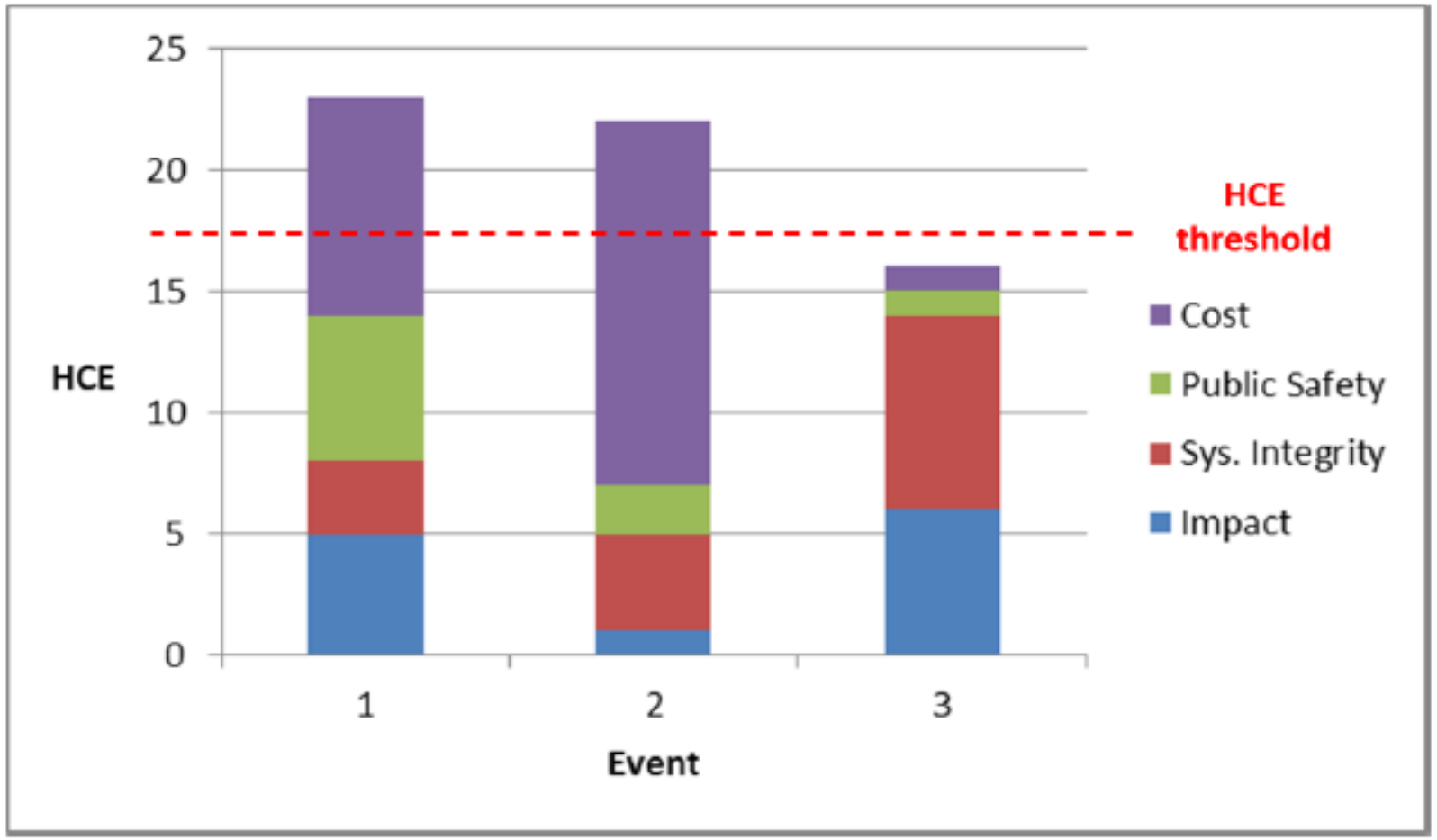
To change the way engineers, operators, & senior leaders understand & mitigate cyber risks for their most critical systems & processes

Phase 1

Identify High Consequence Events (HCEs) that could significantly inhibit an organization's ability to provide services or successfully execute processes considered essential to the business mission.

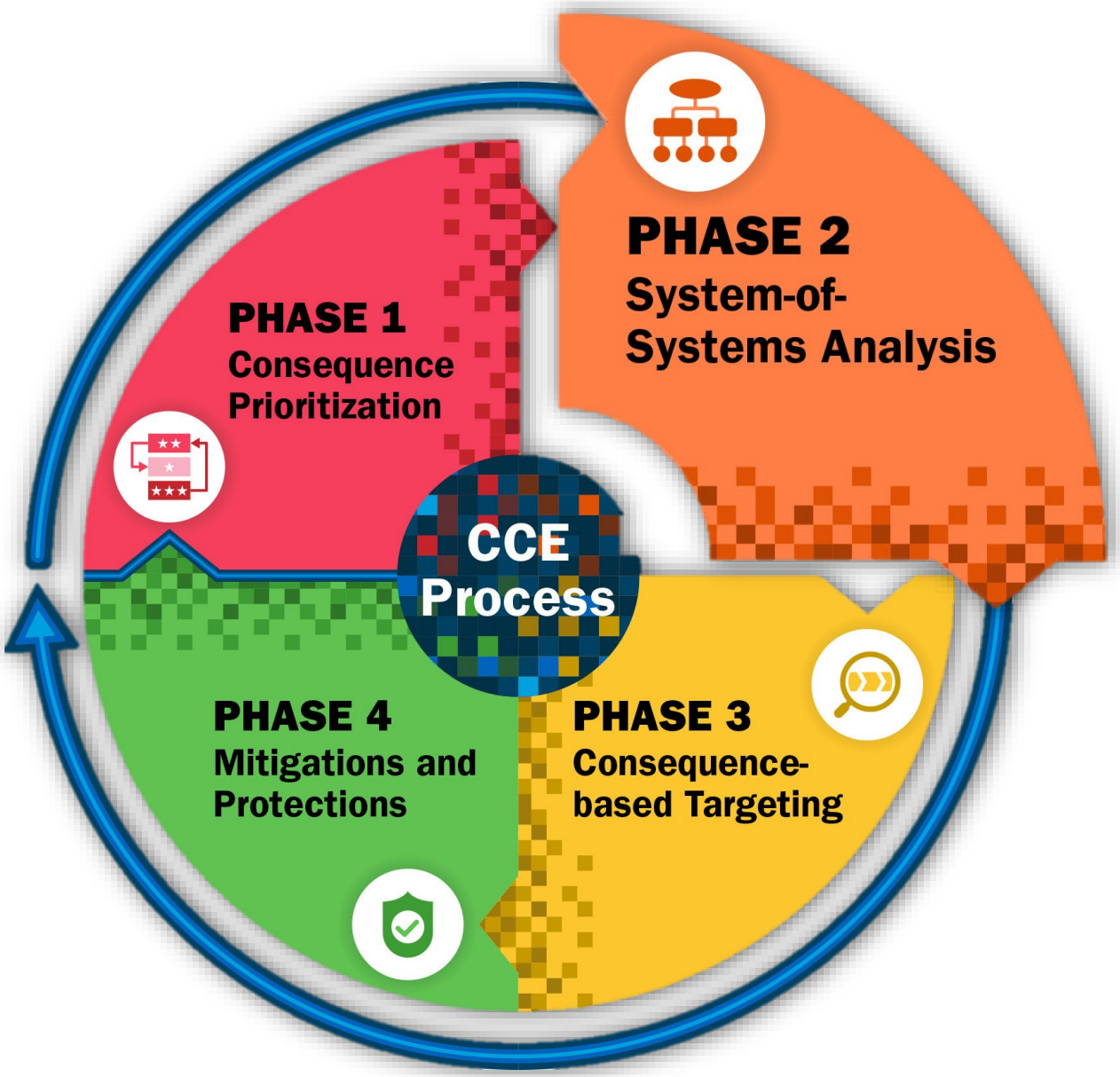


High Consequence Event Thresholds

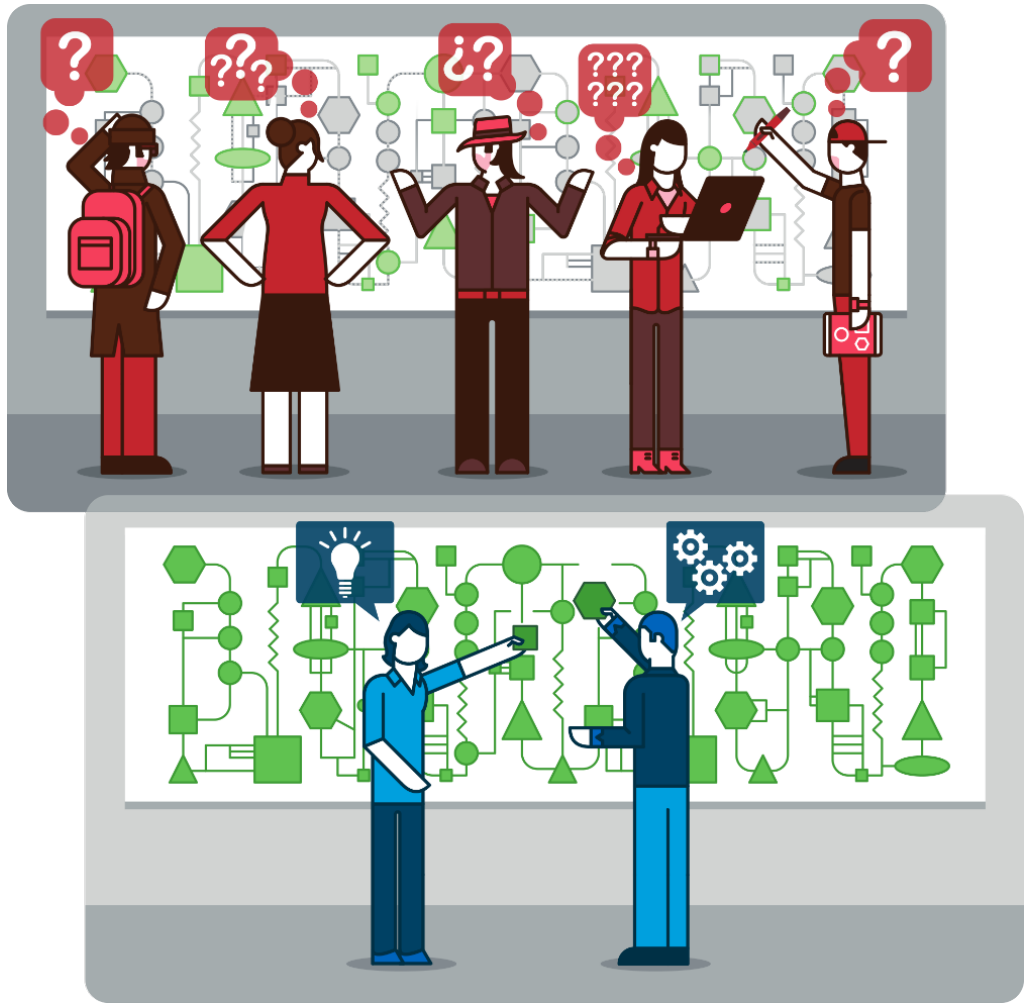


Phase 2

Primarily a data collect effort, the phase focuses on gathering the system and organizational information necessary to build out the HCEs.



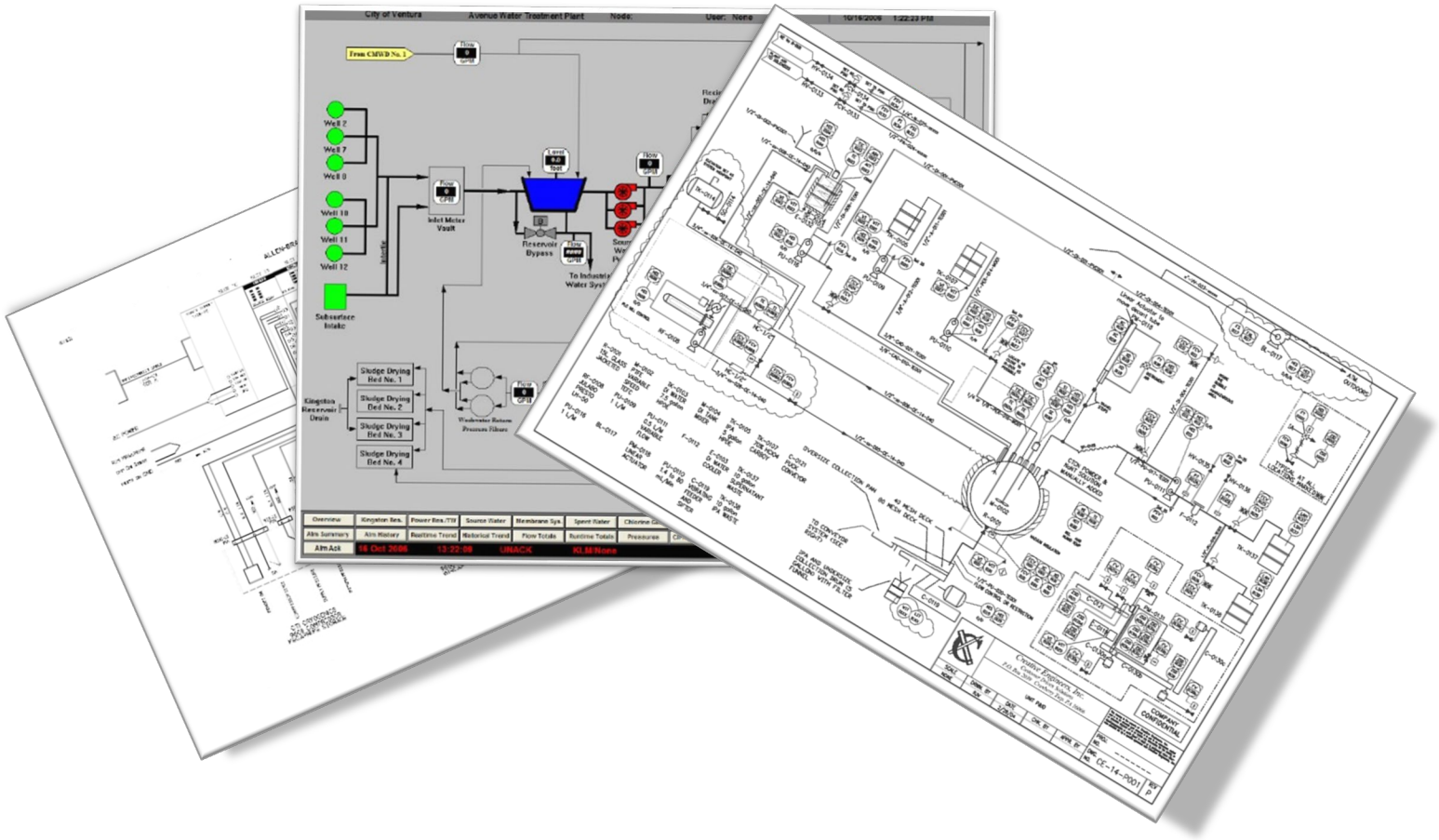
Perfect Knowledge



The adversary will always know at least as much as you do about your technology —maybe even more.

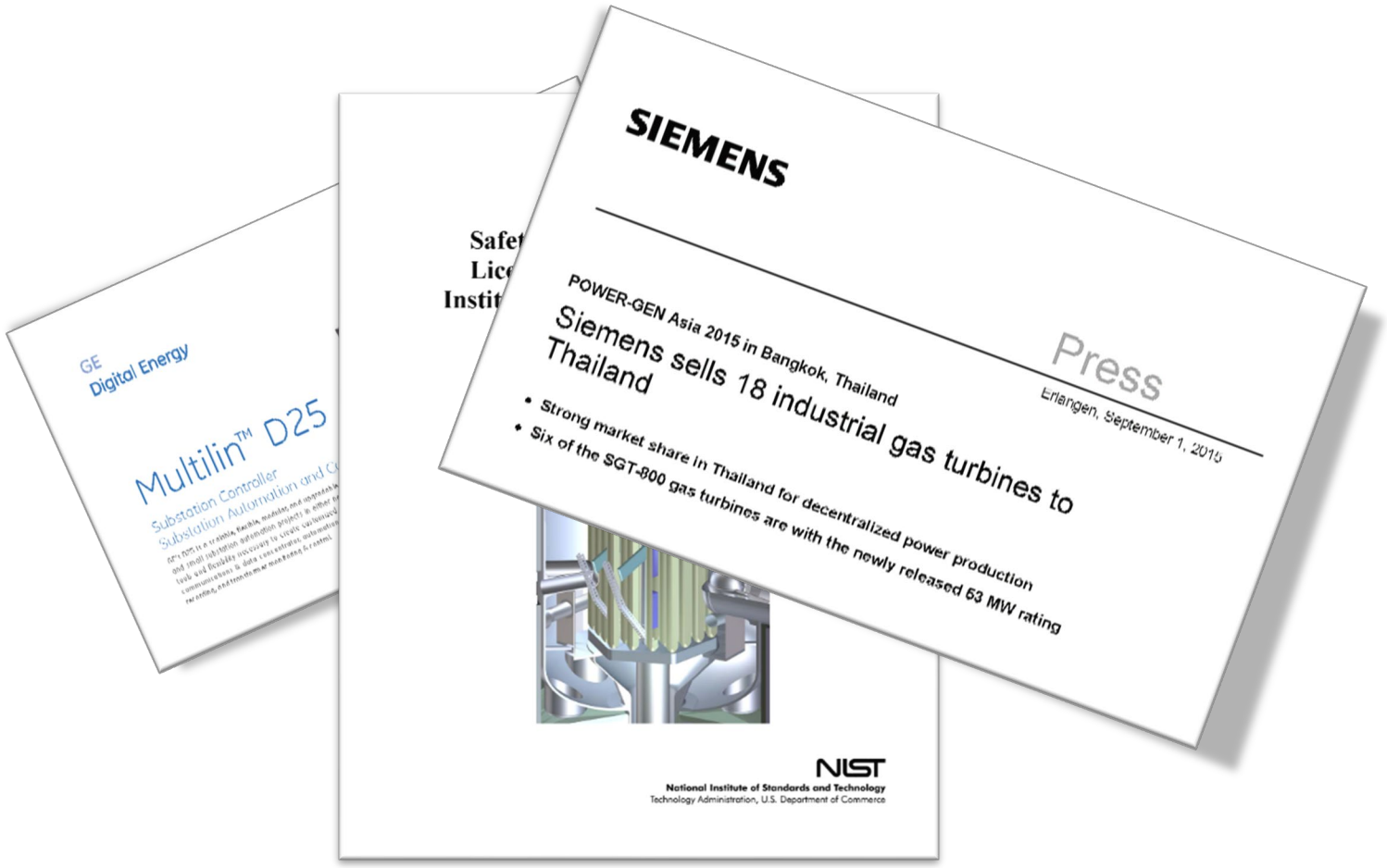
But they won't always know how you deploy your technology.

Information Locations – Insider



- P&IDs
- HMI Programs
- PLC Programs
- Wiring Diagrams
- System Design Documents
- As-build Drawings
- Process Flow Diagrams
- Network Configuration Diagrams

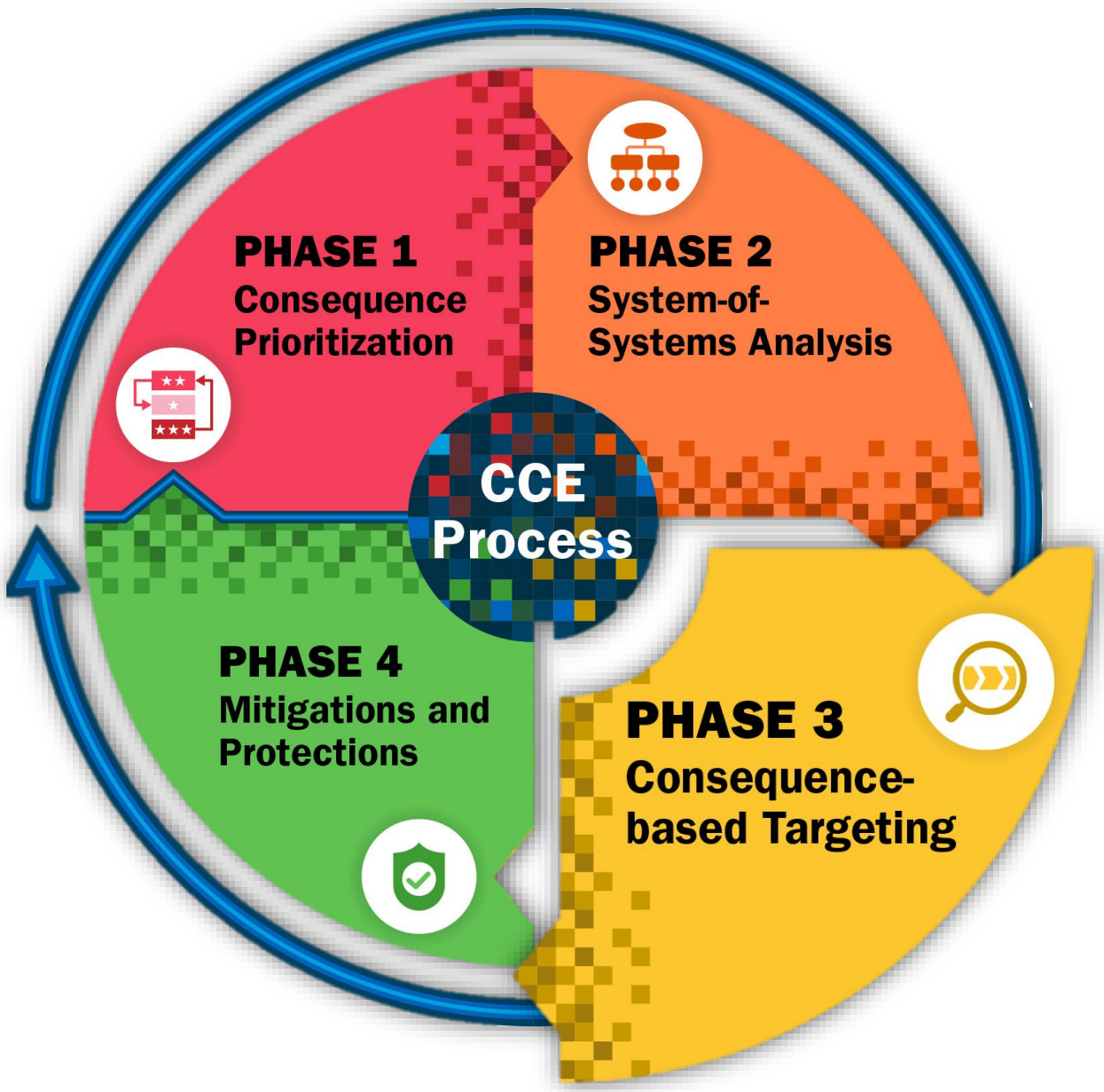
Information Locations – Outsider



- Vendor Website and Publications
- News Articles/Press Releases
- Public Bids
- Environmental/Safety Reports
- Other Regulatory Reports
- Vendor Maintenance Information

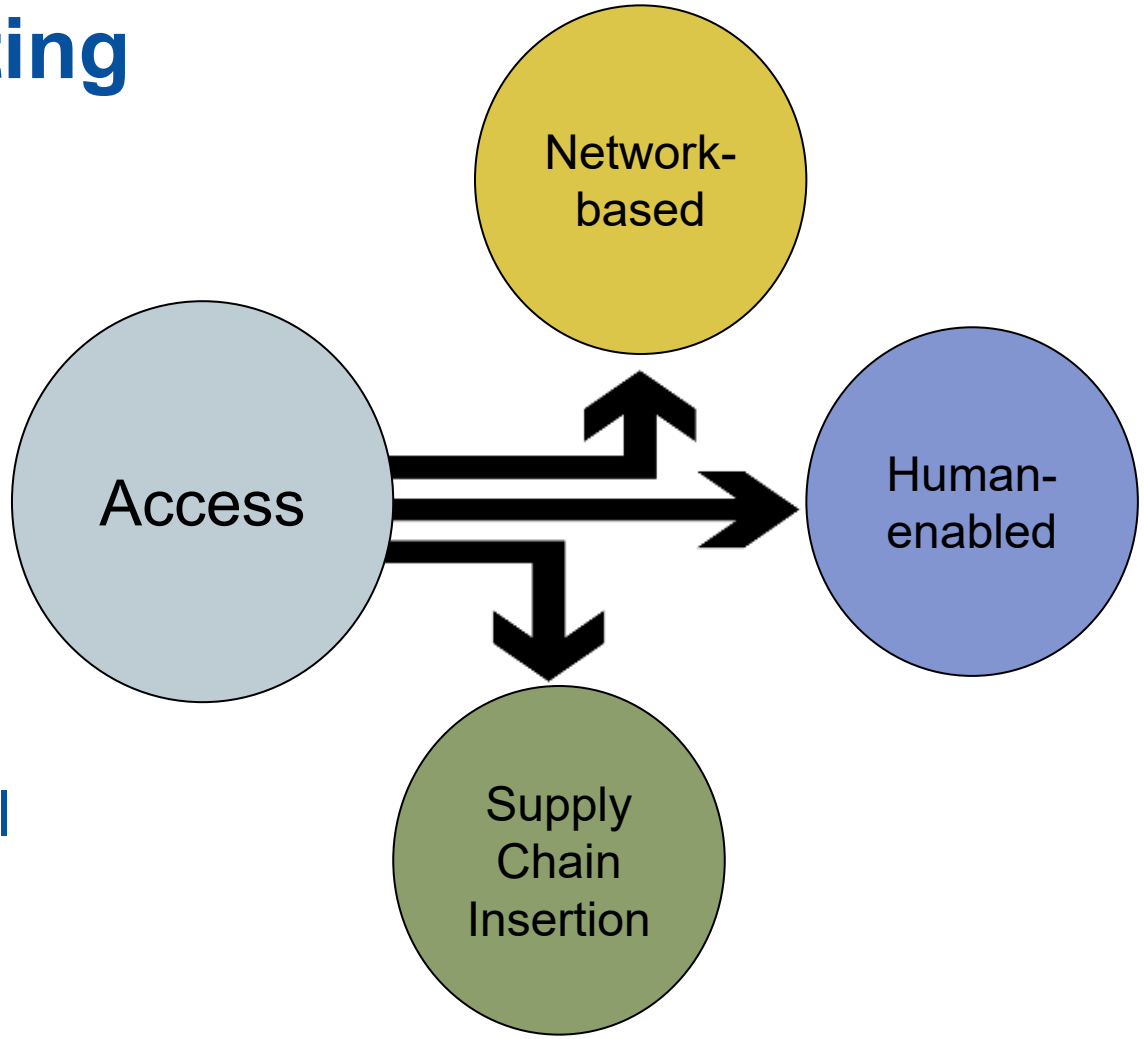
Phase 3

Use adversarial approach in reviewing the data from Phase 2 to identify unverified trust in people, process, and technology. This will highlight steps requested for an adversary to use to achieve HCE through cyber means.



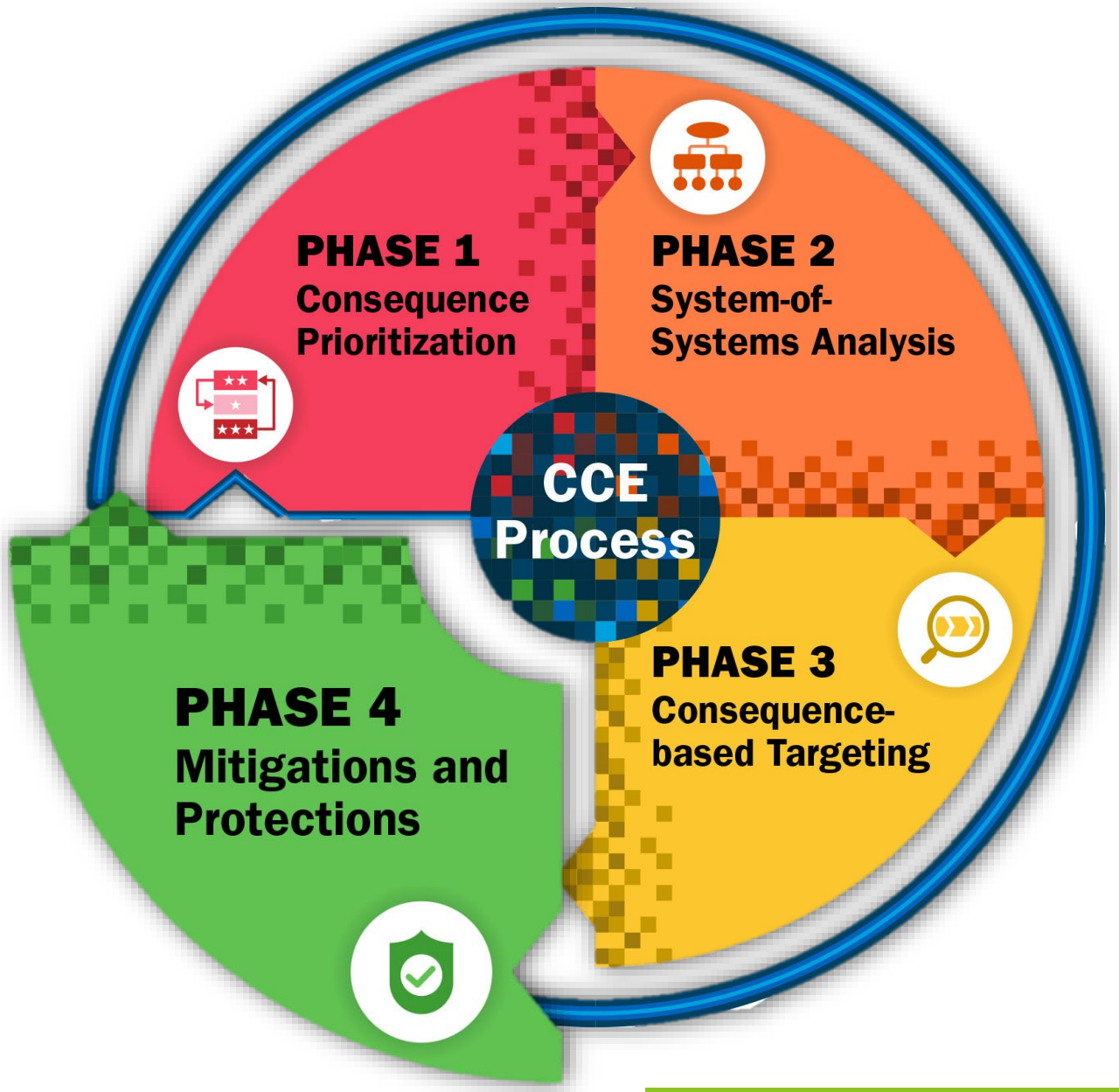
Success of Adversary Targeting

- Targeting expands beyond the traditional cyber realm (i.e., supply chain, human-enabled, etc.)
- The target is expansive
  - Multiple people have access
  - Multitude of potential targets for information or access
- Information required to target critical infrastructure already exists in the public domain
- Top shelf actors can undermine and circumvent security controls



Phase 4

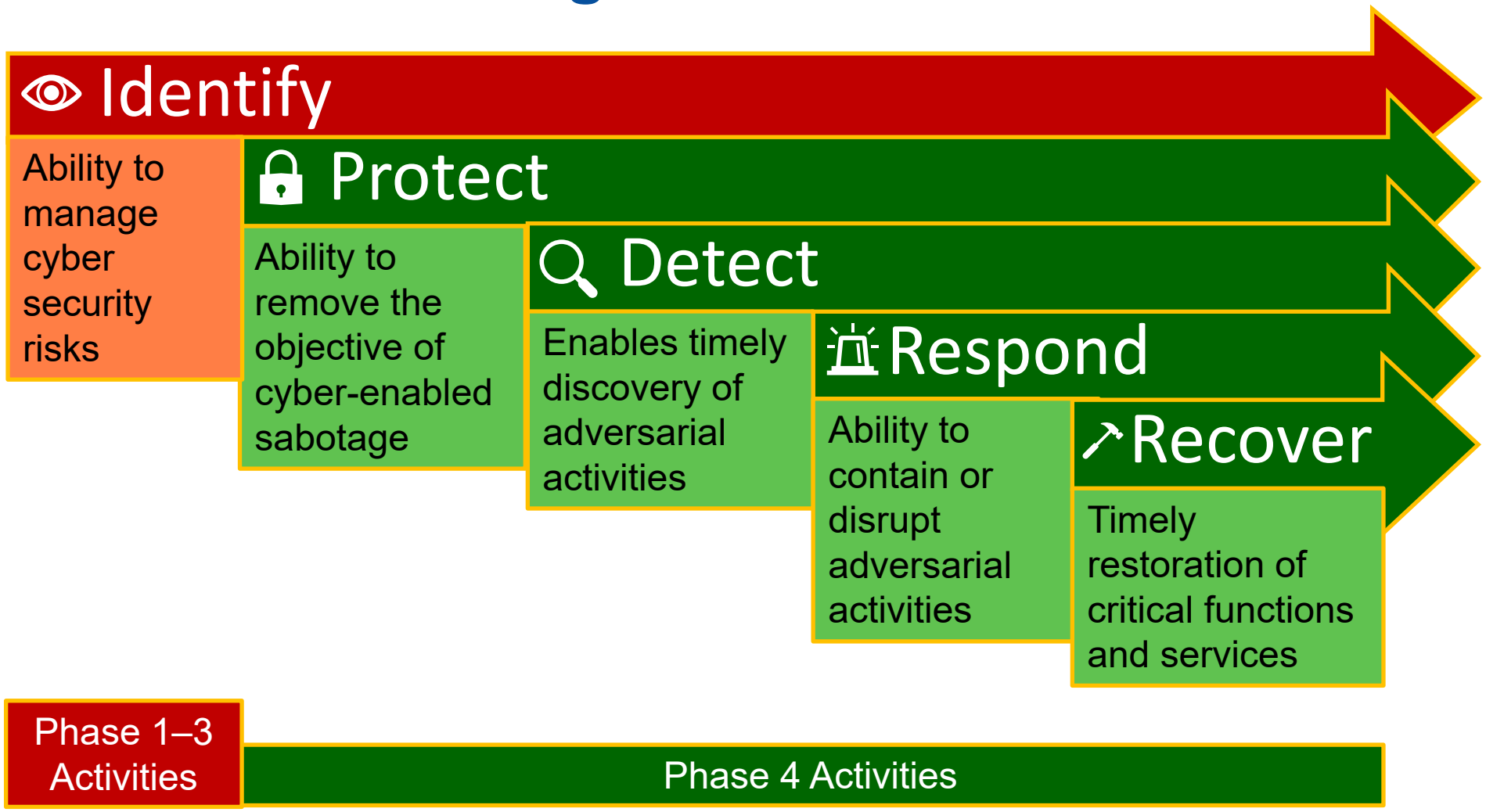
Covers the evaluation and selection of mitigations intended to limit the damage that may result from an HCE.



Protections

Cutting the tree at the trunk, instead of removing branches

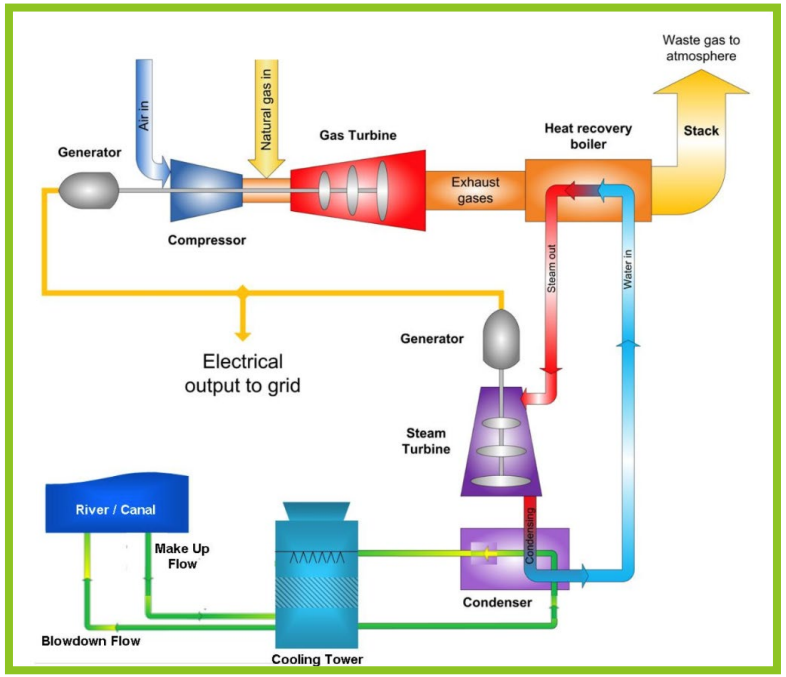
Protections and Mitigations

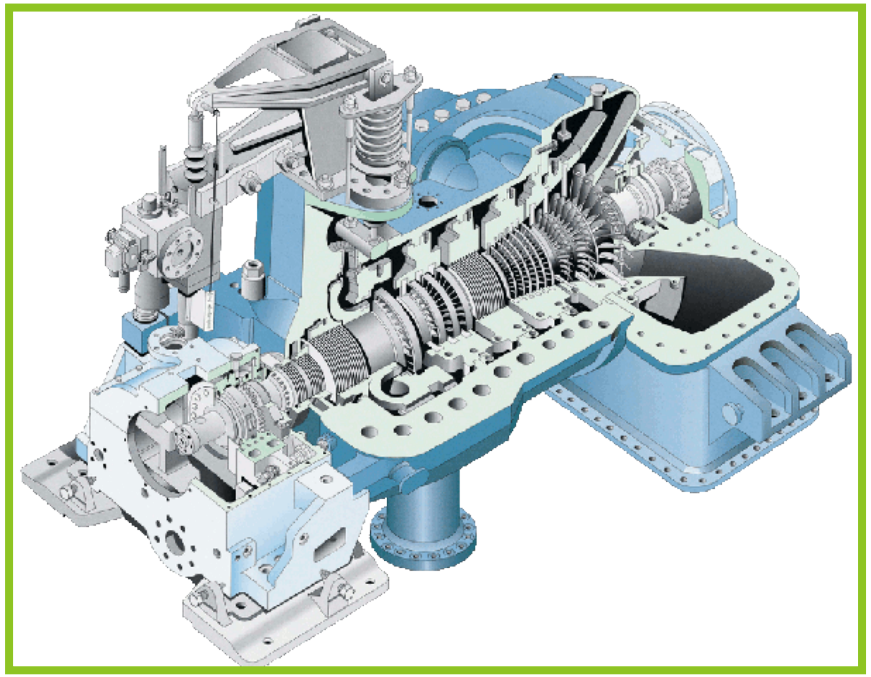


Engineering Out the Cyber Effect

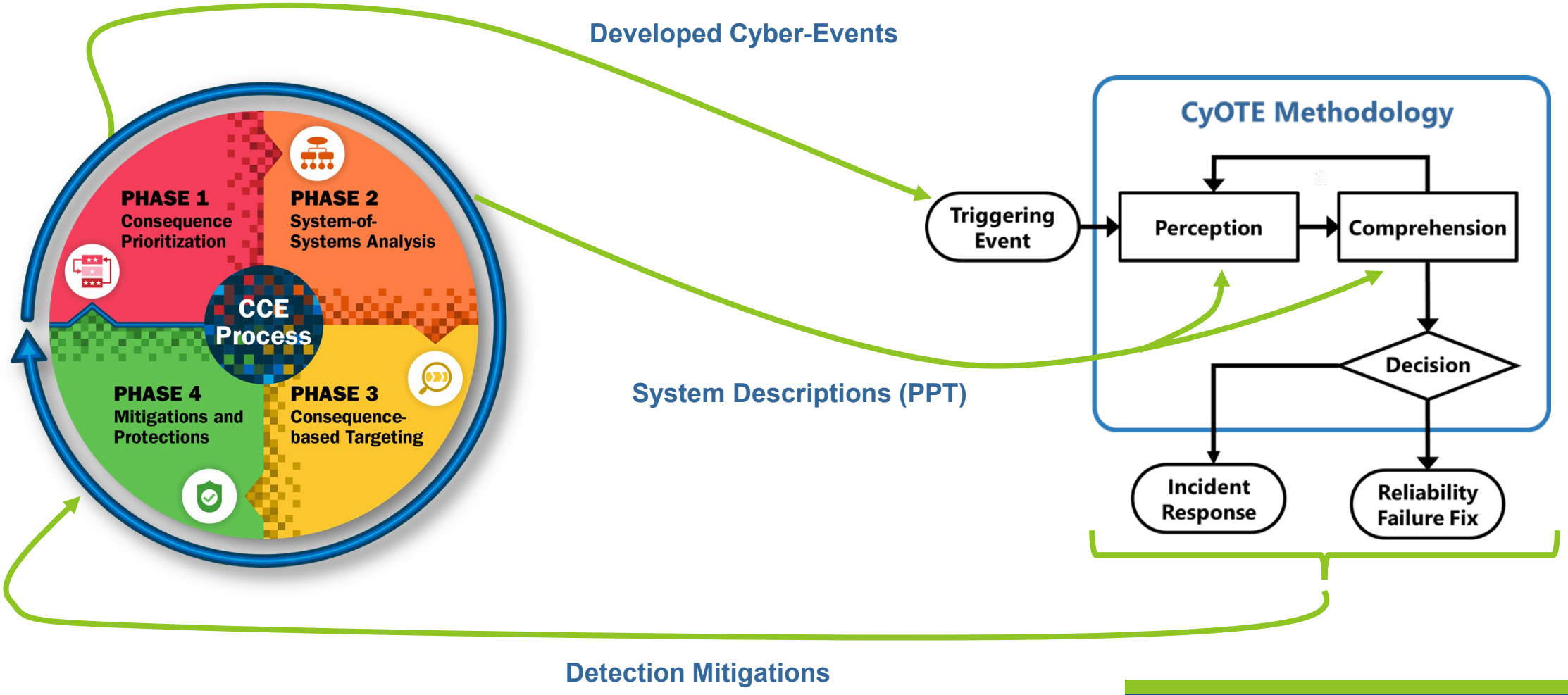
Taken from work during a 2017- 2018 pilot with a major U.S. utility

Employing the adversary perspective is comparable to "disarming the missile before it hits us."

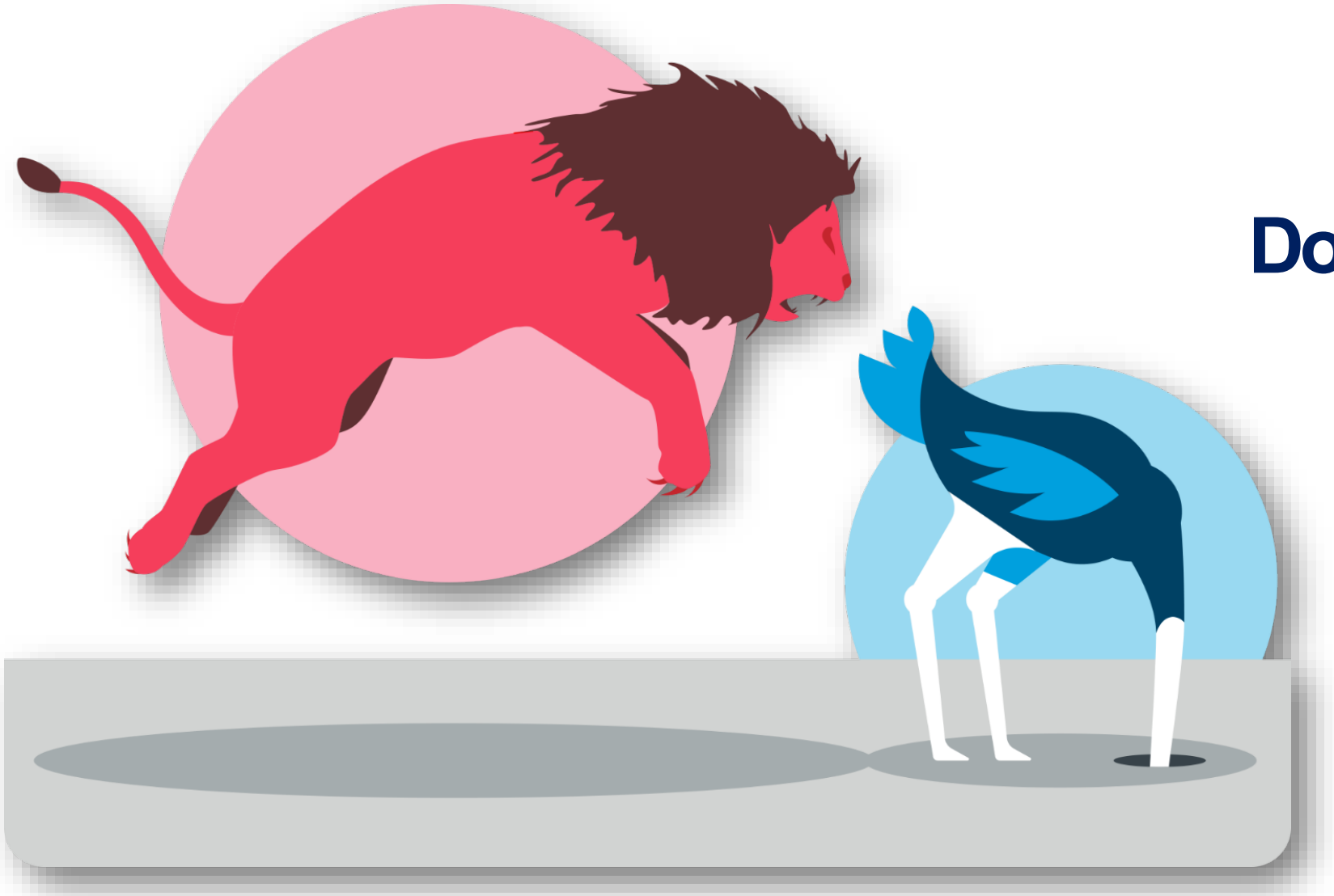




Designing Tripwires for Early Detection



Hiding the Problem . . .



Doesn't Solve It

Questions and Discussion

https://www.inl.gov/cce

2019 R&D 100 Award winner for cyber protection of critical infrastructure

Sam Chanoski

Technical Relationship Manager | Cybercore Integration Center

samuel.chanoski@inl.gov

Idaho National Laboratory | Atlanta, GA


INL
Idaho National Laboratory