# A Introduction: Helping Faculty Teach Analysis Skills

According to published reports by the SANS Institute and other groups [**?**], the US faces a major shortage of security professionals to defend our information infrastructure from attack. In recognition of this need, security has been included as a core topic in the new IEEE/ACM CS2013 Curricula [**?**]. Cybersecurity is also mentioned in more than half of the other knowledge areas. At educational conferences such as SIGCSE and regional CCSC conferences, we are also seeing a growing interest in cybersecurity among faculty who do not have expertise in this area. Since it is still rare for schools to offer cybersecurity as an elective because of the tight constraints of the Computer Science curriculum, most schools do not have the luxury of offering a separate class in cybersecurity. Thus, the first step is to integrate it into other classes both at the upper and lower divisionial levels. We are seeing a growing concensus articulated in the CS 2013 Curricula and in the ACM report "Toward Curricular Guidelines for Cybersecurity" [**?**] to fully integrate cybersecurity into the Computer Science curriculum at multiple levels in multiple courses. The ACM report also highlighted some of the the obstacles, which include the lack of: standard curricula, opportunities for faculty development, and shared faculty resources.

Professors and instructors face a significant number of obstacles to providing students with realistic enough environments where students can safely develop these skills and mindset. Although a variety of curricular resources exist, most of them focus on very specific toolsets or traditional, well-understood types of vulnerabilities and exploits. Among the few "interactive" scenarios that do exist, documentation often does not adequately explain the security implications of the scenarios that students participate in. Even faculty with some experience in systems administration would need to spend a significant amount of time configuring the exercise, and it is generally not flexible enough to be adapted to their needs or wishes. In addition, we plan to offer a webinar for faculty on teaching an introductory Computer Security class. While the webinar addresses faculty with little experience in cybersecurity the EDURange framework address the needs of faculty who have significant experience as well. It will save them time in creating new exercises updating them afterwards, and sharing them with colleagues. Potentially, they could be used to create competitions for intra- and intermural competitions. This would attract mroe students.

For students, the process of analyzing the security properties of computer systems presents a variety of difficulties. Acquiring the mindset necessary to analyze and debug systems – and thereby understand how they can't be trusted, requires a level of engagement that most typical computer science (CS) undergraduate assignments lack and most typical information security courses do not have time for. Students are typically rewarded for following a formulaic trail: a sequence of commonly used tools. In addition, assessing students' analysis skills is difficult problem.

The **EDURange framework** for cybersecurity exercises has been successfully demonstrated in several venues: security classes at two liberal arts colleges, a graduate-level security class, and two workshops for faculty at major conferences. There has been strong interest on the part of faculty participants in using this platform in their classes. The design goals are:

1. engaging for the students
2. easy to assess by faculty
3. easy to configure
4. exciting for the faculty, so that they will be engaged and will recommend them to colleagues

However, one of the potential barriers to distributing EDURange to them is getting faculty to use the hosting environment. EDURange is currently hosted on Amazon's AWS/EC2 virtual cloud environment. This has made it very easy for the PIs to use it in workshops anywhere without having to worry about

installing special software. There are no plugins; the participants only need an ssh client, e.g. PuTTY on Windows. One method for distributing exercises to other faculty would require that they create an Amazon account with their credit card and potentially require their students to also sign up for accounts. We propose lowering the barrier for entry in three ways:

**First**, by creating an umbrella account in which we could enroll faculty and their classes. This facilitates distribution of EDURange and the abililty to provide direct technical support. We have a verbal agreement with Amazon to do this. Currently, we are using an educational grant to provide free service to our alpha-testers.

**Second**, we propose to provide a "help desk" which could guide faculty through any difficulties in setting up exercises and using the AWS interface. From one of our recent workshops, we saw that some faculty felt that they needed more than a three-hour workshop to prepare them for using this environment in their class. We may need to help faculty who are not familiar with AWS or the EDURange framework to set up exercises. Our solution to this problem is to have a team of undergraduates who would staff an online help desk and answer questions ranging from how to set up key authentication, launch VM instances, run scripts to how to modify existing exercises or use them as templates for new exercises.

**Third**, we will run an online course/webinar for faculty on how to teach an introductory cybersecurity course using EDURange and other online resources. The ACM Cybersecurity Guidelines report [**?**] recommended three MOOCs, but there are reasons why a webinar would be more successful in this case. We have already talked with faculty from other schools who teach cybersecurity, and they are interested in working with us to use EDURange in at least one class, share their syllabuses and help deliver this online course. We have talked with Corrinne Sande, a PI for Cyber Watch West, and we would be able to offer this webinar through their agreement with Webex. Instructors who sign up for this course would learn to use EDURange to enhance their curriculum and create new curricula for their classes, which could range from a standard introductory security class to including some security in other classes, e.g. Networking, OS, Database systems, Computer Organization and Programming Languages. We will provide access to EDURange for free to the instructors and their students. It is an open-source project.

Our vision is that EDURange would provide a vehicle for all Computer Science faculty to *address the goals of the IEEE/ACM CS2013 Curricula* report by translating the Information Assurance and Security (IAS) core concepts and outcomes into concrete examples. There are three interconnected activities of this proposal: further developing the EDURange framework to enhance its capabilites for dissemination and assessment, providing support for faculty development through webinars and a rich collection of interactive exercises, and providing a research opportunity for students to work on developing EDURange and to work with faculty who are using it in their classrooms.

**Outcomes** If funded, the outcomes of this project will be:

1. EDURange will be used in over 80 classes at two- and four-year colleges and universities.
2. Faculty at these schools will be able to assess their students on topics in the CS2013 report using EDURange and associated materials.
3. EDURange and associated activites will enhance teaching capabilites and enhance faculty expertise.
4. EDURange will produce a concrete realization of several of the CS 2013 IAS-related Knowledge Units with respect to cybersecurity concepts, skills and learning outcomes.

## A.1 Analysis and the Security Mindset

As security educators, we are motivated by the desire to teach analysis skills and concepts to our students. Analysis skills are fundamental to the security mindset. The security mindset implies the ability to understand a system both from the standpoint of a builder and an attacker. Thus, the security mindset provides the conceptual underpinnings for a student to reason in both defensive and offensive situations. One aspect is failure modes, i.e. how can systems fail and be made to fail. These are things that a defender or attacker needs to keep in mind. Another aspect is questioning and verifying assumptions. This is particularly relevant for the defender.
We want to support courses such as the CS2013 exemplar: "The goal of this course is to introduce students to the challenges, approaches, and techniques for implementing, deploying, and maintaining secure computing systems and networks. The rationale behind this course is to meet the need for information assurance content within the CS curriculum at the same time as tailoring to the diversity of potential career paths in the program's student population." [**?**]

The panel presentation by the authors of the ACM report at SIGGCSE 2014 included the fact that out of 67 Ph.D. recipients in security in 2013, only one joined the ranks of faculty who teach. In addition to providing opportunities for faculty development, we want to interest our undergraduates in becoming cybersecurity educators at the undergraduate and graduate levels.

### Related Work

EDURange provides a unique infrastructure that enables faculty to develop exercises for students, in which they interactively develop their information security analysis skills. Information security education has been a popular, well-studied topic. Preparing a large cybersecurity workforce seems to be a national priority, but emerging viewpoints [**?**] seem to suggest that most efforts to date have not been as effective as government and industry seems to need [**?**]. ** is this still true? ** GovTech.com suggests that there is a "lack of faculty at the university level who can teach cyber-security beyond its "soft side" including policy and analysis."[1]

We believe that we have identified an interesting and previously underexplored approach to enabling students to understand and apply principles and patterns (particularly dealing with the composition of trust). The challenge that we are facing is how to make it more broadly available to faculty and their students.

Judging from the Birds of a Feather sessions on Security at the last two years of SIGCSE, there has been a modest increase in the number of hands-on cybersecurity exercises, not all of which address the security mindset. It is also clear from the workshops we have attended that faculty want to use them but are frustrated because of the difficulty in disseminating and setting them up. The other frameworks that we have tried have some good features that we can emulate and some limitations that we try to avoid

2. Frameworks for Security Labs
DETER, werewolves, RAVE These environments are fine, except that with RAVE, new scenarios and VMs need to be installed by the developers. A faculty member can work with the developers to create new configurations an exercises, they can't just upload some VMs and try them out.

Currently there are a few frameworks for

## A.2 Comparison of EDURange with Existing Projects

As we detail in Table 1, EDURange provides several unique and distinct experiences from existing cybersecurity labs, exercises, and curricula. The PacketWars project is probably the closest existing piece of work

[1] `http://www.govtech.com/security/Cyber-Challenge-Work-Force-041811.html`

to what EDURange proposes, and there has been some work on providing students with access to "live" exercises on a small scale [**?**].

Table 1: *A Summary Comparison of EDURange and Existing Projects.* EDURange focuses on developing analytical skills and understanding system and network failure modes. The table below is not a criticism of existing efforts, but meant to highlight the ways in which our plans for EDURange differ from the characteristics of existing projects – these projects may have been built with different criteria in mind.

| **Project** | **Primary Disadvantage** | **Best Feature** |
|---|---|---|
| Cybersiege | shallow analysis | interactive training scenarios |
| SEED | lacks competitive interaction | comprehensive documentation |
| Security Injections | focus on defensive coding patterns | introduction to basic security |
| CCDC | requires travel; limited remote access | interactive and competitive |
| PacketWars | requires travel; limited availability | contains well-structured scenarios |
| ITSEED | minimal instructor support, distrib by flash drive | good documentation for students |
| Google Gruyere | narrow focus (web apps) | cloud-based; well-documented |
| Security Knitting Kit | not distributed | ?? |
| The RAVE | not very flexible | cloud-based; existing lab manual |
| Seattle Testbed | limited in scope | easy-to-use; well-documented; P2P |

Some of the projects listed in Table 1 seem to have different educational goals in mind. For example, while Cybersiege from Naval Postgraduate School provides a video-game-like, interactive environment, the decisions asked of a participate are mainly requisition and provisioning decisions rather than problems requiring technical analysis skills; this difference speaks to a different training goal. Google's Gruyere is a great example of an interactive, well-documented, scalable cybersecurity exercise, but it only covers the space of web application vulnerabilities. Towson's "Security Injections" mainly focus on several important security programming patterns. While the SEED material from Syracuse presents a mature, well-documented set of exercises, they are not typically interactive or dynamic. Competitions like CCDC seem to be structured in such a way as to require travel to the competition; EDURange envisions a publicly-accessible platform where even remote parties can interact. The RAVE is set up for a specific set of exercises, which are not interactive according to our definition. It is provides good isolation, so that it would be very difficult for a student to gain access to the Internet from the RAVE environment. On the other hand, it limits the insructors in the same way, making it impossible to modify the configuration except through a request to the RAVE developers.

### A.3 Information Security Education

Our philosphy on information security education is based on our work on understanding and teaching the hacker curriculum [**?**] to students. This approach is predicated on the utility of failure modes — rather than teaching students the "success" cases, we attempt to deliver a culture shock that makes them disrespect API boundaries and adopt a cross-layer view of the CS discipline [**?**]. We routinely encourage our students to adopt a dual frame of mind when solving problems [**?**] to prevent artificial abstraction layers from becoming boundaries of competence [**?**].

## EDURange in the Cloud

One of the ways in which EDURange is unique is that it applies Cloud technology to addressing the unmet need of supplying faculty with interactive cybersecurity exercises in a way that is both easy-to-use and flexible. EDURange allows instructors and designers to specify exercises at multiple levels of detail. Using $yaml$ as an intermediate representation, one can specify the structure of an exercise. This intermediate representation is compiled into API calls to AWS to create virtual machines and Chef scripts to install software. The portability of Chef should make it possible to port EDURange to other VMMs such as OpenStack, VSphere, etc. Since $yaml$ is a declarative representation, we need something procedural or object-oriented at a higher level. Bryan Fite [**?**] has identified six types of entities that appear in cybersecurity exercises and competitions:

1. Node, e.g. a VM with attributes which could include players with accounts on that node
2. Network, collections of nodes and the connections among them
3. Software, which is necessary for the correct functioning of the exercise with attributes including version numbers.
4. Constraint, e.g. time limit, bandwidth limit
5. Goal, i.e. learning objective. These can be specified at a low level, such as reading or creating an artifact, reporting an IP address or password.
6. Artifact, e.g. a file that is placed on a target and could be used as evidence of achieving a goal

The next lower level of description is in terms of a $yaml$ file which contains: groups, users, roles, which are also attributes, and packages, which refer to Chef scripts.

With the publication of the IEEE/ACM CS 2013 Curricula and its inclusion of computer security and information assurance, we are redirecting the exercises in EDURange to address the concepts and learning outcomes described in the IAS Knowledge Area. Since those are still at a high level, we hope to contribute to the implementation of the standards by providing concrete examples of exercises and a webinar on how to use them. We recognize that there are two groups of faculty who are our targeted audience: (1) Those who "just want an exercise"/inexperienced, and (2) those who are experienced and want to create a new variation of an exercise for their classes, a competition. or training for a competition. They want access to the configuration.

One of the issues that we have dealt with is the safety of EDURange on AWS. We want to have confidence that a student would not be able to connect to the Internet either accidentally or intentionally through one of the player Nodes. We were able to find a solution to this problem, which we confirmed with Amazon's Web security team.

### EDURange Exercises

There are several examples of exercises that could be implemented in EDURange, and a few of the following have been. Two methologies have been tested: (1) Create a VM manually, and then script it in Chef, and (2) start with a Chef script that was approximately what was needed and iteratively modify it.

#### Recon I

Recon I is a reconnaissance exercise, where students learn how to explore a network. The learning goals for this exercise are:

1. understand networking protocols (TCP, UDP, ICMP) and how they can be exploited for recon.
2. develop the security mindset
3. understand CIDR network configuration and how subdivide a network IP range.
4. use nmap to find hosts and open ports on a network.

Concepts from CS 2013 addressed by this module:

1. risk, threats, vulnerabilities, and attack vectors.
2. network security

This exercise is relevant for both defensive and offensive roles. It currently has one level of difficulty, and we have used it in several workshops.

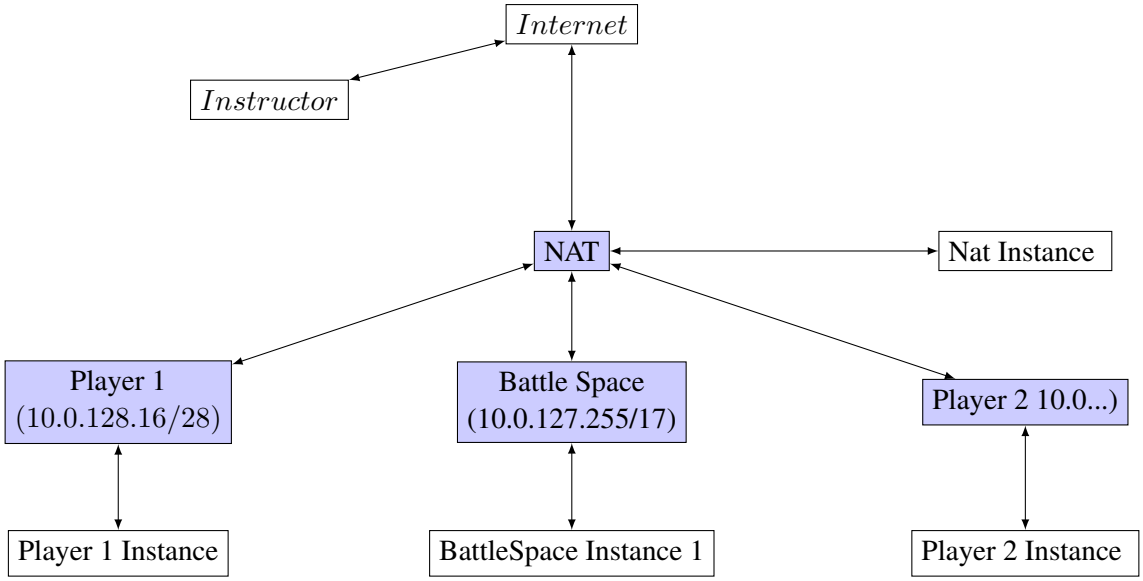


Figure 1: Conceptual diagram of the Recon I game. Note subnets are shaded (blue)

There are a dozen hosts on a remote network, and the student tries to find all of them as quickly as possible, and discover what what ports are open and what services are running. At the knowledge level, the student is learning to use nmap and what options it uses. At a higher level, the student is learning about the TCP, UDP and ICMP protocols and how they can be used in ways that may have not been intended. In more advanced versions, students look for hosts and services that should not be on the network.

EDURange provides the capability to run the same basic scenario, changing the IP addresses and open ports of the target hosts. This allows students to repeat the exercise while trying different options of nmap to find those that meet the goals of a particular variation of the exercise. For example, the instructor might ask students to focus on speed or stealth.

**Elf Infection**

Students are given a VM where one of the utilities is infected and listens on a port to open a reverse shell. They must figure out which program is infected and what it is doing. The learning goals are:

1. understand elf format
2. develop the security mindset
3. distinguish between normal and suspicious behavior of programs.
4. use nmap to find hosts and open ports on a network.

Concepts from CS 2013 addressed by this module:

1. risk, threats, vulnerabilities, and attack vectors. It shows how how an attacker could maintain control of a system or exfiltrate data through infected binary files.
2. network security. The infected software will open a port and send packets to a remote server.
3. trust and trustworthiness.
4. machine-level representation of data

**strace**

Students are given a trace of system calls made while a few programs are running simultaneously. The trace is cleaned up to remove the names of the executable files. Advanced versions can include malware.

The learning goals are:

1. understand how to sort through complex data
2. develop the security mindset
3. distinguish between normal and suspicious behavior.
4. use strace to characterize aspects of program behavior.

Concepts from CS 2013 addressed by this module:

1. risk, threats, vulnerabilities, and attack vectors.
2. trust and trustworthiness.
3. digital forensics

**scapy hunt**

Students craft network packets to detect hosts that are not visible directly on the local network. They observe packets and replaying them with modifications. They gather more infromation by overflows the forwarding table and port knocking.

The learning goals are:

1. understand firewall rules
2. develop the security mindset
3. understand routing tables
4. understand how IP works

Concepts from CS 2013 addressed by this module:

1. risk, threats, vulnerabilities, and attack vectors.
2. network security
3. Access control

**Grammar Fuzzing**

This is an attack/defend exercise, where the defender implements a recognizer for a grammar, e.g. a grammar describing the input to a calculator. The attacker can look at the code and designs input that either creates false postives or false negatives.

The learning goals are:

1. perform input sanitization
2. develop the security mindset
3. understand language security (langsec) [**?**]

Concepts from CS 2013 addressed by this module:

1. risk, threats, vulnerabilities, and attack vectors.
2. language translation

### A.4 Addressing CS2013

Here are the concepts and learning outcomes from CS2013 that we will address:

We will produce additional exercises that will address these goals.

Producing new knowledge about what works effectively. In addition to providing a framework for developing exercises at a high level, but we can also import VMs that collaborators produce. We are putting together this service in AWS which we make available to instructors. This doesn't use the full power of EDURange, but rather is based on the fact that we are providing a service through an AWS account where we can make The EDURange framework provides an easy way to share exercises. Every time we have run a workshop, we have given surveys and received good suggestions on ways to improve the exercises.

## Activities

main purpose of activities is to support faculty development; they need to incorporate security development into a wide range of courses, and therefore they need more context. All activities are aimed at supporting this goal (and these outcomes).

We will bring together a wide range of experts who teach this stuff on a regular basis (plus their students) and we will put together exercises that are specifically mapped to CS 2013 and specific implimentations of their security curriculum...catar a la carte menu to fauclty that don't have that experience.

**Ongoing Activities**

Monitoring and maintanece of EDURange cloud infrastructure as hosted by Amazon. Support for mailing list and community building activities (twitter, etc.?)

Ongoing support for EDURange infrastructure; possibly matched by Amazon

Student-based activities * help desk: direct support our faculty audience/clients; opportunity for professional development: super TA/student aide

purpose is to twofold: close that last small gap in access (give faculty member comfort and confidence)

How do we control access? Faculty needs to commit themselves and students to participating in our assessment (see Section 5) then on FCFS basis, we will offer a student 1, 2, or 3 times? We don't have capacity to help everybody in face-to-face premium mode, they can get the mailing list asychronous support.

Platinum EDURange partners.

"1 out of 64 students went into teaching": gives student opportunity to develop teaching/education technique...apprentice model, exposure to a variety of professors and classroom environments...we don't teach grad students how to teach...this is an opportunity for practical training and course and curriculum management, development, experiential learning for our student...valuable experience for undergrads, also a variety of experience...they are not just pounding out code.. they act as a valuable external resource/expert to the faculty member they are helping.

* module development, multiple benefits to student researchers: pratical hands-on experience in systems and cloud and security, plus develop an appreciation for cybersecurity curriculum development as experssed in CS 2013.

Faculty-based activities

* design and run webinar (plan out curriculum) act as resource faculty audience; offering skeleton of an intro infosec course; cadre of instructors (panel of experts) will be given stipends to support their involvement * piazza * G+ youtube

* money for workshops at SIGCSE where we demo EDURange for attendees — this is place to get feedback; this activity feeds into our assessment and development (they give us ideas, VMs, exercises). Contact/face time target audience.

* guide students and help design scenarios; major elements, maps elements to CS2013, and we will offer documentation (we are the best people to write this b/c we are faculty members...include notes for faculty on the scenario motivation, formative and summative assessments, description of how it maps to CS 2013, how to best use it, keywords/topics, learning objectives, provides default context and possible suggestions for integration into non-security courses.

development of new scenarios and exercises. - take other people's exercises, make accesible - create new exercises of the EDURange style

Are we going to create student assessments? We will do that for a small number of exercises that we create. Our goal is to create the framework for creating assessments. we will not be the only ones creating exercises in EDURange

the webinar; the course template outline...make the point that the course is an example educational environment where EDURange can be mapped to or used.

a section on the EDURange "help desk" (another core expense item)

## Assessment Plan

Answer the question: how will we demonstrate this enhanced value? Raw numbers, plus qualitative application of CS 2013. Demonstrate how much people use EDURange now that they have open access to it.

Assessment Plan – this section will have 2 sub-parts. One on raw metrics of number of users, students, profs, classes, etc. etc.

NB: any discussion of the scoring engine in EDURange probably does not belong here; that is an EDURange I concern, not for this proposal.

The second is on how well the EDURange infrastructure and scenarios map to the skills and knowledge of security throughout the CS 2013 undergrad curriculum. Assessment plan describes the assessment mechanisms, procedures, and practices

First pillar: usage stats, drawn from EDURange and Amazon infrastructure. catelogue frequency and amount of usage per prof or class. How much was EDURange used in particular kinds of classes? Is there a difference in usage given the type of course (e.g., intro security vs. some other course vs. upper-level ugrad

vs. lower-level course). For example, we can say we are all things to all audiences, SecurityInjections may be more appropriate or used more heavily

Report attendance at webinars, downloads of YouTube videos, piazza conversations, etc.

Second Pillar: (a) faculty survey (same instrument as SIGCSE...) - * use this to drive improvement of EDURange: find disastisfied participants in early years, revise exercises and infrastructure along the way

(b) pre/post test on a per scenario basis. Need to have identified knowledge and skills on a per-scenario basis in modules.tex

Main focus is on how well this supports faculty in their job, not necessarily a measurement (assume, that faculty, if well-supported, will do appropriate assessment of *their* students given educational background and institutional standards, etc.), so we will try to do pre/post test and make available, but not main focus of our internal assessment.

Third Piller: How well/completely EDURange maps to CS 2013 infosec topics.

Timely and informed by central and guiding document of CS Ed, particularly since this document goes through great lengths to identify infosec topics throughout the curriculum.

How well does EDURange support / address the need of CS 2013 to weave CS infosec throughout the curriculum. And the faculty are best positioned to tell us this.

modules.tex is an assertion of the relationship between particular modules and particular parts of CS2013. The assessment plan here is based on how well that mapping succeeds in practice. This can be based on questions we ask in the faculty survey, but the *analysis* is broken out under this third pillar.

* how often were you able to use an EDURange scenario as a launch pad to discuss curriculum topic X, Y, Z?

* were there other curriculum topics, skills, or knowledge that it mapped to?

## Management Plan

Timeline of activities, milestones

recruiting students

### List of Milestones

1. organize first webinar
2. run first webinar
3. followup
4. Workshops (ongoing at SIGCSE)
5. SIGCSE, CSAW (highlight cooperation with others)
6. recruit students for helpdesk
7. training first batch of students
8. Deployment of EDURange at first three..five beta users (at end of year 1, in 5 classrooms, not including our institutions)
9. Midterm Assessment report (can comment on internal assessment as well as CS 2013 “reality” in our deployed classrooms) (state of cybersecurity)...beginnging of year 4

10. ??? Coordinate with Bryan Fite's Scenario Description Language: by the end of year 3, we will due diligence on identifying other cyberscenario description languages / standards
11. end of year of year 3, we will have distributed our 6 scenarios to ENSEMBLE; the rest in year 5
12. by the end of year 2, we will have incorporated one IT-SEED external scenario into EDURange

Also include "outcomes" into this list?

### Timeline

### Team Meetings, Coordination, Hackathons

### Dissemination

Audiences EDURange can be useful for novice and experienced instructors in cybersecurity.
CyberwatchWest
ENSEMBLE
workshops at CCSC, SIGCSE, SISMAT, courses, CSAW
also list previous dissmination efforts to demonstrate we've been effective at this

## Data Management

Describe how we will protect PII. Describe any IRB procedures or protocols or training (for PIs and students).

Describe how we will guard and care for and dispose of our experimental data.

How will we make our data and scenarios persistent? Upload into ENSEMBLE.

Aggregate assessment and reports will be available on edurange.org