Operational Cyber Risk Reduction

Dr. April Galyardt

Josh Hammerstein

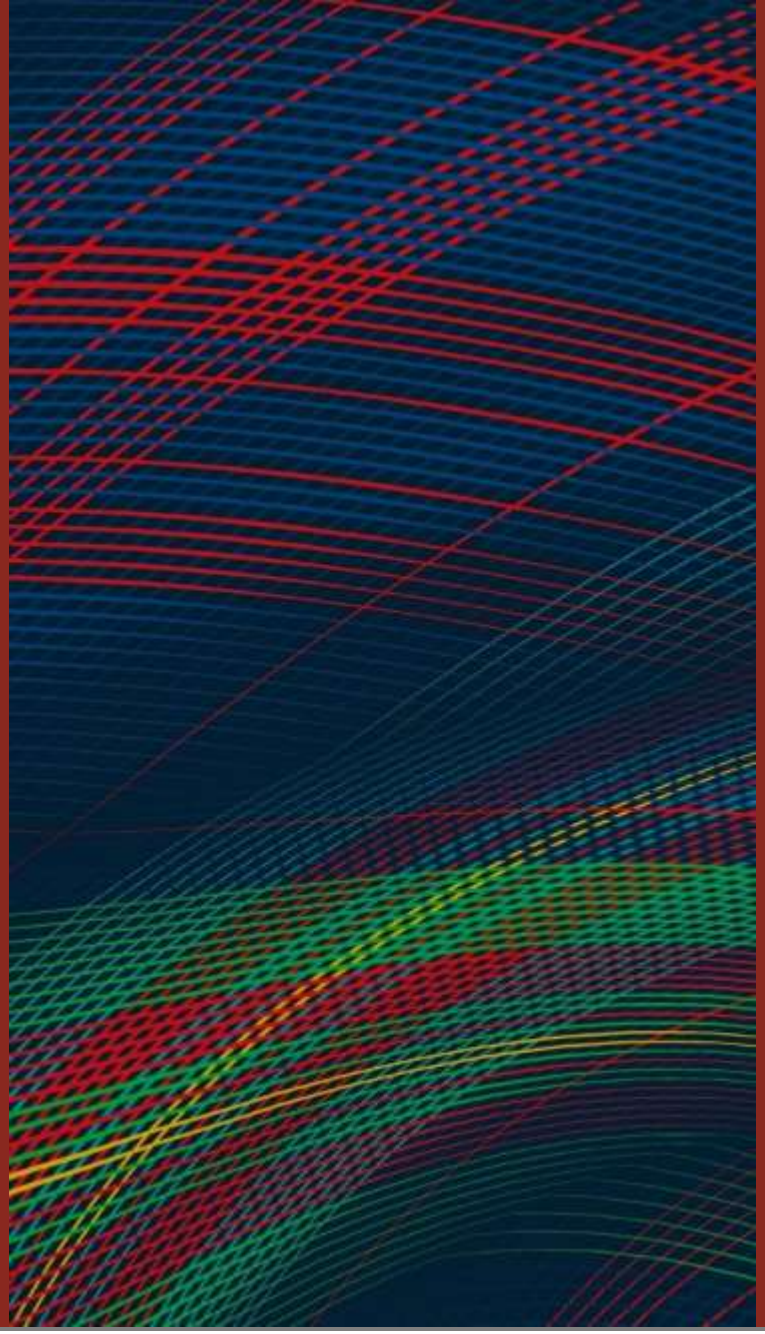
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

DM18-1195

Operational Cyber Risk Reduction

Introduction



Creating Operational Resilience

US Government and DoD can field and operate resilient systems that support the mission even when attacked by a capable adversary.

Enduring Software Challenges

Affordable
Be Affordable such that the cost of acquisition and operations, despite increased capability, is reduced and predictable

Capable
Bring Capabilities that make new missions possible or improve the likelihood of success of existing ones

Trustworthy
Be Trustworthy in construction, correct in implementation, and resilient in the face of operational uncertainties

Timely
Be Timely so that the cadence of fielding is responsive to and anticipatory of the operational tempo of the warfighter

Primary Themes for Cyber Risk Reduction

Better Tools

Can we read the minds of malware authors?

Better Training

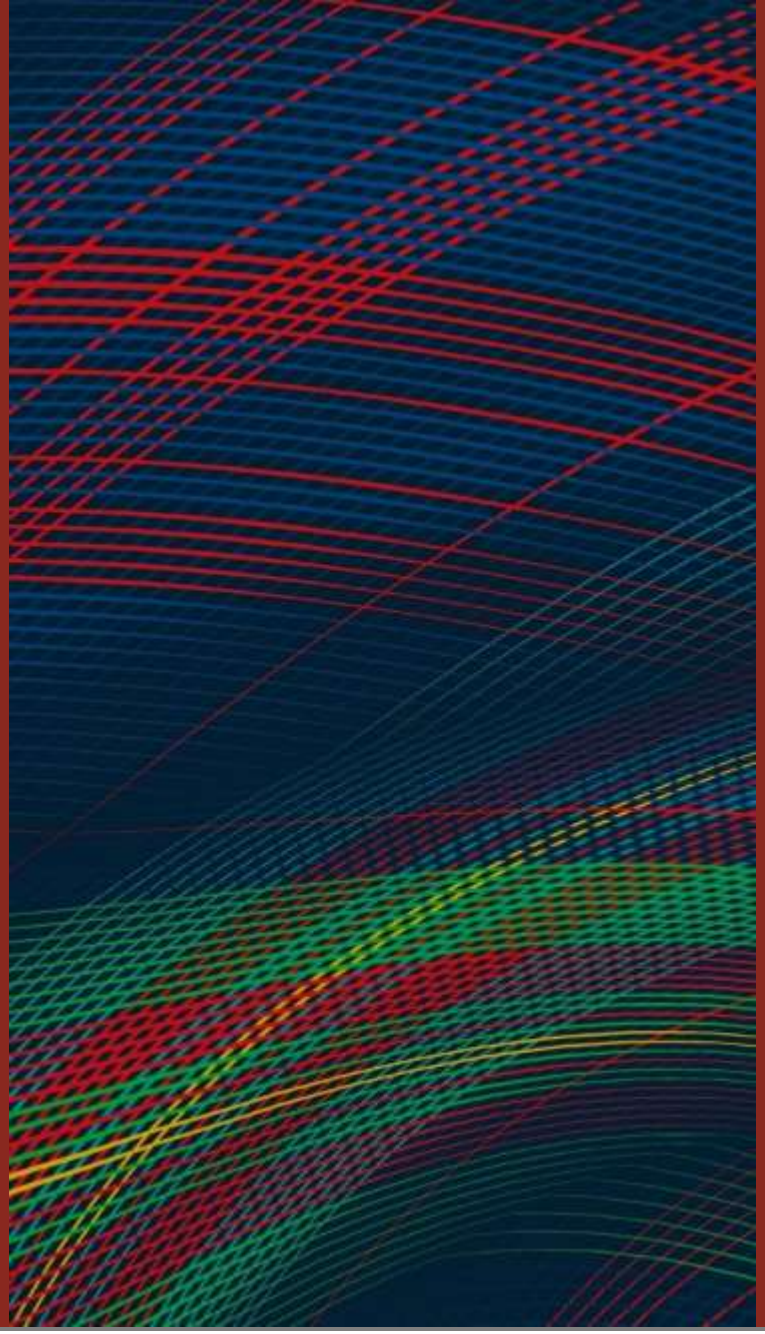
How do we bring the experience of an expert instructor to every trainee?

Better Policies & Practices

How do we handle the next Spectre or Meltdown?

Operational Cyber Risk Reduction

Better Tools



Better Tools: The Big Picture

Problem

Malware analysis and reverse engineering can be tedious and time consuming

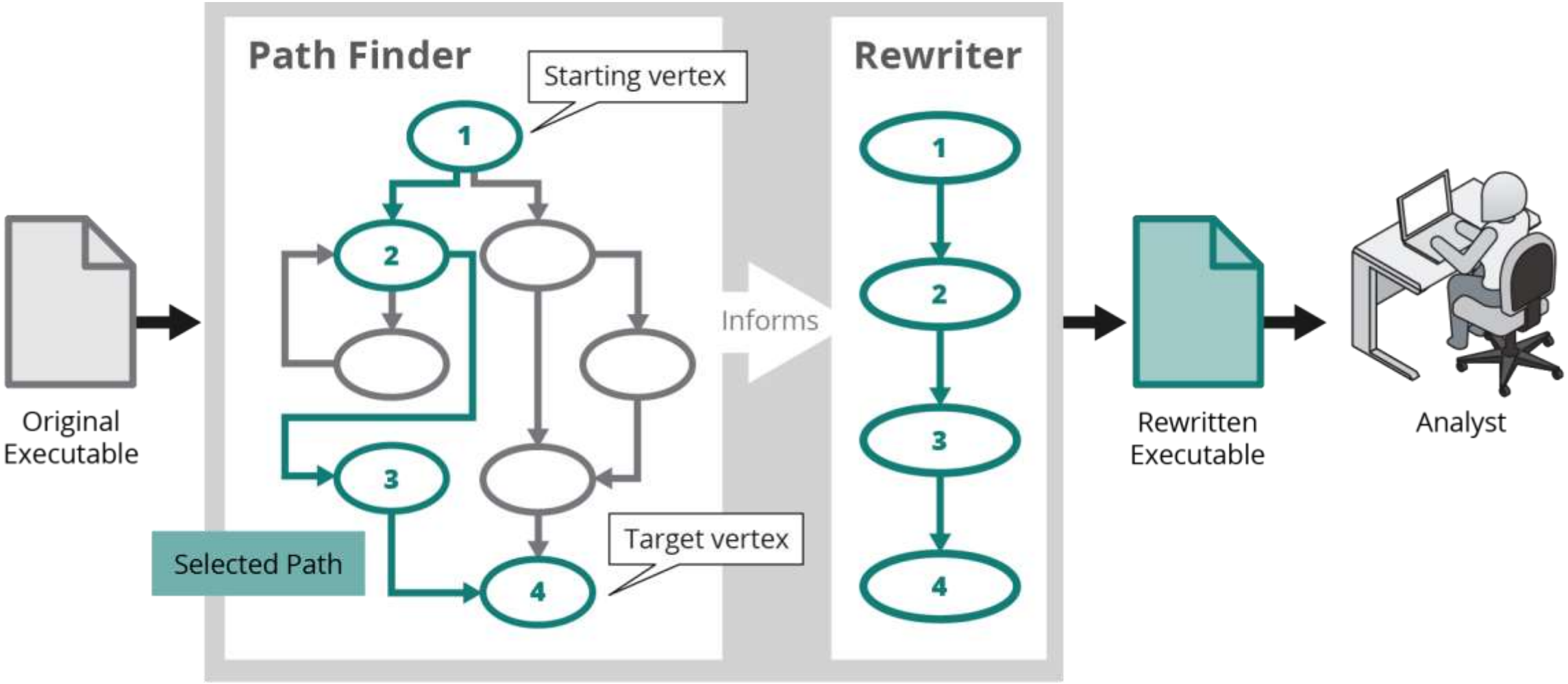
Solution

Help people better understand what executables do

Tools & Capabilities

- Pharos – Open source, automated executable analysis platform built on ROSE
  - Paper next week on recovering object-oriented structures from executables at ACM CCS
- Office of Naval Research, Total Platform Cyber Protection
  - Remove features (complexity) from executable (i.e., late-stage) software

Automated Executable Program Transformation



Recovery of Semantically Meaningful Variable Names

```
cp = buf;
(void)asxTab(level + 1);
for (n = asnContents(asn, buf, 512); n > 0; n--)
{
   printf(" %02X ", *(cp++));
}
```

Original Source Code

```
v14 = &v15;
asxTab(a2 + 1);
for (v13 = asnContents(a1, &v15, 512LL); v13 > 0; --v13)
{
   v9 = (unsigned char*)(v14++);
   printf(" %02X ", *v9);
}
```

Decompiled Source Code

What's Next?

Line-funded Strategic Initiative research project on path finding work in support of Office of Naval Research program

- Combine two approaches with different performance attributes
- Explore binary rewriting aspects of problem in 2019
- Partner with Dr. Arie Gurfinkel to apply PDR model checking algorithms to the problem

Two new LENS projects in 2019

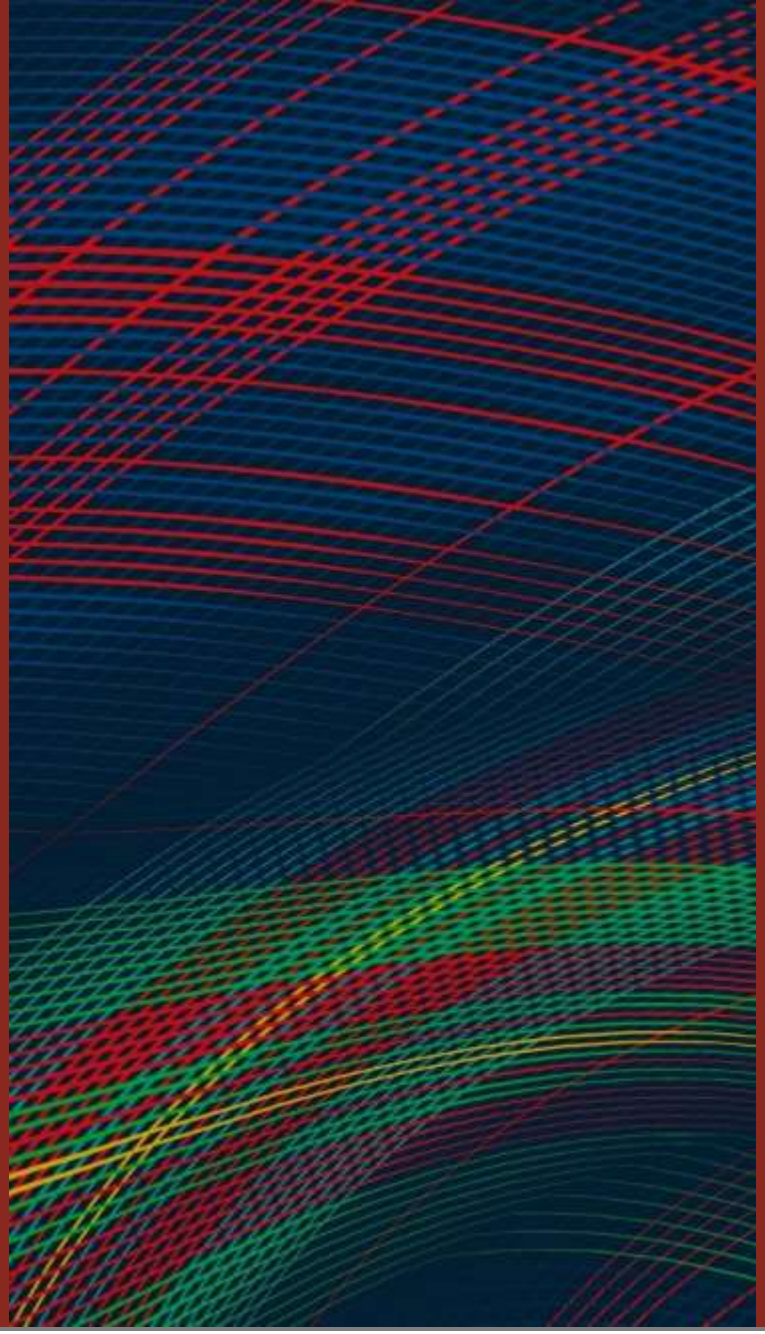
- Investigate accuracy and reliability of ARM executable analysis tools
- Examine efficacy of protections against code reuse (e.g., return oriented programming) attacks

Pharos executable analysis platform undergoing active development

- github.com/cmu-sei/pharos

Operational Cyber Risk Reduction

Better Training



Better Training: The Big Picture

Problem

There is a global shortage of cybersecurity professionals

Solution

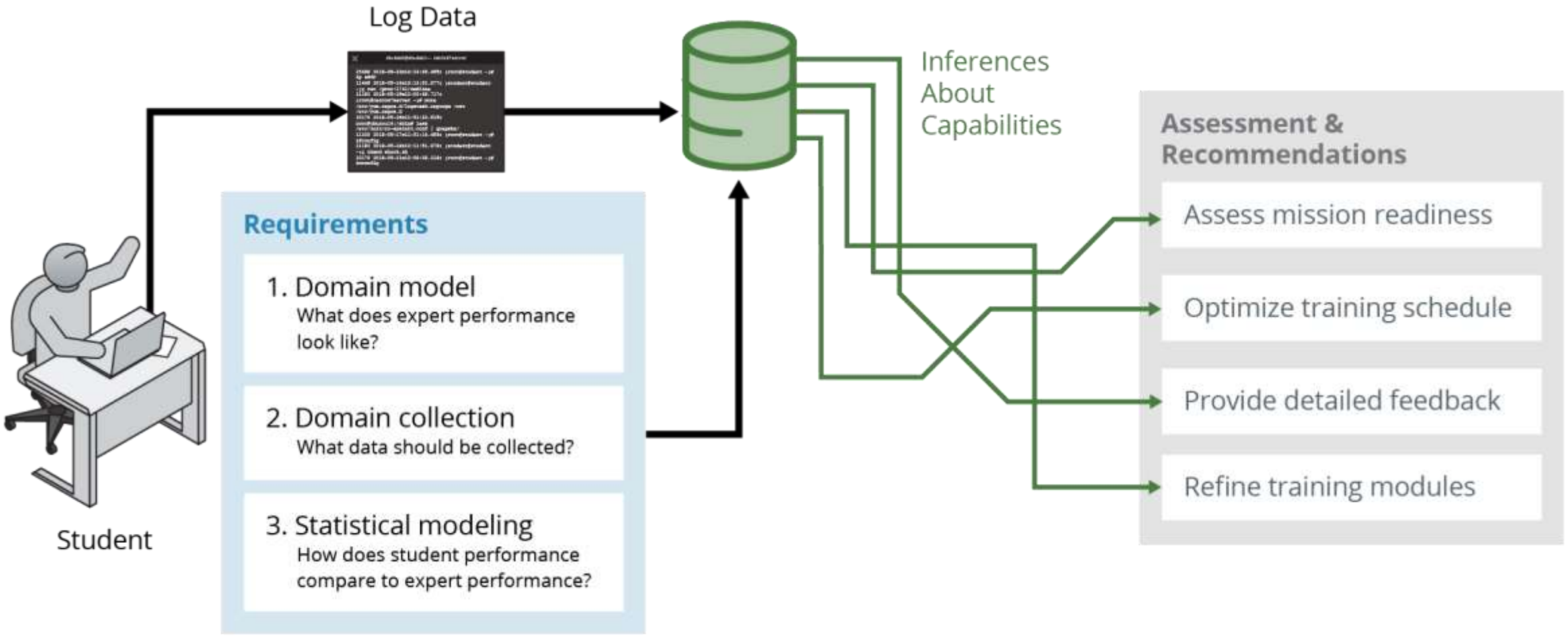
Train people more effectively, more efficiently

Empower DoD's Cyber Mission Force to "Train as You Fight"

Develop and transition cutting-edge prototypes and content

- training and exercise platforms
- modeling and simulation tools
- gamified, on-demand training

We are working towards



Richer performance data than ever before.

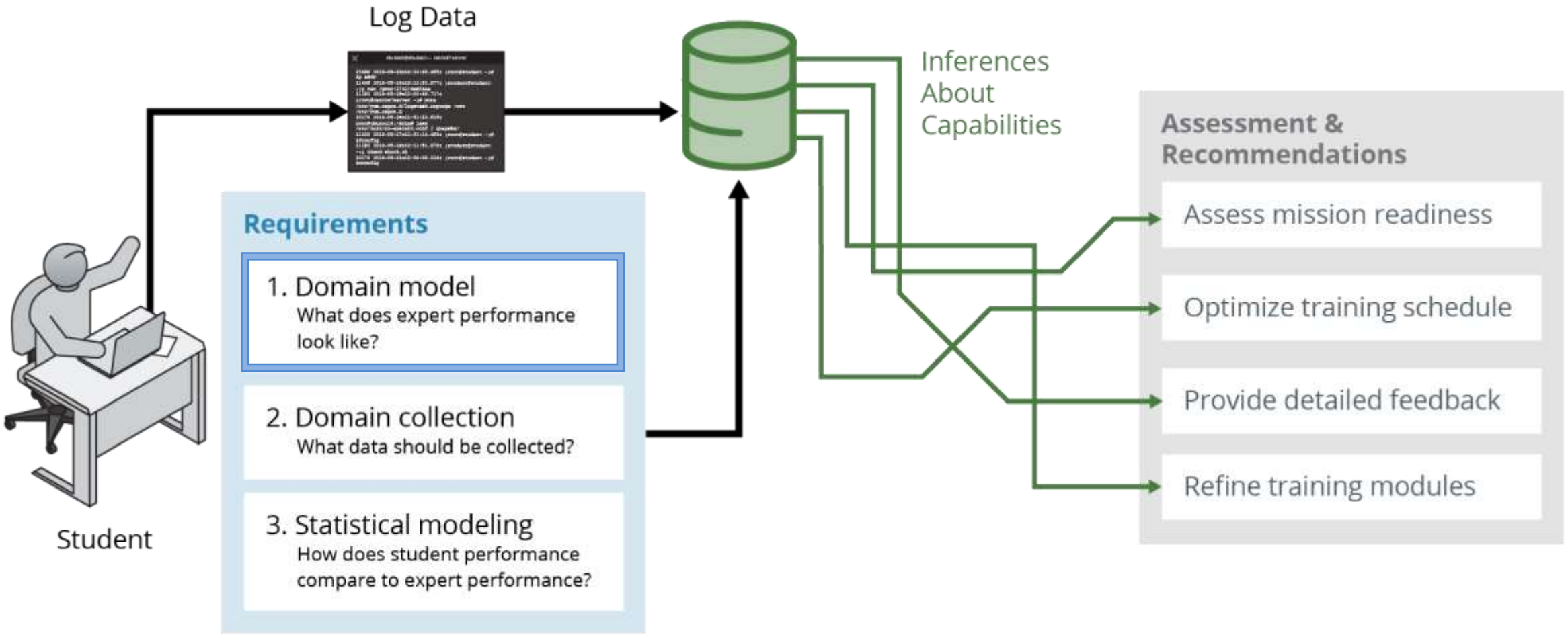
Current practice:

- Subjective assessment of mission readiness
- Multiple choice quiz.

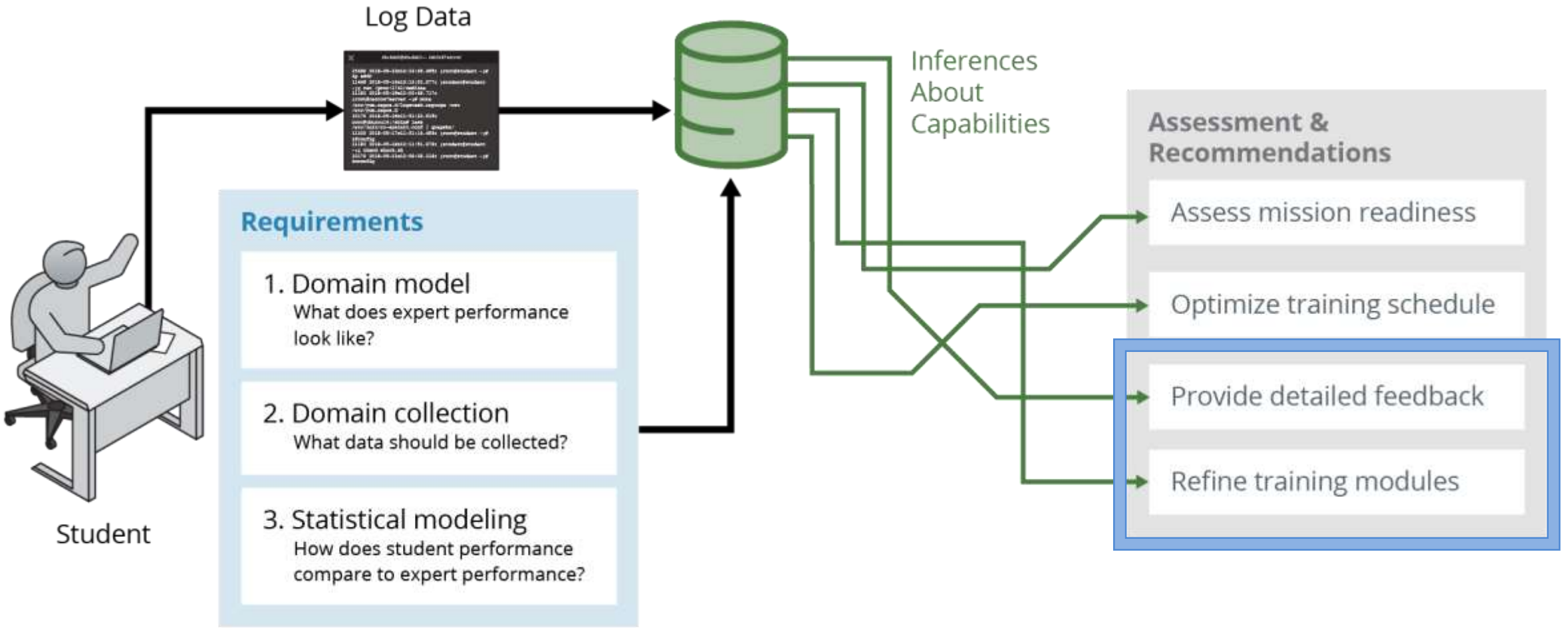
New:

```
11320 2018-05-17T11:51:14.499Z [root@student ~]        # ifconfig
11192 2018-05-18T12:11:51.879Z [student@student ~]     $ chmod shock.sh
10170 2018-05-21T12:08:38.318Z [root@student ~]        # iwconfig
10170 2018-05-22T11:44:05.817Z [root@student ~]        # ifconfig
11034 2018-05-31T12:13:08.082Z [root@student ~]        # rm -f /etc/udev/rules.d/70
                                                         -persistent -net.rules
```

Ongoing projects

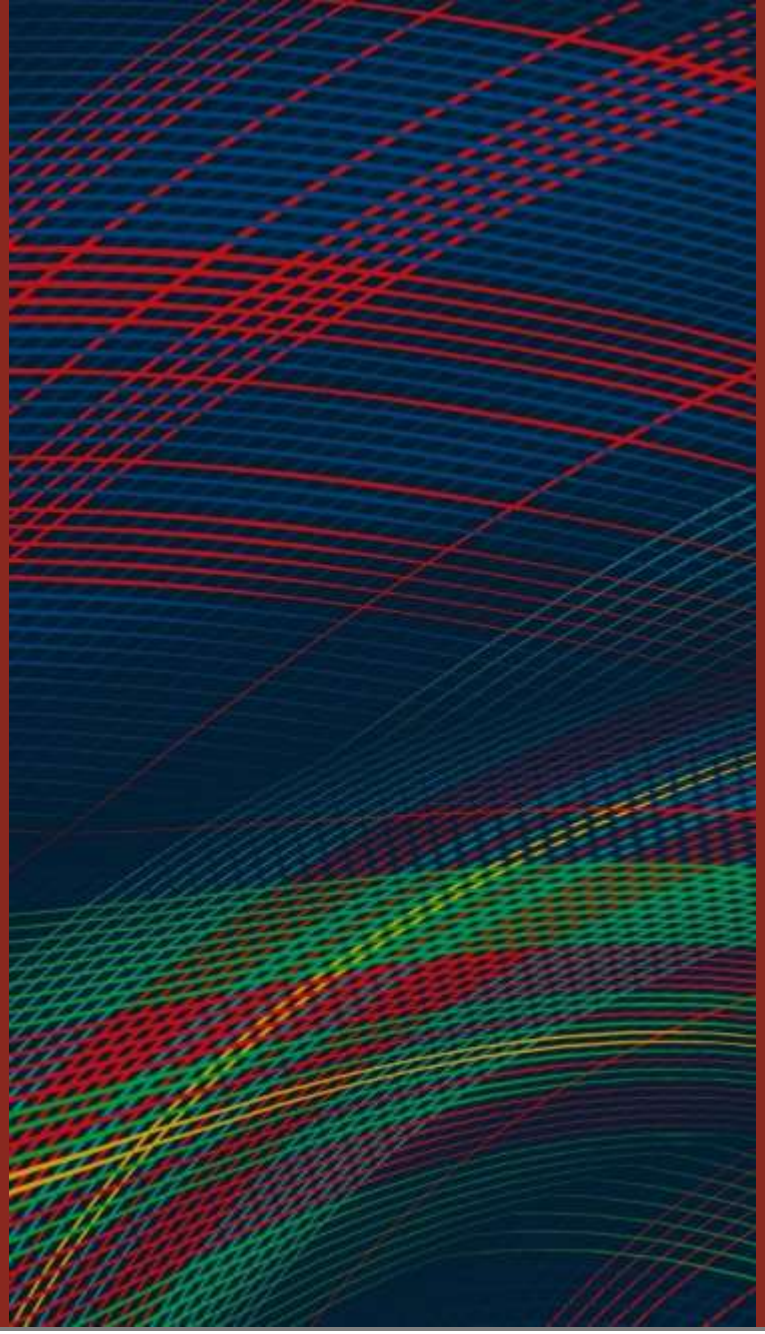


What's Next?



Operational Cyber Risk Reduction

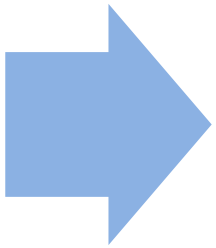
Better Policies and Practices



Better Policies and Practices: The Big Picture

Problem

Vulnerability remediation is a complex multi-factor and multi-party process



Solution

Establish and promote best practices for coordinated vulnerability disclosure

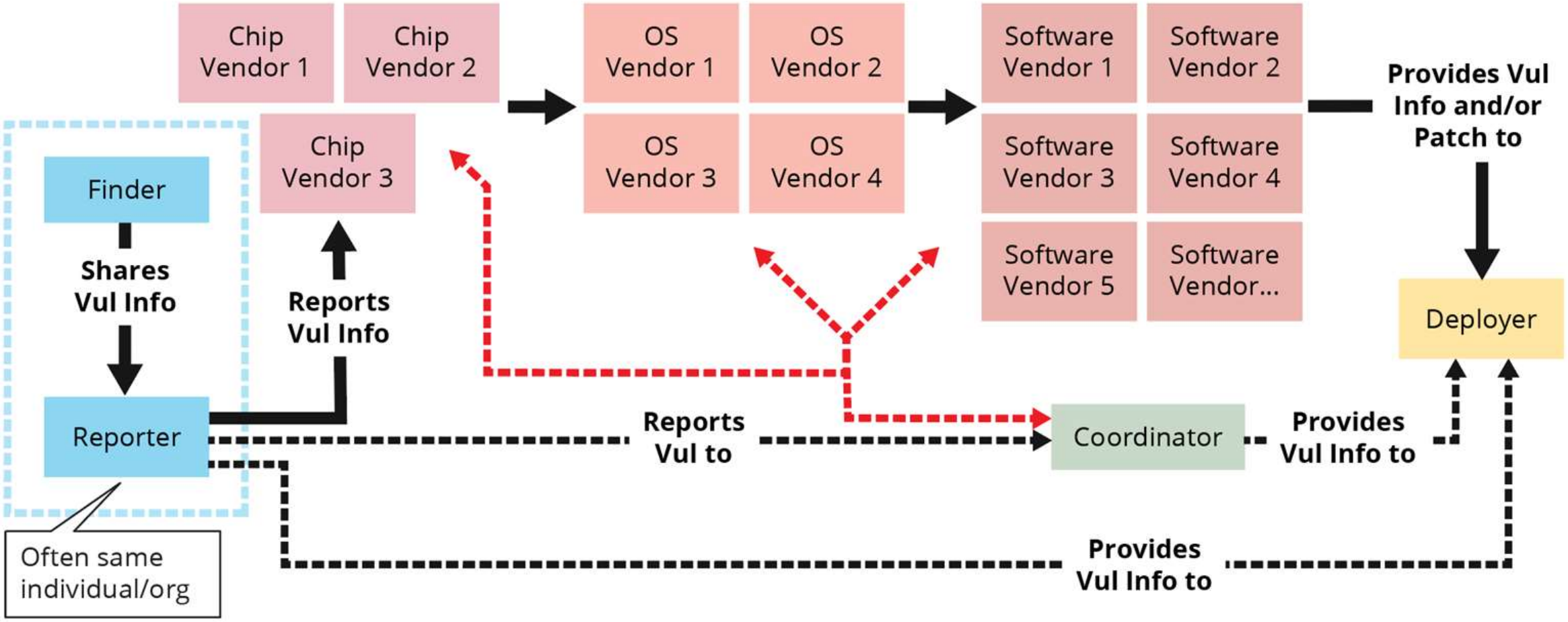
CERT/CC has set the standard for vulnerability disclosure practices for three decades

- *The CERT Guide to Coordinated Vulnerability Disclosure* (2017)
- Co-author ISO/IEC standards on vulnerability disclosure (29147, 30111)
- Chair of vulnerability coordination and Vulnerability Reporting and Data Exchange (VRDX) SIGs in FIRST
- Common Vulnerabilities and Exposures (CVE) board membership since CVE's inception

Current lines of work

- CVD and associated advisory services provided to the public under DHS and DoD (DC3) sponsorship

Multi-party Coordinated Vulnerability Disclosure (CVD)



Modeling the Operations of the Vulnerability Ecosystem

Goal

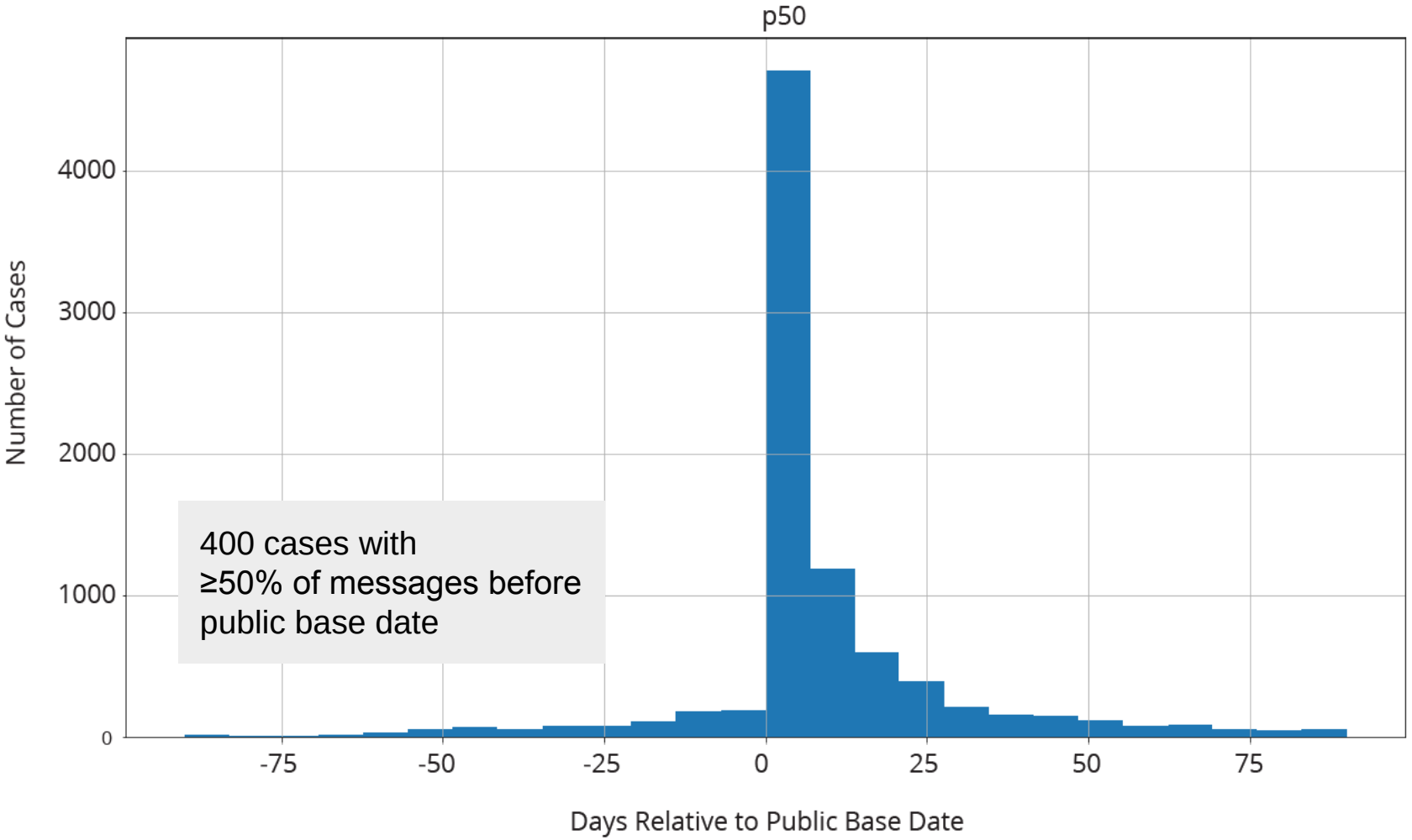
Identify factors that affect a successful coordinated vulnerability disclosure

CVD Data

- 46,000 vulnerabilities reported to CERT/CC from 1993-2017
  - 11,000 vulnerability reports were coordinated by CERT/CC
- Information included:
  - vulnerability description
  - all coordination emails
  - date made public (9,600 of the vulnerabilities)

CVD Workload Analysis

Case Midpoint Relative to Date Public

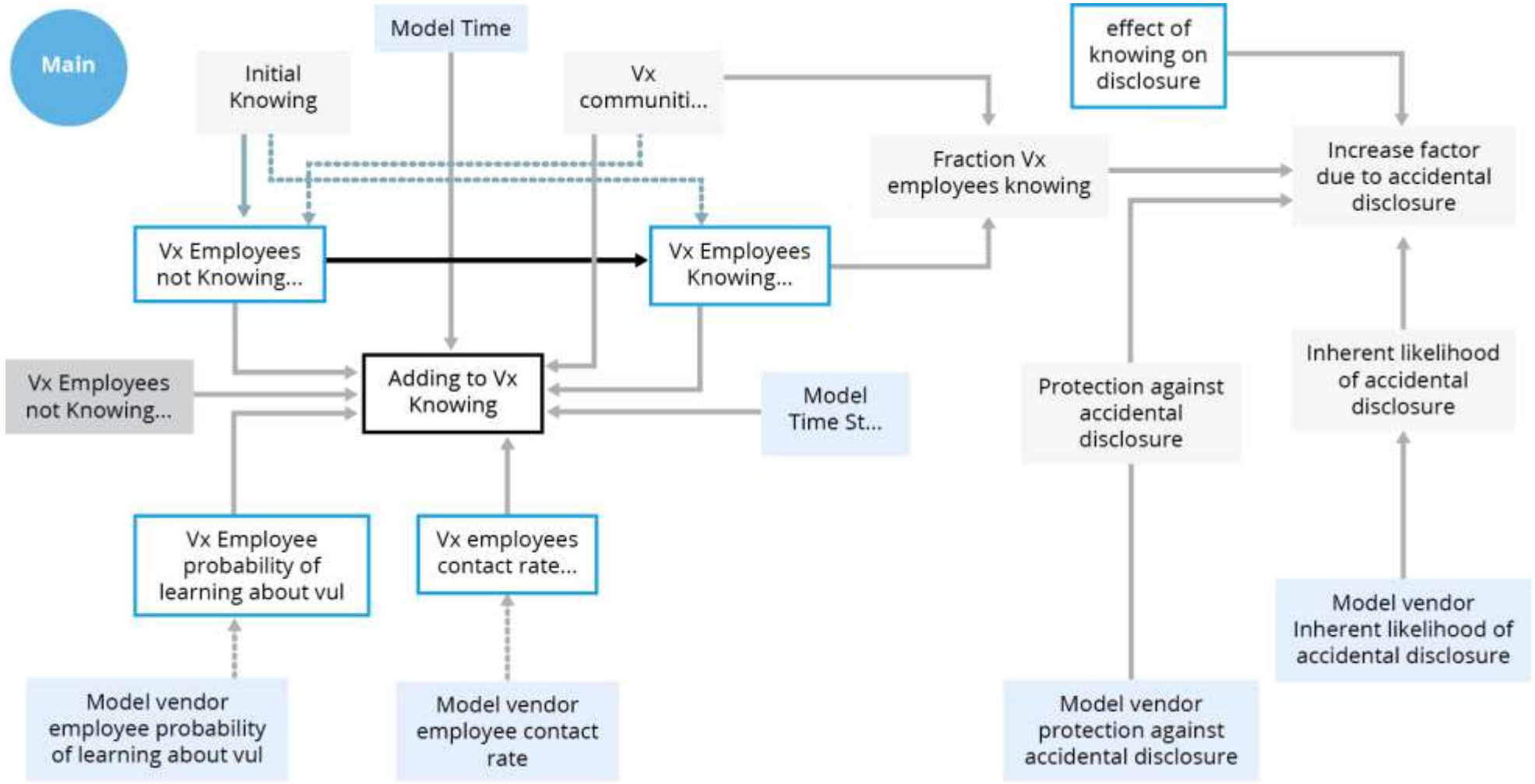


9,200 cases with
>50% of messages after
base date

Relative date on which cases reached 50% of their total messages

Public Base Date (PBD) = min(date_public, date_first_published)

MOVE: Modeling Embargo Success



Outcomes and Moving Forward

Multiparty CVD has gotten the attention of the Senate due to Meltdown and Spectre

- CERT guidelines adopted by Intel and Microsoft
  - cited in Congressional testimony
- Art Manion testimony before Congress

Update *CERT Guide to Coordinated Vulnerability Disclosure*

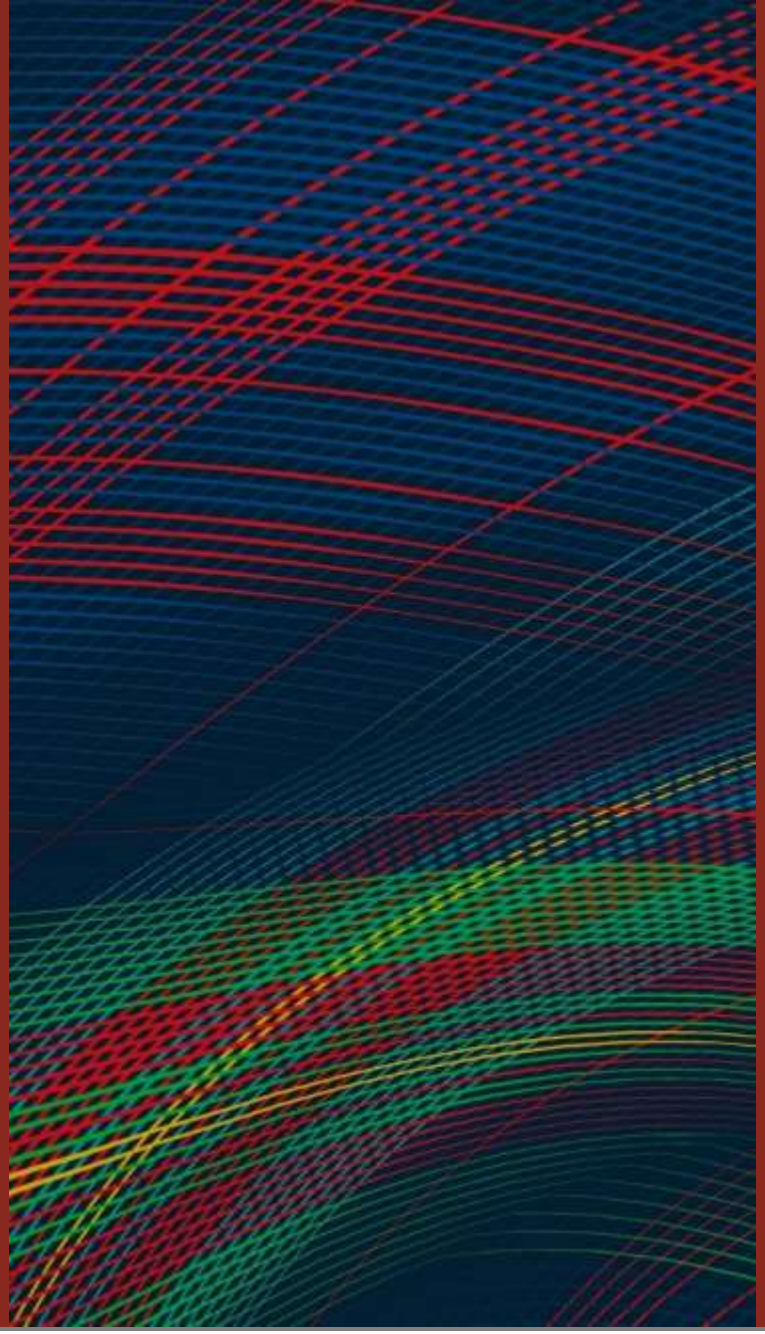
- planned for FY19
- responding to feedback and Congressional interest

Ongoing work

- CVSS is uncorrelated with actual risk
  - FY19: correlate risk with availability of exploits
- FY19: work with DHS and DC3 on vulnerability disclosure process and prioritization

Operational Cyber Risk Reduction

Summary



Goal: Field and Operate Resilient Systems

Better Tools

Can we read the minds of malware authors?

Faster, more meaningful malware analysis

Better Training

How do we bring the experience of an expert instructor to every trainee?

Build profiles of expert performance

Better Policies & Practices

How do we handle the next Spectre or Meltdown?

Improve and increase adoption of CVD practices

Resources

Binary Analysis

- Pharos — github.com/cmu-sei/pharos
- “Using Logic Programming to Recover C++ Classes and Methods from Compiled Executables” — edmcman.github.io/papers/ccs18.pdf

Coordinated Vulnerability Disclosure

- The CERT Guide To Coordinated Vulnerability Disclosure — resources.sei.cmu.edu/library/asset-view.cfm?assetid=503330
- ISO/IEC 29147 — iso.org/standard/45170.html
- ISO/IEC 30111 — iso.org/standard/53231.html
- FIRST Vulnerability Reporting and Data Exchange SIG — first.org/global/sigs/vrdx/
- FIRST Vulnerability Coordination SIG — first.org/global/sigs/vulnerability-coordination/
- Testimony of Art Manion to US Senate Committee on Commerce, Science and Transportation, July 11, 2018 – https://www.commerce.senate.gov/public/index.cfm/hearings?ID=77835497-EC96-41E8-B311-5AF789F38422